smtp-user-enum

Username guessing tool primarily for use against the default Solaris SMTP service. Can use either EXPN, VRFY or RCPT TO.  Recent changes are detailed in the [CHANGELOG](http://pentestmonkey.net/tools/tools/smtp-user-enum/CHANGELOG).

Download smtp-user-enum v1.2 [here](http://pentestmonkey.net/tools/smtp-user-enum/smtp-user-enum-1.2.tar.gz).

MD5 and SHA1 checksums are the packages can be downloaded.  They’re based on the package name (below v.v represents the version, e.g. 1.1):

http://pentestmonkey.net/tools/smtp-user-enum/smtp-user-enum-v.v-beta.tar.gz.md5

http://pentestmonkey.net/tools/smtp-user-enum/smtp-user-enum-v.v-beta.tar.gz.sha1

User documentation is also available in [PDF](http://pentestmonkey.net/tools/smtp-user-enum/smtp-user-enum-user-docs.pdf) format.

smtp-user-enum User Documentation

Contents

* Overview
* Installation
* Usage
* Some Examples
  + Using the SMTP VRFY Command
  + Using the SMTP EXPN Command
  + Using the SMTP RCPT TO Command
  + Enumerating Email Addresses Instead of Usernames
* License

Overview

smtp-user-enum is a tool for enumerating OS-level user accounts on Solaris via the SMTP service (sendmail). Enumeration is performed by inspecting the responses to VRFY, EXPN and RCPT TO commands. It could be adapted to work against other vulnerable SMTP daemons, but this hasn’t been done as of v1.0.

Installation

smtp-user-enum is just a stand alone PERL script, so installation is as simple as copying it to your path (e.g. /usr/local/bin). It has only been tested under Linux so far.

It depends on the following PERL modules which you may need to install first:

* Socket
* IO::Handle
* IO::Select
* IO::Socket::INET
* Getopt::Std

If you have PERL installed, you should be able to install the modules from CPAN:

# perl -MCPAN -e shell

cpan> install Getopt::Std

Usage

smtp-user-enum simply needs to be passed a list of users and at least one target running an SMTP service.

smtp-user-enum v1.0 ( http://pentestmonkey.net/tools/smtp-user-enum )

Usage: smtp-user-enum.pl [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 From email address to use for "RCPT TO" guessing (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

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

-v Verbose

-h This help message

Some Examples

For all of the examples below we need a list of potential usernames. The following output demostrates the format for this list:

$ head users.txt

root

bin

daemon

adm

lp

sync

shutdown

halt

mail

news

Using the SMTP VRFY Command

The output below shows how the SMTP server responds differently to VRFY requests for valid and invalid users. It is recommended that a manual check like the following is carried out before running smtp-user-enum. Obviously the tool won’t work if the server doesn’t respond differently to requests for valid and invalid users.

$ telnet 10.0.0.1 25

Trying 10.0.0.1...

Connected to 10.0.0.1.

Escape character is '^]'.

220 myhost ESMTP Sendmail 8.9.3

HELO

501 HELO requires domain address

HELO x

250 myhost Hello [10.0.0.99], pleased to meet you

VRFY root

250 Super-User <root@myhost>

VRFY blah

550 blah... User unknown

To use smtp-user-enum to enumerate valid usernames using the VRFY command, first prepare a list of usernames (users.txt) and run the tool as follows:

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

Starting smtp-user-enum v1.0 ( http://pentestmonkey.net/tools/smtp-user-enum )

----------------------------------------------------------

| Scan Information |

----------------------------------------------------------

Mode ..................... VRFY

Worker Processes ......... 5

Usernames file ........... users.txt

Target count ............. 1

Username count ........... 47

Target TCP port .......... 25

Query timeout ............ 5 secs

Relay Server ............. Not used

######## Scan started at Sun Jan 21 18:01:50 2007 #########

root@10.0.0.1: Exists

bin@10.0.0.1: Exists

daemon@10.0.0.1: Exists

lp@10.0.0.1: Exists

adm@10.0.0.1: Exists

uucp@10.0.0.1: Exists

postmaster@10.0.0.1: Exists

nobody@10.0.0.1: Exists

ftp@10.0.0.1: Exists

######## Scan completed at Sun Jan 21 18:01:50 2007 #########

9 results.

47 queries in 1 seconds (47.0 queries / sec)

It’s worth noting that postmaster is not actually a valid OS-level user account – it’s a mail alias.

Using the SMTP EXPN Command

The output below shows how the SMTP server responds differently to EXPN requests for valid and invalid users.

$ telnet 10.0.0.1 25

Trying 10.0.0.1...

Connected to 10.0.0.1.

Escape character is '^]'.

