

Lab1 Submission: Zenmap

Samantha Jackson

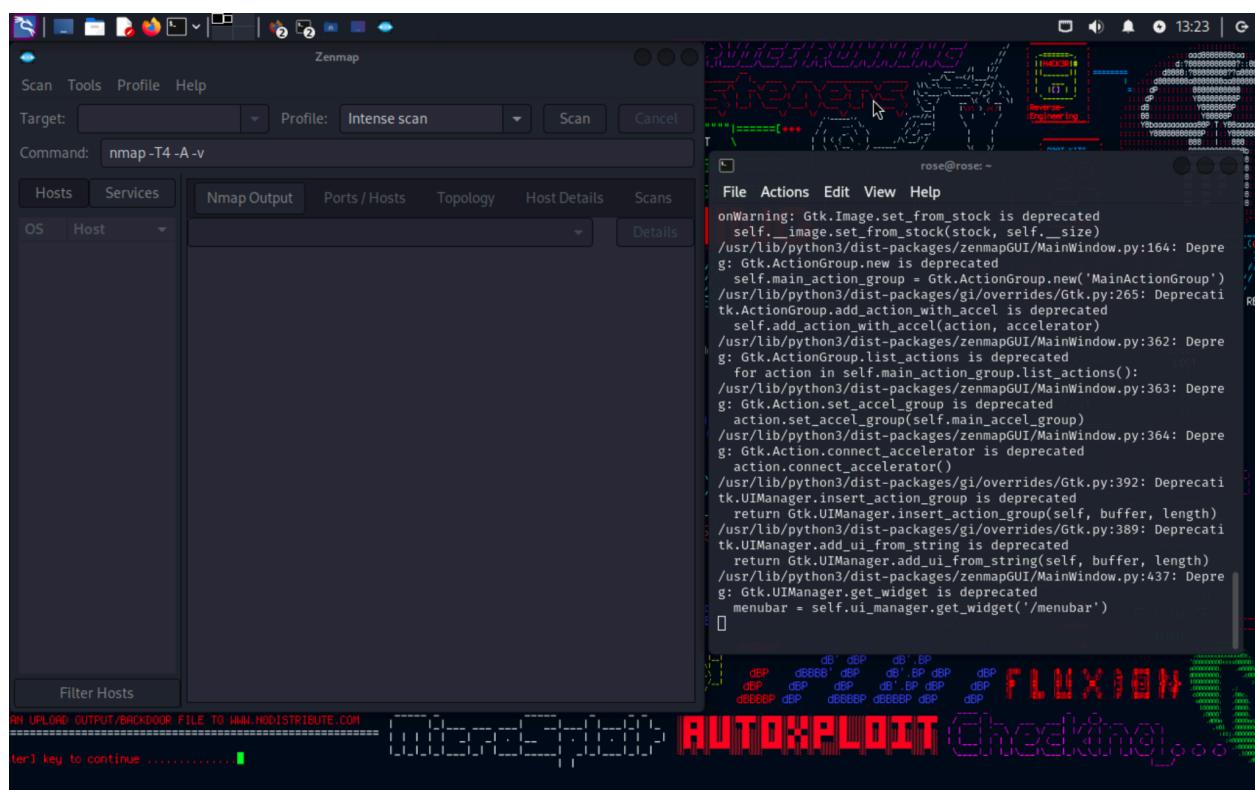
CSCI 4321

Computer Security

January 22, 2025

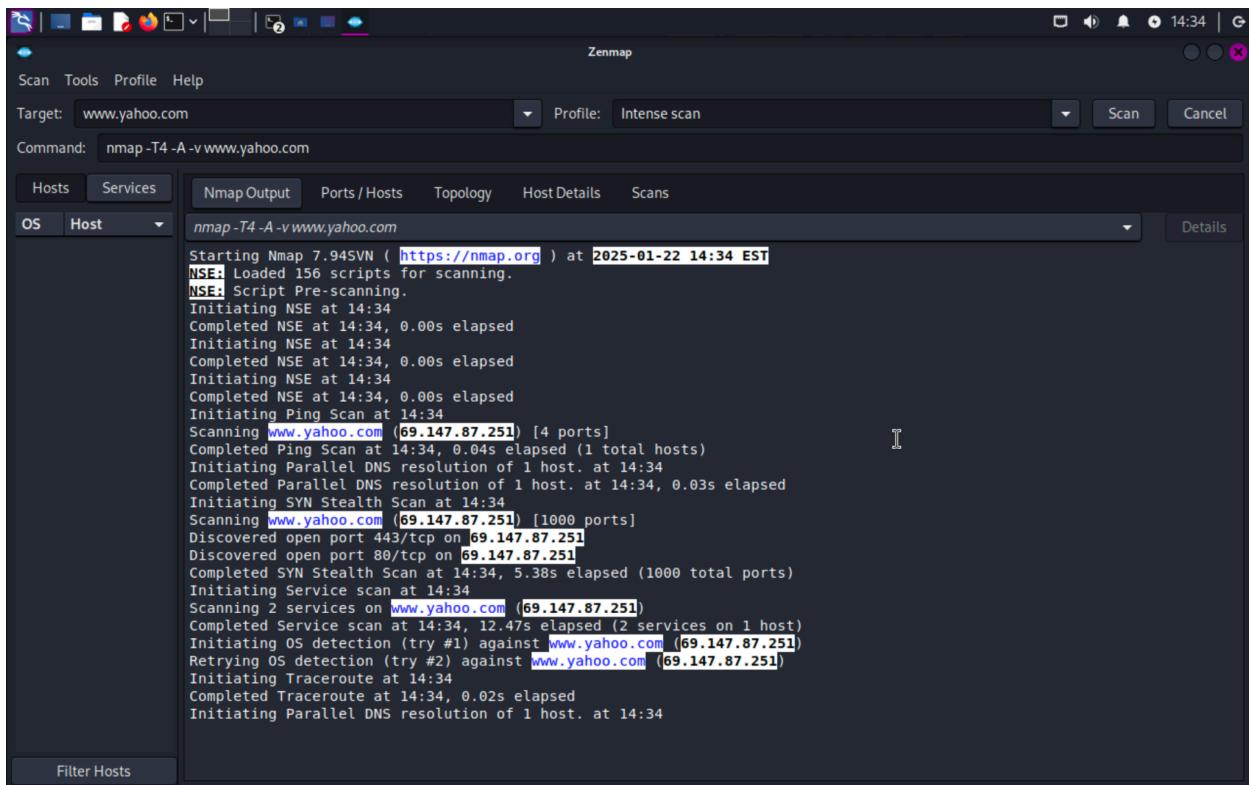
Kali Installation

A Kali Linux ARM ISO was installed from the Kali Linux website and was downloaded in VMWare. The most popular packages were preinstalled, this included the Zenmap package. Zenmap is a GUI version of the NMAP network scanner.



Zenmap

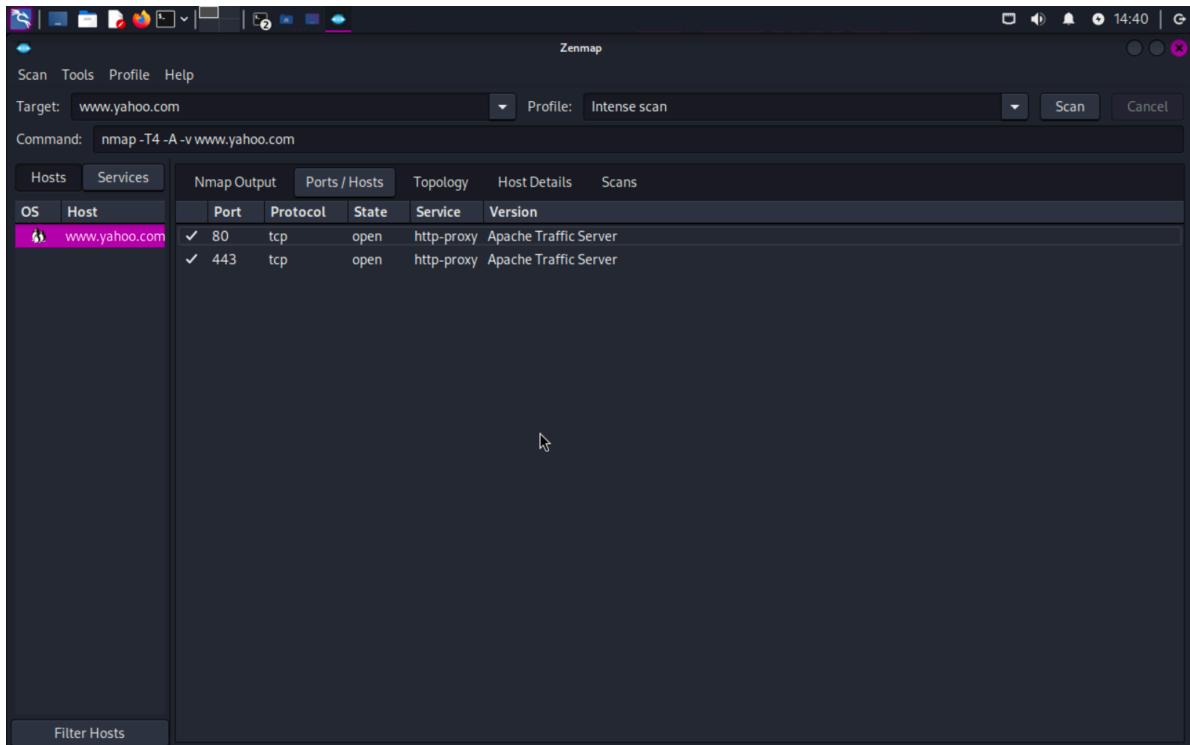
For the tutorial I used this link <https://youtu.be/0uGyMpUdKpU?si=qR0j6u9ZHaMwMZ-Z> to get an idea of how the Zenmap package works. Zenmap primarily uses NMAP console commands. For this example we'll target the www.yahoo.com hostname and use an intense scan profile. The console command will be nmap -T4 -A -v www.yahoo.com



