# Mini project -2

# Network scanning

Submitted by - Aditi Devi Prasad

Batch - August 2024

Date – 02/12/2024

Network scanning is a process of scanning the targeted network to find the active devices and IP address associated with these active devices, port numbers, and services on those port numbers so that we can define the loopholes across the particular network. This process is malicious.

**Methodology:**

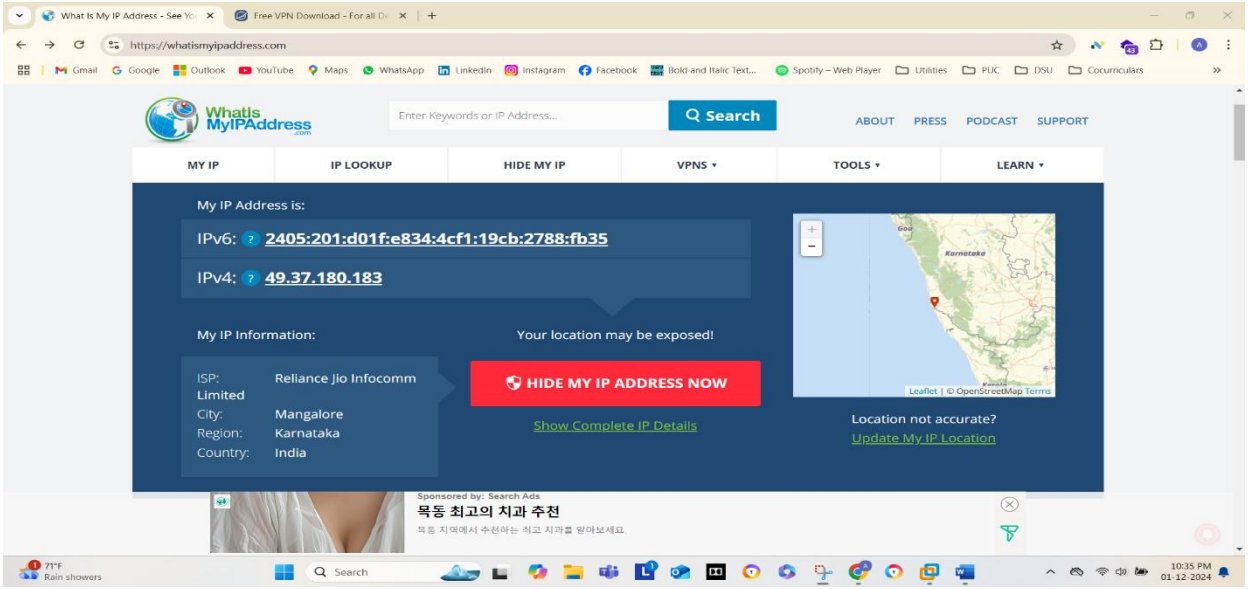
- Aiming the target.
- Scan their IP range of addresses.
- Scan their Open ports.
- Check the services running on open ports.
- Find the service versions of open ports.
- Check the operating system of the target.
- Bypass the security devices.
- Choose the right type of scan.

**Types of network scan:**

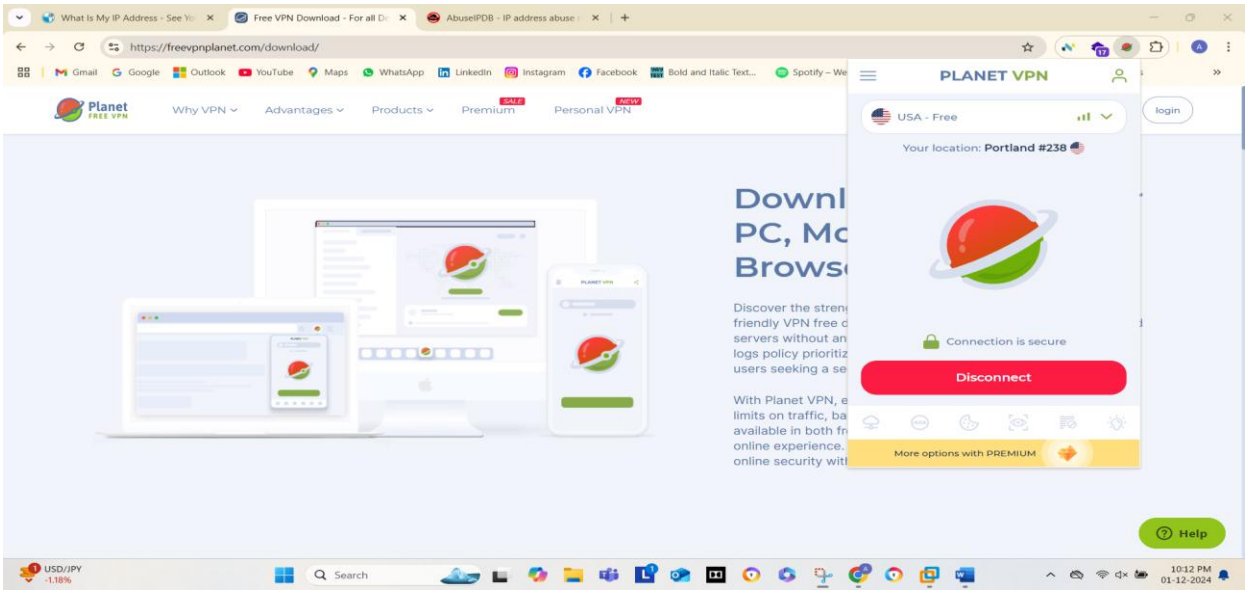
- TCP scan – by '-sT'
- UDP scan – by '-sU'
- Syn scan (stealth scan) – by '-sS'
- XMas and IDLE scan – by '-SX' and '-SI'

