*The following is going to outline performing host discovery, port scanning, service version detection, and vulnerability scanning and detection using Nmap.*

**Host Discovery**

# nmap –sn 10.38.1.1/24

# arp-scan –localnet

# fping

Using Wireshark to perform passive reconnaissance on the active network.

**Port Scanning and host finger printing**

# nmap –sS –sV –reason 10.38.1.114

# nmap –sS –sV –p- --reason 10.38.1.114

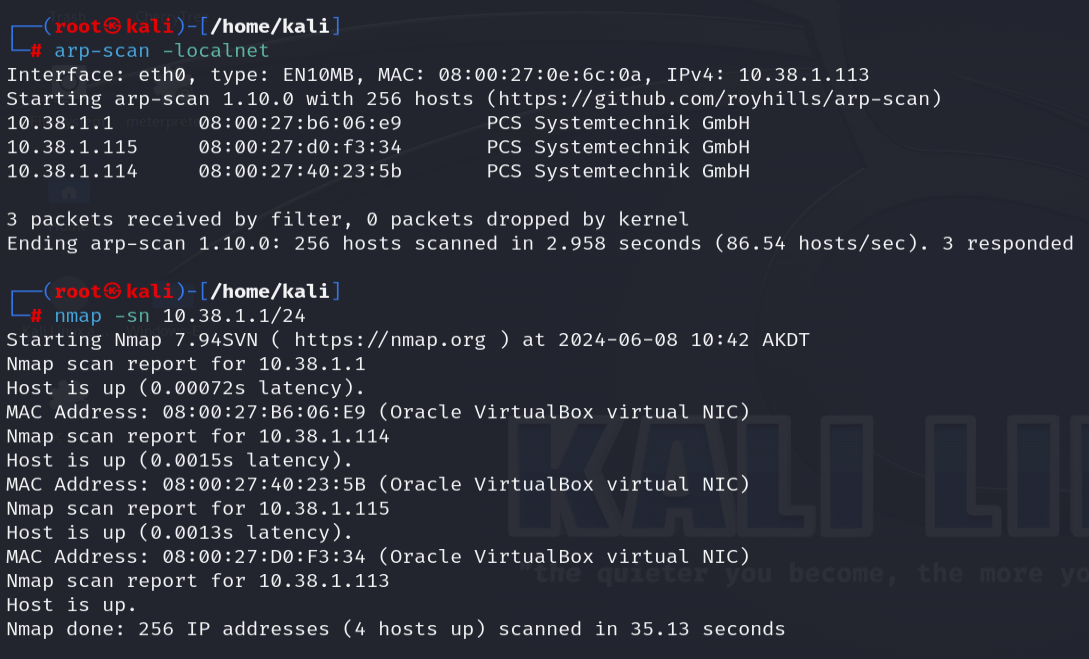
# nmap –sS –sV –sU –reason 10.38.1.114

# nmap –sS –sV –p1-10000 –reason 10.38.1.114

From there do fingerprinting on individual ports:

