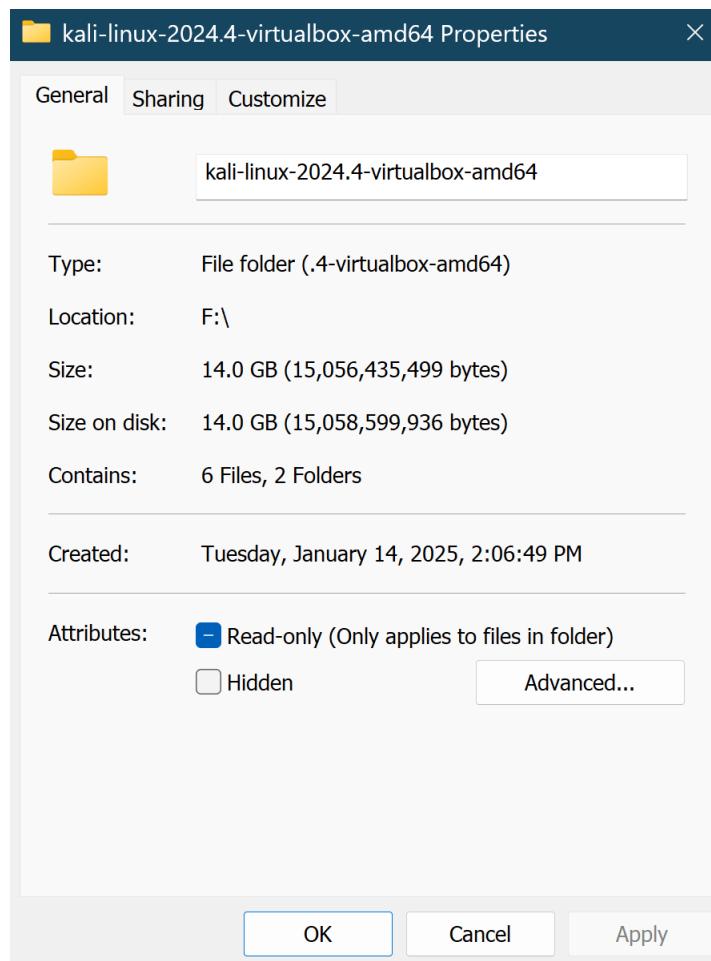


Lab1: Zenmap

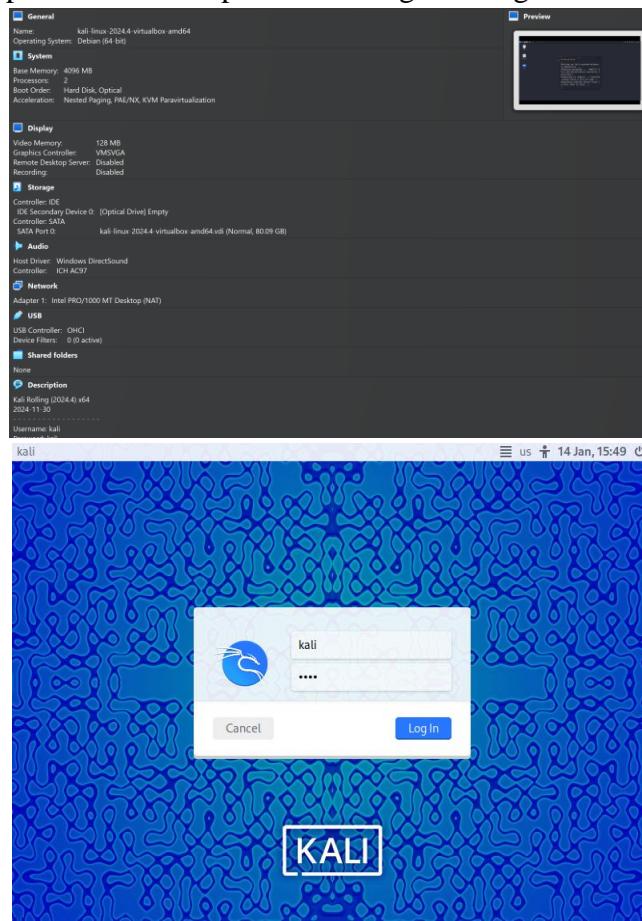
Joshua Ludolf
CSCI 4321
Computer Security
January 14, 2025

- The latest version of Kali Linux can be downloaded from their official website <https://www.kali.org>. From this website, I downloaded: VirtualBox (VDI) 64bit Download Size: 3.2GB (14.0GB when I extracted it from zipped folder). This image(based on the website) has the username: kali and the password kali.



