Nmap for Everyone

Journey from Nmap Beginner to Professional

v1.0

Contributor Authors

Rohit Pol 

Aniket Kadam 

Sarika Patil 

Mentor and Reviewer

Kuldeep Sonar 

June, 2024

Description

This is a free to use, free to share, free to redistribute guide. Feel free to modify, use, change, market, this guide for your professional and/or academics, do whatever you want with it as long as you give the appropriate credit where credit is due, which means giving the contributor authors the credit they deserve for writing it. Don’t forget to give credit(s) to Contributor Authors.

What We Expect from You

Nothing Big :D

We are happy to hear word of appreciations/encouragement from user(s) of this guide. Feel free to connect and follow us on LinkedIn® for any feedback(s), comment(s), suggestion(s), review(s).

Fair Use Notice

The material on this guide is provided for educational, teaching and informational purposes. The material on this guide is distributed without profit to those who have an interest in using the included information for research and educational purposes. use copyrighted material from this guide for purposes of your own that go beyond 'fair use', you must obtain permission from the copyright owner. The information on this guide does not constitute legal or technical advice.

Disclaimer

This guide is *only* for testing purposes and can only be used where strict consent has been given. Do not use this for illegal purposes.

This guide and used tools Kali Linux/Nmap/Metasploitable 1 are distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE

Please Read Carefully Before Using This Guide

Usage of Kali Linux and Nmap and Metasploitable 1 for attacking targets without prior mutual consent is illegal. It is the end user's responsibility to obey all applicable local, state and federal laws. Creators and/or reviewer of this Guide assume no liability and are not responsible for any misuse or damage caused by these program(s) and/or guide. We used here intentionally vulnerable target(s), within controlled lab environment and limited to specified scope to develop this guide only.

You are using this guide which means

You

Carefully Referred, Understood and Accepted

Following on Page Number 2 and 3

Description | Fair Use Notice | Disclaimer | Please Read Carefully Before Using This Guide

Index

Background

We created this guide keeping in mind that power of Nmap require to utilize from beginner to professional level. We tried our best to keep this guide as much as in simple and lucid way to understand who willing to start career journey in cyber security to who already using Nmap in professional environment. No matters you are not pro at Linux OS, we are sure you able to use Nmap by referring this guide smoothly.

To create this guide, we used hypervisor two based lab scenario, in VMware Player where two guest operating systems installed and configured. Attacker machine Kali Linux having IP address 192.168.29.32 and Target is intentionally vulnerable machine Metasploitable 1 having IP address 192.168.29.185, both machines connected via NAT.

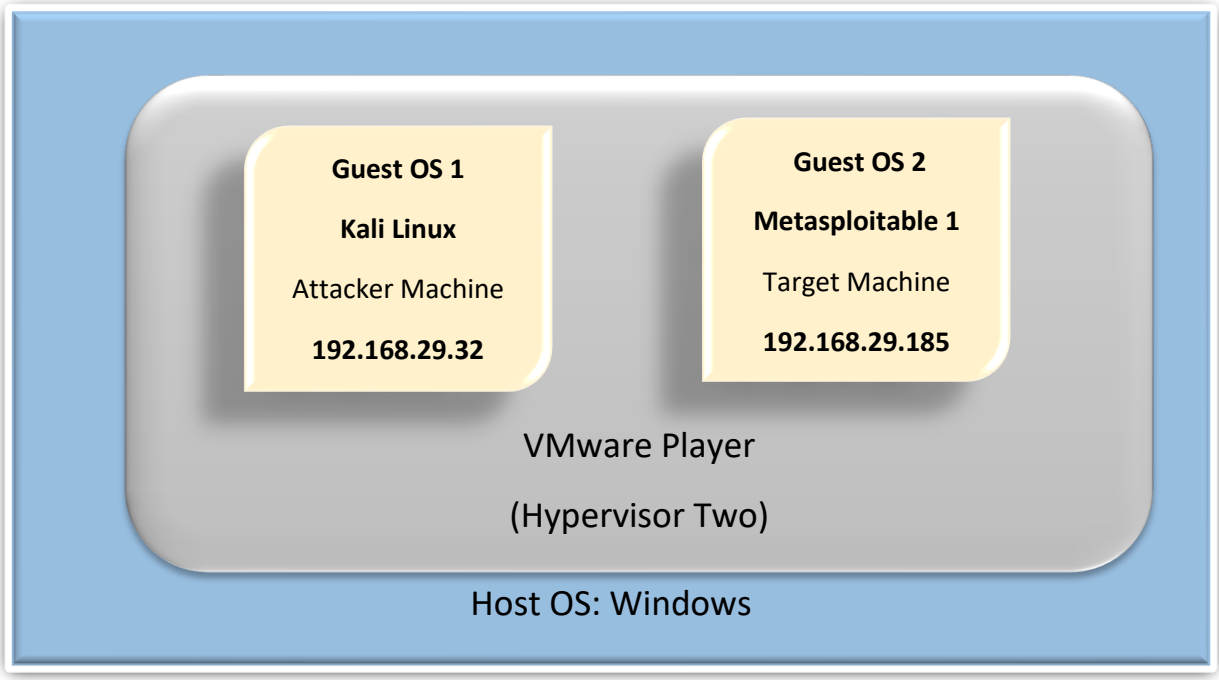


Image 1: Lab Scenario

While referring this guide replace your Virtual machines address respectively for Kali Linux and Metasploitable 1. Concept remains same even in case any other hypervisor two application used for example VirtualBox and/or Hyper-V any other Intentionally Target machine is used example from Vuln-Hub platform.

This guide is not any specific to any host platform, not matters even if you might use Windows or Linux or MAC. You just require to take care of

Hypervisor two application which is compatible with yours respective Host OS platform.

Accessing Nmap in Kali Linux

Nmap command line version available in Kali Linux, accessed by various ways

1. From Kali Linux Application Path

Kali Linux Original (Offensive) and Kali Linux Purple (Defensive)

a. Click on Dragon Icon at yours Lefthand Upper Corner → 01 – Information Gathering → nmap

Image 2: Accessing Nmap via Application

b. Click on Dragon Icon at yours Lefthand Upper Corner → 01 – Information Gathering → Network & Port Scanners → nmap

Image 3: Accessing Nmap via Application subcategory Network & Port Scanner

c. Click on Dragon Icon at yours Lefthand Upper Corner → 02 – Vulnerability Analysis → nmap

Image 4: Accessing Nmap via Application subcategory Vulnerability Analysis

d. Click on Dragon Icon at yours Lefthand Upper Corner → In Search Bar → Type nmap → click on nmap

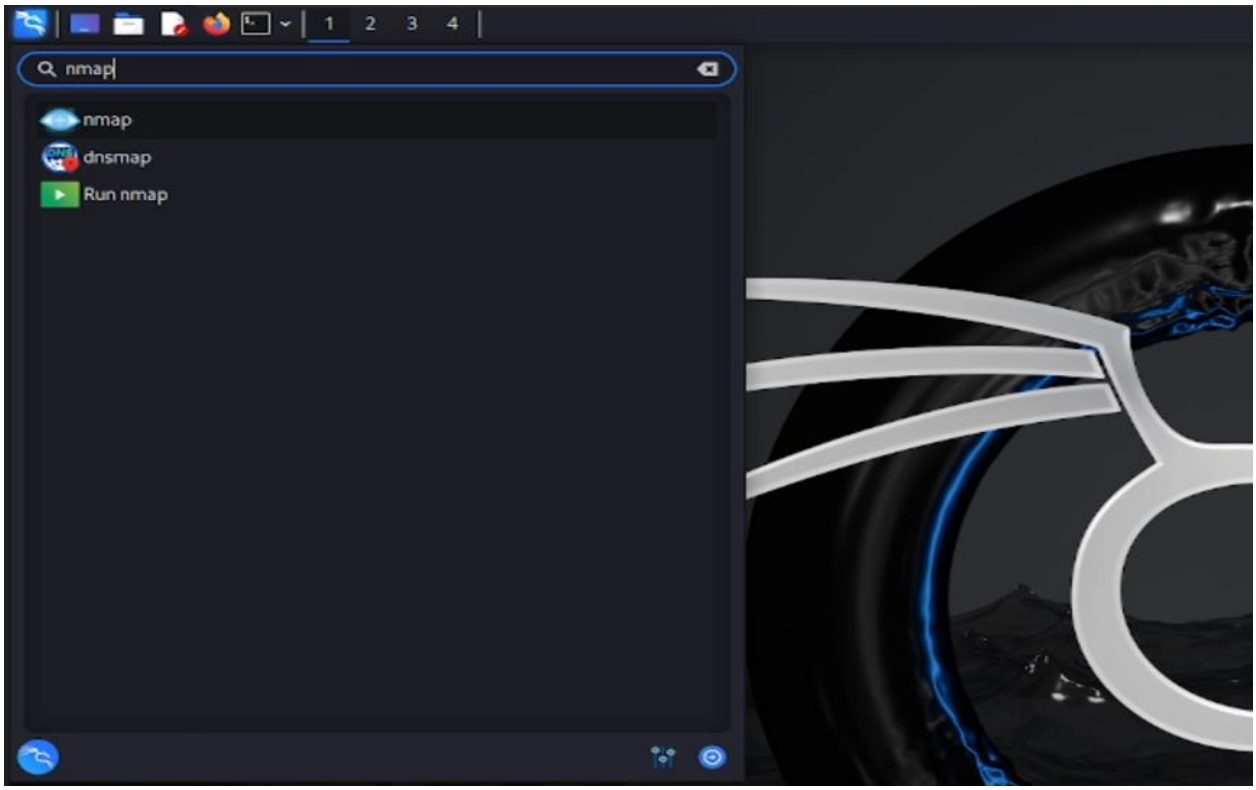


Image 5: Accessing Nmap via Application Search Bar

2. From Kali Linux Terminal

Click on Title Bar of Kali Linux → hover mouse pointer to small back box icon → it will show message banner as a Terminal Emulator → click on same icon to launch Terminal

Image 6: Accessing Terminal from Title Bar

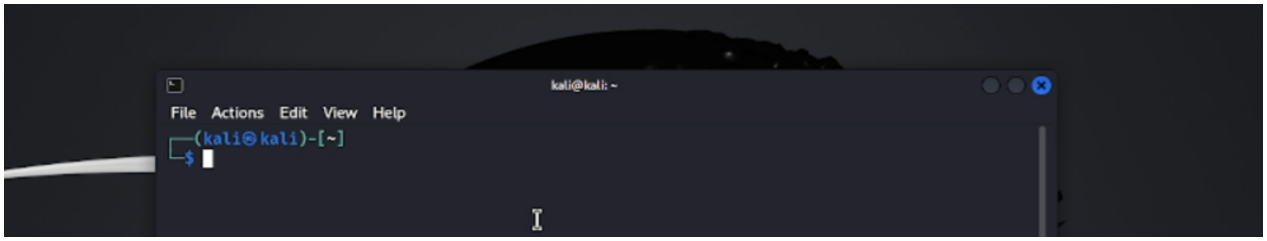


Image 7: Interface of Terminal with Standard Access Level

Normally Nmap accesses via standard user in Kali Linux

Example: *nmap -h*

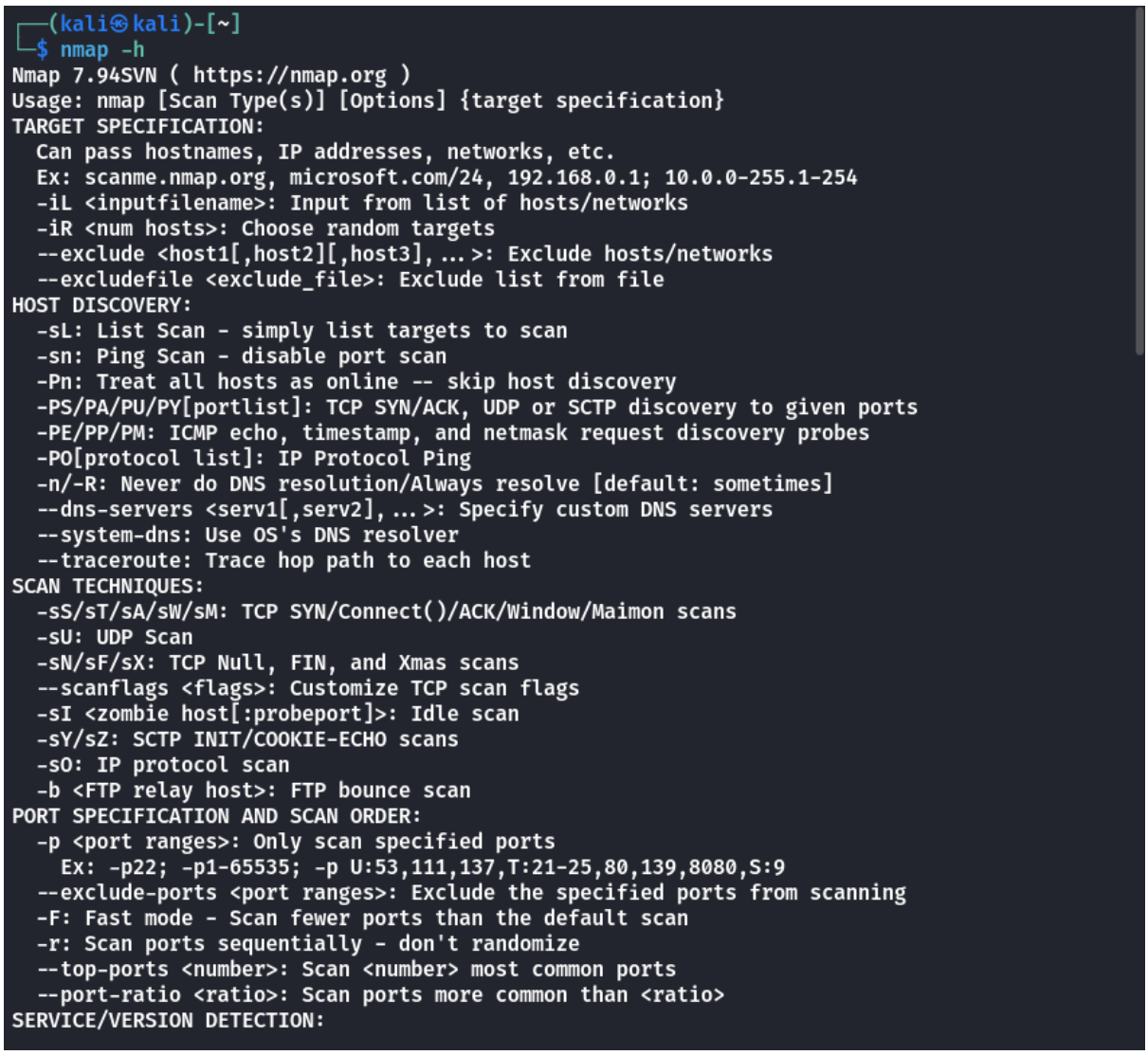


Image 8: Accessing Nmap with Standard User Access and without Sudo

If any specific option requires root access that can be achieved through sudo command

Example: *sudo nmap -O <Target IP>*

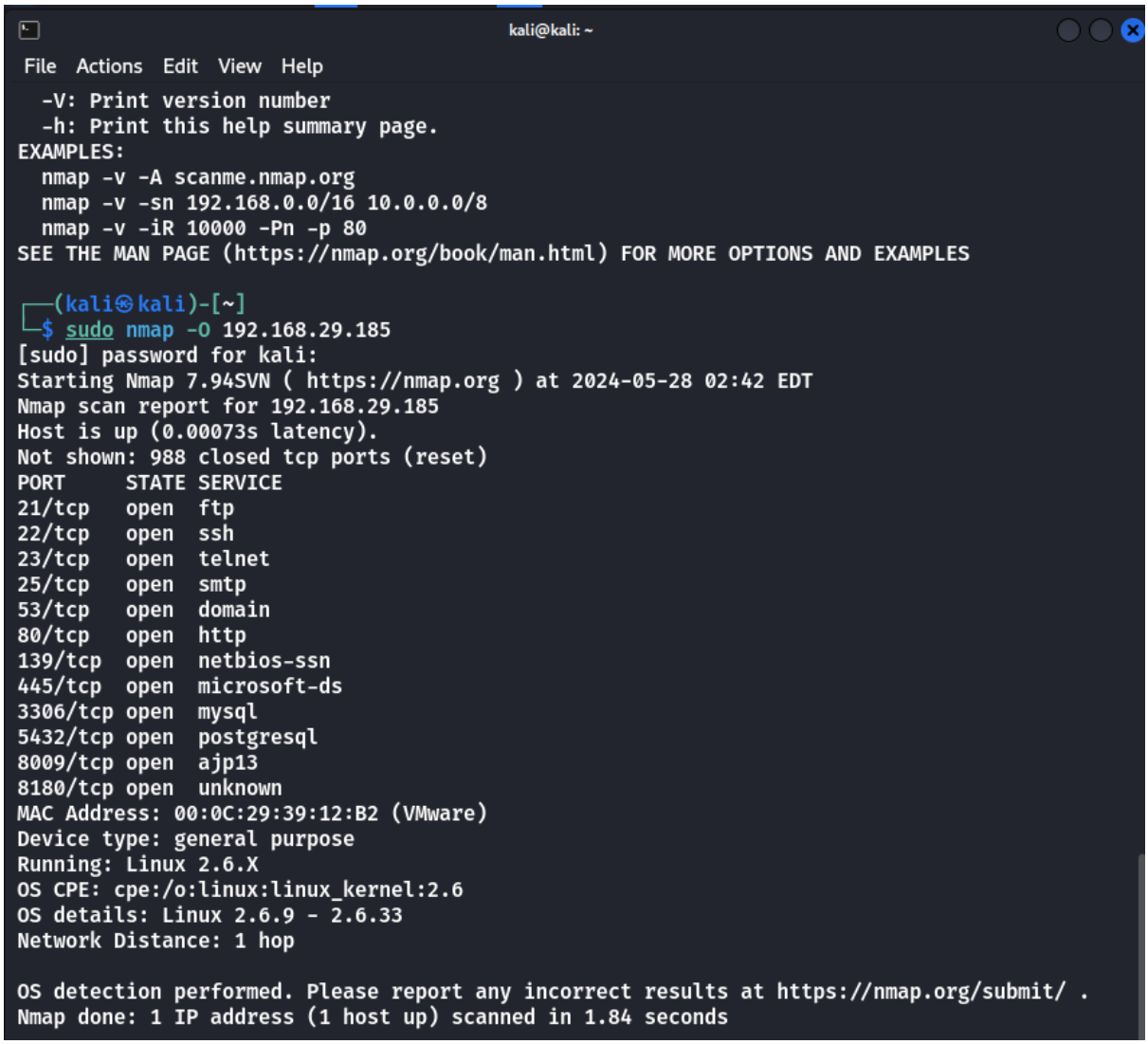


Image 9: Accessing Nmap with Sudo Access (Root Access Privilege)

In this guide we preferred root access through *sudo su* command to avoid use of *sudo* command every time while using nmap.

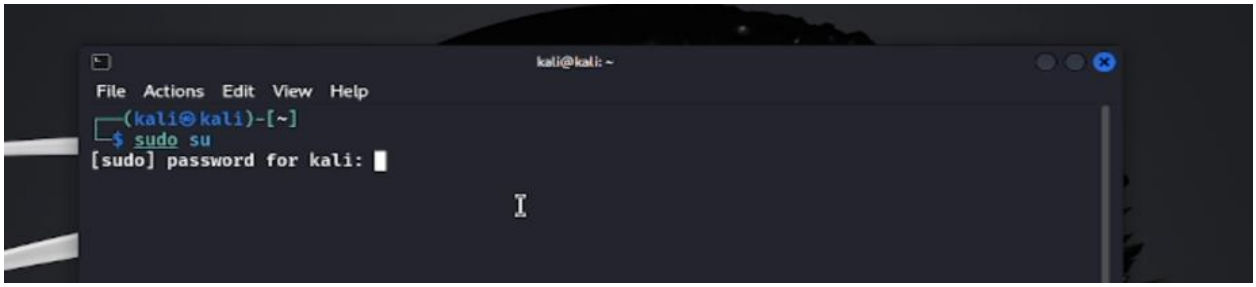


Image 10: Accessing Root access level

Image 11: Switch to Root User

Although it's not a recommended way to access nmap always as it might make harm to Linux OS if something accidently entered by user, specifically by users those are new to Linux OS. It's always recommended to use *sudo* command always even it seems lengthier repetitive way.

Tools Used

	Tool Name	Download URL
1	**VMware Player**	https://www.vmware.com/products/workstation-player/workstation-player-evaluation.html.html
2	**Kali Linux**	https://cdimage.kali.org/kali-2024.1/kali-linux-2024.1-installer-amd64.iso
3	**Metasploitable**	https://www.vulnhub.com/entry/metasploitable-1,28/
4	**Nmap**	https://nmap.org/download.html

1. Basic Scanning Techniques

1.1. nmap -v <target IP>

- **Command Breakdown**

Syntax	nmap	-v	<target IP>
Example	nmap	-v	192.168.29.185
Detail	Initiates Nmap	Enables Verbose Mode	Targets IP Address

Table 1: Nmap Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-v:** The verbose flag is this. By increasing the output's verbosity, it gives more thorough information about the scanning procedure. Nmap will show you more information about each step it takes, including scan details and progress, when you use the -v option.
- **192.168.29.185:** Nmap is going to scan this IP address. Targeted in this instance is the device that has IP address 192.168.29.185.

