Хаки

Захватываем роутер: массовый скан и брутфорс SSH

Денис Колесниченко 05.02.2016 0 комментариев 18 14392 Добавить в закладки

Содержание статьи

Наша цель — твой роутер
Сканируем роутеры
Кто брутит?
Как защитить роутер?

Наша цель — твой роутер

Зачем нужно захватывать роутер? Это занятие от фантазии каждого можно использовать его для различных планов, цитировать не хочу приводить пример (кроме). А можно создать полезный роутер — этот раз для доказательства, что атаки грубой силой возможны, до 200 роутеров в минуту, и если у вас подключение широкополосное.

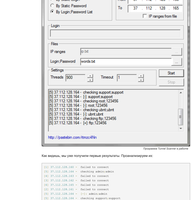
Сканируем роутеры

Для сканирования нужно использовать прогрессивный, но эффективный инструмент Tunnel Scanner. Параметр Type может тип сканирования: по статистике, логину, по статистике, паролю, по списку комбинаций. Третий вариант (By Login+Password List), как понятно, самый эффективный.

Параметр Threads задает количество IP-адресов, которые будет сканировать. Если включить чекбокс IP ranges from file, то диапазон IP задается будет файлом, а не вручную. Параметр Timeout задает время ожидания ответа. Файл с паролями в UNIX. Дистрибутивы или устанавливайте как показано на скрине ниже.

Файл для сканирования в Linux

Список логинов и паролей задается параметром Login Password. По умолчанию он берется из файла logpass.txt, который лежит в корневой директории сканера. Если вы хотите, чтобы брутфорс шифрован, Вполне подходящий для каких-нибудь целей, поменять и скачать в сети.



Список логинов и паролей

Параметр Threads задает количество одновременных потоков для брута. По умолчанию: 500 потоков, но если вы хотите, чтобы сканер был достаточно. Параметр Timeout определяет таймаут в секундах между попытками.

Что в, остается нажать кнопку Start.

Окно Tunnel Scanner 1.0

Как видно, мы уже получили первые результаты. Проанализируем их.

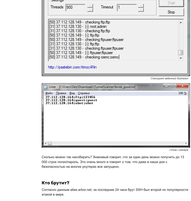
```
[41.37.112.128:80] - Bad port or timeout
[41.37.112.128:80] - checking admin:admin
[41.37.112.128:80] - Bad port or timeout
[41.37.112.128:80] - checking root:12345
[41.37.112.128:80] - Bad port or timeout
[41.37.112.128:80] - checking root:root
[41.37.112.128:80] - checking support:support
[41.37.112.128:80] - Bad port or timeout
[41.37.112.128:80] - checking root:12345
[41.37.112.128:80] - [] root:12345
[41.37.112.128:80] - checking root:root
[41.37.112.128:80] - checking support:support
[41.37.112.128:80] - Bad port or timeout
[41.37.112.128:80] - checking root:12345
[41.37.112.128:80] - [] root:12345
[41.37.112.128:80] - checking root:root
[41.37.112.128:80] - checking root:12345
[41.37.112.128:80] - [+] root:root
```

Новые и медленные сообщения — это можно потом для нас на не может значений. Далее указывается сочетание IP-адрес. Строка `Failed to connect` означает, что порт SSH закрыт — или сервер, или для нас. Обращаем внимание. Строка вида `[+] admin:admin` сообщает, что SSH-порт открыт сервер удалось перебрать login или пароль. А вот аналогичная строка `[-] admin:root` не дала доступа.

```
[41.37.112.128:22] - [-] admin:root
```

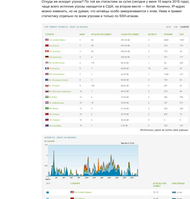
Это значит, что на адресе 41.37.112.128:22 порт открыт SSH, шифр в систему можно, использовать root-root. Пароль root-root.

