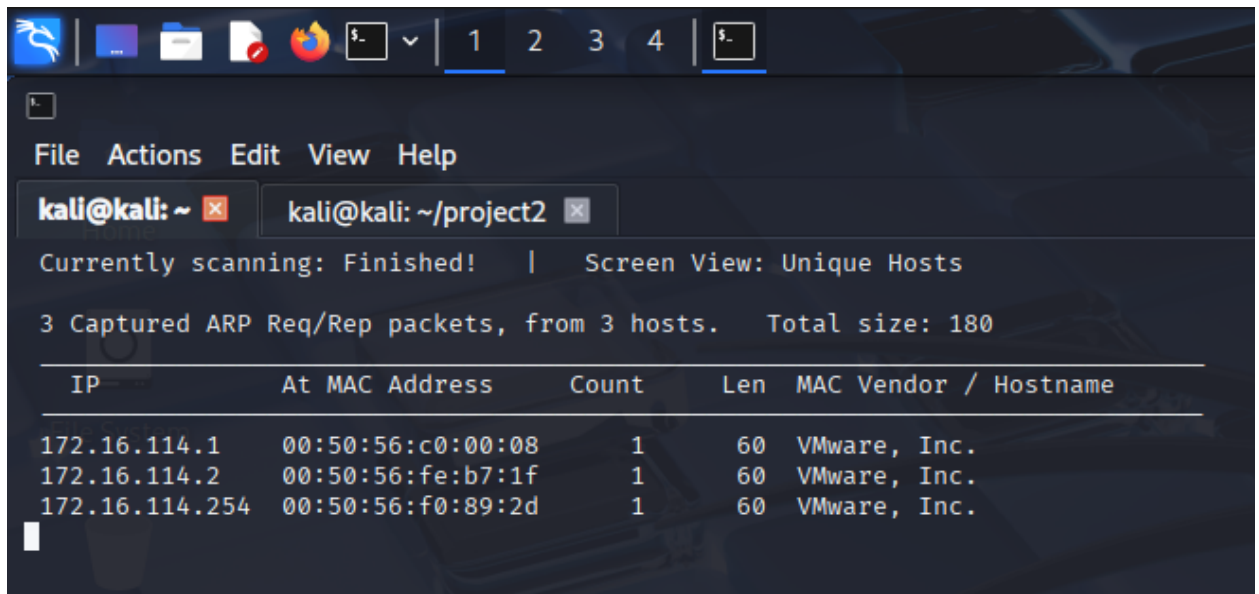


Cybersecurity Footptinting and Scanning Lab

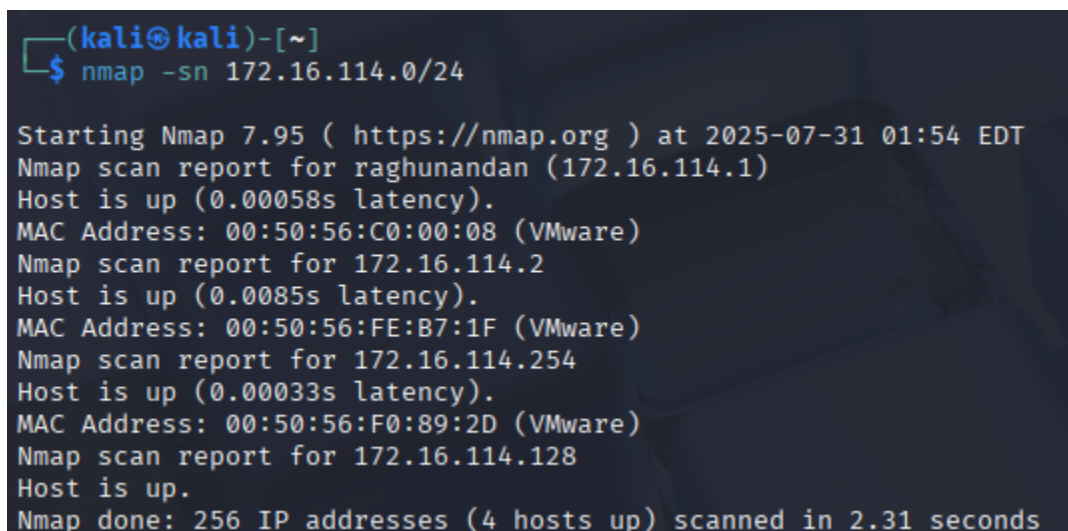
Performed by: Raghunandan Sharma

1. `sudo netdiscover -r 172.16.114.0/24`



```
kali@kali: ~ | kali@kali: ~/project2
Currently scanning: Finished! | Screen View: Unique Hosts
3 Captured ARP Req/Rep packets, from 3 hosts. Total size: 180
+-----+-----+-----+-----+-----+-----+
| IP | At MAC Address | Count | Len | MAC Vendor / Hostname |
+-----+-----+-----+-----+-----+-----+
| 172.16.114.1 | 00:50:56:c0:00:08 | 1 | 60 | VMware, Inc. |
| 172.16.114.2 | 00:50:56:fe:b7:1f | 1 | 60 | VMware, Inc. |
| 172.16.114.254 | 00:50:56:f0:89:2d | 1 | 60 | VMware, Inc. |
+-----+-----+-----+-----+-----+-----+
```

