Network Mapper

Detailed Report on the Use of Nmap with Various Options

CFCS2R
CENTER FOR CYBER
SECURITY STUDIES & RESEARCH

Introduction

Nmap (Network Mapper) is a popular tool used in cybersecurity to scan networks and find information about devices, services, and potential security issues. It's widely used because it offers many different options to perform various types of scans, which can help in understanding how a network is structured and where it might be vulnerable.

In this report, we will explore over 38 Nmap options, explaining what each one does, how it is used, and where it can be applied in real-world scenarios. By running these scans in a safe test environment, we'll gain practical knowledge about how to use Nmap effectively to improve network security.

Abstract

This report explores **Nmap (Network Mapper)**, a popular tool used in cybersecurity for scanning networks and finding security issues. It looks at over 38 different Nmap options, explaining what they do, how to use them, and where they are useful in real-life situations. The options are tested in a safe environment, with examples to show how Nmap can help in checking network security, finding devices, and fixing problems. The goal of this report is to help readers understand how Nmap works and how it can be used in cybersecurity.

Nmap

Nmap (Network Mapper) is a free tool used to scan and explore networks. It helps network administrators and cybersecurity professionals find devices, open ports, running services, and possible security issues on a network. Nmap is one of the most popular tools for checking the security of a network.

Nmap is mainly used for:

- **Network Scanning**: It shows which devices are connected to a network.
- **Port Scanning**: Nmap checks which ports are open and ready to receive data.
- **Service Detection**: It tells you what software is running on open ports, such as web servers or mail servers.
- **Operating System Detection**: Nmap can guess the operating system of a device based on how it responds to scans.
- **Vulnerability Detection**: By using special scripts, Nmap can detect security weaknesses in services or software on the network.

How Does Nmap Work?

Nmap works by sending packets (small pieces of data) to the target device or network. It analyzes the responses to figure out:

- What devices are online**.**
- Which ports are open or closed**.**
- What services are running on the open ports**.**

Nmap uses different scanning techniques to gather this information. Some of the popular ones include:

- **SYN Scan (-sS)**: A fast and stealthy scan that doesn't fully connect to the port, making it harder for the target to detect.
- **Connect Scan (-sT)**: This fully connects to the port, but it's easier to detect by firewalls and logs.
- **UDP Scan (-sU)**: Used for scanning services that run on UDP, like DNS.

Scripts in Nmap

Nmap also has a scripting engine called **NSE (Nmap Scripting Engine)**. These scripts allow Nmap to perform more advanced tasks like:

- **Vulnerability Scanning**: Detecting security weaknesses using --script vuln.
- **Brute-force Attacks**: Trying to guess login credentials for services.
- **Service Information**: Gathering detailed information about running services like web servers.

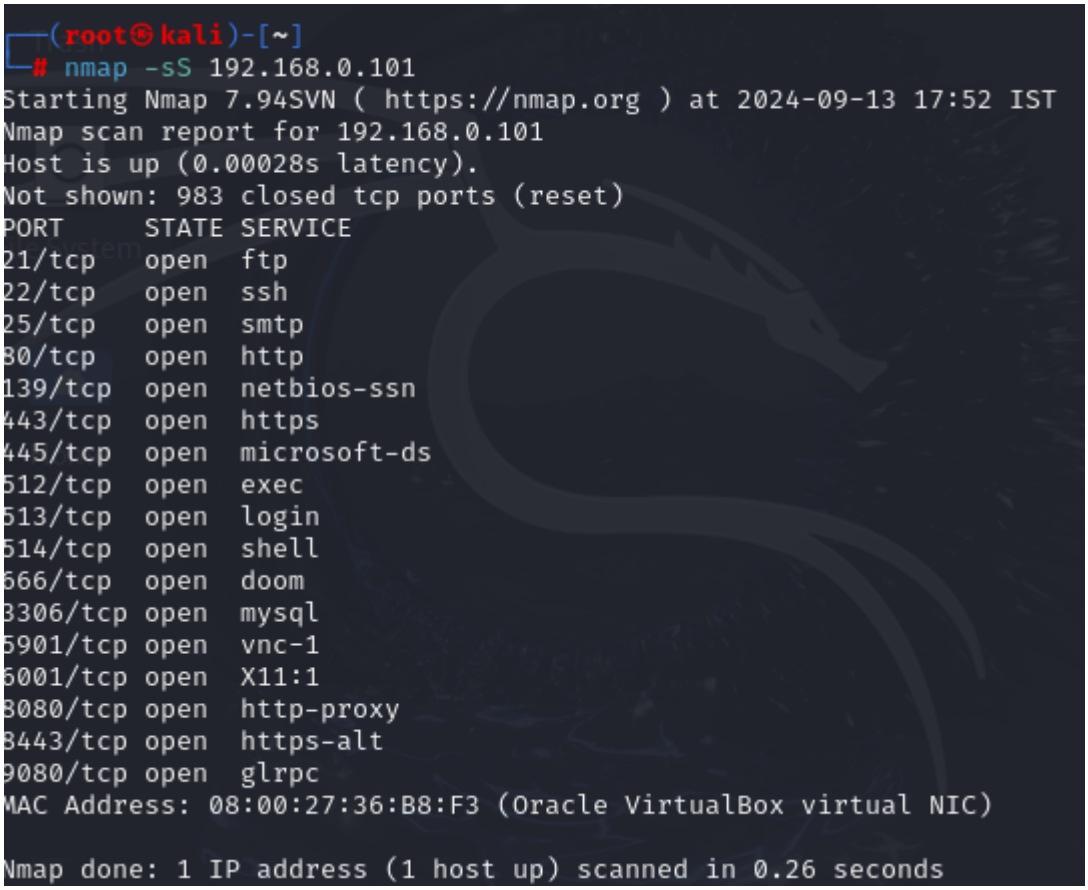
Nmap in Real Life

Nmap is used in various ways:

- **Penetration Testing**: Ethical hackers use Nmap to find weaknesses in networks that need fixing.
- **Network Troubleshooting**: Admins use Nmap to check if devices and services are running properly.
- **Security Audits**: It's used to check if firewalls and other security measures are properly set up.

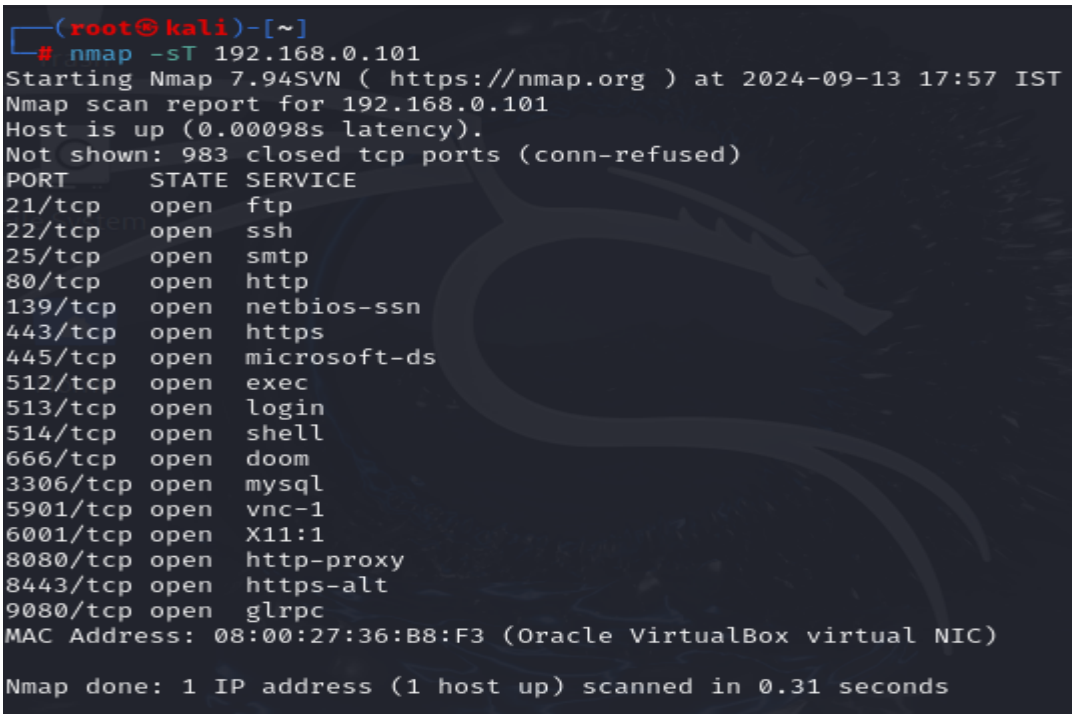
NMAP options in brief

1. **-sS (TCP SYN scan)**
   - **Purpose**: Scans ports without fully connecting to them, making it faster and less noticeable.
   - **Usage**: nmap -sS [target]
   - **Real World Application**: Great for quickly checking which ports are open without alerting the target.
   - **Example Command**: nmap –sS 192.168.0.101

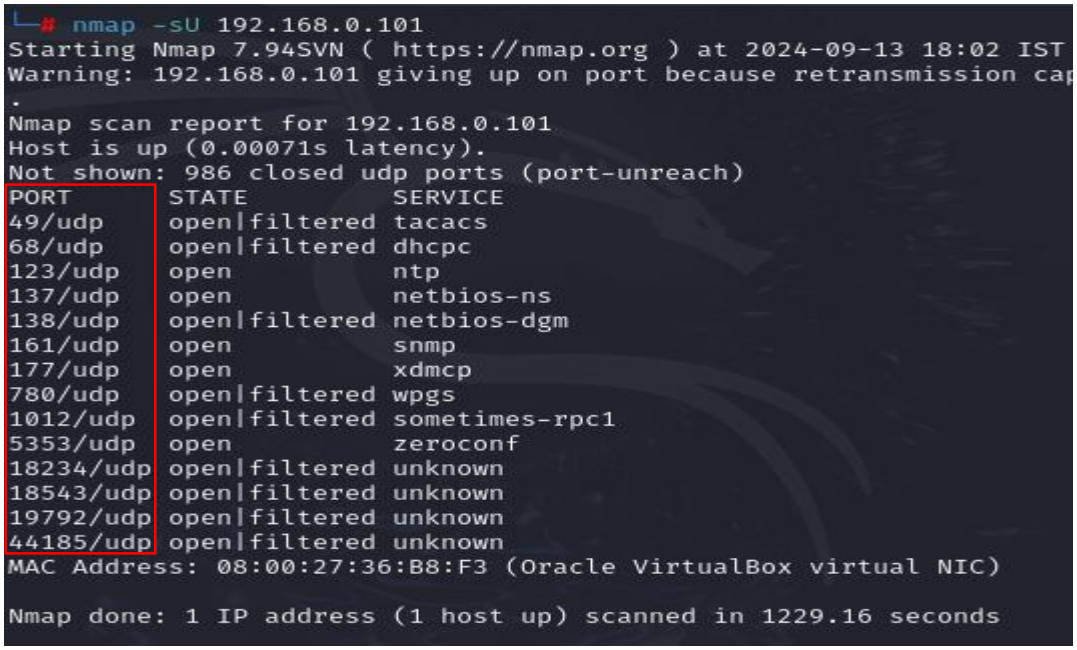


2. **-sT (TCP Connect scan)**
   - **Purpose**: Fully connects to each port, making it easier to detect but doesn't need special permissions.
   - **Usage**: nmap -sT [target]
   - **Real World Application**: Use this if you don’t have special permissions, but it’s easier to detect by firewalls.

