Lab 6: Perform SMTP Enumeration

Lab Scenario

As an ethical hacker or penetration tester, the next step is to perform SMTP enumeration. SMTP enumeration is performed to obtain a list of valid users, delivery addresses, message recipients on an SMTP server.

Lab Objectives

- Perform SMTP enumeration using Nmap

Overview of SMTP Enumeration

The Simple Mail Transfer Protocol (SMTP) is an internet standard based communication protocol for electronic mail transmission. Mail systems commonly use SMTP with POP3 and IMAP, which enable users to save messages in the server mailbox and download them from the server when necessary. SMTP uses mail exchange (MX) servers to direct mail via DNS. It runs on TCP port 25, 2525, or 587.

Task 1: Perform SMTP Enumeration using Nmap

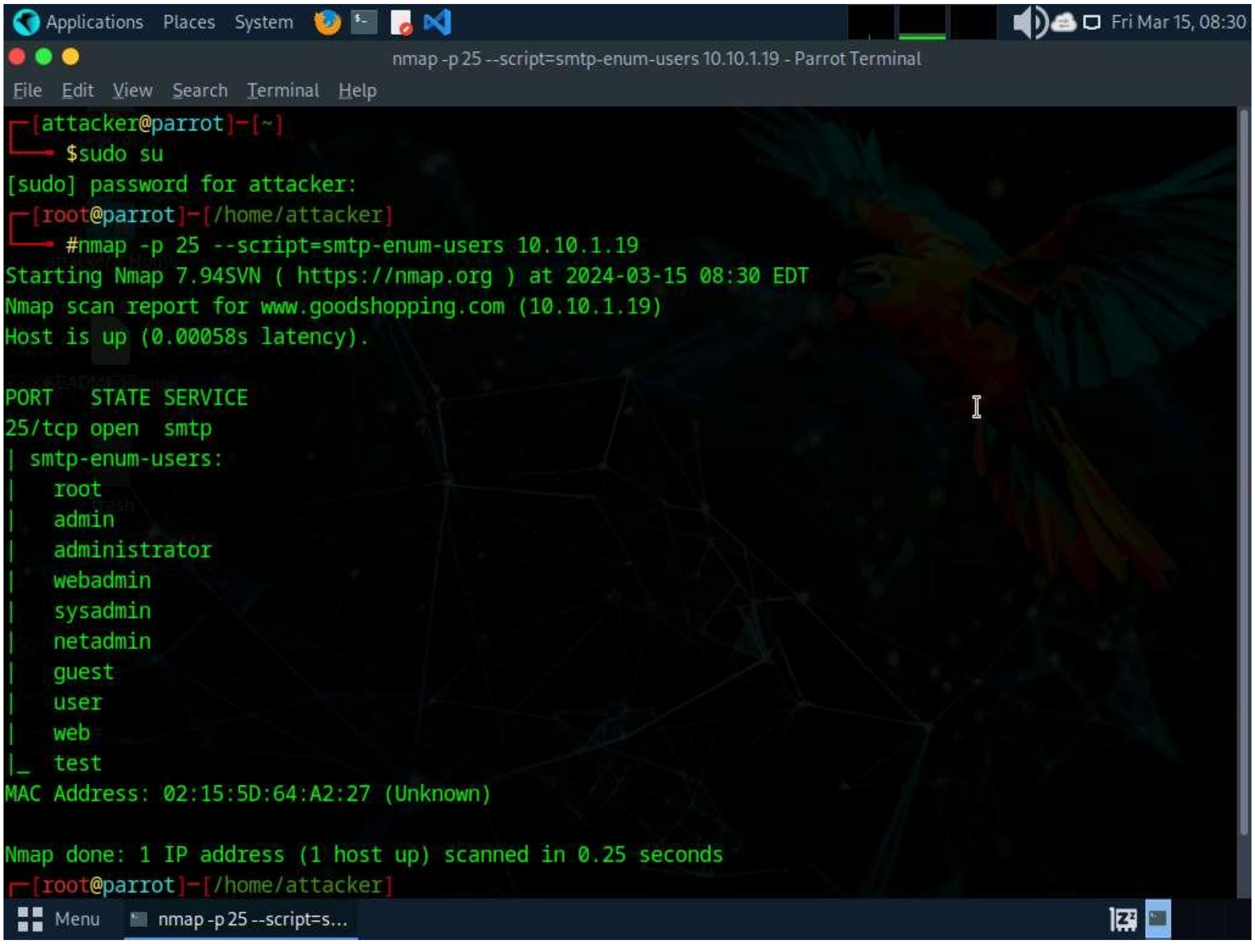
The Nmap scripting engine can be used to enumerate the SMTP service running on the target system, to obtain information about all the user accounts on the SMTP server.

