Linux Incident Response - using lsof to check network connections

Taz Wake | Halkyn Consulting Ltd | Originally published 2023-10-24

The command in Linux stands for "list open files." It is a powerful and versatile utility that provides information about files and processes that are currently opened or in use by the operating system. This includes regular files, directories, network sockets, block special files, character special files, and even files opened by processes for executing commands. works by querying the kernel and the filesystem, which is a virtual filesystem in Linux providing detailed information about running processes and their resources.

When it comes to network connections, can be invaluable for forensic investigators. By utilizing various command line arguments, investigators can determine what network connections exist on a system, providing crucial insights into potential malicious activities, unauthorized access, or suspicious communication with external entities.

To find network connections using , investigators can utilize the following command line arguments:

1. **List all network connections:** The most basic usage of without any arguments, will list all open files, including network connections.

This can be very noisy though with around 200,000 results being fairly normal. The output looks something like this:

As you can see, it's difficult to read and will quickly fill up a terminal window.

The range of fields returned can also vary, but you should expect to see headings such as:

- **COMMAND:** This field shows the name of the command or the process associated with the open file or resource.
- **PID:** The Process IDentifier is the unique numerical identifier assigned to a running process by the operating system.
- **USER:** This field displays the username of the owner of the process that has the file open.
- **FD:** File Descriptor represents how the file is opened. It includes file descriptors like cwd (current working directory), txt (text file), mem (memory-mapped file), etc.
- **TYPE:** Indicates the type of the node associated with the file. It can be REG (regular file), DIR (directory), FIFO (named pipe), etc.
- **DEVICE:** The device number where the file resides, typically major and minor numbers identifying a device in the directory.

- **SIZE/OFF:** For regular files, this shows the file's size in bytes. For block devices, it shows block size. For network connections, it displays the socket's send and receive buffer size.
- **NODE:** This field shows the node number of the file or the resource. In the case of regular files, it can help identify the inode number.
- **NAME:** The file name or the resource name associated with the open file.

2. **Show network connections for a specific process:** Investigators can use -p as an argument, followed by a process ID to display network connections related to a specific process.

3. **List network connections for a specific user:** Using the option followed by a username, investigators can filter network connections based on a specific user.

4. **Show network connections using a specific port:** Investigators can identify processes that are using a specific port by specifying the port number.

Forensic analysts can use these commands when investigating a potential security breach to identify open network connections, their associated processes, and the files or resources they are interacting with.

For example, if a suspicious process is identified, running provides detailed information about the network connections made by that process. If the investigator wants to understand which users are involved in network activities, can provide relevant details.

Additionally, pinpointing network connections on a specific port (like port 80 for HTTP traffic) can help identify potential communication channels with external servers, shedding light on the nature of the network activity and facilitating a more comprehensive forensic analysis.

If you want to know more about this and practice your Linux DFIR skills against real-world evidence, then have a look at https://sans.org/for577, the Linux Incident Response and Threat Hunting course provided by SANS Institute / SANS Digital Forensics and Incident Response

---

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858