NAME: Eric Somogyi

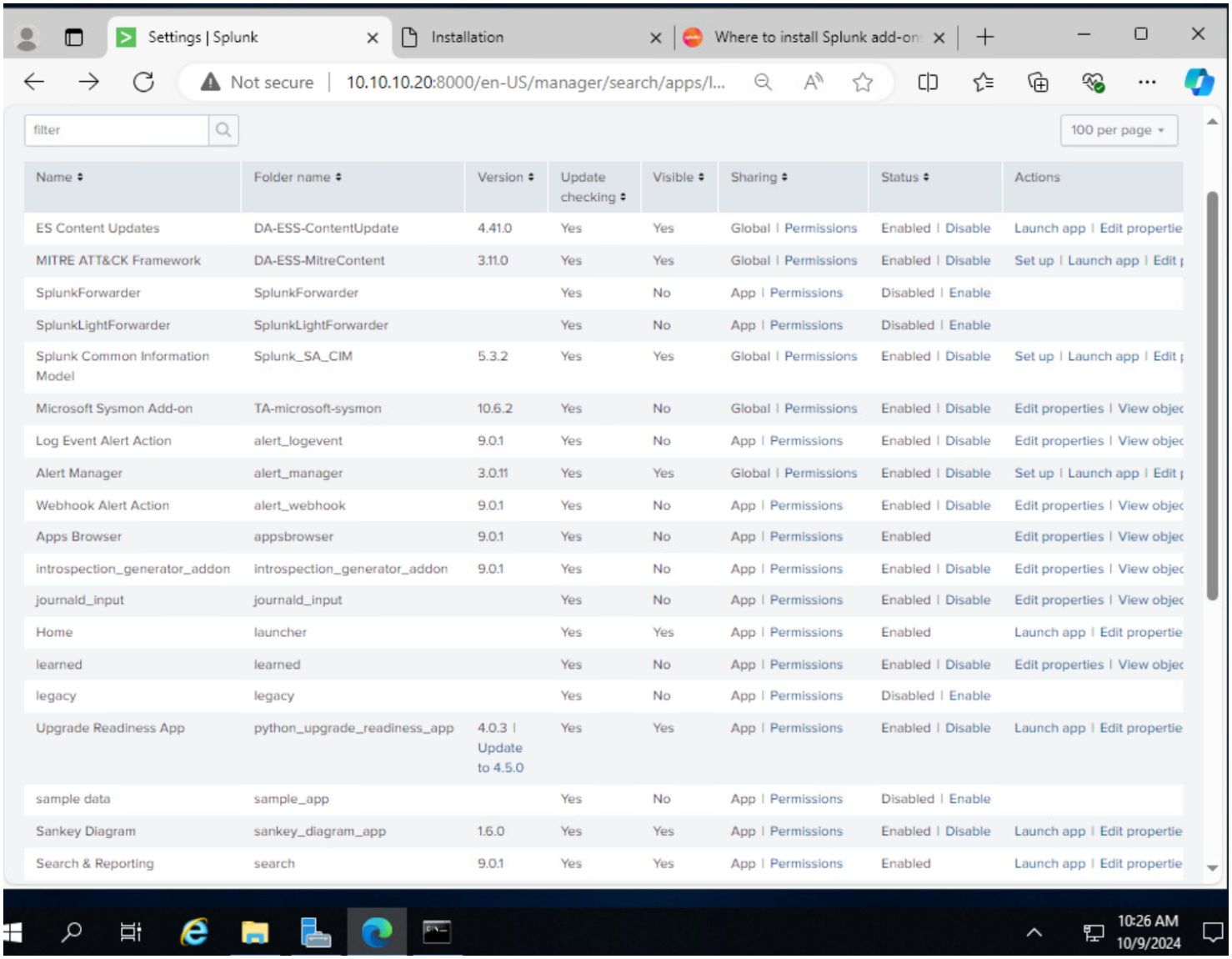
Homework/Lab #4 – CSEC 489

5 Points

Part 1 – Installation

When complete, return to 10.10.10.20:8000/ and take a screenshot of your installed apps.

Answer: See screenshot below



Name	Folder name	Version	Update checking	Visible	Sharing	Status	Actions
ES Content Updates	DA-ESS-ContentUpdate	4.41.0	Yes	Yes	Global | Permissions	Enabled | Disable	Launch app | Edit propertie
MITRE ATT&CK Framework	DA-ESS-MitreContent	3.11.0	Yes	Yes	Global | Permissions	Enabled | Disable	Set up | Launch app | Edit p
SplunkForwarder	SplunkForwarder		Yes	No	App | Permissions	Disabled | Enable	
SplunkLightForwarder	SplunkLightForwarder		Yes	No	App | Permissions	Disabled | Enable	
Splunk Common Information Model	Splunk_SA_CIM	5.3.2	Yes	Yes	Global | Permissions	Enabled | Disable	Set up | Launch app | Edit p
Microsoft Sysmon Add-on	TA-microsoft-sysmon	10.6.2	Yes	No	Global | Permissions	Enabled | Disable	Edit properties | View objec
Log Event Alert Action	alert_logevent	9.0.1	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objec
Alert Manager	alert_manager	3.0.11	Yes	Yes	Global | Permissions	Enabled | Disable	Set up | Launch app | Edit p
Webhook Alert Action	alert_webhook	9.0.1	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objec
Apps Browser	appsbrowser	9.0.1	Yes	No	App | Permissions	Enabled	Edit properties | View objec
introspection_generator_addon	introspection_generator_addon	9.0.1	Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objec
journald_input	journald_input		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objec
Home	launcher		Yes	Yes	App | Permissions	Enabled	Launch app | Edit propertie
learned	learned		Yes	No	App | Permissions	Enabled | Disable	Edit properties | View objec
legacy	legacy		Yes	No	App | Permissions	Disabled | Enable	
Upgrade Readiness App	python_upgrade_readiness_app	4.0.3 | Update to 4.5.0	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit propertie
sample data	sample_app		Yes	No	App | Permissions	Disabled | Enable	
Sankey Diagram	sankey_diagram_app	1.6.0	Yes	Yes	App | Permissions	Enabled | Disable	Launch app | Edit propertie
Search & Reporting	search	9.0.1	Yes	Yes	App | Permissions	Enabled	Launch app | Edit propertie

