Использование Hydra

Этап 3

Абу Сувейлим Мухаммед Мунифович

Содержание

# 1 Цель работы

Выполнить простейшие команды инструмента Hydra.

# 2 Задание

Взломать пароль по имени пользователя.

# 3 Теоретическое введение

Hydra - это программное обеспечение с открытым исходным кодом для перебора паролей в реальном времени от различных онлайн сервисов, веб-приложений, FTP, SSH и других протоколов. Это распараллеленный взломщик для входа в систему, он поддерживает множество протоколов для осуществления атак. Пользователь быстро и с легкостью может добавить новые модули. Hydra предоставляет специалистам в сфере ИБ возможность узнать, насколько легко можно получить несанкционированный доступ к системе с удаленного устройства. [1]

# 4 Выполнение лабораторной работы

Для начала создаим новый пользователь testuser (рис. 1):



Рис. 1: Пользователь testuser

Проверим данные пользователя (рис. 2):

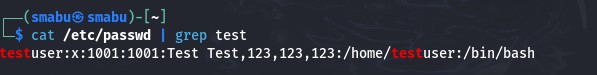


Рис. 2: Команда cat | grep

Далее, определим ip адресс машинной (рис. 3):

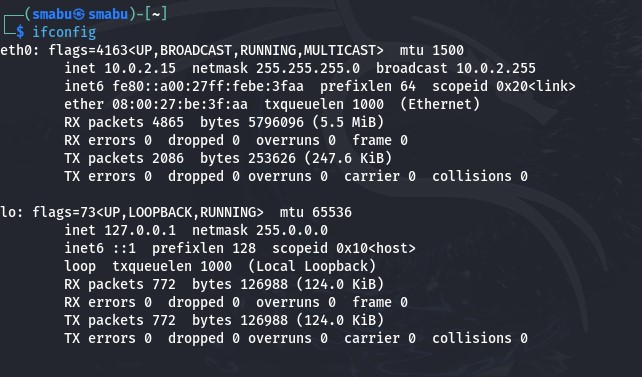


Рис. 3: Команда ifconfig

Наконец то указывается список пользователей и паролей, ip адресс, протокол и выполняем команду (рис. 4):

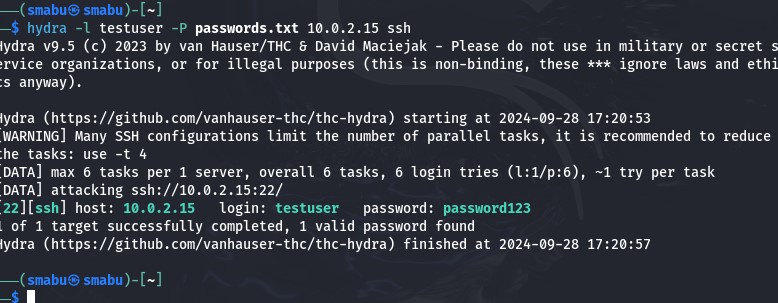


Рис. 4: Команда hydra

Получили логин “testuser” и пароль “password123”

# 5 Выводы

В результате выполнения работы мы повысили свои навыки использования инструмента Hydra. [2]

# Список литературы

1. cryptoparty. [DVWA – Уязвимое веб-приложение](https://itsecforu.ru/2018/02/14/5071/). 2018.

2. Парасрам Шива Х.Т. Замм Алекс. Kali Linux. Тестирование на проникновение и безопасность. СПб, 2020. 448 с.