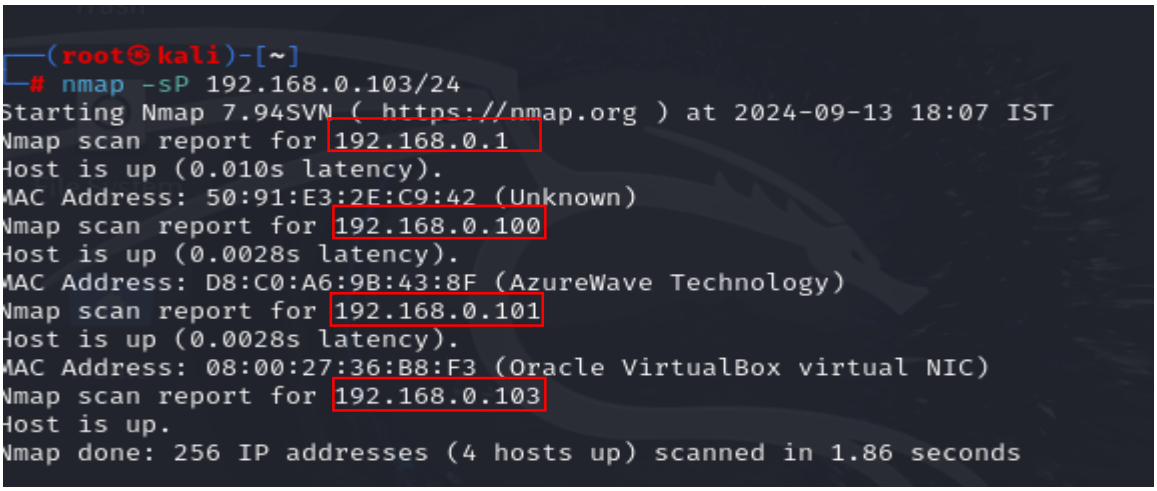
- **Example Command**: nmap –sT 192.168.0.101



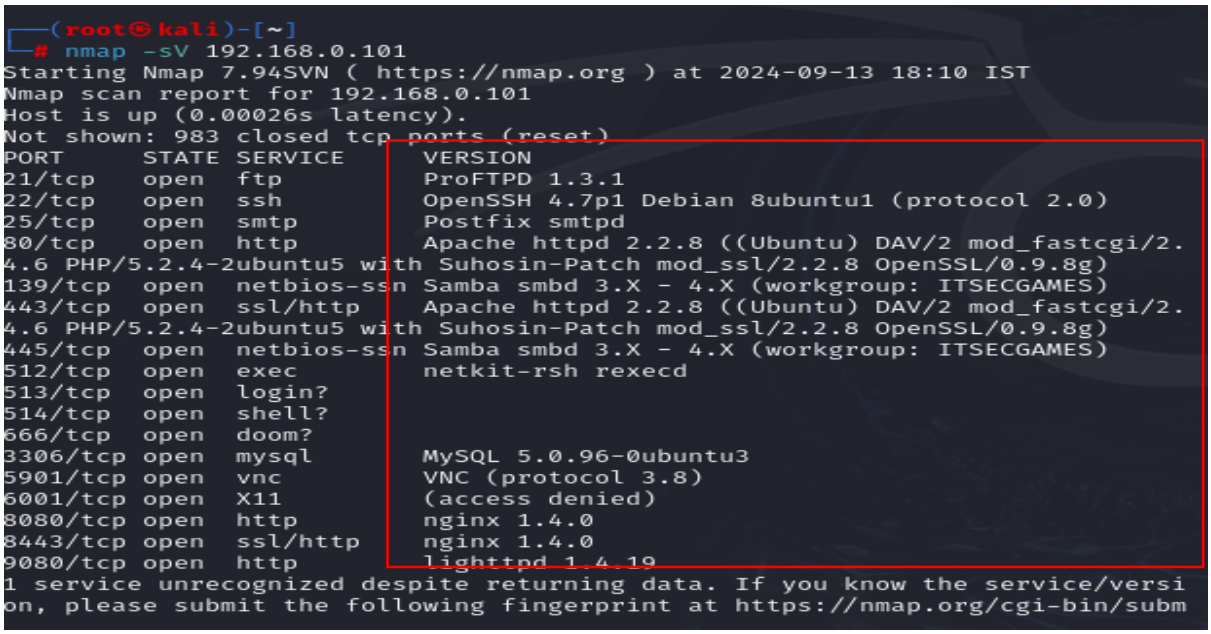
3. **-sU (UDP scan)**
   - **Purpose**: Scans for open UDP ports, which can be slower because it doesn't use a handshake like TCP.
   - **Usage**: nmap -sU [target]
   - **Real World Application**: For finding services like DNS and SNMP running over UDP.
   - **Example Command**:nmap –sU 192.168.0.101



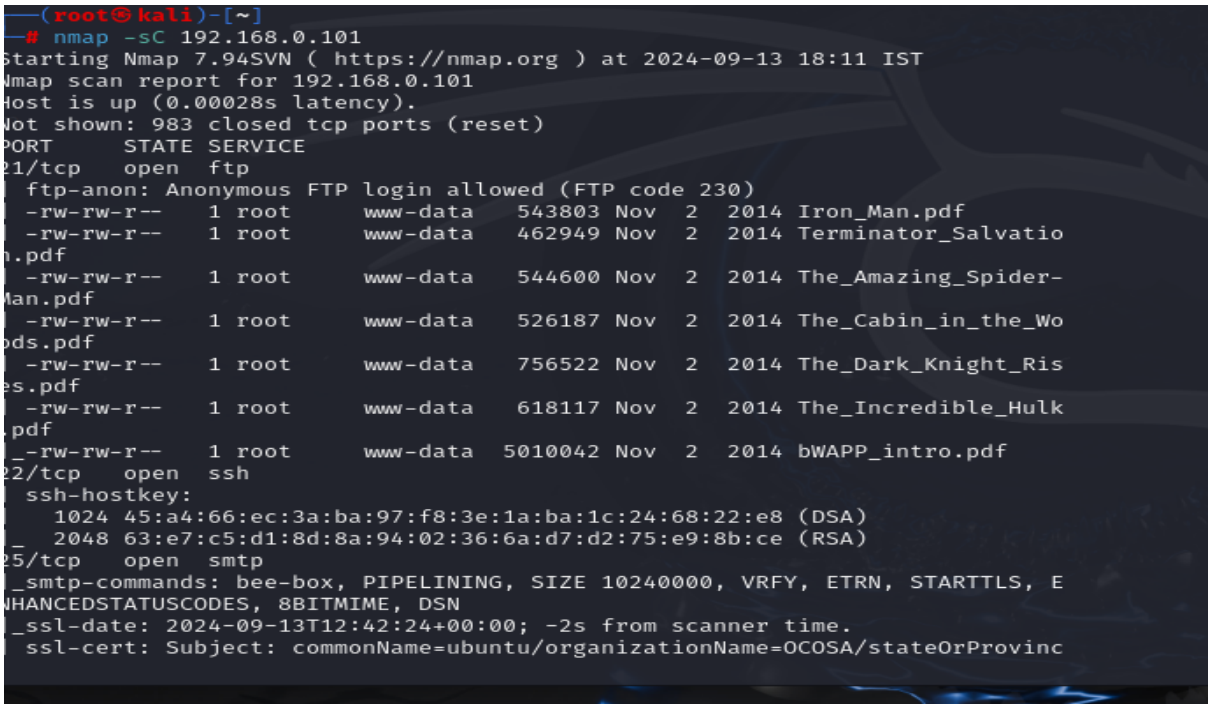
4. **-sP (Ping scan)**
    - **Purpose**: Checks which devices are up on a network by sending ping requests.
    - **Usage**: nmap -sP [target]
    - **Real World Application**: Useful for quickly identifying which devices are online without scanning ports.
    - **Example Command**:nmap –sP 192.168.0.103/24

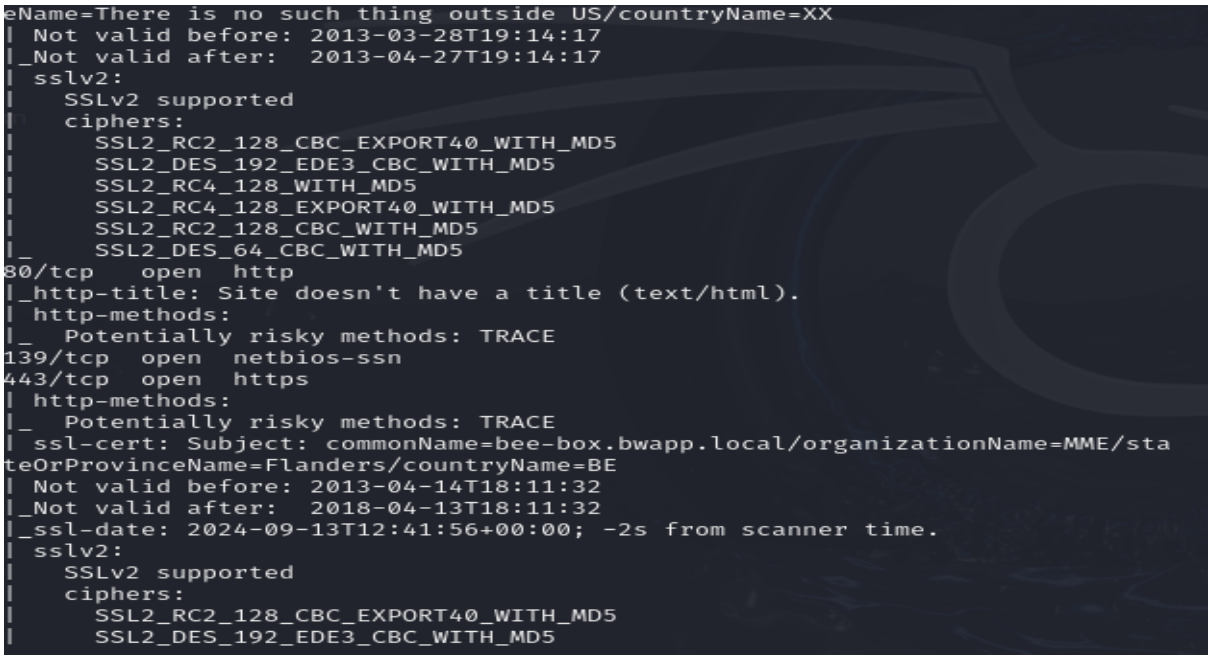


5. **-sV (Service version detection)**
    - **Purpose**: Identifies the software version running on open ports.
    - **Usage**: nmap -sV [target]
    - **Real World Application**: To gather more detailed information about the services running on a device.
    - **Example Command**:nmap –sV 192.168.0.101