Part 2 – Configuration

1) **Include screenshots above. What do you think of this rule? Is it a good rule (low false positive, high true positives)? (1 pt)**

Answer:

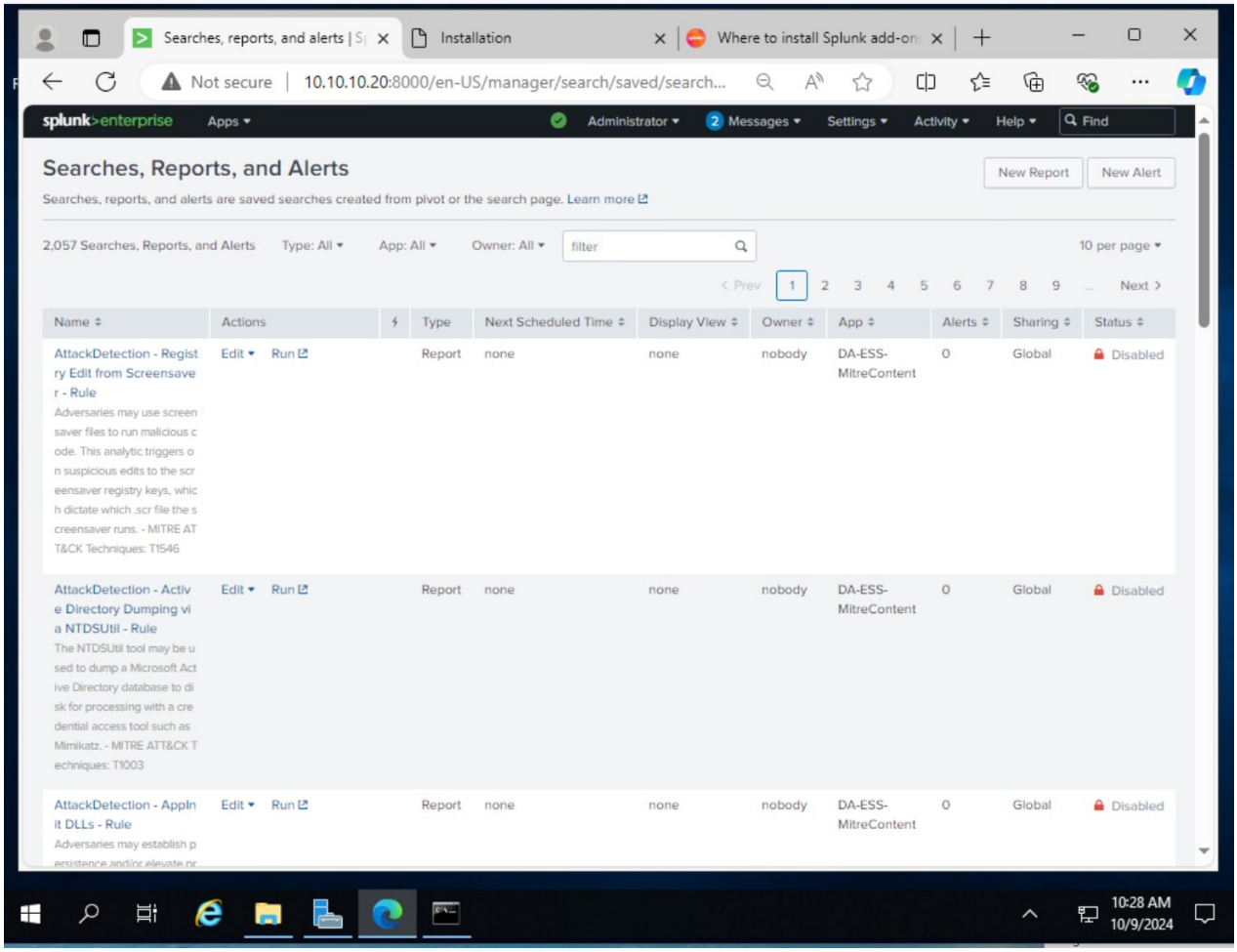
I think this rule is great to try and catch an attacker through these action logs. It is one way to monitor specific commands when an attacker is learning information about a device. It states in the rule description that an adversary may use common command line network commands to try and find out basic network configuration and account information. The listed techniques used that I searched for based on the MITRE Enterprise Technique ID # are: Account Discovery (local, domain, email, cloud) , Permission Group Discovery (Local, Domain, Cloud), System Network Configuration Discovery (Internet Connection/Wi-Fi), System Owner/User Discovery, Process Discovery, and System Service Discovery.

Next, in this case, since a true positive is when the computer actually has the virus and the test results would be positive, the settings in the search box in this rule would actually produce results that do in fact tell the truth because if there are records being produced while a device is on, but the authorized user is away, then we know that the "allowed" entries/processes being produced that match this rule, are an attacker/adversary.

Furthermore, I copy pasted into Google one of the lines in the search code called 'security_content_ctime(firstTime)' and this Splunk webpage came up https://research.splunk.com/endpoint/ad03bfcf-8a91-4bc2-a500-112993deba87/ and this quote confirms furthermore that just having this line of code in the rule is amazing.

