Данный стенд состоит из 3х машин

- Kali Linux 2021
- Ubuntu Linux 20.04 №1 (Уязвимый сервер)
- Ubuntu Linux 20.04 №2 (Пользователь)

Принцип работы

1) Хакер получает ip-адрес. Пробует к нему подключиться. Видит , что это веб-приложение DVWA , предназначенное для тренировки навыков специалистов по информационной безопасности.
2) Он проводит Command Injection, тем самым получая reverse shell сервера.
3) Первым делом злоумышленник проводит сканирование на поиск интересных текстовых файлов, которые могут нести в себе полезную информацию. Он находит файл “passwords.txt” с паролями и запоминает его.
4) После этого он пробует подняться до рута, ищет файлы с CAP_SETUID
5) Попытка оказывается успешной и злоумышленник повышает привилегии. Получает root.
6) Теперь можно изучить сеть с помощью nmap.
7) Получив ip адрес третьей машины, хакер подключается по открытому порту ssh от рута с помощью полученного ранее пароля.
8) Найден флаг /root/proof.txt

Уязвимости

1) Command Injection(внедрение кода)
2) Разглашение конфиденциальных данных
3) Возможность повышения привилегий из-за наличия файлов с CAP_SETUID
4) Включен **root доступ по SSH**