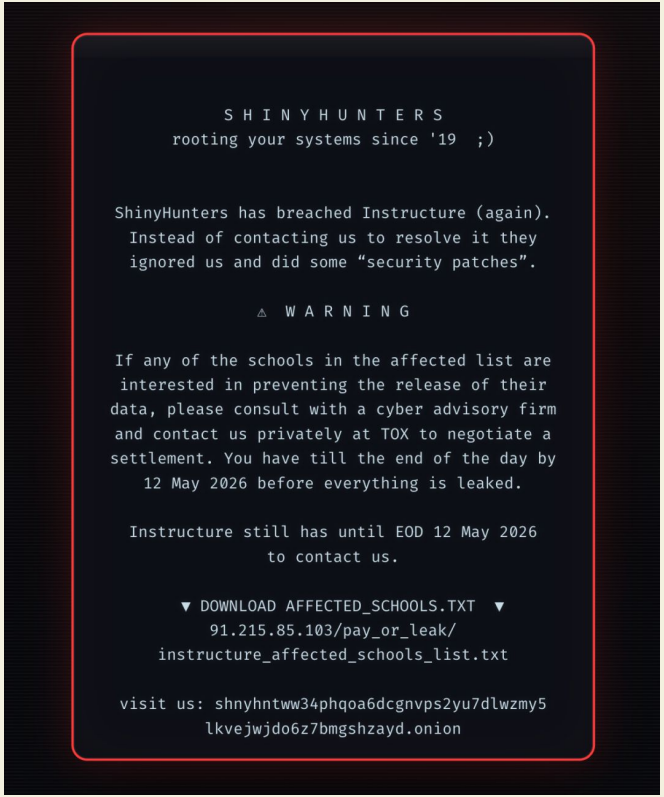
Incident Response and Linux Defense

Lecture 16 - ECS198F SQ26

Incident Response (IR)

Reality

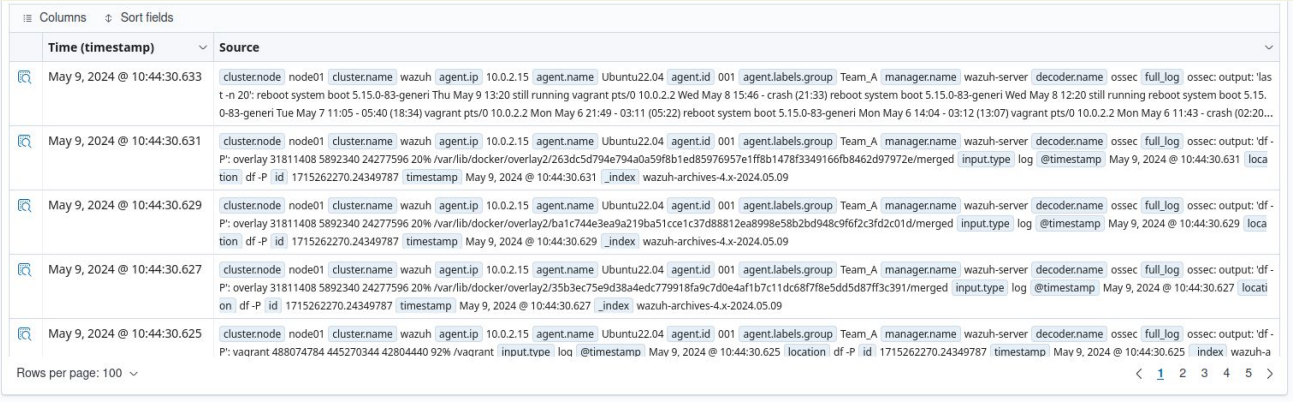

S H I N Y H U N T E R S
rooting your systems since '19 ;)
ShinyHunters has breached Instructure (again). Instead of contacting us to resolve it they ignored us and did some “security patches”.
⚠ W A R N I N G
If any of the schools in the affected list are interested in preventing the release of their data, please consult with a cyber advisory firm and contact us privately at TOX to negotiate a settlement. You have till the end of the day by 12 May 2026 before everything is leaked.
Instructure still has until EOD 12 May 2026 to contact us.
▼ DOWNLOAD AFFECTED_SCHOOLS.TXT ▼
91.215.85.103/pay_or_leak/instructure_affected_schools_list.txt
visit us: shnyhntww34phqoa6dcgnvps2yu7dlwzmy5lkvejwjdo6z7bmgshzayd.onion

Scenario

- Your security team discovers an anomaly
- What do you do?

Identify

- Was it an attack? False alarm?
- Look through logs
- Who/What/When/Where/Why
- How severe?




Canvas what the heck
Canvas is currently undergoing

Contain

- Limit damage, prevent further damage
- Isolate a network (network segmentation)
- Potentially take servers down (e.g. Canvas)

Eradicate

- Remove malicious content
- Restore from backups
- Harden the system
  - Apply security patches
  - Remove backdoors
- Anti-malware

Recover

- Put restored systems back into prod
- Ensure that the flaws which enabled the incident are removed
- Monitor for re-exploitation

Lessons Learned

- Document incident
- Update procedures

Prerequisites for IR

In order for IR to succeed, what must we do *before* any attacks happen?

How do we reduce the likelihood of attacks?

When attacks happen, how do we make sure we are ready to perform IR?

Defense

Scenario

The software team has set up a system. You don’t know what it does.

Keeping IR in mind, What do you do?

Enumerate

What is running on the system?

`ss -plntu`

- See open TCP and UDP ports

`systemctl list-units --state=active`

- See running services

Backup

Store config files, databases, etc. safely

If hackers delete data, we must have something to roll back to during IR

Two main things to focus on:

- Configs (outlines how the service runs)
- Data (the info the service stores)

Investigate

Look through configs. What problems exist?

Write down all observations — **Document**!

Remediate

Use your documentation

- Separate features from vulnerabilities
- Patch vulnerabilities

Fortify

Set up firewalls, logging systems, IR procedures, …

Make yourself more prepared for IR

Linux

Configuring Services

Config files exist in `/etc/`

E.g. FTP: `/etc/vsftpd.conf`

Config files outline a service's operation

- In UNIX, everything is a file

Config-Based Components of Linux

- `iptables/nftables` – firewalls and routing
- `systemd` – process management

- `systemd-timer` and `cron` – runs tasks at set intervals
- `PAM` – handles authentication for the system