> "The following analytic detects the execution of query.exe with command-line arguments aimed at discovering logged-in users. It leverages data from Endpoint Detection and Response (EDR) agents, focusing on process names and command-line executions. This activity is significant as adversaries may use query.exe to gain situational awareness and perform Active Directory discovery on compromised endpoints. If confirmed malicious, this behavior could allow attackers to identify active users, aiding in further lateral movement and privilege escalation within the network." – research.splunk.com

See three Screenshots Below



Searches, reports, and alerts | Sp | Installation | Where to install Splunk add-ons

Not secure | 10.10.10.20:8000/en-US/manager/search/saved/search...

splunk>enterprise Apps ▾ Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Searches, Reports, and Alerts

New Report | New Alert

Searches, reports, and alerts are saved searches created from pivot or the search page. Learn more

12 Searches, Reports, and Alerts | Type: All ▾ | App: All ▾ | Owner: All ▾ | host discovery | 100 per page ▾

Name	Actions		Type	Next Scheduled Time	Display View	Owner	App	Alerts	Sharing	Status
AttackDetection - Host Discovery Commands - Rule	Edit ▾ Run		Report	none	none	nobody	DA-ESS-MitreContent	0	Global	Disabled
ESCU - Allow Network Discovery In Firewall - Rule			Alert	none	none	admin	DA-ESS-ContentUpdate	0	Global	Disabled

Edit ▾ menu:
- Edit Search
- Edit Permissions
- Edit Schedule
- Edit Acceleration
- Edit Summary Indexing
- Enable
- Advanced Edit
- Clone
- Embed
- Move
- Delete

10:31 AM 10/9/2024

Searches, reports, and alerts | Sp | Installation | Where to install Splunk add-ons

Not secure | 10.10.10.20:8000/en-US/manager/search/saved/search...

Edit Search

Title: AttackDetection - Host Discovery Commands - Rule

Description: When entering on a host for the first time, an adversary may try to discover information about the host. There are several built-in Windows commands that can be used to learn about the software configurations, active users, administrators, and networking configuration. These commands should be monitored to identify when an adversary is learning information about the system and environment. - MITRE ATT&CK

Search:

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_ti
    ) as lastTime FROM datamodel=Endpoint.Processes
WHERE Processes.action="allowed" AND  (Processes.process_exec="hostname.exe" OR
    Processes.process_exec="ipconfig.exe" OR Processes.process_exec="net.exe" O
    Processes.process_exec="quser.exe" OR Processes.process_exec="qwinsta.exe"
    Processes.process_exec="systeminfo.exe" OR Processes.process_exec="tasklist
    .exe" OR Processes.process_exec="whoami.exe" OR (Processes.process_exec="sc
    .exe" AND (Processes.process="* query *" OR Processes.process="* qc *")))
BY Processes.user, Processes.dest, Processes.action, Processes.process_name,
    Processes.process, Processes.process_path, Processes.parent_process_name,
    Processes.parent_process, Processes.parent_process_path
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

Earliest time: -24h

Time specifiers: y, mon, d, h, m, s Learn More

Latest time: now

Cancel | Save

Searches, reports, an ✕ | Search | Splunk 9.0.1 ✕

Not secure | 10.10.10.20:8000/en-US/app/DA-ES

MITRE ATT&CK Compliance | MITRE ATT&CK Matrix | MITRE ATT&CK Triggered Tactics &

AttackDetection - Host Discovery Comma...

```
| tstats `security_content_summariesonly` count min(_time) as firstTime max(_time)
WHERE Processes.action="allowed" AND  (Processes.process_exec="hostname.exe" OR Pr
    .exe" OR Processes.process_exec="quser.exe" OR Processes.process_exec="qwinsta
    .process_exec="tasklist.exe" OR Processes.process_exec="whoami.exe" OR (Proces
    Processes.process="* qc *")))
BY Processes.user, Processes.dest, Processes.action, Processes.process_name, Proce
    Processes.parent_process, Processes.parent_process_path
| `drop_dm_object_name(Processes)`
| `security_content_ctime(firstTime)`
| `security_content_ctime(lastTime)`
```

✓ **5 events** (10/8/24 6:45:59.000 PM to 10/9/24 6:45:59.000 PM) No Event Sampling

Events | Patterns | **Statistics (5)** | Visualization

20 Per Page | Format | Preview

user	dest	action	process_name	process	process_path	parent_process_name	parent_process	parent_process_path
Administrator	WIN-N7EOH88RCVT	allowed	HOSTNAME.EXE	hostname	C:\Windows\System32\HOSTNAME.EXE	cmd.exe	"C:\Windows\system32\cmd.exe"	C:\Windows\System32\
Administrator	WIN-N7EOH88RCVT	allowed	ipconfig.exe	ipconfig	C:\Windows\System32\ipconfig.exe	cmd.exe	"C:\Windows\system32\cmd.exe"	C:\Windows\System32\
Administrator	WIN-N7EOH88RCVT	allowed	net.exe	net	C:\Windows\System32\net.exe	cmd.exe	"C:\Windows\system32\cmd.exe"	C:\Windows\System32\
Administrator	WIN-N7EOH88RCVT	allowed	quser.exe	quser	C:\Windows\System32\quser.exe	cmd.exe	"C:\Windows\system32\cmd.exe"	C:\Windows\System32\
Administrator	WIN-N7EOH88RCVT	allowed	tasklist.exe	tasklist	C:\Windows\System32\tasklist.exe	cmd.exe	"C:\Windows\system32\cmd.exe"	C:\Windows\System32\

