```
┌──(kali㉿kali)-[~/Desktop/project/project_ intro]
└─$ bash intro.sh
Please run as root.
```

```
┌──(root㉿kali)-[/home/kali/Desktop/project/project_ intro]
└─# bash intro.sh
═══════════════════════════════════════════════
        Network Analysis and Mapping Script
═══════════════════════════════════════════════

[+] Checking and installing required tools...
   [*] nmap is already installed. Skipping installation.
   [*] arp-scan is already installed. Skipping installation.
   [*] tshark is already installed. Skipping installation.
   [*] jq is already installed. Skipping installation.
[+] All required tools are installed.

[+] Setting up output file: network_info.txt

[+] Scanning for devices' IP addresses...
[+] Devices' IP addresses saved to output file.

[+] Scanning for devices' MAC addresses and vendors...
[+] Devices' MAC addresses and vendors saved to output file.

[+] Fetching router's internal and external IP addresses...
[+] Router IP addresses saved to output file.

[+] Scanning for device names...
[+] Device names saved to output file.

[+] Fetching DNS and DHCP server information...
[+] DNS and DHCP information saved to output file.

[+] Fetching ISP information...
[+] ISP information saved to output file.
```

```
[+] Checking connection type...
[+] Connection type saved to output file.

[+] Displaying instructions to check public IP on Shodan...
[+] Instructions saved to output file.

[+] Fetching WHOIS information for public IP...
[+] WHOIS information saved to output file.

[+] Capturing network traffic and identifying top three protocols...
Running as user "root" and group "root". This could be dangerous.
Capturing on 'eth0'
7
[+] Protocols information saved to output file.

[+] Explaining captured protocols...
[+] Protocol explanations saved to output file.

[+] Identifying port numbers for captured protocols...
[+] Port numbers saved to output file.


[+] Script execution complete. Check 'network_info.txt' for the results.

┌──(root㉿kali)-[/home/kali/Desktop/project/project_ intro]
└─#
```

```
Network and System Information
==============================

1.1 Devices IP Addresses:
---------------------------------
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-23 04:35 EST
Nmap scan report for 192.168.189.1
Host is up (0.00028s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.189.2
Host is up (0.00016s latency).
MAC Address: 00:50:56:ED:0E:F4 (VMware)
Nmap scan report for 192.168.189.254
Host is up (0.00029s latency).
MAC Address: 00:50:56:FD:FC:15 (VMware)
Nmap scan report for 192.168.189.145
Host is up.
Nmap scan report for 192.168.189.166
Host is up.
Nmap scan report for 192.168.189.1
Host is up (0.00023s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.189.2
Host is up (0.00013s latency).
MAC Address: 00:50:56:ED:0E:F4 (VMware)
Nmap scan report for 192.168.189.254
Host is up (0.00015s latency).
MAC Address: 00:50:56:FD:FC:15 (VMware)
Nmap scan report for 192.168.189.145
Host is up.
Nmap scan report for 192.168.189.166
Host is up.
Nmap done: 512 IP addresses (10 hosts up) scanned in 7.03 seconds
```

```
1.2 Devices MAC Address and Vendor (partial):
--------------------------------
Interface: eth0, type: EN10MB, MAC: 00:0c:29:63:dc
Starting arp-scan 1.10.0 with 256 hosts (https://g
192.168.189.1   00:50:56:c0:00:08   VMware, Inc.
192.168.189.2   00:50:56:ed:0e:f4   VMware, Inc.
192.168.189.254 00:50:56:fd:fc:15   VMware, Inc.

3 packets received by filter, 0 packets dropped by
Ending arp-scan 1.10.0: 256 hosts scanned in 1.957
```

```
1.3 Router's Internal and External IP Addresses (partial):
-------------------------------
Router Internal IP: 192.168.189.2
192.168.189.2
Router External IP: 31.187.78.XXX
```

```
1.4 Device Names:
-----------------------------------
Nmap scan report for 192.168.189.1
Nmap scan report for 192.168.189.2
Nmap scan report for 192.168.189.254
Nmap scan report for 192.168.189.145
Nmap scan report for 192.168.189.166
Nmap scan report for 192.168.189.1
Nmap scan report for 192.168.189.2
Nmap scan report for 192.168.189.254
Nmap scan report for 192.168.189.145
Nmap scan report for 192.168.189.166
```

1.5 DNS and DHCP IP Addresses:

DNS Server: 192.168.189.2
DNS Server: 192.168.189.2
DHCP Server: 192.168.189.254;

1.6 Internet Service Provider (ISP):

ISP: PacketHub S.A.

```
1.7 Connection Type (Ethernet or Wireless):
-------------------------------------------
eth0 - ethernet
eth1 - ethernet
lo - loopback
```

```
2.1 Shodan Check for Public IP:
-------------------------------
Visit https://shodan.io and check your public IP: 31.187.78.209
```

```
2.2 WHOIS for Public IP Address:
-----------------------------------
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See https://docs.db.ripe.net/terms-conditions.html

% Note: this output has been filtered.
%       To receive output for a database update, use the "-B" flag.

% Information related to '31.187.78.128 - 31.187.78.255'

% Abuse contact for '31.187.78.128 - 31.187.78.255' is 'abuse@packethub.tech'

inetnum:        31.187.78.128 - 31.187.78.255
netname:        PACKETHUB-20221107
descr:          Packethub S.A.
country:        IL
org:            ORG-PS409-RIPE
admin-c:        AG25300-RIPE
tech-c:         AG25300-RIPE
status:         ASSIGNED PA
mnt-by:         TERRATRANSIT-MNT
created:        2022-11-07T10:48:54Z
last-modified:  2022-11-07T10:48:54Z
source:         RIPE

organisation:   ORG-PS409-RIPE
```

2.3 Network Protocol Ports in Use:

53
80
443
32968
35486
35488
35766
36744

```
2.3.3 Port Online Lookup Results:
--------------------------------
- Port 53: DNS - Resolves domain names to IP addresses.
- Port 80: HTTP - Used for web page traffic.
- Port 443: HTTPS - Secure web page traffic.
- Port 36054: Unknown Port
- Port 38712: Unknown Port
- Port 39332: Unknown Port
```