

Forum:[Hack Forums](#)

Thread: [How I Approach a Basic Linux Security Investigation](#)

FatCat - October 6, 2026, 7:40 pm

When learning cybersecurity, I think it is useful to have a simple and repeatable process instead of immediately jumping into complex tools.

Here is a basic workflow I use when investigating suspicious activity on a Linux system.

1. CHECK THE NETWORK

First, I want to understand what interfaces and routes exist:

```
ip addr
ip route
```

Then I check active connections and listening services:

```
sudo ss -tulpn
sudo ss -tunap
```

This can help identify unexpected listening ports or connections to unfamiliar addresses.

2. IDENTIFY THE PROCESS

If I find a suspicious connection, I try to determine which process created it.

For example:

```
sudo lsof -i
```

Or for a specific port:

```
sudo lsof -i :PORT
```

I can then examine the process:

```
ps aux | grep PROCESS_NAME
```

Important information includes the process name, PID, user and command line.

3. CHECK THE LOGS

Logs can provide additional context about what happened.

For SSH:

```
journalctl -u ssh
```

For recent events:

```
journalctl -u ssh --since "1 hour ago"
```

I can also search for failed authentication attempts:

```
journalctl -u ssh | grep -i "failed"
```

When investigating an incident, timestamps are especially useful because they allow different events to be correlated.

4. INVESTIGATE SUSPICIOUS FILES

If a suspicious executable or script is discovered, I would first identify the file:

```
file suspicious_file
```

Then calculate its SHA-256 hash:

```
sha256sum suspicious_file
```

I can also inspect readable strings:

```
strings suspicious_file
```

The hash can be compared against known information from an authorized threat intelligence source.

5. CHECK DNS ACTIVITY

If the system is communicating with an unfamiliar domain or IP, DNS information can provide useful context.

For example:

```
dig example.com
```

Reverse lookup:

```
dig -x IP_ADDRESS
```

Network traffic can also be examined with tcpdump:

```
sudo tcpdump -i eth0 port 53
```

6. DOCUMENT EVERYTHING

One of the most important parts of an investigation is documenting what was observed.

I would record:

- Date and time
- Source IP
- Destination IP
- Ports
- Username
- Process/PID
- File path
- File hash
- Relevant logs
- DNS activity
- Initial hypothesis
- Evidence collected
- Final conclusion

FINAL THOUGHT

The goal is not to assume that every unusual event is malicious.

A process, open port or external connection may be completely legitimate.

The purpose of the investigation is to collect enough evidence to determine what is happening and whether the activity is expected.

This basic workflow can also be expanded with tools such as Wireshark, Nmap, SIEM platforms and threat intelligence sources.

What is the first thing you normally check when you notice something suspicious on a Linux machine?

Raijin - October 6, 2026, 7:52 pm

Nicely written and explained.