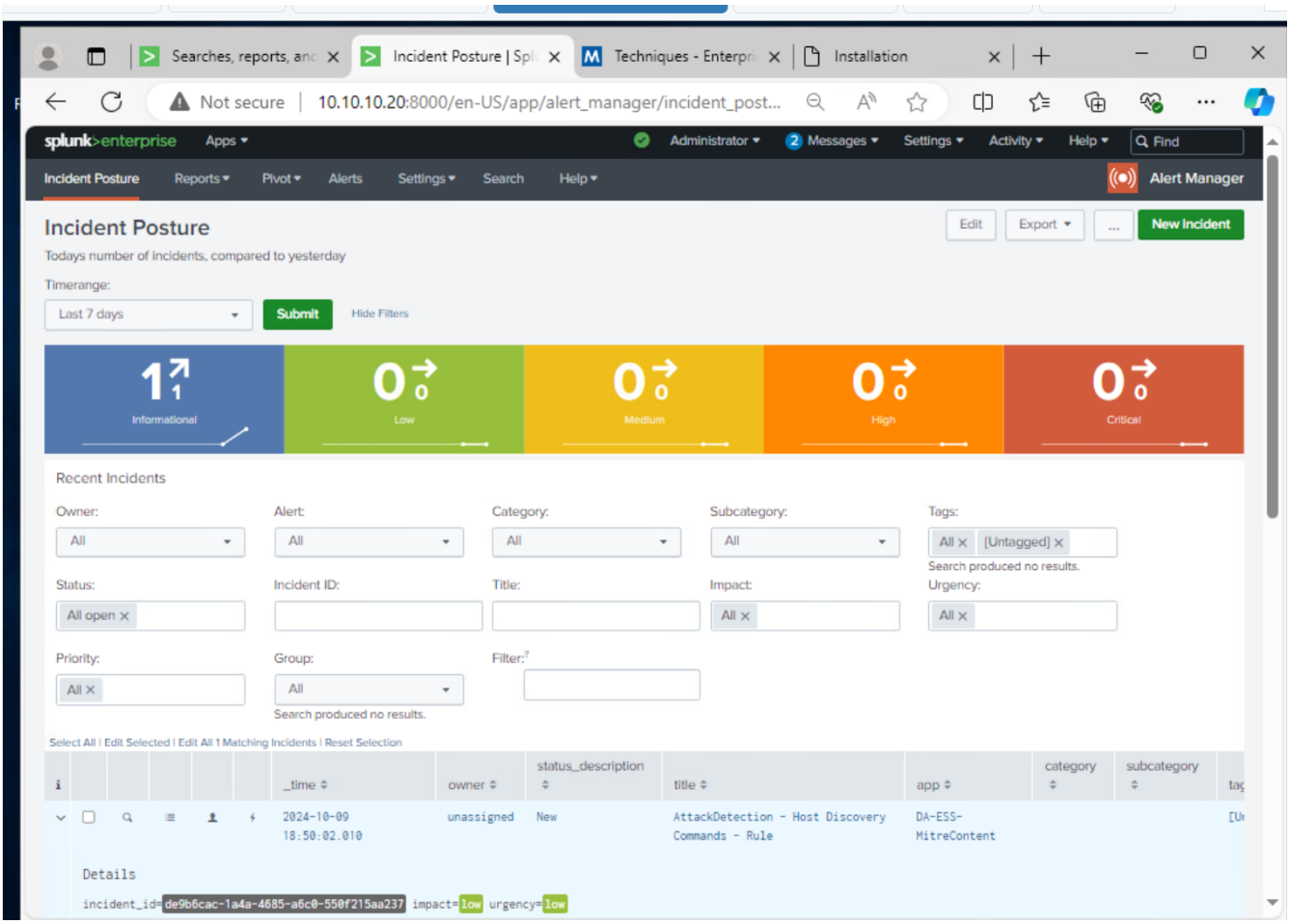
Administrator: Command Prompt

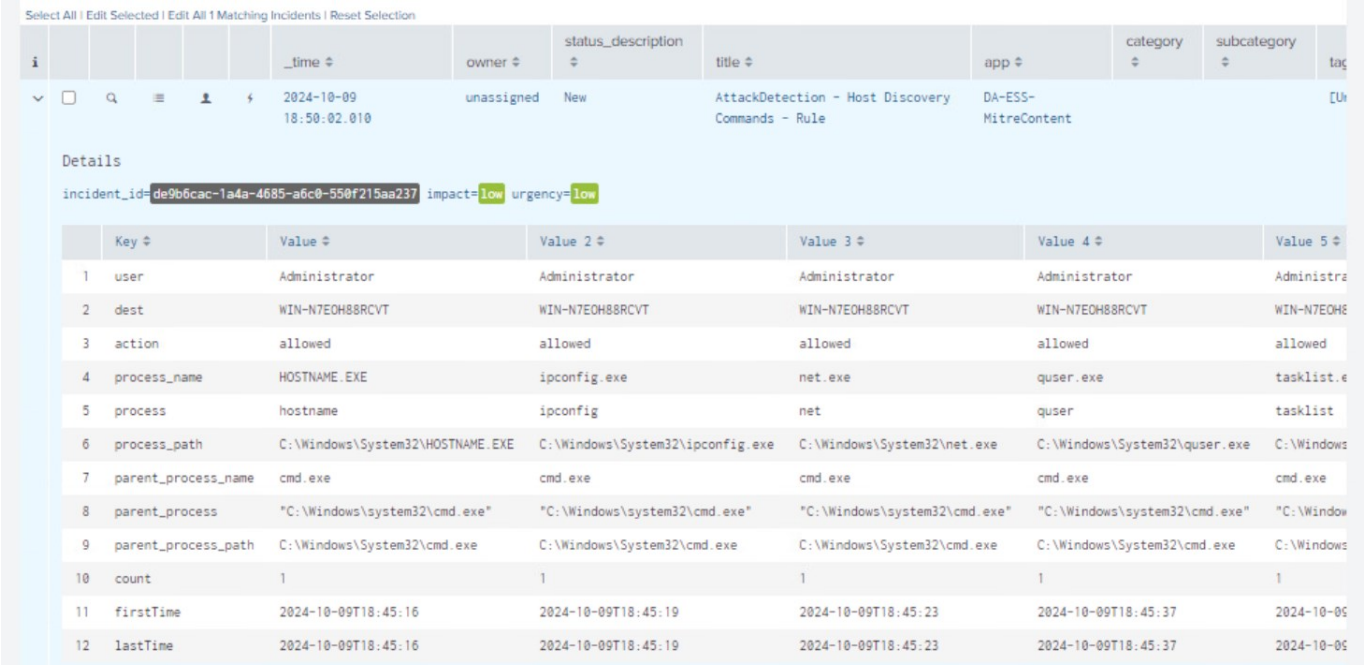
```
Ethernet adapter Ethernet1:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::7d2f:39fd:2e9c:54b1%
7
   IPv4 Address. . . . . . . . . . . : 10.20.20.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.20.20.254

Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c474:674b:b553:8470%
4
   IPv4 Address. . . . . . . . . . . : 10.10.10.15
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.254

C:\>net
The syntax of this command is:

NET
```

