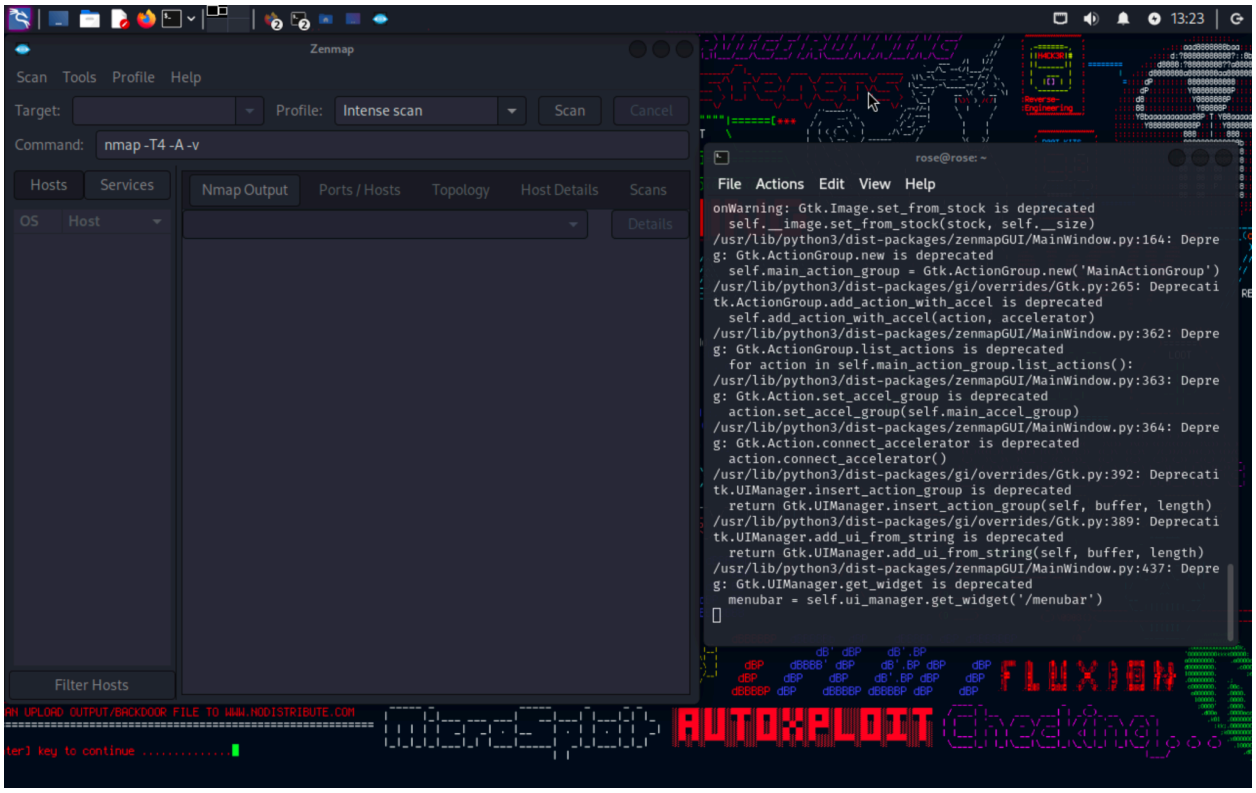
Lab1 Submission: Zenmap

Samantha Jackson
CSCI 4321
Computer Security
January 22, 2025

