Презентация о выполнении. Индивидуальный проект.

Этап 3

Сироджиддинов Камолиддин, НКНбд-01-21

Российский университет дружбы народов, Москва, Россия

Цель работы

Цель работы

Исследование и применение инструмента Hydra для подбора имени пользователя и пароля с использованием brute-force атаки на HTTP POST форму, а также анализ результатов выполнения.

Исходные данные:

IP сервера: `178.72.90.181` Сервис: `HTTP` на стандартном `80` порту Форма авторизации: Метод отправки данных - `POST` по адресу: `http://178.72.90.181/cgi-bin/luci`, Параметры формы: `username=root&password=test_password` Сообщение при неудачной аутентификации: `"Invalid username and/or password! Please try again."` Используемая утилита: `Hydra`

1. Обновление системы

```
┌──(kamoliddin㉿root)-[~]
└─$ sudo apt-get install hydra
Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
hydra is already the newest version (9.5-1+b2).
hydra set to manually installed.
The following packages were automatically installed and are no longer require
d:
  ibverbs-providers libboost-iostreams1.83.0 libboost-thread1.83.0
  libcephfs2 libdaxctl1 libgfapi0 libgfrpc0 libgfxdr0 libglusterfs0
  libibverbs1 libndctl6 libpmem1 libpython3.11-dev librados2 librdmacm1t64
  python3-lib2to3 python3.11 python3.11-dev python3.11-minimal
  samba-ad-provision samba-dsdb-modules samba-vfs-modules
Use 'sudo apt autoremove' to remove them.
0 upgraded, 0 newly installed, 0 to remove and 974 not upgraded.
```

Figure 1: 1

Заключение

Заключение

В ходе работы было продемонстрировано использование инструмента Hydra для проведения атаки на HTTP POST форму методом brute-force. С помощью указанной команды удалось успешно подобрать пароль для пользователя.

Полученный результат подтверждает эффективность метода brute-force при наличии недостаточно защищённого веб-сервиса с простыми паролями и отсутствием дополнительных защитных механизмов (например, блокировки после нескольких неудачных попыток входа).