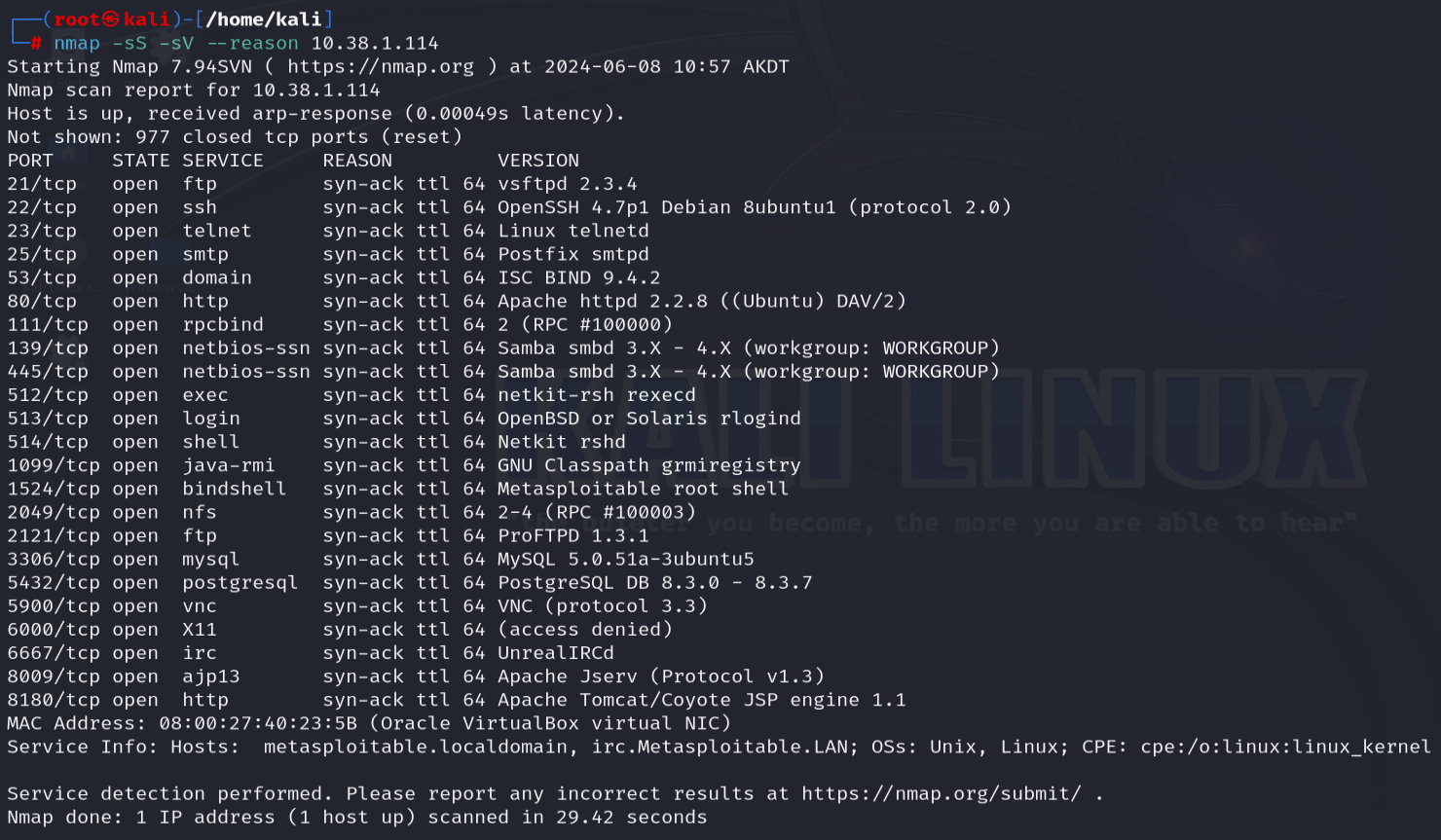
Fingerprint with the use nmap scripts and see what information I’m able to locate.

