ITS60 – Cybersecurity Operations Capstone Project – Week 1 Lab Project
Title: End-to-End SOC Engagement Simulation
Date: ____________
Student Name: Jesus Ortiz

🔷 Objective:

Establish situational awareness by performing asset discovery and documenting the network layout, then configuring basic centralized log ingestion. These actions create visibility into the environment, which will be leveraged in future threat detection, vulnerability assessment, and incident response.

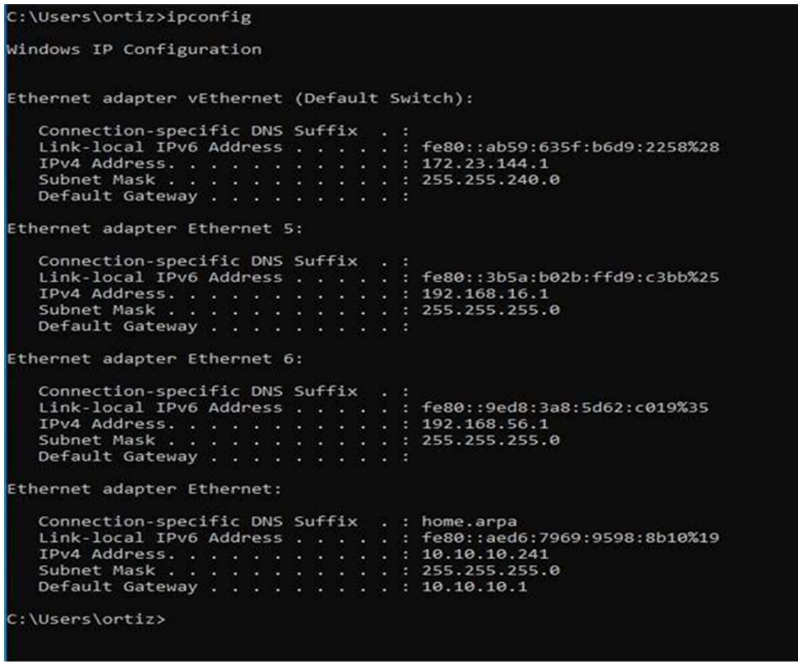
🔷 Terminology

- **Reconnaissance** – Gathering system and network information.
- **Asset Inventory** – List of all systems, services, and IPs in an environment.
- **Network Topology** – Logical and/or physical layout of a network.
- **Log Ingestion** – Collecting and importing logs into a central system.
- **MITRE ATTsCK** – A framework for classifying adversary tactics and techniques.

🔷 Part 1: Network Discovery and Asset Mapping

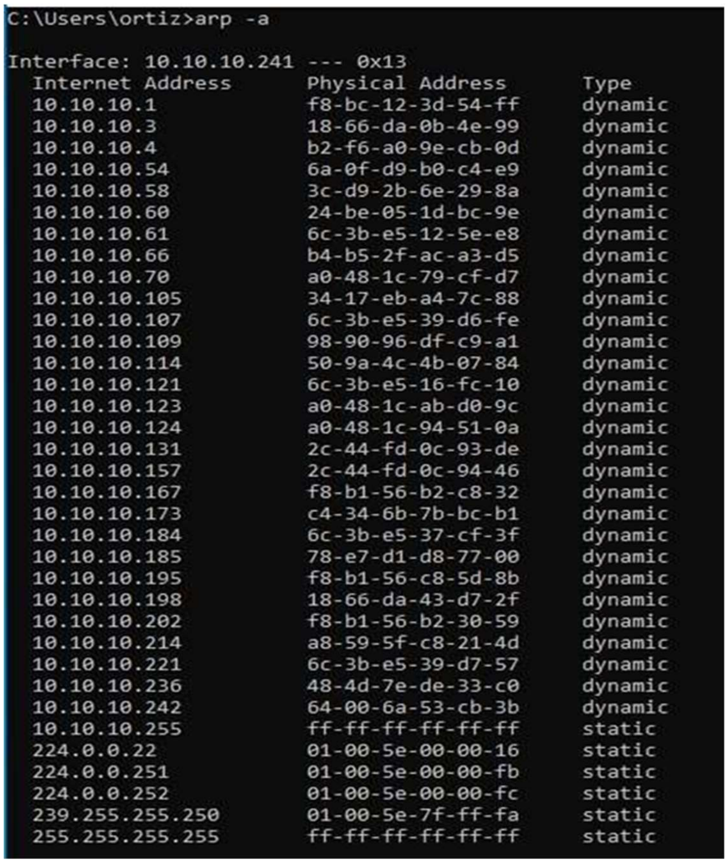
Instructions:

1. On **Windows**, open Command Prompt:
   - **ipconfig** – Show IP configuration.



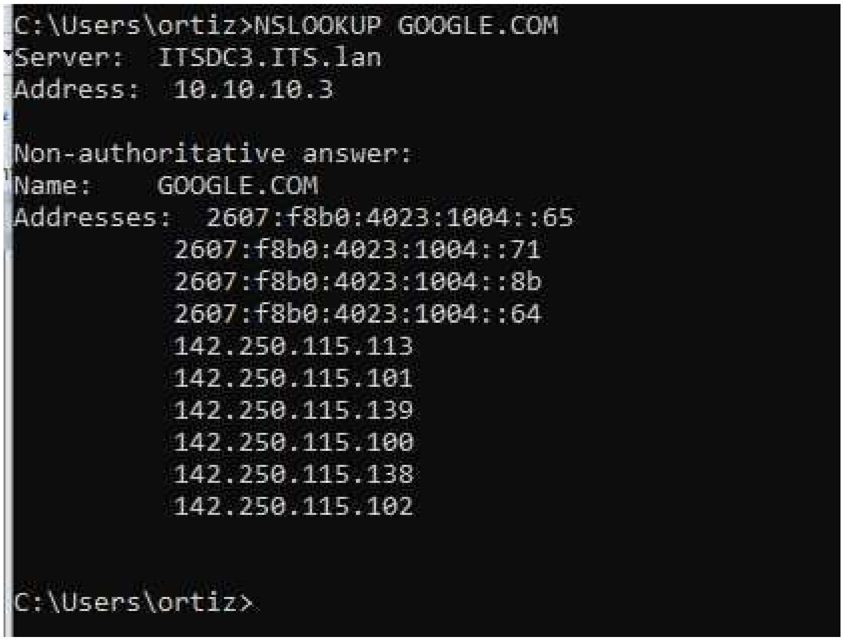
```
C:\Users\ortiz>ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::ab59:635f:b6d9:2258%28
   IPv4 Address. . . . . . . . . . . : 172.23.144.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 5:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::3b5a:b02b:ffd9:c3bb%25
   IPv4 Address. . . . . . . . . . . : 192.168.16.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet 6:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::9ed8:3a8:5d62:c019%35
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : home.arpa
   Link-local IPv6 Address . . . . . : fe80::aed6:7969:9598:8b10%19
   IPv4 Address. . . . . . . . . . . : 10.10.10.241
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.1

C:\Users\ortiz>
```

- **arp -a** – List known IP-to-MAC mappings.



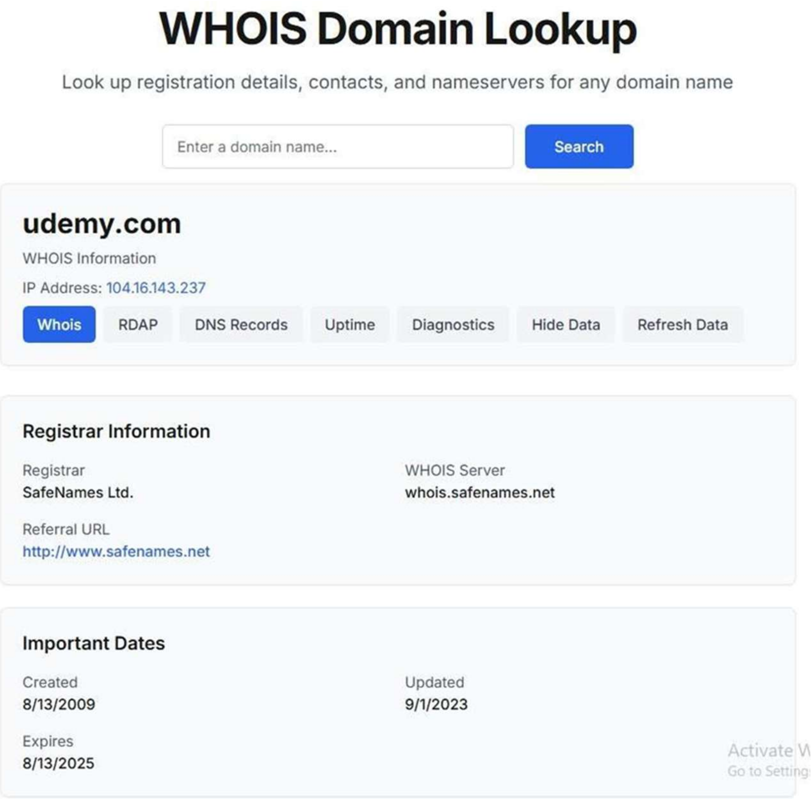
```
C:\Users\ortiz>arp -a

Interface: 10.10.10.241 --- 0x13
  Internet Address      Physical Address      Type
  10.10.10.1            f8-bc-12-3d-54-ff     dynamic
  10.10.10.3            18-66-da-0b-4e-99     dynamic
  10.10.10.4            b2-f6-a0-9e-cb-0d     dynamic
  10.10.10.54           6a-0f-d9-b0-c4-e9     dynamic
  10.10.10.58           3c-d9-2b-6e-29-8a     dynamic
  10.10.10.60           24-be-05-1d-bc-9e     dynamic
  10.10.10.61           6c-3b-e5-12-5e-e8     dynamic
  10.10.10.66           b4-b5-2f-ac-a3-d5     dynamic
  10.10.10.70           a0-48-1c-79-cf-d7     dynamic
  10.10.10.105          34-17-eb-a4-7c-88     dynamic
  10.10.10.107          6c-3b-e5-39-d6-fe     dynamic
  10.10.10.109          98-90-96-df-c9-a1     dynamic
  10.10.10.114          50-9a-4c-4b-07-84     dynamic
  10.10.10.121          6c-3b-e5-16-fc-10     dynamic
  10.10.10.123          a0-48-1c-ab-d0-9c     dynamic
  10.10.10.124          a0-48-1c-94-51-0a     dynamic
  10.10.10.131          2c-44-fd-0c-93-de     dynamic
  10.10.10.157          2c-44-fd-0c-94-46     dynamic
  10.10.10.167          f8-b1-56-b2-c8-32     dynamic
  10.10.10.173          c4-34-6b-7b-bc-b1     dynamic
  10.10.10.184          6c-3b-e5-37-cf-3f     dynamic
  10.10.10.185          78-e7-d1-d8-77-00     dynamic
  10.10.10.195          f8-b1-56-c8-5d-8b     dynamic
  10.10.10.198          18-66-da-43-d7-2f     dynamic
  10.10.10.202          f8-b1-56-b2-30-59     dynamic
  10.10.10.214          a8-59-5f-c8-21-4d     dynamic
  10.10.10.221          6c-3b-e5-39-d7-57     dynamic
  10.10.10.236          48-4d-7e-de-33-c0     dynamic
  10.10.10.242          64-00-6a-53-cb-3b     dynamic
  10.10.10.255          ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

- **nslookup google.com** – DNS resolution test.



