

Forum:[Hack Forums](#)

Thread: [Linux Security Cheat Sheet SOC & Network Analysis](#)

FatCat - October 6, 2026, 7:32 pm

Linux SECURITY CHEAT SHEET
SOC & NETWORK ANALYSIS

A practical Linux security reference for beginners learning SOC analysis, network investigation and incident response.

CONTENTS

- 01. Network Interfaces
- 02. Listening Ports
- 03. Processes
- 04. Network Connections
- 05. DNS Investigation
- 06. SSH Log Analysis
- 07. Log Searching
- 08. Traffic Capture
- 09. File Hashing
- 10. Investigation Workflow
- 11. SOC Scenarios
- 12. Investigation Checklist
- 13. Quick Reference

=====
1. NETWORK INTERFACES
=====

Show network interfaces and IP addresses:

```
ip addr
```

Show routing table:

```
ip route
```

Show DNS configuration:

```
resolvectl status
```

=====
2. LISTENING PORTS
=====

Show listening TCP/UDP ports:

`sudo ss -tulpn`

Show active connections:

`sudo ss -tunap`

Useful for identifying unexpected services and connections.

3. PROCESSES

List running processes:

`ps aux`

Show processes in real time:

`top`

Find a specific process:

`ps aux | grep PROCESS_NAME`

4. NETWORK CONNECTIONS

Show processes using network connections:

`sudo lsof -i`

Check a specific port:

`sudo lsof -i :22`

5. DNS INVESTIGATION

DNS lookup:

`dig example.com`

Short result:

`dig +short example.com`

Reverse DNS:

dig -x IP_ADDRESS

6. SSH LOG ANALYSIS

View SSH logs:

```
journalctl -u ssh
```

Recent SSH events:

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

Find failed authentication:

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

Find invalid users:

```
journalctl -u ssh | grep -i "invalid user"
```

7. LOG SEARCHING

Search a log:

```
grep -i "failed" /var/log/auth.log
```

Search recursively:

```
grep -Rni "keyword" /var/log/
```

Last 50 lines:

```
tail -n 50 /var/log/auth.log
```

Follow a log in real time:

```
tail -f /var/log/auth.log
```

8. TRAFFIC CAPTURE

Capture traffic:

```
sudo tcpdump -i eth0
```

Capture DNS:

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

Capture HTTP:

```
sudo tcpdump -i eth0 port 80
```

Capture traffic from a host:

```
sudo tcpdump -i eth0 host IP_ADDRESS
```

9. FILE HASHING

SHA256:

```
sha256sum FILE
```

MD5:

```
md5sum FILE
```

Hashes help verify file integrity and identify known files.

10. INVESTIGATION WORKFLOW

When investigating suspicious activity:

1. Identify the suspicious IP/domain.
2. Check active network connections.
3. Identify the associated process.
4. Check the process owner.
5. Review authentication/system logs.
6. Determine when activity started.
7. Calculate hashes of suspicious files.
8. Correlate events with other logs.
9. Document your findings.

11. PRACTICAL SOC SCENARIOS

SCENARIO 1 — SSH BRUTE-FORCE

Check recent SSH activity:

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

Search failed attempts:

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

Questions:

- Which IP generated most attempts?
- Which usernames are being targeted?
- When did the activity begin?
- Were any successful logins made?

SCENARIO 2 — UNKNOWN LISTENING SERVICE

List listening services:

```
sudo ss -tulpn
```

Identify the process:

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

Investigate the process:

```
ps aux | grep PROCESS_NAME
```

Questions:

- What program opened the port?
- Which user is running it?
- Is the service expected?
- Is it exposed to the network?

SCENARIO 3 — SUSPICIOUS OUTBOUND CONNECTION

Check active connections:

```
sudo ss -tunap
```

Identify network processes:

```
sudo lsof -i
```

Check the process:

```
ps aux | grep PROCESS_NAME
```

Reverse DNS:

`dig -x IP_ADDRESS`

Questions:

- Which process created the connection?
- Which user owns it?
- Is the destination expected?
- Does the destination have a suspicious reputation?

SCENARIO 4 — SUSPICIOUS FILE

Identify the file:

`file suspicious_file`

Calculate SHA256:

`sha256sum suspicious_file`

Inspect readable strings:

`strings suspicious_file`

Check permissions:

`ls -la suspicious_file`

Questions:

- What type of file is it?
- Does its hash match a known malicious sample?
- Does it contain suspicious URLs or commands?
- Who owns the file?

SCENARIO 5 — UNUSUAL DNS TRAFFIC

Capture DNS traffic:

`sudo tcpdump -i eth0 port 53`

Specific host:

`sudo tcpdump -i eth0 host IP_ADDRESS and port 53`

Look for:

- Repeated requests
- Unusual domains
- High-frequency queries
- Unexpected DNS servers
- Unusual query patterns

Questions:

- Which process generates the traffic?
- Is the destination expected?
- Does the domain have a suspicious reputation?
- Does the activity occur periodically?

=====

12. INVESTIGATION CHECKLIST

=====

- ☐ Date/time
- ☐ Source IP
- ☐ Destination IP
- ☐ Source/destination port
- ☐ Username
- ☐ Process name/PID
- ☐ File path
- ☐ SHA256 hash
- ☐ Relevant logs
- ☐ DNS queries
- ☐ Network connections
- ☐ Initial hypothesis
- ☐ Evidence collected
- ☐ Final conclusion

=====

13. QUICK REFERENCE

=====

NETWORK

ip addr
ip route
ss -tulpn
ss -tunap

PROCESSES

ps aux
top
lsof

DNS

dig
dig +short
dig -x

LOGS

journalctl
grep
tail
less

TRAFFIC

tcpdump

FILES

file

strings

sha256sum

md5sum

IMPORTANT

Use these commands only on systems you own or are authorized to investigate.

This cheat sheet is intended for cybersecurity education, SOC analysis and authorized security testing.

Version 1.0

Feedback and suggestions are welcome.