6. **-sC (Default script scan)**
    - **Purpose**: Runs a set of default Nmap scripts to check for vulnerabilities and additional information.
    - **Usage**: nmap -sC [target]
    - **Real World Application**: For a basic security scan to check for known issues.
    - **Example Command**:nmap –sC 192.168.0.101





```
3306/tcp open  mysql
| mysql-info:
|   Protocol: 10
|   Version: 5.0.96-0ubuntu3
|   Thread ID: 40
|   Capabilities flags: 41516
|   Some Capabilities: Support41Auth, Speaks41ProtocolNew, SupportsTransacti
ons, ConnectWithDatabase, SupportsCompression, LongColumnFlag
|   Status: Autocommit
|_  Salt: V>p=}!'?G)5mH`)JxAxY
5901/tcp open  vnc-1
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|_    VNC Authentication (2)
6001/tcp open  X11:1
8080/tcp open  http-proxy
|_http-open-proxy: Proxy might be redirecting requests
|_http-title: Site doesn't have a title (text/html).
8443/tcp open  https-alt
|_http-title: Site doesn't have a title (text/html).
| tls-nextprotoneg:
|_  http/1.1
|_ssl-date: 2024-09-13T12:41:55+00:00; -2s from scanner time.
| ssl-cert: Subject: commonName=bee-box.bwapp.local/organizationName=MME/sta
teOrProvinceName=Flanders/countryName=BE
| Not valid before: 2013-04-14T18:11:32
|_Not valid after:  2018-04-13T18:11:32
9080/tcp open  glrpc
MAC Address: 08:00:27:36:B8:F3 (Oracle VirtualBox virtual NIC)
```

```
9080/tcp open  glrpc
MAC Address: 08:00:27:36:B8:F3 (Oracle VirtualBox virtual NIC)

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.28a)
|   Computer name: bee-box
|   NetBIOS computer name:
|   Domain name:
|   FQDN: bee-box
|_  System time: 2024-09-13T14:41:55+02:00
|_clock-skew: mean: -24m02s, deviation: 53m39s, median: -2s
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_nbstat: NetBIOS name: BEE-BOX, NetBIOS user: <unknown>, NetBIOS MAC: <unkn
own> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

Nmap done: 1 IP address (1 host up) scanned in 75.06 seconds
```

7. **-sW (TCP Window scan)**
   - **Purpose**: Uses TCP window size changes to detect open ports.
   - **Usage**: nmap -sW [target]
   - **Real World Application**: A less common, alternative scan for finding open ports.
   - **Example Command**:nmap –sW 192.168.0.101

```
┌──(root㉿kali)-[~]
└─# nmap -sW 192.168.0.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-13 18:12 IST
Nmap scan report for 192.168.0.101
Host is up (0.00025s latency).
All 1000 scanned ports on 192.168.0.101 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:36:B8:F3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

8. **-sO (IP Protocol scan)**
    - **Purpose**: Scans to find which IP protocols (like TCP, UDP, ICMP) are supported on the target.
    - **Usage**: nmap -sO [target]
    - **Real World Application**: Useful when you're not sure which protocols are in use.
    - **Example Command**:nmap –sO 192.168.0.101

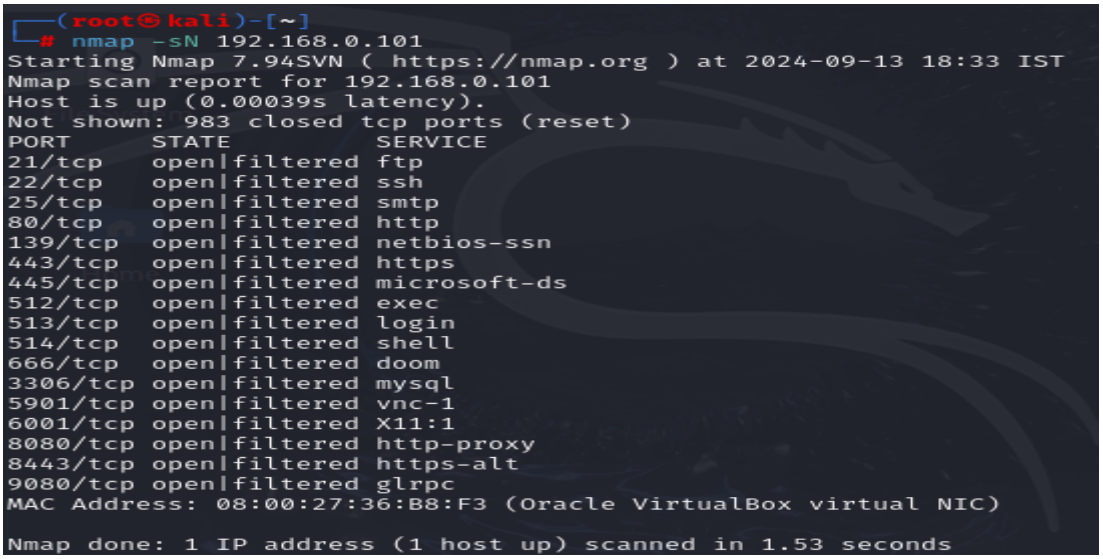
```
┌──(root㉿kali)-[~]
└─# nmap -sO 192.168.0.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-13 18:15 IST
Warning: 192.168.0.101 giving up on port because retransmission cap hit (10)
.
Nmap scan report for 192.168.0.101
Host is up (0.00068s latency).
Not shown: 218 closed n/a protocols (proto-unreach), 35 open|filtered n/a pr
otocols (no-response)
PROTOCOL STATE SERVICE
1        open  icmp
6        open  tcp
17       open  udp
MAC Address: 08:00:27:36:B8:F3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 520.65 seconds
```

9. **-sA (TCP ACK scan)**
    - **Purpose**: Checks whether ports are filtered by a firewall without determining if they are open or closed.
    - **Usage**: nmap -sA [target]
    - **Real World Application**: For testing firewall rules without revealing port statuses.
    - **Example Command**:nmap –sA 192.168.0.101

```
┌──(root㉿kali)-[~]
└─# nmap -sA 192.168.0.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-13 18:31 IST
Nmap scan report for 192.168.0.101
Host is up (0.00021s latency).
All 1000 scanned ports on 192.168.0.101 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 08:00:27:36:B8:F3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

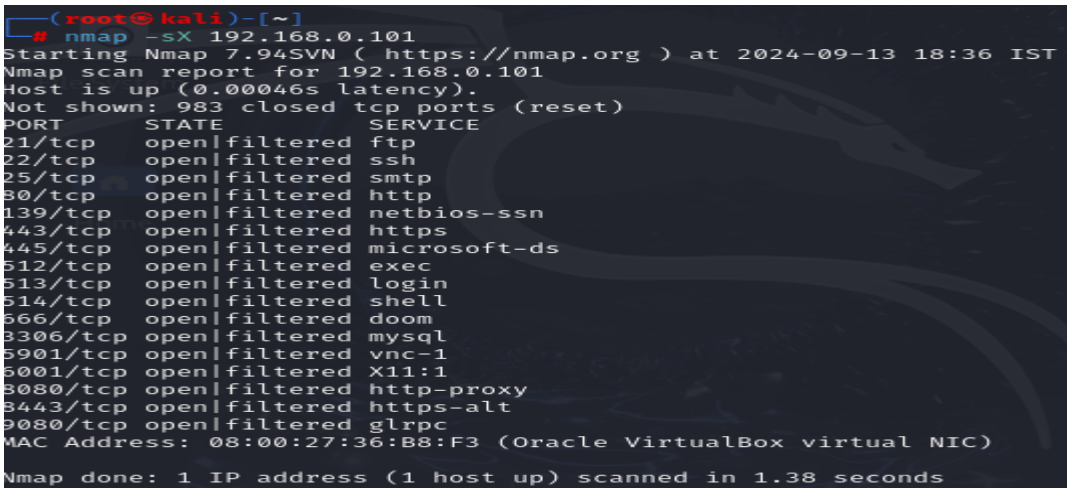
10.**-sN (TCP Null scan)**

- **Purpose**: Sends packets with no flags set to bypass firewalls and determine if ports are open.
- **Usage**: nmap -sN [target]
- **Real World Application**: To check if firewalls are blocking scans based on the TCP flags.
- **Example Command**:nmap –sN 192.168.0.101



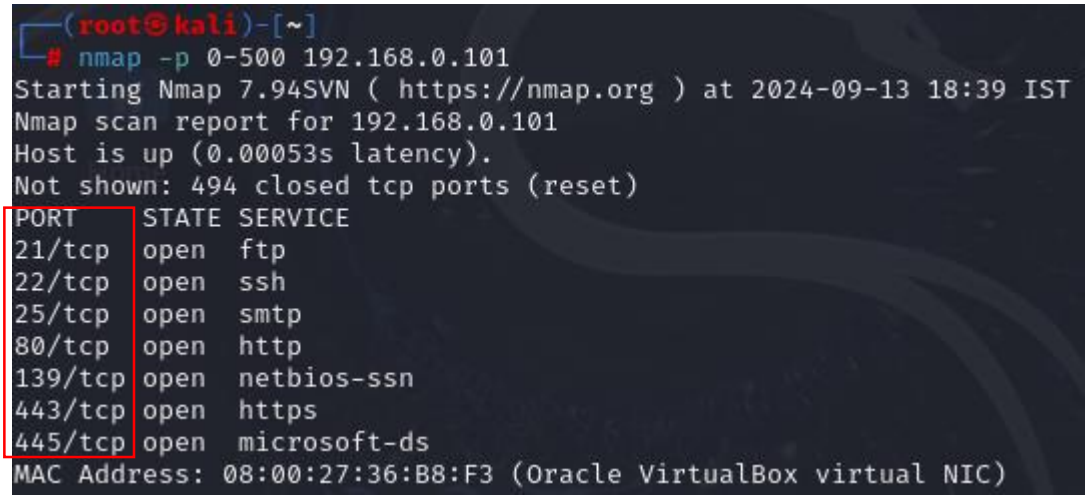
11.**-sX (TCP Xmas scan)**

- **Purpose**: Sends packets with unusual flag combinations (like a Christmas tree) to trick firewalls.
- **Usage**: nmap -sX [target]
- **Real World Application**: A stealthy scan for detecting open ports through firewalls.
- **Example Command**:nmap –sX 192.168.0.101



12.**-p (Port range specification)**

- **Purpose**: Specifies which ports to scan.
- **Usage**: nmap -p [port-range] [target]
- **Real World Application**: Use this when you want to scan specific ports, like nmap -p 80,443 [target] for HTTP/HTTPS.
- **Example Command**:nmap -p 0-500 192.168.0.101

