Модуль 22. Разведка и закрепление в ОС Linux

22.4. Повышение привилегий

В рамках юнита рассмотрено три техники повышения привилегий:

1. **sudo misconfiguration**
   При проведении данной атаки мы должны внимательно смотреть какие процессы/команды/приложения мы можем запускать с использованием *sudo* из под данного пользователя. Самая важная команда здесь — `sudo -l`, которая позволяет увидеть, какие команды могут быть запущены с использованием прав *root*. Далее уже необходимо исходить из доступных пользователю команд.
2. **kernel exploits**
   Эксплойты ядра используют уязвимости в ядре для выполнения кода с привилегиями *root*. Очень часто можно найти системы, уязвимые для эксплойтов ядра. Отслеживать устаревшие системы может быть сложно, и они могут быть исключены из исправлений из-за проблем совместимости с определёнными службами или приложениями. Данная атака от пентестера, как мы с вами, предполагает только проверку наличия для версии ядра жертвы эксплойта, его компиляцию и использование. Чтобы узнать версию ядра используется команда `uname -a`. Остальное — гугл и прямые руки.
3. **buffer overflow**
   Атаки данного типа строятся на особенностях некоторых языков программирования, а именно на небезопасной работе с памятью. Выражается это в возможности, при соблюдении некоторых условностей, «перезаписывании» участка памяти и перенаправлении потока программы в нужное нам русло. Для реализации данной атаки нужно предварительно проверить параметры на возможность их перезаписи (путём доведения до ошибки), после чего используя исходники, дебагерры и дизассемблеры, чтобы разобраться с возможными векторами атак.

Основные понятия модуля

Повышение привилегий — это использование компьютерного бага, уязвимостей, ошибки в конфигурации операционной системы или программного обеспечения с целью повышения уровня доступа к вычислительным ресурсам, которые обычно защищены от пользователя. В итоге приложение, обладающее бóльшими полномочиями, чем предполагалось системным администратором, может совершать неавторизированные действия.

Sticky bit — если применяется закреплённый *sticky bit*, пользователь может удалить файл, только если он является пользователем-владельцем файла или каталога, в котором содержится файл.

SGID — это идентификатор группы. При применении к исполняемому файлу он даёт пользователю, который исполняет файл, разрешения владельца группы этого файла.

SUID — разрешение на установку идентификатора пользователя. Это означает, что при исполнении данного процесса/программы пользователь временно получает права *root*.

Буфер — это область памяти, используемая для временного хранения данных при вводе или выводе.

Регистр памяти — специальная ячейка памяти в процессоре.

EIP/RIP регистр — данный регистр хранит в себе информацию о следующей команде, точнее о ячейке памяти, где она хранится.

Разведка — самый важный этап любого пентеста.

Основные команды модуля:

```
cat /etc/issue — команда для получения информации об имеющемся дистрибутиве.
/sbin/ifconfig -a — команда работы/получения информации о сетевых интерфейсах.
iptables -L — просмотра таблиц правил фильтрации IP-пакетов.
hostname — отображение текущего хоста, домена или имени узла системы.
ps aux | grep root — отображение сервисов, работающих с правами root.
dpkg -l — отображает информацию об установленных пакетах.
```

```
id — эта команда выводит информацию об указанном пользователе USERNAME или текущем пользователе,
который запустил данную команду и не указал явно имя пользователя
cat /etc/passwd | cut -d: -f1 — выводит всех пользователей
grep -v -E "^#" /etc/passwd | awk -F: '$3 == 0 { print $1}' — выводит пользователей с root правами
awk -F: '($3 == "0") {print}' /etc/passwd — то же, что и выше
sudo -l — выводит процессы, которые может запустить от имени root, используя sudo пользователь
netstat -antup
cat /etc/passwd — выводит хеши паролей
cat /etc/group — выводит содержимое файла group
cat /etc/shadow — выводит содержимое файла shaow
find / -perm -1000 -type d 2>/dev/null — выводит Sticky bit процессы
find / -perm -g=s -type f 2>/dev/null — выводит SGID процессы
find / -perm -u=s -type f 2>/dev/null — выводит SUID процессы
```