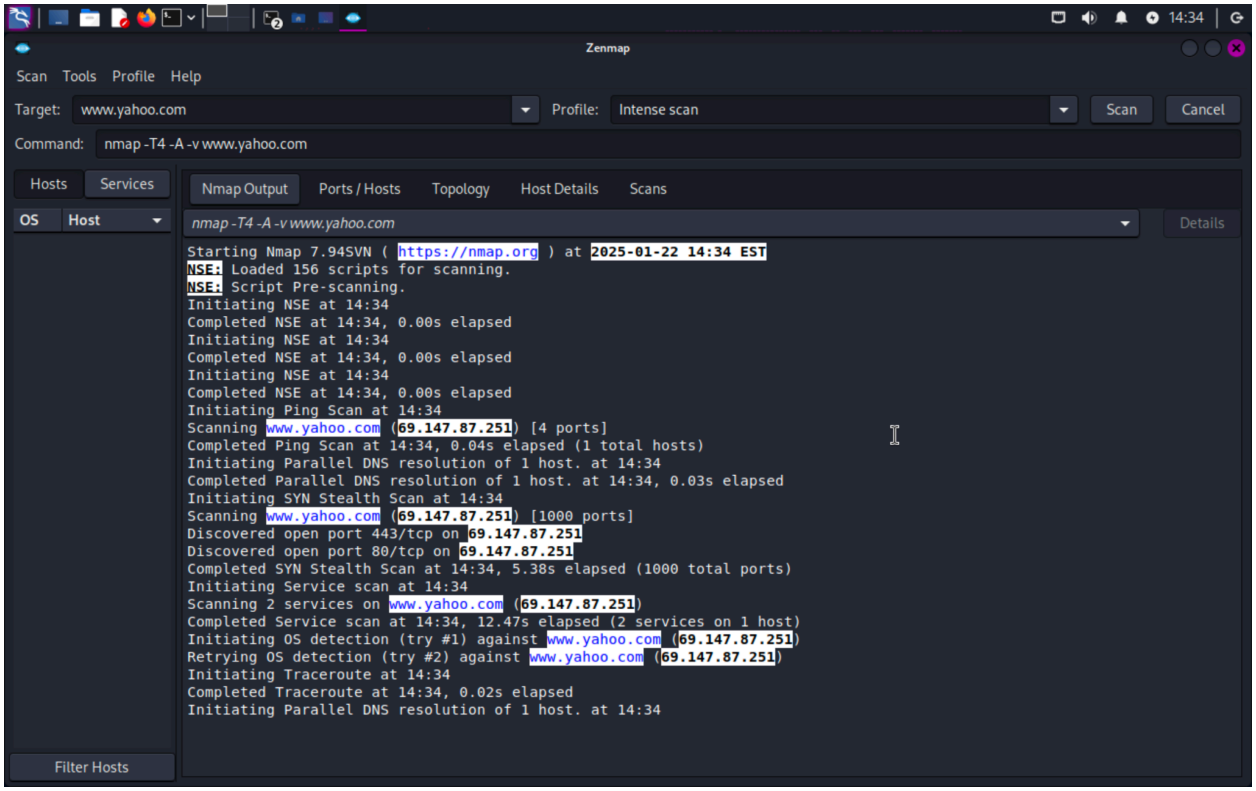
Kali Installation

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.