220 myhost ESMTP Sendmail 8.9.3

HELO

501 HELO requires domain address

HELO x

250 myhost Hello [10.0.0.99], pleased to meet you

EXPN root

250 Super-User <root@myhost>

EXPN blah

550 blah... User unknown

To use smtp-user-enum to enumerate valid usernames using the VRFY command, first prepare a list of usernames (users.txt) and run the tool as follows (unsurprisingly, we get the same results as above):

$ smtp-user-enum.pl -M EXPN -U users.txt -t 10.0.0.1

Starting smtp-user-enum v1.0 ( http://pentestmonkey.net/tools/smtp-user-enum )

----------------------------------------------------------

| Scan Information |

----------------------------------------------------------

Mode ..................... EXPN

Worker Processes ......... 5

Usernames file ........... users.txt

Target count ............. 1

Username count ........... 47

Target TCP port .......... 25

Query timeout ............ 5 secs

Relay Server ............. Not used

######## Scan started at Sun Jan 21 18:01:50 2007 #########

root@10.0.0.1: Exists

bin@10.0.0.1: Exists

daemon@10.0.0.1: Exists

lp@10.0.0.1: Exists

adm@10.0.0.1: Exists

uucp@10.0.0.1: Exists

postmaster@10.0.0.1: Exists

nobody@10.0.0.1: Exists

ftp@10.0.0.1: Exists

######## Scan completed at Sun Jan 21 18:01:50 2007 #########

9 results.

47 queries in 1 seconds (47.0 queries / sec)

Using the SMTP RCPT TO Command

The output below shows how the SMTP server responds differently to RCPT TO requests for valid and invalid users. This is often to the most useful technique as VRFY and EXPN are often disabled to prevent username enumeration.

$ telnet 10.0.0.1 25

Trying 10.0.0.1...

Connected to 10.0.0.1.

Escape character is '^]'.

220 myhost ESMTP Sendmail 8.9.3

HELO

501 HELO requires domain address

HELO x

250 myhost Hello [10.0.0.99], pleased to meet you

MAIL FROM:root

250 root... Sender ok

RCPT TO:root

250 root... Recipient ok

RCPT TO: blah

550 blah... User unknown

To use smtp-user-enum to enumerate valid usernames using the RCPT TO command, first prepare a list of usernames (users.txt) and run the tool as follows (again, the results are the same as above):

$ smtp-user-enum.pl -M RCPT -U users.txt -t 10.0.0.1

Starting smtp-user-enum v1.0 ( http://pentestmonkey.net/tools/smtp-user-enum )

----------------------------------------------------------

| Scan Information |

----------------------------------------------------------

Mode ..................... RCPT

Worker Processes ......... 5

Usernames file ........... users.txt

Target count ............. 1

Username count ........... 47

Target TCP port .......... 25

Query timeout ............ 5 secs

Relay Server ............. Not used

######## Scan started at Sun Jan 21 18:01:50 2007 #########

root@10.0.0.1: Exists

bin@10.0.0.1: Exists

daemon@10.0.0.1: Exists

lp@10.0.0.1: Exists

adm@10.0.0.1: Exists

uucp@10.0.0.1: Exists

postmaster@10.0.0.1: Exists

nobody@10.0.0.1: Exists

ftp@10.0.0.1: Exists

######## Scan completed at Sun Jan 21 18:01:50 2007 #########

9 results.

47 queries in 1 seconds (47.0 queries / sec)

Enumerating Email Addresses Instead of Usernames

Version 1.1 adds support for optionally appending a domain name to the end of each username:

$ ./smtp-user-enum.pl -D example.com -M RCPT -U users.txt -t 10.0.0.1

Starting smtp-user-enum v1.1 ( http://pentestmonkey.net/tools/smtp-user-enum )

 ----------------------------------------------------------

|                   Scan Information                       |

----------------------------------------------------------

Mode ..................... RCPT

Worker Processes ......... 5

Usernames file ........... users.txt

Target count ............. 1

Username count ........... 47

Target TCP port .......... 25

Query timeout ............ 5 secs

Target domain ............ example.com

######## Scan started at Wed Jan 16 20:43:58 2008 #########

10.0.0.1: bin@example.com exists

10.0.0.1: daemon@example.com exists

10.0.0.1: root@example.com exists

10.0.0.1: postmaster@example.com exists

######## Scan completed at Wed Jan 16 20:43:58 2008 #########

4 results.

7 queries in 1 seconds (47.0 queries / sec)

License

This tool may be used for legal purposes only. Users take full responsibility for any actions performed using this tool. The author accepts no liability for damage caused by this tool. If these terms are not acceptable to you, then do not use this tool.

In all other respects the GPL version 2 applies:

This program is free software; you can redistribute it and/or modify

it under the terms of the GNU General Public License version 2 as

published by the Free Software Foundation.

This program is distributed in the hope that it will be useful,

but WITHOUT ANY WARRANTY; without even the implied warranty of

MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the

GNU General Public License for more details.

You should have received a copy of the GNU General Public License along

with this program; if not, write to the Free Software Foundation, Inc.,

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.