Official incident report

Event ID:118

Rule Name: SOC168 - Whoami Command Detected in Request Body

Made By

LinkedIn: Engineer.Ahmed Mansour

Link: https://www.linkedin.com/in/ahmed-mansour-5631b5323/

Github link: https://github.com/AhmedMansour93

Table of contents

Event Details

Event ID:
118

Event Date and Time:
Feb, 28, 2022, 04:12 AM

Rule:
SOC168 - Whoami Command Detected in Request Body

Level:
Security Analyst

Hostname:
WebServer1004

HTTP Request Method:
POST

Requested URL:
https://172.16.17.16/video/

User-Agent:
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)

Alert Trigger Reason:
Request Body Contains whoami string

Device Action:
Allowed

Network Information Details

Destination Address:
172.16.17.16 internal

Source Address:
61.177.172.87 external

External / Internal Attack:

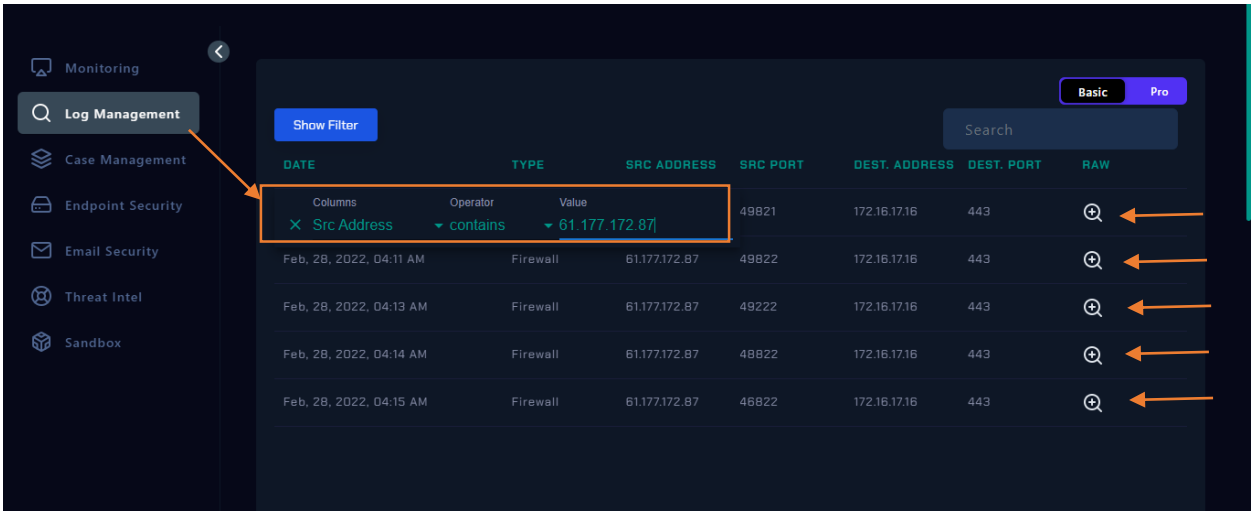
Based on the event details, the attack appears to be **external**.

Analysis:

Log Management

We'll proceed by entering the source IP address and reviewing the results.

Please refer to the attached image for further details regarding the attack.



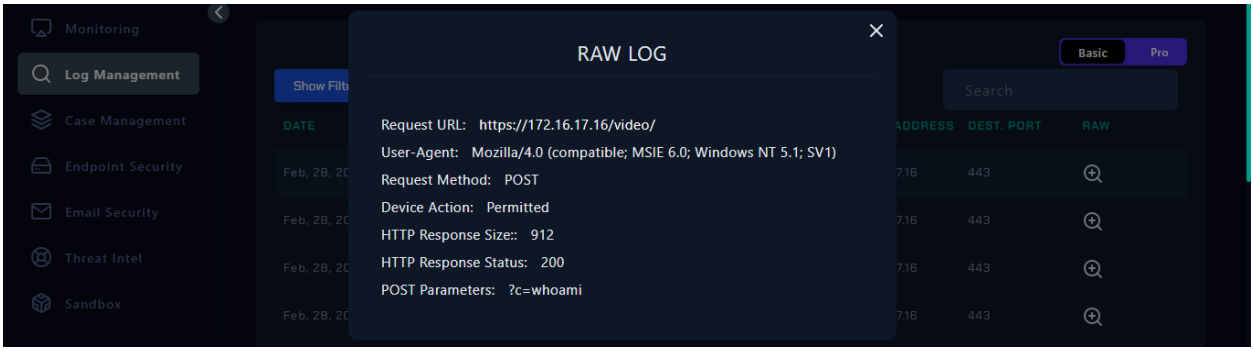
5 Logs records for the source IP.