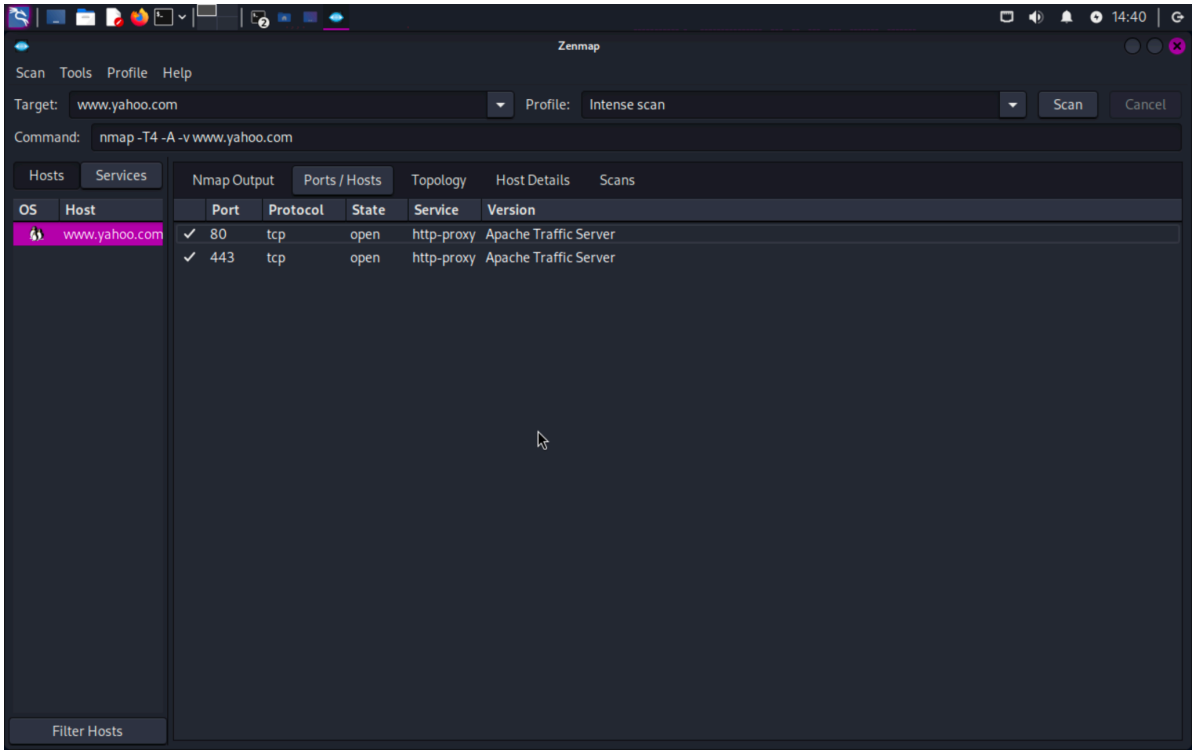


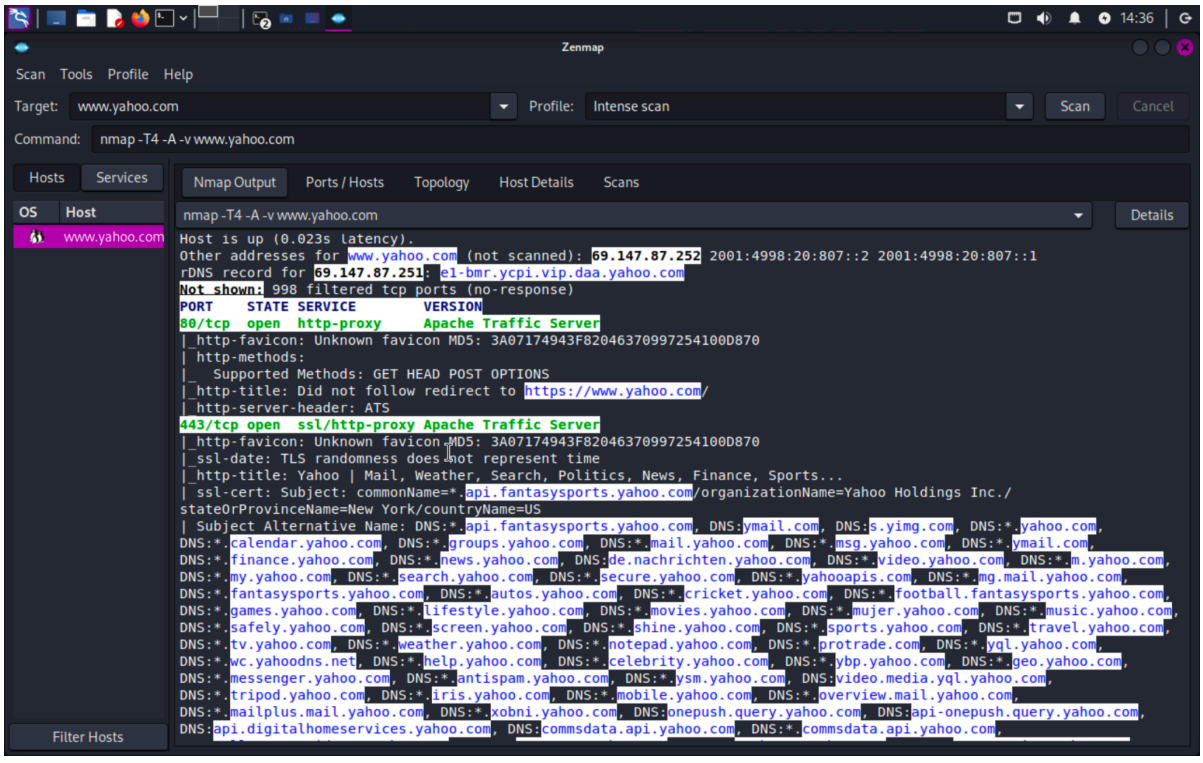
Zenmap

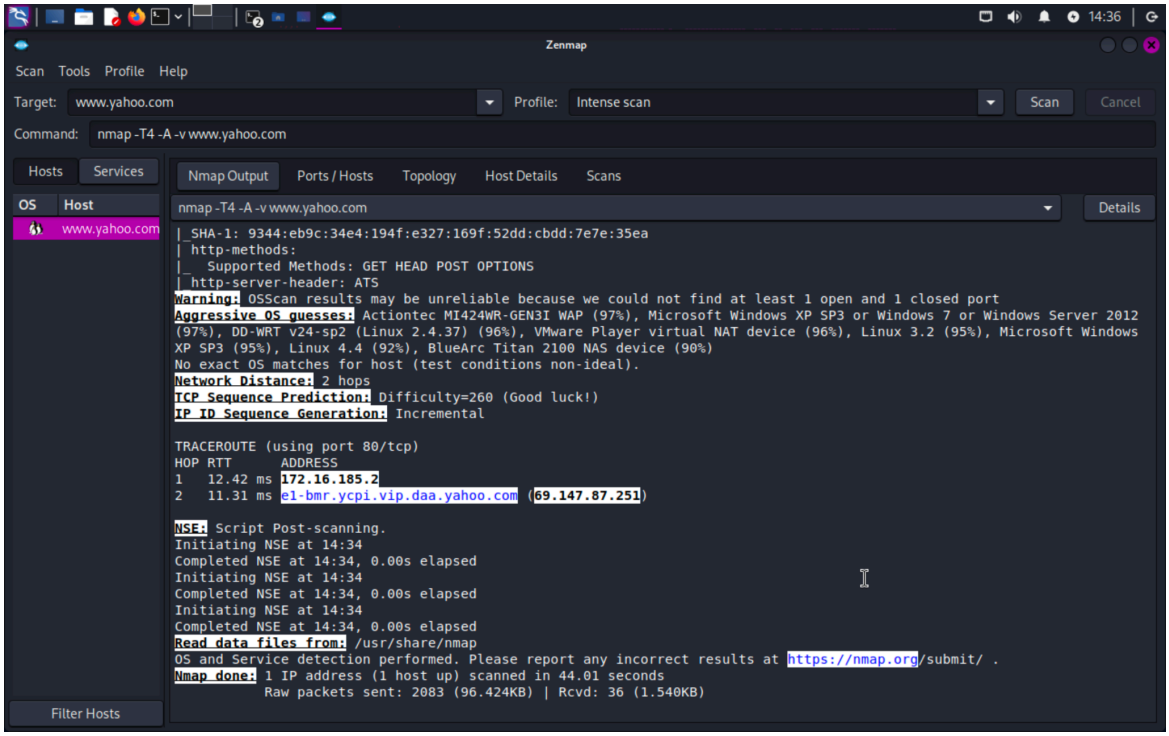
For the tutorial I used this link https://youtu.be/0uGyMpUdKpU?si=qR0j6u9ZHaMwMZ-Z to get an idea of how the Zenmap package works. Zenmap primarily uses NMAP console commands. For this example we'll target the www.yahoo.com hostname and use an intense scan profile. The console command will be nmap -T4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



