



```
[root@kali:~]# ./msfconsole
[*] msf6 v6.4.9-dev
[+] 2648 exploits - 1248 auxiliary - 423 post
[+] 1468 payloads - 47 encoders - 11 nops
[+] 9 evasion
Metasploit Documentation: https://docs.metasploit.com/
msf6 > search smtp_enum
Matching Modules
-----

| Name                             | Disclosure Date | Rank   | Check | Description                   |
|----------------------------------|-----------------|--------|-------|-------------------------------|
| auxiliary/scanner/smtp/smtp_enum |                 | normal | no    | SMTP User Enumeration Utility |


Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smtp/smtp_enum
msf6 > use auxiliary/scanner/smtp/smtp_enum
msf6 auxiliary(scanner/smtp/smtp_enum) > show options
Module options (auxiliary/scanner/smtp/smtp_enum):
-----

| Name      | Current Setting                                               | Required | Description                                                                                            |
|-----------|---------------------------------------------------------------|----------|--------------------------------------------------------------------------------------------------------|
| RHOSTS    |                                                               | yes      | The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html |
| REPORT    | 25                                                            | yes      | The target port (TCP)                                                                                  |
| THREADS   | 1                                                             | yes      | The number of concurrent threads (max one per host)                                                    |
| UNIXONLY  | true                                                          | yes      | Skip Microsoft banned servers when testing unix users                                                  |
| USER_FILE | /usr/share/metasploit-framework/data/wordlists/unix_users.txt | yes      | The file that contains a list of probable users accounts.                                              |


View the full module info with the info, or info -d command.
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOSTS 192.168.40.104
RHOSTS => 192.168.40.104
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit
[*] 192.168.40.104:25 - 192.168.40.104:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[*] 192.168.40.104:25 - 192.168.40.104:25 users found - backup, bin, anonymous, Aliased, ftp, games, mail, irc, libnntp, list, lpx, mail, min, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sym, vpopd
[*] 192.168.40.104:25 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

```
[kali㉿kali:~] $ nc 192.168.40.104 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
421 4.4.2 metasploitable.localdomain Error: timeout exceeded
[kali㉿kali:~] $ nc 192.168.40.104 25
220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY
501 5.5.4 Syntax: VRFY address
CLEAR
502 5.5.2 Error: command not recognized
^C
[*] 1468 payloads - 47 encoders - 11 nops
[*] 9 evasion
[kali㉿kali:~] $ nc 192.168.40.104 25 https://docs.metasploit.com/
VRFY220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
VRFY syslog
502 5.5.2 Error: command not recognized
^C
[*] Cleaning Modules

[kali㉿kali:~] $ nc 192.168.40.104 25
Disclosure Date Rank Gmetad Description
220 metasploitable.localdomain ESMTP Postfix (Ubuntu) 2019-06-01 normal No SMTP User Enumeration Utility
VRFY syslog arf/scanner/smtp/smtp_enum
252 2.0.0 syslog
VRFY asha
550 5.1.1 <asha>: Recipient address rejected: User unknown in local recipient table scanner/smtp/smtp_enum
421 4.4.2 metasploitable.localdomain Error: timeout exceeded
msf6 > use auxiliary/scanner/smtp/smtp_enum
[*] msf6 > show options
[kali㉿kali:~] msf6 > show options
Module Options (auxiliary/scanner/smtp/smtp_enum):
Name Current Setting Required Description
yes The target host(s), see https://docs.metasploit.com
yes The target port (TCP)
yes The number of threads (max min per host)
```

# Report : I got the ip from metasploitable2

then I used msfconsole, then I searched and enumerated on smtp, then I set my RHOSTS and I exploited. After that I opened another path to verify the user I got from exploiting.