Please refer to the attached image for further details regarding the attack.

We will explain all of them step by step

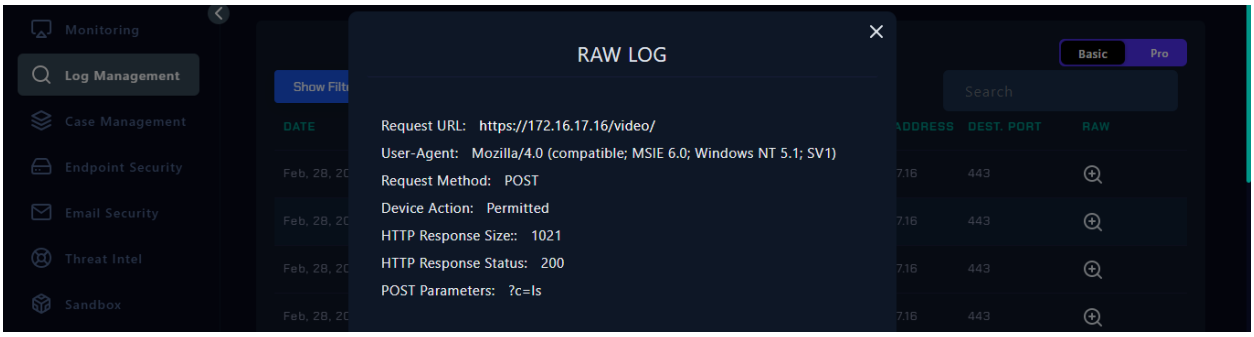
Log Analysis

- **Log1:**



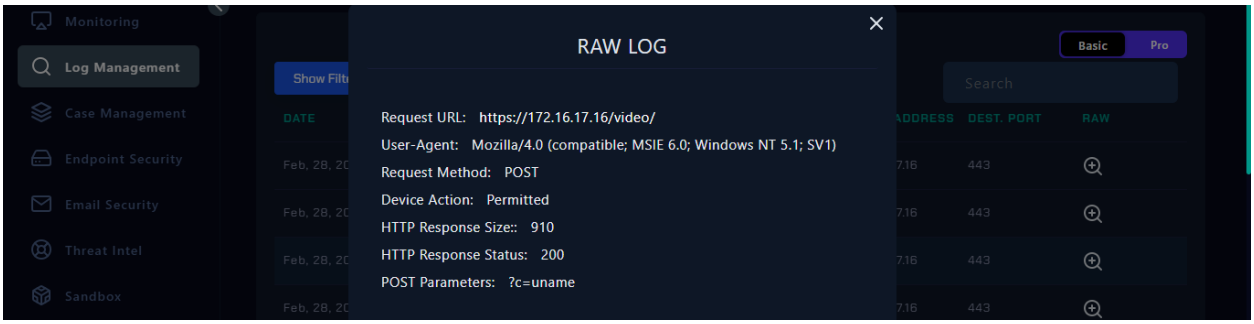
Explanation: A POST request was made to the URL `https://172.16.17.16/video/`. The request included the parameter `?c=whoami`, which is a command used to display the current user. The server responded with a status of 200 and a response size of 912 bytes.

