Scanner SMTP Auxiliary Modules a11y.text Scanner SMTP Auxiliary Modules smtp_enum a11y.text smtp_enum The SMTP Enumeration module will connect to a given mail server and use a wordlist to enumerate users that are present on the remote system. msf > use auxiliary/scanner/smtp/smtp_enum

msf auxiliary(smtp_enum) > show options

Module options (auxiliary/scanner/smtp/smtp_enum):

Name	Current Setting	Required	Description
RHOSTS		yes	The target address range or CIDR identifier
RPORT	25	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads
UNIXONLY	true	yes	Skip Microsoft bannered 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. Using the module is a simple matter of feeding it a host or range of hosts to scan and a wordlist containing usernames to enumerate. msf auxiliary(smtp_enum) > set RHOSTS 192.168.1.56

RHOSTS => 192.168.1.56

msf auxiliary(smtp_enum) > run

[*] 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)

[*] Domain Name: localdomain

[+] 192.168.1.56:25 - Found user: ROOT

[+] 192.168.1.56:25 - Found user: backup

[+] 192.168.1.56:25 - Found user: bin

[+] 192.168.1.56:25 - Found user: daemon

[+] 192.168.1.56:25 - Found user: distccd

[+] 192.168.1.56:25 - Found user: ftp

[+] 192.168.1.56:25 - Found user: games

[+] 192.168.1.56:25 - Found user: gnats

[+] 192.168.1.56:25 - Found user: irc

[+] 192.168.1.56:25 - Found user: libuuid

[+] 192.168.1.56:25 - Found user: list

[+] 192.168.1.56:25 - Found user: lp

[+] 192.168.1.56:25 - Found user: mail

[+] 192.168.1.56:25 - Found user: man

[+] 192.168.1.56:25 - Found user: news

[+] 192.168.1.56:25 - Found user: nobody

[+] 192.168.1.56:25 - Found user: postgres

[+] 192.168.1.56:25 - Found user: postmaster

[+] 192.168.1.56:25 - Found user: proxy

[+] 192.168.1.56:25 - Found user: root

[+] 192.168.1.56:25 - Found user: service

[+] 192.168.1.56:25 - Found user: sshd

[+] 192.168.1.56:25 - Found user: sync

[+] 192.168.1.56:25 - Found user: sys

[+] 192.168.1.56:25 - Found user: syslog

[+] 192.168.1.56:25 - Found user: user

[+] 192.168.1.56:25 - Found user: uucp

[+] 192.168.1.56:25 - Found user: www-data

[-] 192.168.1.56:25 - EXPN : 502 5.5.2 Error: command not recognized

[+] 192.168.1.56:25 Users found: ROOT, backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, news, nobody, postgres, postmaster, proxy, root, service, sshd, sync, sys, syslog, user, uucp, www-data

[*] 192.168.1.56:25 No e-mail addresses found.

[*] Scanned 1 of 1 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(smtp_enum) > Since the email username and system username are frequently the same, you can now use any enumerated users for further logon attempts against other network services. smtp_version a11y.text smtp_version Poorly configured or vulnerable mail servers can often provide an initial foothold into a network but prior to launching an attack, we want to fingerprint the server to make our targeting as precise as possible. The smtp_version module, as its name implies, will scan a range of IP addresses and determine the version of any mail servers it encounters. msf > use auxiliary/scanner/smtp/smtp_version

msf auxiliary(smtp_version) > show options

Module options:

Name	Current Setting	Required	Description
RHOSTS		yes	The target address range or CIDR identifier
RPORT	25	yes	The target port
THREADS	1	yes	The number of concurrent threads

```
msf auxiliary(smtp_version) > set RHOSTS 192.168.1.0/24

RHOSTS => 192.168.1.0/24

msf auxiliary(smtp_version) > set THREADS 254

THREADS => 254

msf auxiliary(smtp_version) > run


[*] 192.168.1.56:25 SMTP 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)\x0d\x0a

[*] Scanned 254 of 256 hosts (099% complete)

[*] Scanned 255 of 256 hosts (099% complete)

[*] Scanned 256 of 256 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(smtp_version) > Next Scanner SNMP Auxiliary Modules Prev Scanner SMB Auxiliary

Modules
```