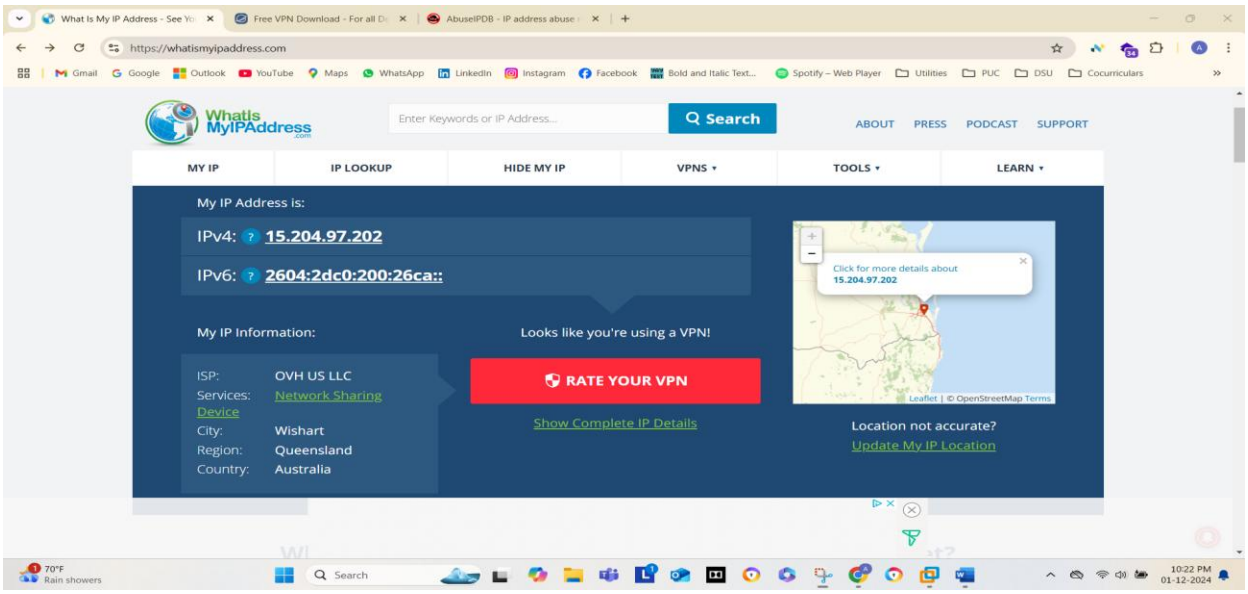
Firstly, we have to become anonymous before performing all these. This can be achieved by two methods for wireless networks.

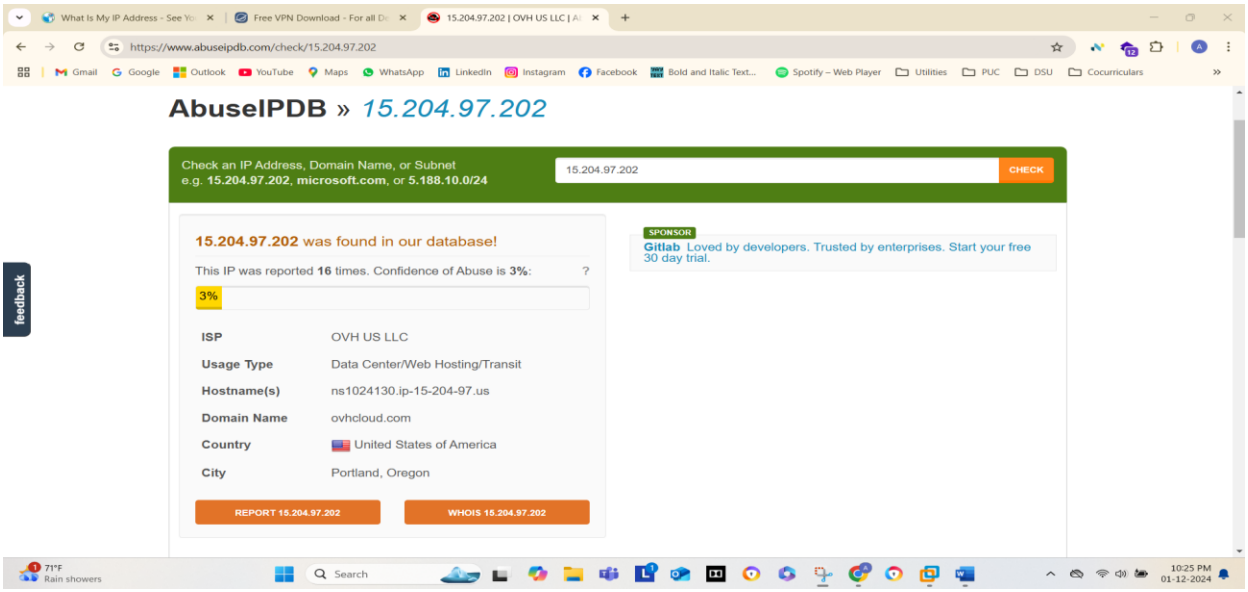
1. By VPN – not the best way as there is a chance of DNS data leakage.
   My IP address:



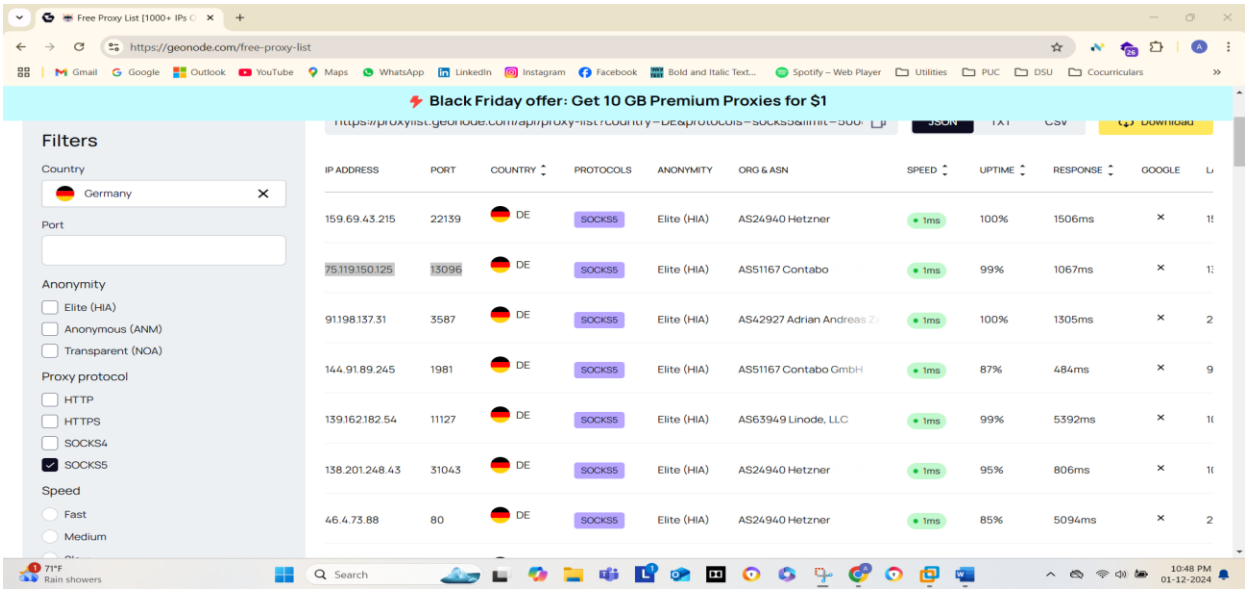
My IP after using VPN:

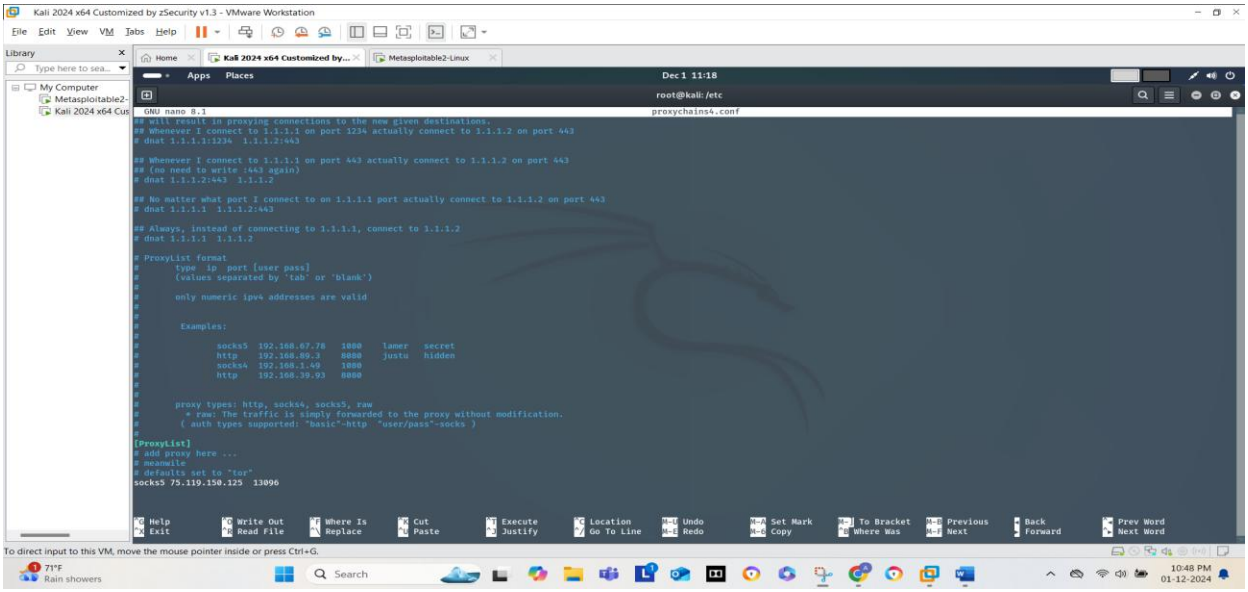


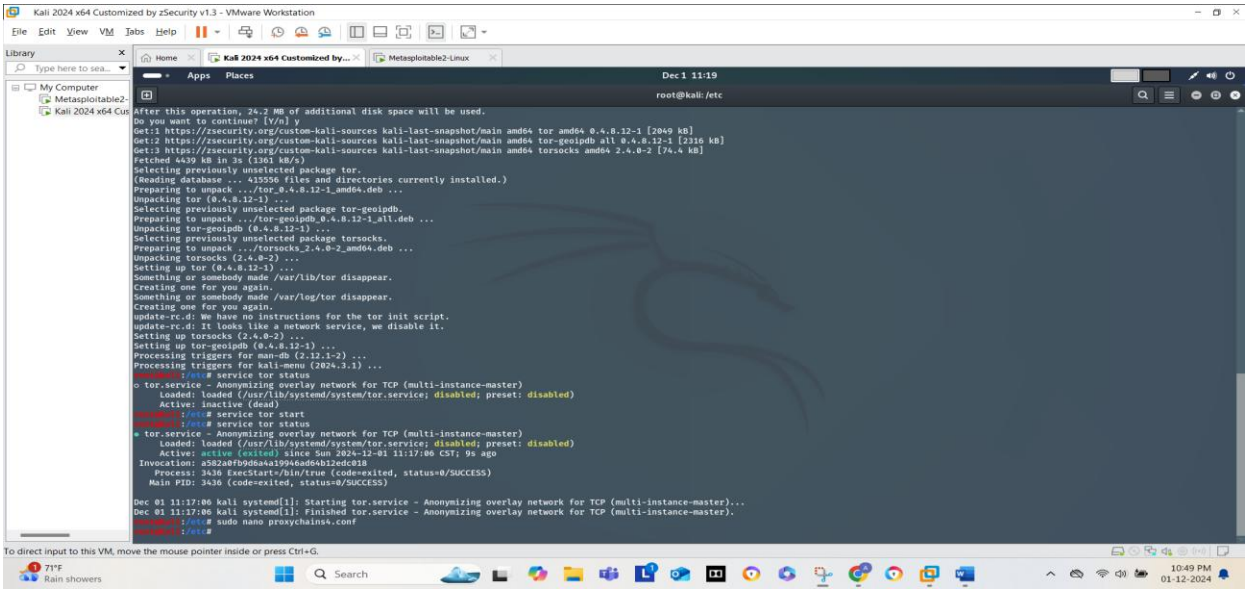



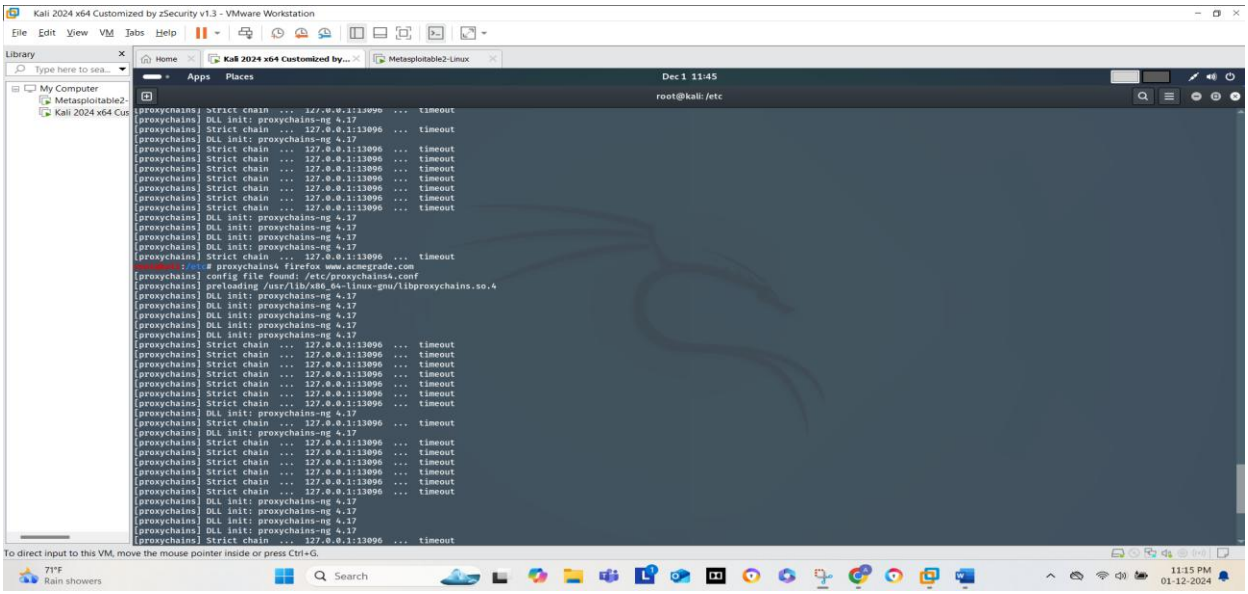



2. By Proxychains: This is the safest method as it uses proxy DNS servers itself.We are using only one proxy here and activate the TOR.