The screenshot shows the Zenmap application window. At the top, there's a toolbar with icons for file operations like Open, Save, and Print. Below the toolbar is a menu bar with Scan, Tools, Profile, and Help. The main area has tabs for Scan, Tools, Profile, and Help, with Profile currently selected. Under Profile, it says "Profile: Intense scan". Below that is a Command field containing "nmap -T4 -A -v www.yahoo.com". The main pane displays the Nmap output. The output starts with "Starting Nmap 7.94SVN (https://nmap.org) at 2025-01-22 14:34 EST". It then lists various NSE (Nmap Script Engine) scripts being loaded and run. The output continues with "Initiating Ping Scan at 14:34", "Scanning www.yahoo.com (69.147.87.251) [4 ports]", and "Completed Ping Scan at 14:34, 0.04s elapsed (1 total hosts)". It then moves on to "Initiating Parallel DNS resolution of 1 host. at 14:34", "Completed Parallel DNS resolution of 1 host. at 14:34, 0.03s elapsed", and "Initiating SYN Stealth Scan at 14:34". The output continues with "Scanning www.yahoo.com (69.147.87.251) [1000 ports]", "Discovered open port 443/tcp on 69.147.87.251", "Discovered open port 80/tcp on 69.147.87.251", and "Completed SYN Stealth Scan at 14:34, 5.38s elapsed (1000 total ports)". It then performs a "Service scan" and "OS detection" on the discovered ports. Finally, it completes the "Traceroute" and "Parallel DNS resolution".

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 14:34 EST
NSE: Loaded 150 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Script Pre-scanning.