```
C:\Users\ortiz>NSLOOKUP GOOGLE.COM
Server:  ITSDC3.ITS.lan
Address:  10.10.10.3

Non-authoritative answer:
Name:    GOOGLE.COM
Addresses:  2607:f8b0:4023:1004::65
          2607:f8b0:4023:1004::71
          2607:f8b0:4023:1004::8b
          2607:f8b0:4023:1004::64
          142.250.115.113
          142.250.115.101
          142.250.115.139
          142.250.115.100
          142.250.115.138
          142.250.115.102


C:\Users\ortiz>
```

- Use https://who.is for WHOIS info.



WHOIS Domain Lookup

Look up registration details, contacts, and nameservers for any domain name

udemy.com

WHOIS Information

IP Address: 104.16.143.237

Registrar Information

Registrar: SafeNames Ltd.

WHOIS Server: whois.safenames.net

Referral URL: http://www.safenames.net

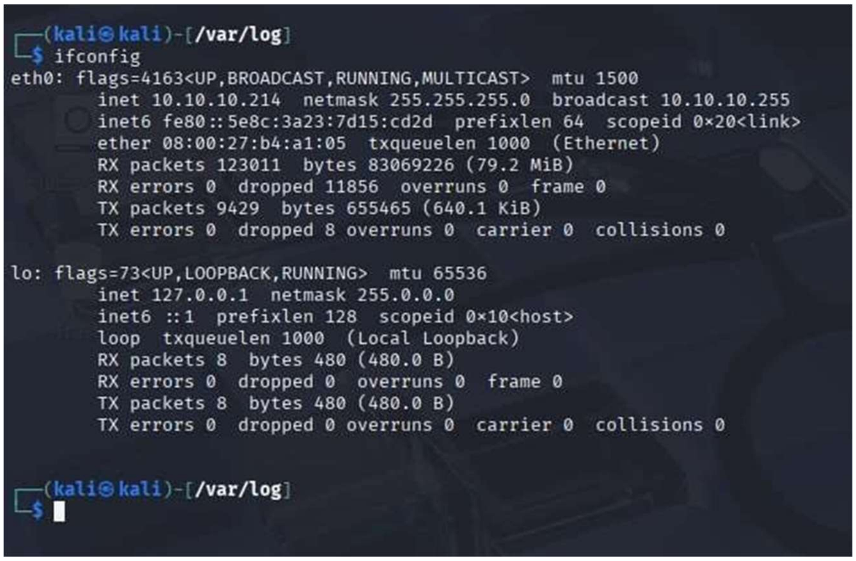
Important Dates

Created: 8/13/2009

Updated: 9/1/2023

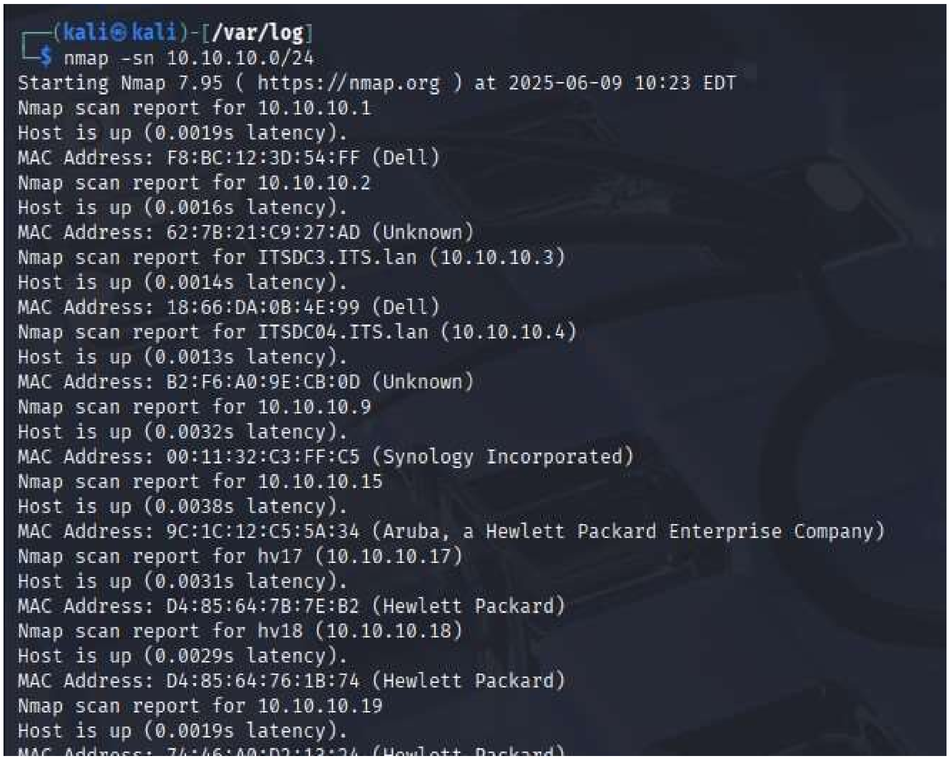
Expires: 8/13/2025

2. On **Kali Linux**, open Terminal:
   - **ifconfig** – Show IP information.



```
┌──(kali㉿kali)-[/var/log]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.10.10.214  netmask 255.255.255.0  broadcast 10.10.10.255
        inet6 fe80::5e8c:3a23:7d15:cd2d  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:b4:a1:05  txqueuelen 1000  (Ethernet)
        RX packets 123011  bytes 83069226 (79.2 MiB)
        RX errors 0  dropped 11856  overruns 0  frame 0
        TX packets 9429  bytes 655465 (640.1 KiB)
        TX errors 0  dropped 8 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 8  bytes 480 (480.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8  bytes 480 (480.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0


┌──(kali㉿kali)-[/var/log]
└─$ █
```

- **nmap -sn 10.10.10.0/24** – Detect live hosts on your subnet.



