

smtp-user-enum

Username guessing tool primarily for use against the default Solaris SMTP service. Can use either EXPN, VRFY or RCPT TO.

Installed size: 98 KB

How to install: sudo apt install smtp-user-enum

Dependencies:

- libio-socket-ip-perl
- libsocket-perl
- perl

```
root@kali:~/# smtp-user-enum -h
```

```
smtp-user-enum v1.2 ( http://pentestmonkey.net/tools/smtp-user-enum )
```

Usage: smtp-user-enum [options] (-u username | -U file-of-usernames) (-t host | -T file-of-targets)

options are:

-m n Maximum number of processes (default: 5)

-M mode Method to use for username guessing EXPN, VRFY or RCPT (default: VRFY)

-u user Check if user exists on remote system

-f addr MAIL FROM email address. Used only in "RCPT TO" mode (default: user@example.com)

-D dom Domain to append to supplied user list to make email addresses (Default: none)

Use this option when you want to guess valid email addresses instead of just usernames

e.g. "-D example.com" would guess foo@example.com, bar@example.com, etc.
Instead of

simply the usernames foo and bar.

-U file File of usernames to check via smtp service

-t host Server host running smtp service

-T file File of hostnames running the smtp service

-p port TCP port on which smtp service runs (default: 25)

-d Debugging output

-w n Wait a maximum of n seconds for reply (default: 5)

-v Verbose

-h This help message

Also see `smtp-user-enum-user-docs.pdf` from the `smtp-user-enum` tar ball.

Examples:

```
$ smtp-user-enum -M VRFY -U users.txt -t 10.0.0.1
```

```
$ smtp-user-enum -M EXPN -u admin1 -t 10.0.0.1
```

```
$ smtp-user-enum -M RCPT -U users.txt -T mail-server-ips.txt
```

```
$ smtp-user-enum -M EXPN -D example.com -U users.txt -t 10.0.0.1
```