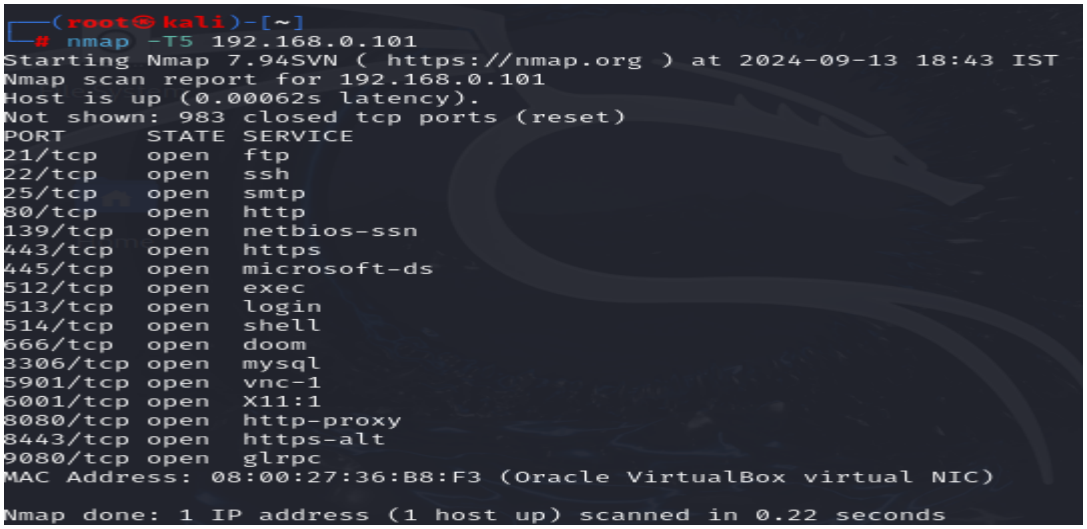


13.**-F (Fast scan)**

- **Purpose**: Scans fewer ports to finish quickly.
- **Usage**: nmap -F [target]
- **Real World Application**: When you need results fast and don't require a deep scan.
- **Example Command**:nmap -F 192.168.0.101

14.**-T0 to -T5 (Timing template)**

- **Purpose**: Adjusts the speed of the scan, with -T0 being the slowest and stealthiest, and -T5 being the fastest.
- **Usage**: nmap -T4 [target]
- **Real World Application**: Slow scans like -T0 are good for avoiding detection, while -T4 or -T5 is good for speed when detection isn't an issue.
- **Example Command**:nmap -T5 192.168.0.101

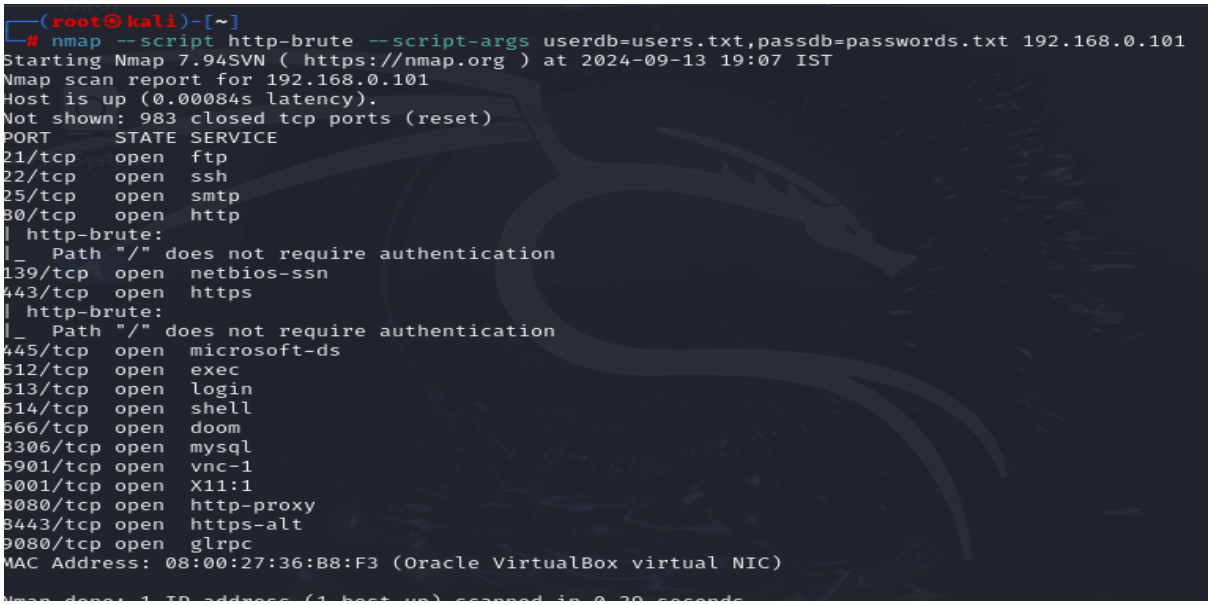


15.**--script (Nmap Scripting Engine)**

- **Purpose**: Runs Nmap scripts to perform more advanced tasks like vulnerability detection.
- **Usage**: nmap --script [script-name] [target]
- **Real World Application**: For more complex scans, like nmap --script vuln [target] to find vulnerabilities.
- **ExampleCommand:** nmap --script vuln 192.168.0.101

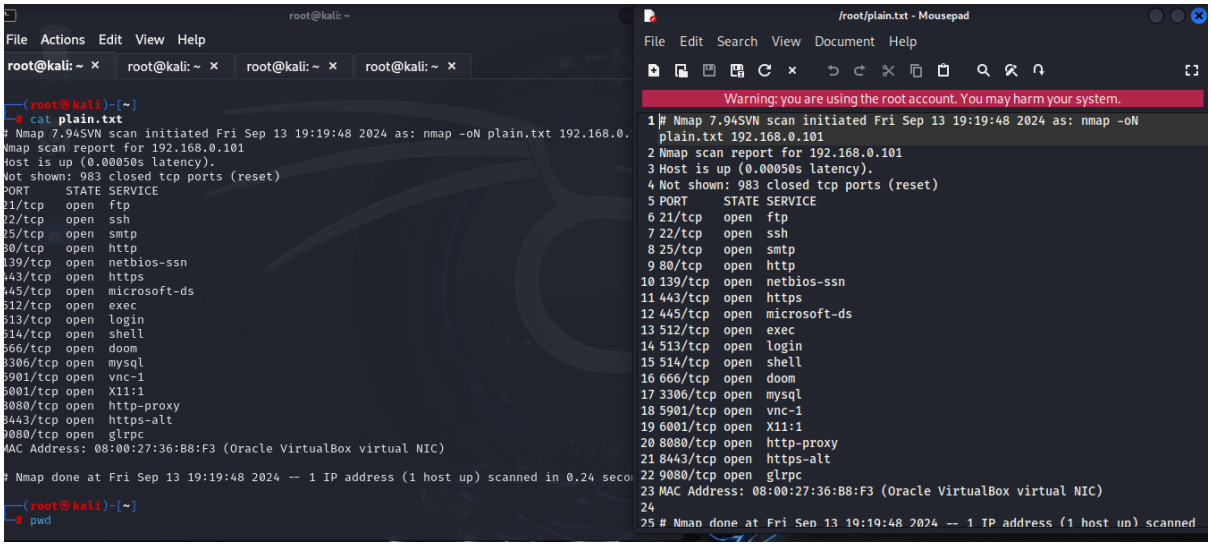
16.**--script-args (Script arguments)**

- **Purpose**: Passes extra options to Nmap scripts.
- **Usage**: nmap --script [script-name] --script-args [arguments] [target]
- **Real World Application**: To customize how scripts run, such as specifying login credentials for authentication checks.
- **ExampleCommand:** nmap --script http-brute --script-args userdb=users.txt,passdb=passwords.txt 192.168.0.101



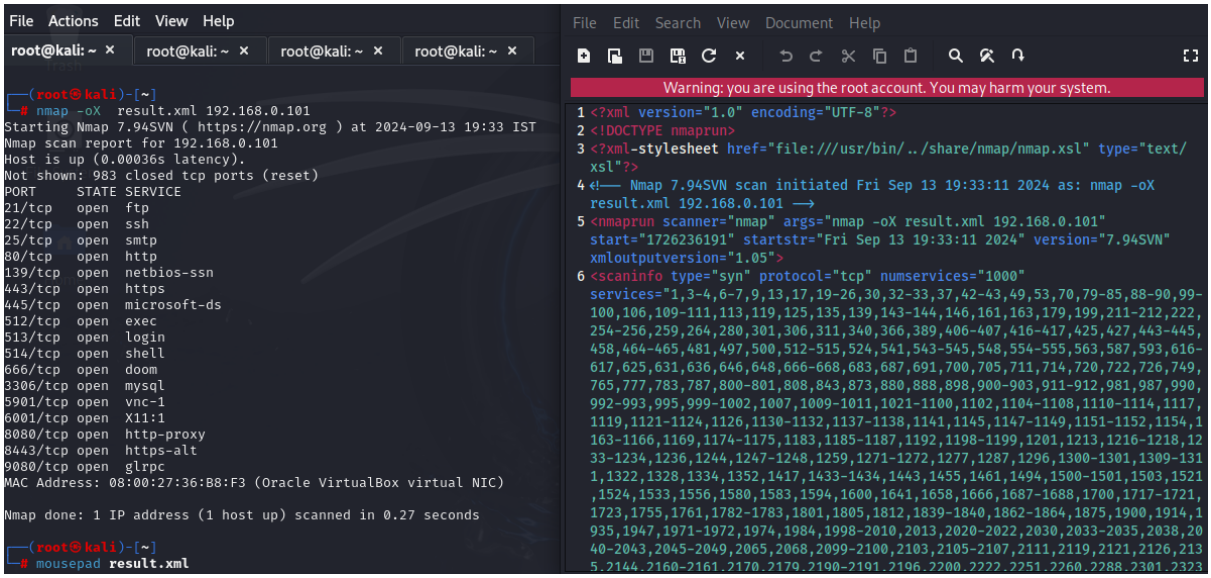
17.**-oN (Normal output)**

- **Purpose**: Saves the scan results in a human-readable format.
- **Usage**: nmap -oN [filename] [target]
- **Real World Application**: For saving the scan results in plain text format.
- **ExampleCommand:** nmap -oN plain.txt 192.168.0.101



