

Red Team Debrief

ISU1 - Oct 2026

Professionally unprofessional.



AI Everywhere

So much AI usage...

We do not want to read thousands of words of earnbacks...

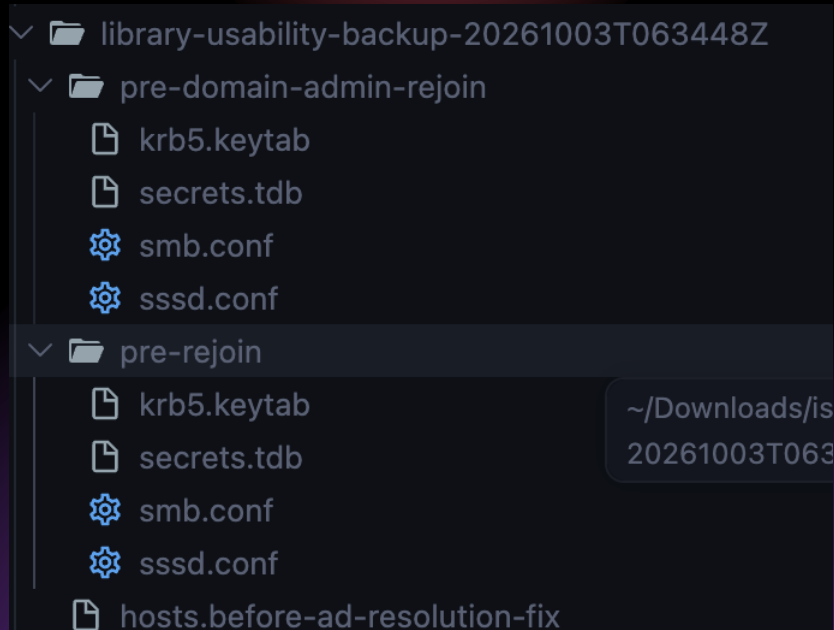
Quantity does not equal quality.

deploy_audit.sh

```
#!/usr/bin/env bash
#
# deploy_audit.sh – one-shot auditd + parser deploy for the apt-based CDC Linux boxes
#   Targets: WWW (Ubuntu 24.04), Canvas (Ubuntu 22.04), DB (Debian 11)
#   NOT for the Library box (Arch-based Hannah Montana Linux).
#
# Installs auditd, loads exec + identity rules, drops execlog/identlog/privlog
# into /usr/local/bin, and turns on NTP. Idempotent – safe to re-run.
#
# Usage:  sudo bash deploy_audit.sh
#
```

AI leaves so much garbage

Think about what AI is leaving behind, we found keytabs, shadow, and more.



```
root@lib:~# ls
before6.rules.pre-guest-proxy-only-20261006T060641Z
before.rules.pre-guest-egress-20261006T005216Z
before.rules.pre-guest-proxy-only-20261006T060641Z
environment.pre-desktop-proxy-20261006T0450Z
guest-home.pre-profile-reset-20261006T062102Z
guest-profile-reset-setup-20261006T062102Z
hosts.pre-canvas-local-dns-20261006T0452Z
root@lib:~#
```

```
iptables-before-guest-deny
library-capture-removal-20261010T160940Z
library-cdc-disable-20261010T155703Z
library-cdc-disable-20261010T155803Z
library-execution-hardening-20261006T145758Z
library-guest-hardening-r2-20261006T150609Z
library-hardening-20261003T070858Z
```

```
library-hardening-20261004T155529Z
library-hardening-r3-20261006T152649Z
library-hardening-r3-20261006T152705Z
library-hardening-r4-20261006T153929Z
library-rdp-ssh-remediation-20261006_235551
library-rdp-user-hardening-20261007_000219
library-session-lockdown-20261007_000855
```

```
library-session-persistence-removal-20261010T161612Z
library-session-persistence-removal-20261010T161652Z
library-smb-hardening-20261004T224002Z
library-usability-backup-20261003T063448Z
retired-lunch-info-20261004T180126Z
sshd_config.pre-guest-hardening-20261006T061214Z
```

AI leaves so much garbage

And it did for us too

[REDACTED]

Accurate and thorough. Correctly identifies the blue flag as a readable file in C:\Windows\System32 (a read, not a deletion), cites specific RDP (TS 1149) Administrator logons from Red source ranges with timestamps, the credential spray, and the IT-admin session, and confirms the post-compromise Administrator password rotation. Detection (SACL Audit-Success-on-read + 4663 to Wazuh) and mitigations (rotate admin, limit Domain Admins, restrict/alert RDP) are concrete and realistic. Minor deduction: exact capture vector asserted as an RDP desktop read where SMB C\$ was equally possible, though both are covered. Strong completeness and verified-accurate against our capture record.

[REDACTED]

Re-review by red team. Your AI mixed up some things that happened.

Opencode sessions on DB

AI is everywhere

Sessions

Fri Oct 09 2026

● PostgreSQL vulnerability scan findings

Wed Oct 07 2026

Installing Wazuh agent for 33.96.5.70

pin/unpin ctrl+f delete ctrl+d rename ctrl+r

Most Common Exploit

Default Creds!!!!