```
┌──(kali㉿kali)-[/var/log]
└─$ nmap -sn 10.10.10.0/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-09 10:23 EDT
Nmap scan report for 10.10.10.1
Host is up (0.0019s latency).
MAC Address: F8:BC:12:3D:54:FF (Dell)
Nmap scan report for 10.10.10.2
Host is up (0.0016s latency).
MAC Address: 62:7B:21:C9:27:AD (Unknown)
Nmap scan report for ITSDC3.ITS.lan (10.10.10.3)
Host is up (0.0014s latency).
MAC Address: 18:66:DA:0B:4E:99 (Dell)
Nmap scan report for ITSDC04.ITS.lan (10.10.10.4)
Host is up (0.0013s latency).
MAC Address: B2:F6:A0:9E:CB:0D (Unknown)
Nmap scan report for 10.10.10.9
Host is up (0.0032s latency).
MAC Address: 00:11:32:C3:FF:C5 (Synology Incorporated)
Nmap scan report for 10.10.10.15
Host is up (0.0038s latency).
MAC Address: 9C:1C:12:C5:5A:34 (Aruba, a Hewlett Packard Enterprise Company)
Nmap scan report for hv17 (10.10.10.17)
Host is up (0.0031s latency).
MAC Address: D4:85:64:7B:7E:B2 (Hewlett Packard)
Nmap scan report for hv18 (10.10.10.18)
Host is up (0.0029s latency).
MAC Address: D4:85:64:76:1B:74 (Hewlett Packard)
Nmap scan report for 10.10.10.19
Host is up (0.0019s latency).
MAC Address: 74:46:A0:D2:13:24 (Hewlett Packard)
```

Output from this section builds the inventory and map used in Part 2 and enables correlation with logs in Week 2.

➢ **Deliverables:**

- Screenshots of ARP and Nmap results.
- Table of discovered devices (IP, hostname, OS if known).

◆ Part 2: Log Collection Setup

Instructions:

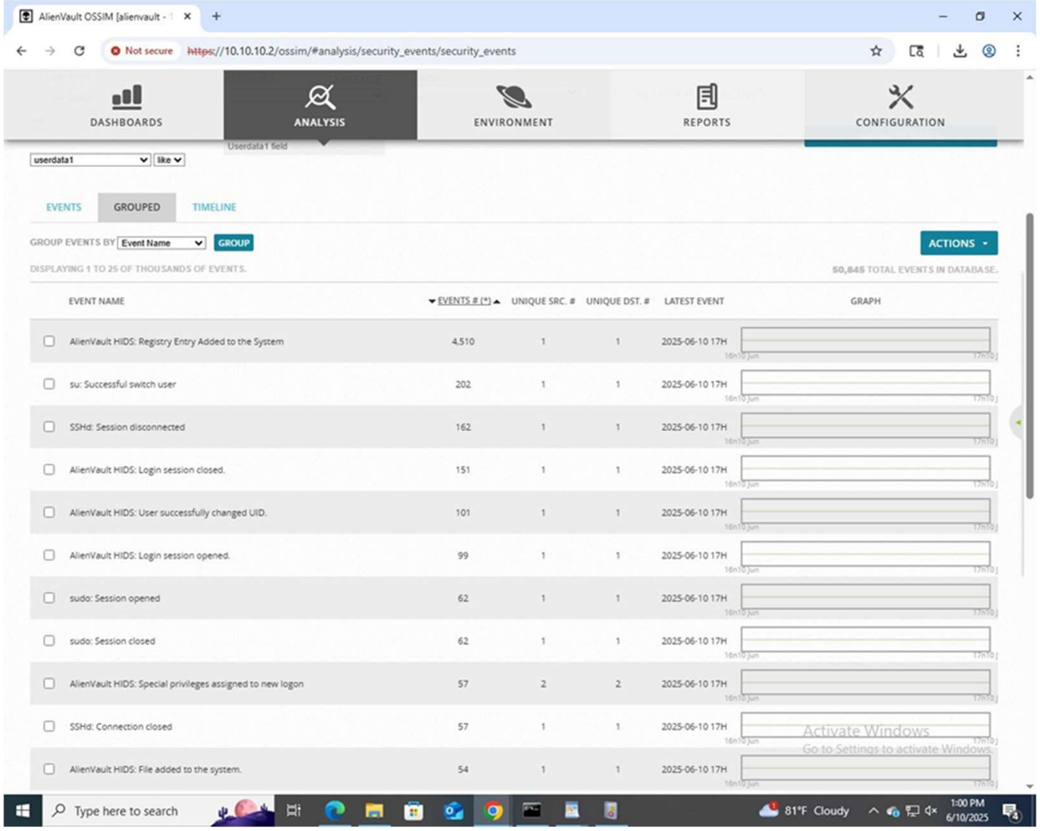
1. Choose a centralized log collector:
    - ○ **AlienVault** (Open Source): prebuilt VM
        - ▪ Username**: student**
        - ▪ Password**: Pass@2024**
2. Configure log sources:
    - ○ **Windows Workstation**:
        - ▪ Open Event Viewer → Export logs or configure forwarding.
    - ○ **Kali Linux**:
        - ▪ Run **journalctl -xe** or set up **rsyslog** to forward to the collector.

This data will be used in Week 2 to detect malicious activity.

3. Confirm logs are visible in the dashboard.

Deliverables:

- Screenshot of dashboard with 10+ log events.

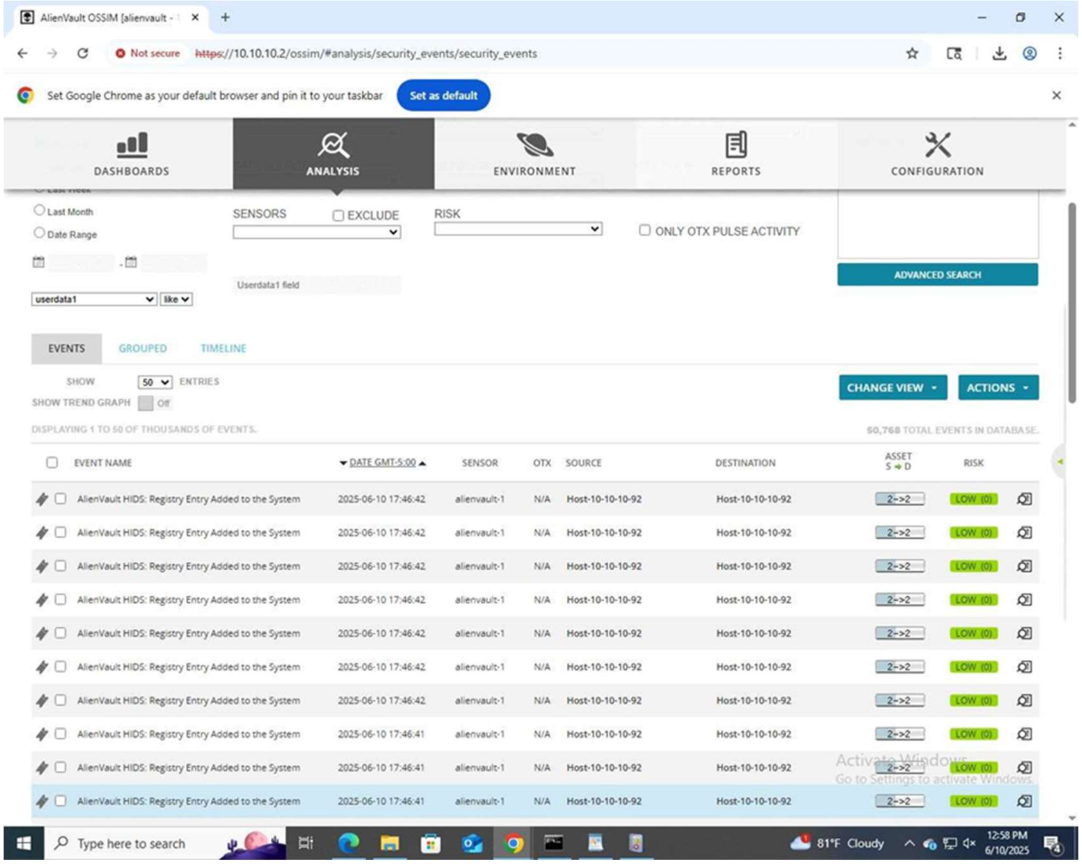


DISPLAYING 1 TO 25 OF THOUSANDS OF EVENTS.

50,845 TOTAL EVENTS IN DATABASE.

	EVENT NAME	EVENTS # (*)	UNIQUE SRC. #	UNIQUE DST. #	LATEST EVENT	GRAPH
□	AlienVault HIDS: Registry Entry Added to the System	4,510	1	1	2025-06-10 17H	
□	su: Successful switch user	202	1	1	2025-06-10 17H	
□	SSHd: Session disconnected	162	1	1	2025-06-10 17H	
□	AlienVault HIDS: Login session closed.	151	1	1	2025-06-10 17H	
□	AlienVault HIDS: User successfully changed UID.	101	1	1	2025-06-10 17H	
□	AlienVault HIDS: Login session opened.	99	1	1	2025-06-10 17H	
□	sudo: Session opened	62	1	1	2025-06-10 17H	
□	sudo: Session closed	62	1	1	2025-06-10 17H	
□	AlienVault HIDS: Special privileges assigned to new logon	57	2	2	2025-06-10 17H	
□	SSHd: Connection closed	57	1	1	2025-06-10 17H	
□	AlienVault HIDS: File added to the system.	54	1	1	2025-06-10 17H	

- Short list of captured log types (e.g., login, service errors).



AlienVault OSSIM [alienvault -

Not secure https://10.10.10.2/ossim/#analysis/security_events/security_events

Set Google Chrome as your default browser and pin it to your taskbar Set as default

○ Last Month
○ Date Range

SENSORS □ EXCLUDE

RISK

□ ONLY OTX PULSE ACTIVITY

userdata1 like

Userdata1 field

SHOW 50 ENTRIES

SHOW TREND GRAPH Off

DISPLAYING 1 TO 50 OF THOUSANDS OF EVENTS.

50,768 TOTAL EVENTS IN DATABASE.

EVENT NAME	DATE GMT-5:00	SENSOR	OTX	SOURCE	DESTINATION	ASSET S → D	RISK
AlienVault HIDS: Registry Entry Added to the System	2025-06-10 17:46:42	alienvault-1	N/A	Host-10-10-10-92	Host-10-10-10-92	2->2	LOW (0)
AlienVault HIDS: Registry Entry Added to the System	2025-06-10 17:46:42	alienvault-1	N/A	Host-10-10-10-92	Host-10-10-10-92	2->2	LOW (0)
AlienVault HIDS: Registry Entry Added to the System	2025-06-10 17:46:42	alienvault-1	N/A	Host-10-10-10-92	Host-10-10-10-92	2->2	LOW (0)
AlienVault HIDS: Registry Entry Added to the System	2025-06-10 17:46:42	alienvault-1	N/A	Host-10-10-10-92	Host-10-10-10-92	2->2	LOW (0)
AlienVault HIDS: Registry Entry Added to the System	2025-06-10 17:46:42	alienvault-1	N/A	Host-10-10-10-92	Host-10-10-10-92	2->2	LOW (0)
AlienVault HIDS: Registry Entry Added to the System	2025-06-10 17:46:42	alienvault-1	N/A	Host-10-10-10-92	Host-10-10-10-92	2->2	LOW (0)
AlienVault HIDS: Registry Entry Added to the System	2025-06-10 17:46:42	alienvault-1	N/A	Host-10-10-10-92	Host-10-10-10-92	2->2	LOW (0)
AlienVault HIDS: Registry Entry Added to the System	2025-06-10 17:46:41	alienvault-1	N/A	Host-10-10-10-92	Host-10-10-10-92	2->2	LOW (0)
AlienVault HIDS: Registry Entry Added to the System	2025-06-10 17:46:41	alienvault-1	N/A	Host-10-10-10-92	Host-10-10-10-92	2->2	LOW (0)
AlienVault HIDS: Registry Entry Added to the System	2025-06-10 17:46:41	alienvault-1	N/A	Host-10-10-10-92	Host-10-10-10-92	2->2	LOW (0)

Activate Windows
Go to Settings to activate Windows.

Type here to search

81°F Cloudy

12:58 PM
6/10/2025

Reflection Questions

1. What tool revealed the most useful data?
   NMAP, and Alien Vault OSSIM

2. How does knowing your assets help in detection?
   Asset discovery and documenting your network layout are foundational for threat detection, providing the necessary visibility and context for vulnerability management, incident response, risk mitigation, and compliance.

3. Why is centralized logging critical for SOC?