Logs	1/14/2025 2:37 PM	File folder
kali-linux-2024.4-virtualbox-amd64.vb...	1/14/2025 2:54 PM	VirtualBox Machin...
kali-linux-2024.4-virtualbox-amd64.vb...	1/14/2025 2:54 PM	VBOX-PREV File
kali-linux-2024.4-virtualbox-amd64.vdi	1/14/2025 3:04 PM	Virtual Disk Image
kali-linux-2024.4-virtualbox-amd64-1....	11/30/2024 8:31 AM	VirtualBox Machin...

- After completing the download, I added (it was already in VirtualBox format - .vbox) the image in virtual box for the image disk that I downloaded. Additionally, I changed the background wallpaper of the desktop to be more simplistic and elegant design.





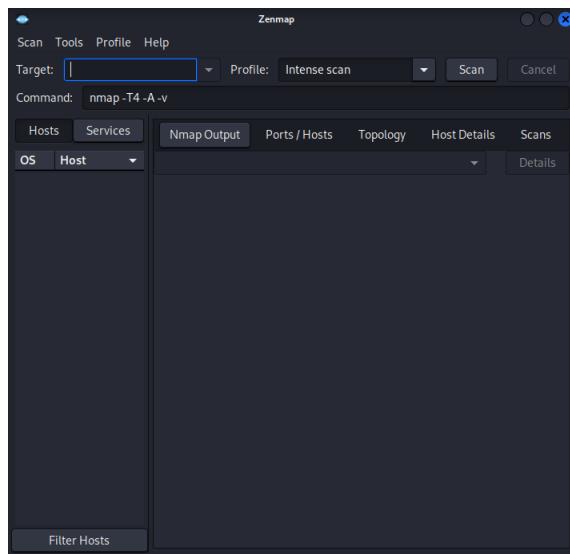
- I ran the following command to get lastest installation of Kali Linux: sudo apt-get update && sudo apt-get upgrade -y.

```
(kali㉿kali)-[~]
$ sudo apt-get update && sudo
apt-get upgrade
Hit:1 http://http.kali.org/kali
  kali-rolling InRelease
Reading package lists... Done
Reading package lists... Done
Building dependency tree... Done
Reading state information... 0%
Reading state information... Done
Calculating upgrade... Done
The following packages were automatically installed and are no
longer required:
  libfbio1 libc++1-19
  libc++abi1-19 libegl-dev
  libgl1-mesa-dev libgles-dev

Updating certificates in /etc/ssl/certs...
0 added, 0 removed; done.
Running hooks in /etc/ca-certificates/update.d...
done.
Processing triggers for php8.2-cli (8.2.27-1) ...
Processing triggers for libapache2-mod-php8.2 (8.2.27-1) ...
Processing triggers for ca-certificates-java (20240118) ...
done.

(kali㉿kali)-[~]
$
```

- Zenmap is a GUI version of NMAP network scanner (which is largely used as **port scanner/mapper**)



- The tool uses nmap console commands, for example, I selected a host and start intense scan, the console command will be nmap -T4 -A -v www.yahoo.com

A screenshot of the Zenmap software interface, specifically the "Nmap Output" tab. The window title is "Zenmap". The menu bar includes "Scan", "Tools", "Profile", and "Help". Below the menu is a "Target" field with "www.yahoo.com", a "Profile" dropdown set to "Intense scan", and "Scan" and "Cancel" buttons. The "Command" field contains "nmap -T4 -A -v www.yahoo.com". The main area has tabs for "Hosts", "Services", "Nmap Output", "Ports / Hosts", "Topology", "Host Details", and "Scans". The "Nmap Output" tab is selected. A dropdown menu under "Hosts" shows "OS" and "Host". The right side of the window displays the Nmap command and its progress:

```
nmap -T4 -A -v www.yahoo.com
Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-14 17:03 EST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:03
Completed NSE at 17:03, 0.00s elapsed
Initiating NSE at 17:03
Completed NSE at 17:03, 0.00s elapsed
Initiating NSE at 17:03
Completed NSE at 17:03, 0.00s elapsed
Initiating NSE at 17:03
Completed NSE at 17:03, 0.00s elapsed
Initiating Ping Scan at 17:03
Scanning www.yahoo.com (69.147.87.251) [4 ports]
Completed Ping Scan at 17:03, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:03
Completed Parallel DNS resolution of 1 host. at 17:03, 0.05s elapsed
Initiating SYN Stealth Scan at 17:03
Scanning www.yahoo.com (69.147.87.251) [1000 ports]
Discovered open port 80/tcp on 69.147.87.251
Discovered open port 443/tcp on 69.147.87.251
Completed SYN Stealth Scan at 17:03, 4.92s elapsed (1000 total ports)
```