➢ **Output Image**

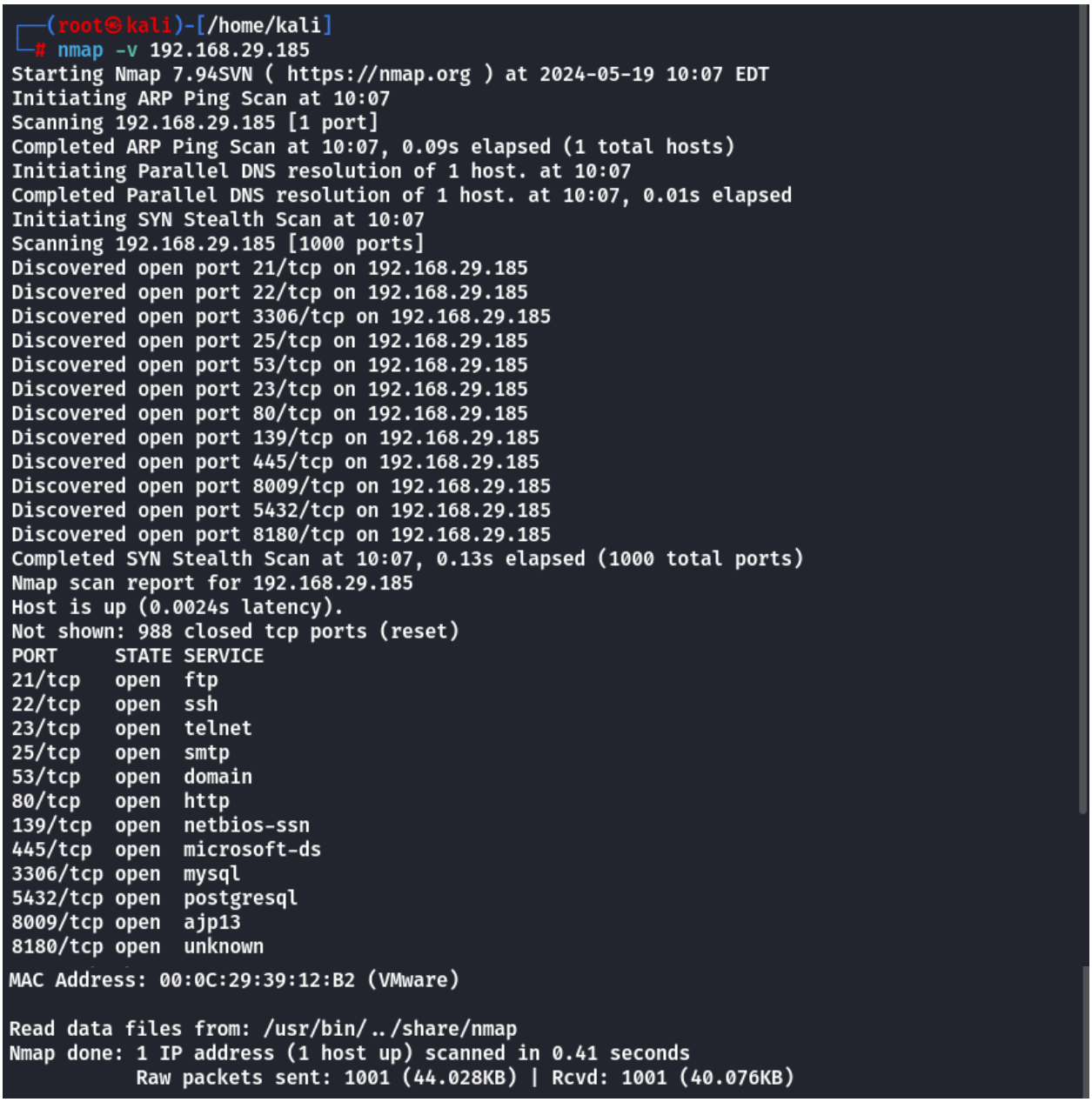


Image 12: Nmap Verbose Scanning

➢ **Steps Performed by the Command**

- **ARP Ping Scan (on local networks):**
  - Nmap queries the host's uptime via ARP requests.
  - Because ARP is faster and more dependable, it is utilized for local network scans.
- **DNS Resolution:**
  - Nmap attempts, if appropriate, to resolve the target IP address's hostname.

- **Port Scanning:**
  - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
  - Unless otherwise noted, the default scan examines the 1000 most frequently used ports.
- **Service Detection:**
  - Nmap looks for open ports and tries to identify the services that are using them.
- **OS Detection and Version Detection (if applicable):**
  - Nmap has the ability to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

1.2. nmap -sS -v <target IP>

- **Command Breakdown**

Syntax	nmap	-sS	-v	<target IP>
Example	nmap	-sS	-v	192.168.29.185
Detail	Initiates Nmap	TCP SYN Scan	Enables Verbose Mode	Targets IP Address

Table 2: Nmap TCP SYN and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-sS:** This flag describes how to perform a TCP SYN scan. Nmap sends SYN packets to the target ports during a SYN scan, sometimes referred to as a "half-open" scan, and then examines the responses to ascertain whether the ports are open, closed, or filtered. Because it does not finish the TCP handshake, it is more covert than other scan types.
- **-v:** The verbose flag is this. By increasing the output's verbosity, it gives more thorough information about the scanning procedure. When Nmap is used, it will show more information about its actions at each stage, such as scan details and progress.
- **192.168.29.185:** The intended IP address is this one. In order to learn more about open ports and the services that are using them, Nmap will scan this IP address.

➢ **Output Image**

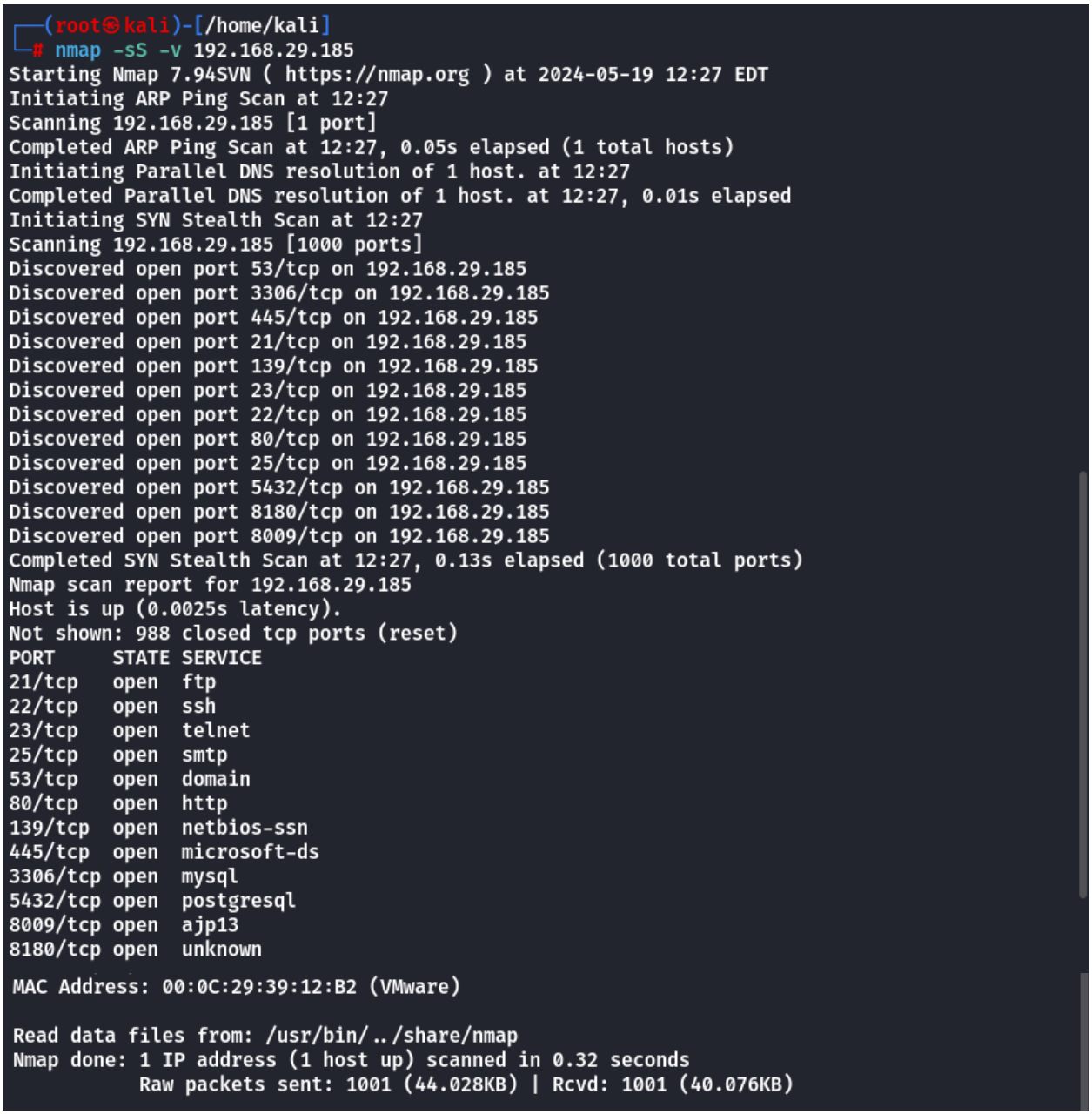


Image 13: Nmap TCP SYN and Verbose Scanning

➢ **Steps Performed by the Command**

- **ARP Ping Scan (on local networks):**
  - Nmap queries the host's uptime via ARP requests.
  - Because ARP is faster and more dependable, it is utilized for local network scans.
- **DNS Resolution:**
  - Nmap attempts to resolve the target IP address's hostname, if applicable.
- **Port Scanning(-sS):**

- On the given IP address, Nmap runs a TCP SYN scan. To find out whether the ports are open, closed, or filtered, it sends SYN packets to each port and watches for a response.
- The TCP SYN scan method is specified by the -sS flag. Nmap uses this kind of scan to find out if the target ports are open, closed, or filtered by sending SYN packets to them and examining the responses. Because it doesn't finish the TCP handshake, the scan is covert and more difficult to identify.

- **Service Detection:**
  - Nmap makes an effort to determine which services are utilizing the open ports it finds.
- **OS Detection and Version Detection (if applicable):**
  - Although it isn't enabled by default in this command, Nmap can also try to identify the target's operating system and service versions.

1.3. nmap -sT -v <target IP>

- **Command Breakdown**

Syntax	nmap	-sT	-v	<target IP>
Example	nmap	-sT	-v	192.168.29.185
Detail	Initiates Nmap	TCP Connect Scan	Enables Verbose Mode	Targets IP Address

Table 3: Nmap TCP Connect and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-sT:** This flag describes how to do a TCP connect scan. Nmap tries to finish the TCP three-way handshake with the target ports during a TCP connect scan. While not as covert as a SYN scan, this kind of scan is accurate and dependable.
- **-v:** The verbose flag is this. By increasing the output's verbosity, it gives more thorough information about the scanning procedure. When Nmap is used, it will show more information about its actions at each stage, such as scan details and progress.
- **192.168.29.185:** The target IP address is this. This IP address will be scanned by Nmap to learn more about open ports and the services that are using them.

➢ **Output Image**

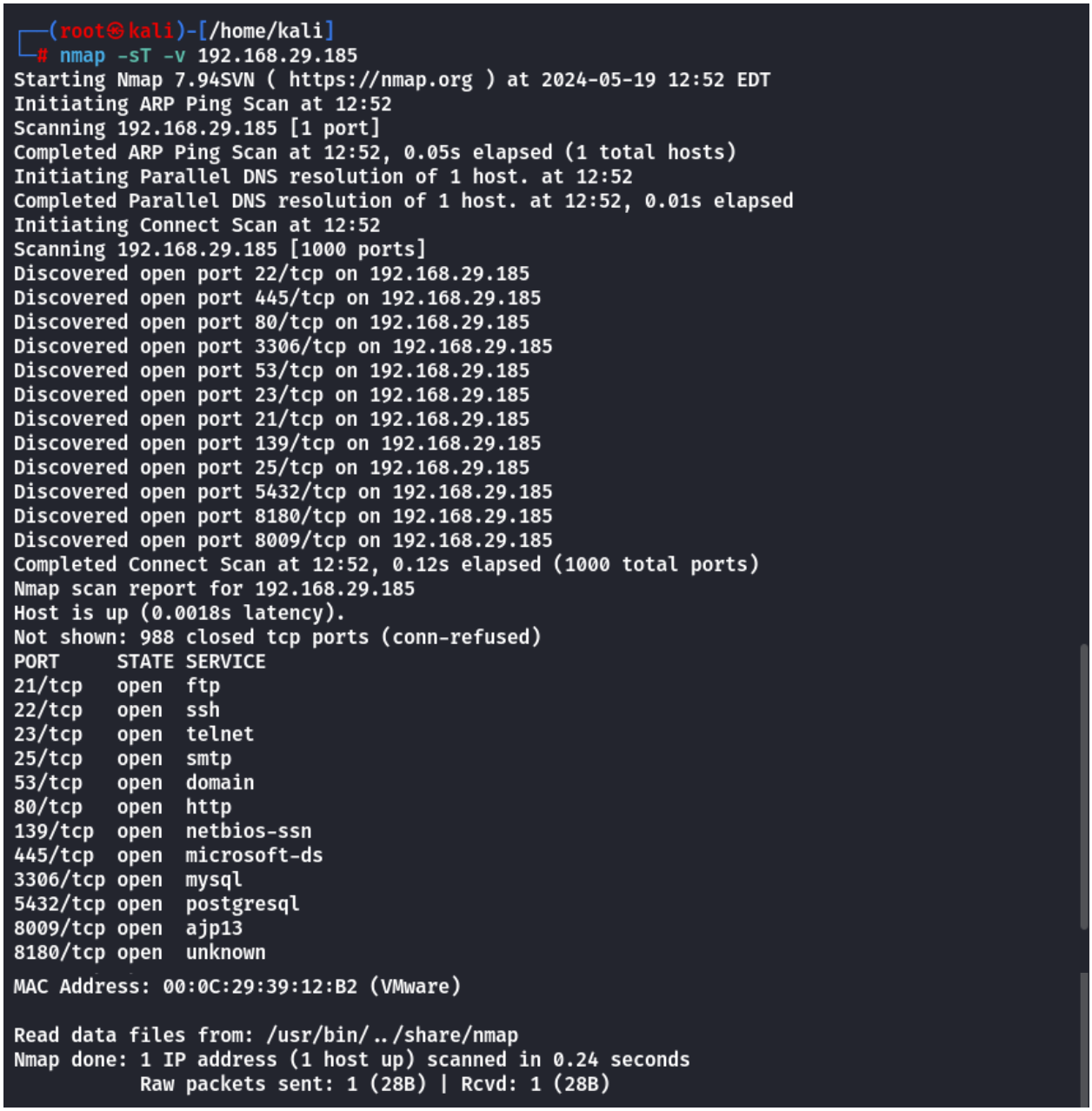


Image 14: Nmap TCP Connect and Verbose Scanning

➢ **Steps Performed by the Command**

- **ARP Ping Scan (on local networks):**
  - To find out whether the host is up, Nmap sends ARP requests.
  - Due to its increased speed and reliability, ARP is utilized for local network scans.
- **DNS Resolution:**

- If the target IP address has a hostname, Nmap attempts to resolve it.

- **Port Scanning(-sT):**
  - Nmap connects to the given IP address and runs a TCP connect scan. It makes an effort to finish the TCP three-way handshake with every port in order to ascertain whether it is filtered, closed, or open.
  - The TCP connect scan method is indicated by the -sT flag. Nmap tries to finish the TCP three-way handshake with the target ports during this kind of scan. Compared to SYN scans, this method is more dependable but less covert.
- **Service Detection:**
  - Nmap looks for open ports and tries to identify the services that are using them.
- **OS Detection and Version Detection (if applicable):**
  - While not enabled by default in this command, Nmap can also attempt to detect the operating system and versions of services running on the target.

1.4. nmap -sU -v <target IP>

- **Command Breakdown**

Syntax	nmap	-sU	-v	<target IP>
Example	nmap	-sU	-v	192.168.29.185
Detail	Initiates Nmap	UDP Scan	Enables Verbose Mode	Targets the Address

Table 4: Nmap UDP and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-sU:** This flag describes how to use the UDP scan method. Nmap uses a UDP scan to find out if target ports are open, closed, or filtered by sending UDP packets to them and examining the responses. UDP scans are frequently employed to identify services that might not reply to TCP queries.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Nmap provides further information about its actions at each stage, including scan details and progress, when it is used.
- **192.168.29.185:** The target IP address is this. This IP address will be scanned by Nmap in order to collect data about open UDP ports and the services that are using them.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sU -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 18:32 EDT
Initiating ARP Ping Scan at 18:32
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 18:32, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:32
Completed Parallel DNS resolution of 1 host. at 18:32, 0.01s elapsed
Initiating UDP Scan at 18:32
Scanning 192.168.29.185 [1000 ports]
Increasing send delay for 192.168.29.185 from 0 to 50 due to max_successful_tryno increase
to 4
Increasing send delay for 192.168.29.185 from 50 to 100 due to 11 out of 12 dropped probes
since last increase.
Increasing send delay for 192.168.29.185 from 100 to 200 due to 11 out of 11 dropped probes
 since last increase.
UDP Scan Timing: About 9.28% done; ETC: 18:38 (0:05:03 remaining)
Increasing send delay for 192.168.29.185 from 200 to 400 due to 11 out of 11 dropped probes
 since last increase.
Increasing send delay for 192.168.29.185 from 400 to 800 due to 11 out of 11 dropped probes
 since last increase.
UDP Scan Timing: About 13.00% done; ETC: 18:40 (0:06:48 remaining)
UDP Scan Timing: About 15.82% done; ETC: 18:42 (0:08:04 remaining)
UDP Scan Timing: About 18.75% done; ETC: 18:43 (0:08:44 remaining)
UDP Scan Timing: About 22.95% done; ETC: 18:44 (0:09:17 remaining)
UDP Scan Timing: About 38.68% done; ETC: 18:47 (0:08:40 remaining)
UDP Scan Timing: About 45.58% done; ETC: 18:47 (0:07:58 remaining)
Discovered open port 53/udp on 192.168.29.185
UDP Scan Timing: About 51.50% done; ETC: 18:47 (0:07:13 remaining)
UDP Scan Timing: About 57.25% done; ETC: 18:48 (0:06:28 remaining)
Stats: 0:09:36 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 62.47% done; ETC: 18:48 (0:05:46 remaining)
UDP Scan Timing: About 68.02% done; ETC: 18:48 (0:04:58 remaining)
Discovered open port 137/udp on 192.168.29.185
UDP Scan Timing: About 73.23% done; ETC: 18:48 (0:04:11 remaining)
UDP Scan Timing: About 78.67% done; ETC: 18:48 (0:03:22 remaining)
UDP Scan Timing: About 83.88% done; ETC: 18:48 (0:02:33 remaining)
UDP Scan Timing: About 89.02% done; ETC: 18:48 (0:01:45 remaining)
UDP Scan Timing: About 94.07% done; ETC: 18:48 (0:00:57 remaining)
```

```
Completed UDP Scan at 18:50, 1025.56s elapsed (1000 total ports)
Nmap scan report for 192.168.29.185
Host is up (0.0012s latency).
Not shown: 953 closed udp ports (port-unreach)
PORT      STATE         SERVICE
53/udp    open          domain
68/udp    open|filtered dhcpc
88/udp    open|filtered kerberos-sec
137/udp   open          netbios-ns
138/udp   open|filtered netbios-dgm
199/udp   open|filtered smux
207/udp   open|filtered at-7
445/udp   open|filtered microsoft-ds
500/udp   open|filtered isakmp
513/udp   open|filtered who
776/udp   open|filtered wpages
789/udp   open|filtered unknown
903/udp   open|filtered ideafarm-panic
1043/udp  open|filtered boinc
1045/udp  open|filtered fpitp
2160/udp  open|filtered apc-2160
2223/udp  open|filtered rockwell-csp2
5355/udp  open|filtered llmnr
16086/udp open|filtered unknown
17417/udp open|filtered unknown
17533/udp open|filtered unknown
17629/udp open|filtered unknown
17888/udp open|filtered unknown
17989/udp open|filtered unknown
19096/udp open|filtered unknown
19717/udp open|filtered unknown
20465/udp open|filtered unknown
21803/udp open|filtered unknown
28465/udp open|filtered unknown
31059/udp open|filtered unknown
32528/udp open|filtered unknown
32777/udp open|filtered sometimes-rpc18
33355/udp open|filtered unknown
34358/udp open|filtered unknown
36489/udp open|filtered unknown
40708/udp open|filtered unknown
42056/udp open|filtered unknown
42577/udp open|filtered unknown
45928/udp open|filtered unknown
49162/udp open|filtered unknown
49174/udp open|filtered unknown
49259/udp open|filtered unknown
50497/udp open|filtered unknown
57813/udp open|filtered unknown
57958/udp open|filtered unknown
58797/udp open|filtered unknown
64513/udp open|filtered unknown
MAC Address: 00:0C:29:39:12:B2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1025.73 seconds
           Raw packets sent: 1745 (82.972KB) | Rcvd: 1046 (76.328KB)
```

Image 15: Nmap UDP and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - If appropriate, Nmap attempts to resolve the target IP address's hostname.
  - **Port Scanning (-sU):**
    - Nmap scans the specified IP address using UDP. In order to ascertain whether the ports are open, closed, or filtered, it sends UDP packets to each port and examines the responses.
    - The UDP scan method is specified by the -sU flag. Nmap uses this kind of scan to find out if the target ports are open, closed, or filtered by sending UDP packets to them and examining the responses. This kind of scan can be helpful in identifying services that might not reply to TCP queries.
  - **Service Detection:**
    - Nmap looks for open UDP ports and tries to identify the services that are using them.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

1.5. nmap -sA -v <target IP>

- **Command Breakdown**

Syntax	nmap	-sA	-v	<target IP>
Example	nmap	-sA	-v	192.168.29.185
Detail	Initiates Nmap	ACK Scan	Enables Verbose Mode	Targets IP Address

Table 5: Nmap TCP Acknowledgement and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-sA:** This flag describes how to do an ACK scan. Finding out which ports are filtered and whether a host is firewall protected are the main uses of an ACK scan.
- **-v:** The verbose flag is this. By increasing the output's verbosity, it gives more thorough information about the scanning procedure. When Nmap is used, it will show more information about its actions at each stage, such as scan details and progress.
- **192.168.29.185:** This IP address is intended for use. To learn more about the ports current status in respect to firewall regulations, Nmap will scan this IP address.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sA -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 19:58 EDT
Initiating ARP Ping Scan at 19:58
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 19:58, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:58
Completed Parallel DNS resolution of 1 host. at 19:58, 0.00s elapsed
Initiating ACK Scan at 19:58
Scanning 192.168.29.185 [1000 ports]
Completed ACK Scan at 19:58, 0.14s elapsed (1000 total ports)
Nmap scan report for 192.168.29.185
Host is up (0.0014s latency).
All 1000 scanned ports on 192.168.29.185 are in ignored states.
Not shown: 1000 unfiltered tcp ports (reset)
MAC Address: 00:0C:29:39:12:B2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.29 seconds
           Raw packets sent: 1001 (40.028KB) | Rcvd: 1001 (40.028KB)
```

Image 16: Nmap TCP Acknowledgement and Verbose Scanning

➢ **Steps Performed by the Command**

- **ARP Ping Scan (on local networks):**
  - Find out whether the host is up, Nmap sends ARP requests.
  - Due to its increased speed and reliability, ARP is utilized for local network scans.
- **DNS Resolution:**
  - Nmap attempts to resolve the target IP address's hostname, if applicable.
- **Port Scanning (-sA):**
  - Nmap scans the specified IP address for ACKs. In order to ascertain whether the ports are filtered (by a firewall) or unfiltered, it sends TCP ACK packets to each port and examines the responses.
  - The ACK scan method is specified by the -sA flag. This scan is intended to map out firewall rule sets, ascertain whether a host is firewall-protected, and if so, identify the filtered ports. In order to accomplish this, it sends TCP ACK packets to the intended ports and examines the replies.
- **Service Detection:**
  - As establishing firewall rules is the main goal rather than service detection, this step is skipped in an ACK scan.