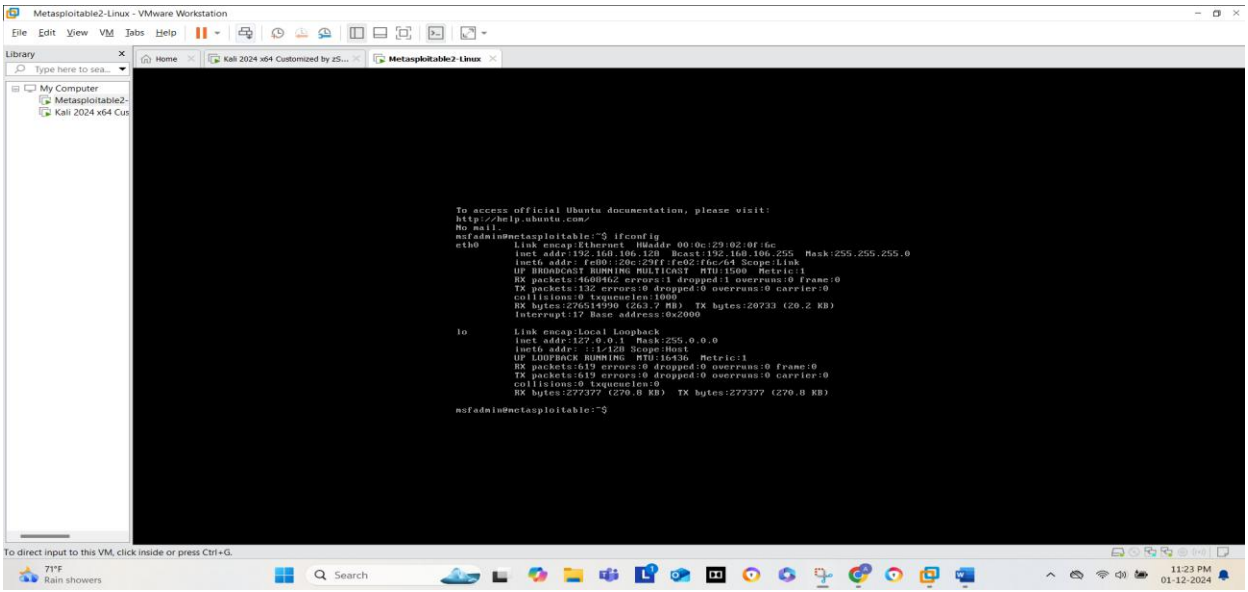



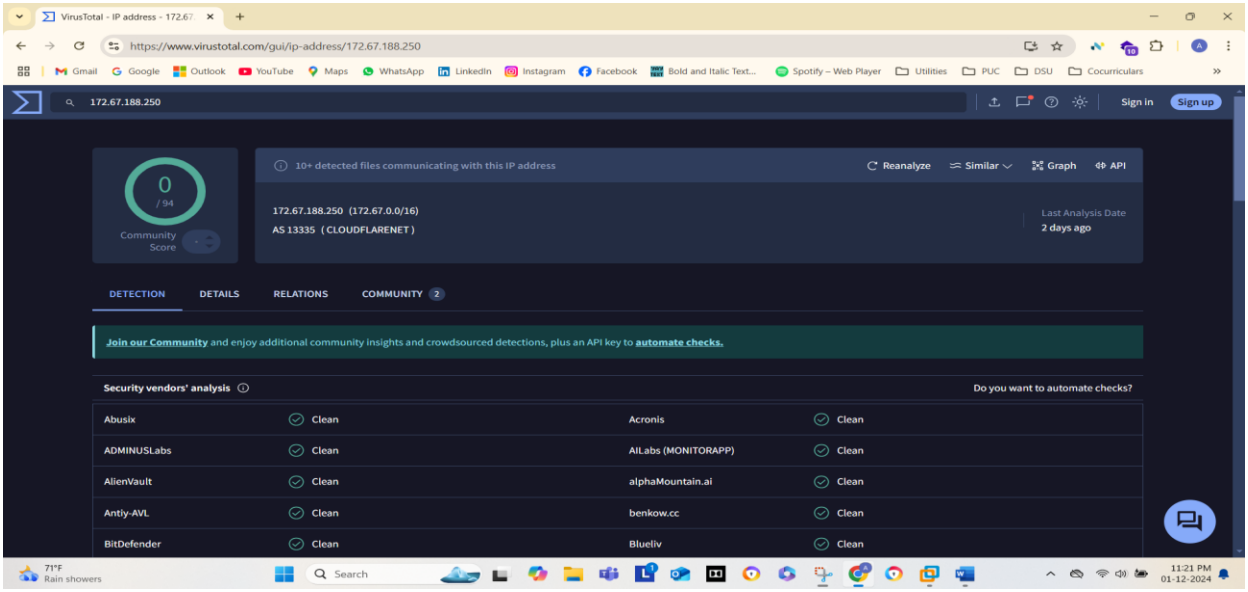


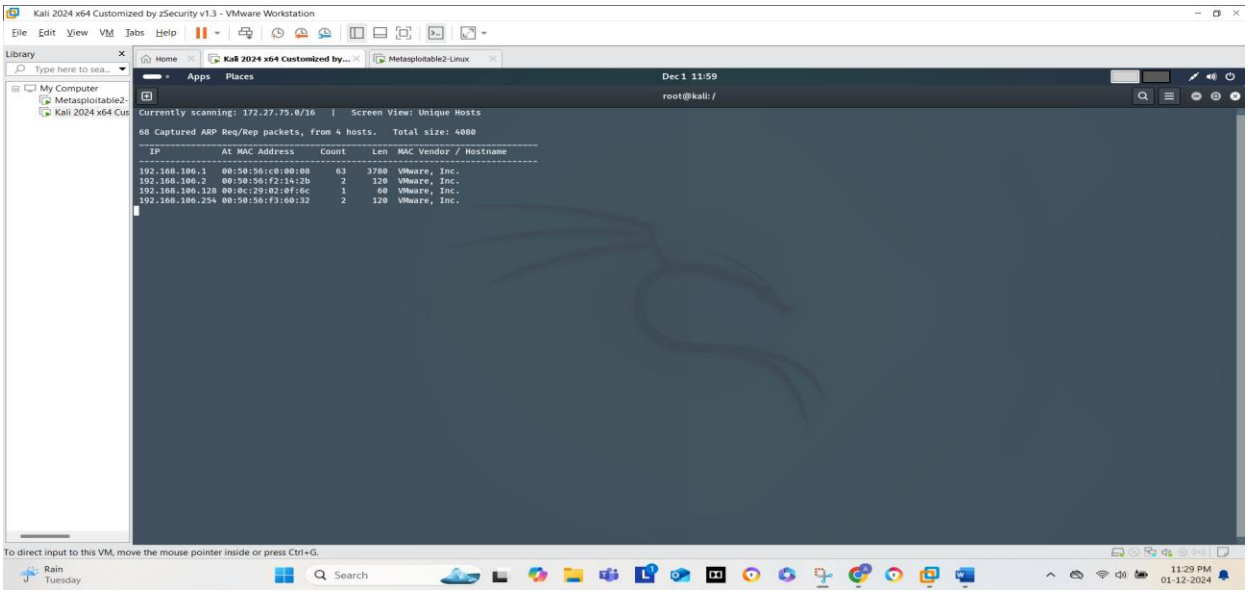

Hence, we became anonymous.