- The first information I extracted from the tools is the TCP/UDP ports' status (i.e. either open, filters, or closed)

```

Starting Nmap 7.95 ( https://nmap.org ) at 2025-01-14
17:03 EST
NSE: Loaded 157 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 17:03
Completed NSE at 17:03, 0.00s elapsed
Initiating NSE at 17:03
Completed NSE at 17:03, 0.00s elapsed
Initiating NSE at 17:03
Completed NSE at 17:03, 0.00s elapsed
Initiating Ping Scan at 17:03
Scanning www.yahoo.com [69.147.87.251] (4 ports)
Completed Ping Scan at 17:03, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 17:03
Completed Parallel DNS resolution of 1 host. at 17:03, 0.05s elapsed
Initiating SYN Stealth Scan at 17:03
Scanning www.yahoo.com [69.147.87.251] [1000 ports]
Discovered open port 80/tcp on 69.147.87.251
Discovered open port 443/tcp on 69.147.87.251
Completed SYN Stealth Scan at 17:03, 4.92s elapsed (1000 total ports)

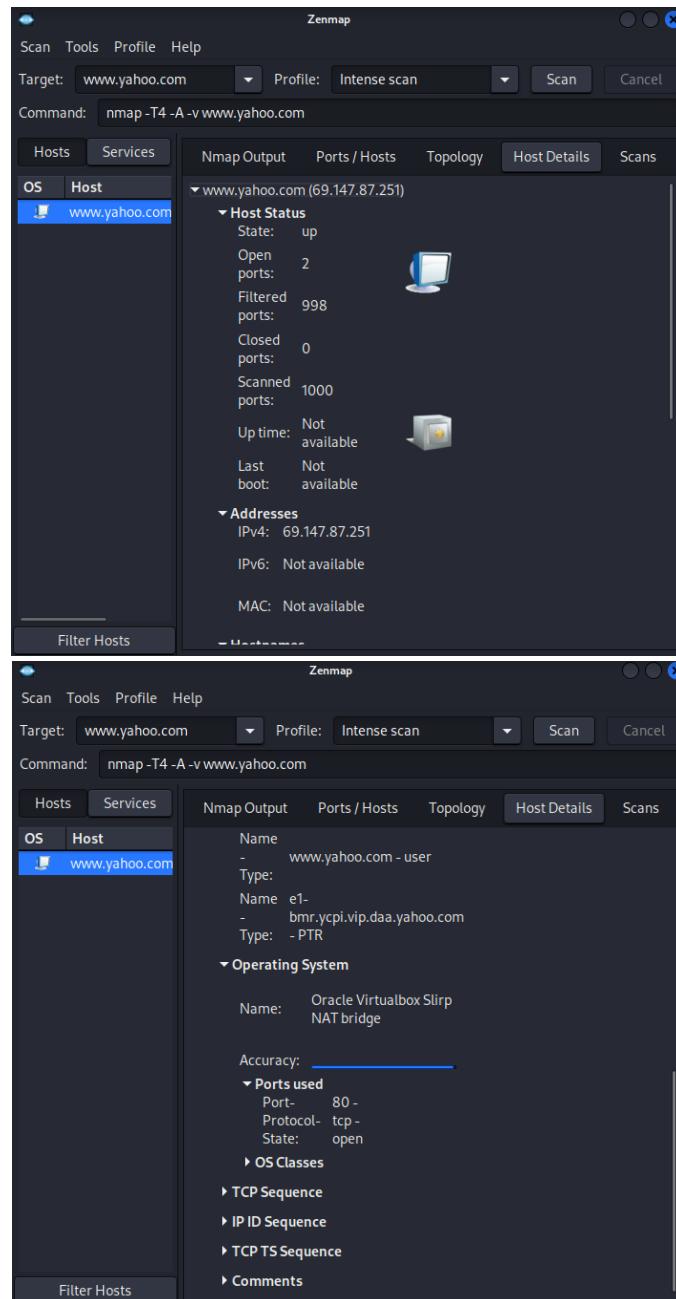
```

PORT	STATE	SERVICE	VERSION
80/tcp	open	http-proxy	Apache Traffic Server
		http-title: Did not follow redirect to https://	
		www.yahoo.com/	
		_http-server-header: ATS	
		_http-favicon: Unknown favicon MD5:	
	3A07174943F82046370997254100D870		
		http-methods:	
		Supported Methods: GET HEAD POST OPTIONS	
443/tcp	open	ssl/http-proxy	Apache Traffic Server
		http-methods:	
		Supported Methods: GET HEAD POST OPTIONS	
		_http-favicon: Unknown favicon MD5:	
	3A07174943F82046370997254100D870		
		_ssl-date: TLS randomness does not represent time	
		_http-server-header: ATS	
		_http-title: Yahoo Mail, Weather, Search, Politics, News, Finance, Sports...	

