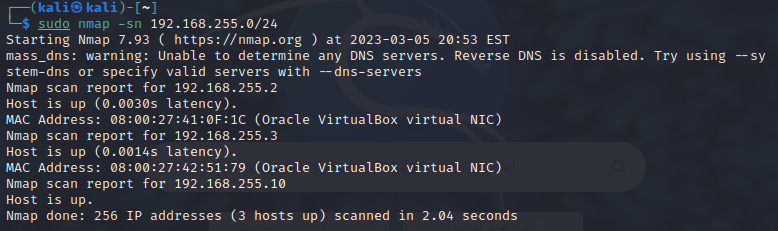
**Lab 4**

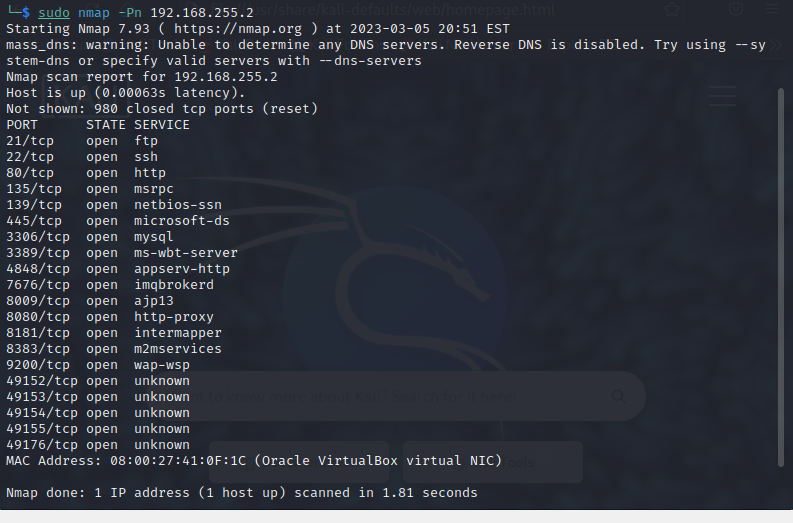
1. The -sn switch is a ping scan that is used to disable and/or suppress any port scans.
2. Run the command “sudo -sn 192.168.255.0/24”.



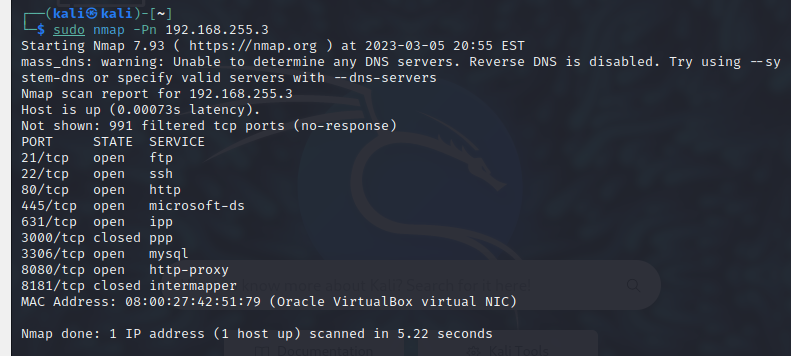
1. Explain what the –Pn switch does.

The -Pn switch treats all hosts as online and skips host discovery.

1. Run the command “sudo nmap –Pn 192.168.255.2”.



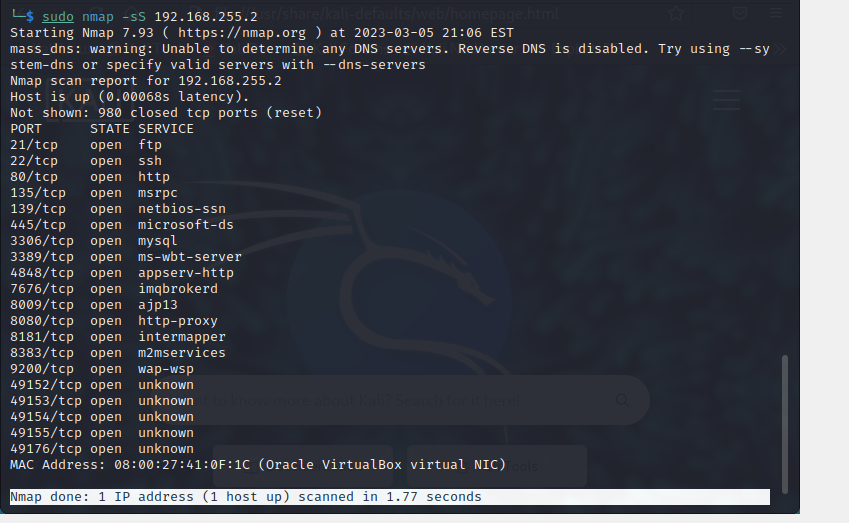
1. Run the command “sudo nmap -Pn 192.168.255.3”.



