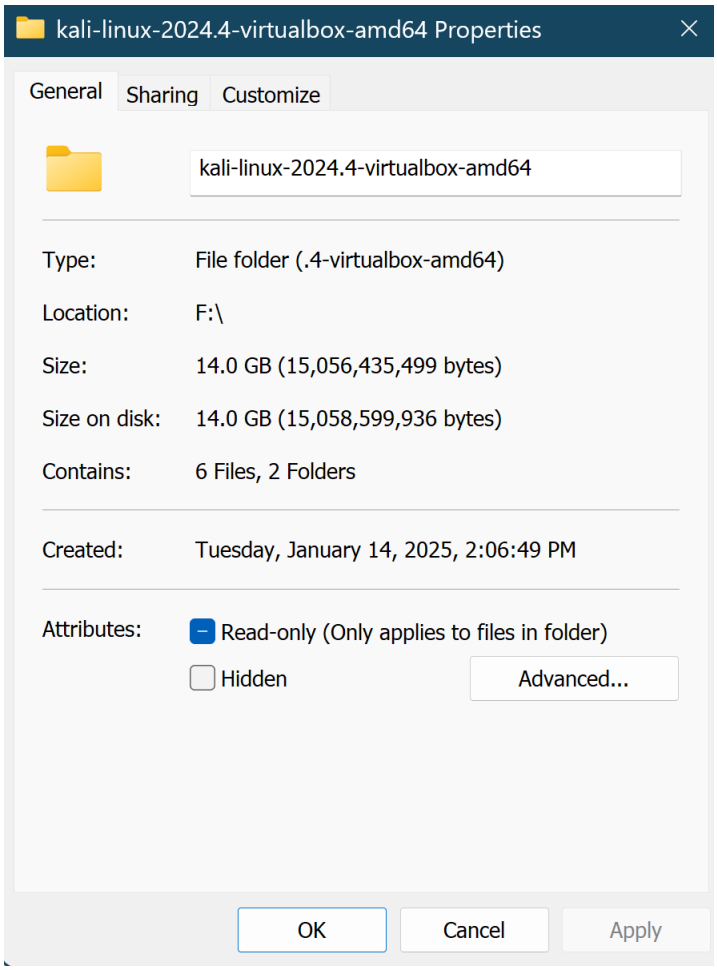
# Lab1: Zenmap

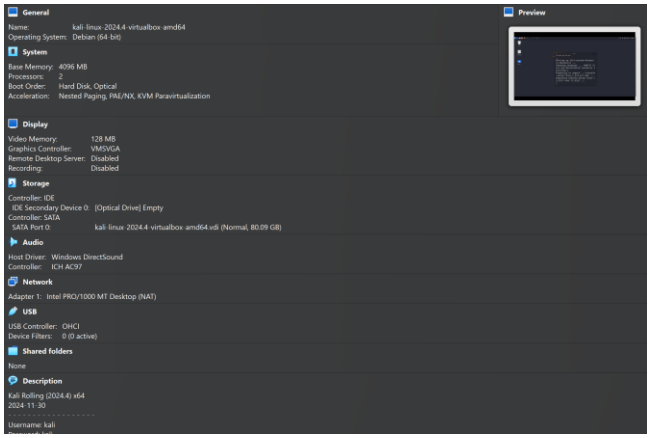
Joshua Ludolf
CSCI 4321
Computer Security
January 14, 2025