Here, we will use the Nmap to perform SMTP enumeration.

1. In the **Parrot Security** machine, open a **Terminal** window and execute **sudo su** to run the programs as a root user (When prompted, enter the password **toor**).
2. Run **nmap -p 25 --script=smtp-enum-users [Target IP Address]** command (here, the target IP address is **10.10.1.19**).

-p: specifies the port, and **--script**: argument is used to run a given script (here, the script is **smtp-enum-users**).

3. The result appears displaying a list of all the possible mail users on the target machine (**10.10.1.19**), as shown in the screenshot below.

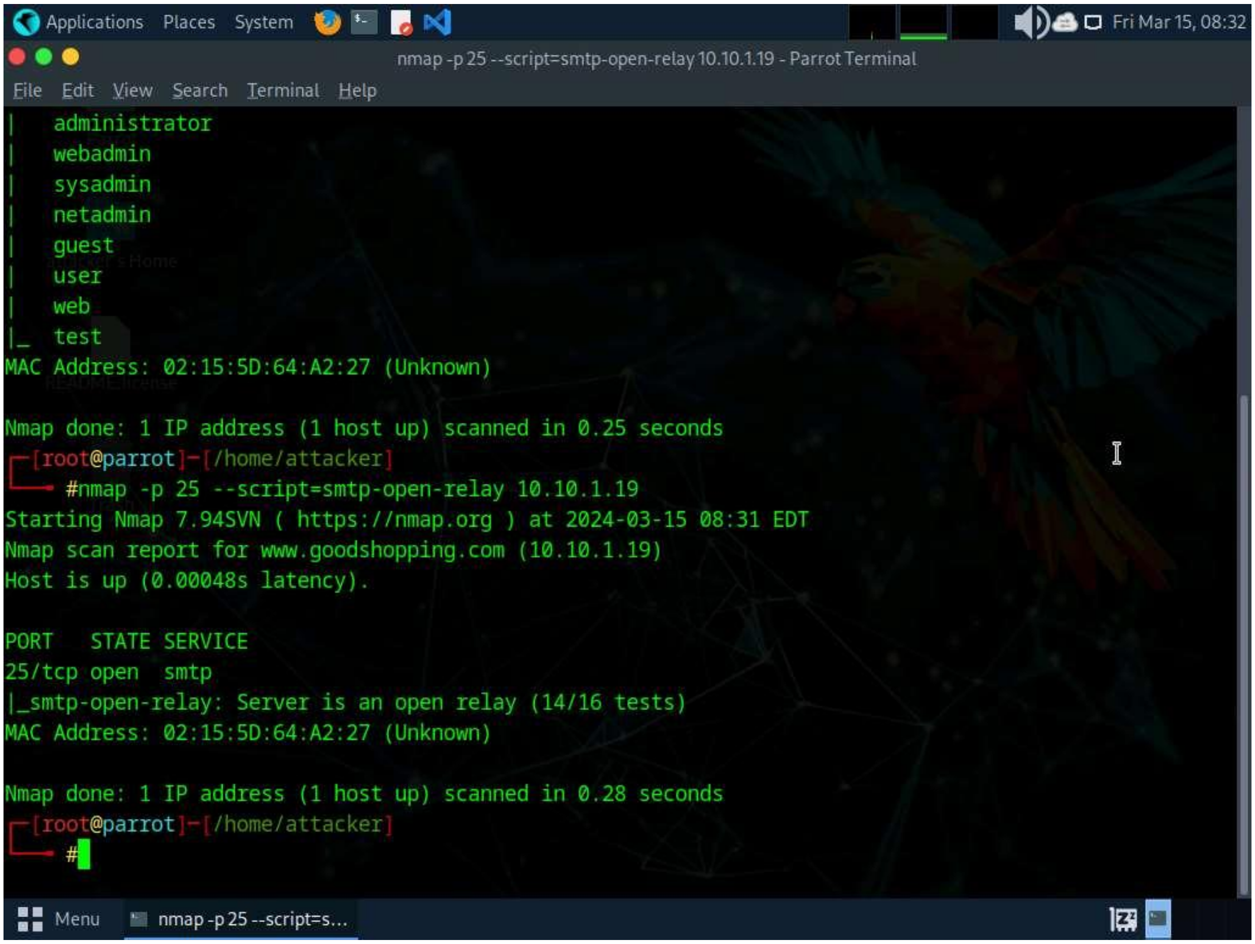


```
┌─[attacker@parrot]─[~]
└──╼ $sudo su
[sudo] password for attacker:
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap -p 25 --script=smtp-enum-users 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:30 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00058s latency).

PORT   STATE SERVICE
25/tcp open  smtp
| smtp-enum-users:
|   root
|   admin
|   administrator
|   webadmin
|   sysadmin
|   netadmin
|   guest
|   user
|   web
|_  test
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
┌─[root@parrot]─[/home/attacker]
```