Part 3 – Analysis

Give it 5-10 minutes, then go to the alert manager application. You should see a new alert in the informational column! Take a full page screenshot including the details of the alert below.

Answer: See Screenshots below





	Key	Value	Value 2	Value 3	Value 4	Value 5
1	user	Administrator	Administrator	Administrator	Administrator	Administra
2	dest	WIN-N7EOH88RCVT	WIN-N7EOH88RCVT	WIN-N7EOH88RCVT	WIN-N7EOH88RCVT	WIN-N7EOH8
3	action	allowed	allowed	allowed	allowed	allowed
4	process_name	HOSTNAME.EXE	ipconfig.exe	net.exe	quser.exe	tasklist.e
5	process	hostname	ipconfig	net	quser	tasklist
6	process_path	C:\Windows\System32\HOSTNAME.EXE	C:\Windows\System32\ipconfig.exe	C:\Windows\System32\net.exe	C:\Windows\System32\quser.exe	C:\Windows
7	parent_process_name	cmd.exe	cmd.exe	cmd.exe	cmd.exe	cmd.exe
8	parent_process	"C:\Windows\system32\cmd.exe"	"C:\Windows\system32\cmd.exe"	"C:\Windows\system32\cmd.exe"	"C:\Windows\system32\cmd.exe"	"C:\Window
9	parent_process_path	C:\Windows\System32\cmd.exe	C:\Windows\System32\cmd.exe	C:\Windows\System32\cmd.exe	C:\Windows\System32\cmd.exe	C:\Windows
10	count	1	1	1	1	1
11	firstTime	2024-10-09T18:45:16	2024-10-09T18:45:19	2024-10-09T18:45:23	2024-10-09T18:45:37	2024-10-09
12	lastTime	2024-10-09T18:45:16	2024-10-09T18:45:19	2024-10-09T18:45:23	2024-10-09T18:45:37	2024-10-09

2) **Include screenshots above. What is the parent process of the command(s) that were run? What were the process names? What user ran the commands? Does this information match with the actions you took? (1 pt)**

Answer:

The parent processes of the command that were run were: “C:\Windows\system32\cmd.exe

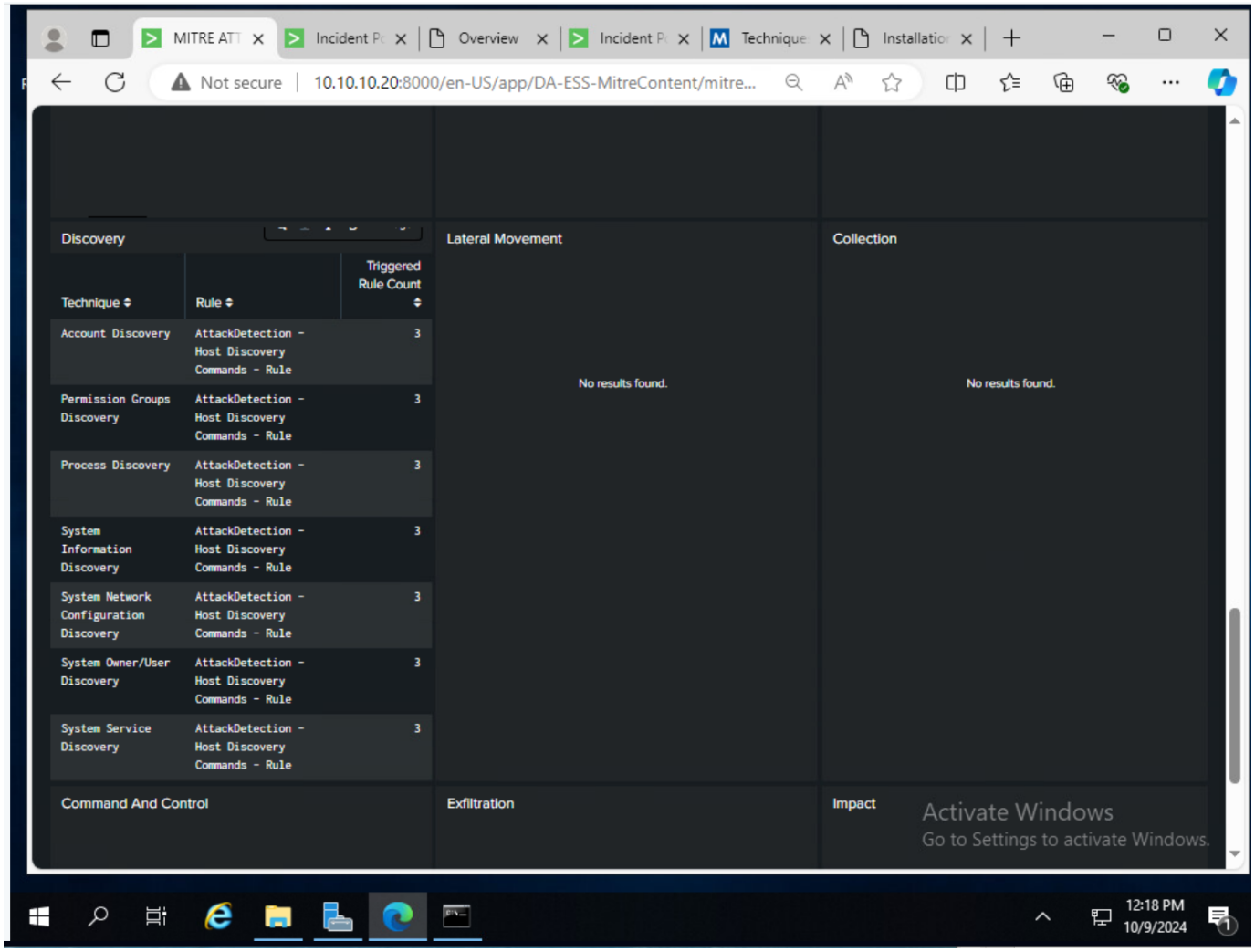
The process names were all cmd.exe.