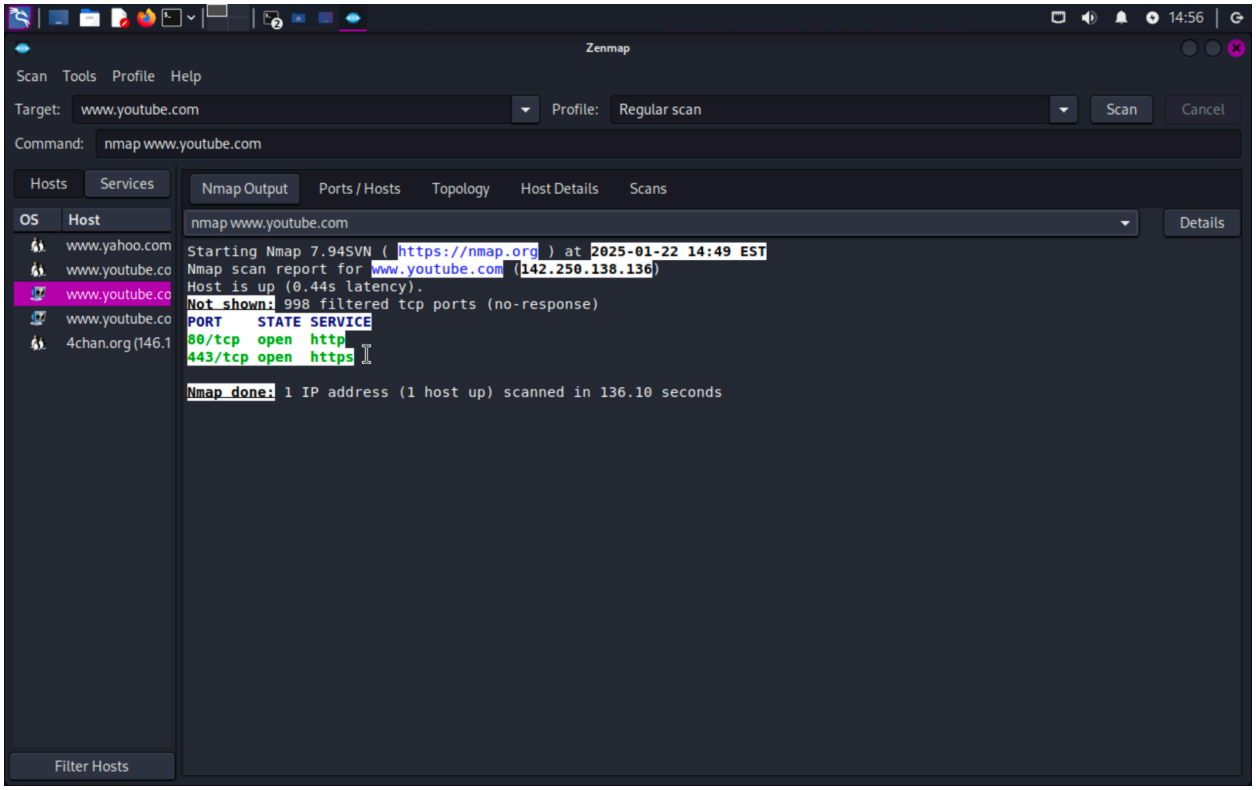
The first piece of information extracted from Zenmap was the TCP port status on 443/TCP and 80/TCP. There were several available tabs that break down the extrapolated data in different formats. For instance the Ports/Host tap displays the ports in a table format. The topology shows the topology of the 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.