4. Run **nmap -p 25 --script=smtp-open-relay [Target IP Address]** command (here, the target IP address is **10.10.1.19**).

-p: specifies the port, and **–script**: argument is used to run a given script (here, the script is **smtp-open-relay**).

5. The result appears displaying a list of open SMTP relays on the target machine (**10.10.1.19**), as shown in the screenshot below.

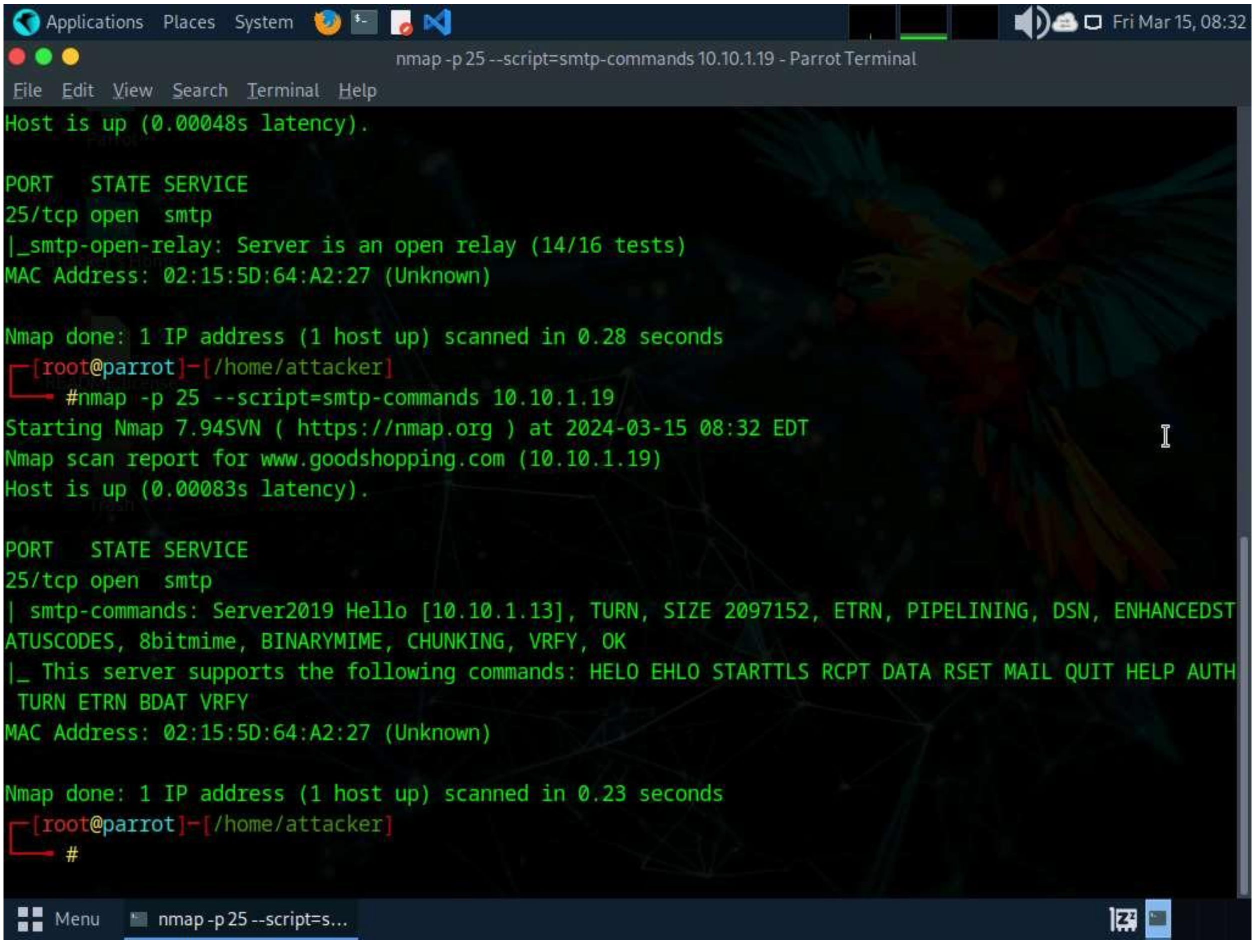

Applications Places System
Fri Mar 15, 08:32
nmap -p 25 --script=smtp-open-relay 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help
Menu
nmap -p 25 --script=s...

```
|   administrator
|   webadmin
|   sysadmin
|   netadmin
|   guest
|   user
|   web
|_  test
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap -p 25 --script=smtp-open-relay 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:31 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00048s latency).

PORT   STATE SERVICE
25/tcp open  smtp
|_smtp-open-relay: Server is an open relay (14/16 tests)
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

6. Run **nmap -p 25 --script=smtp-commands [Target IP Address]** command (here, the target IP address is **10.10.1.19**).

-p: specifies the port, and **–script**: argument is used to run a given script (here, the script is **smtp-commands**).

7. A list of all the SMTP commands available in the Nmap directory appears. You can further explore the commands to obtain more information on the target host.


Applications Places System