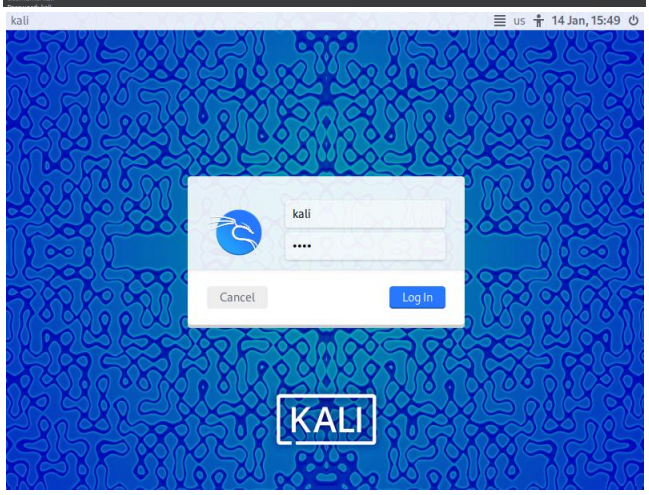
- The latest version of Kali Linux can be downloaded from their official website **https://www.kali.org**. From this website, I downloaded: VirtualBox (VDI) 64bit Download Size: 3.2GB (14.0GB when I extracted it from zipped folder). This image(based on the website) has the username: kali and the password 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... | 7 KB |
| kali-linux-2024.4-virtualbox-amd64.vb... | 1/14/2025 2:54 PM | VBOX-PREV File | 7 KB |
| kali-linux-2024.4-virtualbox-amd64.vdi | 1/14/2025 3:04 PM | Virtual Disk Image | 20,183,361... |
| kali-linux-2024.4-virtualbox-amd64-1.... | 11/30/2024 8:31 AM | VirtualBox Machin... | 3 KB |

- 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.

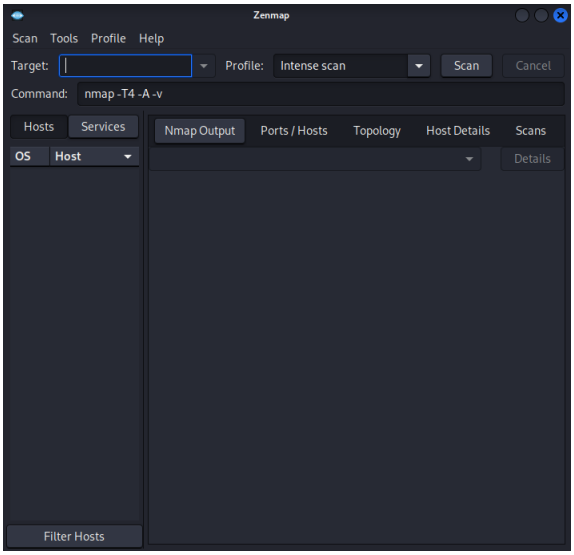


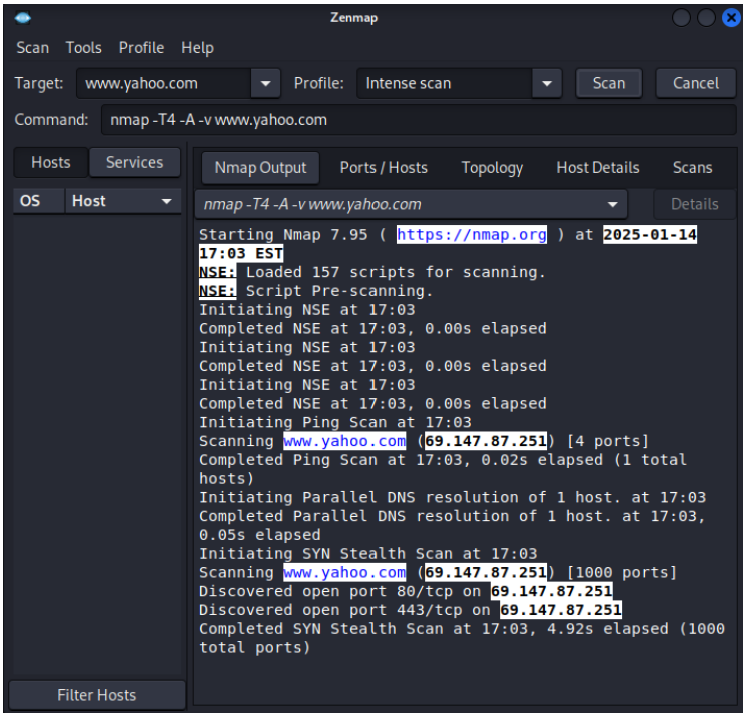

- I ran the following command to get lastest installation of Kali Linux: sudo apt-get update && sudo apt-get upgrade -y.



