Lab 5: Perform Basic Network Scanning in Kali Linux

1. Verify ISP and Public IP Address

Why: To know which ISP you're using and check if your public IP is dynamic or static. This is helpful in identifying if you're behind a proxy or NAT.

Steps:

1.1. Get Your Public IP:

Syntax: curl ifconfig.me

```
File  Actions  Edit  View  Help
┌──(sayujya㉿kali)-[~]
└─$ curl ifconfig.me

110.44.115.199
```

1.2. Get ISP Details Using whois

Syntax: whois <YOUR_PUBLIC_IP>

```
┌──(sayujya㉿kali)-[~]
└─$ whois 110.44.115.199
% [whois.apnic.net]
% Whois data copyright terms    http://www.apnic.net/db/dbcopyright.html

% Information related to '110.44.112.0 - 110.44.127.255'

% Abuse contact for '110.44.112.0 - 110.44.127.255' is 'abuse@vianet.com.np'

inetnum:        110.44.112.0 - 110.44.127.255
netname:        VIANET-NP
descr:          VIA NET COMMUNICATION LTD
country:        NP
org:            ORG-VCPL1-AP
admin-c:        VNCL1-AP
tech-c:         VNCL1-AP
abuse-c:        AV420-AP
status:         ALLOCATED PORTABLE
remarks:        Used for voip
remarks:        ----------------------------------------------------------
remarks:        To report network abuse, please contact mnt-irt
remarks:        For troubleshooting, please contact tech-c and admin-c
remarks:        Report invalid contact via www.apnic.net/invalidcontact
remarks:        ----------------------------------------------------------
mnt-by:         APNIC-HM
mnt-lower:      MAINT-VIANET-NP
mnt-routes:     MAINT-VIANET-NP
mnt-irt:        IRT-VIANET-NP
last-modified:  2024-12-10T03:47:07Z
source:         APNIC

irt:            IRT-VIANET-NP
address:        Jawalakhel Lalitpur Nepal
e-mail:         abuse@vianet.com.np
abuse-mailbox:  abuse@vianet.com.np
admin-c:        OM531-AP
tech-c:         OM531-AP
auth:           # Filtered
remarks:        abuse@vianet.com.np is invalid
```

2. Check Website Response (Slow or Not Working)

Why: To find out whether the issue is with the website server, your network, or DNS resolution.

Steps:

2.1. Ping the Website:

Syntax: ping www.daraz.com.np

```
┌──(sayujya㉿kali)-[~]
└─$ ping www.daraz.com.np
PING www.daraz.com.np (47.246.167.152) 56(84) bytes of data.
64 bytes from 47.246.167.152: icmp_seq=1 ttl=89 time=70.5 ms
64 bytes from 47.246.167.152: icmp_seq=2 ttl=89 time=71.4 ms
64 bytes from 47.246.167.152: icmp_seq=3 ttl=89 time=70.3 ms
64 bytes from 47.246.167.152: icmp_seq=4 ttl=89 time=71.8 ms
64 bytes from 47.246.167.152: icmp_seq=5 ttl=89 time=70.0 ms
64 bytes from 47.246.167.152: icmp_seq=6 ttl=89 time=71.2 ms
^C
--- www.daraz.com.np ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 19127ms
rtt min/avg/max/mdev = 70.033/70.877/71.799/0.628 ms
```