- **OS Detection and Version Detection (if applicable):**
  - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

1.6. nmap -sN -v <target IP>

- **Command Breakdown**

Syntax	nmap	-sN	-v	<target IP>
Example	nmap	-sN	-v	192.168.29.185
Detail	Initiates Nmap	TCP Null Scan	Enables Verbose Mode	Targets IP Address

Table 6: Nmap TCP Null and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-sN:** This flag describes how to perform a TCP Null scan. Sending packets with no flags set is how a null scan operates, and it's helpful for determining open ports by looking for the lack of a response rather than its presence.
- **-v:** The verbose flag is this. By increasing the output's verbosity, it gives more thorough information about the scanning procedure. When Nmap is used, it will show more information about its actions at each stage, such as scan details and progress.
- **192.168.29.185:** This IP address is intended for use. To find out what open ports are and what services are using them, Nmap will scan this IP address.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sN -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-19 21:09 EDT
Initiating ARP Ping Scan at 21:09
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 21:09, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 21:09
Completed Parallel DNS resolution of 1 host. at 21:09, 0.01s elapsed
Initiating NULL Scan at 21:09
Scanning 192.168.29.185 [1000 ports]
Completed NULL Scan at 21:09, 1.36s elapsed (1000 total ports)
Nmap scan report for 192.168.29.185
Host is up (0.0026s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 00:0C:29:39:12:B2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.54 seconds
           Raw packets sent: 1013 (40.508KB) | Rcvd: 989 (39.548KB)
```

Image 17: Nmap TCP Null and Verbose Scanning

➢ **Steps Performed by the Command**

- **ARP Ping Scan (on local networks):**
  - To find out whether the host is up, Nmap sends ARP requests.
  - Due to its increased speed and reliability, ARP is utilized for local network scans.
- **DNS Resolution:**
  - Nmap attempts to resolve the target IP address's hostname, if applicable.
- **Port Scanning (-sN):**
  - Nmap scans the specified IP address for null values. In order to ascertain whether the ports are open, closed, or filtered, it sends TCP packets to each port without any flags set and examines the replies.

- The TCP Null scan method is specified by the -sN flag. Certain firewalls and packet filters can be circumvented by sending TCP packets with no flags set, as this scan does. The response (or lack thereof) helps assess how the ports are doing:
    - If no response is received, the port is considered open or filtered.
    - If an RST (reset) packet is received, the port is considered closed.

- **Service Detection:**
    - Although this is not the main purpose of a Null scan, Nmap makes an effort to identify the services that are operating on the open ports that it finds.
- **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

1.7. nmap -sF -v <target IP>

- **Command Breakdown**

Syntax	nmap	-sF	-v	<target IP>
Example	nmap	-sF	-v	192.168.29.185
Detail	Initiates Nmap	TCP FIN Scan	Enables Verbose Mode	Targets IP Address

Table 7: Nmap TCP Finish and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-sF:** This flag describes how to perform a TCP FIN scan. Sending TCP packets with the FIN flag set allows FIN scans to get past some firewalls and packet filters.
- -**v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Nmap provides further information about its actions at each stage, including scan details and progress, when it is used.
- **192.168.29.185:** This IP address is intended for use. To find out what open ports are and what services are using them, Nmap will scan this IP address.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sF -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 03:32 EDT
Initiating ARP Ping Scan at 03:32
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 03:32, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 03:32
Completed Parallel DNS resolution of 1 host. at 03:32, 0.01s elapsed
Initiating FIN Scan at 03:32
Scanning 192.168.29.185 [1000 ports]
Completed FIN Scan at 03:32, 1.23s elapsed (1000 total ports)
Nmap scan report for 192.168.29.185
Host is up (0.0025s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
53/tcp   open|filtered domain
80/tcp   open|filtered http
139/tcp  open|filtered netbios-ssn
445/tcp  open|filtered microsoft-ds
3306/tcp open|filtered mysql
5432/tcp open|filtered postgresql
8009/tcp open|filtered ajp13
8180/tcp open|filtered unknown
MAC Address: 00:0C:29:39:12:B2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.38 seconds
           Raw packets sent: 1013 (40.508KB) | Rcvd: 989 (39.548KB)
```

Image 18: Nmap TCP Finish and Verbose Scanning

➢ **Steps Performed by the Command**

- **ARP Ping Scan (on local networks):**
  - To find out whether the host is up, Nmap sends ARP requests.
  - Due to its increased speed and reliability, ARP is utilized for local network scans.
- **DNS Resolution:**
  - If the target IP address has a hostname, Nmap attempts to resolve it.
- **Port Scanning (-sF):**
  - Nmap scans the IP address provided with a FIN query. To find out if a port is open, closed, or filtered, it sends TCP packets to each port with the FIN flag set and examines the replies.

- The TCP FIN scan method is specified by the -sF flag. Only the FIN flag is set in the TCP packets sent to each port during this scan. The response (or lack thereof) helps assess how the ports are doing:
    - It is assumed that the port is open or filtered if no response is received.
    - The port is closed in the event that an RST (reset) packet is received.

- **Service Detection:**
    - While this is not the main purpose of a FIN scan, Nmap makes an effort to identify the services that are operating on the open ports that it finds.
- **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

1.8. nmap -sX -v <target IP>

- **Command Breakdown**

Syntax	nmap	-sX	-v	<target IP>
Example	nmap	-sX	-v	192.168.29.185
Detail	Initiates Nmap	TCP Xmas Scan	Enables Verbose Mode	TargetsIP Address

Table 8: Nmap Xmas and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-sX:** The TCP Xmas scan method is specified by this flag. By examining the responses, an Xmas scan can be used to determine open ports since it sends TCP packets with the FIN, PSH, and URG flags set.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Nmap provides further information about its actions at each stage, including scan details and progress, when it is used.
- **192.168.29.185:** The IP address that is being targeted is this one. This IP address will be scanned by Nmap in order to obtain information about open ports and the services that are using them.

- **Output Image**

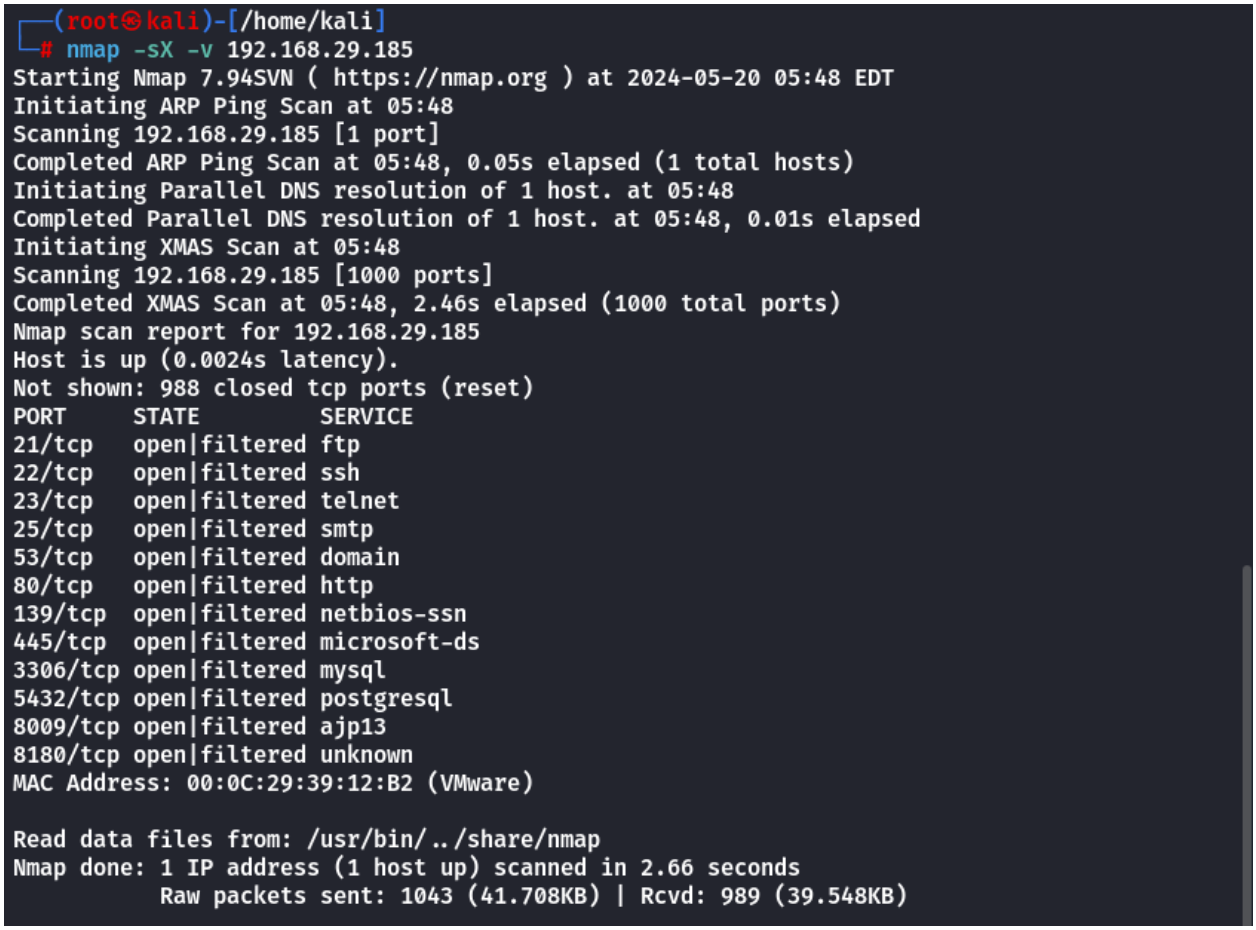


Image 19: Nmap Xmas and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning (-sX):**
    - Nmap scans the specified IP address for Christmas. In order to ascertain whether the ports are open, closed, or filtered,

it sends TCP packets to each port with the FIN, PSH, and URG flags set. Then, it examines the responses to the packets.

- The TCP Xmas scan method is specified by the -sX flag. TCP packets with the FIN, PSH, and URG flags set are sent during this scan. The answer—or lack thereof—helps assess how the ports are doing:
  - It is assumed that the port is open or filtered if no response is received.
  - The port is closed in the event that an RST (reset) packet is received.

- **Service Detection:**
  - Although this is not the main purpose of an Xmas scan, Nmap makes an effort to identify the services that are operating on the open ports it finds.
- **OS Detection and Version Detection (if applicable):**
  - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

1.9. nmap -sP -v <target IP>

- **Command Breakdown**

Syntax	nmap	-sP	-v	<target IP>
Example	nmap	-sP	-v	192.168.29.185
Detail	Initiates Nmap	Ping Scan	Enables Verbose Mode	Targets IP Address

Table 9: Nmap Ping and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-sP:** A ping scan is indicated by this flag. Instead of performing a thorough port scan or service detection, a ping scan is used to see if hosts are up and responding.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Nmap provides further information about its actions at each stage, including scan details and progress, when it is used.
- **192.168.29.185:** The target IP address is this. This IP address will be scanned by Nmap to see if the host is up and running.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sP -v 192.168.29.185
Warning: The -sP option is deprecated. Please use -sn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 06:29 EDT
Initiating ARP Ping Scan at 06:29
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 06:29, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 06:29
Completed Parallel DNS resolution of 1 host. at 06:29, 0.01s elapsed
Nmap scan report for 192.168.29.185
Host is up (0.00036s latency).
MAC Address: 00:0C:29:39:12:B2 (VMware)
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
           Raw packets sent: 1 (28B) | Rcvd: 1 (28B)
```

Image 20: Nmap Ping and Verbose Scanning

➢ **Steps Performed by the Command**

- **ARP Ping Scan (on local networks):**
  - To find out whether the host is up, Nmap sends ARP requests.
  - Due to its increased speed and reliability, ARP is utilized for local network scans.
- **DNS Resolution:**
  - Nmap attempts to resolve the target IP address's hostname, if applicable.
- **Ping Scan(-sP):**
  - Nmap pings the target IP address using ICMP echo request packets.
  - Nmap can send TCP SYN packets to ports 443 and 80 to see if any responses are received if ICMP is blocked.
- **Report Host Status:**
  - Nmap uses the responses it receives to determine whether the host is up or down.

1.10. nmap -sO -v <target IP>

- **Command Breakdown**

Syntax	nmap	-sO	-v	<target IP>
Example	nmap	-sO	-v	192.168.29.185
Detail	Initiates Nmap	IP Protocol Scan	Enables Verbose Mode	Targets IP Address

Table 10: Nmap Protocol and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-sO:** The IP protocol scan is indicated by this flag. This kind of scan ascertains which IP protocols the target host supports (ICMP, TCP, UDP, etc.).
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Nmap provides further information about its actions at each stage, including scan details and progress, when it is used.
- **192.168.29.185:** The IP address that is being targeted is this one. This IP address will be scanned by Nmap to see which IP protocols are supported.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sO -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 07:08 EDT
Initiating ARP Ping Scan at 07:08
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 07:08, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:08
Completed Parallel DNS resolution of 1 host. at 07:08, 0.00s elapsed
Initiating IPProto Scan at 07:08
Scanning 192.168.29.185 [256 ports]
Increasing send delay for 192.168.29.185 from 0 to 5 due to max_successful_tryno increase t
o 4
Increasing send delay for 192.168.29.185 from 5 to 10 due to max_successful_tryno increase
to 5
Increasing send delay for 192.168.29.185 from 10 to 20 due to 11 out of 13 dropped probes s
ince last increase.
Increasing send delay for 192.168.29.185 from 20 to 40 due to 11 out of 11 dropped probes s
ince last increase.
Discovered open port 6/ip on 192.168.29.185
Increasing send delay for 192.168.29.185 from 40 to 80 due to 11 out of 13 dropped probes s
ince last increase.
Increasing send delay for 192.168.29.185 from 80 to 160 due to 11 out of 11 dropped probes
since last increase.
Discovered open port 1/ip on 192.168.29.185
Increasing send delay for 192.168.29.185 from 160 to 320 due to max_successful_tryno increa
se to 6
Increasing send delay for 192.168.29.185 from 320 to 640 due to max_successful_tryno increa
se to 7
Increasing send delay for 192.168.29.185 from 640 to 1000 due to max_successful_tryno incre
ase to 8
Discovered open port 17/ip on 192.168.29.185
Completed IPProto Scan at 07:12, 264.45s elapsed (256 total ports)
Nmap scan report for 192.168.29.185
Host is up (0.00063s latency).
Not shown: 251 closed n/a protocols (proto-unreach)
PROTOCOL STATE         SERVICE
1        open          icmp
2        open|filtered igmp
6        open          tcp
17       open          udp
136      open|filtered udplite
MAC Address: 00:0C:29:39:12:B2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 264.57 seconds
           Raw packets sent: 1358 (27.404KB) | Rcvd: 260 (12.472KB)
```

Image 21: Nmap Protocol and Verbose Scanning

➢ **Steps Performed by the Command**

- **ARP Ping Scan (on local networks):**
  - To find out whether the host is up, Nmap sends ARP requests.
  - Due to its increased speed and reliability, ARP is utilized for local network scans.

- **DNS Resolution:**
  - If the target IP address has a hostname, Nmap attempts to resolve it.
- **IP Protocol Scan(-sO):**
  - Nmap sends packets to the target for every IP protocol (range from 0 to 255).
  - Based on the responses (or lack thereof) it gets from the target host, it decides which protocols are supported. This covers various protocols, including TCP (6), UDP (17), and ICMP (1).
- **Report Protocol Support:**
  - Nmap uses the scan results to report which IP protocols the target host supports.

2. Service and OS Detection

2.1. nmap -sV -v <target IP>

- **Command Breakdown**

Syntax	nmap	-sV	-v	<target IP>
Example	nmap	-sV	-v	192.168.29.185
Detail	Initiates Nmap	Version Detection	Enables Verbose Mode	Targets IP Address

Table 11: Nmap TCP Version Detection and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-sV:** Enables version detection with this flag. Nmap will attempt to ascertain the service version that is operating on open ports.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Nmap provides further information about its actions at each stage, including scan details and progress, when it is used.
- **192.168.29.185:** The target IP address is this. This IP address will be scanned by Nmap to obtain details about open ports and the services (and versions) that are operating on them.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 07:46 EDT
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 07:46
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 07:46, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:46
Completed Parallel DNS resolution of 1 host. at 07:46, 0.01s elapsed
Initiating SYN Stealth Scan at 07:46
Scanning 192.168.29.185 [1000 ports]
Discovered open port 53/tcp on 192.168.29.185
Discovered open port 23/tcp on 192.168.29.185
Discovered open port 80/tcp on 192.168.29.185
Discovered open port 21/tcp on 192.168.29.185
Discovered open port 25/tcp on 192.168.29.185
Discovered open port 139/tcp on 192.168.29.185
Discovered open port 22/tcp on 192.168.29.185
Discovered open port 445/tcp on 192.168.29.185
Discovered open port 3306/tcp on 192.168.29.185
Discovered open port 5432/tcp on 192.168.29.185
Discovered open port 8009/tcp on 192.168.29.185
Discovered open port 8180/tcp on 192.168.29.185
Completed SYN Stealth Scan at 07:46, 0.14s elapsed (1000 total ports)
Initiating Service scan at 07:46
Scanning 12 services on 192.168.29.185
Completed Service scan at 07:47, 11.31s elapsed (12 services on 1 host)
NSE: Script scanning 192.168.29.185.
Initiating NSE at 07:47
Completed NSE at 07:47, 0.07s elapsed
Initiating NSE at 07:47
Completed NSE at 07:47, 0.01s elapsed
Nmap scan report for 192.168.29.185
Host is up (0.0012s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd

25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-
Patch)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:39:12:B2 (VMware)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
kernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit
/ .
Nmap done: 1 IP address (1 host up) scanned in 12.29 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.076KB)
```

Image 22: Nmap TCP Version Detection and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - If the target IP address has a hostname, Nmap attempts to resolve it.
  - **Port Scanning:**
    - To find open ports on the target IP address, Nmap runs a scan. Unless otherwise instructed, it runs a SYN scan by default.
  - **Version Detection(-sV):**
    - To find out which service versions are operating on the open ports, Nmap sends particular probes to them and examines the answers.
    - To determine service versions, it makes use of a large database of probes and anticipated responses.

2.2. nmap -O -v <target IP>

- **Command Breakdown**

Syntax	nmap	-O	-v	<target IP>
Example	nmap	-O	-v	192.168.29.185
Detail	Initiates Nmap	OS Detection	Enables Verbose Mode	Targets IP Address

Table 12: Nmap Operating System Detection and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-O:** OS detection is enabled by this flag. Nmap will make an effort to identify the target host's operating system.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Nmap provides further information about its actions at each stage, including scan details and progress, when it is used.
- **192.168.29.185:** The IP address that is being targeted is this one. This IP address will be scanned by Nmap to learn about open ports, services, and the host's operating system.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -O -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 09:15 EDT
Initiating ARP Ping Scan at 09:15
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 09:15, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:15
Completed Parallel DNS resolution of 1 host. at 09:15, 0.01s elapsed
Initiating SYN Stealth Scan at 09:15
Scanning 192.168.29.185 [1000 ports]
Discovered open port 21/tcp on 192.168.29.185
Discovered open port 80/tcp on 192.168.29.185
Discovered open port 445/tcp on 192.168.29.185
Discovered open port 53/tcp on 192.168.29.185
Discovered open port 22/tcp on 192.168.29.185
Discovered open port 3306/tcp on 192.168.29.185
Discovered open port 23/tcp on 192.168.29.185
Discovered open port 25/tcp on 192.168.29.185
Discovered open port 139/tcp on 192.168.29.185
Discovered open port 8009/tcp on 192.168.29.185
Discovered open port 8180/tcp on 192.168.29.185
Discovered open port 5432/tcp on 192.168.29.185
Completed SYN Stealth Scan at 09:15, 0.13s elapsed (1000 total ports)
Initiating OS detection (try #1) against 192.168.29.185
Nmap scan report for 192.168.29.185
Host is up (0.0012s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:39:12:B2 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.273 days (since Mon May 20 02:43:05 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=204 (Good luck!)
IP ID Sequence Generation: All zeros

Read data files from: /usr/bin/../share/nmap
OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 1.75 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.386KB)
```

Image 23: Nmap Operating System Detection and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - Nmap scans the target IP address to find any open ports. Unless instructed otherwise, it runs a SYN scan by default.
  - **OS Detection:**
    - To find the operating system, Nmap sends the target a variety of probes and examines the answers
    - It matches the responses to a sizable database of recognized OS fingerprints in order to determine the OS.