Initiating NSE at 14:34
Completed NSE at 14:34, 0.00s elapsed
Initiating NSE at 14:34
Completed NSE at 14:34, 0.00s elapsed
Initiating NSE at 14:34
Completed NSE at 14:34, 0.00s elapsed
Initiating NSE at 14:34
Completed NSE at 14:34, 0.00s elapsed
Initiating NSE at 14:34
Completed NSE at 14:34, 0.00s elapsed
Initiating Ping Scan at 14:34
Scanning www.yahoo.com (69.147.87.251) [4 ports]
Completed Ping Scan at 14:34, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 14:34
Completed Parallel DNS resolution of 1 host. at 14:34, 0.03s elapsed
Initiating SYN Stealth Scan at 14:34
Scanning www.yahoo.com (69.147.87.251) [1000 ports]
Discovered open port 443/tcp on 69.147.87.251
Discovered open port 80/tcp on 69.147.87.251
Completed SYN Stealth Scan at 14:34, 5.38s elapsed (1000 total ports)
Initiating Service scan at 14:34
Scanning 2 services on www.yahoo.com (69.147.87.251)
Completed Service scan at 14:34, 12.47s elapsed (2 services on 1 host)
Initiating OS detection (try #1) against www.yahoo.com (69.147.87.251)
Retrying OS detection (try #2) against www.yahoo.com (69.147.87.251)
Initiating Traceroute at 14:34
Completed Traceroute at 14:34, 0.02s elapsed
Initiating Parallel DNS resolution of 1 host. at 14:34
```

The first piece of information extracted from Zenmap was the TCP port status on 443/TCP and 80/TCP. There were several available tabs that break down the extrapolated data in different formats. For instance the Ports/Host tab displays the ports in a table format. The topology shows the topology of the scanned host. The Host Details break down relevant data about the operating system, host name, addresses and status of the domain that was scanned. For our instance Zenmap believes the yahoo domain is using an Actiontec OS.



Zenmap

Scan Tools Profile Help

Target: www.yahoo.com Profile: Intense scan

Command: nmap -T4 -A -v www.yahoo.com

Hosts Services

Nmap Output Ports / Hosts Topology Host Details Scans

nmap -T4 -A -v www.yahoo.com

Host is up (0.023s latency).

Other addresses for www.yahoo.com (not scanned): 69.147.87.252 2001:4998:20:807::2 2001:4998:20:807::1

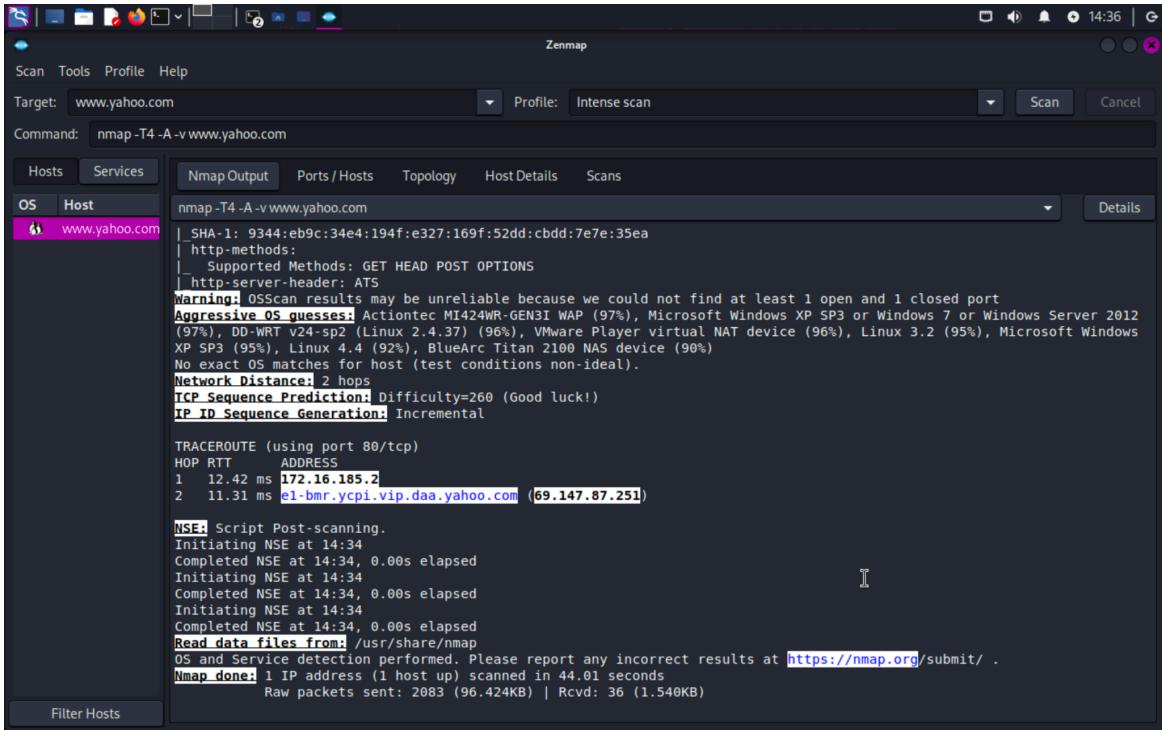
rDNS record for 69.147.87.251: e1-bmr.ycpi.vip.daa.yahoo.com

Not shown: 998 filtered tcp ports (no-response)

| PORT | STATE | SERVICE | VERSION |
|---------|-------|----------------|-----------------------|
| 80/tcp | open | http-proxy | Apache Traffic Server |
| 443/tcp | open | ssl/http-proxy | Apache Traffic Server |

```
|_ http-favicon: Unknown favicon MD5: 3A07174943F82046370997254100D870
|_ http-methods:
|   Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Did not follow redirect to https://www.yahoo.com
|_ http-server-header: ATS
|_ http-server-sub: Yahoo
|_ http-server-sub: Yahoo Holdings Inc.
