IS Assignment #1 (7H)

submitted to: Sir Ahmad Ali Sha

L19-1196 (Zaeem Yousaf)

Oct-03-2022

Contents

1 shell invocation

1. opened shell and typed **whoami** to check the user
2. then used sudu 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.

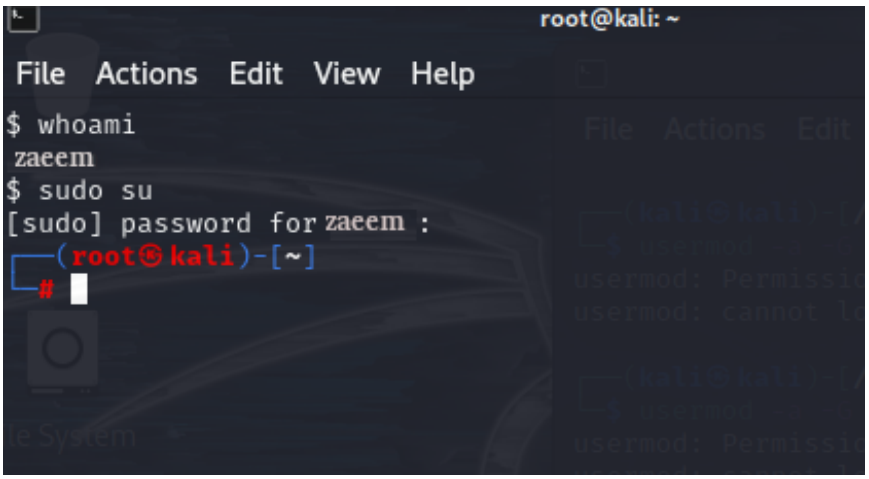


Figure 1: zaeem's shell

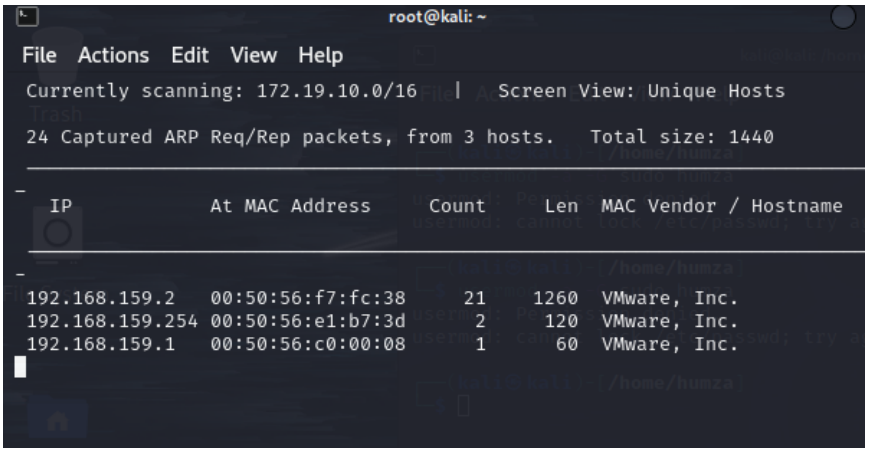


Figure 2: netdiscover command

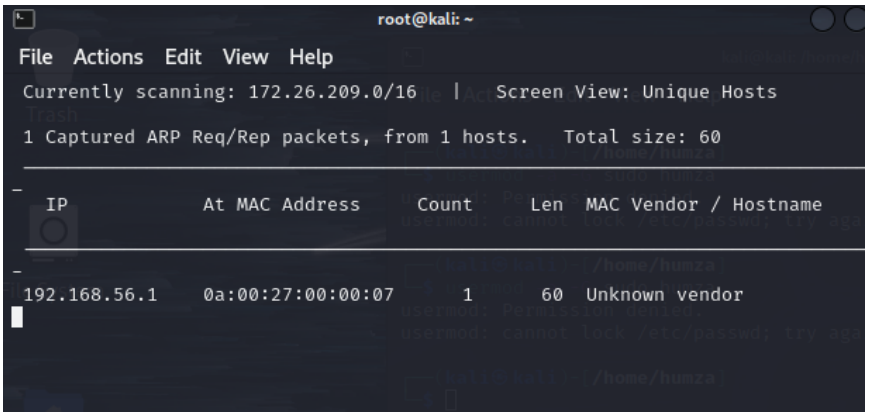