2.3. nmap -A -v <target IP>

- **Command Breakdown**

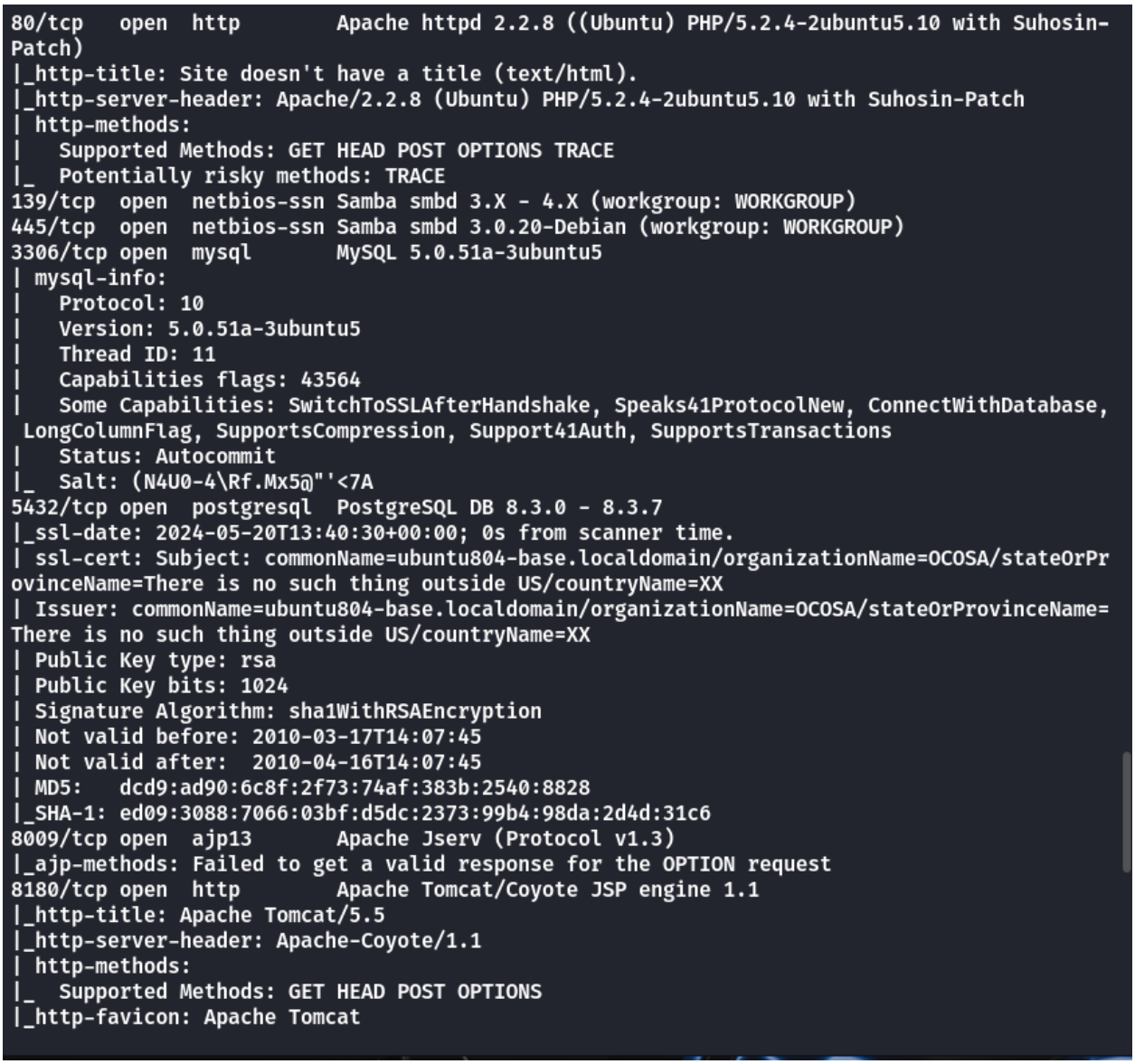
Syntax	nmap	-A	-v	<target IP>
Example	nmap	-A	-v	192.168.29.185
Detail	Initiates Nmap	Aggressive Scan	Enables Verbose Mode	Targets IP Address

Table 13: Nmap Aggressive and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-A:** Aggressive scanning can be enabled with this flag. In addition to OS detection, version detection, script scanning, and traceroute, it combines several other advanced scanning techniques.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Nmap provides further information about its actions at each stage, including scan details and progress, when it is used.
- **192.168.29.185:** The target IP address is this. This IP address will be scanned by Nmap to obtain detailed information about open ports, services that are using them, their versions, the host's operating system, and more.

➢ Output Image

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-20 09:40 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 09:40
Completed NSE at 09:40, 0.00s elapsed
Initiating NSE at 09:40
Completed NSE at 09:40, 0.00s elapsed
Initiating NSE at 09:40
Completed NSE at 09:40, 0.00s elapsed
Initiating ARP Ping Scan at 09:40
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 09:40, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:40
Completed Parallel DNS resolution of 1 host. at 09:40, 0.01s elapsed
Initiating SYN Stealth Scan at 09:40
Scanning 192.168.29.185 [1000 ports]
Discovered open port 23/tcp on 192.168.29.185
Discovered open port 53/tcp on 192.168.29.185
Discovered open port 25/tcp on 192.168.29.185
Discovered open port 139/tcp on 192.168.29.185
Discovered open port 22/tcp on 192.168.29.185
Discovered open port 80/tcp on 192.168.29.185
Discovered open port 21/tcp on 192.168.29.185
Discovered open port 445/tcp on 192.168.29.185
Discovered open port 3306/tcp on 192.168.29.185
Discovered open port 8009/tcp on 192.168.29.185
Discovered open port 5432/tcp on 192.168.29.185
Discovered open port 8180/tcp on 192.168.29.185
Completed SYN Stealth Scan at 09:40, 0.15s elapsed (1000 total ports)
Initiating Service scan at 09:40
Scanning 12 services on 192.168.29.185
Completed Service scan at 09:40, 11.05s elapsed (12 services on 1 host)
Initiating OS detection (try #1) against 192.168.29.185
NSE: Script scanning 192.168.29.185.
Initiating NSE at 09:40
Completed NSE at 09:40, 8.97s elapsed
Initiating NSE at 09:40
```


80/tcp open http Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch)
|_http-title: Site doesn't have a title (text/html).
|_http-server-header: Apache/2.2.8 (Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-Patch
| http-methods:
| Supported Methods: GET HEAD POST OPTIONS TRACE
|_ Potentially risky methods: TRACE
139/tcp open netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp open netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
3306/tcp open mysql MySQL 5.0.51a-3ubuntu5
| mysql-info:
| Protocol: 10
| Version: 5.0.51a-3ubuntu5
| Thread ID: 11
| Capabilities flags: 43564
| Some Capabilities: SwitchToSSLAfterHandshake, Speaks41ProtocolNew, ConnectWithDatabase, LongColumnFlag, SupportsCompression, Support41Auth, SupportsTransactions
| Status: Autocommit
|_ Salt: (N4U0-4\Rf.Mx5@"'<7A
5432/tcp open postgresql PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2024-05-20T13:40:30+00:00; 0s from scanner time.
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Issuer: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2010-03-17T14:07:45
| Not valid after: 2010-04-16T14:07:45
| MD5: dcd9:ad90:6c8f:2f73:74af:383b:2540:8828
|_SHA-1: ed09:3088:7066:03bf:d5dc:2373:99b4:98da:2d4d:31c6
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
|_http-title: Apache Tomcat/5.5
|_http-server-header: Apache-Coyote/1.1
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_http-favicon: Apache Tomcat

```
MAC Address: 00:0C:29:39:12:B2 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Uptime guess: 0.290 days (since Mon May 20 02:43:05 2024)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=201 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_
kernel

Host script results:
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2024-05-20T09:40:21-04:00
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 59m59s, deviation: 2h00m00s, median: 0s
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (un
known)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)

TRACEROUTE
HOP RTT     ADDRESS
1   0.79 ms 192.168.29.185

NSE: Script Post-scanning.
Initiating NSE at 09:40
Completed NSE at 09:40, 0.00s elapsed
Initiating NSE at 09:40
Completed NSE at 09:40, 0.00s elapsed
Initiating NSE at 09:40
Completed NSE at 09:40, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org
/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 22.40 seconds
           Raw packets sent: 1020 (45.626KB) | Rcvd: 1016 (41.386KB)
```

Image 24: Nmap Aggressive and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests. Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - By default, Nmap searches the target IP address for open ports using a SYN scan.
  - **Service Version Detection:**
    - To find out which service versions are operating on the open ports, Nmap sends particular probes to them and examines the answers.
  - **OS Detection:**
    - To find the operating system, Nmap sends the target a variety of probes and examines the answers. It compares the responses to a sizable database of recognized OS fingerprints in order to determine the OS.
  - **Script Scanning:**
    - Nmap collects additional information about vulnerabilities, configuration problems, and other topics by running NSE scripts against the target.
  - **Traceroute:**
    - Nmap locates intermediary devices and their IP addresses by following the network path to the destination.

3. Script Scanning

3.1. nmap --script <script> -v <target IP>

- **Command Breakdown**

Syntax	nmap	--script	<script>	-v	<target IP>
Example	nmap	--script	http-enum	-v	192.168.29.185
Detail	Initiates Nmap	script	HTTP Enumeration Script	Enables Verbose Mode	Targets IP Address

Table 14: Nmap NSE Script and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **--script http-enum:** The Nmap Scripting Engine (NSE) script to be used is specified by this option. The purpose of the http-enum script is to probe the target HTTP server and find frequently used directories and web applications.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Nmap provides further information about its actions at each stage, including scan details and progress, when it is used.
- **192.168.29.185:** The target IP address is this. This IP address will be scanned by Nmap to list all of the directories and web apps on the HTTP server that is operating on it.

➢ **Output Image**

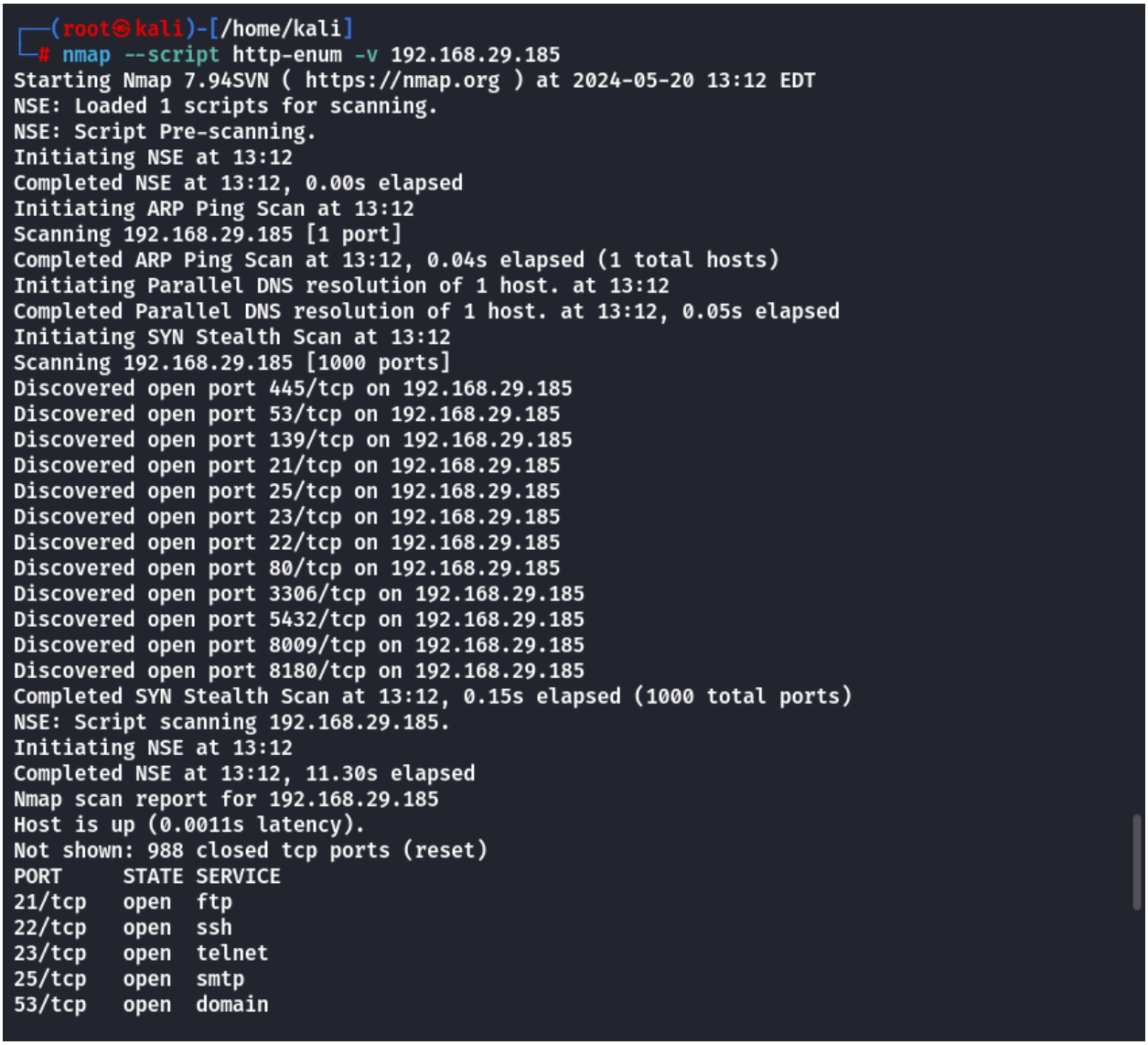


Image 25: Nmap NSE Script and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests. Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - By default, Nmap searches the target IP address for open ports using a SYN scan.
  - **HTTP Enumeration:**
    - Nmap lists popular web apps and directories on the HTTP server by using the http-enum script. In order to determine which directories and web applications are present, it sends HTTP requests to well-known paths and examines the answers.

3.2. nmap --script-help <script> -v

- **Command Breakdown**

Syntax	nmap	--script-help	<script>	-v
Example	nmap	--script-help	http-enum	-v
Detail	Initiates Nmap	Script Documentation Request	HTTP Enumeration Script	Enables Verbose Mode

Table 15: Nmap NSE Script Help

- **nmap:** The Nmap tool can be launched with this command.
- **--script-help:** Detailed help about a particular Nmap script can be displayed using this option.
- **http-enum:** You're looking for assistance with this specific Nmap script. To list all of the directories that a web server uses, utilize the http-enum file.
- **-v:** This indicates verbosity. It gives the output more verbosity and more thorough information about the script.

➢ Output Image

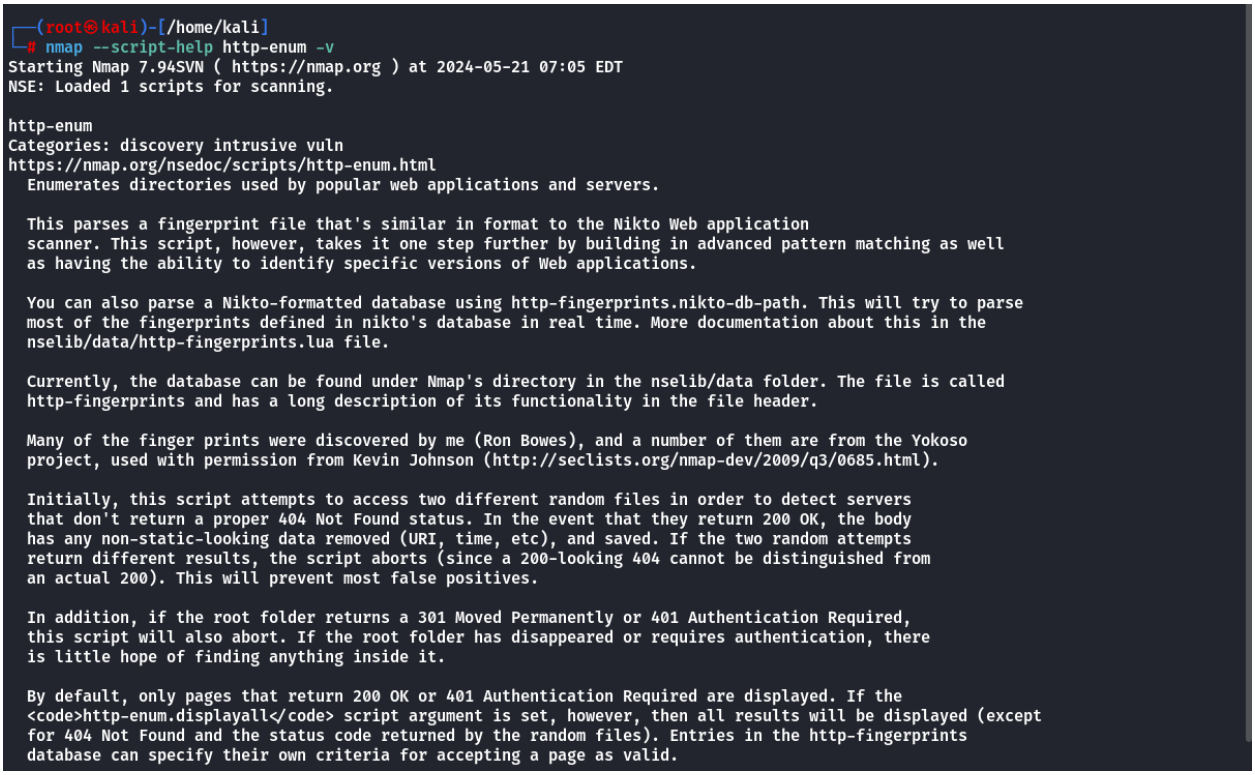


Image 26: Nmap NSE Script Help

➢ Steps Performed by the Command

- **Script Documentation Retrieval:**
  - The --script-help flag tells Nmap to display detailed help information about the specified script (http-enum).
  - Nmap retrieves the http-enum script's documentation, which includes information on the script's goals, usage, parameters, and sample outputs.
- **Verbose Output:**
  - The -v flag provides additional details and context about the script, making the help output more informative.

3.3. nmap --script <script> --script-args <args> -v <target IP>

- **Command Breakdown**

Syntax	nmap	--script	<script>	--script-args	<args>	-v	<target IP>
Example	nmap	--script	http-enum	--script-args	http-enum.displayall	-v	192.168.29.185
Detail	Initiates Nmap	Use to run script	Uses the http-enum Script	specify argument	Displays All Results	Enables Verbose Mode	Targets IP Address

Table 16: Nmap NSE Script Arguments

- **nmap:** The Nmap tool can be launched with this command.
- **--script http-enum:** This option instructs Nmap to use the http-enum script, which lists common files and directories used by servers and web applications.
- **--script-args http-enum.displayall:** This specifies an argument for the http-enum script to display all results, not just the positive matches.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity.
- **192.168.29.185:** The target IP address is this. This IP address will be scanned by Nmap to obtain details about files and web directories.

➢ Output Image

```
┌──(root㉿kali)-[/home/kali]
└─# nmap --script http-enum --script-args http-enum.displayall -v 192.168.29.185

Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 01:12 EDT
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 01:12
Completed NSE at 01:12, 0.00s elapsed
Initiating ARP Ping Scan at 01:12
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 01:12, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:12
Completed Parallel DNS resolution of 1 host. at 01:12, 0.00s elapsed
Initiating SYN Stealth Scan at 01:12
Scanning 192.168.29.185 [1000 ports]
Discovered open port 23/tcp on 192.168.29.185
Discovered open port 53/tcp on 192.168.29.185
Discovered open port 445/tcp on 192.168.29.185
Discovered open port 21/tcp on 192.168.29.185
Discovered open port 80/tcp on 192.168.29.185
Discovered open port 25/tcp on 192.168.29.185
Discovered open port 139/tcp on 192.168.29.185
Discovered open port 3306/tcp on 192.168.29.185
Discovered open port 22/tcp on 192.168.29.185
Discovered open port 5432/tcp on 192.168.29.185
Discovered open port 8009/tcp on 192.168.29.185
Discovered open port 8180/tcp on 192.168.29.185
Completed SYN Stealth Scan at 01:12, 0.15s elapsed (1000 total ports)
NSE: Script scanning 192.168.29.185.
Initiating NSE at 01:12
Completed NSE at 01:12, 5.83s elapsed
Nmap scan report for 192.168.29.185
Host is up (0.0015s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
```