- **Log2:**



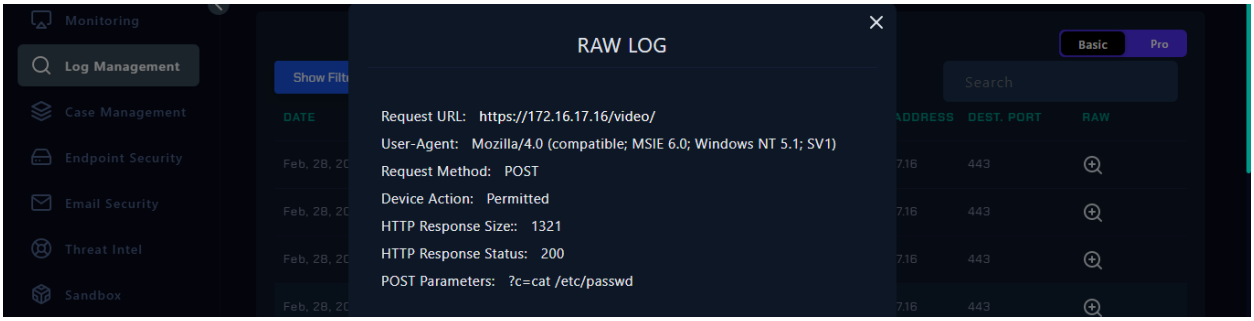
Explanation: Another POST request was made to the same URL with the parameter `?c=ls`, a command that lists directory contents. The response was successful (status 200) with a size of 1021 bytes..

- **Log3:**



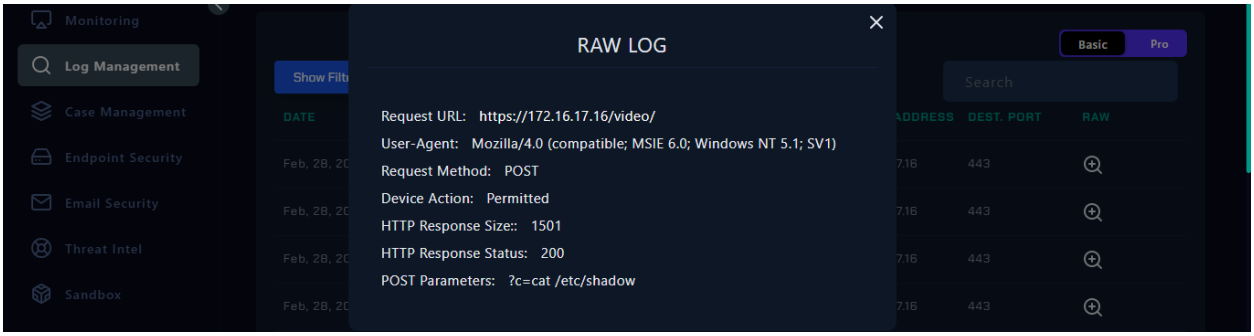
Explanation: A third POST request included the parameter `?c=uname`, which is used to display system information. The server responded with a status 200 and a size of 910 bytes.

- **Log4:**



Explanation: This request utilized the parameter `?c=cat /etc/passwd`, a command that attempts to read the `/etc/passwd` file, which contains user account information. The server responded with a status of 200 and a response size of 1321 bytes, indicating the command was executed successfully.

- **Log5:**



Explanation: The final request included the parameter `?c=cat /etc/shadow`, which attempts to read the `/etc/shadow` file that contains encrypted password data. The server responded with a status of 200 and a size of 1501 bytes, confirming the execution of this command.

Summary of Logs

The logs reveal a series of POST requests made to the URL `https://172.16.17.16/video/` that indicate a Command Injection Attack:

1. **Log 1**: A POST request with the parameter `?c=whoami` was used to identify the current user. The server responded with a status of 200 and a response size of 912 bytes, suggesting that the command was executed.
2. **Log 2**: A POST request with the parameter `?c=ls` was made to list directory contents. The response was successful (status 200) with a size of 1021 bytes, confirming command execution.
3. **Log 3**: Another POST request with the parameter `?c=uname` aimed to retrieve system information. The server response was 200 with a size of 910 bytes, indicating successful command execution.
4. **Log 4**: The parameter `?c=cat /etc/passwd` was used to read the `/etc/passwd` file, which contains user account information. The response size of 1321 bytes with a status of 200 confirms successful execution of the command.
5. **Log 5**: A POST request with the parameter `?c=cat /etc/shadow` attempted to access the `/etc/shadow` file, which holds encrypted password data. The response size of 1501 bytes and status of 200 demonstrate that the command was successfully executed.

Overall, the logs indicate a series of successful command injection attempts aimed at accessing sensitive files on the server.

2. Is Traffic Malicious?

Based on our comprehensive analysis, the traffic identified was **indeed malicious.**

3. What Is The Attack Type?

Our analysis determines that the attack type is a **Command Injection Attack**.