- I cared more about open ports (as typically limited number of ports should be opened, 2 in this case).

Port	Protocol	State	Service	Version
80	tcp	open	http-proxy	Apache Traffic Server
443	tcp	open	http-proxy	Apache Traffic Server

- For the least the host should have 80 open (to enable Internet) ✓
- We can get more details in the hosts or services of the tested domain



What you will do ? Make your own demo and screenshots of Zenmap tool (For simplicity, you can follow the steps describe in one the following two links, either one is fine)

<https://www.youtube.com/watch?v=dlex-fmzrnc>

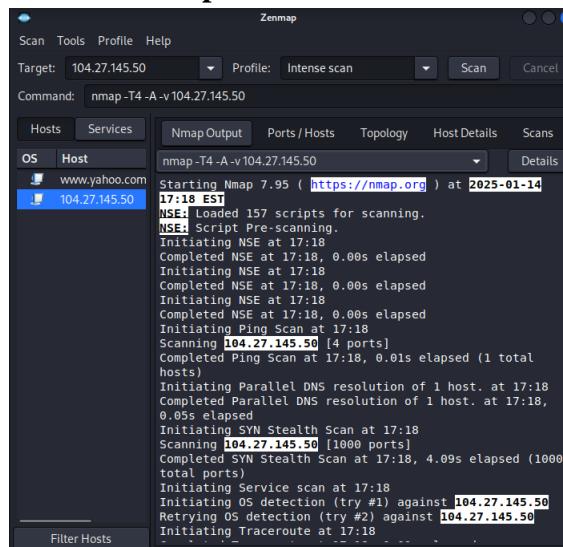
<http://www.techken.in/linux/how-to-use-nmap-in-kali-linux-step-by-step-tutorial/>

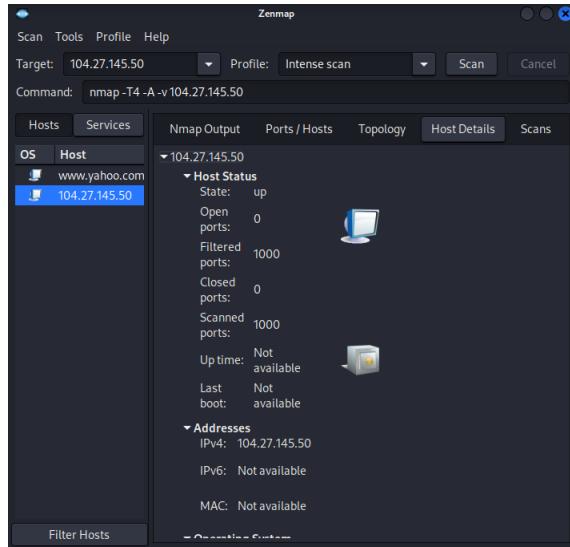
- The links were broken in my case, so I decided to use the following tutorial (<https://youtu.be/dhv2z6sV1bQ?si=2E7uMgX9-OcaWDMx&t=217>):

```
Starting Nmap 6.00 ( http://nmap.org ) at 2012-05-17 12:00+0100 [Debian 3ubuntu7]
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.00031s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
22/tcp      open  ssh
| ssh-hostkey: 1024 2f:4f:4d:4b:4e:4c:4a:4b (Ubuntu)
|_2048 79:f8:3d:4b:4e:4c:4a:4b
80/tcp      open  http
|_http-title: 
9929/tcp    open  netcat
Device type: general purpose
Running: Linux 2.6.X|3.0
OS CPE: cpe:/o:linux:kernel:2.6 cpe:/o:linux:kernel:3.0
OS details: Linux 2.6.32 - 2.6.39, Linux 2.6.38 - 3.0
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
```



- Nmap.org had 0 open ports (couldn't tell till I went to Host Details to ensure this fact, and this is based on the IP Address that I inputed from video as the Target):





- **Summary of what I learned from this lab:**

From this lab, I dove into using Zenmap on Kali Linux, and it was a fascinating experience. I started by downloading the latest version of Kali Linux from their official website and setting it up on VirtualBox. After updating the system, I explored Zenmap, the GUI version of the Nmap network scanner. Understanding that port scanning is a crucial step for both hackers and penetration testers, I performed intense scans to identify the status of TCP/UDP ports. The practical hands-on approach helped me grasp how to use Zenmap effectively, checking for open ports and ensuring essential ones, like port 80, were accessible. Despite some initial hiccups with broken links, I found a helpful YouTube tutorial that guided me through the process. Overall, using Zenmap was a rewarding experience that enhanced my network scanning skills.