```
53/tcp   open  domain
80/tcp   open  http
| http-enum:
|   /tikiwiki/: Tikiwiki (302 Found)
|   /phpinfo.php: Possible information file
|   /sdk/../../../../../../../etc/vmware/hostd/vmInventory.xml: Possible path traversal in V
MWare (CVE-2009-3733) (400 Bad Request)
|   /sdk/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/%2E%2E/etc/vmware/hostd/vmInventory.xml:
Possible path traversal in VMWare (CVE-2009-3733) (400 Bad Request)
|   /../../../../../../../../../../etc/passwd: Possible path traversal in URI (400 Bad Reque
st)
|   /../../../../../../../../../../boot.ini: Possible path traversal in URI (400 Bad Request
)
|   /cgi-bin/: Potentially interesting folder (403 Forbidden)
|   /doc/: Potentially interesting folder (403 Forbidden)
|   /icons/: Potentially interesting folder w/ directory listing
|_  /server-status/: Potentially interesting folder (403 Forbidden)
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown
| http-enum:
|   /admin/: Possible admin folder
|   /admin/index.html: Possible admin folder
|   /admin/login.html: Possible admin folder
|   /admin/admin.html: Possible admin folder
|   /admin/account.html: Possible admin folder
|   /admin/admin_login.html: Possible admin folder
|   /admin/home.html: Possible admin folder
|   /admin/admin-login.html: Possible admin folder
|   /admin/adminLogin.html: Possible admin folder
|   /admin/controlpanel.html: Possible admin folder
|   /admin/cp.html: Possible admin folder
|   /admin/index.jsp: Possible admin folder
|   /admin/login.jsp: Possible admin folder
|   /admin/admin.jsp: Possible admin folder
|   /admin/home.jsp: Possible admin folder
|   /admin/controlpanel.jsp: Possible admin folder
```

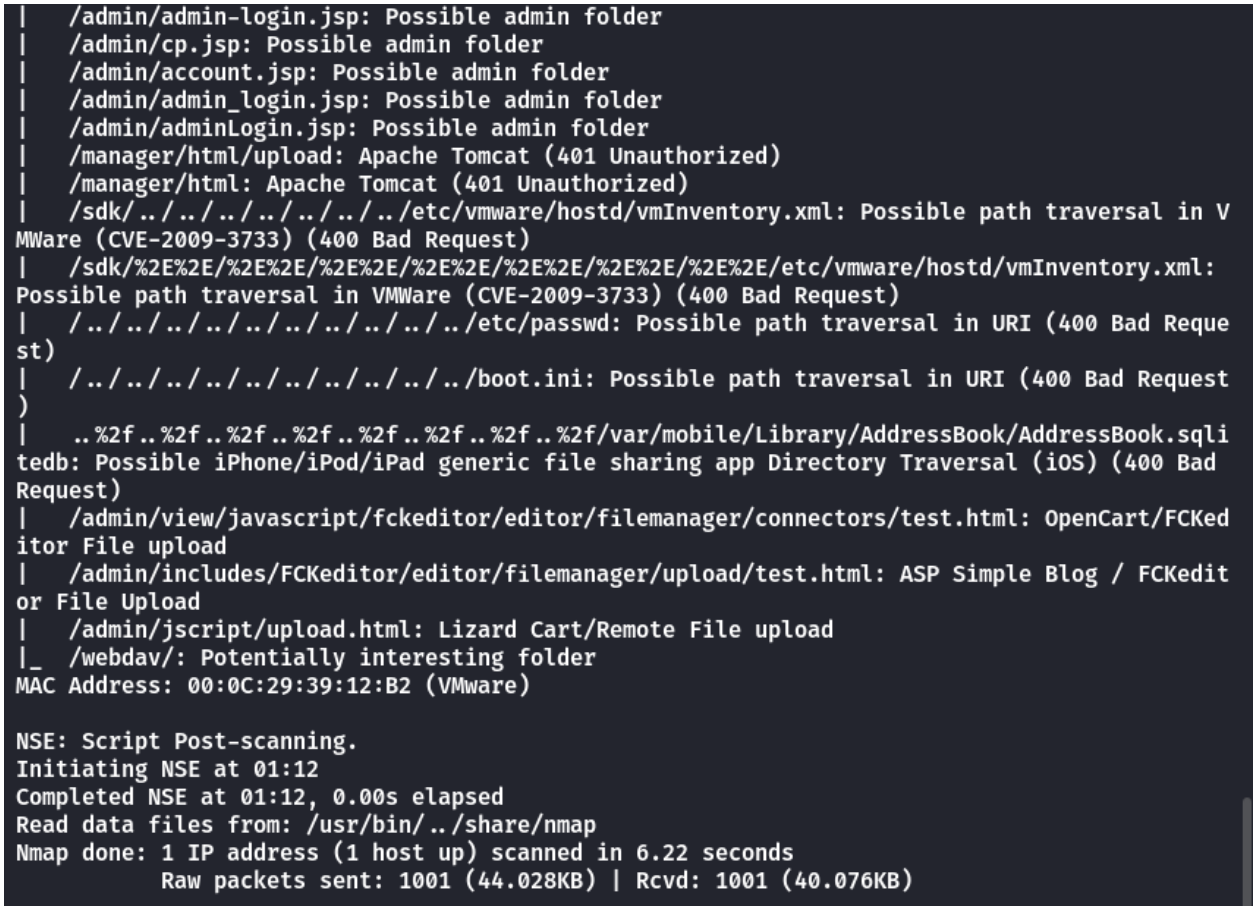


Image 27: Nmap NSE Script Arguments

- **Steps Performed by the Command**
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **HTTP Enumeration:**
    - When the http-enum script runs, the target receives HTTP requests to count the number of files and directories.
    - By passing in the http-enum.displayall argument, the script displays a list of every tested path along with the ones that do and don't exist.
  - **Service Detection:**
    - Nmap looks for open ports and tries to identify the services that are using them.
  - **Output Results:**
    - Nmap provides complete details about the files, directories, and responses from the target web server that are found.

4. Output Options

4.1. nmap -oN <file name> -v <target IP>

- **Command Breakdown**

Syntax	nmap	-oN	<File name>	-v	<target IP>
Example	nmap	-oN	scan_results.txt	-v	192.168.29.185
Detail	Initiates Nmap	Normal Output File	Output File	Enables Verbose Mode	Targets IP Address

Table 17: Nmap Result Output in TXT and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-oN scan_results.txt:** This option indicates that the scan results should be saved to the file scan_results.txt in a standard (human-readable) format.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity.
- **192.168.29.185:** This IP address is intended for use. To find out what open ports are and what services are using them, Nmap will scan this IP address.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -oN scan_results.txt -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 02:07 EDT
Initiating ARP Ping Scan at 02:07
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 02:07, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:07
Completed Parallel DNS resolution of 1 host. at 02:07, 0.01s elapsed
Initiating SYN Stealth Scan at 02:07
Scanning 192.168.29.185 [1000 ports]
Discovered open port 445/tcp on 192.168.29.185
Discovered open port 53/tcp on 192.168.29.185
Discovered open port 22/tcp on 192.168.29.185
Discovered open port 23/tcp on 192.168.29.185
Discovered open port 80/tcp on 192.168.29.185
Discovered open port 3306/tcp on 192.168.29.185
Discovered open port 21/tcp on 192.168.29.185
Discovered open port 139/tcp on 192.168.29.185
Discovered open port 25/tcp on 192.168.29.185
Discovered open port 8009/tcp on 192.168.29.185
Discovered open port 5432/tcp on 192.168.29.185
Discovered open port 8180/tcp on 192.168.29.185
Completed SYN Stealth Scan at 02:07, 0.13s elapsed (1000 total ports)
Nmap scan report for 192.168.29.185
Host is up (0.0019s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown

MAC Address: 00:0C:29:39:12:B2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.076KB)
```

Image 28: Nmap Result Output in TXT and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
    - If nothing else is specified, the default scan looks through the 1000 most frequently used ports.
  - **Service Detection:**
    - Nmap looks for open ports and tries to identify the services that are using them.
  - **Output Results to File:**
    - Nmap stores the outcomes in a format that is readable by humans in scan_results.txt. This contains information on services, open ports, and other pertinent details.

4.2. nmap -oX <file name> -v <target IP>

- **Command Breakdown**

Syntax	nmap	-oX	<file name>	-v	<target IP>
Example	nmap	-oX	scan_results.xml	-v	192.168.29.185
Detail	Initiates Nmap	XML Output File Format	Output File	Enables Verbose Mode	Targets IP Address

Table 18: Nmap Result Output in XML and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-oX scan_results.xml:** Specifies that the scan results should be saved to a file called scan_results.xml and output in XML format.
- **-v:** Enables verbose mode, which gives more thorough output regarding the results and progress of the scan.
- **192.168.29.185:** Nmap will use the target IP address to check for open ports and other network features.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -oX scan_results.xml -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 02:55 EDT
Initiating ARP Ping Scan at 02:55
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 02:55, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:55
Completed Parallel DNS resolution of 1 host. at 02:55, 0.01s elapsed
Initiating SYN Stealth Scan at 02:55
Scanning 192.168.29.185 [1000 ports]
Discovered open port 25/tcp on 192.168.29.185
Discovered open port 21/tcp on 192.168.29.185
Discovered open port 139/tcp on 192.168.29.185
Discovered open port 53/tcp on 192.168.29.185
Discovered open port 22/tcp on 192.168.29.185
Discovered open port 3306/tcp on 192.168.29.185
Discovered open port 23/tcp on 192.168.29.185
Discovered open port 80/tcp on 192.168.29.185
Discovered open port 445/tcp on 192.168.29.185
Discovered open port 5432/tcp on 192.168.29.185
Discovered open port 8180/tcp on 192.168.29.185
Discovered open port 8009/tcp on 192.168.29.185
Completed SYN Stealth Scan at 02:55, 0.15s elapsed (1000 total ports)
Nmap scan report for 192.168.29.185
Host is up (0.0028s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown

MAC Address: 00:0C:29:39:12:B2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.076KB)
```

Image 29: Nmap Result Output in XML and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - Nmap, which is perfect for quicker and more dependable scanning on local networks, sends ARP requests to the target host to see if it is active.
  - **DNS Resolution:**
    - If possible, attempts are made to resolve the domain name linked to the IP address.
  - **Port Scanning:**
    - By sending SYN packets to different ports to check their status without completing the TCP handshake, it performs a less intrusive SYN scan by default.
  - **Service Detection:**
    - Makes an effort to determine which services are using any open ports that are found during the port scan.
  - **Outputs Results in XML Format:**
    - Nmap stores detailed scan results, including details about open ports, services, and the scan configuration, to scan_results.xml.

4.3. nmap -oG <file name> -v <target IP>

- **Command Breakdown**

Syntax	nmap	-oG	<file name>	-v	<target IP>
Example	nmap	-oG	grep_results.txt	-v	192.168.29.185
Detail	Initiates Nmap	grepable Output File Format	Output File	Enables Verbose Mode	Targets IP Address

Table 19: Nmap Result Output in Grepable Format and Verbose Scanning

- **nmap:** This command launches the network scanning and security application Nmap.
- **-oG grep_results.txt:** This option instructs Nmap to write the scan results to a file called grep_results.txt in a "grepable" format. The format is intended to be easily parsed by command-line utilities or automated scripts.
- **-v:** By doing this, verbose mode is enabled, which expands on the amount of information Nmap shows about the scan as it goes along.
- **192.168.29.185:** Nmap will search this IP address as its target to find open ports and service details.

➢ **Output Image**

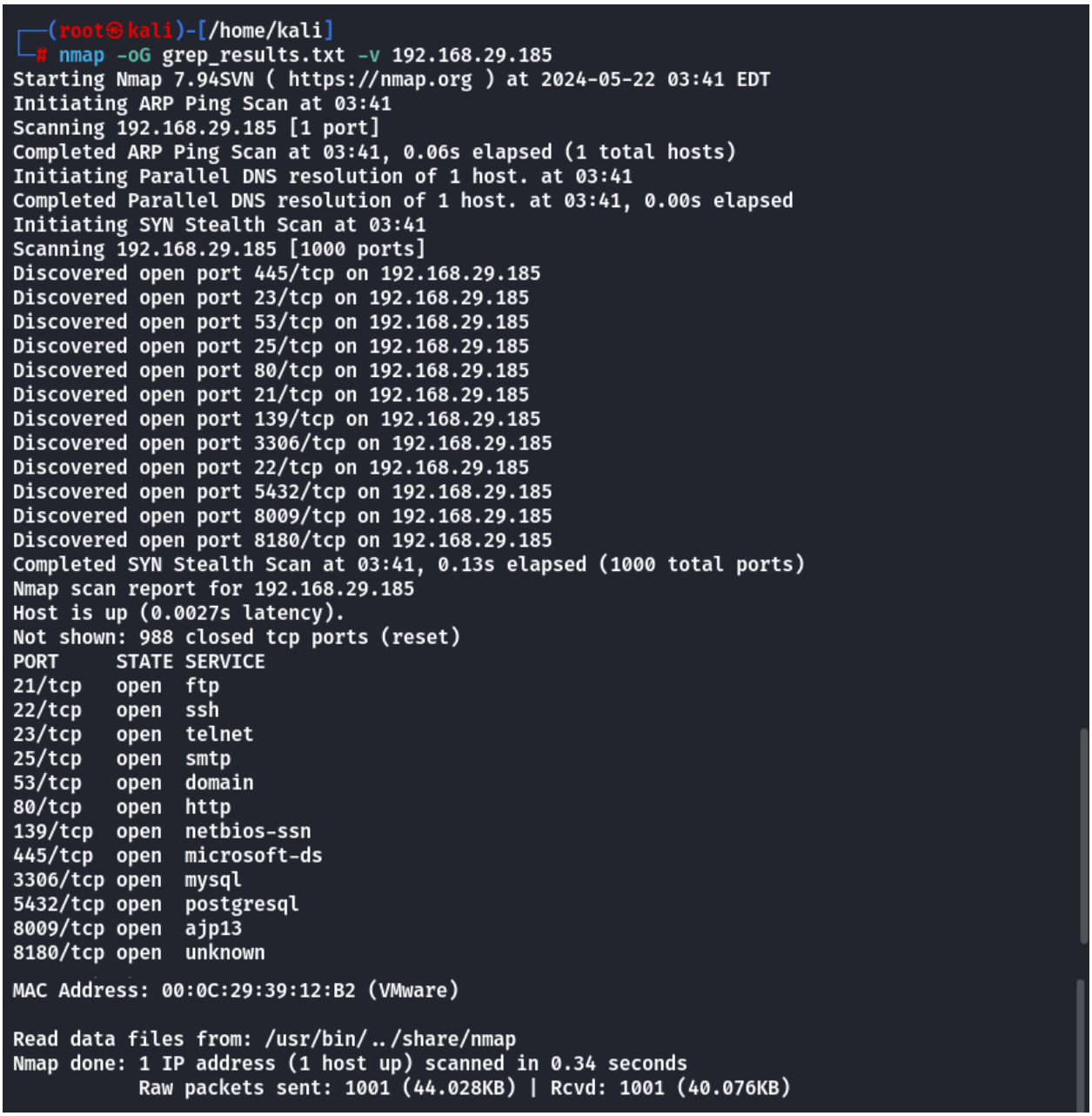


Image 30: Nmap Result Output in Grepable Format and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - ARP requests can be used by Nmap to find out whether a host is up on local networks. This works faster and gets past firewalls on networks.
  - **DNS Resolution:**
    - Nmap will try to find the hostname of the target.
  - **Port Scanning:**
    - In order to find out which ports are open, Nmap typically performs a SYN scan (or another type based on context) by sending SYN packets to various ports.
  - **Service Detection:**
    - Nmap attempts to determine which services are executing on each open port after port discovery.
  - **Outputs Results in Grepable Format:**
    - The format of the scan results, which is optimized for parsing with grep, is saved to grep_results.txt, making it simple to search and filter the results.

4.4. nmap -oA <base name> -v <target IP>

- **Command Breakdown**

Syntax	nmap	-oA	<base name>	-v	<target IP>
Example	nmap	-oA	scan_results	-v	192.168.29.185
Detail	Initiates Nmap	Creates three files in different formats	Output Files	Enables Verbose Mode	Targets IP Address

Table 20: Nmap Result Output in All Available Three Format and Verbose Scanning

- **Initiates Nmap:** Nmap is launched by the command with the given output and verbosity options.
- **Enables Verbose Mode:** When the -v option is used, Nmap will provide more thorough feedback throughout the scan, outlining its actions at each stage.
- **Sets Output Formats:** The -oA option creates three files in different formats: plain text (.nmap), XML (.xml), and grepable (.gnmap), facilitating various types of analysis or reporting.
- **Targets IP Address:** Nmap looks at the given IP address to find open ports, information about services, and possibly even information about the operating system.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -oA scan_results -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 04:16 EDT
Initiating ARP Ping Scan at 04:16
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 04:16, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 04:16
Completed Parallel DNS resolution of 1 host. at 04:16, 0.00s elapsed
Initiating SYN Stealth Scan at 04:16
Scanning 192.168.29.185 [1000 ports]
Discovered open port 21/tcp on 192.168.29.185
Discovered open port 80/tcp on 192.168.29.185
Discovered open port 23/tcp on 192.168.29.185
Discovered open port 22/tcp on 192.168.29.185
Discovered open port 3306/tcp on 192.168.29.185
Discovered open port 139/tcp on 192.168.29.185
Discovered open port 53/tcp on 192.168.29.185
Discovered open port 445/tcp on 192.168.29.185
Discovered open port 25/tcp on 192.168.29.185
Discovered open port 8009/tcp on 192.168.29.185
Discovered open port 8180/tcp on 192.168.29.185
Discovered open port 5432/tcp on 192.168.29.185
Completed SYN Stealth Scan at 04:16, 0.13s elapsed (1000 total ports)
Nmap scan report for 192.168.29.185
Host is up (0.0023s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown

MAC Address: 00:0C:29:39:12:B2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.30 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.076KB)
```

Image 31: Nmap Result Output in All Available Three Format and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether a host on a local network is online, Nmap may issue ARP requests.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target's hostname to aid in identifying the machine on the network.
  - **Port Scanning:**
    - To find open ports, Nmap typically sends SYN packets and tracks the responses; however, the precise process may differ depending on the network and Nmap's configuration.
  - **Service Detection:**
    - Nmap searches for services running on ports after they are discovered; this information is helpful for penetration testing and network management.
  - **Output to Files:**
    - Results are saved in three formats: normal (scan_results.nmap), XML (scan_results.xml), and grepable (scan_results.gnmap), making the data usable in a variety of tools and contexts.