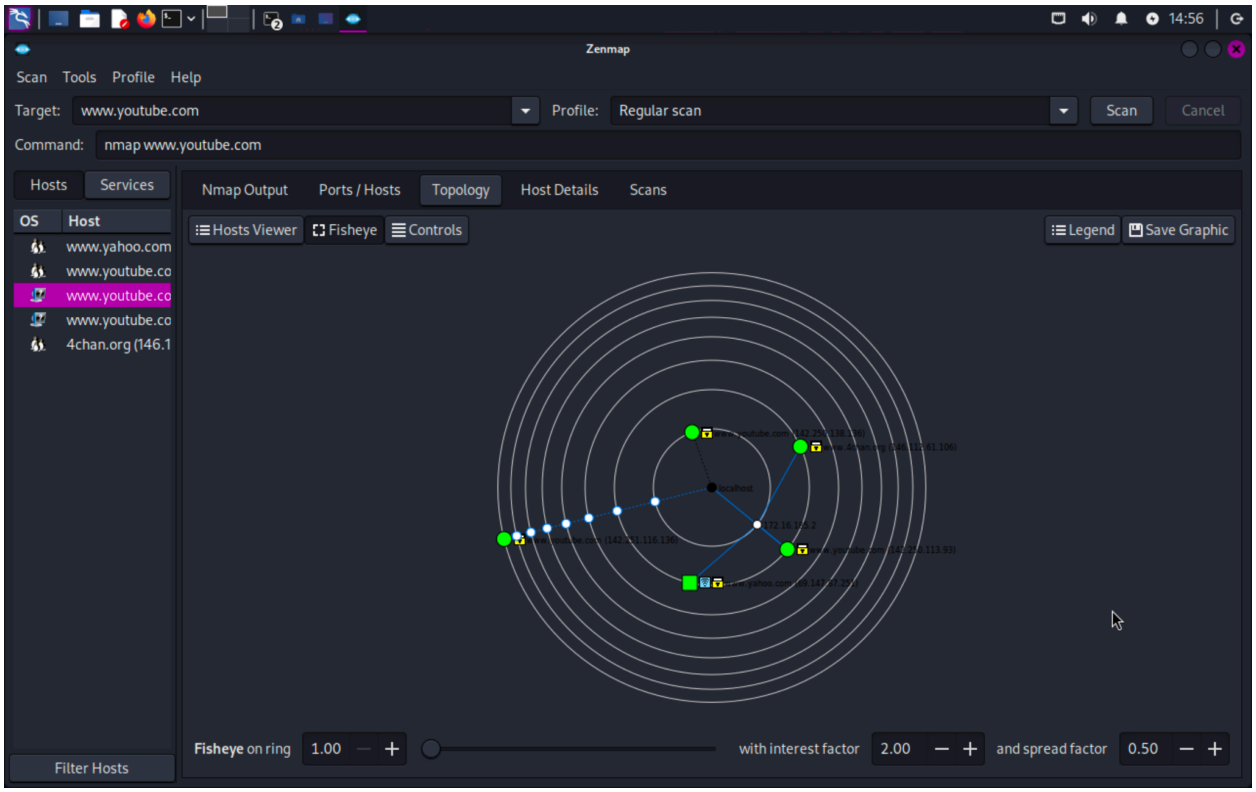

14:40
Zenmap
Scan Tools Profile Help
Target: www.yahoo.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v www.yahoo.com
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
www.yahoo.com
Port
Protocol
State
Service
Version
80
tcp
open
http-proxy
Apache Traffic Server
443
tcp
open
http-proxy
Apache Traffic Server
Filter Hosts