   Centralized logging is critical for Security Operations Centers because it provides the foundational visibility needed to effectively detect, investigate, and respond to security threats.

4. How might attackers exploit unmonitored systems?
   Attackers exploit unmonitored systems by gaining unauthorized access and

operating undetected, often through exploiting vulnerabilities in outdated software, misconfigurations, or by targeting endpoints as easy entry points. This allows them to move laterally within the network without raising suspicion, potentially leading to data breaches and other malicious activity.

Instructor Initials: __________________________

ITS60 – Cybersecurity Operations
Capstone Project – Week 2 Lab
Project Title: Threat Intelligence C Malicious Activity Detection
Date: ____________
Student Name: _________________________________

◆ Objective:

Use threat intelligence feeds to analyze logs collected in Week 1, ***identify Indicators of Compromise (IOCs***), and detect suspicious behaviors using MITRE ATTCCK mapping.

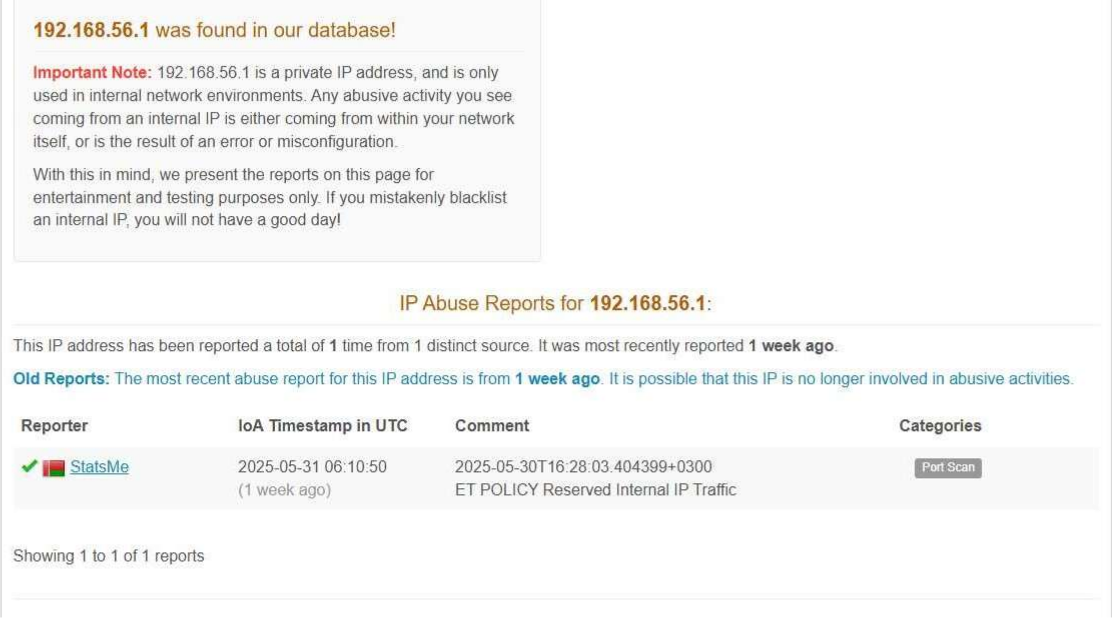
◆ Terminology

- **Threat Intelligence** – Contextual threat knowledge.
- **IOC** – Indicators of Compromise (e.g., malicious IPs, hashes).
- **Abnormal Events** – Suspicious log patterns.
- **Log Correlation** – Finding connections among multiple logs.
- **MITRE Techniques** – Known attacker behaviors and tactics.

◆ Part 1: IOC Lookup and Threat Feed Analysis

F Instructions:

1. Visit:
   - https://abuseipdb.com
2. Look up 2 IPs from your Week 1 logs.
   192.168.56.1, 192.168.16.1
3. Record:
   - Threat category
   - Region
   - Comments or scores



192.168.56.1 was found in our database!

Important Note: 192.168.56.1 is a private IP address, and is only used in internal network environments. Any abusive activity you see coming from an internal IP is either coming from within your network itself, or is the result of an error or misconfiguration.

With this in mind, we present the reports on this page for entertainment and testing purposes only. If you mistakenly blacklist an internal IP, you will not have a good day!

IP Abuse Reports for **192.168.56.1**:

This IP address has been reported a total of **1** time from **1** distinct source. It was most recently reported **1 week ago**.

Old Reports: The most recent abuse report for this IP address is from **1 week ago**. It is possible that this IP is no longer involved in abusive activities.

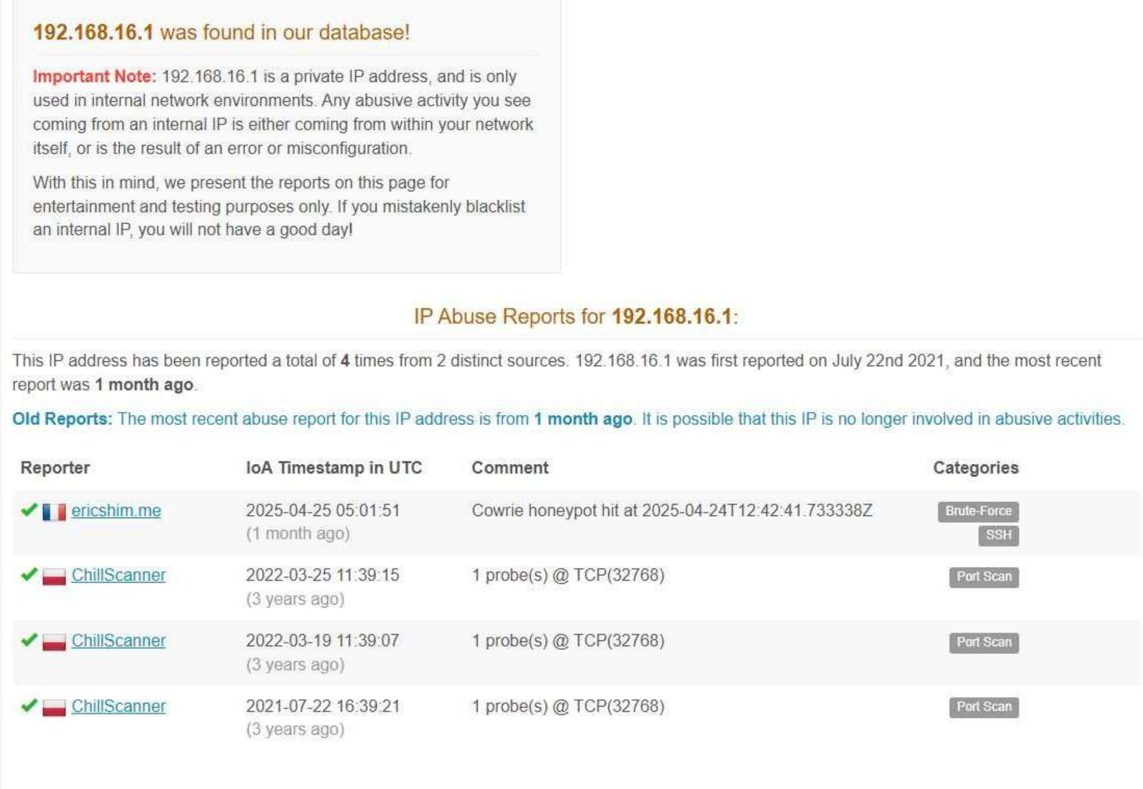
Reporter	IoA Timestamp in UTC	Comment	Categories
✓ StatsMe	2025-05-31 06:10:50 (1 week ago)	2025-05-30T16:28:03.404399+0300 ET POLICY Reserved Internal IP Traffic	Port Scan

Showing 1 to 1 of 1 reports

Location : Belarus

Comment : 2025-05-30T16:28:03.404399+0300 ET POLICY

Reserved Internal IP Traffic Threat Categories: Port Scan



192.168.16.1 was found in our database!

Important Note: 192.168.16.1 is a private IP address, and is only used in internal network environments. Any abusive activity you see coming from an internal IP is either coming from within your network itself, or is the result of an error or misconfiguration.

With this in mind, we present the reports on this page for entertainment and testing purposes only. If you mistakenly blacklist an internal IP, you will not have a good day!

IP Abuse Reports for **192.168.16.1**:

This IP address has been reported a total of **4** times from 2 distinct sources. 192.168.16.1 was first reported on July 22nd 2021, and the most recent report was **1 month ago**.

Old Reports: The most recent abuse report for this IP address is from **1 month ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp in UTC	Comment	Categories
✓ ericshim.me	2025-04-25 05:01:51 (1 month ago)	Cowrie honeypot hit at 2025-04-24T12:42:41.733338Z	Brute-Force SSH
✓ ChillScanner	2022-03-25 11:39:15 (3 years ago)	1 probe(s) @ TCP(32768)	Port Scan
✓ ChillScanner	2022-03-19 11:39:07 (3 years ago)	1 probe(s) @ TCP(32768)	Port Scan
✓ ChillScanner	2021-07-22 16:39:21 (3 years ago)	1 probe(s) @ TCP(32768)	Port Scan

Location : France

Comments : Cowrie Honeypot hit at 2025-04-24T12:42:41.733338Z Threat Categories: Brute-Force, SSH

■ These findings guide detection in Part 2 and response actions in Week 4.

Deliverables:

- IOC summary table (IP, threat type, comments)

1-paragraph summary: how threat feeds assisted analysis

Summary:

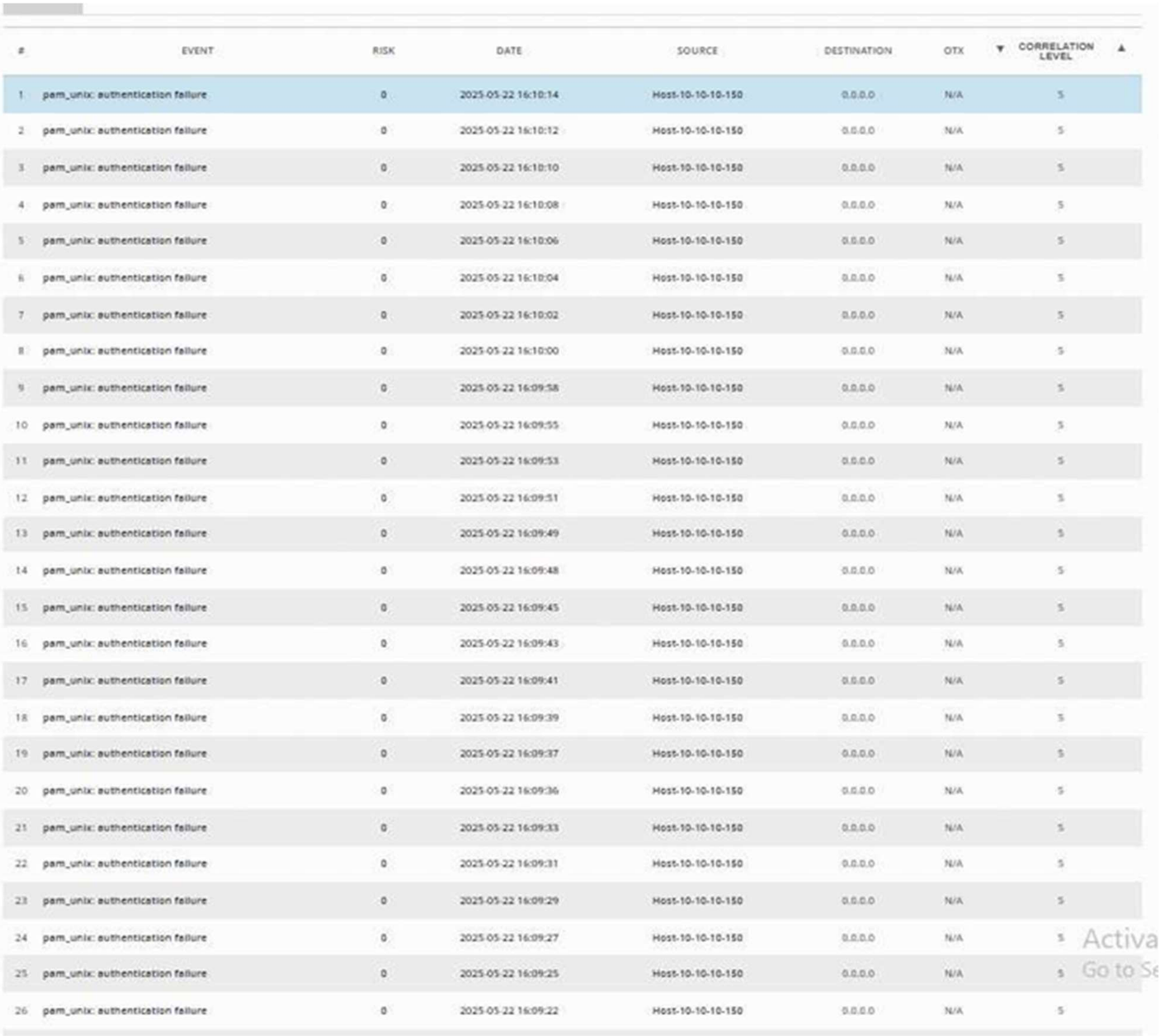
Threat feeds play a crucial role in assisting analysis by providing real-time, curated information on emerging threats and vulnerabilities. These feeds aggregate data from multiple sources, such as security vendors, government agencies, and open-source platforms, offering insights into known malicious IP addresses, domains, malware signatures, and tactics used by cyber adversaries. By integrating threat feeds into security systems, analysts can quickly identify indicators of compromise (IOCs), track attack patterns, and improve their incident detection and response capabilities. This proactive approach allows security teams to stay ahead of potential threats, prioritize risks, and enhance their overall defense posture.

◆ Part 2: Detect Malicious Patterns in Logs

Instructions:

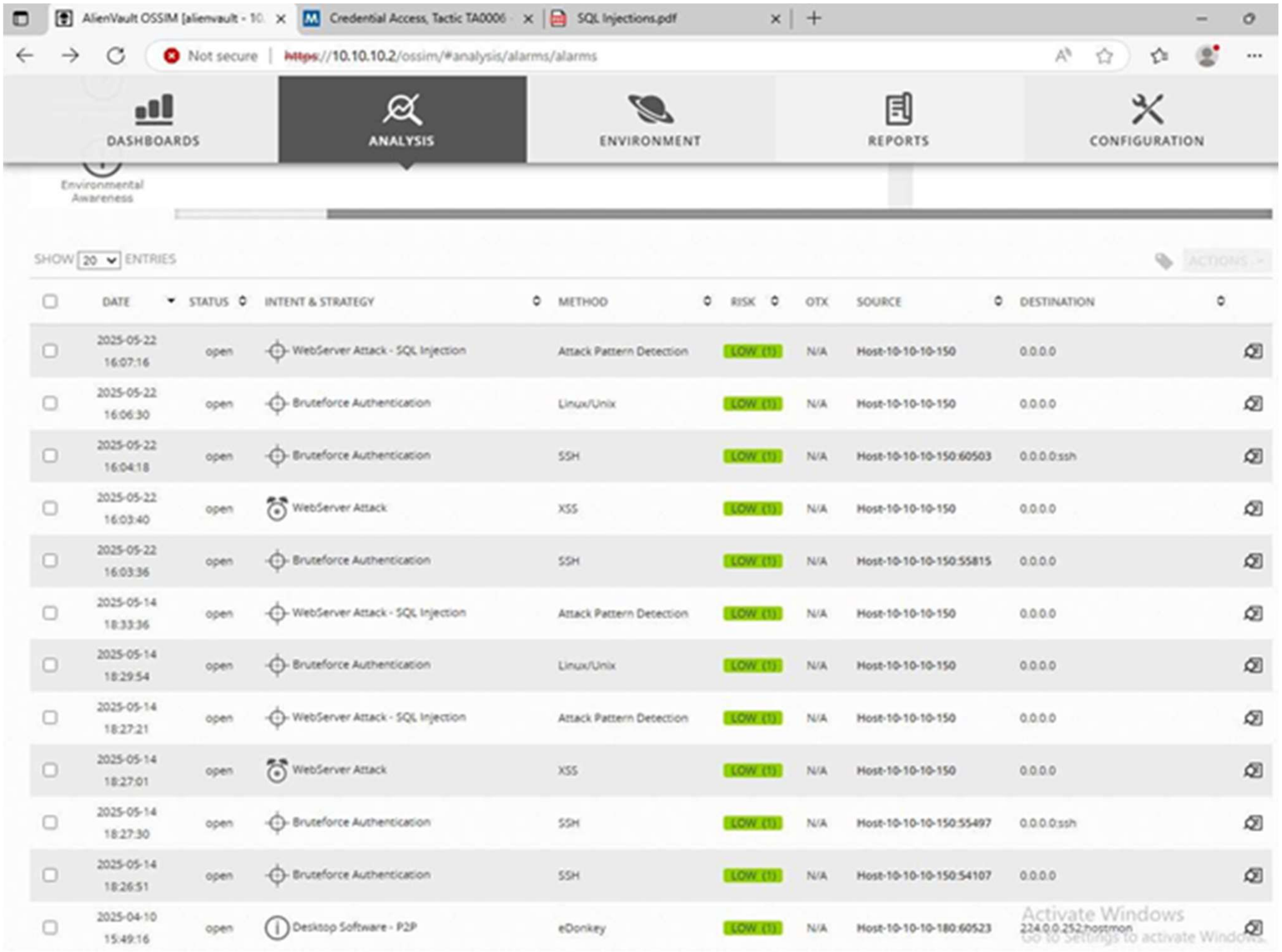
1. Open **AlienVault** dashboard.
2. Search for suspicious activity in Alarms

- Multiple failed login attempts - Brute Force



#	EVENT	RISK	DATE	SOURCE	DESTINATION	OTX	CORRELATION LEVEL
1	pam_unix: authentication failure	0	2025-05-22 16:10:14	Host-10-10-10-150	0.0.0.0	N/A	5