5. Timing and Performance

5.1. nmap -T<0-5> -v <target IP>

- **Command Breakdown**

Syntax	nmap	-T<0-5>	-v	<target IP>
Example	nmap	-T3	-v	192.168.29.185
Detail	Initiates Nmap	Sets Timing Template	Enables Verbose Mode	Targets IP Address

Table 21: Nmap Timing Template Scan and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-T3:** This specifies the timing template. -T3 sets the timing to "normal", balancing speed and accuracy. Nmap has six timing templates: -T0 (paranoid), -T1 (sneaky), -T2 (polite), -T3 (normal), -T4 (aggressive), and -T5 (insane). -T3 is the default setting and is used for general-purpose scanning.
- **-v:** This flag turns on verbose mode, which produces thorough output regarding the status of the scan.
- **192.168.29.185:** This IP address is intended for use. To find out what open ports are and what services are using them, Nmap will scan this IP address.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -T3 -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-22 09:22 EDT
Initiating ARP Ping Scan at 09:22
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 09:22, 0.09s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 09:22
Completed Parallel DNS resolution of 1 host. at 09:22, 0.14s elapsed
Initiating SYN Stealth Scan at 09:22
Scanning 192.168.29.185 [1000 ports]
Discovered open port 139/tcp on 192.168.29.185
Discovered open port 53/tcp on 192.168.29.185
Discovered open port 23/tcp on 192.168.29.185
Discovered open port 80/tcp on 192.168.29.185
Discovered open port 21/tcp on 192.168.29.185
Discovered open port 22/tcp on 192.168.29.185
Discovered open port 445/tcp on 192.168.29.185
Discovered open port 3306/tcp on 192.168.29.185
Discovered open port 25/tcp on 192.168.29.185
Discovered open port 8180/tcp on 192.168.29.185
Discovered open port 8009/tcp on 192.168.29.185
Discovered open port 5432/tcp on 192.168.29.185
Completed SYN Stealth Scan at 09:22, 0.14s elapsed (1000 total ports)
Nmap scan report for 192.168.29.185
Host is up (0.0011s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown

MAC Address: 00:0C:29:39:12:B2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.076KB)
```

Image 32: Nmap Timing Template Scan and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
    - If nothing else is specified, the default scan looks through the 1000 most frequently used ports.
  - **Service Detection:**
    - Nmap looks for open ports and tries to identify the services that are using them.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

5.2. nmap --min-hostgroup <size> -v <target IP>

- **Command Breakdown**

Syntax	nmap	--min-hostgroup <size>	-v	<target IP>
Example	nmap	--min-hostgroup 32	-v	192.168.29.185
Detail	Initiates Nmap	Sets Minimum Host Group Size	Enables Verbose Mode	Targets IP Address

Table 22: Nmap Host Grouping Scan and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **--min-hostgroup 32:** The minimum number of hosts that Nmap will group together for parallel scanning is determined by this option. Nmap employs a technique called hostgrouping, which scans several hosts at once, to increase the effectiveness of large network scans.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Use of the -v option causes Nmap to show more details about each step it is performing, such as scan progress and information.
- **192.168.29.185:** The IP address that is being targeted is this one. This IP address will be scanned by Nmap in order to obtain information about open ports and the services that are using them.

➢ Output Image

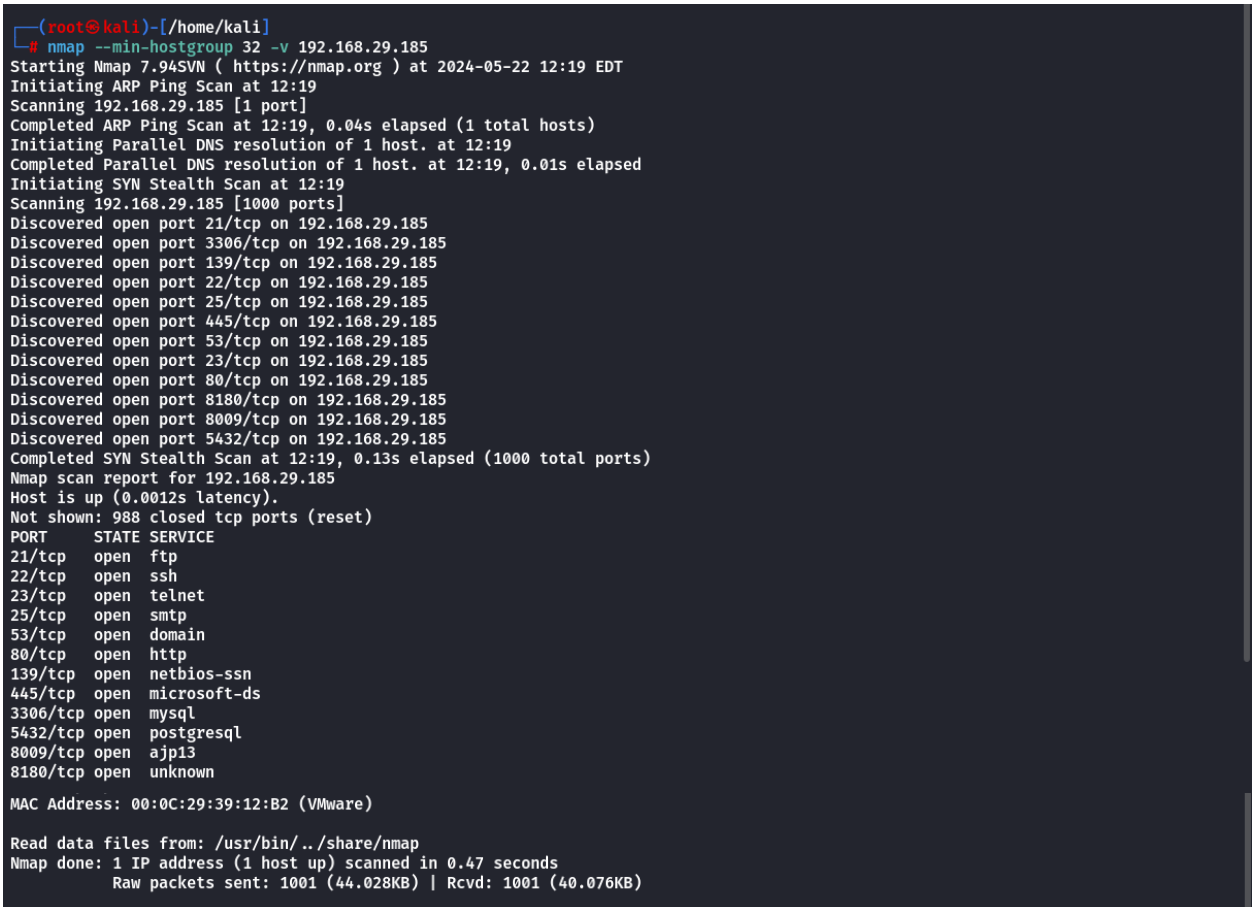


Image 33: Nmap Host Grouping Scan and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
    - If nothing else is specified, the default scan looks through the 1000 most frequently used ports.
  - **Service Detection:**
    - Nmap looks for open ports and tries to identify the services that are using them.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

5.3. nmap --min-parallelism <number> -v <target IP>

- **Command Breakdown**

Syntax	nmap	--min-parallelism <number>	-v	<target IP>
Example	nmap	--min-parallelism 10	-v	192.168.29.185
Detail	Initiates Nmap	Sets Minimum Parallelism	Enables Verbose Mode	Targets IP Address

Table 23: Nmap Min-parallelism and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **--min-parallelism 10:** This setting determines the bare minimum of concurrent tasks that Nmap will carry out while scanning. This can increase the number of parallel operations and speed up the scanning process.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Use of the -v option causes Nmap to show more details about each step it is performing, such as scan progress and information.
- **192.168.29.185:** The intended IP address is this one. In order to learn more about open ports and the services that are using them, Nmap will scan this IP address.

➢ **Output Image**

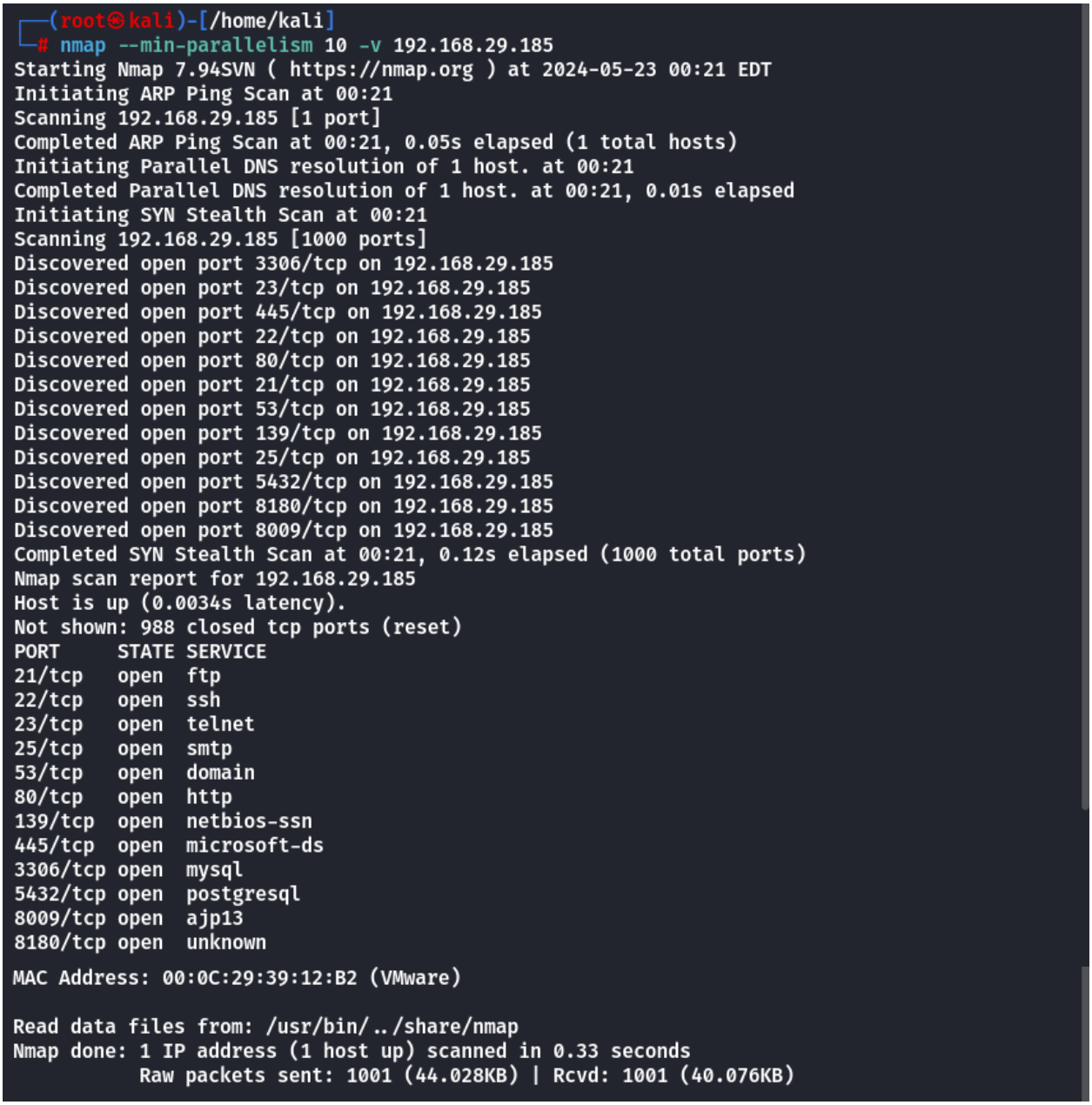


Image 34: Nmap Min-parallelism and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
    - If nothing else is specified, the default scan looks through the 1000 most frequently used ports.
  - **Service Detection:**
    - Nmap looks for open ports and tries to identify the services that are using them.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

6. Firewall Evasion Techniques

6.1. nmap -f -v <target IP>

- **Command Breakdown**

Syntax	nmap	-f	-v	<target IP>
Example	nmap	-f	-v	192.168.29.185
Detail	Initiates Nmap	Enables Packet Fragmentation	Enables Verbose Mode	Targets IP Address

Table 24: Nmap Partial Packet and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-f:** Partial packet scanning is enabled by this setting. Because it breaks up the probe packets into smaller pieces, it can occasionally get past intrusion detection systems (IDS) and firewalls that don't reassemble broken packets.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Use of the -v option causes Nmap to show more details about each step it is performing, such as scan progress and information.
- **192.168.29.185:** This IP address is intended for use. To find out what open ports are and what services are using them, Nmap will scan this IP address.

➢ **Output Image**

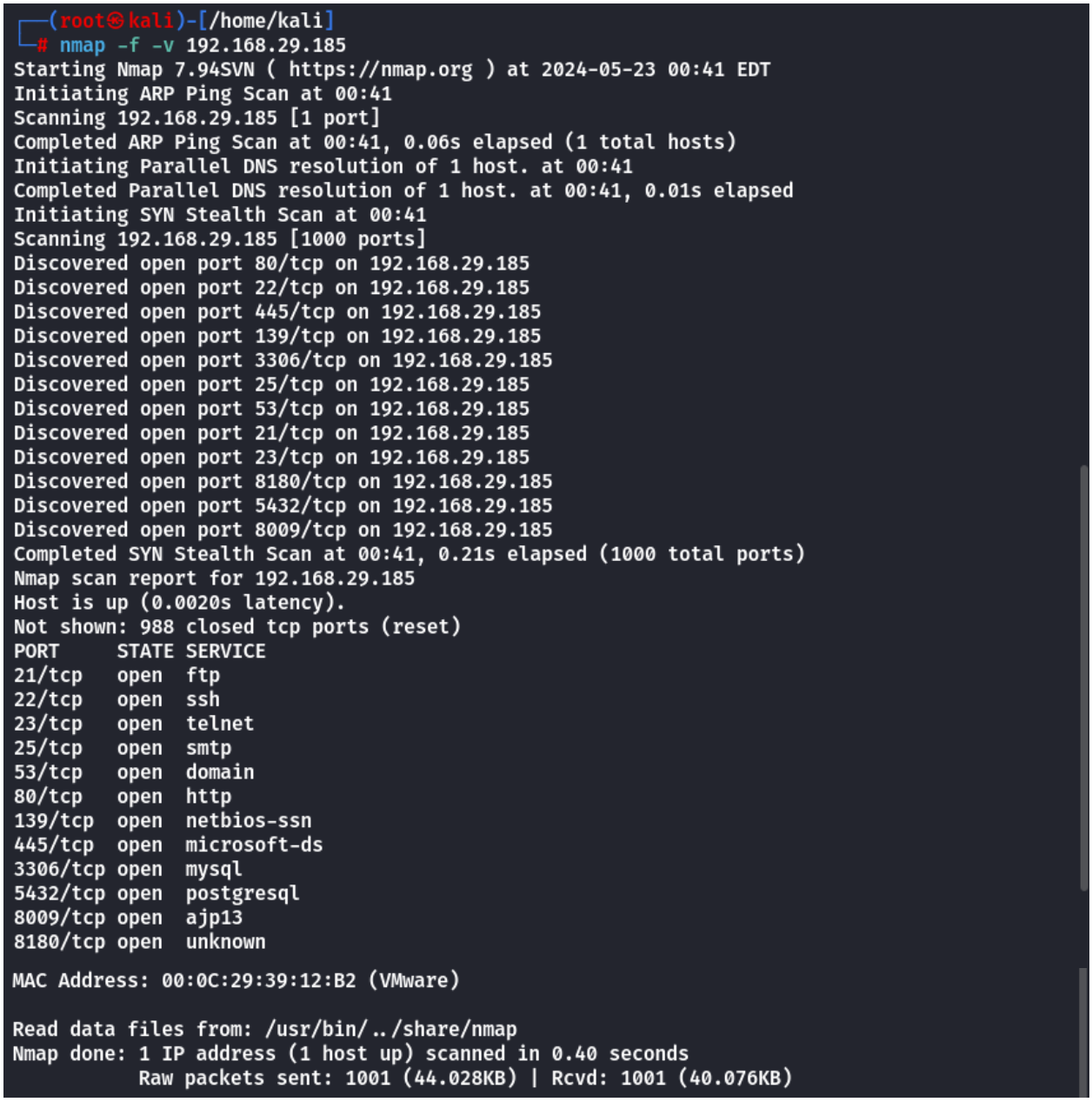


Image 35: Nmap Partial Packet and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning with Fragmentation:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
    - To avoid being detected by certain security measures, the -f option divides these packets into smaller pieces.
  - **Service Detection:**
    - Nmap looks for open ports and tries to identify the services that are using them.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

6.2. nmap -D <decoy1, decoy2, [ME], ...> -v <target IP>

- **Command Breakdown**

Syntax	nmap	-D	<decoy1, decoy2, [ME], ...>	-v	<target IP>
Example	nmap	-D	10.0.0.1,192.168.29.1, ME	-v	192.168.29.185
Detail	Initiates Nmap	Enables Decoy Scan	Enables Verbose Mode	Enables Verbose Mode	Targets IP Address

Table 25: Nmap Decoy and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-D 10.0.0.1,192.168.29.1, ME:** To hide the origin of the scan, this option provides a list of fictitious IP addresses. In this instance, the decoy addresses are 10.0.0.1 and 192.168.29.1, while ME denotes the scanner's actual IP address.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Use of the -v option causes Nmap to show more details about each step it is performing, such as scan progress and information.
- **192.168.29.185:** The target IP address is this. This IP address will be scanned by Nmap to learn more about open ports and the services that are using them.

➢ Output Images

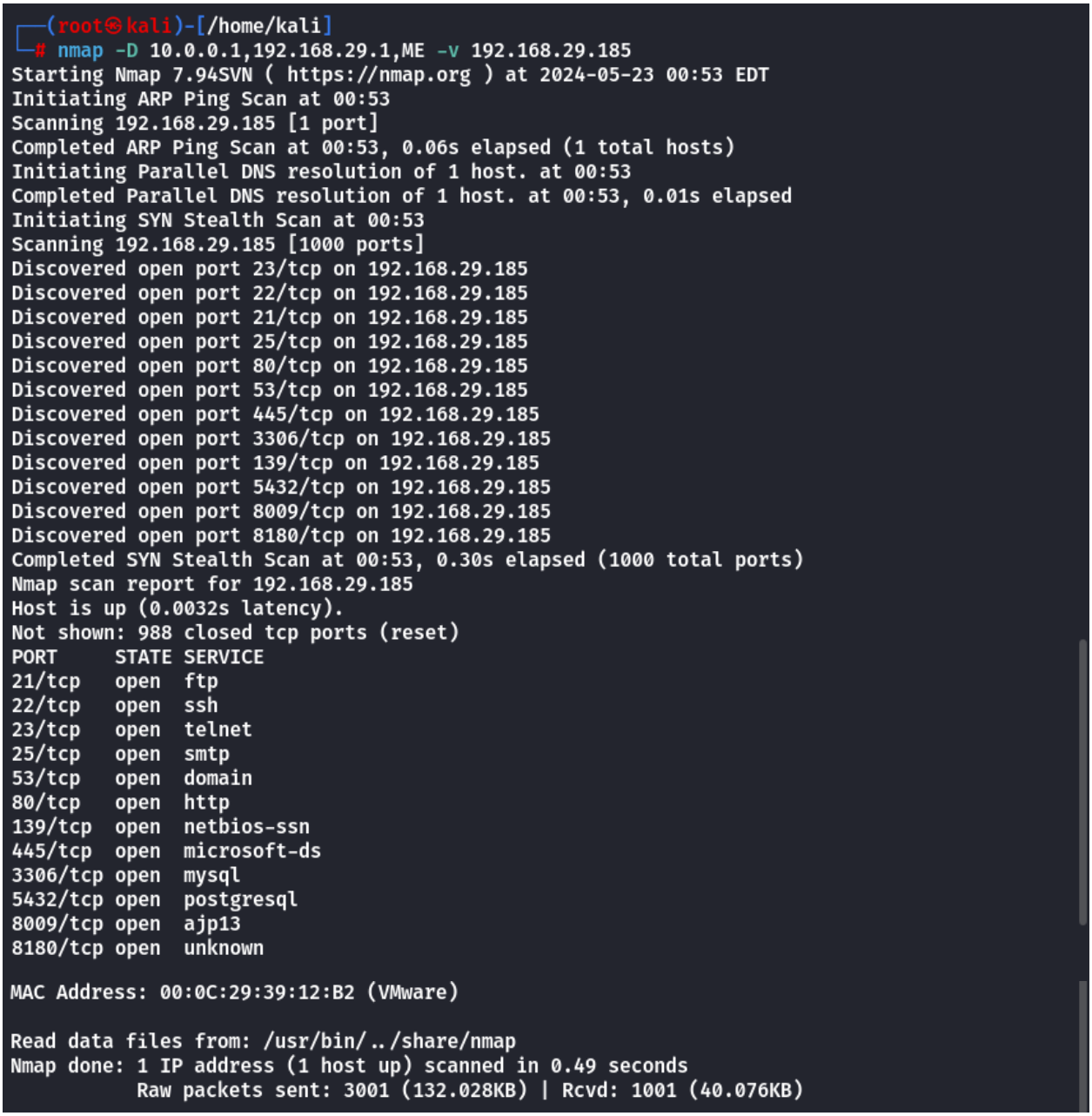


Image 36: Nmap Decoy and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning with Decoys:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
    - The target will perceive the scan as coming from multiple sources because the -D option adds decoy addresses to the scan.
  - **Service Detection:**
    - Nmap looks for open ports and tries to identify the services that are using them.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

6.3. nmap --mtu <val> -v <target IP>

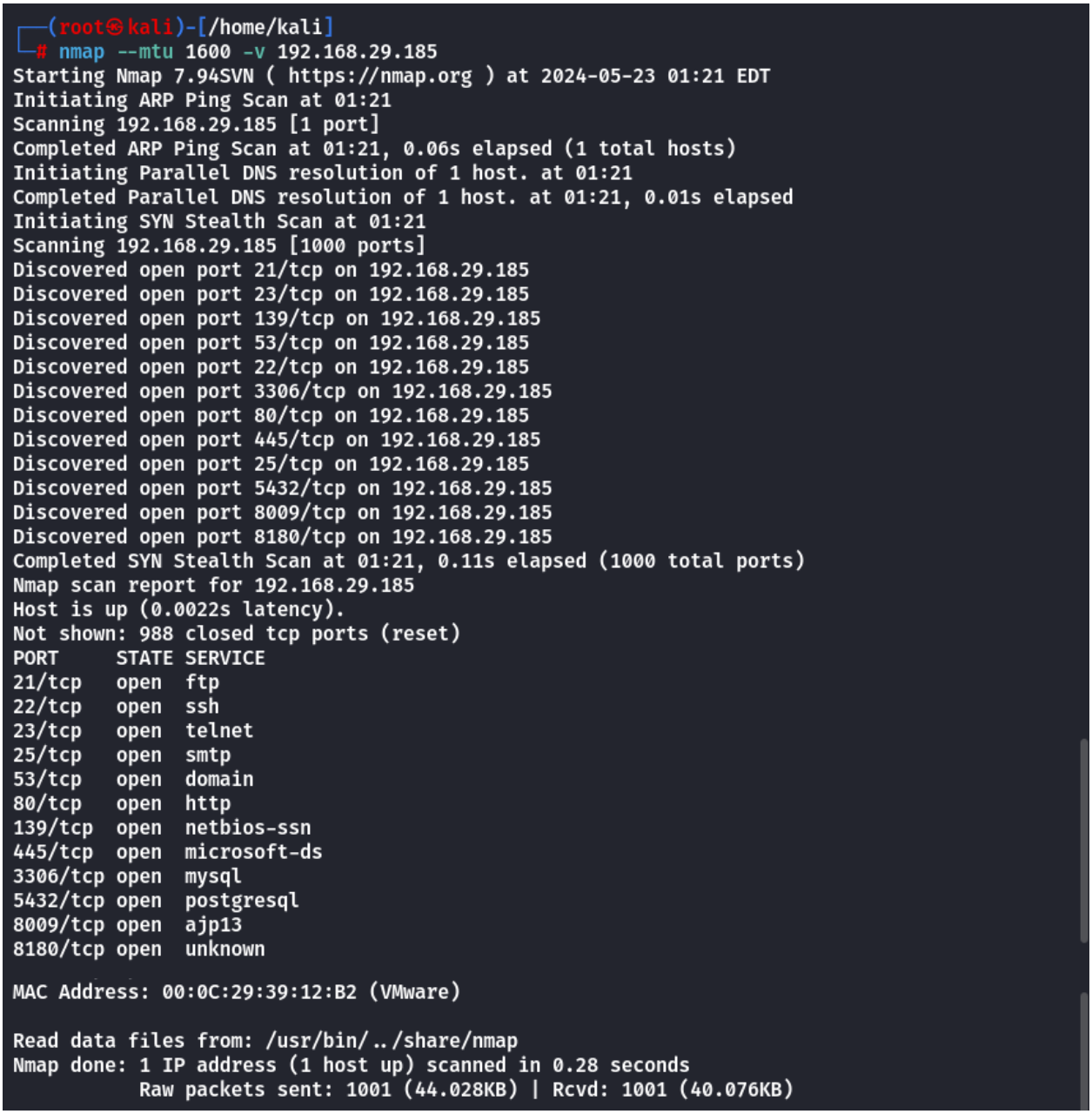
- **Command Breakdown**

Syntax	nmap	--mtu <val>	-v	<target IP>
Example	nmap	--mtu 1600	-v	192.168.29.185
Detail	Initiates Nmap	Sets MTU to 1600	Enables Verbose Mode	Targets IP Address

Table 26: Nmap MTU and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **--mtu 1600:** With this option, Nmap's packets' maximum transmission unit (MTU) is set to 1600 bytes. This may be used to get around some network security devices and fragment packets.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Use of the -v option causes Nmap to show more details about each step it is performing, such as scan progress and information.
- **192.168.29.185:** This IP address is intended for use. To find out what open ports are and what services are using them, Nmap will scan this IP address.

➢ **Output Image**



