Хакерские утилиты

Сабина Жигальская
Специалист по комплексной защите информации

Skillbox

Цель урока

Узнать основные утилиты для хакеров.

John the Ripper

John The Ripper — это инструмент
с открытым исходным кодом
для взлома паролей методом перебора.

John the Ripper

Установка утилиты:

aptitude install john

Hydra

THC Hydra — это программное обеспечение для взлома аутентификации с помощью перебора.

Если John The Ripper можно использовать для проверки надёжности паролей офлайн, то Hydra аналогичный инструмент, работающий онлайн.

Hydra

Запуск утилиты:

$ hydra опции логины пароли -s порт адрес_цели модуль параметры_модуля

Hydra

Простейший вариант использования THC-Hydra — найти в интернете стандартные списки паролей для Brute Force, подключить их при помощи опций и ждать результата.

Также понадобятся данные сервера, на который будет осуществляться атака.

Перечни паролей подходят и от других программ вроде John the Ripper.

Maltego

Maltego — это инструмент не для тестирования на проникновение, а скорее для аналитики. Он позволяет найти связи между различными субъектами и объектами.

Maltego позволяет вычислять сетевую и доменную информацию, такую как:

- доменные имена
- Whois-информация
- DNS-записи
- Netblocks
- IP-адреса и т. д.

Maltego

Запуск из терминала: набираем **maltego** и нажимаем Enter.

Для использования этой утилиты необходима регистрация.

Далее открываем свою почту и подтверждаем аккаунт, кликнув по ссылке активации.

Metasploit

Metasploit — это очень популярная платформа для тестирования безопасности систем.

Это самая мощная платформа для разработки, тестирования и использования кода эксплойтов. Она содержит инструменты, которые позволяют объединить работу различных компонентов.

Metasploit

Запуск производится командой:

Msfconsole

Все модули делятся на несколько типов, в зависимости от предоставляемой функциональности:

- Exploit
- Payload
- Post
- Encoder
- NOP
- Auxiliry

Metasploit

На официальном сайте разработчика размещён Metasploit Framework Pro User Guide, подробно описывающий все возможные фичи пакета и их применение в реальных условиях.

Nikto

Nikto — классический инструмент для сканирования серверов на наличие уязвимостей.

Программа проводит поиск по базе более 6 000 потенциально опасных файлов, выявляет устаревшие версии сетевого ПО для более чем 1 300 программ, проверяет конфигурационные файлы сервера.

Nikto

Прежде чем начинать сканирование с помощью Nikto, лучше предварительно провести разведку с помощью Maltego.

Nikto

Установка утилиты:

apt install nikto

Просмотр параметров:

nikto -Help

Nikto

У Nikto есть много вариантов использования, но для наших целей понадобится базовый синтаксис <IP или hostname> с фактическим IP-адресом или именем хоста без угловых скобок:

nikto -h <IP or hostname>

nikto -h <IP or hostname> -ssl — если у сайта есть SSL

Nikto

Можно использовать Nikto в локальной сети, чтобы найти embedded-сервера, такие как страница логина роутера или HTTP-сервис на другой машине, который представляет из себя просто сервер без веб-сайта.

Чтобы узнать IP-адрес, нужно использовать **ifconfig**.

Nikto

Важное преимущество Nikto: информацию, полученную при сканировании, можно экспортировать в формат, который сможет прочитать Metasploit.

Для этого в конец команд для выполнения сканирования, приведённых выше, нужно добавить флаги **-Format msf+.**

Выводы урока

- Существует множество программ, дающих хакеру удобные и надёжные инструменты на все случаи жизни

- Находя с их помощью уязвимости, специалист по кибербезопасности может предупреждать различные атаки и заранее устранять уязвимости

Выводы модуля

- Разобрались с пакетными менеджерами
- Научились компилировать код
- Узнали, что deb — это архивы
- Узнали, как работать с интерфейсным инструментом yum
- Научились работать с утилитами по безопасности
- Изучили утилиты для хакеров