2	pam_unix: authentication failure	0	2025-05-22 16:10:12	Host-10-10-10-150	0.0.0.0	N/A	5
3	pam_unix: authentication failure	0	2025-05-22 16:10:10	Host-10-10-10-150	0.0.0.0	N/A	5
4	pam_unix: authentication failure	0	2025-05-22 16:10:08	Host-10-10-10-150	0.0.0.0	N/A	5
5	pam_unix: authentication failure	0	2025-05-22 16:10:06	Host-10-10-10-150	0.0.0.0	N/A	5
6	pam_unix: authentication failure	0	2025-05-22 16:10:04	Host-10-10-10-150	0.0.0.0	N/A	5
7	pam_unix: authentication failure	0	2025-05-22 16:10:02	Host-10-10-10-150	0.0.0.0	N/A	5
8	pam_unix: authentication failure	0	2025-05-22 16:10:00	Host-10-10-10-150	0.0.0.0	N/A	5
9	pam_unix: authentication failure	0	2025-05-22 16:09:58	Host-10-10-10-150	0.0.0.0	N/A	5
10	pam_unix: authentication failure	0	2025-05-22 16:09:55	Host-10-10-10-150	0.0.0.0	N/A	5
11	pam_unix: authentication failure	0	2025-05-22 16:09:53	Host-10-10-10-150	0.0.0.0	N/A	5
12	pam_unix: authentication failure	0	2025-05-22 16:09:51	Host-10-10-10-150	0.0.0.0	N/A	5
13	pam_unix: authentication failure	0	2025-05-22 16:09:49	Host-10-10-10-150	0.0.0.0	N/A	5
14	pam_unix: authentication failure	0	2025-05-22 16:09:48	Host-10-10-10-150	0.0.0.0	N/A	5
15	pam_unix: authentication failure	0	2025-05-22 16:09:45	Host-10-10-10-150	0.0.0.0	N/A	5
16	pam_unix: authentication failure	0	2025-05-22 16:09:43	Host-10-10-10-150	0.0.0.0	N/A	5
17	pam_unix: authentication failure	0	2025-05-22 16:09:41	Host-10-10-10-150	0.0.0.0	N/A	5
18	pam_unix: authentication failure	0	2025-05-22 16:09:39	Host-10-10-10-150	0.0.0.0	N/A	5
19	pam_unix: authentication failure	0	2025-05-22 16:09:37	Host-10-10-10-150	0.0.0.0	N/A	5
20	pam_unix: authentication failure	0	2025-05-22 16:09:36	Host-10-10-10-150	0.0.0.0	N/A	5
21	pam_unix: authentication failure	0	2025-05-22 16:09:33	Host-10-10-10-150	0.0.0.0	N/A	5
22	pam_unix: authentication failure	0	2025-05-22 16:09:31	Host-10-10-10-150	0.0.0.0	N/A	5
23	pam_unix: authentication failure	0	2025-05-22 16:09:29	Host-10-10-10-150	0.0.0.0	N/A	5
24	pam_unix: authentication failure	0	2025-05-22 16:09:27	Host-10-10-10-150	0.0.0.0	N/A	5
25	pam_unix: authentication failure	0	2025-05-22 16:09:25	Host-10-10-10-150	0.0.0.0	N/A	5
26	pam_unix: authentication failure	0	2025-05-22 16:09:22	Host-10-10-10-150	0.0.0.0	N/A	5

- Alarm Dashboard showing SQL Injection Attempts and Brute Force attempts



AlienVault OSSIM [alienvault - 10.
Credential Access, Tactic TA0006
SQL Injections.pdf
Not secure
https://10.10.10.2/ossim/#analysis/alarms/alarms
DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
CONFIGURATION
Environmental Awareness
ACTIONS

SHOW 20 ENTRIES

☐	DATE	STATUS	INTENT & STRATEGY	METHOD	RISK	OTX	SOURCE	DESTINATION
☐	2025-05-22 16:07:16	open	WebServer Attack - SQL Injection	Attack Pattern Detection	LOW (1)	N/A	Host-10-10-10-150	0.0.0.0
☐	2025-05-22 16:06:30	open	Bruteforce Authentication	Linux/Unix	LOW (1)	N/A	Host-10-10-10-150	0.0.0.0
☐	2025-05-22 16:04:18	open	Bruteforce Authentication	SSH	LOW (1)	N/A	Host-10-10-10-150:60503	0.0.0.0:ssh
☐	2025-05-22 16:03:40	open	WebServer Attack	XSS	LOW (1)	N/A	Host-10-10-10-150	0.0.0.0
☐	2025-05-22 16:03:36	open	Bruteforce Authentication	SSH	LOW (1)	N/A	Host-10-10-10-150:55815	0.0.0.0
☐	2025-05-14 18:33:36	open	WebServer Attack - SQL Injection	Attack Pattern Detection	LOW (1)	N/A	Host-10-10-10-150	0.0.0.0
☐	2025-05-14 18:29:54	open	Bruteforce Authentication	Linux/Unix	LOW (1)	N/A	Host-10-10-10-150	0.0.0.0
☐	2025-05-14 18:27:21	open	WebServer Attack - SQL Injection	Attack Pattern Detection	LOW (1)	N/A	Host-10-10-10-150	0.0.0.0
☐	2025-05-14 18:27:01	open	WebServer Attack	XSS	LOW (1)	N/A	Host-10-10-10-150	0.0.0.0
☐	2025-05-14 18:27:30	open	Bruteforce Authentication	SSH	LOW (1)	N/A	Host-10-10-10-150:55497	0.0.0.0:ssh
☐	2025-05-14 18:26:51	open	Bruteforce Authentication	SSH	LOW (1)	N/A	Host-10-10-10-150:54107	0.0.0.0
☐	2025-04-10 15:49:16	open	Desktop Software - P2P	eDonkey	LOW (1)	N/A	Host-10-10-10-180:60523	224.0.0.252:hostmon

3. Map these findings to MITRE ATTCCK (e.g., T1110: Brute Force).

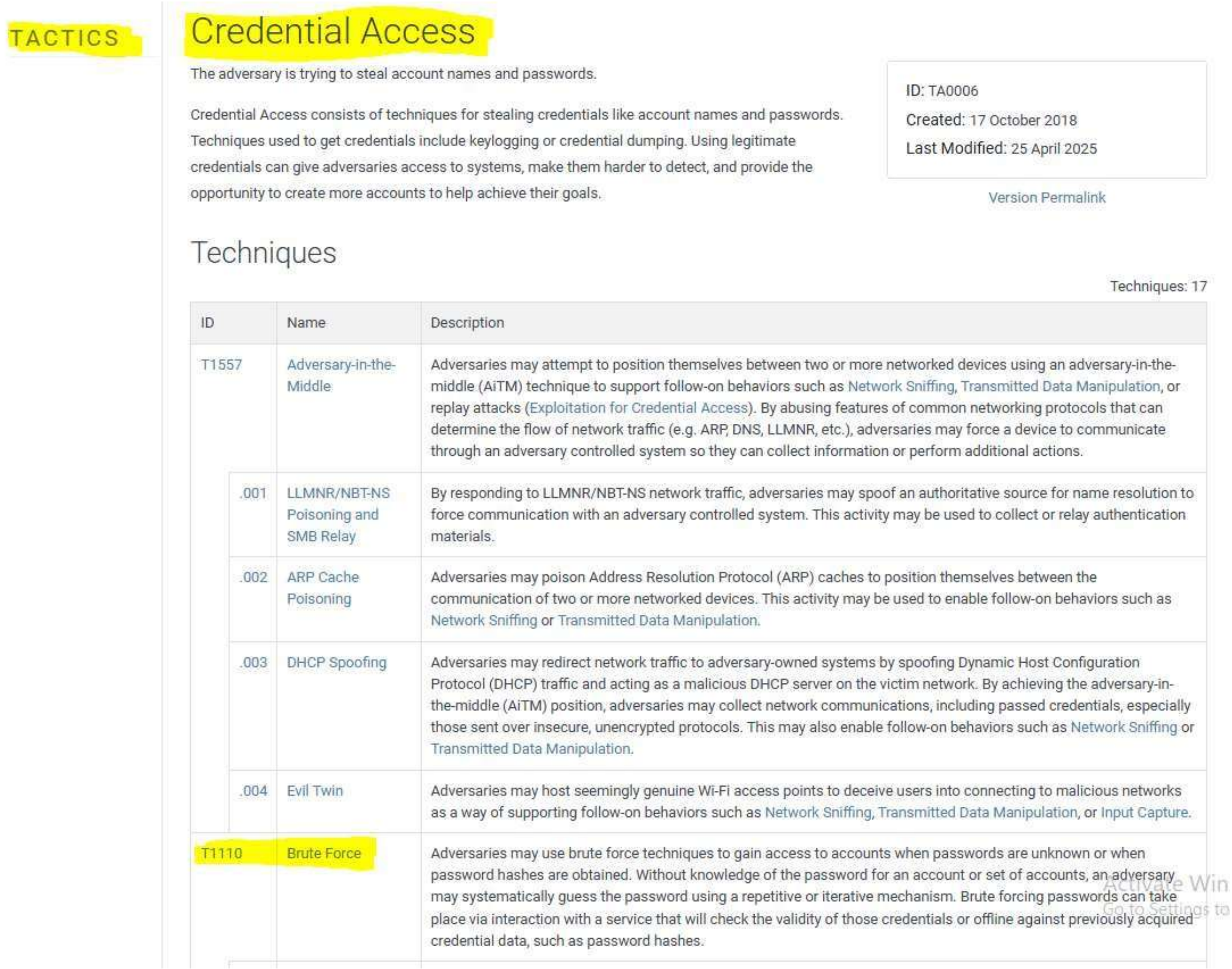
🟦 These patterns will be used for vulnerability prioritization and incident planning in Week 3 and 4.

Deliverables:

- Summary of suspicious behaviors found
- MITRE mapping for at least 2 tactics

Summary:
Suspicious behavior found came from a singular IP, 10.10.10.150. This host tried multiple attacks on May 22 2025 including SQL Injection, Cross Site Scripting and multiple Brute force attacks. Below are screen shots from Alienvault logs showing the attacks

MITRE Mapping for Brute Force – Credential Access



TACTICS

Credential Access

The adversary is trying to steal account names and passwords.

Credential Access consists of techniques for stealing credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping. Using legitimate credentials can give adversaries access to systems, make them harder to detect, and provide the opportunity to create more accounts to help achieve their goals.

ID: TA0006
Created: 17 October 2018
Last Modified: 25 April 2025

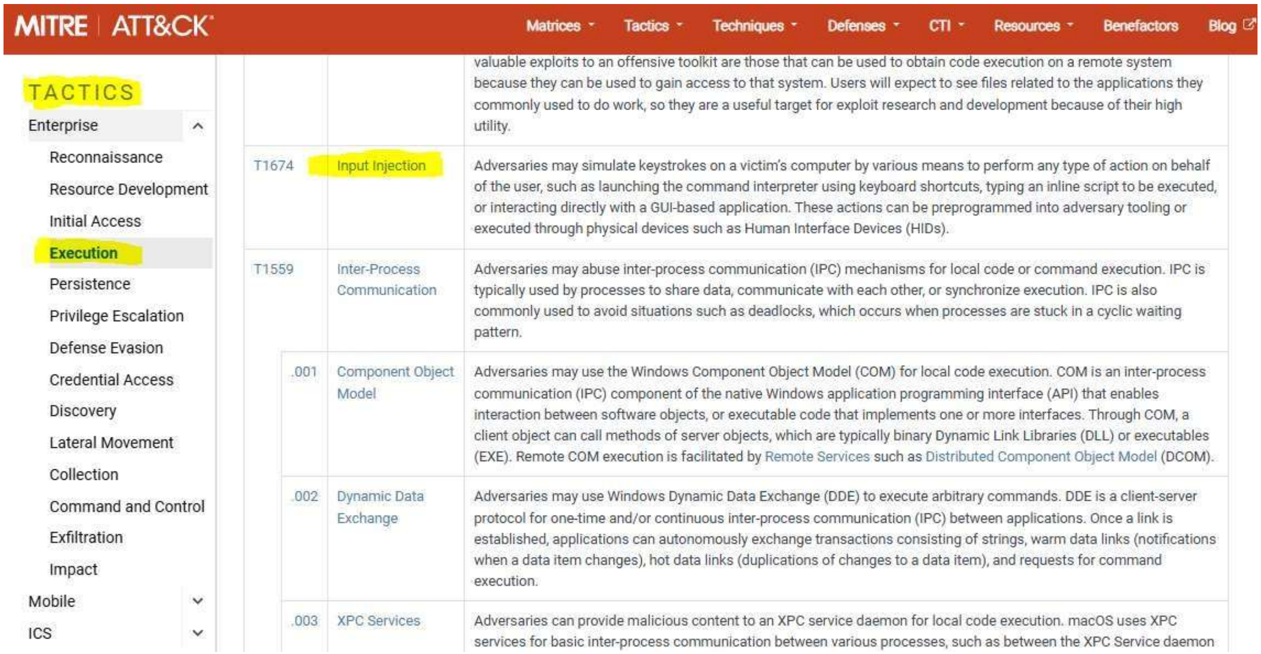
Version Permalink

Techniques

Techniques: 17

ID		Name	Description