So now, we can start our network scanning procedure one by one.

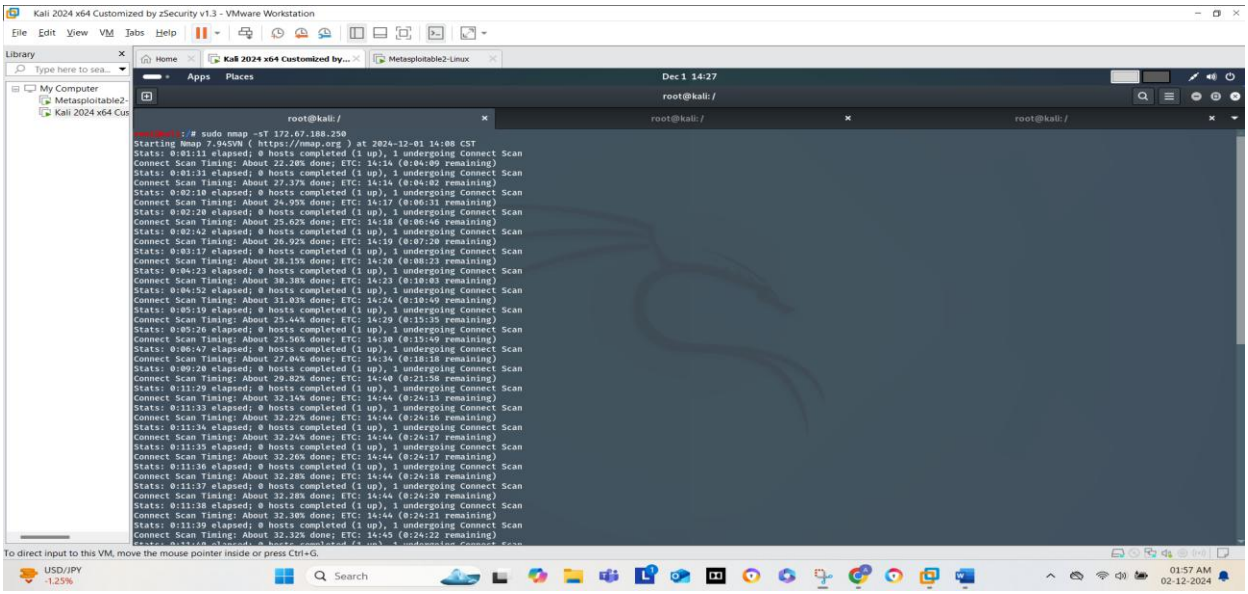
1. We will find the IP range.



