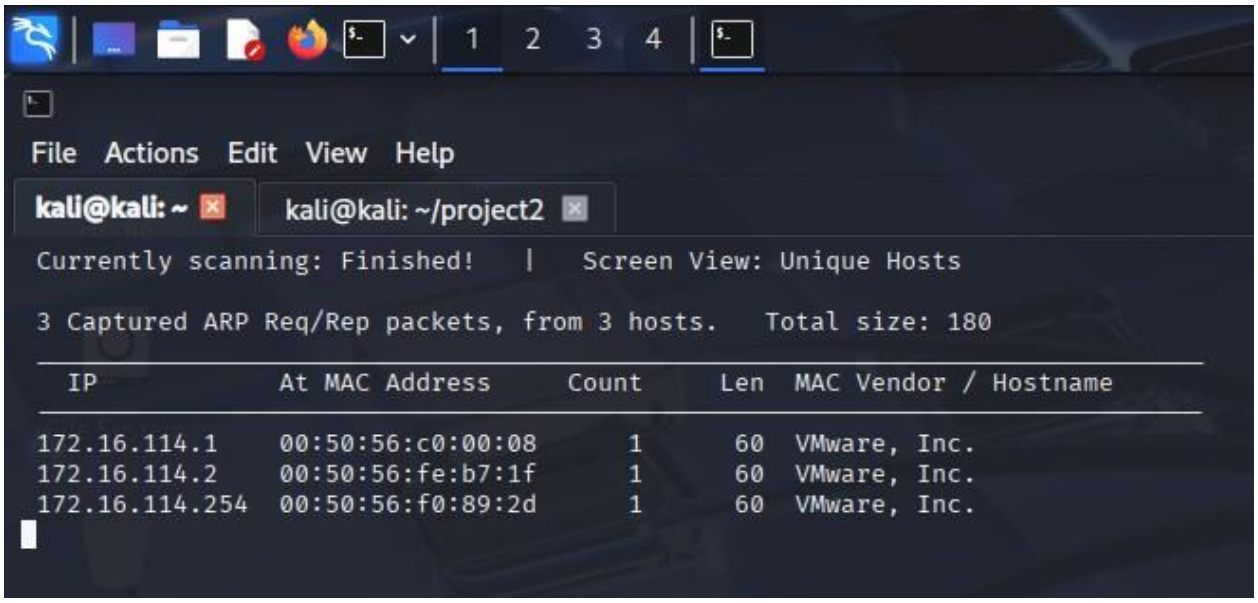
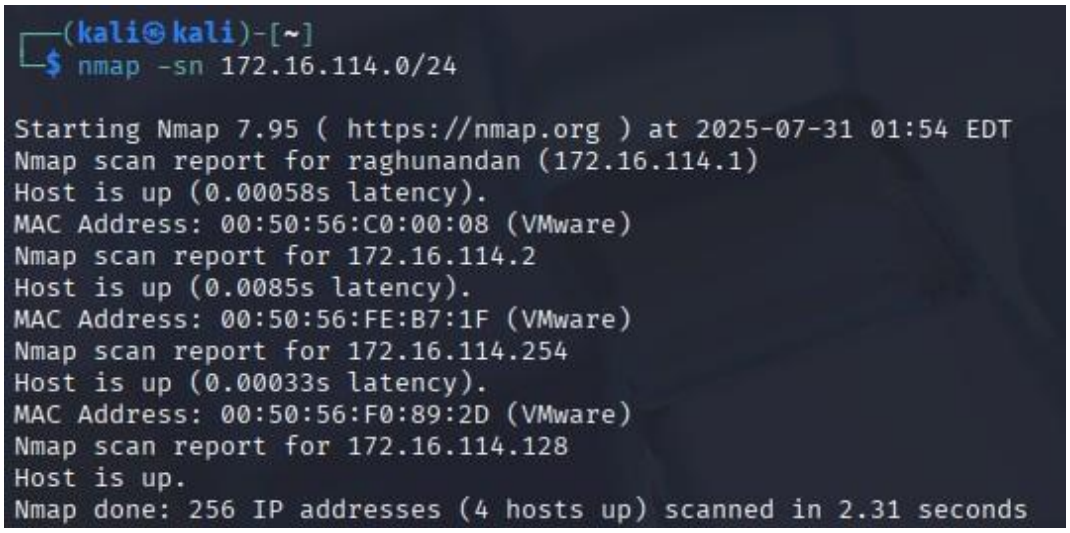
Cybersecurity and Footprinting Lab

Performed by: Daksh(2023A7R003)