T1557		Adversary-in-the-Middle	Adversaries may attempt to position themselves between two or more networked devices using an adversary-in-the-middle (AiTM) technique to support follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or replay attacks (Exploitation for Credential Access). By abusing features of common networking protocols that can determine the flow of network traffic (e.g. ARP, DNS, LLMNR, etc.), adversaries may force a device to communicate through an adversary controlled system so they can collect information or perform additional actions.
	.001	LLMNR/NBT-NS Poisoning and SMB Relay	By responding to LLMNR/NBT-NS network traffic, adversaries may spoof an authoritative source for name resolution to force communication with an adversary controlled system. This activity may be used to collect or relay authentication materials.
	.002	ARP Cache Poisoning	Adversaries may poison Address Resolution Protocol (ARP) caches to position themselves between the communication of two or more networked devices. This activity may be used to enable follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation.
	.003	DHCP Spoofing	Adversaries may redirect network traffic to adversary-owned systems by spoofing Dynamic Host Configuration Protocol (DHCP) traffic and acting as a malicious DHCP server on the victim network. By achieving the adversary-in-the-middle (AiTM) position, adversaries may collect network communications, including passed credentials, especially those sent over insecure, unencrypted protocols. This may also enable follow-on behaviors such as Network Sniffing or Transmitted Data Manipulation.
	.004	Evil Twin	Adversaries may host seemingly genuine Wi-Fi access points to deceive users into connecting to malicious networks as a way of supporting follow-on behaviors such as Network Sniffing, Transmitted Data Manipulation, or Input Capture.
T1110		Brute Force	Adversaries may use brute force techniques to gain access to accounts when passwords are unknown or when password hashes are obtained. Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism. Brute forcing passwords can take place via interaction with a service that will check the validity of those credentials or offline against previously acquired credential data, such as password hashes.

MITRE Mapping for SQL Injection – Execution



			valuable exploits to an offensive toolkit are those that can be used to obtain code execution on a remote system because they can be used to gain access to that system. Users will expect to see files related to the applications they commonly used to do work, so they are a useful target for exploit research and development because of their high utility.
T1674		Input Injection	Adversaries may simulate keystrokes on a victim's computer by various means to perform any type of action on behalf of the user, such as launching the command interpreter using keyboard shortcuts, typing an inline script to be executed, or interacting directly with a GUI-based application. These actions can be preprogrammed into adversary tooling or executed through physical devices such as Human Interface Devices (HIDs).
T1559		Inter-Process Communication	Adversaries may abuse inter-process communication (IPC) mechanisms for local code or command execution. IPC is typically used by processes to share data, communicate with each other, or synchronize execution. IPC is also commonly used to avoid situations such as deadlocks, which occurs when processes are stuck in a cyclic waiting pattern.
	.001	Component Object Model	Adversaries may use the Windows Component Object Model (COM) for local code execution. COM is an inter-process communication (IPC) component of the native Windows application programming interface (API) that enables interaction between software objects, or executable code that implements one or more interfaces. Through COM, a client object can call methods of server objects, which are typically binary Dynamic Link Libraries (DLL) or executables (EXE). Remote COM execution is facilitated by Remote Services such as Distributed Component Object Model (DCOM).
	.002	Dynamic Data Exchange	Adversaries may use Windows Dynamic Data Exchange (DDE) to execute arbitrary commands. DDE is a client-server protocol for one-time and/or continuous inter-process communication (IPC) between applications. Once a link is established, applications can autonomously exchange transactions consisting of strings, warm data links (notifications when a data item changes), hot data links (duplications of changes to a data item), and requests for command execution.
	.003	XPC Services	Adversaries can provide malicious content to an XPC service daemon for local code execution. macOS uses XPC services for basic inter-process communication between various processes, such as between the XPC Service daemon

Reflection Questions

1. What threat intel platform was most useful?

https://abuseipdb.com was very useful in identifying what Ips have been reported for suspicious activity and what that activity was,

2. How did logs confirm or contradict the intel?

The logs contradicted the intel because the Ip's searched were not present on in the logs. And the Ip's present on the logs were not present on the intel platforms as a reported suspicious IP.

3. What would help make the analysis easier?

Having a better understanding of how to navigate Alien vault to ensure were looking at the right data/logs that need to be analyzed

4. Why is TTP mapping better than signature-based detection?

