

Forum:[Hack Forums](#)

Thread: [From Pwned to Patched: A Blue Team Guide to Analyzing Linux Logs](#)

Oh_Well - August 22, 2025, 3:41 am

From Pwned to Patched
A Blue Team guide to analyzing Linux Logs

? The breach is over. The system is back online. Now the real work begins: the forensic analysis.

How did they get in? What did they do? This guide will walk you through analyzing Linux log files to answer these critical questions. This is digital detective work at its finest.

1. Follow the Evidence

Golden Rules of Digital Forensics:

- Assume nothing - Verify every finding
- Trust nothing on the system itself (logs can be altered)
- Corroborate findings across multiple sources
- Your goal: Create an accurate timeline of the attack

2. Critical Log Files & Locations

Logs are your primary evidence. Know where to look first:

Log File
Purpose
Priority

/var/log/auth.log (Debian/Ubuntu)	/var/log/secure (RHEL/CentOS)
SSH logins, sudo commands, failed authentication	
CRITICAL	

/var/log/syslog
General system activity
HIGH

/var/log/apt/ or /var/log/yum.log
Package installations (did they install tools?)
HIGH

/var/log/httpd/ or /var/log/apache2/[br]/var/log/nginx/
Web server access and errors
HIGH

~/.bash_history
Command history (often cleared by attackers)
MEDIUM

3. Your Forensic Toolkit

You don't need fancy software. The built-in Linux tools are incredibly powerful:

grep - The #1 tool for searching text patterns

awk - Processing and analyzing structured data

sed - Filtering and transforming text streams

cat, head, tail, less - Viewing files efficiently

journalctl - Querying the systemd journal

sort, uniq - Organizing and deduplicating data

4. Analysis Step 1: The Initial Foothold (SSH Attacks)

Most common entry point: SSH brute-force attacks. Start here:

Code # Find all failed login attempts
grep "Failed password" /var/log/auth.log

Identify top attacking IPs (sorted by attempt count)
grep "Failed password" /var/log/auth.log | awk '{print \$11}' | sort | uniq -c | sort -nr

Check for successful logins during the incident timeframe
grep "Accepted password" /var/log/auth.log | grep "Jun 4"
grep "session opened" /var/log/auth.log | grep "Jun 4"

Look for unauthorized SSH key additions
grep "key added" /var/log/auth.log

? Pro Tip: Cross-reference successful logins with your known user locations. A login from Russia when your admin is in New York is suspicious.

5. Analysis Step 2: Privilege Escalation (sudo & su)

How did they get root access?

```
Code # Track all sudo command usage
grep "sudo:" /var/log/auth.log | grep "COMMAND"
```

```
# Find successful privilege escalations to root
grep "su:" /var/log/auth.log | grep "session opened"
```

```
# Check for new user/group additions (backdoor accounts)
grep "new user" /var/log/auth.log
grep "new group" /var/log/auth.log
grep "usermod" /var/log/auth.log
```

```
# Look for password changes (especially for system accounts)
grep "password changed" /var/log/auth.log
```

? Red Flag: An attacker adding themselves to the sudo group is a classic persistence technique.

6. Analysis Step 3: Persistence & Data Exfiltration

What did they do to maintain access and what data did they steal?

```
Code # Check for suspicious cron jobs (common persistence method)
grep "CRON" /var/log/syslog | grep -v "session closed"
ls -la /etc/cron* /var/spool/cron*
```

```
# Find large file transfers in web server logs (potential data theft)
# Files over 10MB downloaded from your server
awk '($10 > 10000000) {print $1, $4, $7, $10}' /var/log/nginx/access.log | sort | uniq
```

```
# Check for unusual network connections
ss -tulwn | grep ESTAB
netstat -an | grep ESTABLISHED
```

```
# Look for file modifications in sensitive directories
find /etc /home /root -type f -mtime -1 -ls 2>/dev/null
```

7. Creating the Attack Timeline

Pull it all together into a coherent story:

```
Code # Search all logs for a specific time window
grep "Jun  4 14:" /var/log/*log | sort
```

```
# Use journalctl for a unified timeline view
journalctl --since "2025-08-21 14:00:00" --until "2025-08-21 15:00:00" \
-o short-full --no-pager
```

```
# Combine multiple log sources for complete picture
(grep "Jun  4 14:" /var/log/auth.log; \
grep "Jun  4 14:" /var/log/syslog; \
grep "04/Jun/2023:14:" /var/log/nginx/access.log) | sort
```