1. sudo netdiscover -r 172.16.114.0/24



2. nmap -sn 192.168.1.0/24



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: DD-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 virtu
al 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
```

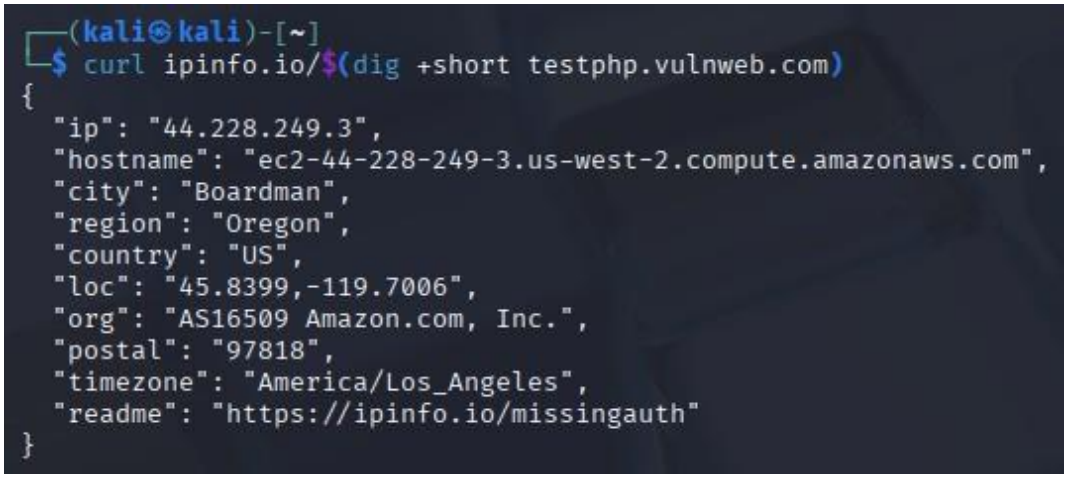
4. nmap -A 172.168.114.128

```
┌──(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: DD-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 X
P 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
```

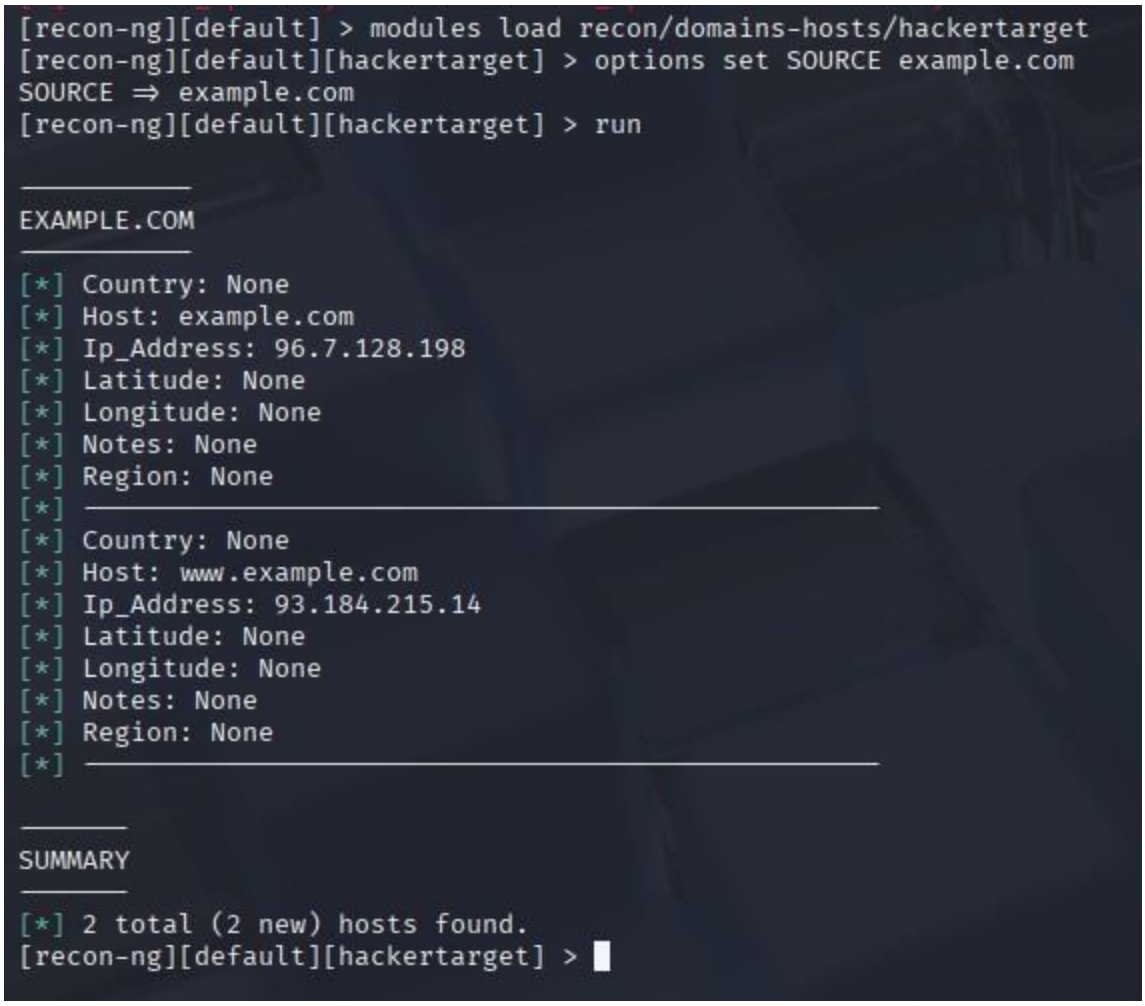
5. nmap -A 172.168.114.128 -oN scan_results.txt
   cat scan_results.txt