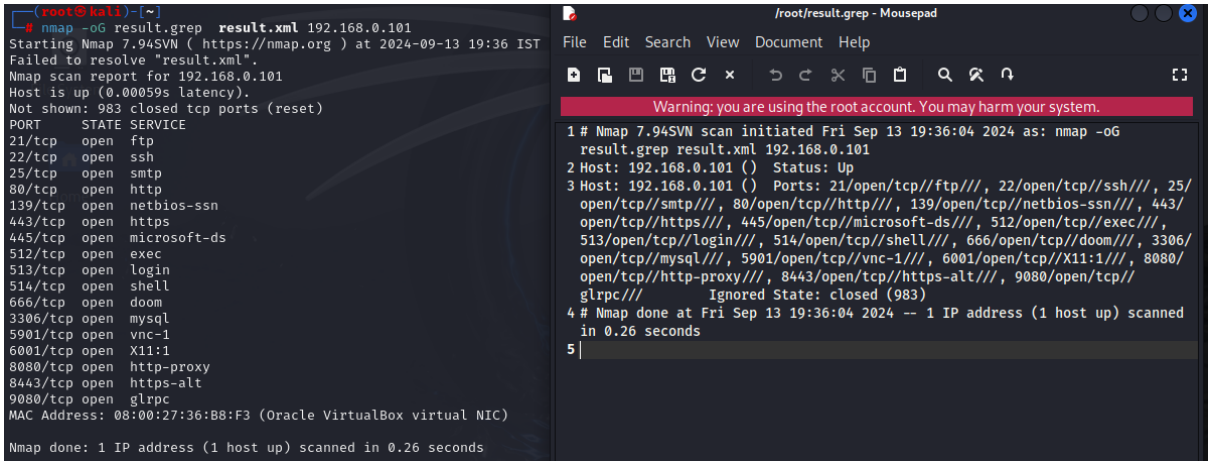
18.**-oX (XML output)**

- **Purpose**: Saves scan results in XML format.
- **Usage**: nmap -oX [filename] [target]
- **Real World Application**: Use this when you need to process the scan results with other tools that use XML.
- **ExampleCommand:** nmap -oX result.xml 192.168.0.101



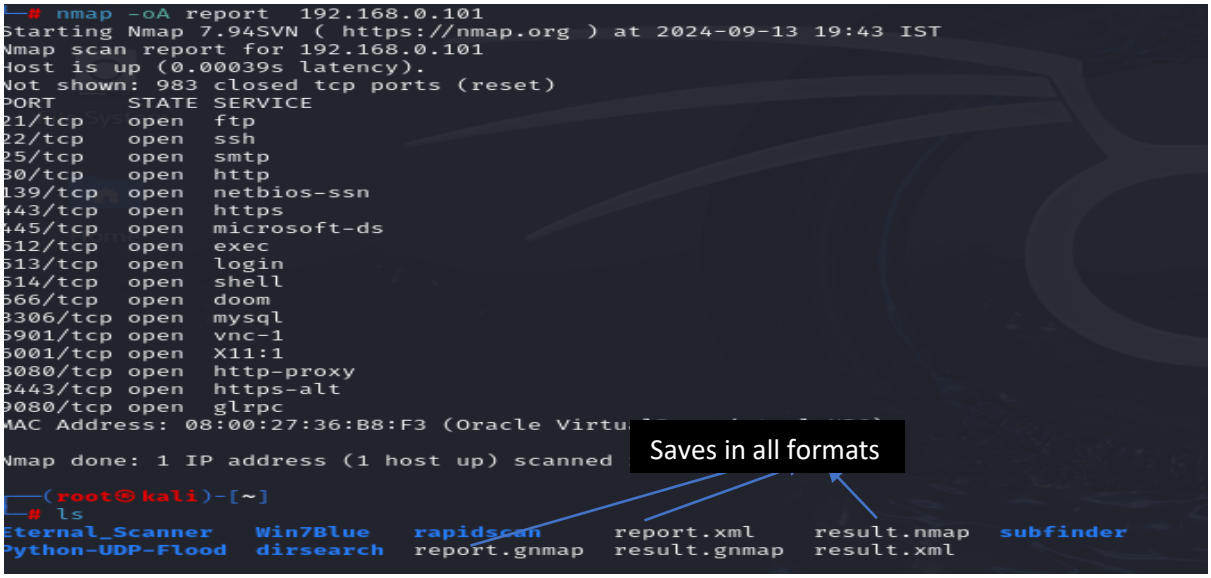
19.**-oG (Grepable output)**

- **Purpose**: Saves results in a format that’s easy to search through using the grep command.
- **Usage**: nmap -oG [filename] [target]
- **Real World Application**: Useful if you plan to filter or search the scan results later.
- **ExampleCommand:** nmap -oG result.grep result.xml 192.168.0.101



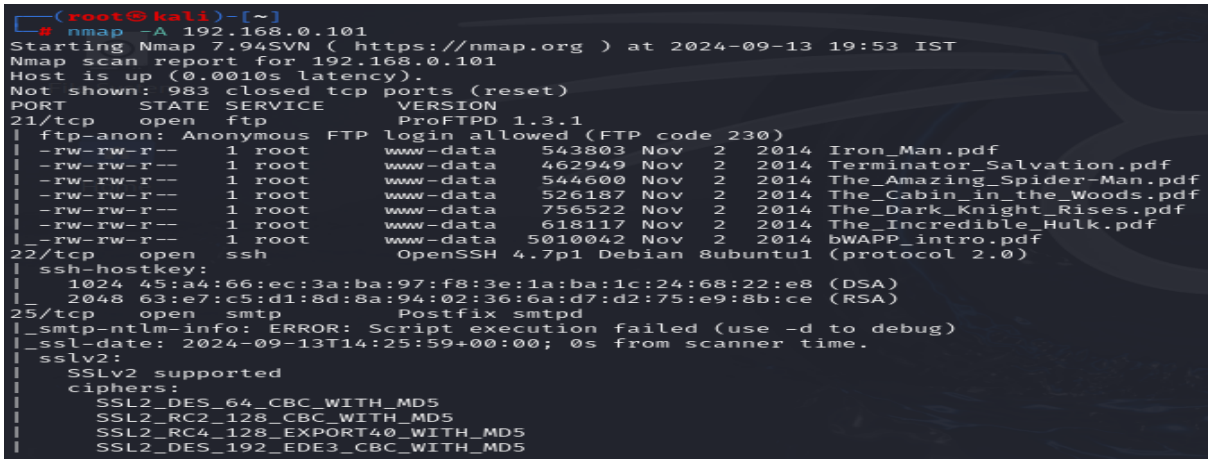
20.**-oA (Output all formats)**

- **Purpose**: Saves scan results in normal, XML, and grepable formats at the same time.
- **Usage**: nmap -oA [basename] [target]
- **Real World Application**: For saving results in all formats when you want flexibility.
- **ExampleCommand:** nmap -oA report 192.168.0.101



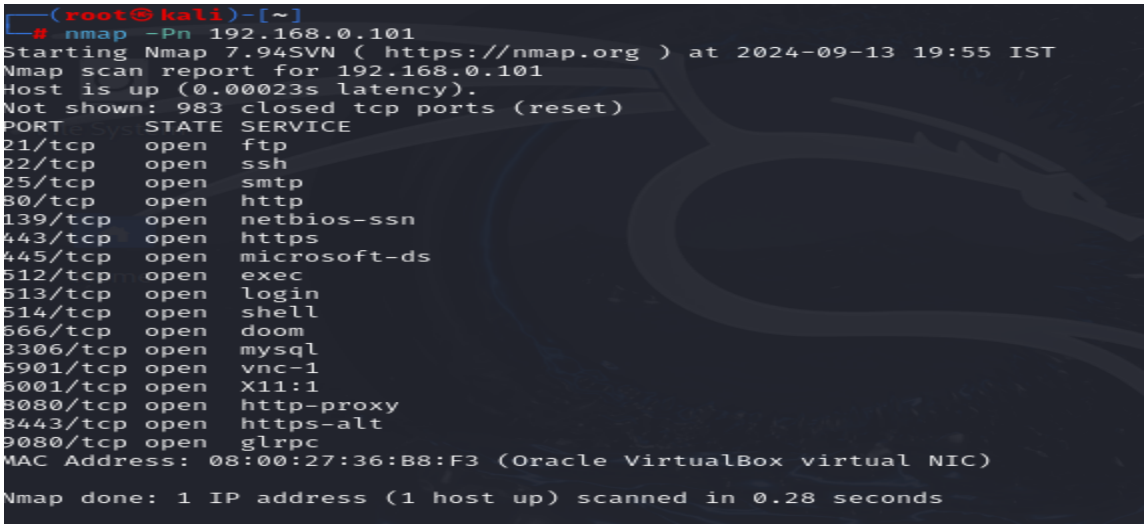
21.**-A (Aggressive scan options)**

- **Purpose**: Performs a more detailed scan, including OS detection, version detection, and more.
- **Usage**: nmap -A [target]
- **Real World Application**: When you need a thorough scan and detailed information.
- **ExampleCommand:** nmap -A 192.168.0.101



22.**-PN or -Pn (No Ping)**

- **Purpose**: Skips the ping step, assuming the target is online.
- **Usage**: nmap -Pn [target]
- **Real World Application**: Useful if the target blocks ping requests but you still want to scan it.
- **ExampleCommand:** nmap -Pn 192.168.0.101



23.**-D (Decoy scan)**

- **Purpose**: Sends the scan from multiple fake IP addresses to hide your real IP. RND:5: This generates 5 random decoy IP addresses along with your real IP to confuse the target about which one is real.
- **Usage**: nmap -D RND:10 [target]
- **Real World Application**: Use this for hiding your identity during a scan.
- **ExampleCommand:** nmap -D 192.168.0.1,192.168.0.101,192.168.0.103

