****

|  |
| --- |
| ***BS Cyber Security Department AU*** |

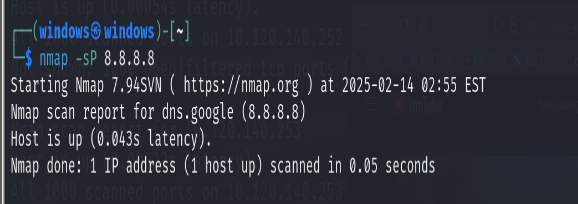
|  |  |
| --- | --- |
| **Registration ID** | **233026** |
| **Submitted By** | **Muhammad Sohaib Rafiq** |
| **Submitted To** | **Sir Moshin Sarfraz** |
| **Date of Submission** | **12/02/2024** |
| **Lab NO.** | **1** |
| **Subject** | **OS LAB** |

***1. Ping Sweep:***

***• Command: nmap -sP 192.168.1.0/24***

***• Result: number of hosts in up state***

***• MAC addresses***



Stealth Port Scan:

• Command: nmap -sS 192.168.1.1

• Result:

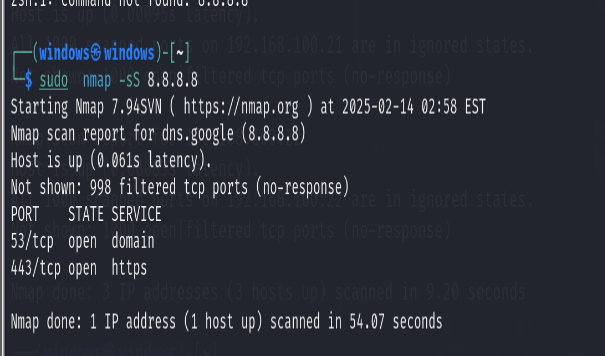
• states whether the hosts is in up or down state

• MAC address

• Scans 1000 well known ports and displays their state

(open/close/filtered/unfiltered)

• Services running on open ports



3. Scan Of Range Of IPs:

• Command: nmap -sF 192.168.1.0/24

• Result:

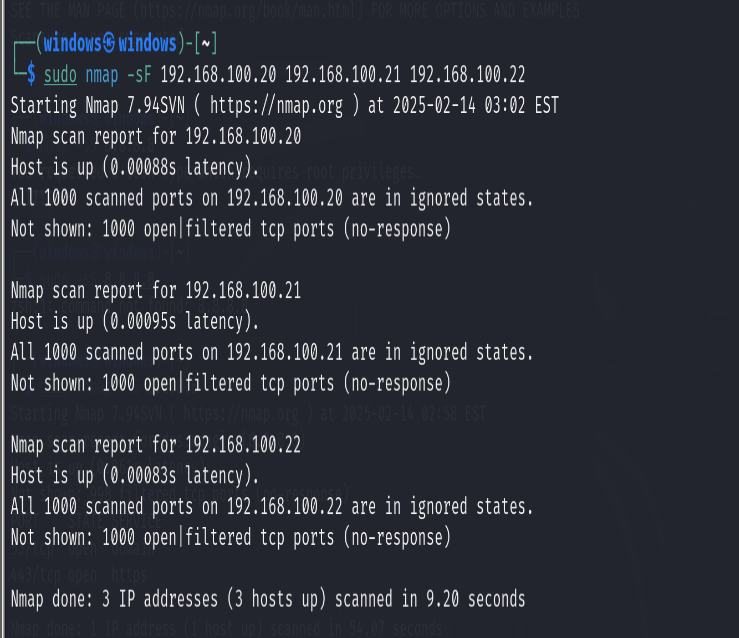
• states whether the hosts is in up or down state

• MAC address

• Scans 1000 ports and displays their state

(open/close/filtered/unfiltered)

