

## TASK : 2

# Networking Toolkit – PoC

This Proof of Concept demonstrates how to gather key network information, check connectivity, and perform DNS lookups using a simple shell script.

---

## Instructions

We created a script `netinfo.sh` that performs the following tasks:

- 📌 Displays IP address, subnet mask, and default gateway
  - 📌 Lists open ports using `ss` or `netstat`
  - 📌 Pings `google.com` and logs the response
  - 📌 Resolves the IP address of `openai.com` using `nslookup`
  - 📌 Stores the entire output in `network_report.txt`
- 

## Script Creation

```
echo '#!/bin/bash'

echo "Network Configuration:"
ip addr show

echo -e "\nDefault Gateway:"
ip route | grep default

echo -e "\nOpen Ports:"
ss -tuln

echo -e "\nPing google.com:"
ping -c 4 google.com

echo -e "\nDNS Lookup for openai.com:"
```

```
nslookup openai.com
' > netinfo.sh
```

## Make the script executable

```
chmod +x netinfo.sh
```

## Run the script

```
./netinfo.sh | tee network_report.txt
```

```
(kali㉿kali)-[~]
$ nano netinfo.sh

(kali㉿kali)-[~]
$ chmod +x netinfo.sh

(kali㉿kali)-[~]
$ ./netinfo.sh

IP Address, Subnet Mask, and Default Gateway:
    inet 127.0.0.1/8 scope host lo
    inet 172.16.16.167/21 brd 172.16.23.255 scope global dynamic noprefixroute wlan0
default via 172.16.1.1 dev wlan0 proto dhcp src 172.16.16.167 metric 600
Open Ports (ss):
Netid State  Recv-Q Send-Q           Local Address:Port  Peer Address:Port
udp    UNCONN  0      0             0.0.0.0:36359       0.0.0.0:*
udp    UNCONN  0      0             172.16.16.167:3702  0.0.0.0:*
udp    UNCONN  0      0             239.255.255.250:3702 0.0.0.0:*
udp    UNCONN  0      0             *:43833            *:
udp    UNCONN  0      0 [fe80::996a:769c:9a82:2102]wlan0:3702 [::]:*
udp    UNCONN  0      0 [ff02::c]wlan0:3702 [::]:*
tcp    LISTEN  0     128             0.0.0.0:22         0.0.0.0:*
tcp    LISTEN  0     128             [::]:22           [::]:*

Ping google.com:
PING google.com (142.251.223.14) 56(84) bytes of data:
64 bytes from lcmaaa-ao-in-f14.1e100.net (142.251.223.14): icmp_seq=1 ttl=118 time=4.65 ms
64 bytes from lcmaaa-ao-in-f14.1e100.net (142.251.223.14): icmp_seq=2 ttl=116 time=14.1 ms
64 bytes from lcmaaa-ao-in-f14.1e100.net (142.251.223.14): icmp_seq=3 ttl=116 time=18.6 ms
64 bytes from lcmaaa-ao-in-f14.1e100.net (142.251.223.14): icmp_seq=4 ttl=118 time=91.2 ms

--- google.com ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3005ms
rtt min/avg/max/mdev = 4.651/32.129/91.185/34.463 ms
DNS Lookup for openai.com:
Server:      8.8.8.8
Address:     8.8.8.8#53
```