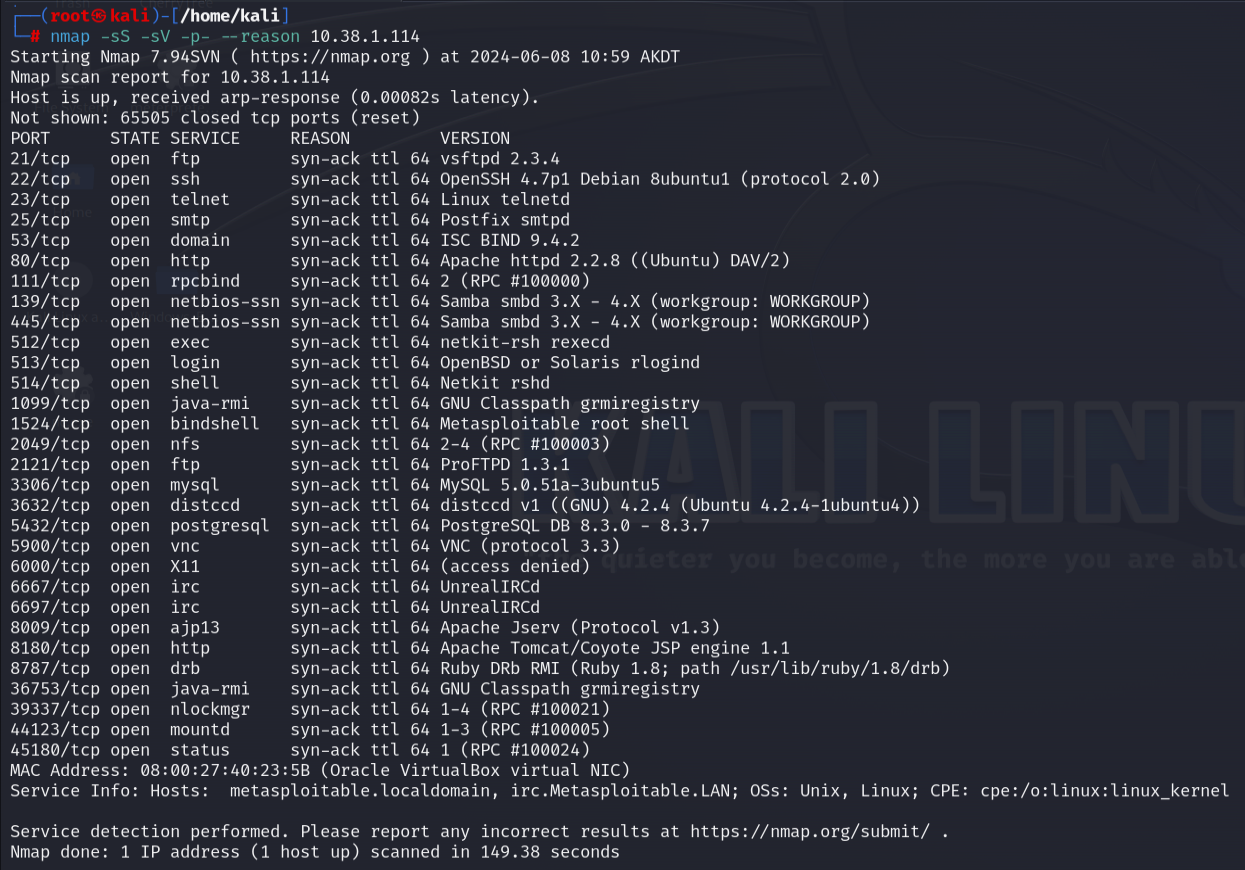
**Host Discovery**

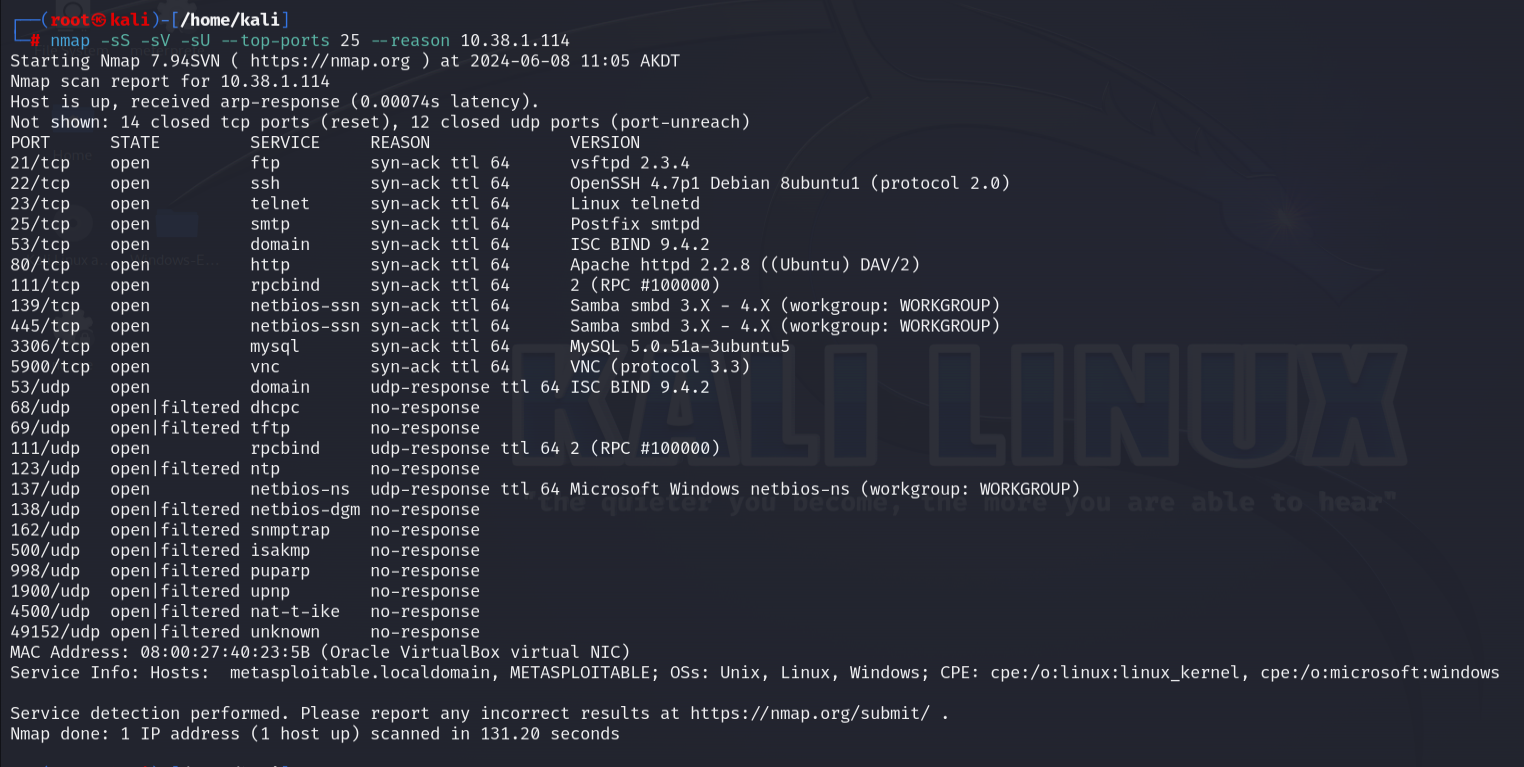