TTP mapping is superior to signature-based detection because it focuses on behavioral analysis rather than static identifiers. Signature-based methods rely on known malware signatures, making them ineffective against zero-day attacks or adversaries using evasion techniques. TTP mapping analyzes an attacker's tactics, techniques, and procedures, allowing security teams to detect threats based on actions rather than predefined patterns. This approach improves threat hunting, incident response, and long-term defense strategies by identifying adversary behaviors instead of specific malware signatures.

Instructor Initials: ___________________________

ITS60 – Cybersecurity Operations
Capstone Project – Week 3 Lab
Project Title: Vulnerability Analysis and Risk Prioritization
Date: ____________
Student Name: _________________________________

🔹 Objective:

Conduct vulnerability scans and align discovered risks with observations from Week 2 to prioritize remediation steps.

🔹 Terminology

- **Vulnerability Scan** – Scan for system/software weaknesses.
- **CVSS** – Common Vulnerability Scoring System.
- **Risk Matrix** – Visual representation of impact and likelihood.
- **Remediation** – Actions taken to fix or reduce vulnerabilities.

🔹 Part 1: Perform a Vulnerability Scan with OSSIM or OpenVAS

Instructions:

1. Deploy AlienVault OSSIM
2. Run a scan on the same IPs discovered in Week 1.
3. Export findings with CVEs and severity.

These findings will align with logs from Week 2 to determine whether vulnerabilities were exploited.

Deliverables:

- Screenshot of scan dashboard
- Top 3 vulnerabilities (CVE, name, CVSS score)

🔹 Part 2: Risk Analysis and Mitigation Strategy

Instructions:

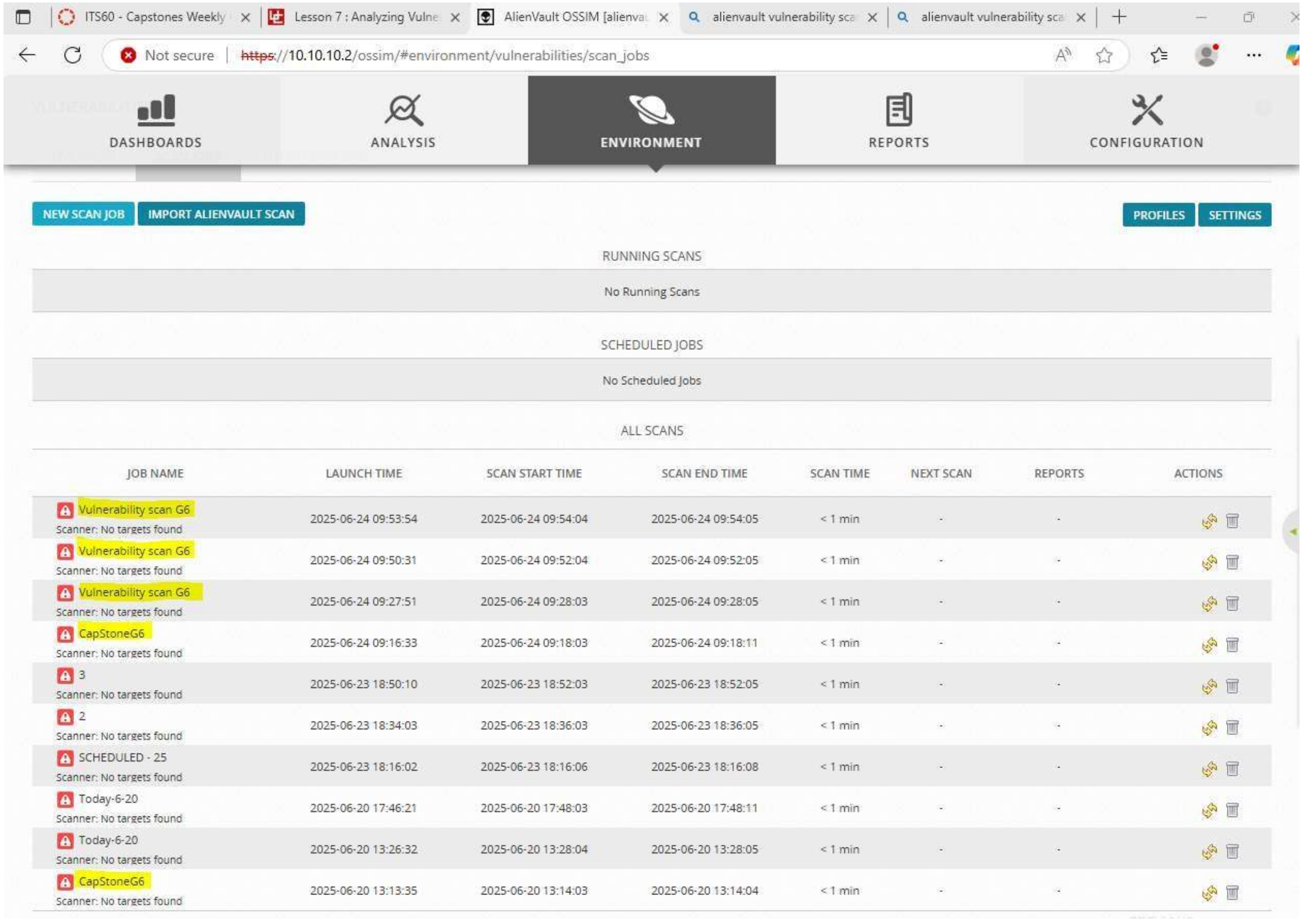
1. For each CVE, rate risk (High/Med/Low) using CVSS + exposure.
2. Map to previous logs or IOCs (e.g., is this CVE being attacked?).
3. Write one remediation suggestion per issue.

These prioritized risks prepare the response strategy for Week 4.

Deliverables:

- Risk matrix table
- Remediation summary per CVE

Alienvault Vulnertability scan did not work due to a server error. Capstone group 6 tried multiple scans on separate days and they all say “Scanner: No targets found” even though the Agent is installed and running on the machine running the scan.


ITS60 - Capstones Weekly
Lesson 7 : Analyzing Vulne
AlienVault OSSIM [alienva
alienvault vulnerability sca
alienvault vulnerability sca
Not secure
https://10.10.10.2/ossim/#environment/vulnerabilities/scan_jobs
DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
CONFIGURATION
NEW SCAN JOB
IMPORT ALIENVAULT SCAN
PROFILES
SETTINGS

RUNNING SCANS

No Running Scans

SCHEDULED JOBS

No Scheduled Jobs

ALL SCANS

JOB NAME	LAUNCH TIME	SCAN START TIME	SCAN END TIME	SCAN TIME	NEXT SCAN	REPORTS	ACTIONS
Vulnerability scan G6 Scanner: No targets found	2025-06-24 09:53:54	2025-06-24 09:54:04	2025-06-24 09:54:05	< 1 min	-	-	
Vulnerability scan G6 Scanner: No targets found	2025-06-24 09:50:31	2025-06-24 09:52:04	2025-06-24 09:52:05	< 1 min	-	-	
Vulnerability scan G6 Scanner: No targets found	2025-06-24 09:27:51	2025-06-24 09:28:03	2025-06-24 09:28:05	< 1 min	-	-	
CapStoneG6 Scanner: No targets found	2025-06-24 09:16:33	2025-06-24 09:18:03	2025-06-24 09:18:11	< 1 min	-	-	
3 Scanner: No targets found	2025-06-23 18:50:10	2025-06-23 18:52:03	2025-06-23 18:52:05	< 1 min	-	-	
2 Scanner: No targets found	2025-06-23 18:34:03	2025-06-23 18:36:03	2025-06-23 18:36:05	< 1 min	-	-	
SCHEDULED - 25 Scanner: No targets found	2025-06-23 18:16:02	2025-06-23 18:16:06	2025-06-23 18:16:08	< 1 min	-	-	
Today-6-20 Scanner: No targets found	2025-06-20 17:46:21	2025-06-20 17:48:03	2025-06-20 17:48:11	< 1 min	-	-	
Today-6-20 Scanner: No targets found	2025-06-20 13:26:32	2025-06-20 13:28:04	2025-06-20 13:28:05	< 1 min	-	-	
CapStoneG6 Scanner: No targets found	2025-06-20 13:13:35	2025-06-20 13:14:03	2025-06-20 13:14:04	< 1 min	-	-	

Reflection Questions

1. Which vulnerabilities were likely exploited?

Unsure as the scans weren’t working

2. How did logs from Week 2 help validate this?

Unsure as the scans weren’t working

3. What makes a vulnerability more urgent to fix?

Exploit Availability, CVSS Score, Asset values, and attack surface all make up how likely a vulnerability is to be exploited.

4. How does OSSIM support real-time monitoring?

OSSIM (Open Source Security Information Management) supports real-time monitoring by combining several powerful tools and techniques into a unified SIEM platform

Instructor Initials: ___________________________

ITS60 – Cybersecurity Operations
Capstone Project – Week 4 Lab
Project Title: Incident Response and SOC Reporting
Date: ____________
Student Name: _________________________________

◆ Objective:

Use data from the past three weeks to simulate incident response and generate a professional SOC report.

◆ Terminology

- **Incident Response** – Managing and containing security breaches.
- **Containment** – Preventing further damage.
- **Eradication** – Removing threats.
- **Recovery** – Restoring systems.
- **SOC Report** – Documentation summarizing the incident.

◆ Part 1: Build an Incident Response Plan

Instructions:

1. Choose one event from Week 2 or CVE from Week 3.
2. Use IR phases:
   - Identification
   - Containment
   - Eradication
   - Recovery

■ Connect each step to earlier evidence and logs.

Deliverables:

- Completed Incident Response table or template
- Reference to source logs/CVE/intel used

◆ Part 2: Final SOC Report

Instructions:

1. Summarize:
   - Key findings across all weeks
   - Assets affected

