ident-user-enum

ident-user-enum is a simple PERL script to query the ident service (113/TCP) in order to determine the owner of the process listening on each TCP port of a target system.

This can help to prioritise target service during a pentest (you might want to attack services running as root first).  Alternatively, the list of usernames gathered can be used for password guessing attacks on other network services.

Download

[ident-user-enum v1.0 tar ball](http://pentestmonkey.net/tools/ident-user-enum/ident-user-enum-1.0.tar.gz)

Install

The INSTALL file in the distribution tarball contains the instructions you need to get up and running:

$ cat INSTALL

1. Install the dependencies

Install PERL using your package manager.

Install the following PERL modules:

\* IO::Socket::INET

\* Net::Ident

These may be available through your package manager.  If not, then

install them from CPAN:

# perl -MCPAN -e shell

# install IO::Socket::INET

# install Net::Ident

2. "Install" ident-user-enum.pl

It's just a PERL script, so no installation is necessary, but probably

want to copy it into your path and set appropriate permissions:

# install -o root -m 0755 ident-user-enum.pl /usr/local/bin/

Running

$ ./ident-user-enum.pl 10.0.0.1 21 80 113 443

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

10.0.0.1:21    <unknown>

10.0.0.1:80    www-run

10.0.0.1:113   root

10.0.0.1:443  www-run

Note that some ident services lie, e.g. return “nobody” for all services.  This is good from a security perspective, but bad for you as a pentester.

You should only get an “<unknown>” response if the target port is closed or firewalled.