Повышение привилегий в Linux

Сабина Жигальская
Специалист по комплексной защите информации

Skillbox

Цель урока

Узнать, как происходит повышение прав пользователей.

Под рутом — нельзя!

Работать в линуксе под рутом категорически
не рекомендуется.

Исключения: конфигурирование сервера, установки
и обновления ПО и прочих административных задач.

Эксплойты

Большинство способов получения прав суперпользователя в Linux сводятся к использованию эксплойтов.

В чём преимущество использования эксплойтов? Большинство эксплойтов используют уязвимости в ядре ОС, что позволяет получить максимальные привилегии.

Алгоритм действий

В общем виде алгоритм действий выглядит следующим образом:

1. Определить версию ядра и дистрибутива
2. Получить список доступных инструментов для сборки эксплойта
3. Доставить эксплойт на целевую машину
4. Скомпилировать (при необходимости) и запустить
5. Наслаждаться полученным рутом

Определение версии ядра

Версию ядра можно узнать с помощью известной команды **uname -a**.

В файле ***-release**, лежащем в каталоге etc, можно узнать дистрибутив Linux.

Поиск эксплойта

Ресурсы поиска нужного эксплойта:

- exploit-db
- 1337day
- SecuriTeam
- ExploitSearch
- securityreason

Дополнительную информацию можно получить:

- www.cvedetails.com
- packetstormsecurity.org
- cve.mitre.org

Передача эксплойта

Популярная утилита переброски эксплойта — **netcat**

nc -l -p 1234 > out.file

После передачи эксплойта

Далее, когда наш эксплойт оказался на принимающей стороне, он запускается с помощью обычной компиляции.

Всё зависит уже от типа эксплойта. Главное — понять сам алгоритм, ведь первые 3 шага будут стандартными для всех случаев.

Выводы урока

- Вариантов, как можно повысить права, достаточно много, мы рассмотрели алгоритм действий
- Знать это необходимо для того, чтобы понимать, как действует злоумышленник

Выводы модуля

- Узнали про права доступа и что такое команды sudo и su
- Поговорили про модели доступов
- Узнали, что такое привилегии пользователей
- Обсудили, как происходит повышение привилегий несанкционированных пользователей