2. `nmap -sn 192.168.1.0/24`



```
(kali@kali)-[~]
$ nmap -sn 172.16.114.0/24

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 01:54 EDT
Nmap scan report for raghunandan (172.16.114.1)
Host is up (0.00058s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 172.16.114.2
Host is up (0.0085s latency).
MAC Address: 00:50:56:FE:B7:1F (VMware)
Nmap scan report for 172.16.114.254
Host is up (0.00033s latency).
MAC Address: 00:50:56:F0:89:2D (VMware)
Nmap scan report for 172.16.114.128
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.31 seconds
```

3. nmap -sS -sV -O 172.168.114.128

```
(kali@kali)-[~]
$ nmap -sS -sV -O 172.168.114.128

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 01:57 EDT
Nmap scan report for 172.168.114.128
Host is up (0.019s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp?
554/tcp   open  rtsp?
1723/tcp  open  pptp?
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: DO-WRT v24-sp2 (Linux 2.4.37) (97%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (97%), Actiontec MI424WR-GEN3I WAP (96%), Linux 3.2 (95%), VMware Player virtual NAT device (95%), Linux 4.4 (93%), Microsoft Windows XP SP3 (93%), BlueArc Titan 2100 NAS device (90%)
No exact OS matches for host (test conditions non-ideal).

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 183.93 seconds
```

4. nmap -A 172.168.114.128

```
(kali@kali)-[~]
$ nmap -A 172.168.114.128

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 02:01 EDT
Nmap scan report for 172.168.114.128
Host is up (0.0052s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp?
554/tcp   open  rtsp?
1723/tcp  open  pptp?
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: DO-WRT v24-sp2 (Linux 2.4.37) (97%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (97%), Actiontec MI424WR-GEN3I WAP (96%), Linux 4.4 (95%), Microsoft Windows XP SP3 (95%), VMware Player virtual NAT device (95%), Linux 3.2 (92%), BlueArc Titan 2100 NAS device (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.34 ms 172.16.114.2
2 0.24 ms 172.168.114.128

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 242.69 seconds
```

5. nmap -A 172.168.114.128 -oN scan_results.txt cat scan_results.txt

```
(kali@kali)-[~]
$ nmap -A 172.168.114.128 -oN scan_results.txt

Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-31 02:07 EDT
Nmap scan report for 172.168.114.128
Host is up (0.0051s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp?
554/tcp   open  rtsp?
1723/tcp  open  pptp?
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (97%), DO-WRT v24-sp2 (Linux 2.4.37) (97%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (97%), Linux 3.2 (95%), Microsoft Windows XP SP3 (95%), VMware Player virtual NAT device (95%), Linux 4.4 (92%), BlueArc Titan 2100 NAS device (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.11 ms 172.16.114.2
2 0.25 ms 172.168.114.128

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 239.51 seconds

(kali@kali)-[~]
$ cat scan_results.txt
# Nmap 7.95 scan initiated Thu Jul 31 02:07:23 2025 as: /usr/lib/nmap/nmap --privileged -A -oN scan_results.txt 172.168.114.128
Nmap scan report for 172.168.114.128
Host is up (0.0051s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp?
554/tcp   open  rtsp?
1723/tcp  open  pptp?
Warning: OSscan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Actiontec MI424WR-GEN3I WAP (97%), DO-WRT v24-sp2 (Linux 2.4.37) (97%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (97%), Linux 3.2 (95%), Microsoft Windows XP SP3 (95%), VMware Player virtual NAT device (95%), Linux 4.4 (92%), BlueArc Titan 2100 NAS device (90%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 0.11 ms 172.16.114.2
2 0.25 ms 172.168.114.128

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Jul 31 02:11:22 2025 -- 1 IP address (1 host up) scanned in 239.51 seconds
```

6. curl ipinfo.io/\$(dig +short testphp.vulnweb.com)

```
(kali㉿kali)-[~]  
$ curl ipinfo.io/$(dig +short testphp.vulnweb.com)  
{  
  "ip": "44.228.249.3",  
  "hostname": "ec2-44-228-249-3.us-west-2.compute.amazonaws.com",  
  "city": "Boardman",  
  "region": "Oregon",  
  "country": "US",  
  "loc": "45.8399,-119.7006",  
  "org": "AS16509 Amazon.com, Inc.",  
  "postal": "97818",  
  "timezone": "America/Los_Angeles",  
  "readme": "https://ipinfo.io/missingauth"  
}
```