```
┌──(root㉿kali)-[/home/kali]
└─# nmap --mtu 1600 -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 01:21 EDT
Initiating ARP Ping Scan at 01:21
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 01:21, 0.06s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 01:21
Completed Parallel DNS resolution of 1 host. at 01:21, 0.01s elapsed
Initiating SYN Stealth Scan at 01:21
Scanning 192.168.29.185 [1000 ports]
Discovered open port 21/tcp on 192.168.29.185
Discovered open port 23/tcp on 192.168.29.185
Discovered open port 139/tcp on 192.168.29.185
Discovered open port 53/tcp on 192.168.29.185
Discovered open port 22/tcp on 192.168.29.185
Discovered open port 3306/tcp on 192.168.29.185
Discovered open port 80/tcp on 192.168.29.185
Discovered open port 445/tcp on 192.168.29.185
Discovered open port 25/tcp on 192.168.29.185
Discovered open port 5432/tcp on 192.168.29.185
Discovered open port 8009/tcp on 192.168.29.185
Discovered open port 8180/tcp on 192.168.29.185
Completed SYN Stealth Scan at 01:21, 0.11s elapsed (1000 total ports)
Nmap scan report for 192.168.29.185
Host is up (0.0022s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown

MAC Address: 00:0C:29:39:12:B2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.076KB)
```

Image 37: Nmap MTU and Verbose Scanning

- **Steps Performed by the Command**
  - **Packet Fragmentation:**
    - Packets sent by Nmap may become fragmented because of their 1600-byte MTU. This can help you get around some network security measures.
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
  - **Service Detection:**
    - Nmap looks for open ports and tries to identify the services that are using them.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

7. Miscellaneous

7.1. nmap --reason -v <target IP>

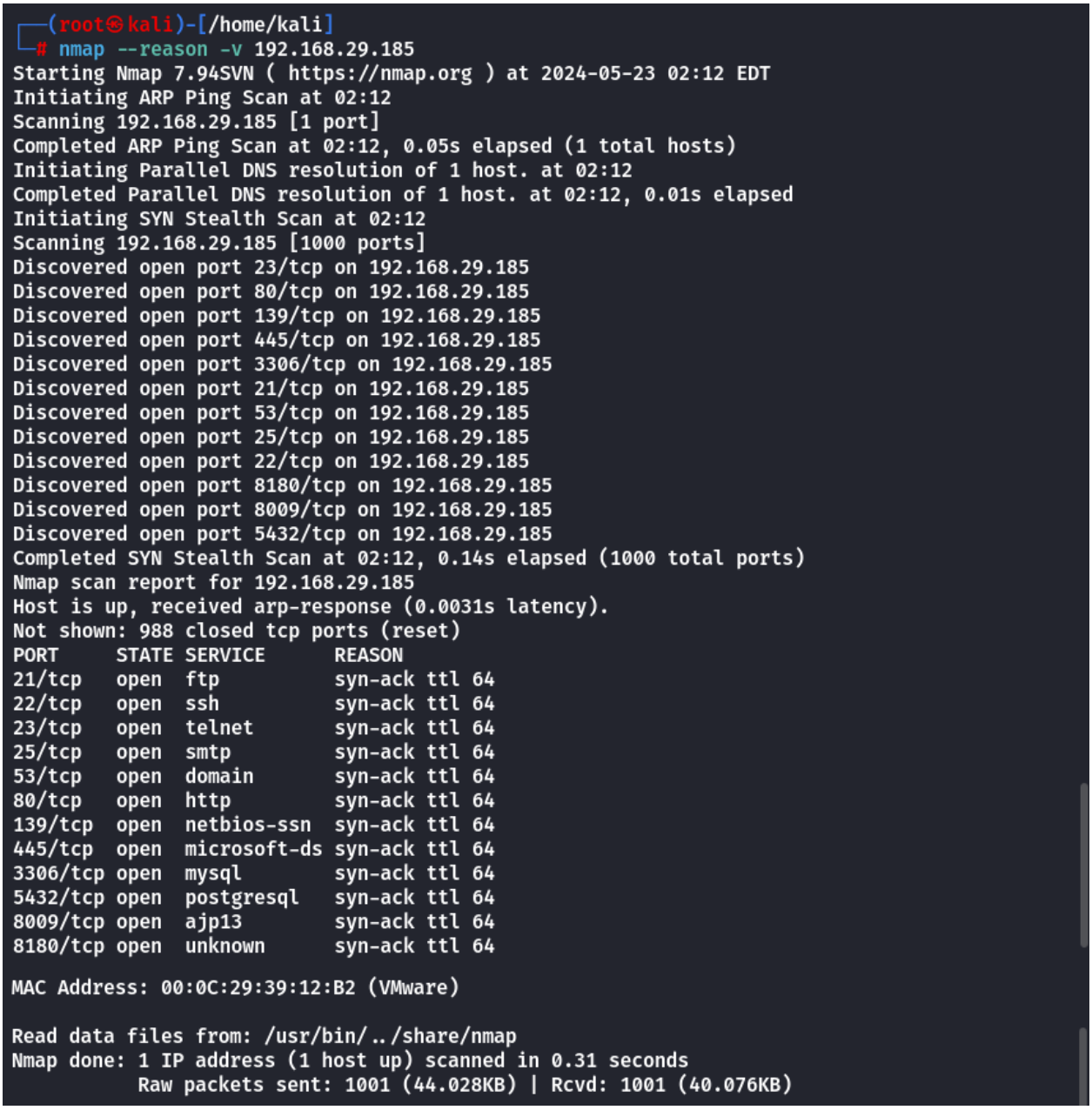
- **Command Breakdown**

Syntax	nmap	--reason	-v	<target IP>
Example	nmap	--reason	-v	192.168.29.185
Detail	Initiates Nmap	Includes Reasons for Port States	Enables Verbose Mode	Targets IP Address

Table 27: Nmap Reason and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **--reason:** This option instructs Nmap to add a note in the output explaining why each port is in a specific state (such as open, closed, or filtered). This can give the scan results additional context for understanding.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Use of the -v option causes Nmap to show more details about each step it is performing, such as scan progress and information.
- **192.168.29.185:** This IP address is intended for use. To find out what open ports are and what services are using them, Nmap will scan this IP address.

➢ **Output Image**



```
┌──(root㉿kali)-[/home/kali]
└─# nmap --reason -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 02:12 EDT
Initiating ARP Ping Scan at 02:12
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 02:12, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 02:12
Completed Parallel DNS resolution of 1 host. at 02:12, 0.01s elapsed
Initiating SYN Stealth Scan at 02:12
Scanning 192.168.29.185 [1000 ports]
Discovered open port 23/tcp on 192.168.29.185
Discovered open port 80/tcp on 192.168.29.185
Discovered open port 139/tcp on 192.168.29.185
Discovered open port 445/tcp on 192.168.29.185
Discovered open port 3306/tcp on 192.168.29.185
Discovered open port 21/tcp on 192.168.29.185
Discovered open port 53/tcp on 192.168.29.185
Discovered open port 25/tcp on 192.168.29.185
Discovered open port 22/tcp on 192.168.29.185
Discovered open port 8180/tcp on 192.168.29.185
Discovered open port 8009/tcp on 192.168.29.185
Discovered open port 5432/tcp on 192.168.29.185
Completed SYN Stealth Scan at 02:12, 0.14s elapsed (1000 total ports)
Nmap scan report for 192.168.29.185
Host is up, received arp-response (0.0031s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE      REASON
21/tcp   open  ftp          syn-ack ttl 64
22/tcp   open  ssh          syn-ack ttl 64
23/tcp   open  telnet       syn-ack ttl 64
25/tcp   open  smtp         syn-ack ttl 64
53/tcp   open  domain       syn-ack ttl 64
80/tcp   open  http         syn-ack ttl 64
139/tcp  open  netbios-ssn  syn-ack ttl 64
445/tcp  open  microsoft-ds syn-ack ttl 64
3306/tcp open  mysql        syn-ack ttl 64
5432/tcp open  postgresql   syn-ack ttl 64
8009/tcp open  ajp13        syn-ack ttl 64
8180/tcp open  unknown      syn-ack ttl 64

MAC Address: 00:0C:29:39:12:B2 (VMware)

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 (40.076KB)
```

Image 38: Nmap Reason and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
    - The --reason flag makes sure that each port's state and reason are included in the output.
  - **Service Detection:**
    - Nmap looks for open ports and tries to identify the services that are using them.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

7.2. nmap --open -v <target IP>

- **Command Breakdown**

Syntax	nmap	--open	-v	<target IP>
Example	nmap	--open	-v	192.168.29.185
Detail	Initiates Nmap	Displays Only Open Ports	Enables Verbose Mode	Targets IP Address

Table 28: Nmap Display Only Open port and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **--open:** Nmap will only display open ports in the output if this option is enabled. Ports that are filtered or closed won't show up.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Use of the -v option causes Nmap to show more details about each step it is performing, such as scan progress and information.
- **192.168.29.185:** This IP address is intended for use. To find out what open ports are and what services are using them, Nmap will scan this IP address.

➢ **Output Image**

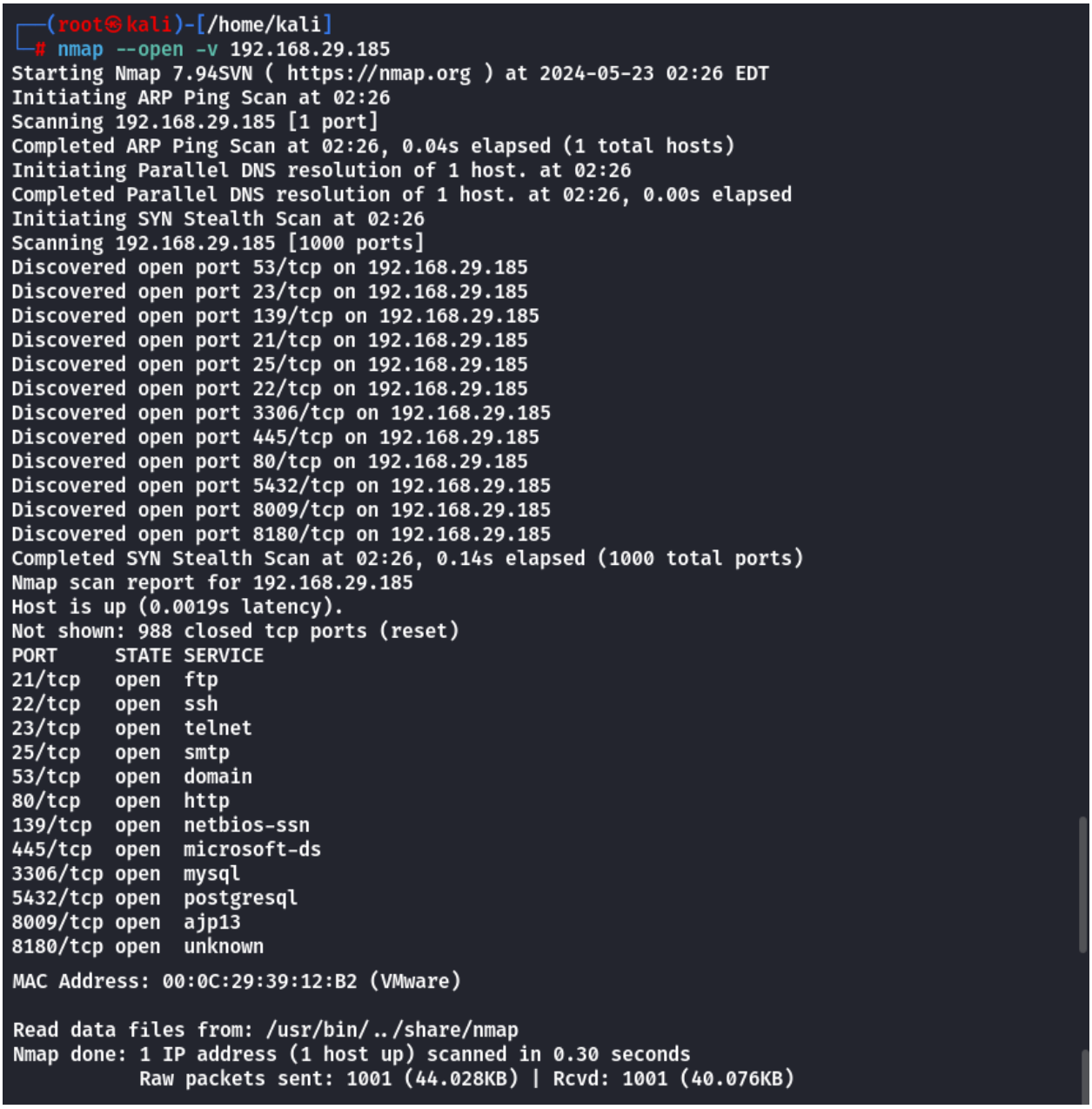


Image 39: Nmap Display Only Open port and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
    - Only ports that respond as open are shown, thanks to the --open flag.
  - **Service Detection:**
    - Nmap looks for open ports and tries to identify the services that are using them.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

7.3. nmap -p <port no.> --packet-trace -v <target IP>

- **Command Breakdown**

Syntax	nmap	-p <port no.>	--packet-trace	-v	<target IP>
Example	nmap	-p 80	--packet-trace	-v	192.168.29.185
Detail	Initiates Nmap	Targets Port 80	Enables Packet Trace	Enables Verbose Mode	Targets IP Address

Table 29: Nmap Port Number and Packet Trace and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-p 80:** This option instructs Nmap to scan the target IP address's port 80 only. HTTP services usually run on port 80.
- **--packet-trace:** During the scan, this option instructs Nmap to show information about the packets that were sent and received. Debugging and comprehending the intricacies of network communication can benefit from it.
- **-v:** This option instructs Nmap to show information about the packets that were sent and received throughout the scan. It is helpful for debugging and comprehending the network communication's intricate details.
- **192.168.29.185:** This IP address is intended for use. To obtain information about port 80, Nmap will scan this IP address.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -p 80 --packet-trace -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 03:10 EDT
Initiating ARP Ping Scan at 03:10
Scanning 192.168.29.185 [1 port]
SENT (0.0470s) ARP who-has 192.168.29.185 tell 192.168.29.32
RCVD (0.0476s) ARP reply 192.168.29.185 is-at 00:0C:29:39:12:B2
Completed ARP Ping Scan at 03:10, 0.05s elapsed (1 total hosts)
NSOCK INFO [0.1060s] nsock_iod_new2(): nsock_iod_new (IOD #1)
NSOCK INFO [0.1060s] nsock_connect_udp(): UDP connection requested to 2405:201:20:3023::c0a8
:1d01:53 (IOD #1) EID 8
NSOCK INFO [0.1070s] nsock_read(): Read request from IOD #1 [2405:201:20:3023::c0a8:1d01:53]
 (timeout: -1ms) EID 18
NSOCK INFO [0.1070s] nsock_iod_new2(): nsock_iod_new (IOD #2)
NSOCK INFO [0.1070s] nsock_connect_udp(): UDP connection requested to 192.168.29.1:53 (IOD #
2) EID 24
NSOCK INFO [0.1070s] nsock_read(): Read request from IOD #2 [192.168.29.1:53] (timeout: -1ms
) EID 34
Initiating Parallel DNS resolution of 1 host. at 03:10
NSOCK INFO [0.1070s] nsock_write(): Write request for 45 bytes to IOD #1 EID 43 [2405:201:20
:3023::c0a8:1d01:53]
NSOCK INFO [0.1070s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [24
05:201:20:3023::c0a8:1d01:53]
NSOCK INFO [0.1070s] nsock_trace_handler_callback(): Callback: WRITE SUCCESS for EID 43 [240
5:201:20:3023::c0a8:1d01:53]
NSOCK INFO [0.1070s] nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 24 [1
92.168.29.1:53]
NSOCK INFO [0.1090s] nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [2405
:201:20:3023::c0a8:1d01:53] (45 bytes): 8E...........185.29.168.192.in-addr.arpa.....
NSOCK INFO [0.1090s] nsock_read(): Read request from IOD #1 [2405:201:20:3023::c0a8:1d01:53]
 (timeout: -1ms) EID 50
NSOCK INFO [0.1090s] nsock_iod_delete(): nsock_iod_delete (IOD #1)
NSOCK INFO [0.1090s] nevent_delete(): nevent_delete on event #50 (type READ)
NSOCK INFO [0.1090s] nsock_iod_delete(): nsock_iod_delete (IOD #2)
NSOCK INFO [0.1090s] nevent_delete(): nevent_delete on event #34 (type READ)
Completed Parallel DNS resolution of 1 host. at 03:10, 0.00s elapsed
Initiating SYN Stealth Scan at 03:10
Scanning 192.168.29.185 [1 port]
SENT (0.1509s) TCP 192.168.29.32:41435 > 192.168.29.185:80 S ttl=58 id=34537 iplen=44  seq=3
975863850 win=1024 <mss 1460>
RCVD (0.1514s) TCP 192.168.29.185:80 > 192.168.29.32:41435 SA ttl=64 id=0 iplen=44  seq=1427
396853 win=5840 <mss 1460>
Discovered open port 80/tcp on 192.168.29.185
Completed SYN Stealth Scan at 03:10, 0.04s elapsed (1 total ports)
Nmap scan report for 192.168.29.185
Host is up (0.00059s latency).

PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:39:12:B2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```

Image 40: Nmap Port Number and Packet Trace and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - For local network scans, ARP is utilized because it's more.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - Nmap scans port 80 using the SYN protocol.
    - To ensure that every packet sent and received during the scan is displayed, use the --packet-trace option.
  - **Service Detection:**
    - If port 80 is open, Nmap tries to find the service that is using it.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

7.4. nmap --traceroute -v <target IP>

- **Command Breakdown**

Syntax	nmap	--traceroute	-v	<target IP>
Example	nmap	--traceroute	-v	192.168.29.185
Detail	Initiates Nmap	Performs a Traceroute	Enables Verbose Mode	Targets IP Address

Table 30: Nmap Traceroute and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **--traceroute:** By selecting this option, Nmap is instructed to traceroute to the desired IP address. Traceroute sends packets with increasing Time-to-Live (TTL) values and records the response from each hop along the path to determine the path packets take from the source machine to the target machine.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Use of the -v option causes Nmap to show more details about each step it is performing, such as scan progress and information.
- **192.168.29.185:** This IP address is intended for use. This IP address will be scanned and a traceroute will be made using Nmap.

➢ **Output Image**

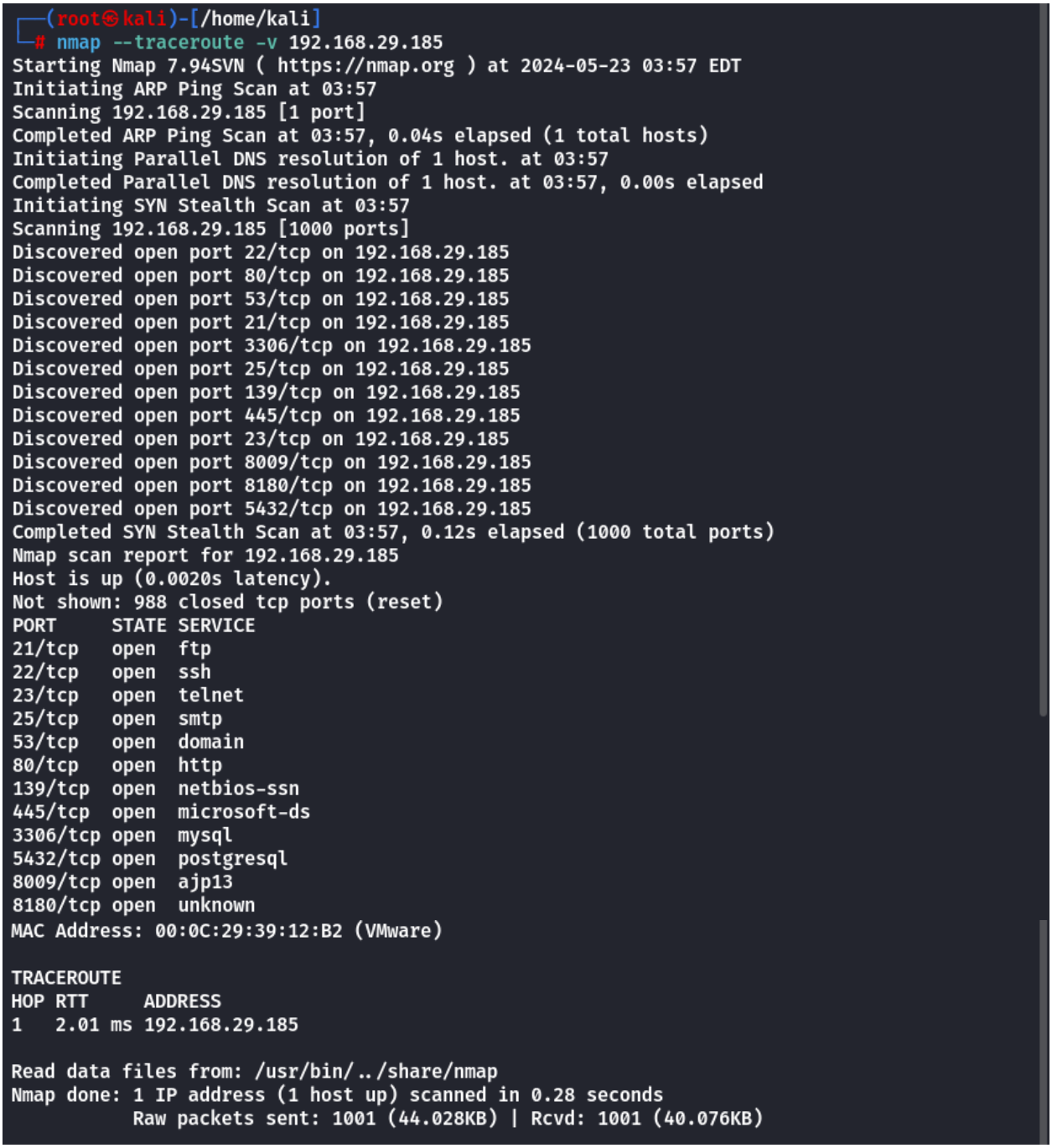


Image 41: Nmap Traceroute and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
  - **Service Detection:**
    - Nmap looks for open ports and tries to identify the services that are using them.
  - **Traceroute:**
    - Nmap maps the path that packets take to get to the target by executing a traceroute to the IP address.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

8. Host Discovery

8.1. nmap -Pn -v <target IP>

- **Command Breakdown**

Syntax	nmap	-Pn	-v	<target IP>
Example	nmap	-Pn	-v	192.168.29.185
Detail	Initiates Nmap	Skips Host Discovery	Enables Verbose Mode	Targets IP Address

Table 31: Nmap Skip Host Discovery/Don't Use ICMP and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-Pn:** Assuming that the host is up, this option instructs Nmap to bypass the host discovery stage. This is helpful in cases where the first ping scan might be blocked or for scanning hosts hidden behind firewalls.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Use of the -v option causes Nmap to show more details about each step it is performing, such as scan progress and information.
- **192.168.29.185:** This IP address is intended for use. Nmap is going to examine this IP address.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -Pn -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 07:17 EDT
Initiating ARP Ping Scan at 07:17
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 07:17, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 07:17
Completed Parallel DNS resolution of 1 host. at 07:17, 13.00s elapsed
Initiating SYN Stealth Scan at 07:17
Scanning 192.168.29.185 [1000 ports]
Discovered open port 445/tcp on 192.168.29.185
Discovered open port 80/tcp on 192.168.29.185
Discovered open port 25/tcp on 192.168.29.185
Discovered open port 53/tcp on 192.168.29.185
Discovered open port 21/tcp on 192.168.29.185
Discovered open port 22/tcp on 192.168.29.185
Discovered open port 139/tcp on 192.168.29.185
Discovered open port 3306/tcp on 192.168.29.185
Discovered open port 23/tcp on 192.168.29.185
Discovered open port 8180/tcp on 192.168.29.185
Discovered open port 5432/tcp on 192.168.29.185
Discovered open port 8009/tcp on 192.168.29.185
Completed SYN Stealth Scan at 07:17, 0.12s elapsed (1000 total ports)
Nmap scan report for 192.168.29.185
Host is up (0.0030s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp open  mysql
5432/tcp open  postgresql
8009/tcp open  ajp13
8180/tcp open  unknown

MAC Address: 00:0C:29:39:12:B2 (VMware)

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.27 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.076KB)
```