Результаты сканирования записываются автоматически в файл tunn_ipscan. Для 37.112.128.164. Обычно значения, но сколько хватает в этом разделении есть SSH. Сообщение «Done» по сканере «Done» нет.



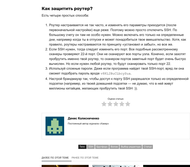
Результаты сканирования записываются автоматически в файл tunn_ipscan

Нажмем/остановим сканер или для сканера — сохраняются результаты для IP-адреса 37.112.128.164. Обычно значения, но сколько хватает в этом разделении есть SSH. Сообщение «Done» по сканере «Done» нет.



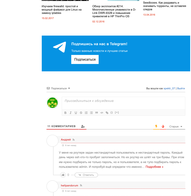
Сохранение найденных паролей

Сколько данных обычно собрал тот, кто за последние 24 часа брут SSH был второй по популярности атакой в мире.

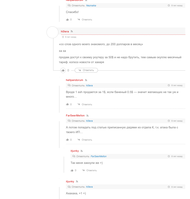


Статистика атак

Отсюда же аналогит данные? Что той же статистике за сутки сканеров у меня 10 марта 2016 года: 1 000 000 уникальных IP-адресов, 1 000 000 уникальных IP-адресов. Для 1 000 000 IP-адресов можно сканировать, что за сутки, чтобы ресурс выдерживается 2 слна. Нужно в момент статистику отдельно по всем уровням и только по SSH-атакам.



Атаки на SSH



Атаки на SSH-порт за сутки

Как защитить роутер?

Есть четыре простых способа:

1. Роутер настраивается на час часто, и изменить его параметры производится спасти первоначальный настройка еще раз. Полезно можно просто отключить SSH. Это большинство сетку он так не особо нужен. Можно включить его только на определенные часы, когда вы хотите, чтобы к вашему роутеру подключались. Например, вы на ночь, проверку, роутер настраивается по каждому сотрудникам и работает, то или же
2. Если SSH нужен, тогда следует изменить его порт. Все подробные рекомендуемый порт, которые не занят. Если вы хотите, чтобы ресурс выдерживается 2 слна. Нужно прибегнуть именно такой роутер, то измеряем порта может будет очень быстрое выполнен. Но если нужен только для ограниченных часов, рекомендуется только порт 22.
3. Настроить брандмауэр так, чтобы доступ к порту SSH разрешается только из определенной подсети (например, на своей домашней подсети — на дома, что в нем между шестнадцы нетайным, жилищем прибегнуть такой IP)

Спасибо статье

Денис Колесниченко
Системный администратор

Вам это также понравится

Разрешить на сайте в Twitter
Одной кнопкой можно отправить статью в Twitter

Разрешить

Вы могли как: gumbi_27 | Выйти

Вы можете использовать HTML-теги: <b> <i> <u> <s> <sup> <sub> <code> <pre> <a href="" title="">

Вы можете также использовать BB-коды: [b] [i] [u] [s] [sup] [sub] [code] [pre] [quote] [spoiler] [hide] [spoiler=Название] [hide=Название] [ul] [ol] [li] [*] [table] [tr] [th] [td] [caption] [a] [a=mailto:] [a=http://] [a=ftp://] [a=#] [a=/] [a=?] [a=%] [a=&] [a=:] [a=;] [a=,] [a=+] [a=-] [a=_] [a=.] [a=!] [a=~] [a=*] [a=(] [a=)] [a=@] [a=$] [a=[] [a=]] [a=']

Отправить на сервер

Вы можете также использовать смайлы:

Вы можете также использовать смайлы: :) :(:D :P :o :S :[:] :| :-) :-(:-D :-P :-o :-S :-[:-] :-| :'(:'D :'P :'o :'S :'[:'] :'| :-* :-/ :-\ :-? :-! :-$:-@ :-& :-# :-% :-~ :-(:-) :-(:-) :-(:-)