The Administrator user ran the commands.

Yes, this information matches the actions that I took. I literally typed in hostname (enter), then ipconfig, then net, then quser, then tasklist last. So I know the results in the screenshot are 100% accurate.

This application provides a visualization and breakdown of different mitre TTPs. Scroll down to the Discovery tactic and take a screenshot of what is displayed.

Answer: See Screenshot below.



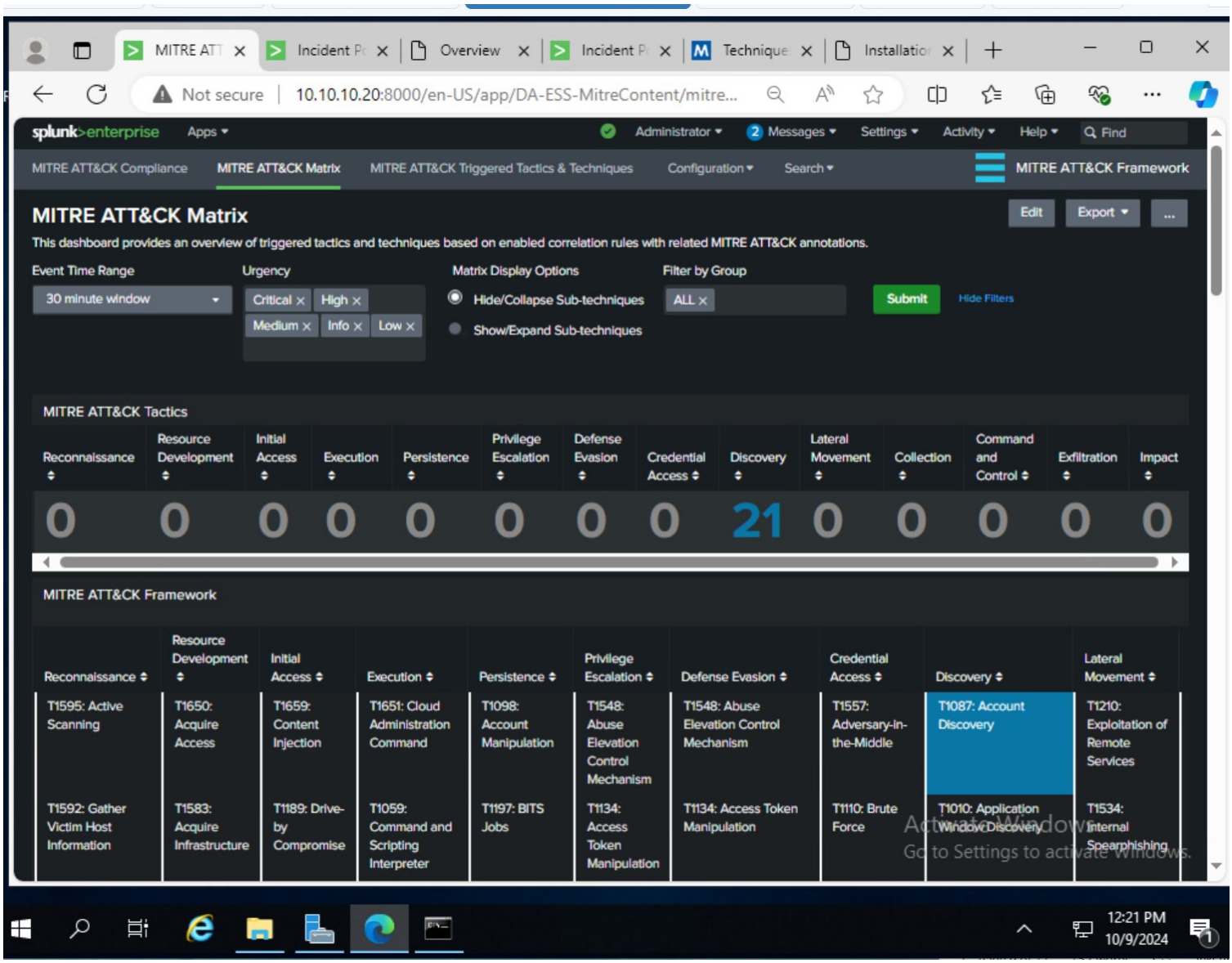
3) **Include screenshots above. How many tactics have hits? What are they? (1pt)**

Answer:

Only one tactic has hits, which is the TA007 Discovery MITRE tactic.

They hits would be classified as related to the following techniques: T1087 (Account Discovery), T1069 (Permission Groups Discovery), T1057 (Process Discovery), T1082 (System Information Discovery), T1016 (System Network Configuration Discovery), T1033 (System Owner/User Discovery), T1007 (System Service Discovery), which are the ones in the rule and also the ones in the Discovery section in the screenshot above.