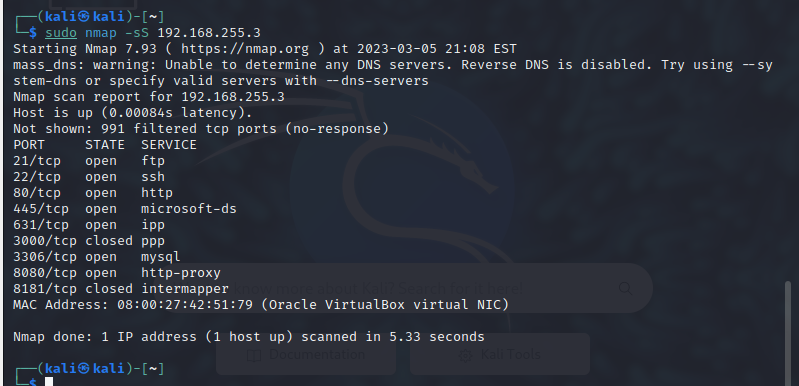
1. Explain what the -sS switch does.

The -sS switch is a TCP SYN scan, which determines if the host is online or accepts permissions.

1. Run the command “sudo nmap -sS 192.168.255.2”.



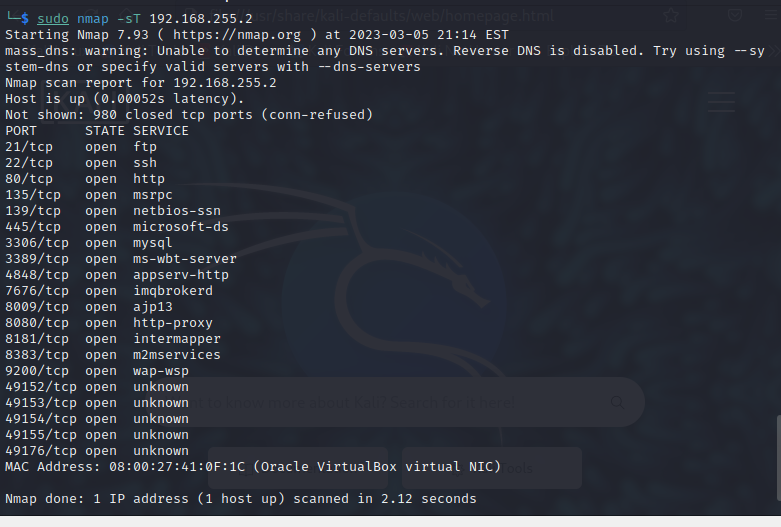
1. Run the command “sudo nmap -sS 192.168.255.3”.



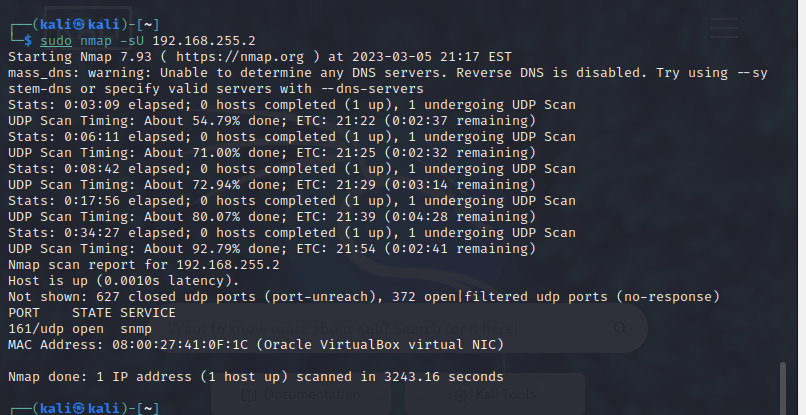
1. Explain what the -sT and -sU switch does.