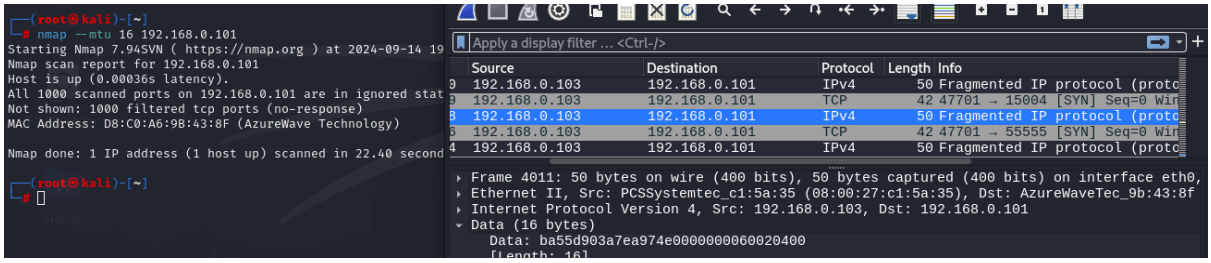
24.**-f (Fragment packets)**

- **Purpose**: Breaks the scan packets into smaller pieces to avoid detection by firewalls.
- **Usage**: nmap -f [target]
- **Real World Application**: To bypass firewalls that block large scan packets.
- **ExampleCommand:** nmap -f 192.168.0.101

```
┌──(root㉿kali)-[~]
└─# nmap -f 192.168.0.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-13 18:40 IST
Nmap scan report for 192.168.0.101
Host is up (0.00031s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 08:00:27:36:B8:F3 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

25.**--mtu (Set the maximum transmission unit size)**

- **Purpose**: Adjusts the size of the packets being sent.
- **Usage**: nmap --mtu [size] [target]
- **Real World Application**: For testing how a network handles different packet sizes.
- **ExampleCommand:** nmap --mtu 16 192.168.0.101



26.**-v (Increase verbosity)**

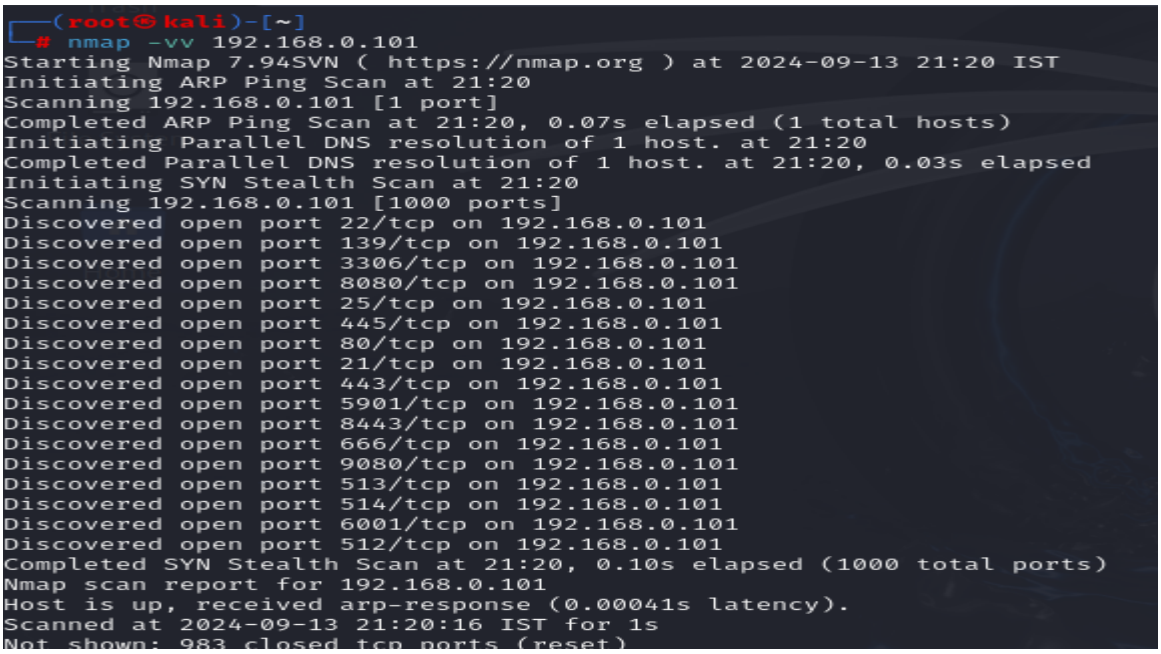
- **Purpose**: Displays more detailed output during the scan.
- **Usage**: nmap -v [target]
- **Real World Application**: When you want to see what Nmap is doing in real-time.
- **ExampleCommand:** nmap -v 192.168.0.101

```
┌──(root㉿kali)-[~]
└─# nmap -v 192.168.0.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-13 21:24 IST
Initiating ARP Ping Scan at 21:24
Scanning 192.168.0.101 [1 port]
Completed ARP Ping Scan at 21:24, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:24
Completed Parallel DNS resolution of 1 host. at 21:24, 0.02s elapsed
Initiating SYN Stealth Scan at 21:24
Scanning 192.168.0.101 [1000 ports]
Discovered open port 443/tcp on 192.168.0.101
Discovered open port 25/tcp on 192.168.0.101
Discovered open port 139/tcp on 192.168.0.101
Discovered open port 21/tcp on 192.168.0.101
Discovered open port 8080/tcp on 192.168.0.101
Discovered open port 22/tcp on 192.168.0.101
Discovered open port 80/tcp on 192.168.0.101
Discovered open port 445/tcp on 192.168.0.101
Discovered open port 3306/tcp on 192.168.0.101
Discovered open port 513/tcp on 192.168.0.101
Discovered open port 9080/tcp on 192.168.0.101
Discovered open port 6001/tcp on 192.168.0.101
Discovered open port 5901/tcp on 192.168.0.101
Discovered open port 8443/tcp on 192.168.0.101
Discovered open port 666/tcp on 192.168.0.101
Discovered open port 514/tcp on 192.168.0.101
Discovered open port 512/tcp on 192.168.0.101
Completed SYN Stealth Scan at 21:24, 0.12s elapsed (1000 total ports)
Nmap scan report for 192.168.0.101
Host is up (0.00022s latency).
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE
```

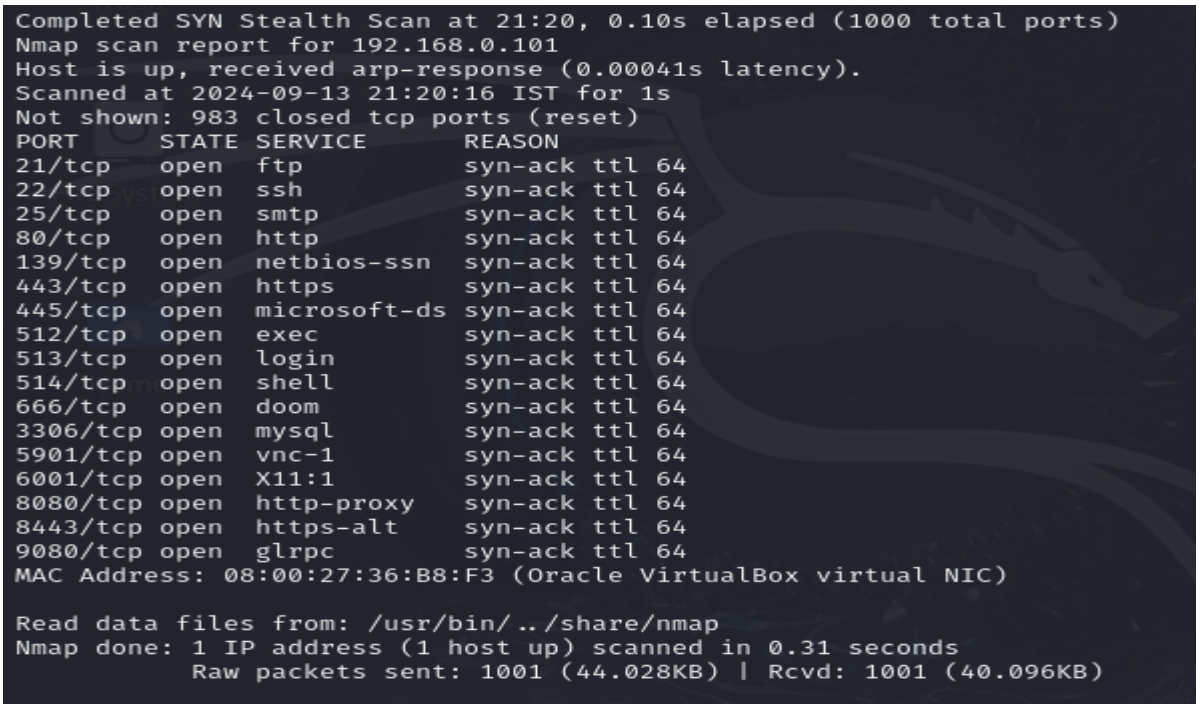
```
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
25/tcp   open  smtp
80/tcp   open  http
139/tcp  open  netbios-ssn
443/tcp  open  https
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
666/tcp  open  doom
3306/tcp open  mysql
5901/tcp open  vnc-1
6001/tcp open  X11:1
8080/tcp open  http-proxy
8443/tcp open  https-alt
9080/tcp open  glrpc
MAC Address: 08:00:27:36:B8:F3 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.33 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.096KB)
```

27.**-vv (Very verbose)**

- **Purpose**: Shows even more detailed output than -v.
- **Usage**: nmap -vv [target]
- **Real World Application**: For maximum detail during a scan.
- **ExampleCommand:** nmap -vv 192.168.0.101



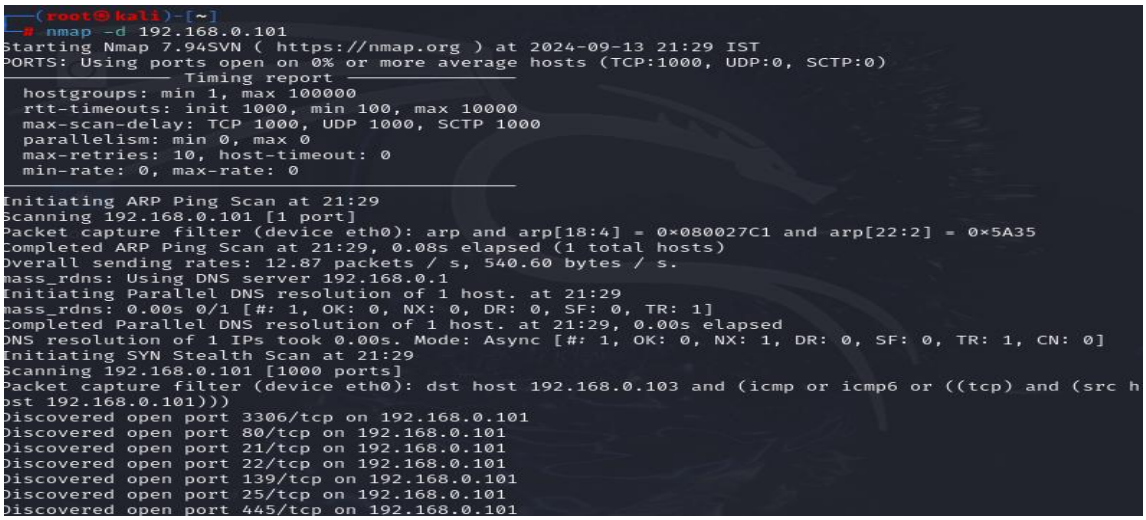
```
┌──(root㉿kali)-[~]
└─# nmap -vv 192.168.0.101
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-13 21:20 IST
Initiating ARP Ping Scan at 21:20
Scanning 192.168.0.101 [1 port]
Completed ARP Ping Scan at 21:20, 0.07s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:20
Completed Parallel DNS resolution of 1 host. at 21:20, 0.03s elapsed
Initiating SYN Stealth Scan at 21:20
Scanning 192.168.0.101 [1000 ports]
Discovered open port 22/tcp on 192.168.0.101
Discovered open port 139/tcp on 192.168.0.101
Discovered open port 3306/tcp on 192.168.0.101
Discovered open port 8080/tcp on 192.168.0.101
Discovered open port 25/tcp on 192.168.0.101
Discovered open port 445/tcp on 192.168.0.101
Discovered open port 80/tcp on 192.168.0.101
Discovered open port 21/tcp on 192.168.0.101
Discovered open port 443/tcp on 192.168.0.101
Discovered open port 5901/tcp on 192.168.0.101
Discovered open port 8443/tcp on 192.168.0.101
Discovered open port 666/tcp on 192.168.0.101
Discovered open port 9080/tcp on 192.168.0.101
Discovered open port 513/tcp on 192.168.0.101
Discovered open port 514/tcp on 192.168.0.101
Discovered open port 6001/tcp on 192.168.0.101
Discovered open port 512/tcp on 192.168.0.101
Completed SYN Stealth Scan at 21:20, 0.10s elapsed (1000 total ports)
Nmap scan report for 192.168.0.101
Host is up, received arp-response (0.00041s latency).
Scanned at 2024-09-13 21:20:16 IST for 1s
Not shown: 983 closed tcp ports (reset)
```