• Services running on open ports

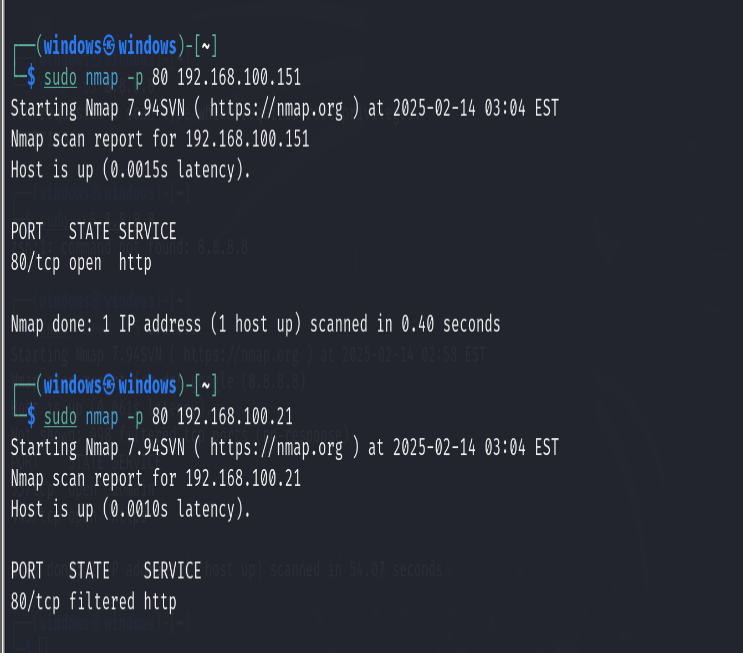


Scan Of Single Port:

• nmap -p 22 192.168.1.1

• only scans single specified port and shows state of port and service

being used on it

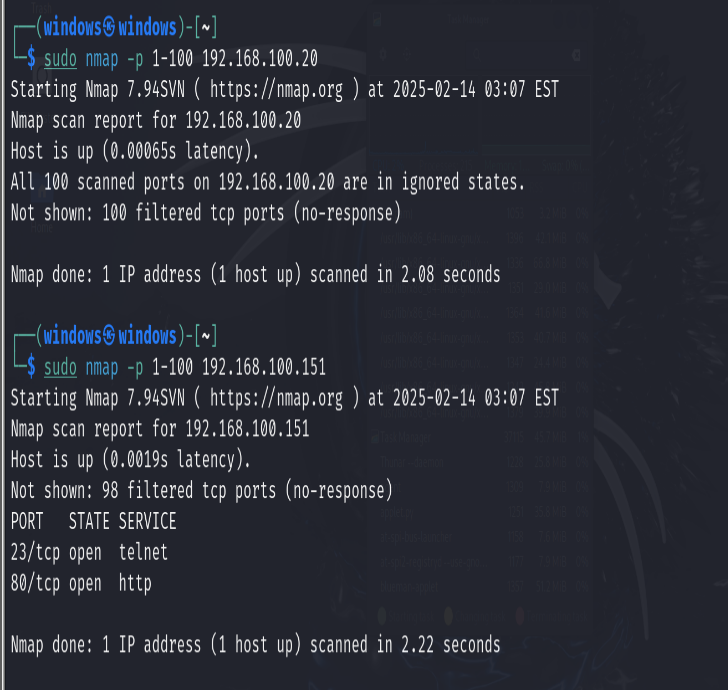


5. Scan Of Range Of Ports:

• nmap -p 1-100 192.168.1.1

• scans a range of ports which shows port state and service being applied

on it



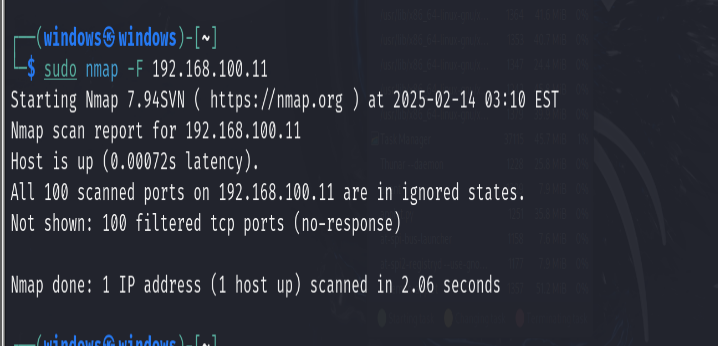
6. Scan Of 100 Most Common Ports:

• nmap -F 192.168.1.1

• scans 100 most common ports of website or device and shows their

state and services

• also known as Fast Scan



7. OS Detection:

• Command: nmap -O 192.168.1.1

• Result:

• states whether the hosts is in up or down state

• MAC address

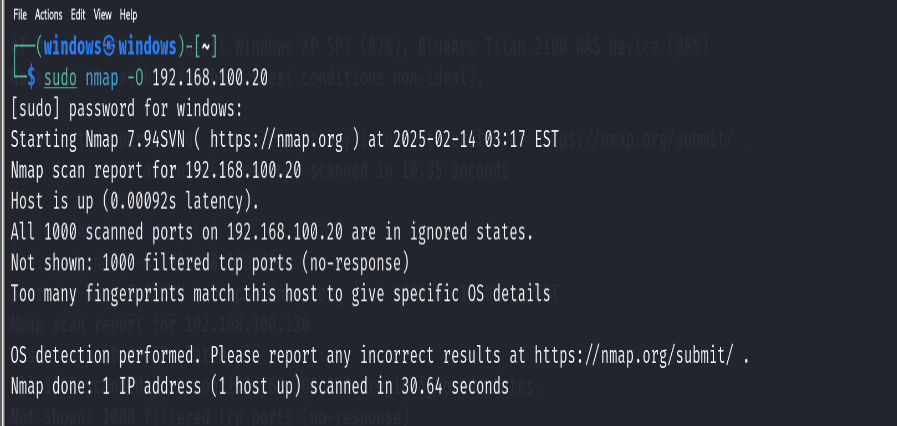
• Scans 1000 well knownports and displays their state

(open/close/filtered/unfiltered)

• Services running on open ports

• Device type (switch, general purpose, server etc)