See Screenshot below:



Part 4 – Custom Rules

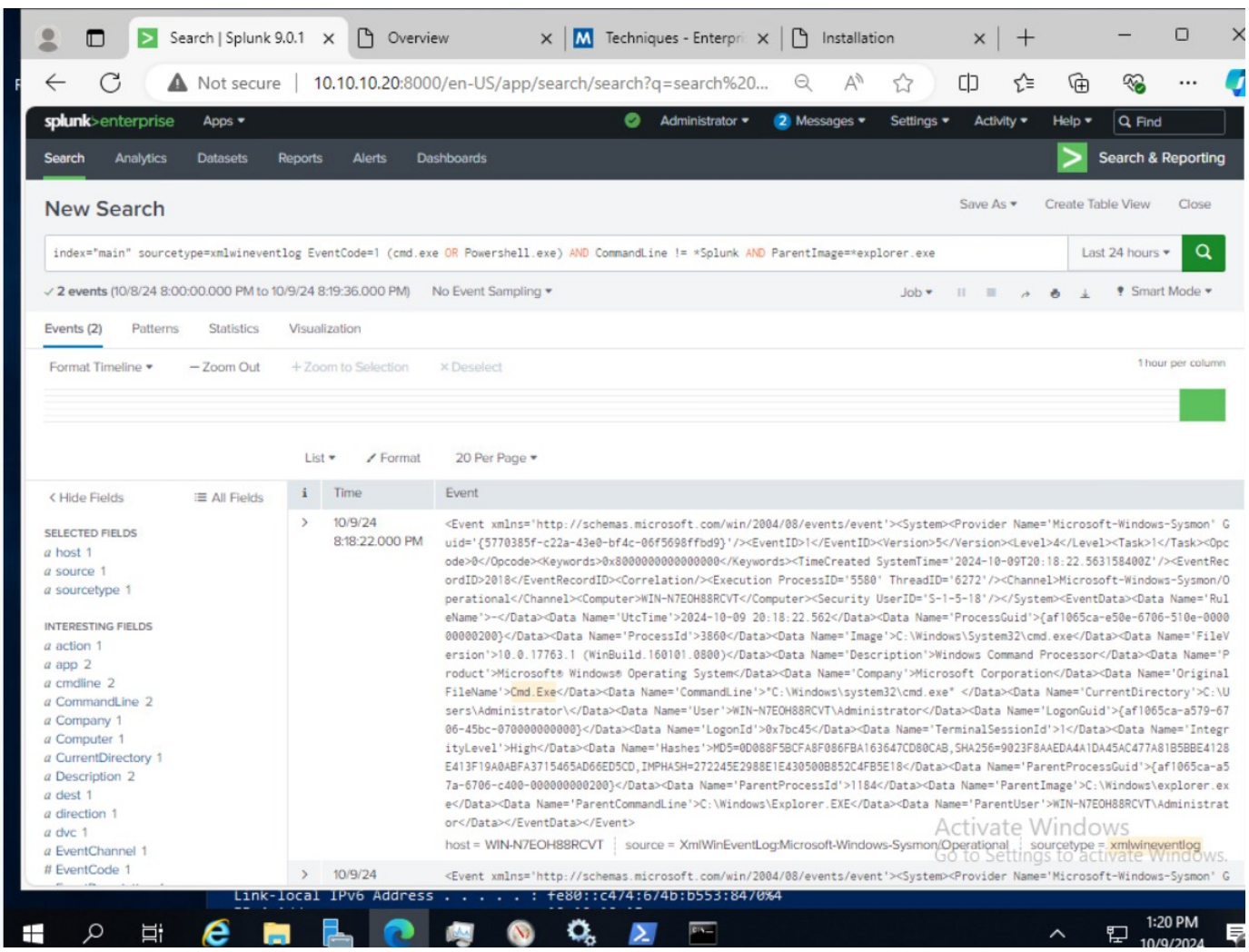
4) What does this search look for? How might this be malicious? How might it not? (1pt)

Answer:

This search looks for event logs in the default main index in Splunk for process creation events. Of these process creation events, it's filtering through only events that involved executed cmd.exe or powershelle.exe. The != after CommandLine means it wants to exclude anything with "Splunk" word in it. ***However,*** I redid the search and I deleted the AND CommandLine != *Splunk and I got the same results. Lastly, the ParentImage= explorer means it is only asking to see logs where the .exe events that were executed were executed in explorer.exe.