Figure 3: netdiscover specifying ethernet

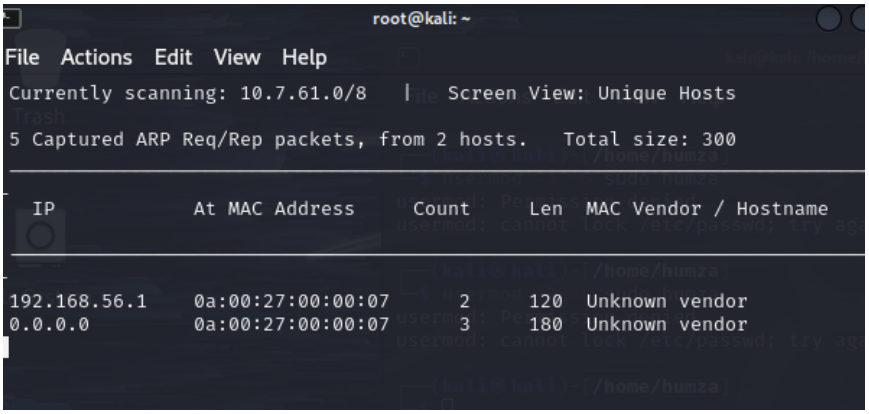


Figure 4: netdiscover's output after a while

3 nmap

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

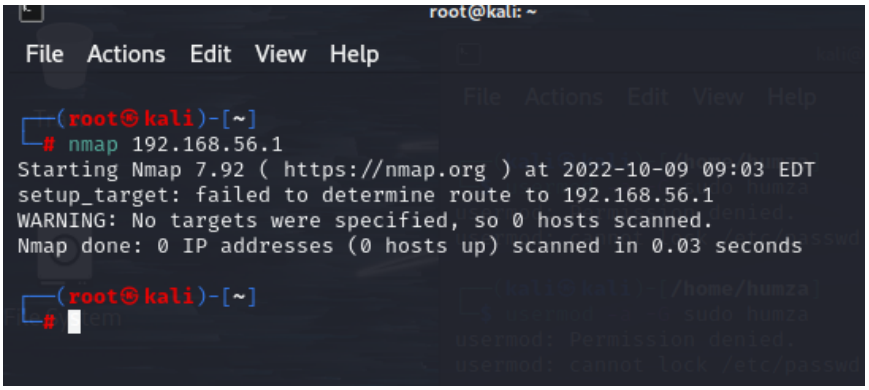


Figure 5: nmap 192.168.56.1

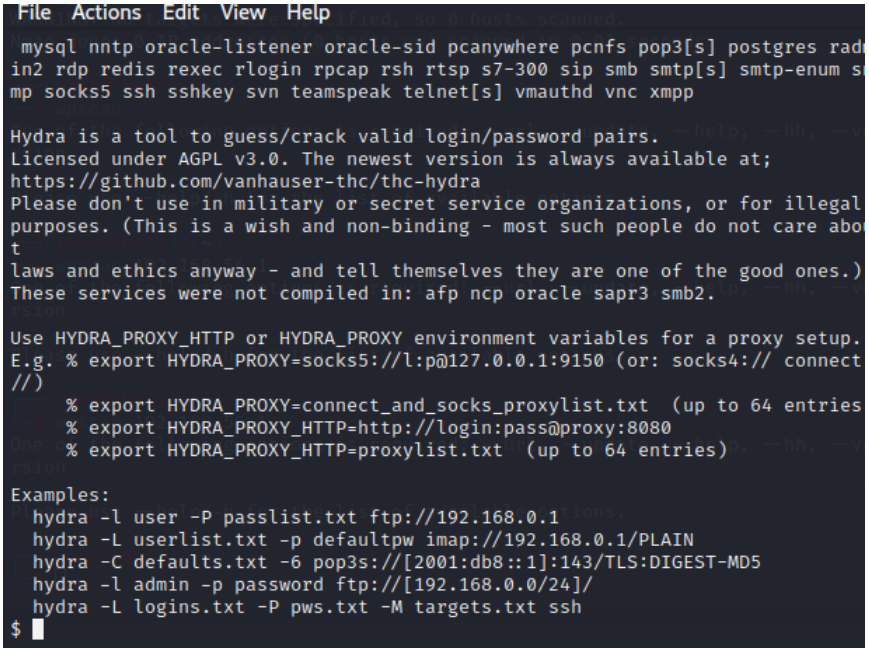
4 wpscan

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

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