Scanner FTP Auxiliary Modules a11y.text Scanner FTP Auxiliary Modules anonymous a11y.text anonymous The ftp/anonymous scanner will scan a range of IP addresses searching for FTP servers that allow anonymous access and determines where read or write permissions are allowed.

```
msf > use auxiliary/scanner/ftp/anonymous
msf auxiliary(anonymous) > show options
```

Module options:

Name	Current Setting	Required	Description
FTPPASS	mozilla@example.com	no	The password for the specified username
FTPUSER	anonymous	no	The username to authenticate as
RHOSTS		yes	The target address range or CIDR identifier
RPORT	21	yes	The target port
THREADS	1	yes	The number of concurrent threads Configuring the module is a simple matter of setting the IP range we wish to scan along with the number of concurrent threads and let it run. msf auxiliary(anonymous) > set RHOSTS 192.168.1.200-254

```
RHOSTS => 192.168.1.200-254
msf auxiliary(anonymous) > set THREADS 55
THREADS => 55
msf auxiliary(anonymous) > run

[*] 192.168.1.222:21 Anonymous READ (220 mailman FTP server (Version wu-2.6.2-5) ready.)
[*] 192.168.1.205:21 Anonymous READ (220 oracle2 Microsoft FTP Service (Version 5.0).)
[*] 192.168.1.215:21 Anonymous READ (220 (vsFTPd 1.1.3))
[*] 192.168.1.203:21 Anonymous READ/WRITE (220 Microsoft FTP Service)
```

[*] 192.168.1.227:21 Anonymous READ (220 srv2 Microsoft FTP Service (Version 5.0).)

[*] 192.168.1.204:21 Anonymous READ/WRITE (220 Microsoft FTP Service)

[*] Scanned 27 of 55 hosts (049% complete)

[*] Scanned 51 of 55 hosts (092% complete)

[*] Scanned 52 of 55 hosts (094% complete)

[*] Scanned 53 of 55 hosts (096% complete)

[*] Scanned 54 of 55 hosts (098% complete)

[*] Scanned 55 of 55 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(anonymous) > ftp_login a11y.text ftp_login The ftp_login auxiliary module will scan a range of IP addresses attempting to log in to FTP servers. msf > use auxiliary/scanner/ftp/ftp_login

msf auxiliary(ftp_login) > show options

Module options (auxiliary/scanner/ftp/ftp_login):

Name	Current Setting	Required	Description
BLANK_PASSWORDS	false	no	Try blank passwords for all users
BRUTEFORCE_SPEED	5	yes	How fast to bruteforce, from 0 to 5
DB_ALL_CREDS	false	no	Try each user/password couple stored in the current database
DB_ALL_PASS	false	no	Add all passwords in the current database to the list
DB_ALL_USERS	false	no	Add all users in the current database to the list
PASSWORD		no	A specific password to authenticate with

PASS_FILE /usr/share/wordlists/fasttrack.txt no File containing passwords, one per line

Proxies no A proxy chain of format type:host:port[,type:host:port][...]

RECORD_GUEST false no Record anonymous/guest logins to the database

RHOSTS yes The target address range or CIDR identifier

RPORT 21 yes The target port (TCP)

STOP_ON_SUCCESS false yes Stop guessing when a credential works for a host

THREADS 1 yes The number of concurrent threads

USERNAME no A specific username to authenticate as

USERPASS_FILE no File containing users and passwords separated by space, one pair per line

USER_AS_PASS false no Try the username as the password for all users

USER_FILE no File containing usernames, one per line

VERBOSE true yes Whether to print output for all attempts This module can take both wordlists and user-specified credentials in order to attempt to login. msf auxiliary(ftp_login) > set RHOSTS 192.168.69.50-254