4. Is the malicious traffic caused by a planned test?

After reviewing the email security section, it has been confirmed that this malicious traffic **was not the result of a planned test.**

5. Was the Attack Successful?

Yes, the attack was successful. Evidence from the logs shows that commands designed to access sensitive system files (`/etc/passwd` and `/etc/shadow`) were executed successfully, as indicated by the HTTP status codes of 200 and the response sizes correlating with the expected output of these commands.

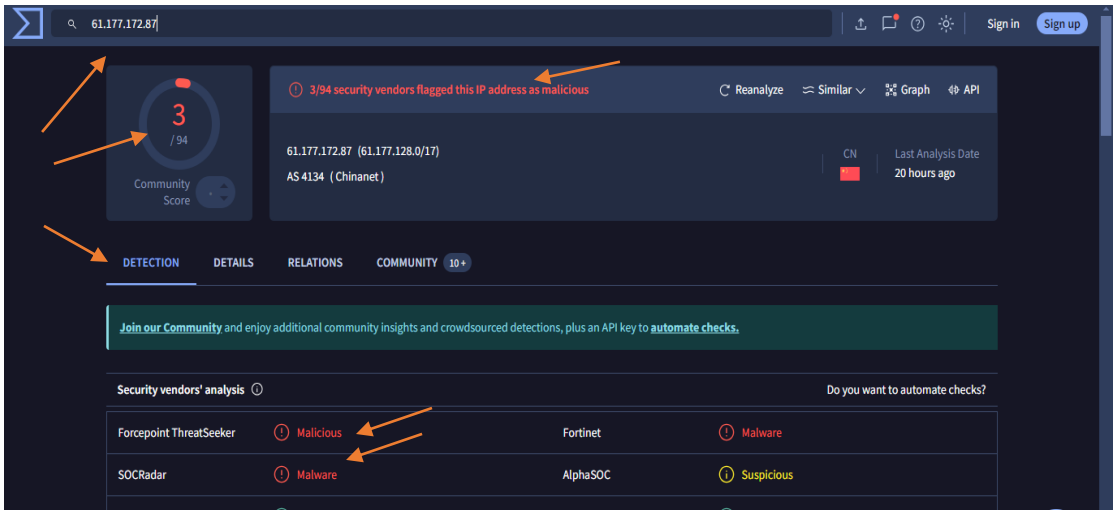
Detection:

Threat Intelligence Results

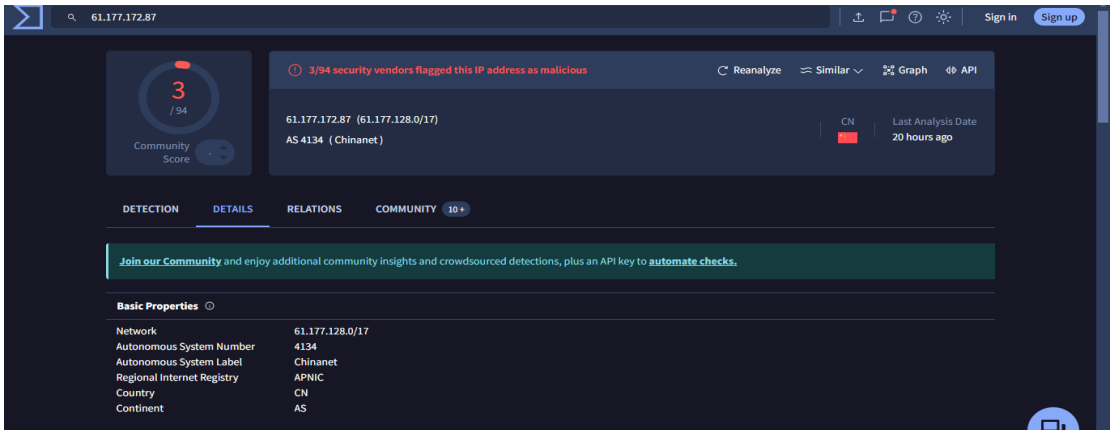
Source IP Analysis on VirusTotal

Objective: Evaluate the source IP address using VirusTotal and review the findings in various sections.