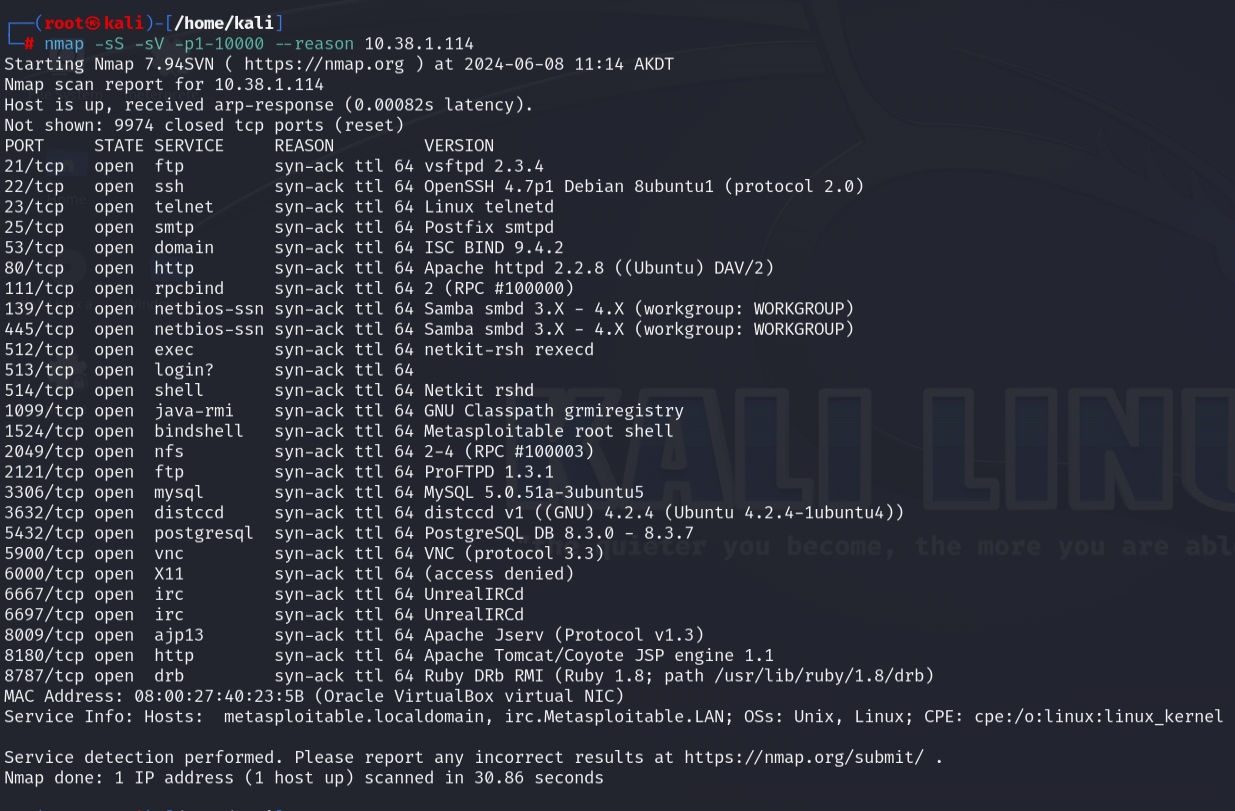




**Port Scanning and Service Detection**







**Web Server Enumeration on Port 80**