The -sT switch does the TCP Connect() scan and the -sU switch does the UDP scan.

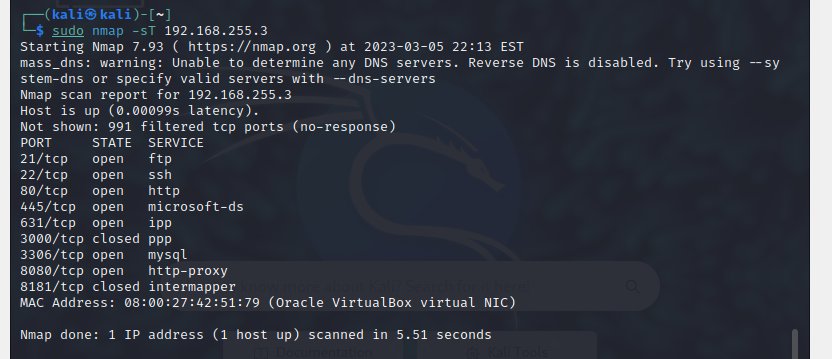
1. Run the command “sudo nmap –sT 192.168.255.2”.



1. Run the command “sudo nmap –sU 192.168.255.2”.



1. Run the command “sudo nmap –sT 192.168.255.3”.



1. Run the command “sudo nmap –sU 192.168.255.3”.

Text

Description automatically generated

1. Explain what the -O switch does.

The -O switch enables OS detection.