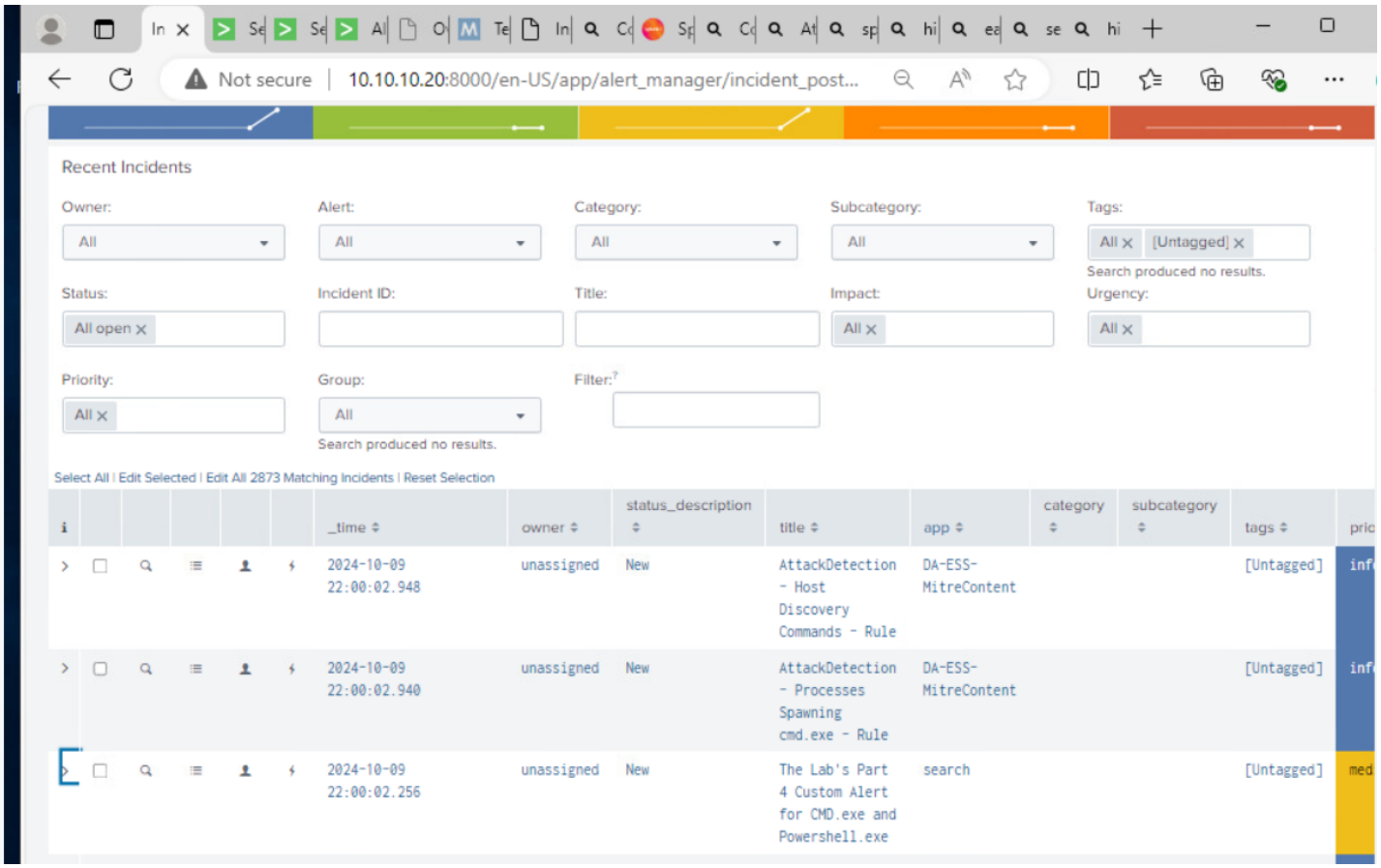
This might be malicious because we learned in class that when a process/program appears to be opened under the ParentImage=explorer.exe that it looks like normal activity and *could* mean that an adversary is trying to run it. However, it might not be malicious because I deleted the "ParentImage=*explorer.exe" and redid the search and I got 515 event results instead of 2 results. So what I noticed is they are all around the same time and it could be a UniversalSplunkForwarder Install/restart event that actually only occurred during an installation by the original user. Anyways, I don't think the results are malicious.

See Screenshot below



On the windows 2019 host, run cmd.exe and powershell.exe Return to Alert Manager. You should see your new alert hit the queue. Take a screenshot of the alert.

See screenshot from the Alert Manager above.



5) **Include screenshots above. Come up with you own search and make it into an alert. Include the search here, along with a screenshot of the alert triggered in alert manager. (1 pt)**

Answer:

Command I searched in the Search and Reporting search bar:

index="main" (msedge.exe OR ieexplorer.exe)

This search searches for all event logs relating to these two internet browsing programs. I titled it when I saved it as "Internet Explorer/Edge Special Alert".

See Screenshot below of the Alert Manager showing my Alerts.

splunk>enterprise Apps ▾ Administrator ▾ 2 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Search Analytics Datasets Reports Alerts Dashboards Search & Reporting

Alerts

Alerts set a condition that triggers an action, such as sending an email that contains the results of the triggering search to a list of people. Click the name to view the alert. Open the alert in Search to refine the parameters.

2 Alerts All Yours This App's filter

Title	Actions	Owner	App	Sharing	Status
Internet Explorer/Edge Special Alert	Open in Search Edit ▾	admin	search	Private	Enabled
The Lab's Part 4 Custom Alert for CMD.exe and Powershe...	Open in Search Edit ▾	admin	search	Private	Enabled

This alert looks for the Internet Explorer OR Microsoft Edge Browsers Running

Enabled: ..... Yes. Disable
Permissions: ..... Private. Owned by admin. Edit
Modified: ..... Oct 9, 2024 9:46:39 PM
Alert Type: ..... Scheduled. Cron Schedule. Edit
Trigger Condition: .. Number of Results is > 0. Edit
Actions: ..... ✓1 Action Edit
Alert Manager

Not secure | 10.10.10.20:8000/en-US/app/alert_manager/incident_post...

Informational	Low	Medium	High	Critical
2,872 / 2,872	0 / 0	2 / 2	0 / 0	0 / 0

<1m ago

Recent Incidents

Owner: All | Alert: All | Category: All | Subcategory: All | Tags: All × [Untagged] ×
Search produced no results.

Status: All open × | Incident ID: | Title: | Impact: All × | Urgency: All ×

Priority: All × | Group: All | Filter:?
Search produced no results.

Select All | Edit Selected | Edit All 2874 Matching Incidents | Reset Selection

_time	owner	status_description	title	app	category	subcategory	tags	priority
2024-10-09 22:00:03.948		New	Internet Explorer/Edge Special Alert	search			[Untagged]	medium
2024-10-09 22:00:02.948	unassigned	New	AttackDetection - Host Discovery Commands - Rule	DA-ESS-MitreContent			[Untagged]	informational
2024-10-09 22:00:02.940	unassigned	New	AttackDetection - Processes Spawning cmd.exe - Rule	DA-ESS-MitreContent			[Untagged]	informational
2024-10-09 22:00:02.256	unassigned	New	The Lab's Part 4 Custom Alert for CMD.exe and Powershell.exe	search			[Untagged]	medium
2024-10-09	unassigned	New	Eric's Question	search			[Untagged]	informational

3:02 PM
10/9/2024