SMTP:

1. How many commands are allowed on port 25?
   Your response: 10
   According to chatgpt

2. How many users can you enumerate via port 25?
   Your response: 7

```
┌──(kali㉿ntsapi)-[~]
└─$ nano users.txt

┌──(kali㉿ntsapi)-[~]
└─$ cat users.txt
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
news

┌──(kali㉿ntsapi)-[~]
└─$ smtp-user-enum -M VRFY -U users.txt -t 10.13.1.36
Starting smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Mode ..................... VRFY
Worker Processes ......... 5
Usernames file ........... users.txt
Target count ............. 1
Username count ........... 10
Target TCP port .......... 25
Query timeout ............ 5 secs
Target domain ............

######## Scan started at Mon Jun 17 05:31:06 2024 #########
10.13.1.36: root exists
10.13.1.36: daemon exists
10.13.1.36: bin exists
10.13.1.36: lp exists
10.13.1.36: sync exists
10.13.1.36: mail exists
10.13.1.36: news exists
######## Scan completed at Mon Jun 17 05:31:09 2024 #########
7 results.

10 queries in 3 seconds (3.3 queries / sec)
```

3. Send a mail with the email admin@metasploitable.localdomain to root@metasploitable.localdomain by connecting to the smtp server.
   Your response:

```
┌──(kali㉿ntsapi)-[~]
└─$ telnet 10.13.1.36 25
Trying 10.13.1.36 ...
Connected to 10.13.1.36.
Escape character is '^]'.
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
HELO local
250 metasploitable.localdomain
MAIL FROM:admin@metasploitable.localdomain
250 2.1.0 Ok
RCPT TO:root@metasploitable.localdomain
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: Check ME with ssh
After creating this email, use ssh to check if the email exist.
.
250 2.0.0 Ok: queued as 1F5F0CC91
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

4. Connect to ssh with msfadmin:msfadmin creds and check if you have sent the mail
   Your response:

```
┌──(kali㉿ntsapi)-[~]
└─$ ssh -o HostKeyAlgorithms=+ssh-rsa -o PubkeyAcceptedAlgorithms=+ssh-rsa msfadmin@10.13.1.36
msfadmin@10.13.1.36's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Tue Jun 18 03:47:50 2024 from 192.168.149.8
msfadmin@metasploitable:~$
```

```
msfadmin@metasploitable:~$ sudo grep "admin@metasploitable.localdomain" /var/log/mail.log
Jun 17 13:12:58 metasploitable postfix/qmgr[4580]: 9B4A2CC91: from=<admin@metasploitable.localdo
main>, size=436, nrcpt=1 (queue active)
Jun 18 02:47:44 metasploitable postfix/qmgr[4580]: 9FEDECC91: from=<admin@metasploitable.localdo
main>, size=427, nrcpt=1 (queue active)
Jun 18 03:08:07 metasploitable postfix/qmgr[4580]: 7347ECC91: from=<admin@metasploitable.localdo
main>, size=516, nrcpt=1 (queue active)
Jun 18 03:09:21 metasploitable postfix/qmgr[4580]: 12BBDCC91: from=<admin@metasploitable.localdo
main>, size=505, nrcpt=1 (queue active)
Jun 18 03:14:11 metasploitable postfix/qmgr[4580]: E59A2CC94: from=<admin@metasploitable.localdo
main>, size=481, nrcpt=1 (queue active)
Jun 18 03:17:48 metasploitable postfix/qmgr[4580]: 1F5F0CC91: from=<admin@metasploitable.localdo
main>, size=470, nrcpt=1 (queue active)
```