1. Run the command “sudo nmap –O 192.168.255.2”.

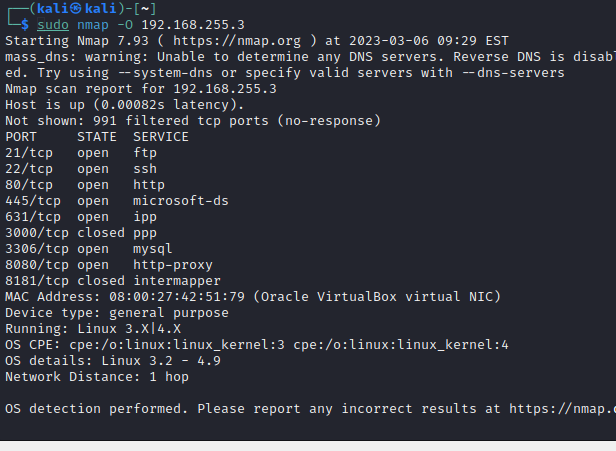
Text

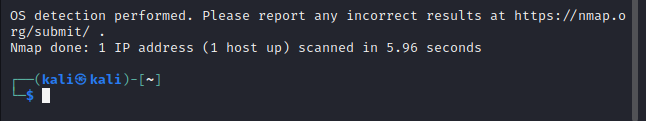
Description automatically generated

Text

Description automatically generated

1. Run the command “sudo nmap –O 192.168.255.3”

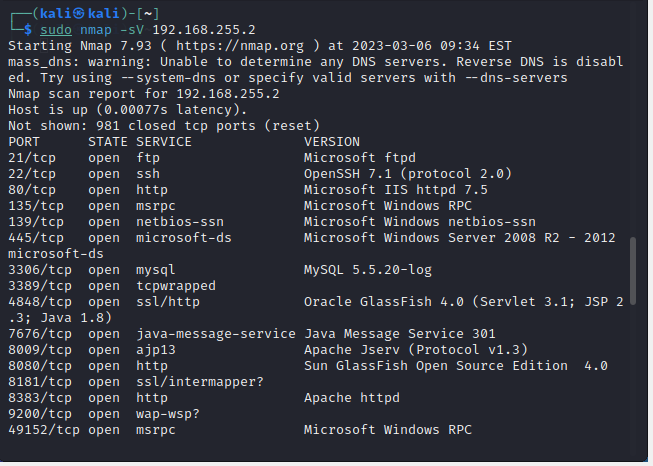


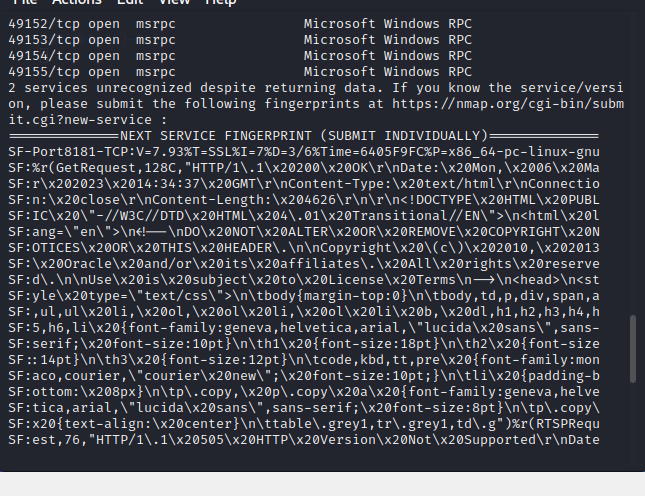


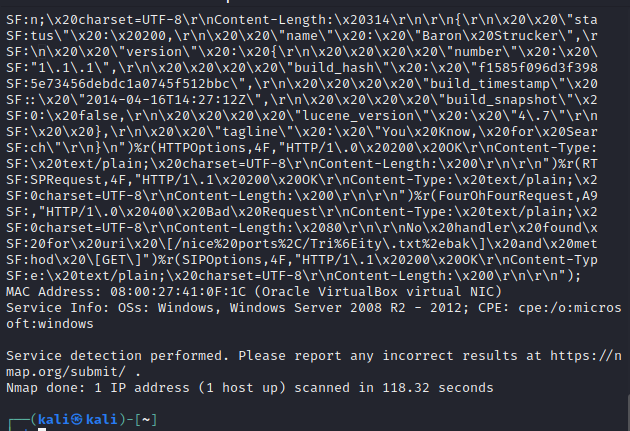
1. Explain what the -sV switch does.

The -sV switch probes open ports to determine service/version information.

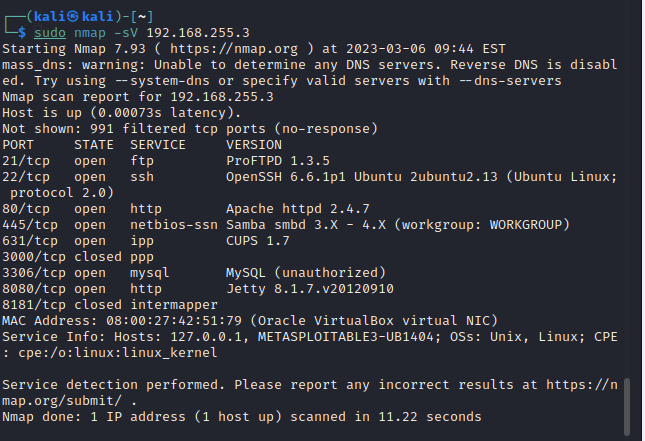
1. Run the command “sudo nmap -sV 192.168.255.2”.







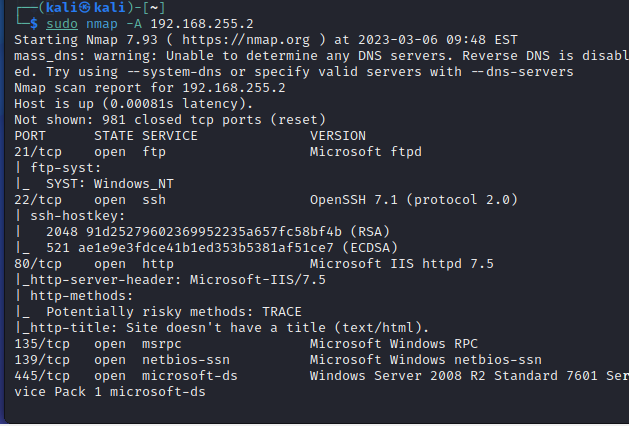
1. Run the command “sudo nmap -sV 192.168.255.3”

