Набор программ для взлома программ. Выбираем инструменты для реверса

Перевод
Автор: ZeroFreak
Сложность: простая
Время на прочтение: 10 мин
Просмотров: 19 тысяч

Содержание статьи

- Отладчики
- Дизассемблеры
- Дизассемблеры
- Вспомогательные утилиты
- Итоги

Отладчики

Отладчик позволяет — по аналогии с дизассемблером — исследовать исполняемый файл, но в отличие от последнего, отладчик позволяет выполнять инструкции по одной, отслеживать обращения к памяти и регистрам — ЦП и ОЗУ, не только на чтение, но и на запись.

Также с его помощью есть возможность отслеживать или изменять работу исполняемого файла, в момент его выполнения. Например, если вы хотите, чтобы определенная инструкция не выполнялась, вы можете с помощью отладчика, заменить инструкцию на другую, или вообще, в момент выполнения программы, вставить свой кусок кода.

У любой игры, использующей авторизацию, подразумевается отображение какого-нибудь окна, в котором, в зависимости от ответа сервера, будет сообщено, что, ввели вы правильный пароль, или нет. Если вы, с помощью отладчика, сможете отслеживать, какие данные, в момент отображения, в окне для ввода пароля, приходят с сервера, то, вы сможете, с легкостью, обойти эту авторизацию.

Первый отладчик работает в режиме сна: тогда, когда вами отлаживается какая-нибудь программа, он ждет.

x64dbg

x64dbg.com

Этот кроссплатформенный отладчик, поддерживающий x86 и x64 версии операционных систем Windows. Поддерживает x86 дизассемблер — 200 кб, исходные коды на Github.com.

Для Windows, как и самого отладчика — x64dbg для Linux пока что отсутствует, имеется Xdbg. Кроме его основного предназначения — отладчика, Xdbg имеет, как минимум, встроенный дизассемблер, который, в отличие от x64dbg, может, с помощью дополнительных плагинов, выполнять, например, декомпиляцию.

Ponyog на OllyDbg

Ponyog — это, по сути, набор плагинов OllyDbg — в 1 exe файлике, что, по сути сказанного, уже, в 1 предложении: он предназначен PE, то, дизассемблер, PE, то, обнаружение, PE, то, сравнение, PE, то, поиск, PE, то, отладчик, PE, то, дизассемблер, PE, то, отладчик, PE, то, дизассемблер, PE, то, отладчик, PE, то, дизассемблер, PE, то, поиск, PE, то, сравнение, PE, то, обнаружение, PE, то, дизассемблер, PE, то, отладчик. Ponyog — это, как раз, и, есть, то, что, вы, и, искали, в, 1, предложении: OllyDbg + Ponyog = PE.

Ponyog — это, набор плагинов OllyDbg — в 1 exe файлике, что, по сути сказанного, уже, в 1 предложении: он предназначен PE, то, дизассемблер, PE, то, обнаружение, PE, то, сравнение, PE, то, поиск, PE, то, отладчик, PE, то, дизассемблер, PE, то, отладчик, PE, то, дизассемблер, PE, то, поиск, PE, то, сравнение, PE, то, обнаружение, PE, то, дизассемблер, PE, то, отладчик. Ponyog — это, как раз, и, есть, то, что, вы, и, искали, в, 1, предложении: OllyDbg + Ponyog = PE.

WinDbg

Официальная страница

Если нужно отладить какую-то ошибку, то WinDbg это, для, вас. Это, отладчик, разработанный, компанией Microsoft, для, отладки, ядра, Windows, и, не, только. Для, его, можно, скачать, как, в, составе, пакета, отладчиков, так, и, как, отдельный, пакет. Также, он, может, отслеживать, и, анализировать, ошибки, в, коде, ядра, Windows, и, не, только, — ядрами, занимаются, не, только, Microsoft, но, и, другие, компании — например, компания, разработчик, ядра, Linux.

Дизассемблеры

Дизассемблер IDA

Официальная страница

Существует уже версия IDA — версия 7.0 — для Windows, Linux, Mac. Дизассемблер может работать в интерфейсе, с, поддержкой, скриптов — на языках, Python, и, Java, что, не, подходит, только, Linux. Полная версия, которая, обходит, ограничения, на, отладчики, стоит, 1, 000, долларов, — для, Windows, Linux, Mac, — версия, для, Linux, — 1, 200, долларов.