|_ http-server-sub: New York
|_ http-server-sub: US
|_ Subject Alternative Name: DNS:api.fantasysports.yahoo.com, DNS:ymail.com, DNS:s.yimg.com, DNS:.yahoo.com, DNS:calendar.yahoo.com, DNS:groups.yahoo.com, DNS:mail.yahoo.com, DNS:msg.yahoo.com, DNS:ymail.com, DNS:finance.yahoo.com, DNS:news.yahoo.com, DNS:de.nachrichten.yahoo.com, DNS:video.yahoo.com, DNS:m.yahoo.com, DNS:my.yahoo.com, DNS:search.yahoo.com, DNS:secure.yahoo.com, DNS:yahooapis.com, DNS:img.mail.yahoo.com, DNS:fantasysports.yahoo.com, DNS:autos.yahoo.com, DNS:cricket.yahoo.com, DNS:football.fantasysports.yahoo.com, DNS:games.yahoo.com, DNS:lifestyle.yahoo.com, DNS:movies.yahoo.com, DNS:mujeer.yahoo.com, DNS:music.yahoo.com, DNS:safety.yahoo.com, DNS:screen.yahoo.com, DNS:shine.yahoo.com, DNS:sports.yahoo.com, DNS:travel.yahoo.com, DNS:tv.yahoo.com, DNS:weather.yahoo.com, DNS:notepad.yahoo.com, DNS:protrade.com, DNS:yql.yahoo.com, DNS:wc.yahoodns.net, DNS:help.yahoo.com, DNS:celebrity.yahoo.com, DNS:ybp.yahoo.com, DNS:geo.yahoo.com, DNS:messenger.yahoo.com, DNS:antispam.yahoo.com, DNS:ysm.yahoo.com, DNS:video.media.yql.yahoo.com, DNS:tripod.yahoo.com, DNS:iris.yahoo.com, DNS:mobile.yahoo.com, DNS:overview.mail.yahoo.com, DNS:mailplus.mail.yahoo.com, DNS:xobni.yahoo.com, DNS:onepush.query.yahoo.com, DNS:api.onepush.query.yahoo.com, DNS:commsdata.api.yahoo.com, DNS:commsdata.api.yahoo.com
```

Filter Hosts



The screenshot shows the Zenmap interface with the following details:

- Scan Type:** Intense scan
- Target:** www.yahoo.com
- Command:** nmap -T4 -A -v www.yahoo.com
- Hosts:** OS Host
- Services:** www.yahoo.com
- Nmap Output:**
 - SHA-1: 9344:eb9c:34e4:194f:e327:169f:52dd:cbdd:7e7e:35ea
 - http-methods:
 - GET HEAD POST OPTIONS
 - Supported Methods: GET HEAD POST OPTIONS
 - http-server-header: ATS
 - 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%), Microsoft Windows XP SP3 or Windows 7 or Windows Server 2012 (97%), DD-WRT V24-sp2 (Linux 2.4.37) (96%), VMware Player virtual NAT device (96%), Linux 3.2 (95%), Microsoft Windows XP SP3 (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
- TCP Sequence Prediction:** Difficulty=260 (Good luck!)