PAM backdoor

SetUID for bash

At 8:01 AM...

```
Pwned! cdc cdc www.team5.isucdc.com
Pwned! cdc cdc www.team2.isucdc.com
Pwned! cdc cdc www.team6.isucdc.com
Pwned! cdc cdc lib.team5.isucdc.com
Pwned! cdc cdc lib.team2.isucdc.com
Pwned! cdc cdc db.team2.isucdc.com
Pwned! cdc cdc db.team6.isucdc.com
Pwned! cdc cdc db.team5.isucdc.com
Pwned! canvas cdc db.team2.isucdc.com
Pwned! canvas cdc db.team6.isucdc.com
Pwned! canvas cdc db.team5.isucdc.com
Pwned! canvas cdc can.team4.isucdc.com
Pwned! canvas cdc db.team4.isucdc.com
Pwned! cdc cdc can.team6.isucdc.com
Pwned! cdc cdc can.team5.isucdc.com
Pwned! cdc cdc can.team2.isucdc.com
Pwned! canvas cdc db.team1.isucdc.com
Pwned! canvas cdc can.team6.isucdc.com
```

```
HELLO FROM
SPARKING
JAGGERS
```

PAM Backdoor

We lost access, but your machines told us the new creds :)

```
1757 49.49.33.40 can.team7.isucdc.com: 2026-10-10_20:06:09 gabrielle.jackson, , From: 12.110.252.4
1758 49.49.33.40 can.team7.isucdc.com: 2026-10-10_20:06:09 gabrielle.jackson, , From: 12.110.252.4
1759 49.49.33.40 can.team7.isucdc.com: 2026-10-10_20:06:10 gabrielle.jackson, , From: 12.110.252.4
1760 49.49.33.30 www.team7.isucdc.com: 2026-10-10_20:06:01 steven.fields, nag950sen, From: 12.110.252.4
1761 79.5.64.30 www.team6.isucdc.com: 2026-10-10_20:05:04 steven.fields, bit426xoc, From: 12.110.252.4
1762 79.5.64.30 www.team6.isucdc.com: 2026-10-10_20:05:05 steven.fields, bit426xoc, From: 12.110.252.4
1763 79.5.64.30 www.team6.isucdc.com: 2026-10-10_20:05:05 steven.fields, bit426xoc, From: 12.110.252.4
1764 64.39.3.100 can.team1.isucdc.com: 2026-10-10_20:04:39 gabrielle.jackson, may647teq, From: 12.110.252.4
1765 64.39.3.100 can.team1.isucdc.com: 2026-10-10_20:04:39 gabrielle.jackson, may647teq, From: 12.110.252.4
1766 64.39.3.100 can.team1.isucdc.com: 2026-10-10_20:04:39 gabrielle.jackson, may647teq, From: 12.110.252.4
1767 64.39.3.100 db.team1.isucdc.com: 2026-10-10_15:05:20 gabrielle.jackson, may647teq, From: 12.110.252.4
1768 64.39.3.100 can.team1.isucdc.com: 2026-10-10_20:04:39 gabrielle.jackson, may647teq, From: 12.110.252.4
1769 64.39.3.100 db.team1.isucdc.com: 2026-10-10_15:05:20 gabrielle.jackson, may647teq, From: 12.110.252.4
1770 64.39.3.100 www.team1.isucdc.com: 2026-10-10_20:05:01 steven.fields, rid115hur, From: 12.110.252.4
1771 64.39.3.100 www.team1.isucdc.com: 2026-10-10_20:05:01 steven.fields, rid115hur, From: 12.110.252.4
1772 200.2.96.40 can.team4.isucdc.com: 2026-10-10_20:05:23 gabrielle.jackson, nez059cug, From: 12.110.252.4
1773 200.2.96.30 www.team4.isucdc.com: 2026-10-10_20:05:09 gabrielle.jackson, nez059cug, From: 12.110.252.4
1774 64.39.3.100 www.team1.isucdc.com: 2026-10-10_20:05:01 steven.fields, rid115hur, From: 12.110.252.4
1775
```

Nice Website You Got There

This site has been defaced by the Red Team

Central Dobson County School District – secure your Canvas LMS.

nyaGVw20UweMApCQaUPWP40rVLI1jQBntgKEprk8lVKHmyxMa

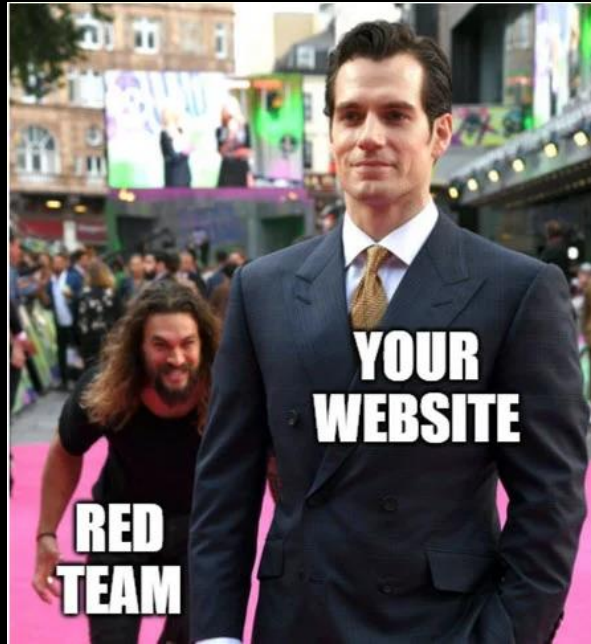
- Added an *index.html* file to `/var/canvas/public`
- Functionality was still there, but users had to go to the login endpoint

Nice Logging!

There was a lot of logging in earnbacks, which helped answer the 5 W's:

WHO
WHAT
WHERE
WHEN
WHY





Questions?