```
┌──(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%), DD-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 X
P 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%), DD-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 X
P 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
```

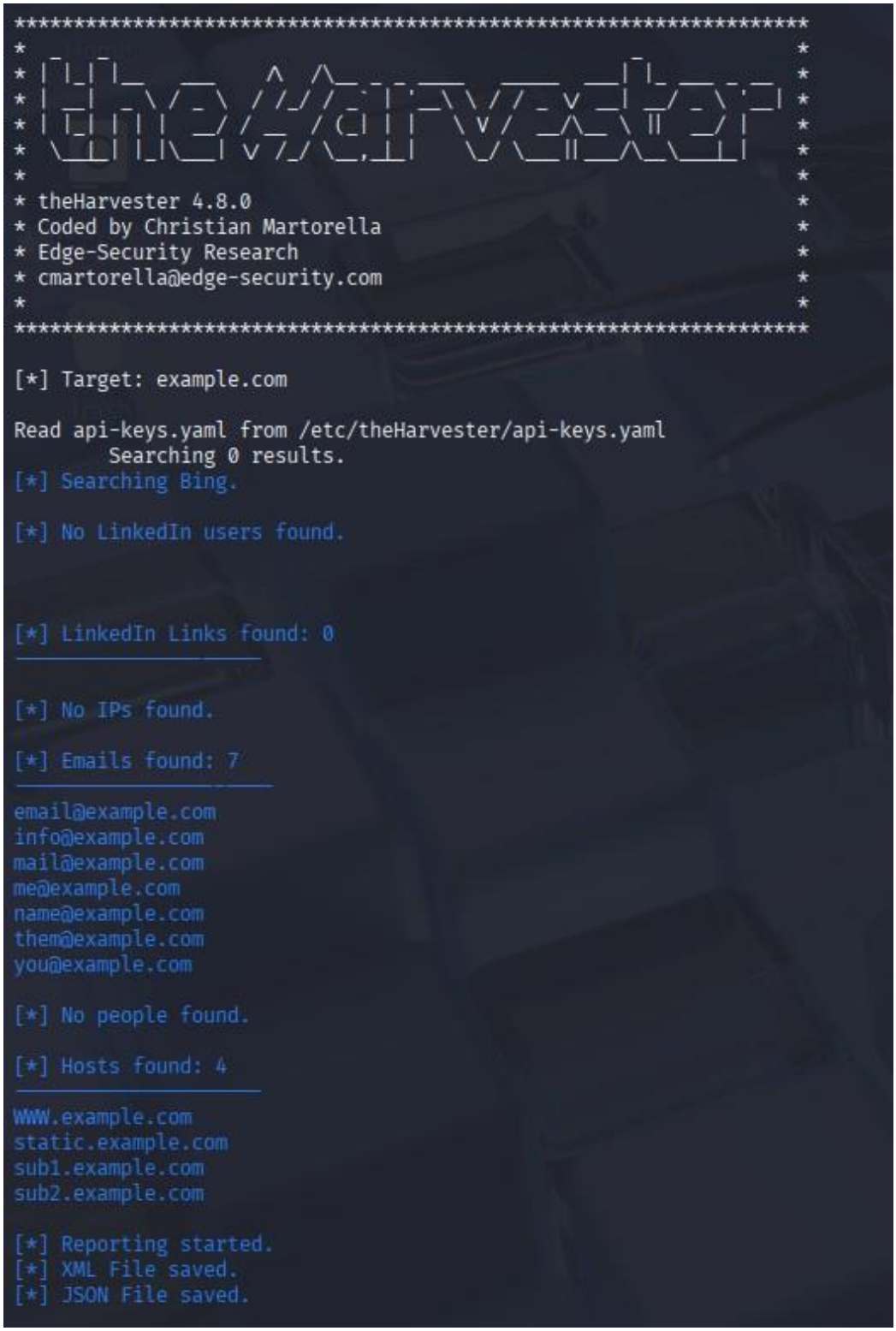
6. curl ipinfo.io/$(dig +short testphp.vulnweb.com)



7. recon-ng
   marketplace install recon/domains-hosts/hackertarget
   modules load recon/domains-hosts/hackertarget
   options set SOURCE example.com
   run
   exit



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



9. amass enum -passive -d example.com