

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: shnyhntww34phqoa6dcgnvps2yu7dlwzmy5  
lkvejwjd06z7bmgshzayd.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?

Time (timestamp)	Source
May 9, 2024 @ 10:44:30.633	clustername: node01 clustername: wazuh agent.ip: 10.0.2.15 agent.name: Ubuntu22.04 agent.id: 001 agent.labels.group: Team_A manager.name: wazuh-server decoder.name: ossec full_log ossec.output: las t-n 20: reboot system boot 5.15.0-83-generi Thu May 9 13:20 still running vagrant pts/0 10.0.2.2 Wed May 8 15:46 - crash (21:33) reboot system boot 5.15.0-83-generi Wed May 8 12:20 still running reboot system boot 5.15.0-83-generi Tue May 7 11:05 - 05:40 (18:34) vagrant pts/0 10.0.2.2 Mon May 6 21:49 - 03:11 (05:22) reboot system boot 5.15.0-83-generi Mon May 6 14:04 - 03:12 (13:07) vagrant pts/0 10.0.2.2 Mon May 6 11:43 - crash (02:20...
May 9, 2024 @ 10:44:30.631	clustername: node01 clustername: wazuh agent.ip: 10.0.2.15 agent.name: Ubuntu22.04 agent.id: 001 agent.labels.group: Team_A manager.name: wazuh-server decoder.name: ossec full_log ossec.output: df- P: overlay 31811408 5892340 24277596 20% /var/lib/docker/overlay2/263dc5d794e794a0a59f8b1ed85976957e1ff8b1478f349166fb8462d97972e/merged input.type: log @timestamp: May 9, 2024 @ 10:44:30.631 location: df-P id: 1715262270.24349787 timestamp: May 9, 2024 @ 10:44:30.631 _index: wazuh-archives-4.x-2024.05.09
May 9, 2024 @ 10:44:30.629	clustername: node01 clustername: wazuh agent.ip: 10.0.2.15 agent.name: Ubuntu22.04 agent.id: 001 agent.labels.group: Team_A manager.name: wazuh-server decoder.name: ossec full_log ossec.output: df- P: overlay 31811408 5892340 24277596 20% /var/lib/docker/overlay2/ba1c744e3ea9a219ba51cce1c37d88812ea8998e58b2bd948c96f2c3fd2c01d/merged input.type: log @timestamp: May 9, 2024 @ 10:44:30.629 location: df-P id: 1715262270.24349787 timestamp: May 9, 2024 @ 10:44:30.629 _index: wazuh-archives-4.x-2024.05.09
May 9, 2024 @ 10:44:30.627	clustername: node01 clustername: wazuh agent.ip: 10.0.2.15 agent.name: Ubuntu22.04 agent.id: 001 agent.labels.group: Team_A manager.name: wazuh-server decoder.name: ossec full_log ossec.output: df- P: overlay 31811408 5892340 24277596 20% /var/lib/docker/overlay2/35b3ec75e9d38a4edc79918fa9c7d0e4af1b7c11dc687f8e5dd5d87f3c391/merged input.type: log @timestamp: May 9, 2024 @ 10:44:30.627 location: df-P id: 1715262270.24349787 timestamp: May 9, 2024 @ 10:44:30.627 _index: wazuh-archives-4.x-2024.05.09
May 9, 2024 @ 10:44:30.625	clustername: node01 clustername: wazuh agent.ip: 10.0.2.15 agent.name: Ubuntu22.04 agent.id: 001 agent.labels.group: Team_A manager.name: wazuh-server decoder.name: ossec full_log ossec.output: df- P: vagrant 488074784 445270344 42804440 92% /vagrant input.type: loq @timestamp: May 9, 2024 @ 10:44:30.625 location: df-P id: 1715262270.24349787 timestamp: May 9, 2024 @ 10:44:30.625 _index: wazuh-a

Rows per page: 100



Canvas what the heck

Canvas is currently undergoing maintenance

Check back soon

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