- IP ID Sequence Generation:** Incremental
- TRACEROUTE (using port 80/tcp):**

| HOP | RTT | ADDRESS |
|-----|----------|---|
| 1 | 12.42 ms | 172.16.185.2 |
| 2 | 11.31 ms | e1-bmr.ycp1.vip.daa.yahoo.com (69.147.87.251) |
- NSE Script Post-scanning.**
 - Initiating NSE at 14:34
 - Completed NSE at 14:34, 0.00s elapsed
 - Initiating NSE at 14:34
 - Completed NSE at 14:34, 0.00s elapsed
 - Initiating NSE at 14:34
 - Completed NSE at 14:34, 0.00s elapsed
 - Read data files from: /usr/share/nmap
- 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 44.01 seconds
- Raw packets sent:** 2083 (96.424KB) | Rcvd: 36 (1.540KB)

For additional testing I also scanned www.youtube.com with a normal Zenmap scan nmap www.youtube.com. This contained significantly less data than the yahoo scan.

Zenmap

Scan Tools Profile Help

Target: www.youtube.com Profile: Regular scan

Command: nmap www.youtube.com

Hosts Services

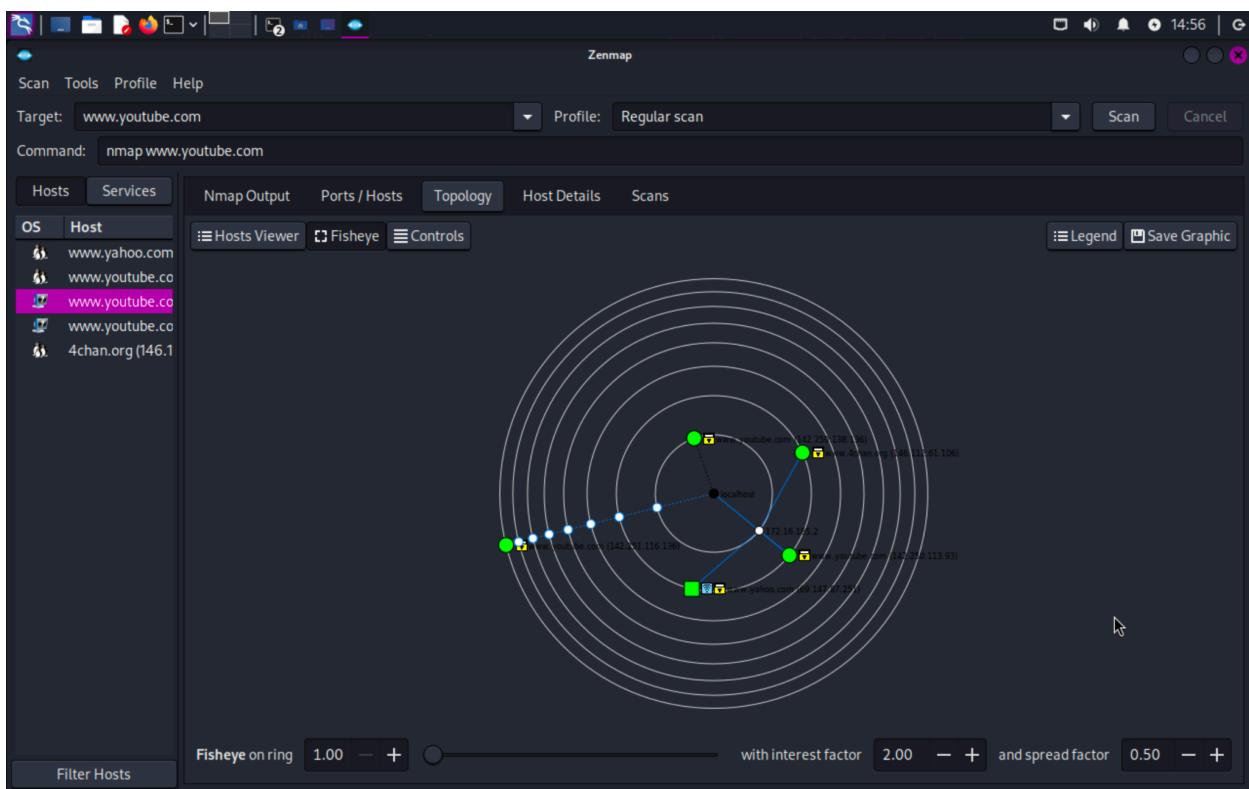