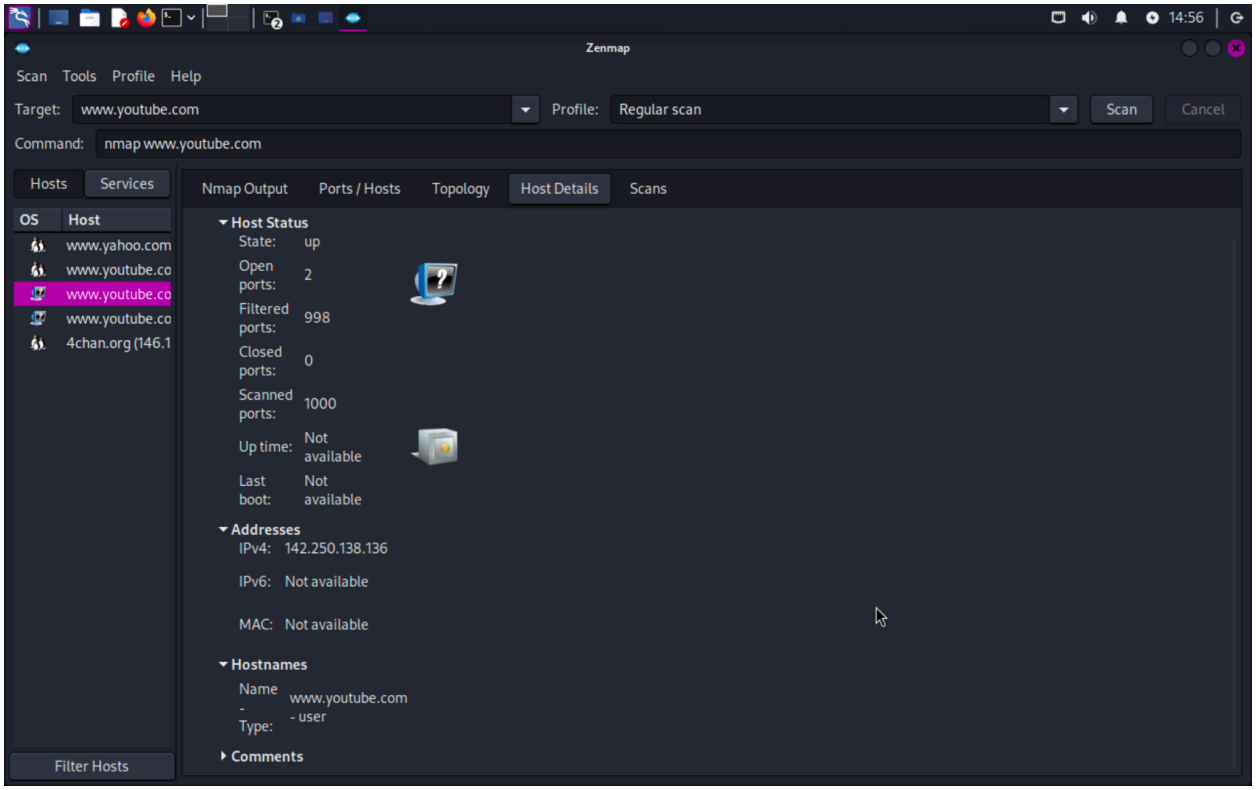

14:36
Zenmap
Scan Tools Profile Help
Target: www.yahoo.com
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v www.yahoo.com
Hosts
Services
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
OS
Host
www.yahoo.com
nmap -T4 -A -v www.yahoo.com
Details
Host is up (0.023s latency).
Other addresses 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
|_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
443/tcp open ssl/http-proxy Apache Traffic Server
|_http-favicon: Unknown favicon MD5: 3A07174943F82046370997254100D870
|_ssl-date: TLS randomness does not represent time
|_http-title: Yahoo | Mail, Weather, Search, Politics, News, Finance, Sports...
| ssl-cert: Subject: commonName=*.api.fantasysports.yahoo.com/organizationName=Yahoo Holdings Inc./
stateOrProvinceName=New York/countryName=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:*.mg.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:*.mujer.yahoo.com, DNS:*.music.yahoo.com,
DNS:*.safely.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:api.digitalhomeservices.yahoo.com, DNS:commsdata.api.yahoo.com, DNS:*.commsdata.api.yahoo.com,
Filter Hosts
]



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
Scan
Cancel
Command: nmap www.youtube.com
Hosts
Services
OS
Host
www.yahoo.com
www.youtube.co
www.youtube.co
www.youtube.co
4chan.org (146.1
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap www.youtube.com
Details
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


Zenmap
Scan Tools Profile Help
Target: www.youtube.com
Profile: Regular scan
Scan
Cancel
Command: nmap www.youtube.com
Hosts
Services
OS
Host
www.yahoo.com
www.youtube.co
www.youtube.co
www.youtube.co
4chan.org (146.1
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
Hosts Viewer
Fisheye
Controls
Legend
Save Graphic
localhost
Fisheye on ring 1.00
with interest factor 2.00
and spread factor 0.50



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.