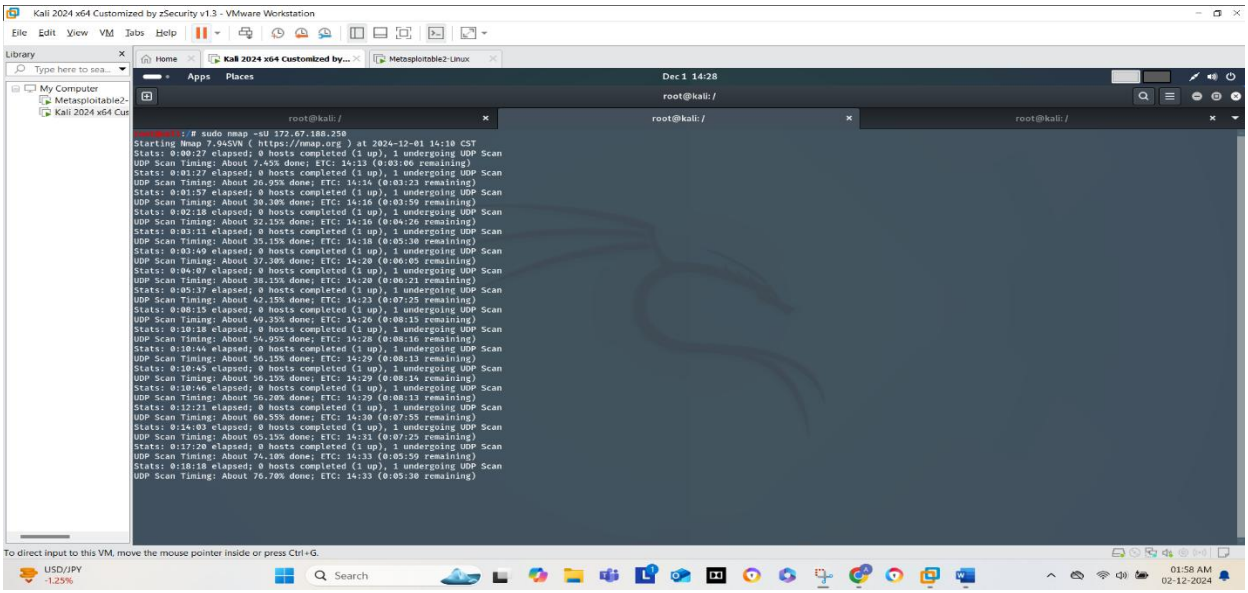


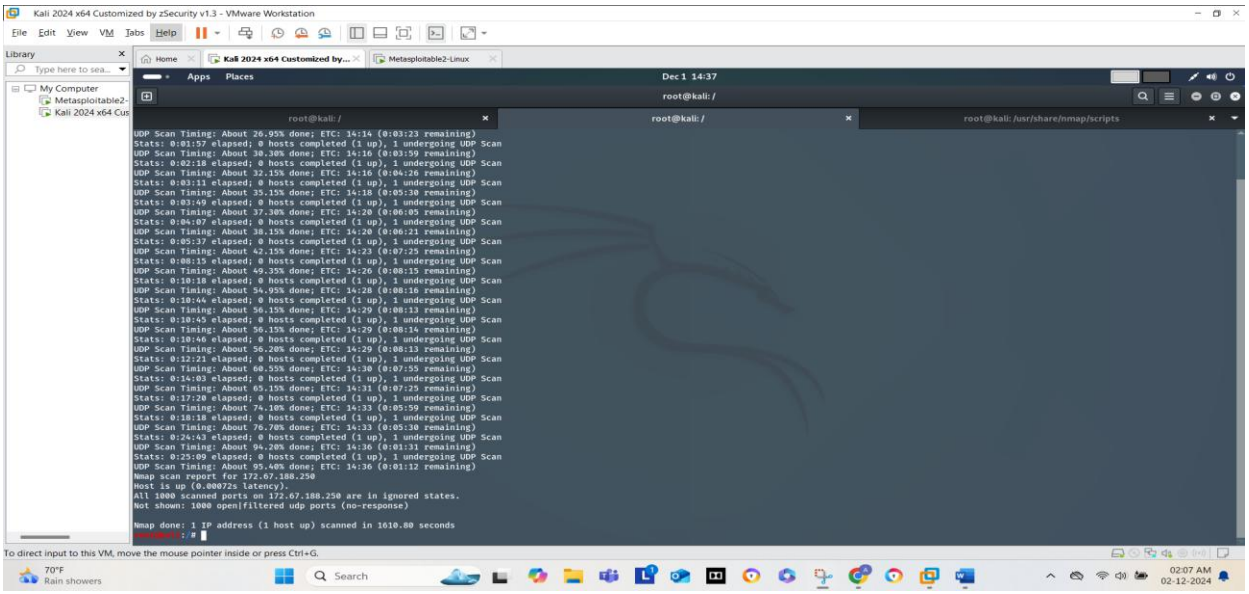




2. We perform TCP scanning:
    - It is useful in finding the security devices and it is the best to use when there are no security devices.
    - It is connection-establishment protocol.
    - The Nmap for it is '-sT'.

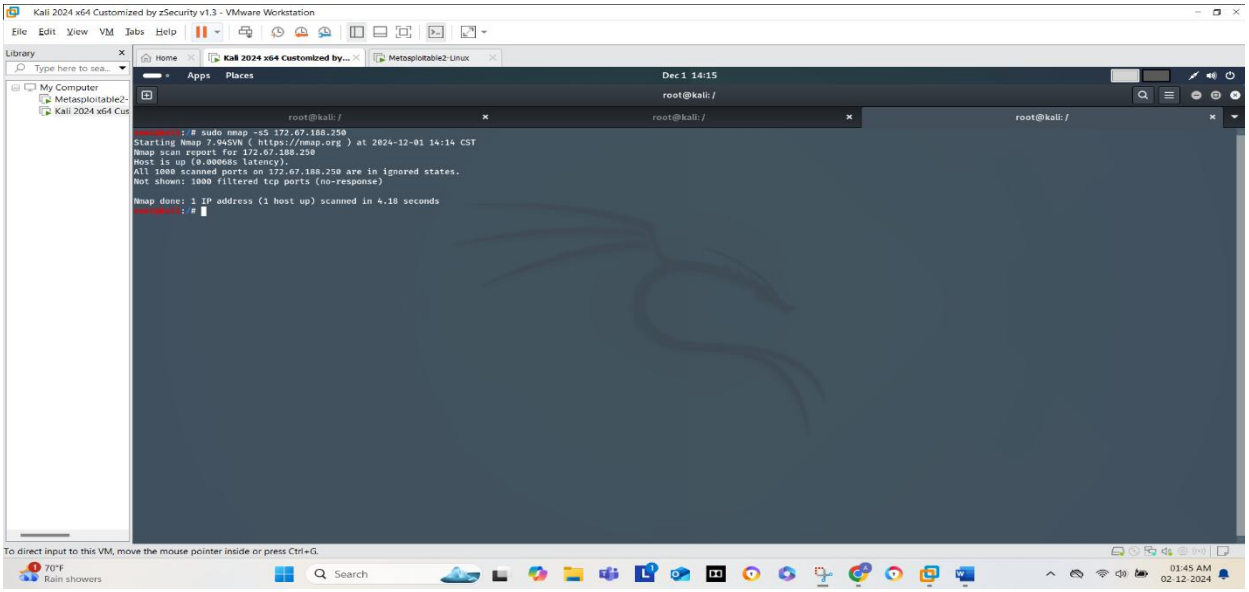



3. We perform UDP scanning:
    - It is not reliable.
    - Only 5% of the internet, works on UDP.
    - It is connectionless protocol.
    - The Nmap for it is '-sU'.