Image 42: Nmap Skip Host Discovery/Don't Use ICMP and Verbose Scanning

- **Steps Performed by the Command**
  - **Skip Host Discovery:**
    - When the -Pn option is used, Nmap is instructed to presume that the host is up without first running a ping scan to confirm.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
  - **Service Detection:**
    - Nmap makes an effort to determine which services are utilizing the open ports it finds.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

8.2. nmap -n -v <target IP>

- **Command Breakdown**

Syntax	nmap	-n	-v	<target IP>
Example	nmap	-n	-v	192.168.29.185
Detail	Initiates Nmap	Skips DNS Resolution	Enables Verbose Mode	Targets IP Address

Table 32: Nmap Skip DNS Resolution and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-n:** Nmap is instructed to completely avoid DNS resolution by using this option. This implies that Nmap won't try to translate an IP address into a hostname.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Use of the -v option causes Nmap to show more details about each step it is performing, such as scan progress and information.
- **192.168.29.185:** This IP address is intended for use. Nmap is going to examine this IP address.

➢ **Output Image**

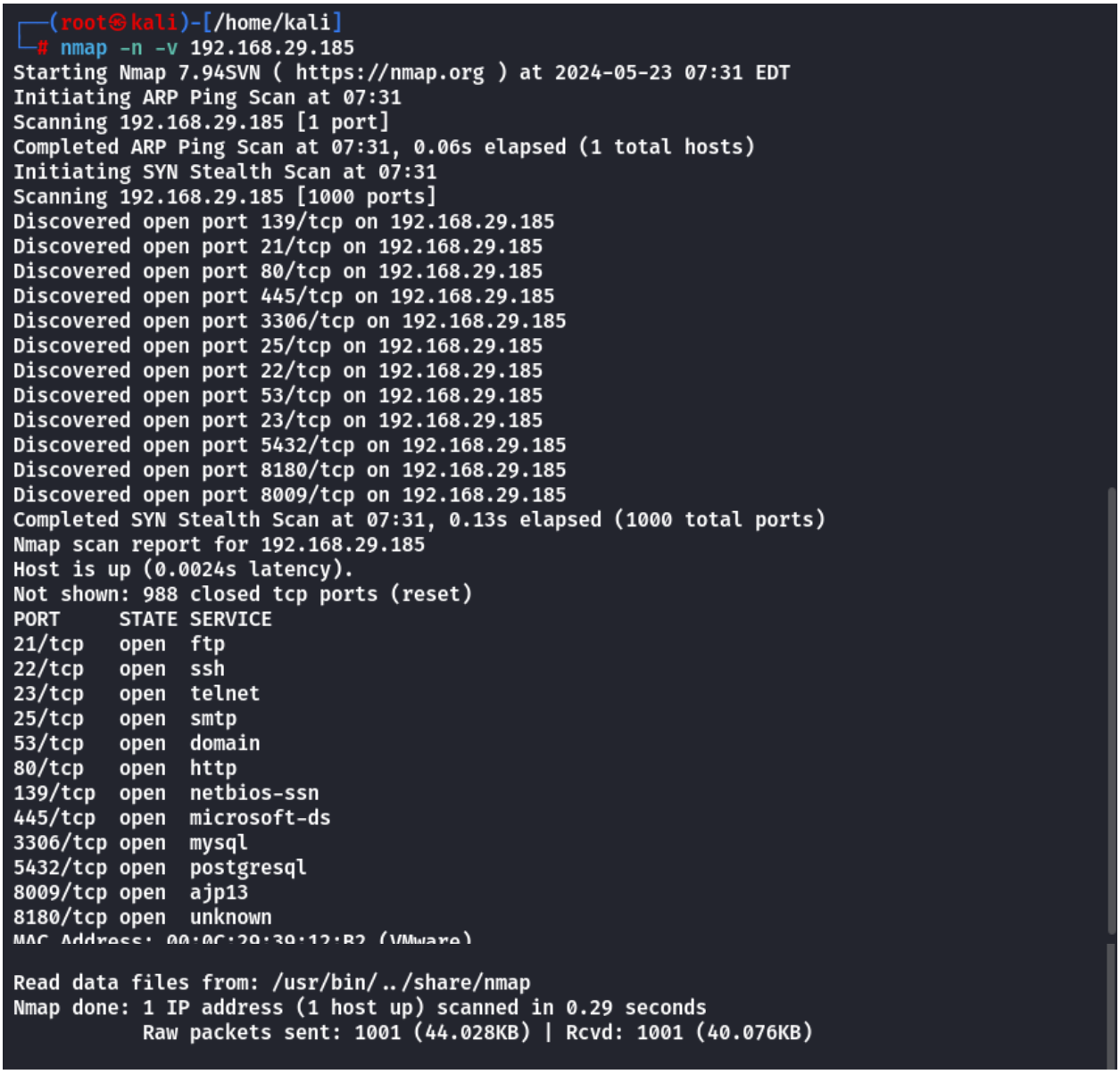


Image 43: Nmap Skip DNS Resolution and Verbose Scanning

- **Steps Performed by the Command**
  - **Skip DNS Resolution:**
    - If DNS resolution is slow or unnecessary, Nmap can expedite the scan by using the -n option, which instructs Nmap to forego the DNS resolution procedure.
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **Port Scanning:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
  - **Service Detection:**
    - Nmap looks for open ports and tries to identify the services that are using them.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

8.3. nmap -sn -v <target IP>

- **Command Breakdown**

Syntax	nmap	-sn	-v	<target IP>
Example	nmap	-sn	-v	192.168.29.185
Detail	Initiates Nmap	Performs a Ping Scan	Enables Verbose Mode	Targets the IP Address

Table 33: Nmap Perform a Ping Scan Only/No Port Scan and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-sn:** This option instructs Nmap to run a "no port scan," which is essentially a ping scan. Nmap won't look for open ports; it will only check if the host is up.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Use of the -v option causes Nmap to show more details about each step it is performing, such as scan progress and information.
- **192.168.29.185:** The IP address that the target is 192.168.29.185. To find out if this IP address is up, use Nmap.

- **Output Image**

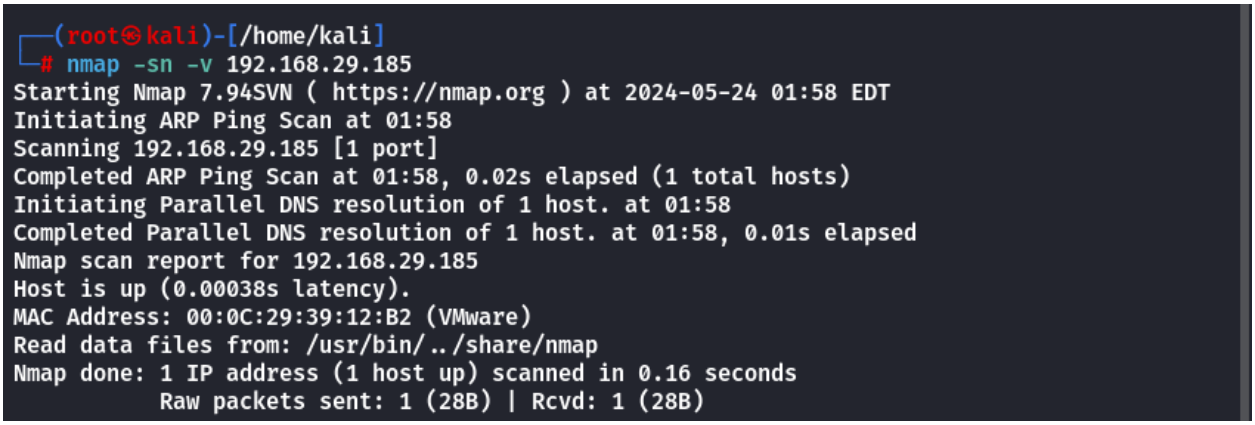


Image 44: Nmap Perform a Ping Scan Only/No Port Scan and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out if the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **ICMP Echo Request:**
    - Nmap probes the target by sending an ICMP Echo Request (ping) to see if it responds.
  - **TCP SYN Ping:**
    - Nmap may also send TCP SYN packets to common ports (like 80 or 443) to see if there is any response, indicating the host is up.
  - **DNS Resolution:**
    - If applicable, Nmap tries to resolve the hostname of the target IP address.

9. DNS

9.1. nmap --dns-servers <DNS IP> -v <target IP>

- **Command Breakdown**

Syntax	nmap	--dns-server <DNS IP>	-v	<target IP>
Example	nmap	--dns-server 8.8.8.8	-v	192.168.29.185
Detail	Initiates Nmap	Specifies Custom DNS Server	Enables Verbose Mode	Targets IP Address

Table 34: Nmap Specify Custom DNS and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **--dns-servers 8.8.8.8:** This option designates a custom DNS server to be used for DNS resolution during the scan (in this example, 8.8.8.8, Google's public DNS server).
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Use of the -v option causes Nmap to show more details about each step it is performing, such as scan progress and information.
- **192.168.29.185:** This IP address is intended for use. Nmap is going to examine this IP address.

➢ **Output Image**

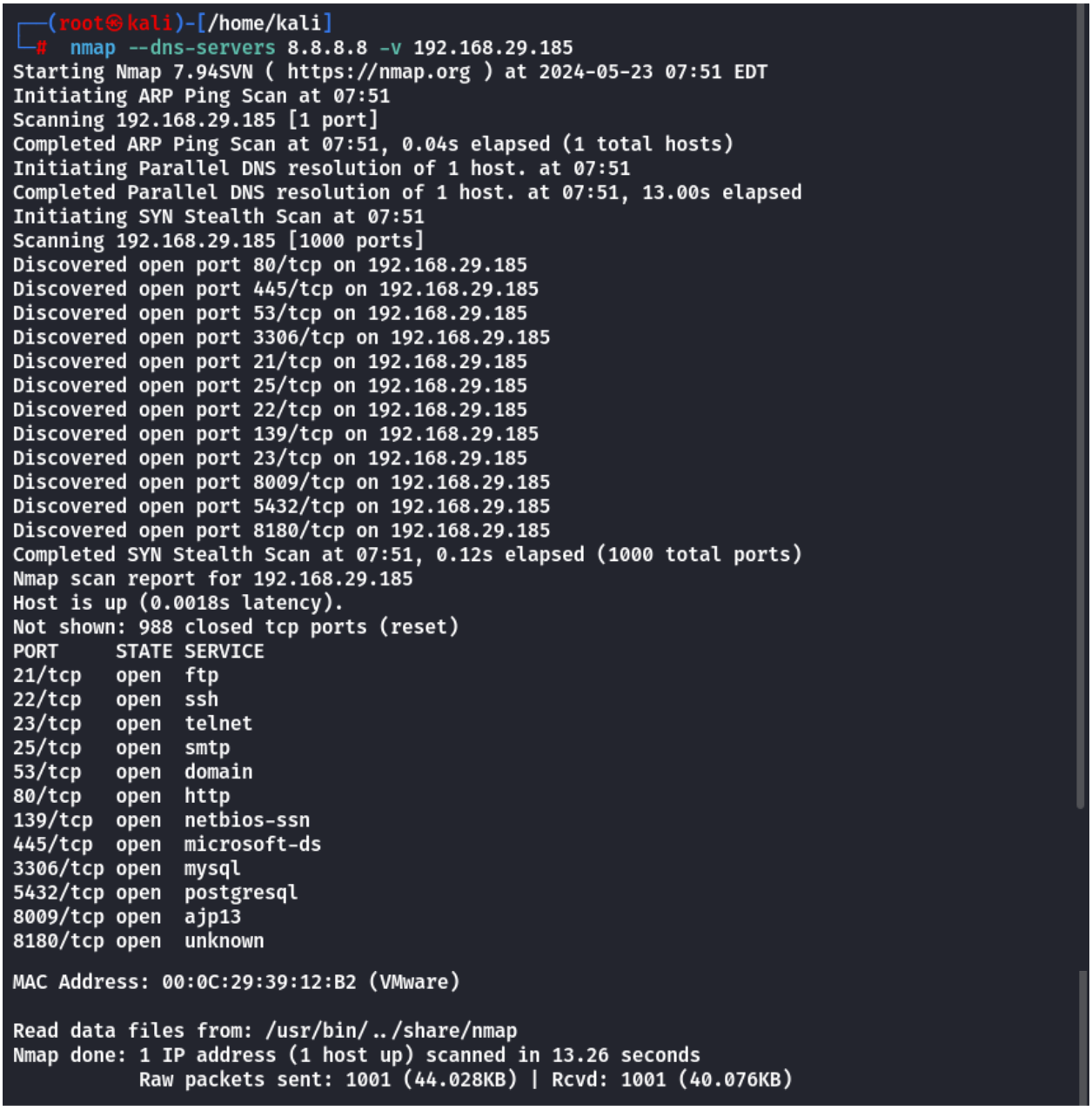


Image 45: Nmap Specify Custom DNS and Verbose Scanning

- **Steps Performed by the Command**
  - **DNS Resolution:**
    - If necessary, Nmap resolves the target IP address's hostname using the designated DNS server (8.8.8.8).
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **Port Scanning:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
  - **Service Detection:**
    - Nmap looks for open ports and tries to identify the services that are using them.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

10. Version Intensity

10.1. nmap -sV --version-intensity <value> -v <target IP>

- **Command Breakdown**

Syntax	Nmap	-sV	--version-intensity <value>	-v	<target IP>
Example	nmap	-sV	--version-intensity 5	-v	192.168.29.185
Detail	Initiates Nmap	Enables Service Version Detection	Sets Version Detection Intensity to 5	Enables Verbose Mode	Targets IP Address

Table 35: Nmap Service Version Detection and Version Detection Intensity and Verbose Scanning

- **nmap:** The Nmap tool can be launched with this command.
- **-sV:** The detection of service versions is enabled by this option. Nmap will attempt to determine which version of the services is executing on the open ports.
- **--version-intensity 5:** The maximum level of version detection intensity, 5, is set by selecting this option. This indicates that Nmap will identify service versions using the most thorough and aggressive techniques.
- **-v:** This indicates verbosity. It provides more thorough information about the scanning process by increasing the output's verbosity. Use of the -v option causes Nmap to show more details about each step it is performing, such as scan progress and information.
- **192.168.29.185:** This IP address is intended for use. Nmap is going to examine this IP address.

➢ **Output Image**

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV --version-intensity 5 -v 192.168.29.185
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 08:19 EDT
NSE: Loaded 46 scripts for scanning.
Initiating ARP Ping Scan at 08:19
Scanning 192.168.29.185 [1 port]
Completed ARP Ping Scan at 08:19, 0.05s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 08:19
Completed Parallel DNS resolution of 1 host. at 08:19, 13.00s elapsed
Initiating SYN Stealth Scan at 08:19
Scanning 192.168.29.185 [1000 ports]
Discovered open port 23/tcp on 192.168.29.185
Discovered open port 53/tcp on 192.168.29.185
Discovered open port 80/tcp on 192.168.29.185
Discovered open port 139/tcp on 192.168.29.185
Discovered open port 445/tcp on 192.168.29.185
Discovered open port 21/tcp on 192.168.29.185
Discovered open port 25/tcp on 192.168.29.185
Discovered open port 3306/tcp on 192.168.29.185
Discovered open port 22/tcp on 192.168.29.185
Discovered open port 8180/tcp on 192.168.29.185
Discovered open port 8009/tcp on 192.168.29.185
Discovered open port 5432/tcp on 192.168.29.185
Completed SYN Stealth Scan at 08:19, 0.12s elapsed (1000 total ports)
Initiating Service scan at 08:19
Scanning 12 services on 192.168.29.185
Completed Service scan at 08:20, 21.03s elapsed (12 services on 1 host)
NSE: Script scanning 192.168.29.185.
Initiating NSE at 08:20
Completed NSE at 08:20, 0.02s elapsed
Initiating NSE at 08:20
Completed NSE at 08:20, 0.01s elapsed
Nmap scan report for 192.168.29.185
Host is up (0.0016s latency).
Not shown: 988 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         ProFTPD 1.3.1
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) PHP/5.2.4-2ubuntu5.10 with Suhosin-P
atch)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 00:0C:29:39:12:B2 (VMware)
Service Info: Host:  metasploitable.localdomain; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_k
ernel

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 34.77 seconds
           Raw packets sent: 1001 (44.028KB) | Rcvd: 1001 (40.076KB)
```

Image 46: Nmap Service Version Detection and Version Detection Intensity and Verbose Scanning

- **Steps Performed by the Command**
  - **ARP Ping Scan (on local networks):**
    - To find out whether the host is up, Nmap sends ARP requests.
    - Due to its increased speed and reliability, ARP is utilized for local network scans.
  - **DNS Resolution:**
    - Nmap attempts to resolve the target IP address's hostname, if applicable.
  - **Port Scanning:**
    - By default, Nmap runs a SYN scan (unless you tell it differently). Sending SYN packets to every port and waiting for a response, this is a covert scan.
  - **Service Detection:**
    - Nmap can identify the service versions operating on the open ports by using the -sV option.
    - Nmap will identify service versions using the most comprehensive techniques if the --version-intensity 5 option is used.
  - **OS Detection and Version Detection (if applicable):**
    - Nmap can also try to identify the operating system and service versions that are installed on the target, even though it is not enabled by default in this command.

Images

Tables

References

1. https://www.kali.org/docs/
2. https://nmap.org/book/man.html
3. https://www.vulnhub.com/entry/metasploitable-1,28/
4. https://docs.vmware.com/en/VMware-Workstation-Player-for-Windows/index.html
5. https://help.ubuntu.com/stable/ubuntu-help/