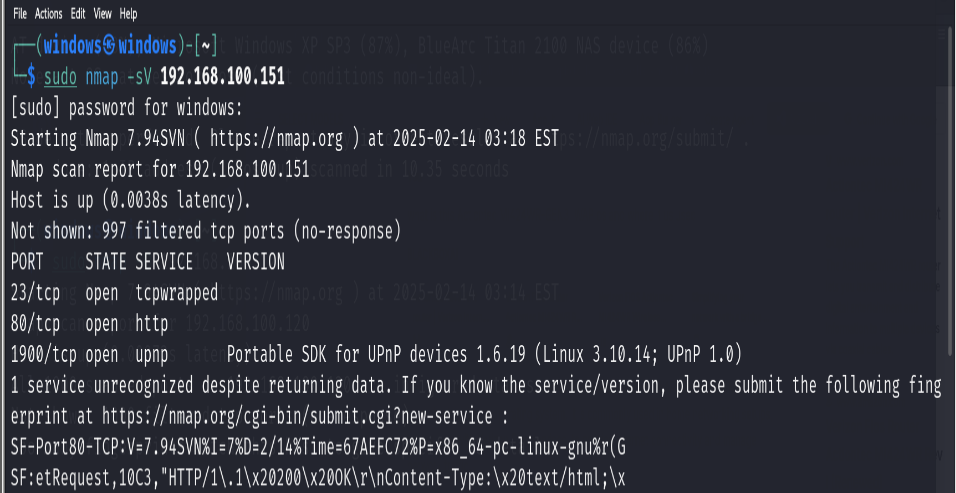
• OS running on host



8. Services Version Detection:

• Command: nmap -sV 192.168.1.1

• Helps to line up exploits for particular service versions

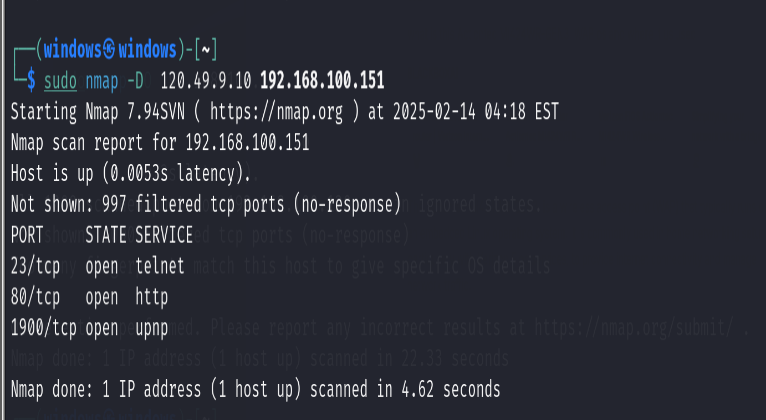


9. Decoy:

• Decoy is used to specify a bunch of IP addresses to give the impression

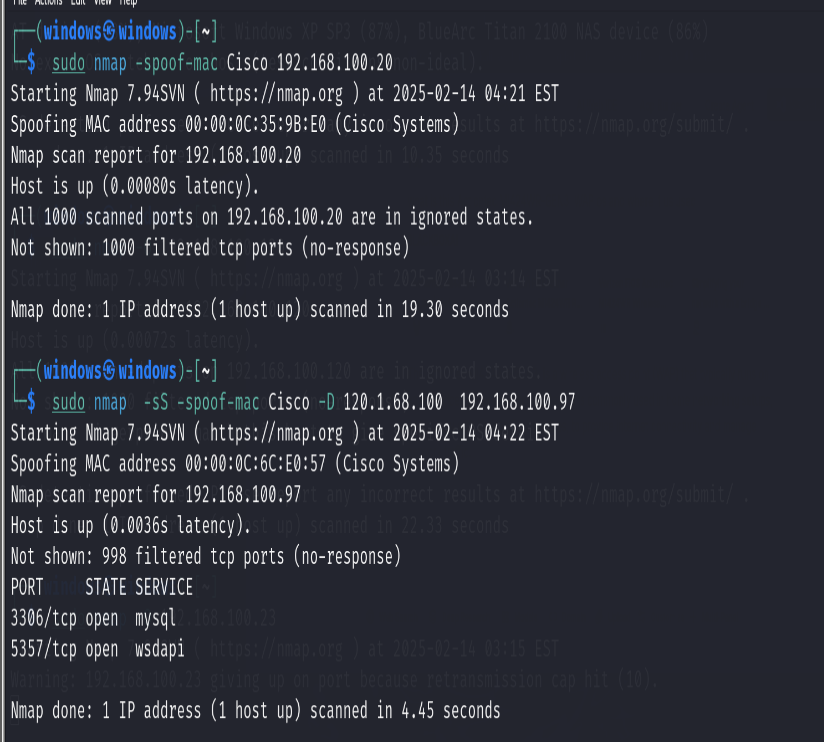
that these specified IP addresses are sending packets.

• Command: nmap -D 56.32.78.109 192.168.1.1



***10. MAC Spoofing:***

***• Command: nmap -sS -spoof-mac Cisco -D 56.32.78.109 192.168.1.1***



11. Zombie Scan:

• In this scan a trusted/innocent computer is used to launch an attack at

victim computer

• This trusted computer is considered as a zombie

• It is important that the zombie computer doesn’t communicate with any

other computer during this attack

• Command: nmap -Pn -sI 192.168.1.1\*zombie\* 192.168.1.10\*victim\*

• -sI is for ideal scan

• -Pn results in packets being sent from zombie IP (without -Pn packets

will be sent from real IP)