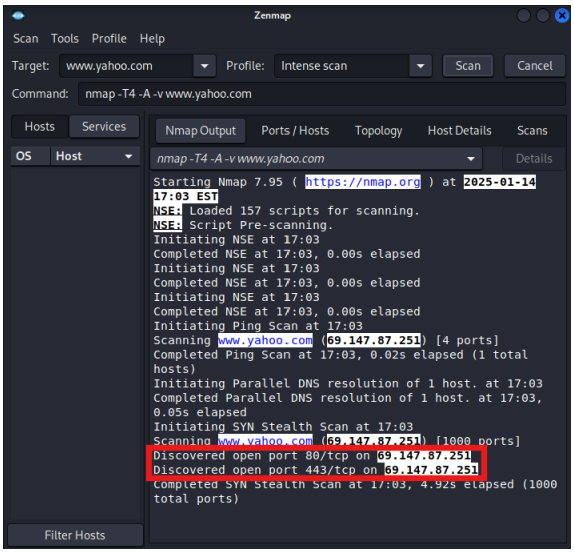
- **Zenmap is a GUI version of NMAP network scanner (which is largely used as port scanner/mapper)**

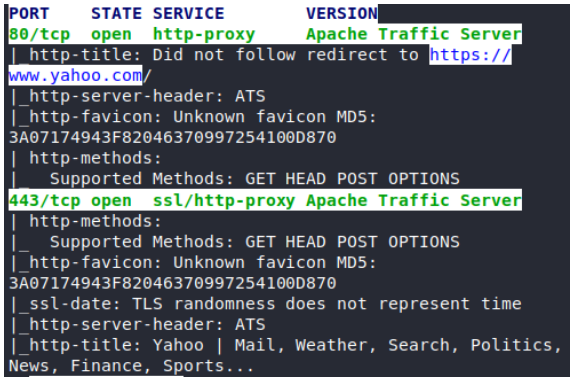



- **The tool uses nmap console commands, for example, I selected a host and start intense scan, the console command will be nmap –T4 –A –v [www.yahoo.com](http://www.yahoo.com)**

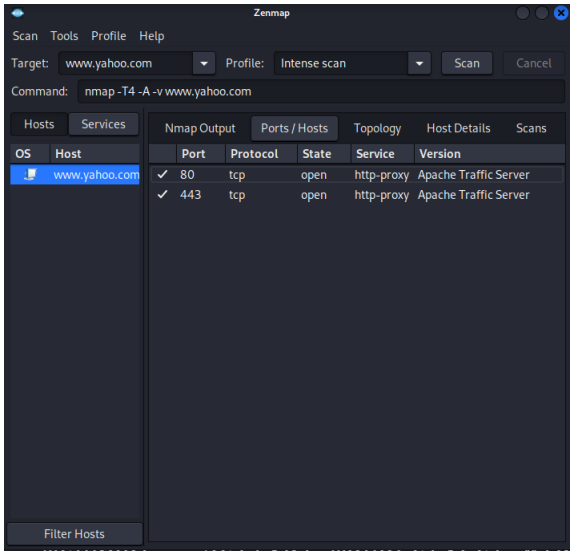



- **The first information I extracted from the tools is the TCP/UDP ports' status (i.e. either open, filters, or closed)**