? Timeline Template:

1. Initial compromise (failed/successful logins)
2. Privilege escalation (sudo usage, user modifications)
3. Reconnaissance (file access, network scans)
4. Persistence (cron jobs, backdoor accounts)
5. Data exfiltration (large downloads, external connections)

8. Post-Incident Hardening

Your analysis should directly inform your security improvements:

Finding
Remediation

SSH brute force attack

- Implement fail2ban: Switch to key-based authentication[br]• Change default SSH port

Vulnerable web application

- Apply security patches: Implement WAF rules[br]• Regular vulnerability scanning

Malicious cron job

- Tighten permissions on /etc/cron*/: Monitor crontab changes[br]• Implement file integrity monitoring

Privilege escalation

- Review sudo permissions: Implement least privilege principle[br]• Enable sudo logging

Conclusion: Never Again

Log analysis isn't about assigning blame, it's about understanding your weaknesses and building a stronger defense. A thorough investigation transforms a security incident from a failure into a

valuable learning experience.

Remember: The best way to win the next fight is to learn from the last one.

Quick Reference Commands

Code # Top attacking IPs

```
grep "Failed password" /var/log/auth.log | awk '{print $11}' | sort | uniq -c | sort -nr
```

Recent activity timeline

```
journalctl --since "yesterday" --until "now" -o short-full
```

Large file transfers

```
awk '($10 > 10000000) {print $1, $4, $7, $10}' /var/log/nginx/access.log
```

Active connections

```
ss -tulwn | grep ESTAB | awk '{print $6}' | cut -d: -f1 | sort | uniq
```

Read the logs. Find the story. Write a better ending next time.

ttbr0 - August 22, 2025, 5:11 am

great to see some defensive content on here. the majority here arent able to appreciate the challenge of playing the other side which is a shame because i think its more interesting. do you have much experience with offense at all or are you purely defense?

Oh_Well - August 22, 2025, 5:53 am

(Aug 22, 2025 05:11 AM)ttbr0 Wrote: [\[CITE\]](#) great to see some defensive content on here. the majority here arent able to appreciate the challenge of playing the other side which is a shame because i think its more interesting. do you have much experience with offense at all or are you purely defense?

I feel like its an ongoing game between reds and blues and I dont have a favorite side to be honest. It's really interesting to see the big picture of how a system is broken, how it remains broken and what someone can do to make it safer until a new thing comes to break it again.

I've found myself in defensive roles quite a few times, mostly because of work, where I had to dig into incidents and figure out what went wrong internally. So that kind of pulled me into defense by necessity.

What's your take on this? Are you team blue all the way?

ttbr0 - August 22, 2025, 6:21 am

(Aug 22, 2025 05:53 AM)Oh_Well Wrote: [\[CITE\]](#) I feel like its an ongoing game between reds and blues and I dont have a favorite side to be honest. It's really interesting to see the big picture of how a system is broken, how it remains broken and what someone can do to make it safer until a new thing comes to break it again.

I've found myself in defensive roles quite a few times, mostly because of work, where I had to dig into incidents and figure out what went wrong internally. So that kind of pulled me into defense by

necessity.

What's your take on this? Are you team blue all the way?

i have never worked in pure defensive roles but it is something that i might want to do in the future if things happen to lead that way. the most interesting things to me is mainly threat hunting or detection engineering. i dont have a defensive background but my background and experience in offense would probably put me in a very good and unique position compared to other traditional defenders. i dont think its common to see defenders with a good offensive background which, in my opinion, is not ideal. you should know how to attack before learning to defend. it makes the most sense.

Oh_Well - August 22, 2025, 7:33 am

(Aug 22, 2025 06:21 AM)ttbr0 Wrote: [\[CITE\]](#) i have never worked in pure defensive roles but it is something that i might want to do in the future if things happen to lead that way. the most interesting things to me is mainly threat hunting or detection engineering. i dont have a defensive background but my background and experience in offense would probably put me in a very good and unique position compared to other traditional defenders. i dont think its common to see defenders with a good offensive background which, in my opinion, is not ideal. you should know how to attack before learning to defend. it makes the most sense.

