DIGITAL FORENSICS AND INCIDENT RESPONSE PROJECT

Contents

1 Initial Assessment

1.1 Unusual/Unauthorized Activity

- SSH brute-force attempts from **192.168.10.128** before successful logins to **john's** account.
- Two successful authentications occurred, followed by a root shell spawn in session **15**.
- */etc/shadow* was read as root. TTY auditing was then disabled and the session ended.
- Observed window: **2024-09-12 | 10:07:46 – 10:18:12 UTC**

1.2 Timeline of Key Events

*Times are in UTC +0

UTC	Key Event
10:07:46.053	Audit service start; rules active
10:08:09 → 10:11:44	SSH brute force from 192.168.10.128
10:09:26.972	SSH success for john, ses=13; TTY audit enabled then disabled
10:12:05.924	SSH success for john, ses=15; 10:12:07.167 attached to /dev/pts/1
10:12:23.283 → 10:12:27.301	sudo -l executed; PAM success; USER_CMD res=failed
10:17:05.345	/usr/bin/zsh started with euid=0 under auid=1001, ses=15
10:17:12.106	id as root
10:17:16.791	whoami as root
10:17:28.012	cat /etc/shadow as root
10:17:37.248	TTY auditing disabled for ses=15
10:17:37.252	Session 15 closed

2 Analysis

2.1 Initial Access Method

- **Valid-credential use after password guessing**. The attacker performed repeated SSH authentication attempts from **192.168.10.128** and then authenticated successfully as **john**.

- **Evidence:**
  - **type=USER_AUTH** and **type=LOGIN** success for **john** from **192.168.10.128** (ses=13 at 10:09:26.972; ses=15 at 10:12:05.924).
  - Prior failures from the same source during 10:08:09–10:11:44 (288 failed attempts)

2.2 Privilege Escalation

- Root shell spawned in **ses=15** at **10:17:05.345** with **euid=0**, **auid=1001**, **ppid=4519**, **pid=4629**, **tty=pts1**.

- **Vector: Unknown**. No preceding EXECVE or SYSCALL in the provided audit log explains transition to root. The *sudo -l* attempt immediately prior did not grant privilege (USER_CMD res=failed).

2.3 Files Accessed/Extracted

- */etc/shadow* accessed at **10:17:28.012** via cat.
- No additional file exfiltration within the provided audit scope.

2.4 Defense Evasion

- TTY auditing disabled at **10:17:37.248** in **ses=15**, reducing post-event visibility.

3 Reporting

3.1 How the Attacker Gained Access

- The attacker gained access by **successfully authenticating over SSH as john** after a brief brute-force phase from **192.168.10.128**.

3.2 Timeline of the Attacker's Activities

- See Initial Assessment for the condensed timeline. Sequence: brute force → two SSH successes → sudo -l denied → root shell start → hash access (*/etc/shadow*) → TTY audit disabled → session closed.

3.3 Potential Vulnerabilities Exploited

- **Password authentication enabled on SSH** without lockout controls or MFA allowed password guessing and credential use.

- **Privilege escalation vector unknown**. Possibilities include a setuid helper or misconfiguration, but no corroborating log entry exists in the provided data.

- Ability for **per-session TTY audit disable** reduced observability.

3.4 Recommendations to Prevent Similar Incidents

3.4.1 Immediate

1. **Contain and preserve**: Image the system; preserve */var/log/**, */etc/**, user homes, and journal. Isolate from network.

2. **Rotate credentials**: Invalidate current */etc/shadow* contents. Enforce unique new passwords.

3. **Harden SSH**:
    - Set PasswordAuthentication no, KbdInteractiveAuthentication no, ChallengeResponseAuthentication no.
    - PermitRootLogin no.
    - Restrict with AllowUsers to named admins.
    - Require **key-only** auth with FIDO2 or hardware-backed keys.
    - Set MaxAuthTries 3, LoginGraceTime 20s. Enable **fail2ban** on sshd.
4. **Rebuild from trusted media** and redeploy config as code after forensic imaging.
5. **Revoke/rotate SSH keys and tokens**, audit *~/.ssh/authorized_keys*.