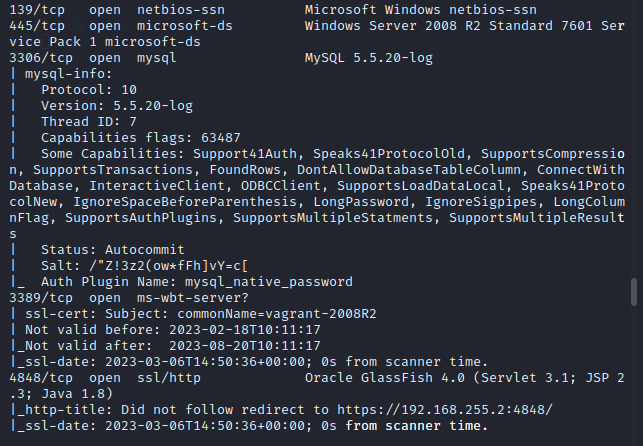


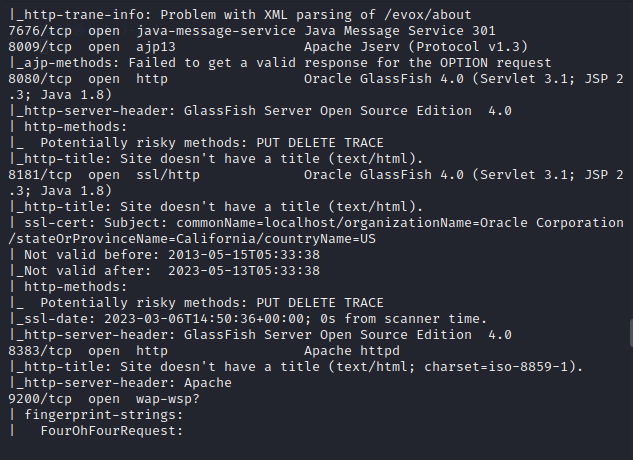
1. Explain what the -A switch does

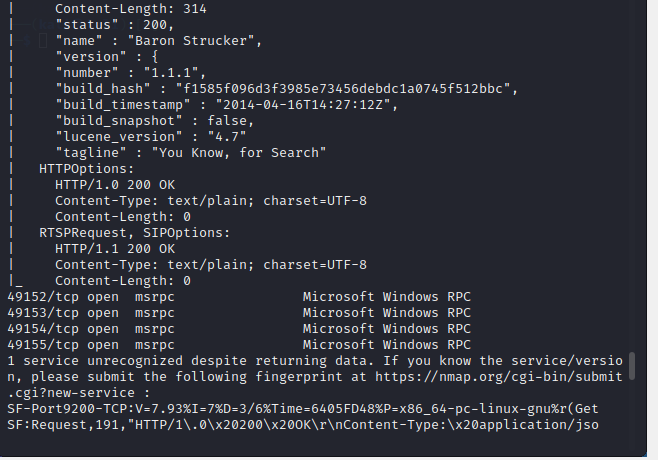
The -A switch enables OS detection, version detection, script scanning, and traceroute.

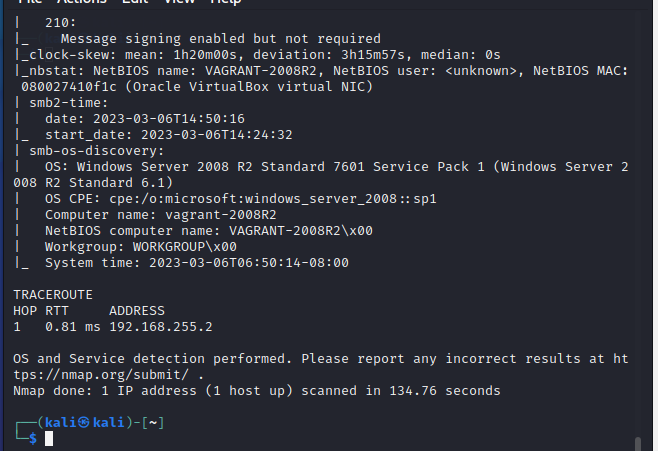
1. Run the command “sudo nmap -A 192.168.255.2”



