

 Student Name: Weicong Xie


 Student Email: Weicongx.wx@gmail.com

## Reflection (Required)


 **Reflection Question #1:** If I had to **explain “what is a cyber breach” in 3 emojis**, they would be...

(Feel free to put other comments about your experience in this unit here, too!)



 **Reflection Question #2:** Which step of the incident response process do you think is most important?

Containment because it protects assets, limits damage, and allows for investigation and recovery. Weak containment means losing millions.

 **Shoutouts:** Share appreciation for anyone who helped you out with this project or made your day a little better!

## Required Challenges (Required)

**Item #1:** A screenshot of your Splunk Malware case in Catalyst:

## Incident #5635: Splunk Malware

Open · 2025-07-22 05:07:25 · 2025-07-22 05:42:50

### Details

CHANGE TEMPLATE

Severity  
High

TLP  
Green

#### Description

Host 192.168.1.10 attempted brute-force login with 3 usernames and successfully authenticated as ABurke. Spoofed its user agent string and uploaded EvilScript.exe at 6/4/2023 17:59. No antivirus alerts, detections, or remediation actions were logged in Splunk.

SAVE DETAILS

### Log

Add a comment...

**admin** today, 05:42 PM

The user's agent string was spoofed, it changed from Firefox/89.0 to Opera/75.0.3969.218 upon uploading the malware

**admin** today, 05:40 PM

The user tried to login using Aburke, Admin, and Pi. There was a large number of failed logins.

**admin** today, 05:35 PM

The IP has a history of abuse, like SSH brute-forces

SetReferences · **admin** · today, 05:31 PM

**admin** today, 05:30 PM

The malware is a macro that attempt to copy, manipulate, and execute files, including Python scripts, from the user's system. These actions are combined with obfuscation techniques and attempts at persistence.

Owner **admin**

### Playbooks

Simple

Enter something to hash

### References

Proof of malicious IP <https://www.abuseipdb.com/check/192.16...>  
Malware's VirusTotal <https://www.virustotal.com/gui/file/208ec2...>

### Artifacts

File hash: 3AADB7E527FC1A050E1C97FEA1CBA4D  
Unknown ? 0  
EvilScript.exe  
Malicious ? 1  
192[.]168[.]1[.]10  
Malicious ? 1

### Related Tickets

### Files

**Item #2:** At least one artifact and notes from an external source:

**Malicious file hash: 3AADB7E527FC1A050E1C97FEA1CBA4D**

**<https://www.virustotal.com/gui/file/208ec23c233580dbfc53aad5655845f7152ada56dd6a5c780d54e84a9d227407/detection>**

**Item #3:** A brief write-up of your findings and Lessons Learned:

**Host 192[.]168[.]1[.]10 attempted brute-force login with 3 usernames and successfully authenticated as ABurke. Spoofed its user agent string and uploaded EvilScript.exe at 6/4/2023 17:59. No antivirus alerts, detections, or remediation actions were logged in Splunk.**

### Lessons learned:

- Implement an antivirus system that:
  - Spots suspicious login activity and temporarily blocks it
  - Identifies maliciously named files and blocks or quarantines it.
  - Run uploaded file hashes onto VirusTotal, block or quarantine if malicious.
  - Send alerts to security when suspicious behavior is detected.

## Stretch Challenge (Optional)

**Bonus Task #1:** Catalyst Investigation – Use Catalyst to manage the incident and fill out the case with the Artifacts, Tasks, and TTPs that you researched:

[Insert Screenshot Here]

**Bonus Task #2:** NIST or Sans Framework Analysis – Write a report that outlines the steps of either the NIST or SANS framework and how it could have prevented the breach:

TODO

---

## Submission Checklist

👉 Check off each of the features you have completed. **You will only be graded on the features you check off.**

### Required Challenges

- ☒ Item #1
- ☒ Item #2
- ☒ Item #3

### Stretch Challenge

- ☐ Bonus Task #1
- ☐ Bonus Task #2