RHOSTS => 192.168.69.50-254

msf auxiliary(ftp_login) > set THREADS 205

THREADS => 205

msf auxiliary(ftp_login) > set USERNAME msfadmin

USERNAME => msfadmin

msf auxiliary(ftp_login) > set PASSWORD msfadmin

PASSWORD => msfadmin

```
msf auxiliary(ftp_login) > set VERBOSE false
VERBOSE => false
msf auxiliary(ftp_login) > run

[*] 192.168.69.51:21 - Starting FTP login sweep
[*] 192.168.69.50:21 - Starting FTP login sweep
[*] 192.168.69.52:21 - Starting FTP login sweep
...snip...
[*] Scanned 082 of 205 hosts (040% complete)
[*] 192.168.69.135:21 - FTP Banner: '220 ProFTPD 1.3.1 Server (Debian)
[::ffff:192.168.69.135]\x0d\x0a'
[*] Scanned 204 of 205 hosts (099% complete)
[+] 192.168.69.135:21 - Successful FTP login for 'msfadmin':'msfadmin'
[*] 192.168.69.135:21 - User 'msfadmin' has READ/WRITE access
[*] Scanned 205 of 205 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ftp_login) > As we can see, the scanner successfully logged in to one of our targets
with the provided credentials. ftp_version a11y.text ftp_version The ftp_version module simply scans
a range of IP addresses and determines the version of any FTP servers that are running. msf > use
auxiliary/scanner/ftp/ftp_version
msf auxiliary(ftp_version) > show options

Module options:

   Name     Current Setting      Required  Description
   ----     ---------------      --------  -----------
```

FTPPASS mozilla@example.com no The password for the specified username

FTPUSER anonymous no The username to authenticate as

RHOSTS yes The target address range or CIDR identifier

RPORT 21 yes The target port

THREADS 1 yes The number of concurrent threads To setup the module, we just set our RHOSTS and THREADS values and let it run. msf auxiliary(ftp_version) > set RHOSTS 192.168.1.200-254

RHOSTS => 192.168.1.200-254

msf auxiliary(ftp_version) > set THREADS 55

THREADS => 55

msf auxiliary(ftp_version) > run

[*] 192.168.1.205:21 FTP Banner: '220 oracle2 Microsoft FTP Service (Version 5.0).\x0d\x0a'

[*] 192.168.1.204:21 FTP Banner: '220 Microsoft FTP Service\x0d\x0a'

[*] 192.168.1.203:21 FTP Banner: '220 Microsoft FTP Service\x0d\x0a'

[*] 192.168.1.206:21 FTP Banner: '220 oracle2 Microsoft FTP Service (Version 5.0).\x0d\x0a'

[*] 192.168.1.216:21 FTP Banner: '220 (vsFTPd 2.0.1)\x0d\x0a'

[*] 192.168.1.211:21 FTP Banner: '220 (vsFTPd 2.0.5)\x0d\x0a'

[*] 192.168.1.215:21 FTP Banner: '220 (vsFTPd 1.1.3)\x0d\x0a'

[*] 192.168.1.222:21 FTP Banner: '220 mailman FTP server (Version wu-2.6.2-5) ready.\x0d\x0a'

[*] 192.168.1.227:21 FTP Banner: '220 srv2 Microsoft FTP Service (Version 5.0).\x0d\x0a'

[*] 192.168.1.249:21 FTP Banner: '220 ProFTPD 1.3.3a Server (Debian) [::ffff:192.168.1.249]\x0d\x0a'

[*] Scanned 28 of 55 hosts (050% complete)

[*] 192.168.1.217:21 FTP Banner: '220 ftp3 FTP server (Version wu-2.6.0(1) Mon Feb 28 10:30:36 EST 2000) ready.\x0d\x0a'

[*] Scanned 51 of 55 hosts (092% complete)

[*] Scanned 52 of 55 hosts (094% complete)

[*] Scanned 53 of 55 hosts (096% complete)

[*] Scanned 55 of 55 hosts (100% complete)

[*] Auxiliary module execution completed

msf auxiliary(ftp_version) > Next Scanner HTTP Auxiliary Modules Prev Scanner Discovery Auxiliary Modules