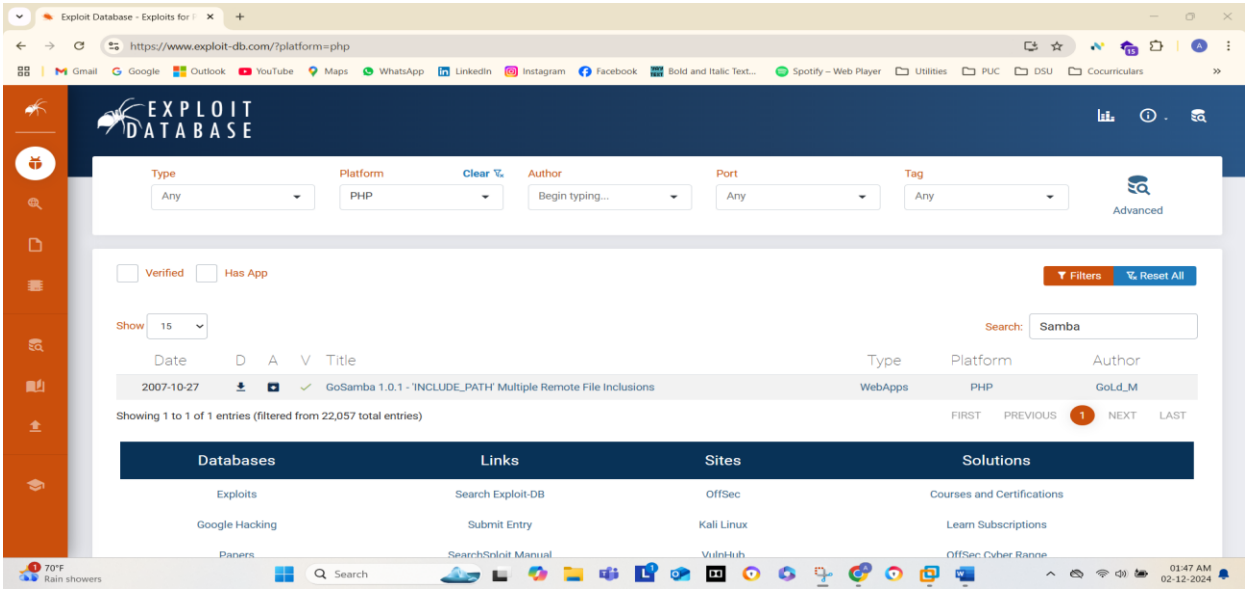


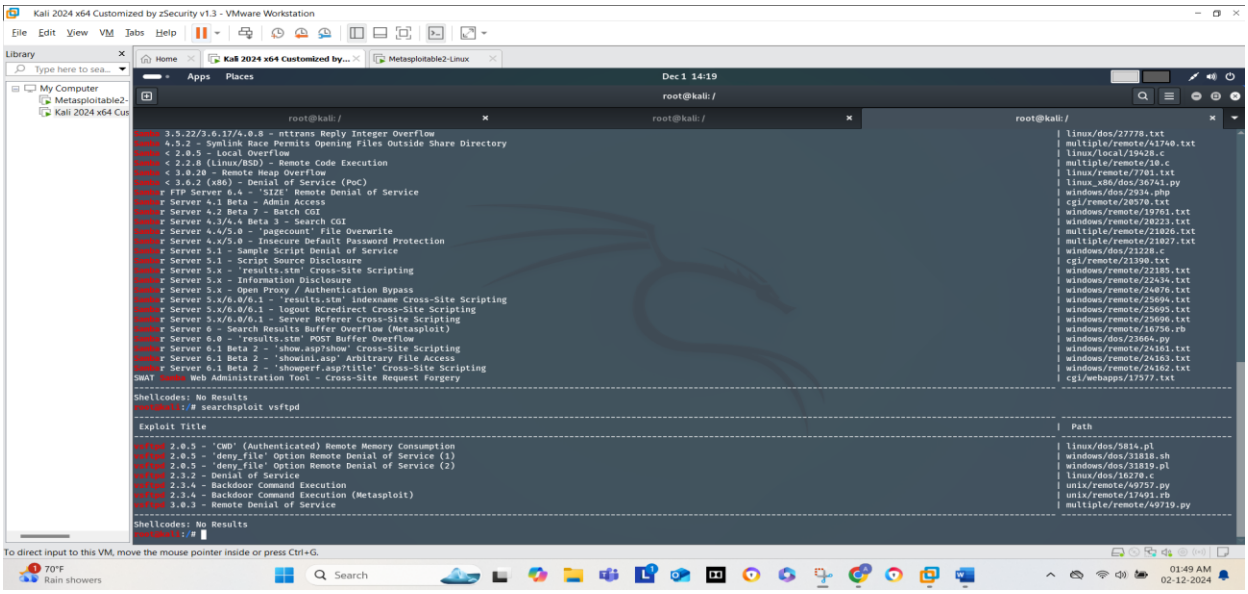



4. We perform synchronous/stealth scanning:
    - This is also a type of TCP scan.
    - These type of scans uses the bypass security devices.
    - It doesn't establish the communication.

