finger-user-enum User Documentation

pentestmonkey@pentestmonkey.net

21 January 2007

Contents

1 Overview

finger-user-enum is a tool for enumerating OS-level user accounts via the finger service. As of release v1.0 it is known to work against the default Solaris daemon. It may not yet work against all daemons since there is no defined format for the data returned by the finger service.

2 Installation

finger-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
```

3 Usage

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

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

Usage: finger-user-enum.pl [options] (-u username|-U users.txt) (-t host|-T ips.txt)

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 finger service
        -t host  Server host running finger service
        -T file  File of hostnames running the finger service
        -r host  Relay.  Intermediate server which allows relaying of finger requests.
        -p port  TCP port on which finger service runs (default: 79)
        -d       Debugging output
        -s n     Wait a maximum of n seconds for reply (default: 5)
        -v       Verbose
        -h       This help message
```

4 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
```

4.1 Normal Usage

The output below shows how the finger daemon responds differently to valid and invalid usernames:

```
$ telnet 10.0.0.1 79
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
root
Login       Name               TTY         Idle    When    Where
root     Super-User            console     2:05 Wed 07:23
Connection closed by foreign host.

$ telnet 10.0.0.1 79
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
blah
Login       Name               TTY         Idle    When    Where
blah                  ???
Connection closed by foreign host.
```

finger-user-enum attempts to automatically parse the results returned by the finger daemon and report only users which exist.

Note: If you ever need to modify the pattern-matching within finger-user-enum (e.g. to support a different finger daemon), you'll need to base the patterns on positive and negative result like those found above.

Here's an example of the most common usage of the tool:

```
$ ./finger-user-enum.pl -U users.txt -t 10.0.0.1
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Worker Processes ......... 5
Usernames file ........... users.txt
Target count ............. 1
Username count ........... 47
Target TCP port .......... 79
Query timeout ............ 5 secs
Relay Server ............. Not used

######## Scan started at Sun Jan 21 19:44:22 2007 #########
root@10.0.0.1: root     Super-User            console     2:03 Wed 07:23 ..
bin@10.0.0.1: bin             ???            pts/1        <Dec 21 13:04> 10.0.0.99
daemon@10.0.0.1: daemon          ???                        < .  .  .  . >..
adm@10.0.0.1: adm      Admin                                < .  .  .  . >..
lp@10.0.0.1: lp       Line Printer Admin                   < .  .  .  . >..
uucp@10.0.0.1: uucp Admin                             < .  .  .  . >..
nobody@10.0.0.1: nobody4  SunOS 4.x Nobody                  < .  .  .  . >..
```

```
ftp@10.0.0.1: ftp      Anonymous FTPUser     674          <Aug 11 14:22> 10.0.0.99
######## Scan completed at Sun Jan 21 19:44:23 2007 #########
8 results.

47 queries in 1 seconds (47.0 queries / sec)
```

4.2 Relaying Queries

It is also possible to use some finger daemons as a relay (i.e. to ask the finger daemon to finger a user on another host). The following output shows how you'd get the finger daemon on 10.0.0.1 to finger users on 10.0.0.2:

```
$ telnet 10.0.0.1 79
Trying 10.0.0.1...
Connected to 10.0.0.1.
Escape character is '^]'.
root@10.0.0.2
[10.0.0.2]
Login       Name                TTY         Idle    When    Where
root     Super-User             console     2:12 Wed 07:23
Connection closed by foreign host.
```

Note that your host won't send any traffic directly to 10.0.0.2 during this request. Queries to 10.0.0.2 originate from 10.0.0.1.

If you need to relay your queries (and the daemon allows relaying) here is the syntax for finger-user-enum:

```
$ ./finger-user-enum.pl -U users.txt -t 10.0.0.2 -r 10.0.0.1
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

 ----------------------------------------------------------
|                   Scan Information                       |
 ----------------------------------------------------------

Worker Processes ......... 5
Usernames file ........... users.txt
Target count ............. 1
Username count ........... 47
Target TCP port .......... 79
Query timeout ............ 5 secs
Relay Server ............. 10.0.0.1

######## Scan started at Sun Jan 21 19:44:29 2007 #########
root@10.0.0.2: root     Super-User            console     2:03 Wed 07:23 ..
bin@10.0.0.2: bin             ???            pts/1        <Dec 21 13:04> 10.0.0.99
lp@10.0.0.2: lp       Line Printer Admin                 < .  .  .  . >..
daemon@10.0.0.2: daemon          ???                        < .  .  .  . >..
adm@10.0.0.2: adm      Admin                                < .  .  .  . >..
uucp@10.0.0.2: uucp Admin                              < .  .  .  . >..
nobody@10.0.0.2: nobody4  SunOS 4.x Nobody                    < .  .  .  . >..
ftp@10.0.0.2: ftp      Anonymous FTPUser     674          <Aug 11 14:22> 10.0.0.99
######## Scan completed at Sun Jan 21 19:44:31 2007 #########
8 results.
```

```
47 queries in 2 seconds (23.5 queries / sec)
```

5 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.
```