3.4.2 Near-term

1. **Sudo hardening**: principle of least privilege; remove broad NOPASSWD/!authenticate.
2. **Add MFA** for SSH administrative access.
3. **Centralize logging off-host**; expand audit rules to watch */etc/shadow*, */etc/sudoers**, */etc/ssh/**; include SYSCALL, EXECVE, CWD, PATH, PROCTITLE.
4. **SUID/Capability baseline** with scheduled diffs and alerting.
5. **Network restrictions**: limit SSH to management VLAN or jump host only.

3.4.3 Mid-term

1. **Detection coverage**: deploy an EDR that captures Linux process, file, and TTY telemetry; alert on root shells where **auid≠0** and on /etc/shadow access.
2. **Credential hygiene program** with periodic rotations and hash-cracking monitoring.

4 Annexes (Evidence)

- **SSH success → ses=13; TTY audit on**

type=USER_AUTH msg=audit(1726135766.828:2766): ... acct="john" exe="/usr/sbin/sshd" hostname=192.168.10.128 addr=192.168.10.128 terminal=ssh res=success

type=LOGIN msg=audit(1726135766.972:2770): ... auid=1001 ... ses=13 res=1

type=CONFIG_CHANGE msg=audit(1726135766.972:2769): ... op=tty_set old-enabled=0 new-enabled=1 ... res=1

- **ses=13; TTY audit off**

type=CONFIG_CHANGE msg=audit(1726135769.218:2848): ... ses=13 ... op=tty_set old-enabled=1 new-enabled=0 ... res=1

- **SSH success → ses=15; TTY attached**

type=USER_AUTH msg=audit(1726135925.916:3193): ... acct="john" ... addr=192.168.10.128 ... res=success

type=LOGIN msg=audit(1726135925.924:3197): ... auid=1001 ... ses=15 res=1

type=USER_LOGIN msg=audit(1726135927.167:3268): ... ses=15 ... terminal=/dev/pts/1 res=success

- **sudo -l executed; command not granted**

type=EXECVE msg=audit(1726135943.283:3269): argc=2 a0="sudo" a1="-l"

type=USER_AUTH msg=audit(1726135947.301:3270): ... exe="/usr/bin/sudo" ... terminal=/dev/pts/1 res=success

type=USER_CMD msg=audit(1726135947.301:3272): ... cmd="list" terminal=pts/1 res=failed

- **Root shell and root commands**

type=SYSCALL msg=audit(1726136225.345:3381): ... ppid=4519 pid=4629 auid=1001 ... euid=0 ... comm="zsh" exe="/usr/bin/zsh" tty=pts1 ses=15

type=EXECVE msg=audit(1726136225.345:3381): argc=1 a0="**zsh**"

---

type=SYSCALL msg=audit(1726136232.106:3383): ... pid=4632 ... euid=0 ... comm="**id**" exe="/usr/bin/id"

type=EXECVE msg=audit(1726136232.106:3383): argc=1 a0="**id**"

---

type=SYSCALL msg=audit(1726136236.791:3384): ... pid=4633 ... euid=0 ... comm="**whoami**" exe="/usr/bin/whoami"

type=EXECVE msg=audit(1726136236.791:3384): argc=1 a0="**whoami**"

---

type=SYSCALL msg=audit(1726136248.012:3385): ... pid=4636 ... euid=0 ... comm="**cat**" exe="/usr/bin/cat"

type=EXECVE msg=audit(1726136248.012:3385): argc=2 a0="**cat**" a1="**/etc/shadow**"

- **Keystrokes and TTY off; session close**

type=TTY msg=audit(1726136254.558:3386): ... comm="zsh" data=69640A77686F616D690A636174202F6574632F736861646F770A657869740A

type=CONFIG_CHANGE msg=audit(1726136257.248:3389): ... op=tty_set old-enabled=1 new-enabled=0 ...

type=USER_END msg=audit(1726136257.252:3390): ... acct="john" ... terminal=ssh res=success

type=CRED_DISP msg=audit(1726136257.252:3391): ... acct="john" ... terminal=ssh res=success

5 Final Determinations

- **Initial access:** Valid credentials over SSH after password guessing.
- **Privilege escalation:** Occurred; **vector unknown** in provided logs.
- **Data at risk:** Local password hashes in */etc/shadow*.
- **Containment seen:** Only that the session ended after TTY audit was disabled.
- **Primary fixes:** Disable SSH password auth, enforce key+MFA, rebuild from trusted media, rotate all credentials, expand audit and central logging, and baseline SUID/capabilities

END OF REPORT