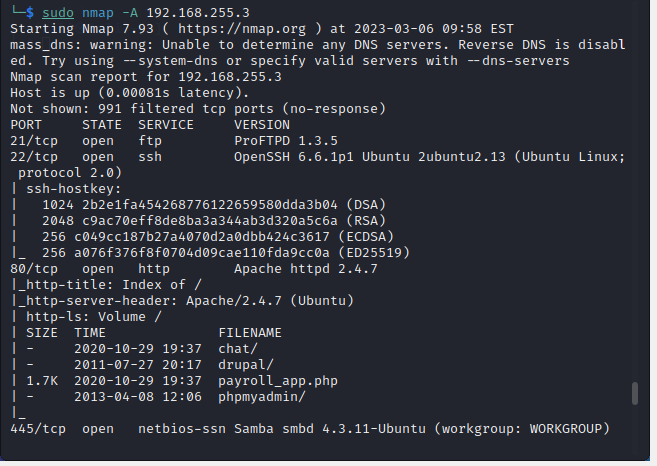


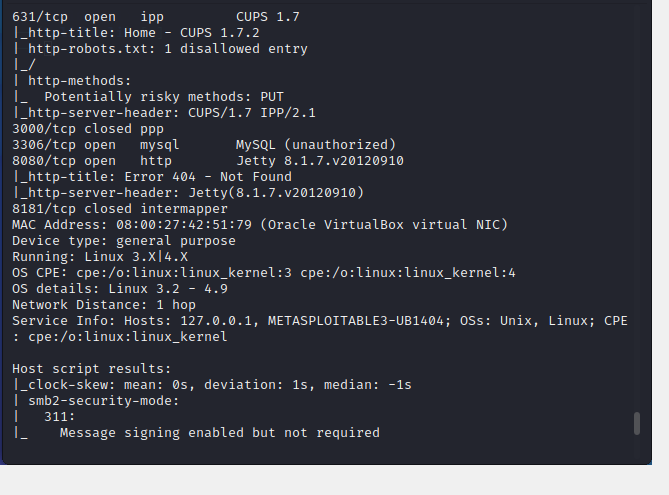


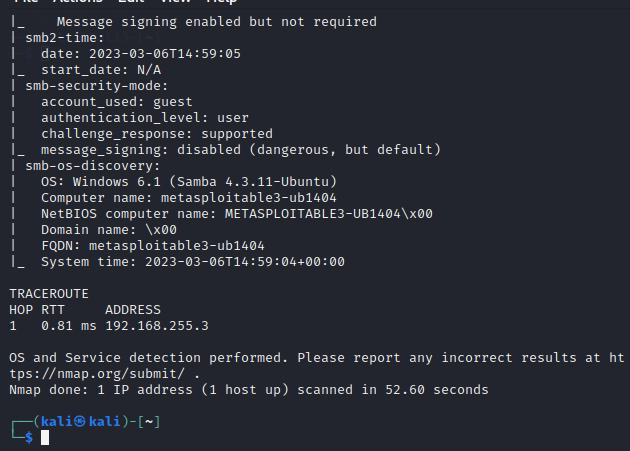




1. Run the command “sudo nmap -A 192.168.255.3”



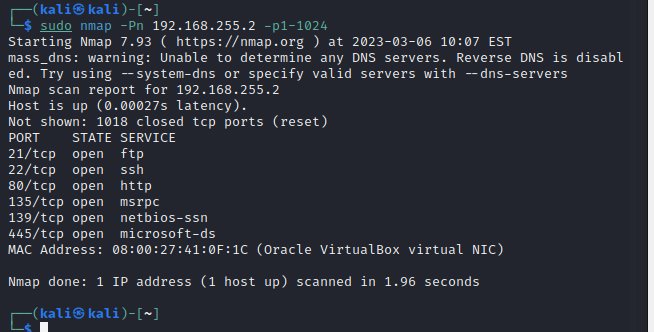




1. Explain what the -p1-1024 switch does.

This switch scans specified ports, with this one scanning a range between ports 1 -1024.

1. Run the command “sudo nmap –Pn 192.168.255.2 -p1-1024”.



1. Run the command “sudo nmap -Pn 192.168.255.3 -p1-1024”.

