Table Of Contents

nixCraft: Linux Tips, Hacks, Tutorials, And Ideas In Blog Format
http://www.cyberciti.biz/

How to: Log connections made by user for any service under Linux

Posted by Vivek Gite <vivek@nixcraft.com>

[1]

Q. I'd like to log information about selected incoming and outgoing TCP/IP connections to a log file. For example, log connection made by user "tom" for the service ftp or ssh? How do I configure Linux to log connections?

A. You can write a perl or shell script to monitor and log all connection. However, there is an easy way out. Use the tool called tcpspy. As name suggest it can spy on users. tcpspy logs information about selected incoming and outgoing TCP/IP connections to syslog. The following information is logged:

a) Username
b) Local address and port
c) Remote address, port, and optionally the filename of the executable

It only support the IPv4 protocol.

Install tcpspy

Use apt-get or yup or ports collection:

```
apt-get install tcpspy
```

Configuration file

The default configuration file is located at /etc/tcpspy.rules.

Sample configuration

Open /etc/tcpspy.rules file:

```
# vi /etc/tcpspy.rules
```

To log connections made by user "tom" for the service "ssh", enter:

```
user "jom" and rport "ssh"
```

You can also enter above rule at command prompt:

```
# tcpspy -e 'user "tom" and rport "ssh"'
```

Log connections made by user "tom" for the service "ftp", enter:

```
# tcpspy -e 'user "tom" and rport "ftp"'
```

Following will log connections made by users "vivek" and "tom" to remote port 25 (SMTP) on machines not on a "intranet" 10.0.0.0/24:

```
# tcpspy -e 'not raddr 10.0.0.0/255.0.0.0 and rport 25 and (user "vivek" or user "tom")'
```

Log connections made by /usr/bin/ftp:

```
# tcpspy -e 'exe "/usr/bin/ftp"'
```

OR combine monitoring for ftp and telnet binary:

```
# tcpspy -e 'exe "/usr/bin/ftp and /usr/bin/telnet"'
```

The -e option is used to set a rule. It can be used to log information about connections matching this rule, overriding the default of logging all connections.

tcpspy rules

- **user "username"** - True if the local username / user initiating or accepting the connection has the effective user id uid.
- **rport "port"** - It Compares the port number of the remote end of the connection i.e outgoing connections
- **lport "port"** - True if the local end of the connection has port number port.
- **exe "pattern"** - True if the full filename (including directory) of the executable that created/accepted the connection matches pattern, a UNIX (glob) style wildcard pattern.
- or - Define logical or (expr1 or expr2)
- and - Define logical and (expr1 and expr2)
- not - Define logical not (not user "vivek")

Refer to tcpspy man page for more syntax option.

```
$ man tcpspy
```