    - Timeline of activity
    - Recommendations
2. Attach evidence (screenshots, CVEs, log entries).

Deliverables:

- Final SOC report (PDF/Docx)
- Evidence appendix

Reflection Questions

1. How did earlier work make the IR process easier?

2. Which step was the most difficult?

3. What’s one thing you’d do differently in the future?

4. How does reporting build credibility in a SOC role?

Instructor Initials: ___________________________

See week 4 below!

Incident Response Plan: SSH Brute Force Attack (AlienVault OSSIM)
Selected CVE: CVE-2016-6210 — Timing attack vulnerability in OpenSSH Source
Intel: OSSIM Alarm Dashboard, asset logs

IR Phase	Response Action
Identification	OSSIM alarms flagged 5 brute force attempts. Four listed method as "SSH" and one a "Linux/Unix." All originated from a suspected mobile device tied to a DHCP IP 10.10.10.150 and same MAC address 92:BE:27:39:79:E3 over multiple days. AlienVault triggered based on failed login attempts consistent with brute force patterns
Containment	Use OSSIM and network access controls to isolate the affected IP and block further outbound traffic from the MAC address. Correlate DHCP logs to determine responsible user. Alerted internal IT/security staff for physical containment
Eradication	Remove device from the network. Performe malware scans and forensics to verify if attacker tools or scripts were installed. If rooted or irreparably compromised, reimage the device. Verify no persistent backdoors or unauthorized SSH keys are present on target systems.
Recovery	Reinforce SSH security by enforcing account lockout policies, MFA where possible, and update OpenSSH to mitigate CVE-2016-6210. Re-add the IP to the DHCP pool after confirming secure configuration. Continue monitoring via OSSIM to ensure no further brute force attempts from same or new sources.

Final SOC Report

Over the 4 weeks completing the CySA+ Capstone, Group 6 was able to conduct multiple steps including End-to-End SOC Engagement Simulation, Threat Intelligence & Malicious Activity Detection, Vulnerability Analysis and Risk Prioritization, and now Incident Response and SOC Reporting.

During week 1, the group conducted network discovery and asset mapping utilizing widows tools such as arp -a in order to identify IP's and mac addresses of connected devices within the network. We also were able to intstall OSSEC HIDS Agent on multiple hosts in order to conduct log aggregation and vulnerability scans via Alienvault OSSIM,

During week 2, after mapping the network and installing the agent, we serached up IP's within the network on Open Source Threat feeds to identify if any IP's have been reported for any reason. 2 IP's came back flagged. The first ip was reported for Port Scans in Belarus, the other was reported for Brute Force Attempts via SSH in France. The group then utilzed Alienvault OSSIM to search for any mailicious activity. The activity found was multiple attempts at conducting SQL Injections, cross site scripting and brute force attacks. These were then mapped via MITRE to Execution and Credential Access Tactics.

During week 3, our group ran into a few issues when trying to complete Vulnerability Analysis and Risk Prioritization. The issue lies in Alienvault OSSIM not being able to connect to any devices with OSSEC HIDS agent installed, thus preventing us from conducting Vulnerability scans. We were,

however, able to link the Brute Force attempts, to CVE-2016-6210 — Timing attack vulnerability in OpenSSH.

This CVE describes a vulnerability in OpenSSH (prior to version 7.3) where the server responds faster to invalid usernames than to valid ones when large passwords are submitted. This creates a timing side- channel that allows attackers to enumerate valid users — a critical first step in launching targeted brute force attacks. OSSIM flagged multiple brute force attempts using the “SSH” and “Linux/Unix” method tags. These likely indicate repeated login attempts over SSH targeting Unix-based systems. If the attacker was using a tool that exploits CVE-2016-6210, they could have first enumerated valid usernames using timing differences, then launched credential guessing attacks against those accounts. The fact that the same MAC address was involved across multiple days suggests persistence.

In the above Incident Response Plan you will find a table with the recommendations for, Identification, Containment, Eradication, and Recovery.

Reflection Questions

1.How did earlier work make the IR process easier?

- Being able to map out the netowrk, look up IP’s on threat feeds and threat hunt on the OSSIM helped making the process more streamlined.

2.Which step was the most difficult?

- Week 3 conducting the vulnerability scans. Since there are issues with the Alienvault server configurations preventing it from connecting to the HIDS agents installed on end user devices, scans were not able to be completed, and prevented us from conducting risk priortization.

3.What’s one thing you’d do differently in the future?

- Work with someone who has more experience in order to learn more efficient ways to complete the tasks that we did.

4.How does reporting build credibility in a SOC role?

- Proper report helps build credibilty because it outlines all of the steps you took to complete the tasks at hand and the ammount of information provided in the detailed reporting adds credibility to your ability to do SOC analysis.