```
Completed SYN Stealth Scan at 21:20, 0.10s elapsed (1000 total ports)
Nmap scan report for 192.168.0.101
Host is up, received arp-response (0.00041s latency).
Scanned at 2024-09-13 21:20:16 IST for 1s
Not shown: 983 closed tcp ports (reset)
PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack ttl 64
22/tcp   open  ssh          syn-ack ttl 64
25/tcp   open  smtp         syn-ack ttl 64
80/tcp   open  http         syn-ack ttl 64
139/tcp  open  netbios-ssn  syn-ack ttl 64
443/tcp  open  https        syn-ack ttl 64
445/tcp  open  microsoft-ds syn-ack ttl 64
512/tcp  open  exec         syn-ack ttl 64
513/tcp  open  login        syn-ack ttl 64
514/tcp  open  shell        syn-ack ttl 64
666/tcp  open  doom         syn-ack ttl 64
3306/tcp open  mysql        syn-ack ttl 64
5901/tcp open  vnc-1        syn-ack ttl 64
6001/tcp open  X11:1        syn-ack ttl 64
8080/tcp open  http-proxy   syn-ack ttl 64
8443/tcp open  https-alt    syn-ack ttl 64
9080/tcp open  glrpc        syn-ack ttl 64
MAC Address: 08:00:27:36:B8:F3 (Oracle VirtualBox virtual NIC)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.096KB)
```

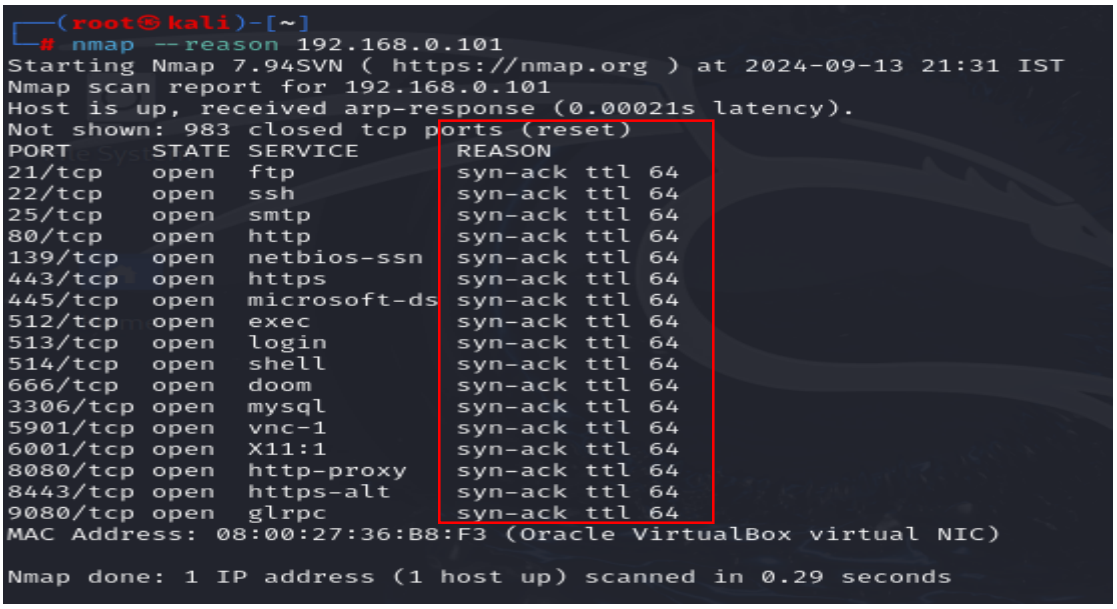
28.**-d (Debugging mode)**

- **Purpose**: Provides debug output to troubleshoot problems.
- **Usage**: nmap -d [target]
- **Real World Application**: For troubleshooting issues with your scans.
- **ExampleCommand:** nmap -d 192.168.0.101



29.**--reason (Display the reason for each host/port state)**

- **Purpose**: Shows why Nmap classified a port as open, closed, or filtered.
- **Usage**: nmap --reason [target]
- **Real World Application**: For understanding the exact reason behind port states.
- **ExampleCommand:** nmap --reason 192.168.0.101



30.**--open (Show only open ports)**

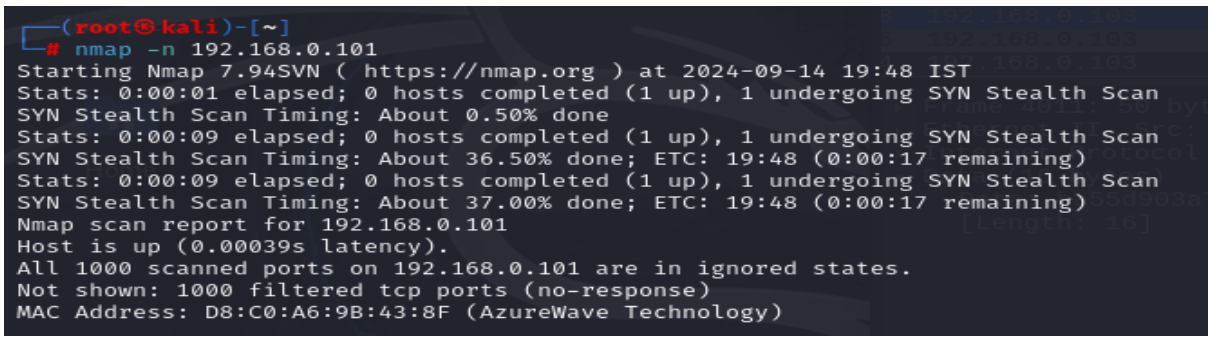
- **Purpose**: Only displays ports that are open.
- **Usage**: nmap --open [target]
- **Real World Application**: To see only open ports and ignore closed or filtered ones.
- **ExampleCommand:** nmap --open 192.168.0.101

31.**-6 (Enable IPv6 scanning)**

- **Purpose**: Scans using IPv6 instead of IPv4.
- **Usage**: nmap -6 [target]
- **Real World Application**: For scanning networks using IPv6 addresses.
- **ExampleCommand:** nmap -6 192.168.0.101

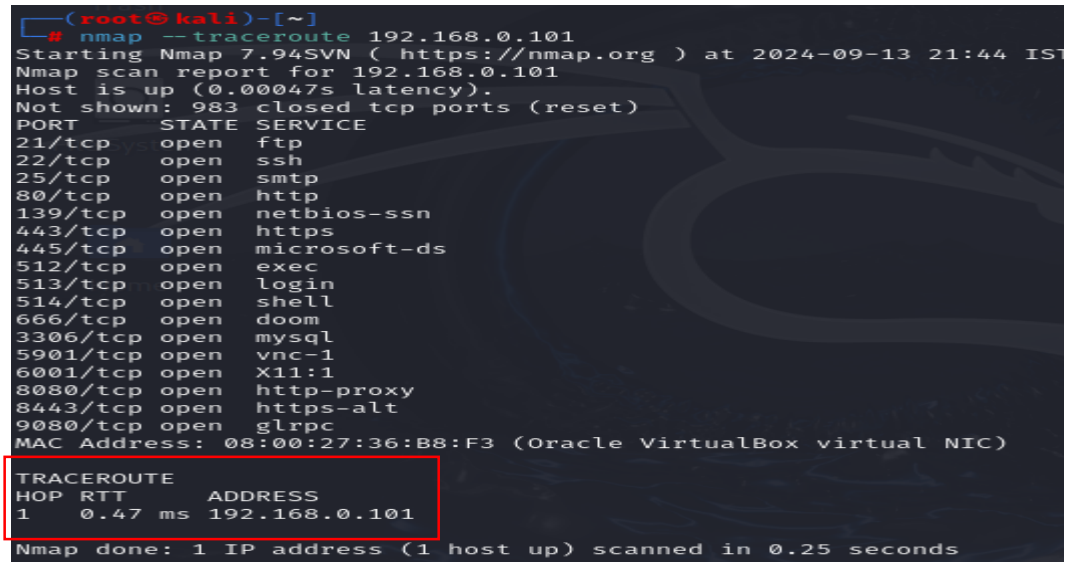
32.**-n (Disable DNS resolution)**

- **Purpose**: Skips resolving IP addresses to domain names.
- **Usage**: nmap -n [target]
- **Real World Application**: Use this when you don’t need DNS resolution to save time.
- **ExampleCommand:** nmap -n 192.168.0.101



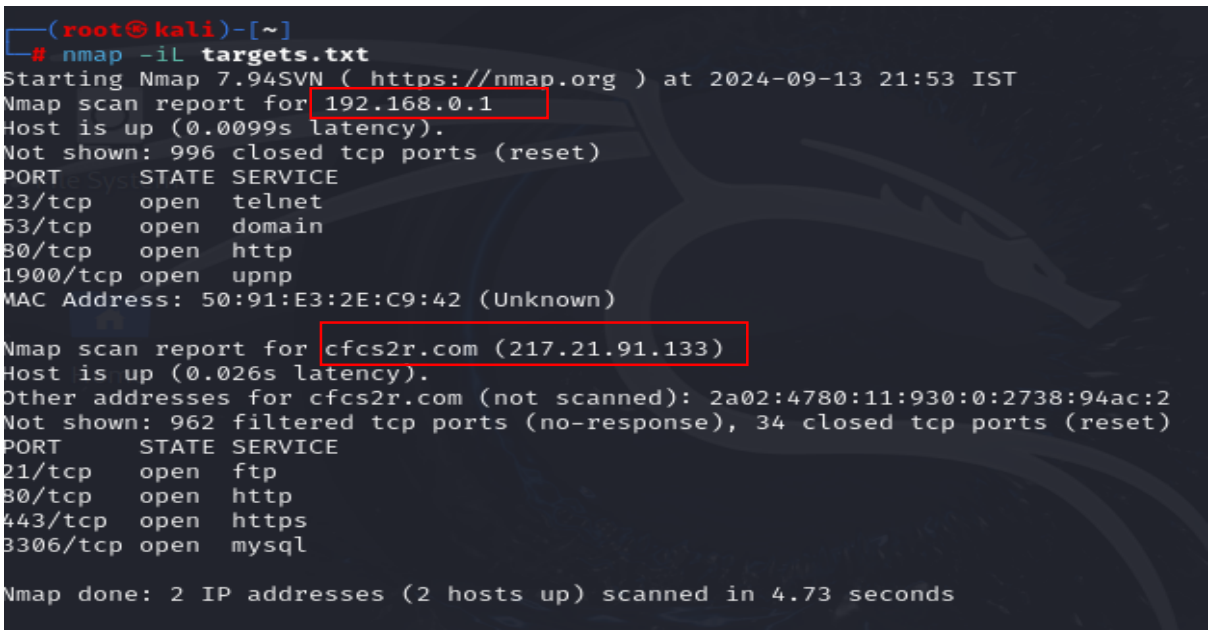
33.**--traceroute (Traceroute to discovered hosts)**

- **Purpose**: Shows the route packets take to reach the target.
- **Usage**: nmap --traceroute [target]
- **Real World Application**: To map the network path to a host.
- **ExampleCommand:** nmap --traceroute 192.168.0.101



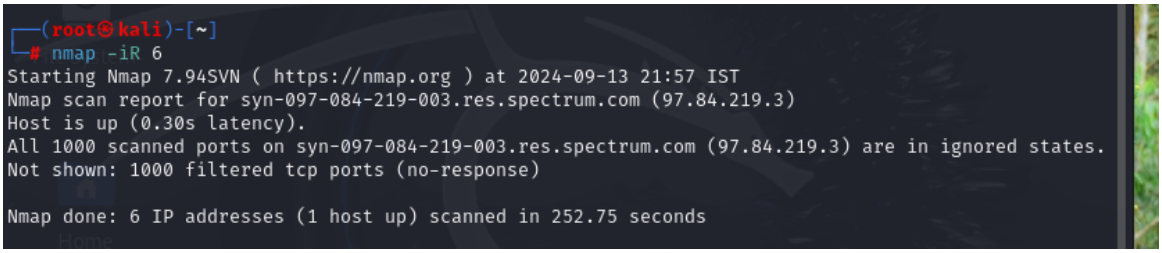
34.**-iL (Input from a file)**

- **Purpose**: Reads a list of targets from a file.
- **Usage**: nmap -iL [filename]
- **Real World Application**: Useful when scanning multiple targets from a file.
- **ExampleCommand:** nmap -iL targets.txt



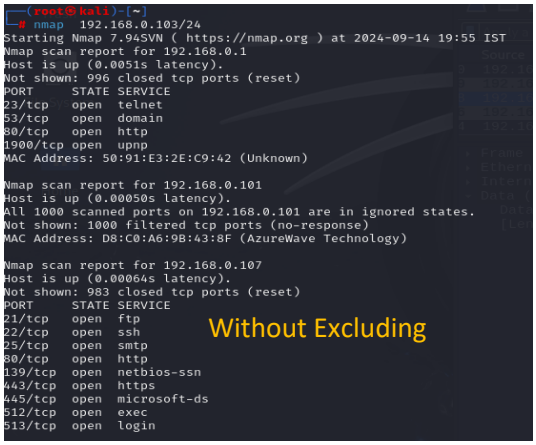
35.**-iR (Random targets)**

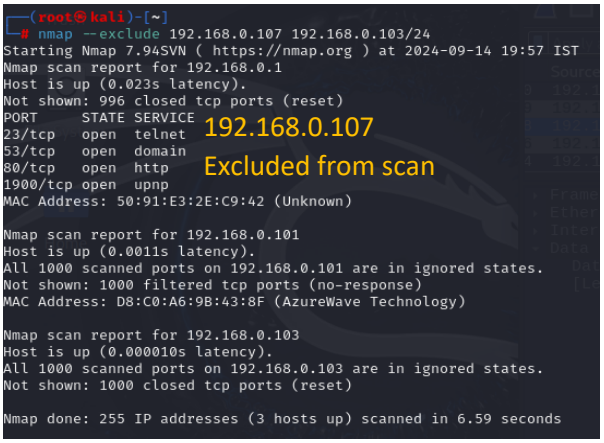
- **Purpose**: Scans random targets across the internet.
- **Usage**: nmap -iR [number]
- **Real World Application**: For testing or experimenting by scanning random hosts.
- **ExampleCommand:** nmap -iR 6



36.**-exclude (Exclude hosts/networks)**

- **Purpose**: Excludes specific IPs or networks from the scan.
- **Usage**: nmap --exclude [target]
- **Real World Application**: To avoid scanning certain hosts you don't want to include.
- **ExampleCommand:** nmap --exclude 192.168.0.107 192.168.0.103/24



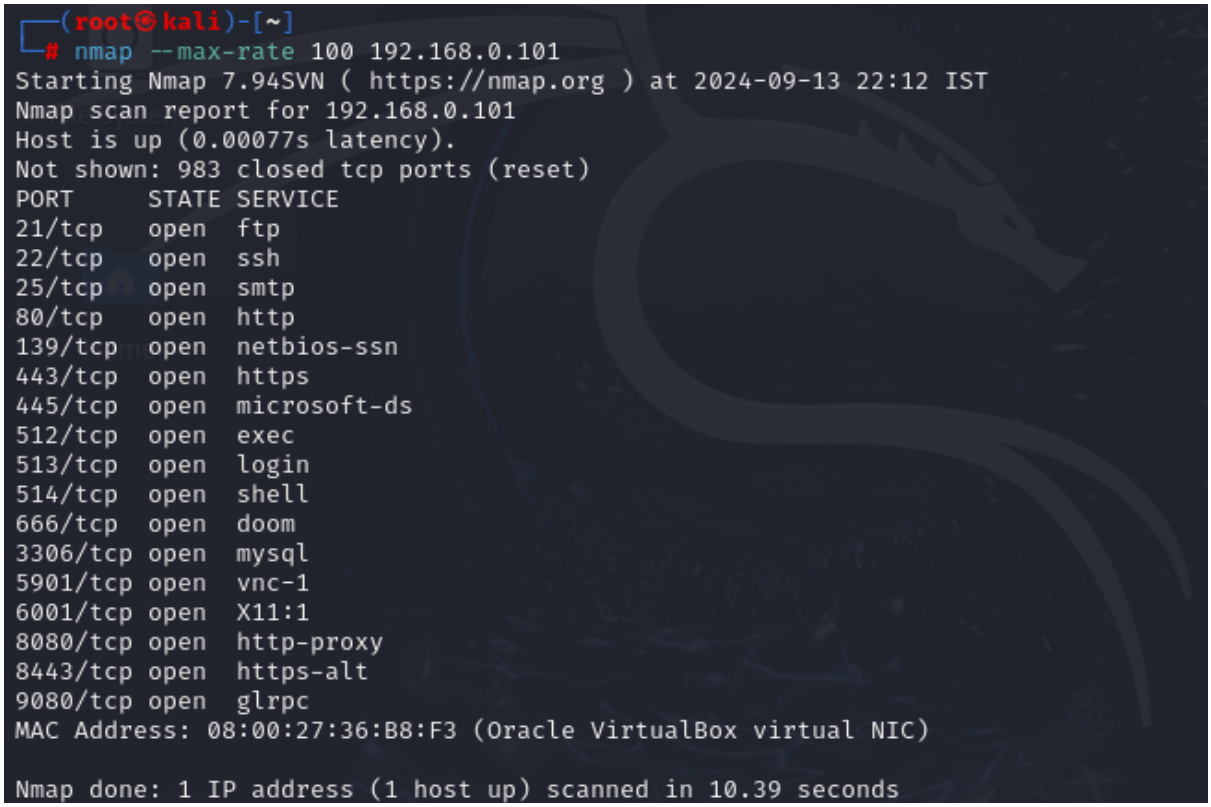


37.**-r (Scan ports consecutively)**

- **Purpose**: Scans ports in order instead of randomly.
- **Usage**: nmap -r [target]
- **Real World Application**: When you want to scan ports in a specific order.
- **ExampleCommand:** nmap -r 192.168.0.101

38.**-max-rate (Set maximum scan rate)**

- **Purpose**: Limits the number of packets sent per second to control the speed of the scan.
- **Usage**: nmap --max-rate [rate] [target]
- **Real World Application**: To control the speed of the scan, especially to avoid overloading the network.
- **ExampleCommand:** nmap --max-rate 100 192.168.0.101



Analysis Of Findings

In this task, we used over 30 different Nmap options to explore how they help scan and gather information about a network. Here's a simple breakdown of what was learned:

✸ Stealthy Scans vs. Regular Scans

- The **SYN Scan (-sS)** is faster and quieter compared to the **Connect Scan (-sT)**. The SYN scan doesn’t fully connect to a port, so it's harder for the target to detect, making it good for staying under the radar.
- The **Connect Scan (-sT)** is easier to notice by firewalls, but it’s useful when you don’t have special permissions to perform more advanced scans. It’s simple but less hidden.

✸ UDP Scanning

- The **UDP Scan (-sU)** is slower than TCP scans because it doesn’t use a handshake like TCP. It's useful for finding services that run over UDP, like DNS or SNMP, but can take more time and may miss some results due to how UDP works.

✸ Finding Service Versions

- The **Service Version Detection (-sV)** option helps find the exact version of software running on open ports. This is important to see if any services are outdated or vulnerable. It gives you more details, which helps identify security risks.

✸ Vulnerability Scan

- By using **--script vuln**, Nmap automatically runs scripts designed to find vulnerabilities in open services on the target. This can identify known vulnerabilities, weak configurations, or misconfigurations in real-time.
- Running the vuln script is essential for security assessments, as it provides detailed reports on known weaknesses, helping prioritize patches and fixes.
- Using the **--script** option with Nmap scripts adds even more information, like detecting vulnerabilities or misconfigurations, making the scan more thorough.

✸ Verbose Scan (-v)

- The **Verbose Scan (-v)** option increases the amount of information displayed during the scan. It provides real-time feedback on what Nmap is doing.
- Using verbose mode is helpful when you want to see the progress of the scan, especially during longer scans. It gives more visibility into the scan process, such as which hosts and ports are being scanned.

✸ Traceroute (--traceroute)

- The **Traceroute** option shows the path that packets take to reach the target. It helps map the network and understand how devices are connected.
- Traceroute provides valuable insight into the network layout, especially when trying to identify intermediate devices like routers or firewalls. This helps in mapping the network structure and understanding the route traffic takes.

✸ Fast Scanning

- Using **Fast Scan (-F)** scans fewer ports, so it's quicker but might miss some open ports. It's useful when you need quick results but don't require a detailed scan of every port

✸ Customizing Output

- With options like **-oN** for normal output or **-oX** for XML output, the scan results can be saved in different formats. This makes it easier to share or analyze the results later, depending on what you need.

✸ Hiding Your Identity

- The **Decoy Scan (-D)** helped mask the true IP address by making it look like the scan was coming from multiple fake addresses. This is useful when you want to make it harder for the target to know who is really scanning them.

✸ Controlling Scan Speed

- The **Max Rate (--max-rate)** option allowed us to slow down the scan by limiting how many packets are sent per second. This is useful to avoid overwhelming the network or getting noticed too easily.

Conclusion

This report looked at over 30 different Nmap options to see how they help in scanning and securing networks. Each option has a specific use, whether it's for scanning quietly or finding detailed information about services.

Options like SYN Scan (-sS) were great for fast and hidden scans, while UDP Scan (-sU) helped find services that don't use the usual TCP protocol. The Service Version Detection (-sV) option gave detailed information about the software running on the network, which is important for spotting vulnerabilities.

We also explored the --script vuln option, which automatically detects known security issues, making it an essential tool for finding weaknesses in a network. Using Verbose Mode (-v) gave us real-time updates during scans, and Traceroute (--traceroute) helped map out how data travels through the network.

Overall, Nmap's various options make it a powerful tool for network scanning, vulnerability detection, and improving network security. Understanding how to use these options effectively can help prevent security threats and keep networks safe.

THANK YOU

Report by:

SriRam Leburi

Contact: 8978715891

Linkedin: www.linkedin.com/in/sriram-leburi-840085215

Date: 15/09/2024