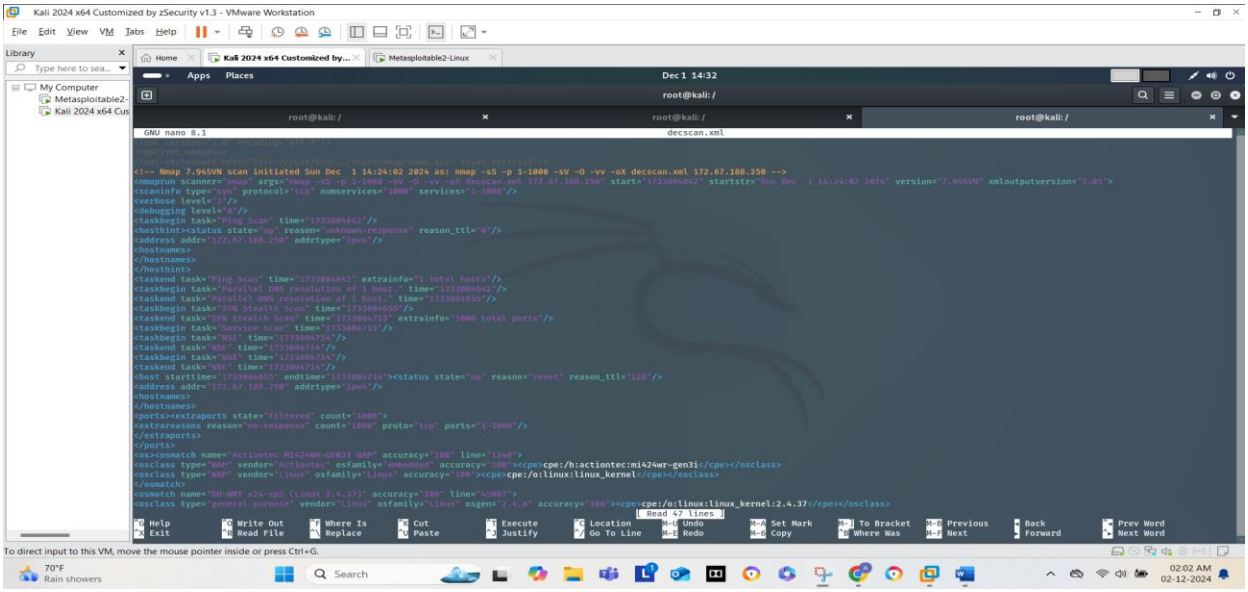



5. We find the vulnerability:

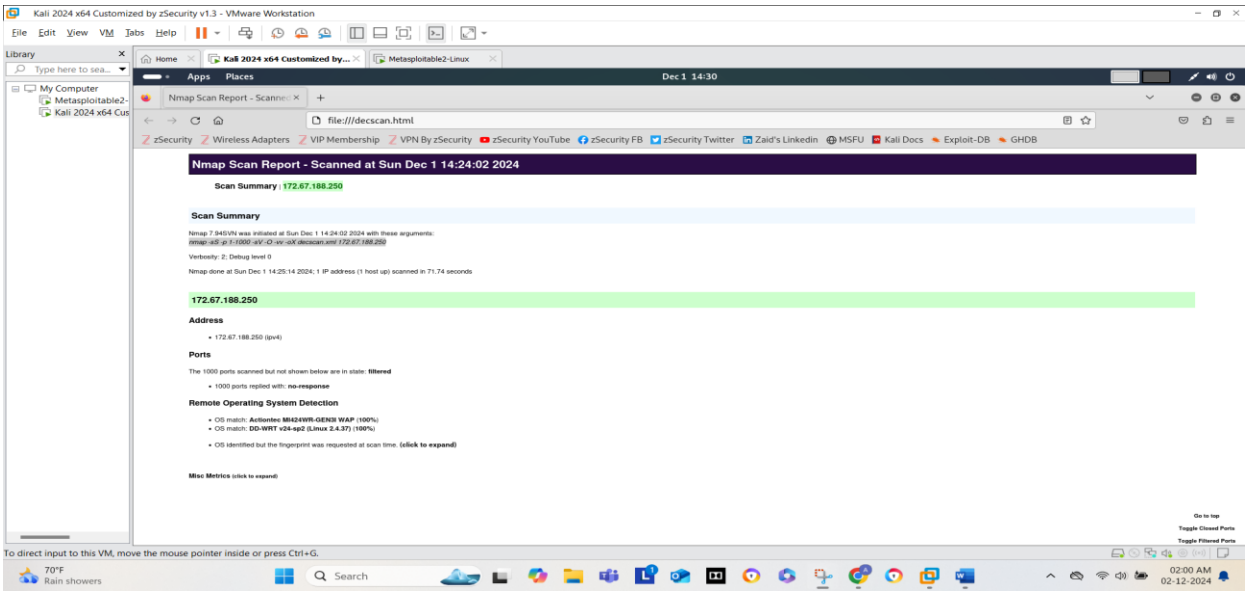


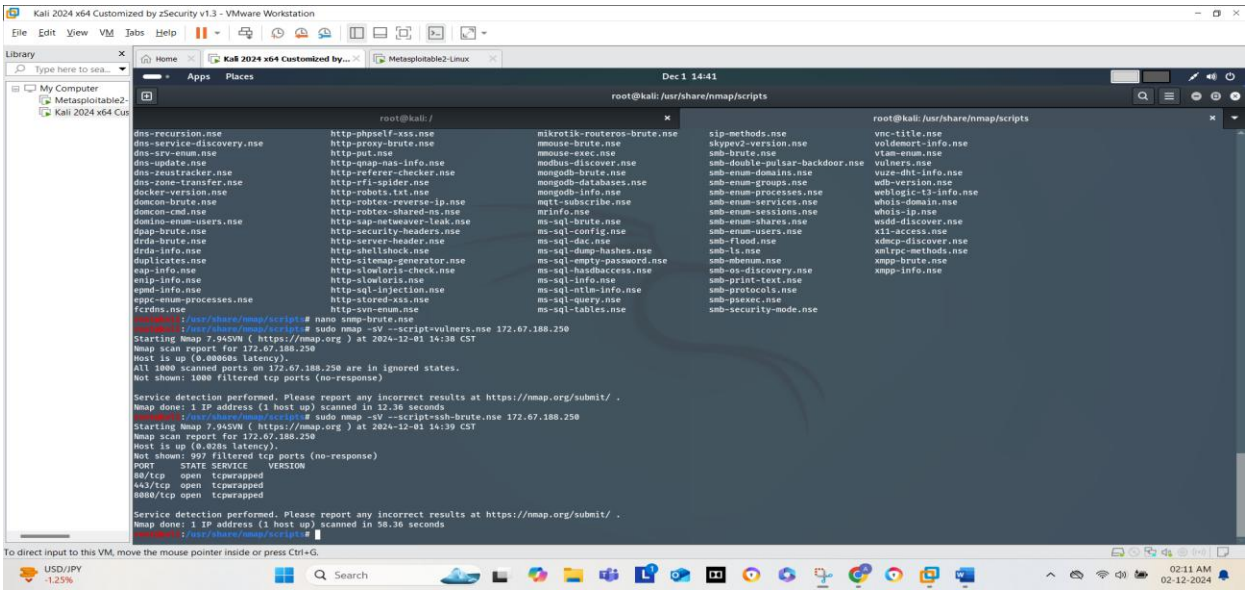

6. We create xml file




7. We convert xml file to html file




NOTE: we can also find the vulnerability by script scanning. It is very advanced technique.




**Summary:**

In conclusion, network scanning is a crucial technique in cybersecurity for identifying vulnerabilities, misconfigurations, and potential threats within a network. By using tools such as port scanners, vulnerability scanners, and network mappers, organizations can gain a clear understanding of their network infrastructure. This proactive approach helps in detecting open ports, services, and devices that could be exploited by malicious actors. Regular network scanning allows security teams to address vulnerabilities before they can be exploited, ensuring the integrity, confidentiality, and availability of critical systems and data. However, it is essential that network scanning is performed ethically, following legal and organizational guidelines, to avoid unintended disruptions or violations of privacy. When combined with other security measures like firewalls, intrusion detection systems, and patch management, network scanning forms a foundational element of an organization's defense against cyber threats.