2.2. Check HTTP Response Headers

Syntax: curl -i https://www.daraz.com.np

```
┌──(sayujya㉿kali)-[~]
└─$ curl -i https://www.daraz.com.np
HTTP/2 200
date: Sat, 10 May 2025 18:29:05 GMT
content-type: text/html; charset=utf-8
vary: Accept-Encoding
vary: Accept-Encoding
x-content-type-options: nosniff
x-download-options: noopen
strict-transport-security: max-age=31536000
x-readtime: 188
vary: Accept-Encoding
x-server-id: 796d9b31cc436b97417757c2dc609f98702be2b3d115650e816c0f0fc00a6113
x-frame-options: SAMEORIGIN
x-xss-protection: 1; mode=block
cache-control: max-age=60, s-maxage=120
cache-control: no-cache, no-store
server: Tengine/Aserver
eagleeye-traceid: 2141047417469017448454337ee378
strict-transport-security: max-age=31536000
timing-allow-origin: *

<!DOCTYPE HTML>

<html><head><meta name="page-url" content="https://pages.daraz.com.np/wow/gcp/route/daraz/np/upr/router?hybrid=1&data_prefetch=true&prefetch_replace=1&at_iframe=1&wh_pid=/lazada/channel/np/homepage/home" ><script>window.gcpMarks = {};
            window.gcpMarks.htmlStart = Date.now();</script>

<link href="//g.lazcdn.com/" rel="preconnect" importance="high"><link href="//lzd-img-global.slatic.net/" rel="preconnect" importance="high"><link href="//acs-m.daraz.com.np" rel="preconnect"><link rel="preload" href="//g.lazcdn.com/res-d/alilog/mlog/aplus/202980191.js" as="script"><link rel="preload" crossorigin="anonymous" href="//g.lazcdn.com/g/woodpeckerx/itrace-next/7?itrace-jserror.iife.js,itrace-interface.iife.js,itrace-perf.iife.js,itrace-flow.iife.js,itrace-blank.iife.js,itrace-resource.iife.js,itrace.iife.js" as="script"><link rel="preload" crossorigin="anonymous" href="https://g.lazcdn.com/res-o/lzdfe/lzd-h5-itrace/index-module.js" as="script"><link rel="preload" crossorigin="anonymous" href="//g.lazcdn.com/res-o/lzd_sec/LWSC/index.js" as="script">
    <link rel="preload" href="//g.lazcdn.com/g/lzd/assets/1.2.13/font/EuclidCircularA-Regular.woff2" as="font" crossorigin="anonymous">
    <link rel="preload" href="//g.lazcdn.com/g/lzd/assets/1.2.13/font/EuclidCircularA-Medium.woff2" as="font" crossorigin="anonymous">
    <link rel="preload" href="//g.lazcdn.com/g/lzd/assets/1.2.13/font/EuclidCircularA-Bold.woff2" as="font" crossorigin="anonymous">
```

2.3. DNS Resolution:

Syntax: nslookup www.daraz.com.np

```
┌──(sayujya㉿kali)-[~]
└─$ nslookup www.daraz.com.np
Server:         192.168.1.1
Address:        192.168.1.1#53

Non-authoritative answer:
www.daraz.com.np        canonical name = daraz.wagbridge.alibaba-inc.com.
daraz.wagbridge.alibaba-inc.com canonical name = daraz.wagbridge.alibaba-inc.com.gds.alibabadns.com.
daraz.wagbridge.alibaba-inc.com.gds.alibabadns.com      canonical name = daraz-sg.alibaba.com.
daraz-sg.alibaba.com    canonical name = daraz-sg.alibaba.com.gds.alibabadns.com.
daraz-sg.alibaba.com.gds.alibabadns.com canonical name = lazada-sg-2.daraz.wagbridge.aserver-lazada.alibaba.com.
lazada-sg-2.daraz.wagbridge.aserver-lazada.alibaba.com  canonical name = lazada-sg-2.daraz.wagbridge.aserver-lazada.alibaba.com.gds.alibabadns.com.
Name:   lazada-sg-2.daraz.wagbridge.aserver-lazada.alibaba.com.gds.alibabadns.com
Address: 47.246.167.240
```