Nmap Output Ports / Hosts Topology Host Details Scans

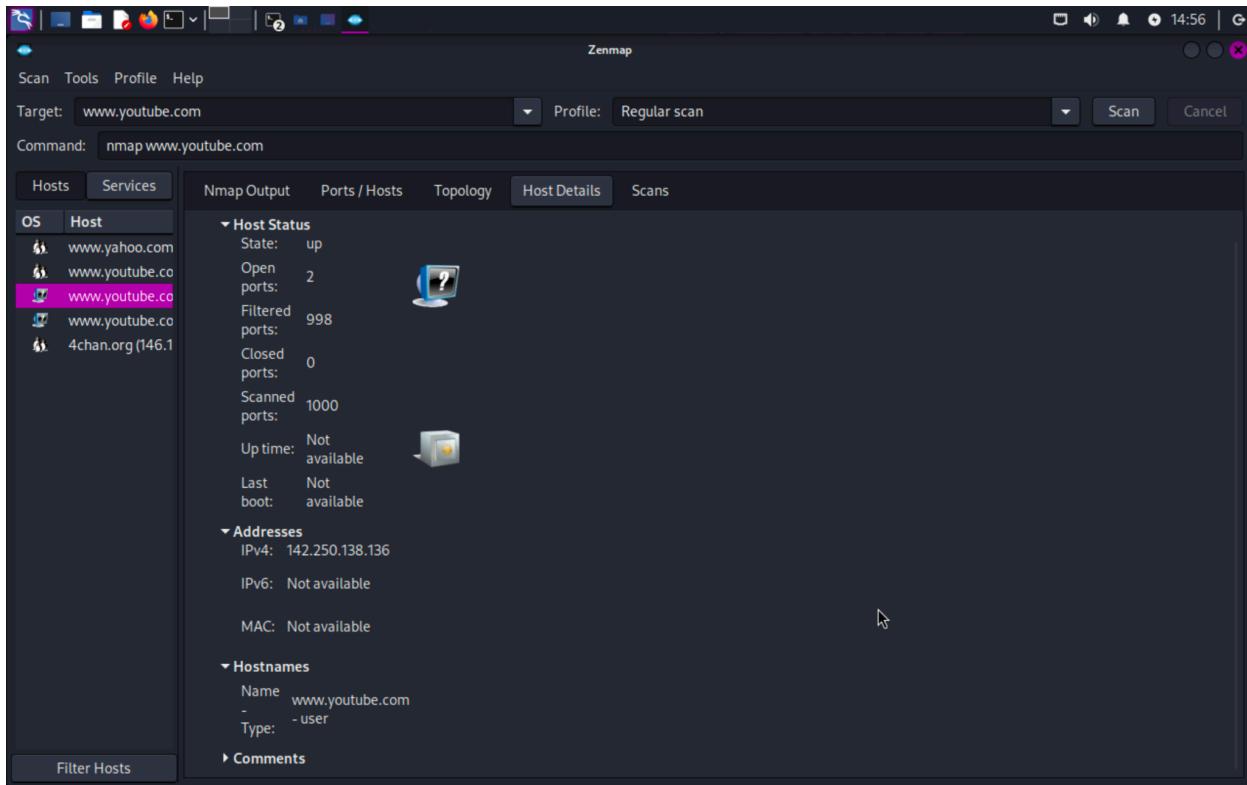
nmap www.youtube.com

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-01-22 14:49 EST
Nmap scan report for www.youtube.com (142.250.138.136)
Host is up (0.44s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```

Nmap done: 1 IP address (1 host up) scanned in 136.10 seconds

Filter Hosts





In this lab I learned how to use Zenmap on Kali Linux. I did this by downloading an instance of Kali Linux iso in VMware Fusion (ARM Branch). Then during the Kali installation I downloaded the popular packages which included Zenmap. Zenmap is an extremely powerful tool for analyzing the topology of a host and it allows a user to determine the status of the hostnames TCP ports. This is extremely useful for network analysis especially for security concerns. This was an extremely interesting and practical package. I hope we will continue to use it going forward.