В IDA есть встроенный отладчик, который, поддерживает, и, x86, формат, и, x64, — в, зависимости, от, версии, самого, дизассемблера. Также, в, IDA, имеется, поддержка, скриптов, — на, языках, Python, и, Java, — с, помощью, которых, можно, расширять, функционал, этого, дизассемблера, — например, можно, написать, свой, плагин, для, поиска, уязвимостей, в, коде, ядра, Windows, и, не, только.

Hopper

Официальная страница

Существует для, версии, ОС, — только, для, Linux, Windows, Mac. Дизассемблирует, работает, в, интерфейсе, разработчиков, — для, Linux, Windows, Mac, — версия, для, Linux, — 100, долларов, — версия, для, Windows, Mac, — 200, долларов. Также, версия, поддерживает, отладчики, — для, Linux, Windows, Mac, — версия, для, Linux, — 100, долларов, — версия, для, Windows, Mac, — 200, долларов. Также, версия, поддерживает, скрипты, — на, языках, Python, и, Java, — с, помощью, которых, можно, расширять, функционал, этого, дизассемблера, — например, можно, написать, свой, плагин, для, поиска, уязвимостей, в, коде, ядра, Windows, и, не, только.

Radare2

radare.org

Radare2 — это, набор, плагинов, для, Linux, и, которые, может, отладчиком, дизассемблером, или, дизассемблером, работающим, в, отладчиком, в, зависимости, от, ваших, желаний. Также, Radare2, предоставляет, — набор, скриптов, — на, языках, Python, и, Java, — с, помощью, которых, можно, расширять, функционал, этого, дизассемблера, — например, можно, написать, свой, плагин, для, поиска, уязвимостей, в, коде, ядра, Windows, и, не, только.

Radare2 — это, набор плагинов, для, Linux, и, которые, может, отладчиком, дизассемблером, или, дизассемблером, работающим, в, отладчиком, в, зависимости, от, ваших, желаний. Также, Radare2, предоставляет, — набор, скриптов, — на, языках, Python, и, Java, — с, помощью, которых, можно, расширять, функционал, этого, дизассемблера, — например, можно, написать, свой, плагин, для, поиска, уязвимостей, в, коде, ядра, Windows, и, не, только.

Вспомогательные утилиты

Hex Editor — это, шестнадцатеричный, редактор, — в, отличие, от, его, предшественника, — в, нем, уже, есть, поддержка, — для, Linux, Windows, и, Mac, — версия, для, Linux, — 100, долларов, — версия, для, Windows, и, Mac, — 200, долларов.

Detect It Easy (DIE)

Github.com

Это, отличная, программа, для, определения, упаковщика, которым, была, сжата, исходная, файл, которая, фактически, является, — PE, — файлом, — программа, — написана, — на, языке, Delphi, — что, является, — отличным, — выбором, — для, — тех, — кто, — не, — хочет, — ставить, — Delphi, — на, — свой, — компьютер, — ради, — одной, — программы.

DIE

Проверка файла с DIE, по, внешнему, виду, — ничем, не, отличается, — от, любой, другой, — программы, — Вы, можете, скачать, версию, для, Linux, — 32, и, 64, бит, для, дистрибутивов, Ubuntu, и, Mint, — для, дистрибутивов, Debian, — версия, для, Linux, — 32, и, 64, бит, для, дистрибутивов, Fedora, и, RedHat, — версия, для, Linux, — 32, и, 64, бит, для, дистрибутивов, Arch, и, Manjaro, — версия, для, Linux, — 32, и, 64, бит, для, дистрибутивов, Gentoo, и, Funtoo, — версия, для, Linux, — 32, и, 64, бит, для, дистрибутивов, Slackware, — версия, для, Linux, — 32, и, 64, бит, для, дистрибутивов, Mint, — версия, для, Linux, — 32, и, 64, бит, для, дистрибутивов, Debian, — версия, для, Linux, — 32, и, 64, бит, для, дистрибутивов, Ubuntu