7. recon-ng

marketplace install recon/domains-hosts/hackertarget

modules load recon/domains-hosts/hackertarget

options set SOURCE example.com

run

exit

```
[recon-ng][default] > modules load recon/domains-hosts/hackertarget
[recon-ng][default][hackertarget] > options set SOURCE example.com
SOURCE ⇒ example.com
[recon-ng][default][hackertarget] > run

-----
EXAMPLE.COM
-----
[*] Country: None
[*] Host: example.com
[*] Ip_Address: 96.7.128.198
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----
[*] Country: None
[*] Host: www.example.com
[*] Ip_Address: 93.184.215.14
[*] Latitude: None
[*] Longitude: None
[*] Notes: None
[*] Region: None
[*] -----

SUMMARY
-----
[*] 2 total (2 new) hosts found.
[recon-ng][default][hackertarget] > █
```

8. `theHarvester -d example.com -b bing,linkedin -f harvester_report.html`

```

*****
*
* [ASCII Art: theHarvester]
*
* theHarvester 4.8.0
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*
*****

[*] Target: example.com

Read api-keys.yaml from /etc/theHarvester/api-keys.yaml
  Searching 0 results.
[*] Searching Bing.

[*] No LinkedIn users found.

[*] LinkedIn Links found: 0
-----

[*] No IPs found.

[*] Emails found: 7
-----
email@example.com
info@example.com
mail@example.com
me@example.com
name@example.com
them@example.com
you@example.com

[*] No people found.

[*] Hosts found: 4
-----
www.example.com
static.example.com
sub1.example.com
sub2.example.com

[*] Reporting started.
[*] XML File saved.
[*] JSON File saved.

```

9. amass enum -passive -d example.com

```
(kali㉿kali)-[~]
└─$ amass enum -passive -d example.com

example.com (FQDN) → ns_record → a.iana-servers.net (FQDN)
example.com (FQDN) → ns_record → b.iana-servers.net (FQDN)
example.com (FQDN) → a_record → 96.7.128.198 (IPAddress)
example.com (FQDN) → a_record → 23.192.228.80 (IPAddress)
example.com (FQDN) → a_record → 23.192.228.84 (IPAddress)
example.com (FQDN) → a_record → 23.215.0.136 (IPAddress)
example.com (FQDN) → a_record → 23.215.0.138 (IPAddress)
example.com (FQDN) → a_record → 96.7.128.175 (IPAddress)
example.com (FQDN) → aaaa_record → 2600:1406:bc00:53::b81e:94c8 (IPAddress)
example.com (FQDN) → aaaa_record → 2600:1406:bc00:53::b81e:94ce (IPAddress)
example.com (FQDN) → aaaa_record → 2600:1408:ec00:36::1736:7f24 (IPAddress)
example.com (FQDN) → aaaa_record → 2600:1408:ec00:36::1736:7f31 (IPAddress)
example.com (FQDN) → aaaa_record → 2600:1406:3a00:21::173e:2e65 (IPAddress)
example.com (FQDN) → aaaa_record → 2600:1406:3a00:21::173e:2e66 (IPAddress)
96.7.128.0/23 (Netblock) → contains → 96.7.128.198 (IPAddress)
96.7.128.0/23 (Netblock) → contains → 96.7.128.175 (IPAddress)
23.192.228.0/22 (Netblock) → contains → 23.192.228.80 (IPAddress)
23.192.228.0/22 (Netblock) → contains → 23.192.228.84 (IPAddress)
23.215.0.0/22 (Netblock) → contains → 23.215.0.136 (IPAddress)
23.215.0.0/22 (Netblock) → contains → 23.215.0.138 (IPAddress)
20940 (ASN) → managed_by → AKAMAI-ASN1 (RIROrganization)
20940 (ASN) → announces → 96.7.128.0/23 (Netblock)
20940 (ASN) → announces → 23.192.228.0/22 (Netblock)
20940 (ASN) → announces → 23.215.0.0/22 (Netblock)
^Ca.iana-servers.net (FQDN) → a_record → 199.43.135.53 (IPAddress)
a.iana-servers.net (FQDN) → aaaa_record → 2001:500:8f::53 (IPAddress)
b.iana-servers.net (FQDN) → a_record → 199.43.133.53 (IPAddress)
b.iana-servers.net (FQDN) → aaaa_record → 2001:500:8d::53 (IPAddress)
^C
```