Fri Mar 15, 08:32
nmap -p 25 --script=smtp-commands 10.10.1.19 - Parrot Terminal
File Edit View Search Terminal Help
Menu
nmap -p 25 --script=s...

```
Host is up (0.00048s latency).

PORT   STATE SERVICE
25/tcp open  smtp
|_smtp-open-relay: Server is an open relay (14/16 tests)
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
┌─[root@parrot]─[/home/attacker]
└──╼ #nmap -p 25 --script=smtp-commands 10.10.1.19
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-15 08:32 EDT
Nmap scan report for www.goodshopping.com (10.10.1.19)
Host is up (0.00083s latency).

PORT   STATE SERVICE
25/tcp open  smtp
| smtp-commands: Server2019 Hello [10.10.1.13], TURN, SIZE 2097152, ETRN, PIPELINING, DSN, ENHANCEDST
ATUSCODES, 8bitmime, BINARYMIME, CHUNKING, VRFY, OK
|_ This server supports the following commands: HELO EHLO STARTTLS RCPT DATA RSET MAIL QUIT HELP AUTH
 TURN ETRN BDAT VRFY
MAC Address: 02:15:5D:64:A2:27 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
┌─[root@parrot]─[/home/attacker]
└──╼ #
```

8. Using this information, the attackers can perform password spraying attacks to gain unauthorized access to the user accounts.
9. This concludes the demonstration of SMTP enumeration using Nmap.
10. Close all open windows and document all the acquired information.

Question 4.6.1.1

Use the Nmap to perform SMTP enumeration to enumerate the list of all the possible mail users on the Windows Server 2019 machine. Enter the number of users enumerated on the target machine