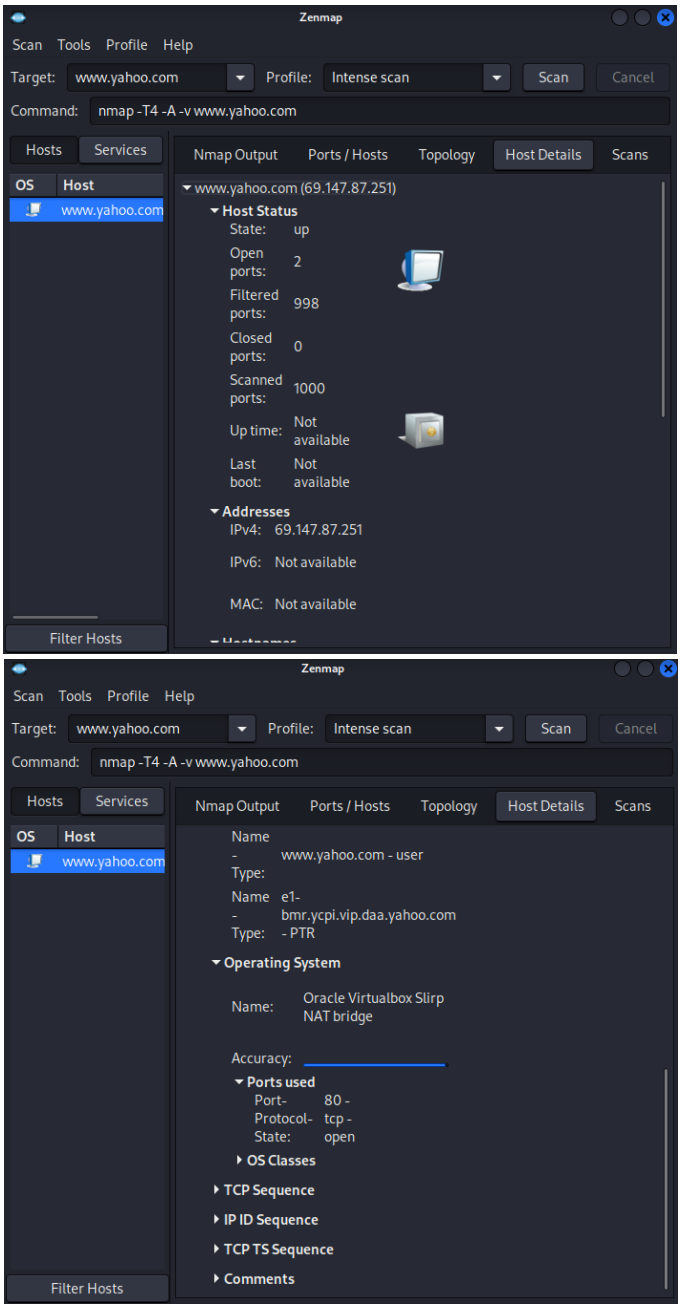



- **I cared more about open ports (as typically limited number of ports should be opened, 2 in this case).**



- **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**



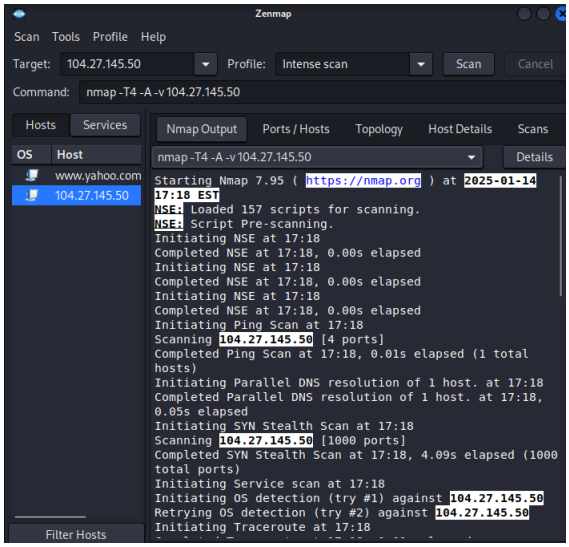

**What you will do ? Make your own demo and screenshots of Zenmap tool (For simplicity, you can follow the steps describe in one the following two links, either one is fine)**

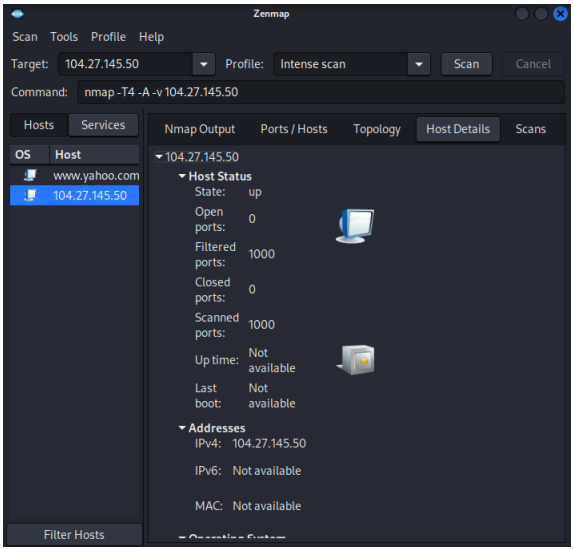
**https://www.youtube.com/watch?v=dlcx-fmzrnc**

**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 ):**


- **Nmap.org had <u>0</u> 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.**