Yeah, totally makes sense. Having an offensive background definitely gives defenders a sharper edge. Knowing how attackers think and operate makes it easier to spot weak points and design more resilient systems.

If you ever do decide to try out a defensive role, I think you'd bring a lot of value!!

Have you thought about what kind of org or environment you'd want to do that in? Something fast paced like a SOC or more strategic like an internal detection team?

ttbr0 - August 22, 2025, 8:41 pm

(Aug 22, 2025 07:33 AM)Oh_Well Wrote: [\[CITE\]](#) Yeah, totally makes sense. Having an offensive background definitely gives defenders a sharper edge. Knowing how attackers think and operate makes it easier to spot weak points and design more resilient systems.

If you ever do decide to try out a defensive role, I think you'd bring a lot of value!!

Have you thought about what kind of org or environment you'd want to do that in? Something fast paced like a SOC or more strategic like an internal detection team?

internal. i hate the idea of working at a soc or mssp because it seems like those teams would be heavily incentivized for profits meaning lower quality people and work. i prefer smaller and tight knit teams with high quality people that have focused goals. i would love to research sophisticated threats around initial access through to establishing c2 comms.

do you work at a mssp or internal? what areas interest you the most about defense?

LawrenceIII - August 22, 2025, 8:53 pm

Well the good thing is I'm starting to understand some of this but it's going to take awhile to really absorb this information.

Oh_Well - August 23, 2025, 4:26 am

(Aug 22, 2025 08:41 PM)ttbr0 Wrote: [\[CITE\]](#) internal. i hate the idea of working at a soc or mssp because it seems like those teams would be heavily incentivized for profits meaning lower quality people and work. i prefer smaller and tight knit teams with high quality people that have focused goals. i would love to research sophisticated threats around initial access through to establishing c2 comms.

do you work at a mssp or internal? what areas interest you the most about defense?

Internal but it's not my main role, I'm a full time dev normally. Mssp is not my style, I think it lacks

innovation and it feels pretty repetitive. I'd want to work on threat intelligence, detection engineering or adversary emulation, but I think my knowledge is still far from doing that.

If you had any good resources to share on those I'd appreciate it!

C2 is a really nice focus and for that u indeed need to know how to work as a red first in order to secure it later!

ttbr0 - August 23, 2025, 7:44 pm

(Aug 23, 2025 04:26 AM)Oh_Well Wrote: [\[CITE\]](#) Internal but it's not my main role, I'm a full time dev normally. Mssp is not my style, I think it lacks innovation and it feels pretty repetitive. I'd want to work on threat intelligence, detection engineering or adversary emulation, but I think my knowledge is still far from doing that.

If you had any good resources to share on those I'd appreciate it!

C2 is a really nice focus and for that u indeed need to know how to work as a red first in order to secure it later!

how did you end up doing internal defense as a dev? how long have you been learning security?

rjusticemi - August 24, 2025, 12:49 pm

Btw, if the /var/log/auth.log file doesn't exist, try running the command journalctl -u ssh

When I first set up my linux servers and wanted to check my SSH logs, that file didn't exist, so I had to run journalctl -u ssh instead to view the SSH logs.

Oh_Well - August 24, 2025, 3:23 pm

(Aug 23, 2025 07:44 PM)ttbr0 Wrote: [\[CITE\]](#) how did you end up doing internal defense as a dev? how long have you been learning security?

No more than a year, and not super consistently either, but there is flexibility so since security is one of those areas that pulls me in, I'm diving into it when I get the chance and understand whats going on.. I don't think I know a lot of stuff yet tbh, but I'm working on it :)

ttbr0 - August 25, 2025, 3:39 am

(Aug 24, 2025 03:23 PM)Oh_Well Wrote: [\[CITE\]](#) No more than a year, and not super consistently either, but there is flexibility so since security is one of those areas that pulls me in, I'm diving into it when I get the chance and understand whats going on.. I don't think I know a lot of stuff yet tbh, but I'm working on it :)

its great that you are interested and motivated. all you need now is time and persistence so keep at it and you will get better.