

IS Assignment #1 (7H)

submitted to: Sir Ahmad Ali Sha

L19-1196 (Zaeem Yousaf)

Oct-03-2022

Contents

1	shell invocation	1
2	netdiscover	1
3	nmap	4
4	wpscan	4
5	hydra	4

1 shell invocation

1. opened shell and typed **whoami** to check the user
2. then used `sudo su` to login as a root

2 netdiscover

We use the `netdiscover` command on the root to see the current computers connected to our network. The command scans the Wi-Fi in this instance, which is our current network. The IP, MAC address, count, vendor, and hostname are then displayed.

let us pass some argument to **netdiscover** – **i eth 0** to speicify ethernet

As the system searches each and every IP address on the network, this command continues to execute for a long. This is how the output appears following the scan.

```
root@kali: ~  
File Actions Edit View Help  
$ whoami  
zaeem  
$ sudo su  
[sudo] password for zaeem :  
(root@kali)-[~]  
#
```

Figure 1: zaeem's shell

```
root@kali: ~  
File Actions Edit View Help  
Currently scanning: 172.19.10.0/16 | Screen View: Unique Hosts  
24 Captured ARP Req/Rep packets, from 3 hosts. Total size: 1440  
+-----+-----+-----+-----+-----+-----+  
IP           At MAC Address      Count  Len  MAC Vendor / Hostname  
+-----+-----+-----+-----+-----+-----+  
192.168.159.2 00:50:56:f7:fc:38    21    1260 VMware, Inc.  
192.168.159.254 00:50:56:e1:b7:3d    2     120 VMware, Inc.  
192.168.159.1 00:50:56:c0:00:08    1      60 VMware, Inc.
```

Figure 2: netdiscover command

```
root@kali: ~  
File Actions Edit View Help  
Currently scanning: 172.26.209.0/16 | Screen View: Unique Hosts  
1 Captured ARP Req/Rep packets, from 1 hosts. Total size: 60  
-----  
IP          At MAC Address    Count  Len  MAC Vendor / Hostname  
-----  
192.168.56.1 0a:00:27:00:00:07    1    60  Unknown vendor
```

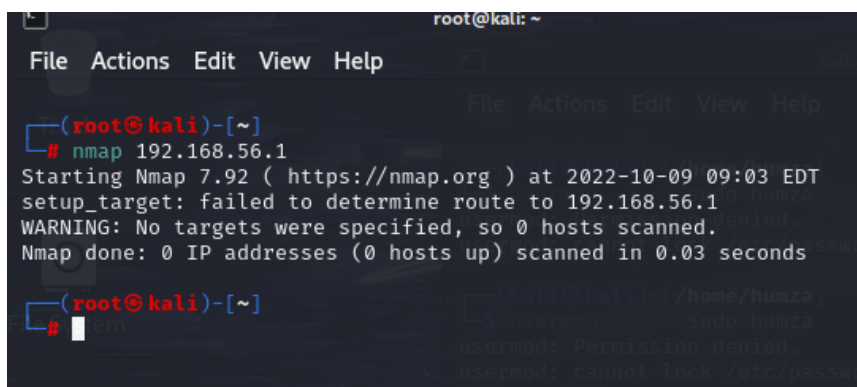
Figure 3: netdiscover specifying ethernet

```
root@kali: ~  
File Actions Edit View Help  
Currently scanning: 10.7.61.0/8 | Screen View: Unique Hosts  
5 Captured ARP Req/Rep packets, from 2 hosts. Total size: 300  
-----  
IP          At MAC Address    Count  Len  MAC Vendor / Hostname  
-----  
192.168.56.1 0a:00:27:00:00:07    2   120  Unknown vendor  
0.0.0.0      0a:00:27:00:00:07    3   180  Unknown vendor
```

Figure 4: netdiscover's output after a while

3 nmap

upon running nmap with the IP address 192.168.56.1, following goes the output.

A terminal window titled 'root@kali: ~' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(root@kali)-[~]'. The command '# nmap 192.168.56.1' is entered. The output is: 'Starting Nmap 7.92 (https://nmap.org) at 2022-10-09 09:03 EDT', 'setup_target: failed to determine route to 192.168.56.1', 'WARNING: No targets were specified, so 0 hosts scanned.', and 'Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds'. The prompt returns to '(root@kali)-[~]'.

```
(root@kali)-[~]  
# nmap 192.168.56.1  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-09 09:03 EDT  
setup_target: failed to determine route to 192.168.56.1  
WARNING: No targets were specified, so 0 hosts scanned.  
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.03 seconds  
  
(root@kali)-[~]  
#
```

Figure 5: nmap 192.168.56.1

4 wpscan

upon running wpscan with the IP address 192.168.56.1, following goes the output.

A terminal window showing the prompt '(root@kali)-[~]' and the command '# wpscan 192.168.56.1' being entered.

```
(root@kali)-[~]  
# wpscan 192.168.56.1
```

Figure 6: wpscan 192.168.56.1

5 hydra

Then, in order to determine the legitimate username/password combinations that might be helpful for accessing this system, Hydra App is employed.

```

File Actions Edit View Help

mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] postgres rad
in2 rdp redis rexec rlogin rpcap rsh rtsp s7-300 sip smb smtp[s] smtp-enum s
mp socks5 ssh sshkey svn teamspeak telnet[s] vmauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs.
Licensed under AGPL v3.0. The newest version is always available at;
https://github.com/vanhauser-thc/thc-hydra
Please don't use in military or secret service organizations, or for illegal
purposes. (This is a wish and non-binding - most such people do not care abo
t
laws and ethics anyway - and tell themselves they are one of the good ones.)
These services were not compiled in: afp ncp oracle sapr3 smb2.

Use HYDRA_PROXY_HTTP or HYDRA_PROXY environment variables for a proxy setup.
E.g. % export HYDRA_PROXY=socks5://l:p@127.0.0.1:9150 (or: socks4:// connect
//)
% export HYDRA_PROXY=connect_and_socks_proxylist.txt (up to 64 entries)
% export HYDRA_PROXY_HTTP=http://login:pass@proxy:8080
% export HYDRA_PROXY_HTTP=proxylist.txt (up to 64 entries)

Examples:
hydra -l user -P passlist.txt ftp://192.168.0.1
hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
hydra -C defaults.txt -6 pop3s://[2001:db8::1]:143/TLS:DIGEST-MD5
hydra -l admin -p password ftp://[192.168.0.0/24]/
hydra -L logins.txt -P pws.txt -M targets.txt ssh
$ █

```

Figure 7: hydra