2.4. Trace Route to Website:

Syntax: traceroute www.daraz.com.np

```
┌──(sayujya㉿kali)-[~]
└─$ traceroute www.daraz.com.np
traceroute to www.daraz.com.np (47.246.165.107), 30 hops max, 60 byte packets
 1  192.168.1.1 (192.168.1.1)  4.654 ms  4.597 ms  4.574 ms
 2  192.168.101.1 (192.168.101.1)  4.553 ms  4.530 ms  4.509 ms
 3  103.41.174.145 (103.41.174.145)  5.145 ms  5.124 ms  10.520 ms
 4  103.41.174.133 (103.41.174.133)  10.496 ms  10.475 ms  5.023 ms
 5  103.10.28.34 (103.10.28.34)  10.408 ms  10.387 ms  10.357 ms
 6  ae0-bg2.vianet.com.np (110.44.112.66)  10.332 ms  5.307 ms  5.267 ms
 7  125.19.67.33 (125.19.67.33)  7.761 ms  7.744 ms  7.726 ms
 8  116.119.121.121 (116.119.121.121)  83.263 ms 182.79.146.196 (182.79.146.196)  69.735 ms 116.119.81.0 (116.119.81.0)  72.538 ms
 9  45102.sgw.equinix.com (27.111.229.234)  70.374 ms  84.789 ms  85.254 ms
10  * * 47.246.115.225 (47.246.115.225)  73.717 ms
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```

3. Scan Website for Open Ports

Why: To detect which ports are open or blocked (e.g., port 3000 for a Node.js app).

Syntax: nmap -p 80,443,3000,8080 www.hamrobazaar.com

```
┌──(sayujya㉿kali)-[~]
└─$ nmap -p 80,443,3000,8080 www.hamrobazaar.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 14:43 EDT
Nmap scan report for www.hamrobazaar.com (104.25.121.14)
Host is up (0.0057s latency).
Other addresses for www.hamrobazaar.com (not scanned): 104.25.120.14

PORT     STATE    SERVICE
80/tcp   open     http
443/tcp  open     https
3000/tcp filtered ppp
8080/tcp open     http-proxy

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

4. Identify Website Hosting and Server Type

Why: To know whether the website is hosted in Nepal or abroad and understand the server details for further scanning.

Syntax: whatweb www.hamrobazaar.com

```
┌──(sayujya㉿kali)-[~]
└─$ whatweb www.hamrobazaar.com
http://www.hamrobazaar.com [301 Moved Permanently] Country[UNITED STATES][US], HTTPServe
r[cloudflare], IP[104.25.121.14], RedirectLocation[https://hamrobazaar.com/], Title[301
Moved Permanently], UncommonHeaders[report-to,nel,cf-ray,alt-svc,server-timing]
https://hamrobazaar.com/ [200 OK] Access-Control-Allow-Methods[*], HTML5, HTTPServer[ngi
nx-more], IP[103.255.126.189], Open-Graph-Protocol[website], Script[application/ld+json]
, Title[Hamrobazar - Nepal's Online Marketplace for Shopping], UncommonHeaders[access-co
ntrol-allow-origin,access-control-allow-methods,access-control-allow-headers], X-Powered
-By[Express]
```

5. Check for ISP-level Port Blocking

Why: Some Nepali ISPs block certain ports (e.g., port 22 SSH, or port 3000 Node.js).

5.1. Scan Your Own Public IP from Another Network or VPN

Syntax: nmap -Pn -p 22,80,443,3000 <YOUR_PUBLIC_IP>

```
┌──(sayujya㉿kali)-[~]
└─$ nmap -Pn -p 22,80,443,3000 110.44.115.199
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-10 14:48 EDT
Nmap scan report for 110.44.115.199
Host is up.

PORT     STATE    SERVICE
22/tcp   filtered ssh
80/tcp   filtered http
443/tcp  filtered https
3000/tcp filtered ppp

Nmap done: 1 IP address (1 host up) scanned in 16.24 seconds
```

Conclusion

Using Kali Linux and tools like nmap, curl, traceroute, ping, and whois, you can:

- Identify your ISP and IP location.
- Troubleshoot website accessibility.
- Check for blocked or open ports.
- Determine if a Nepali website is hosted locally or abroad.
- Analyze possible ISP or firewall restrictions.