1. **Detection Section**
    - **Status:** The Detection section shows us its **malicious IP.**

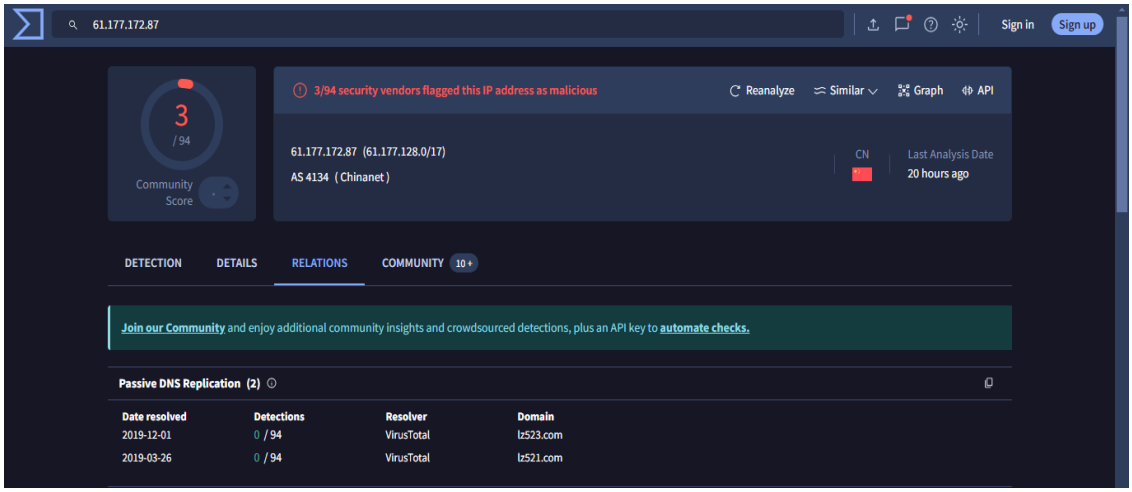


    - **Reference:** View Detection Section
2. **Details Section**
    - **Status:** The Details section is clear, with no additional issues or anomalies noted. This section provides standard information about the IP address.

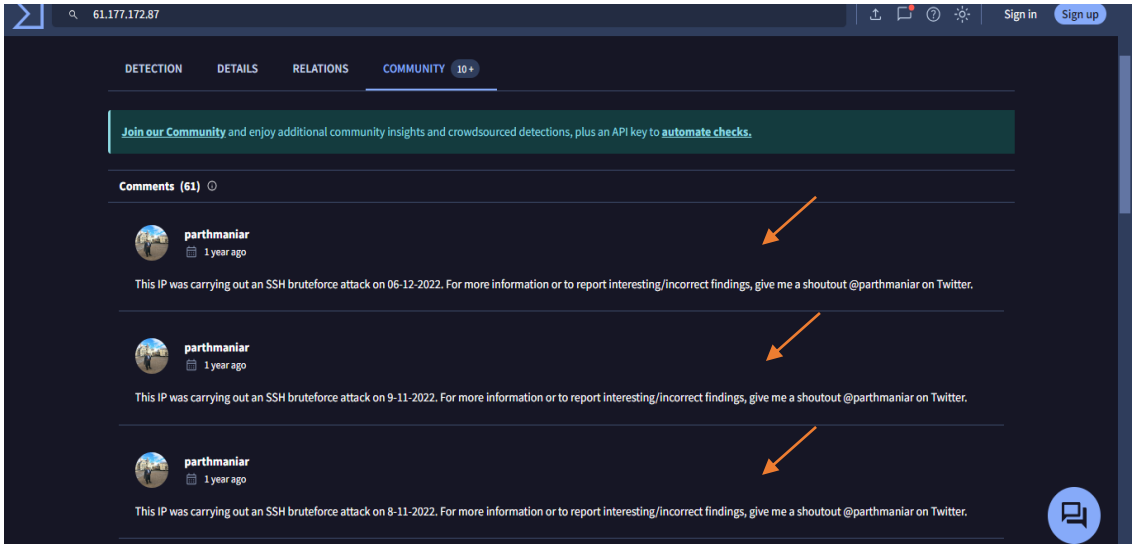


    - **Reference:** View Details Section

3. **Relation Section**
    - **Status:** The Relation section is clear.



    - **Reference:** View Relations Section
4. **Community Section**
    - **Status:** The Community section is not clear, there is more than 10 comments.



    - **Reference:** View Community Section

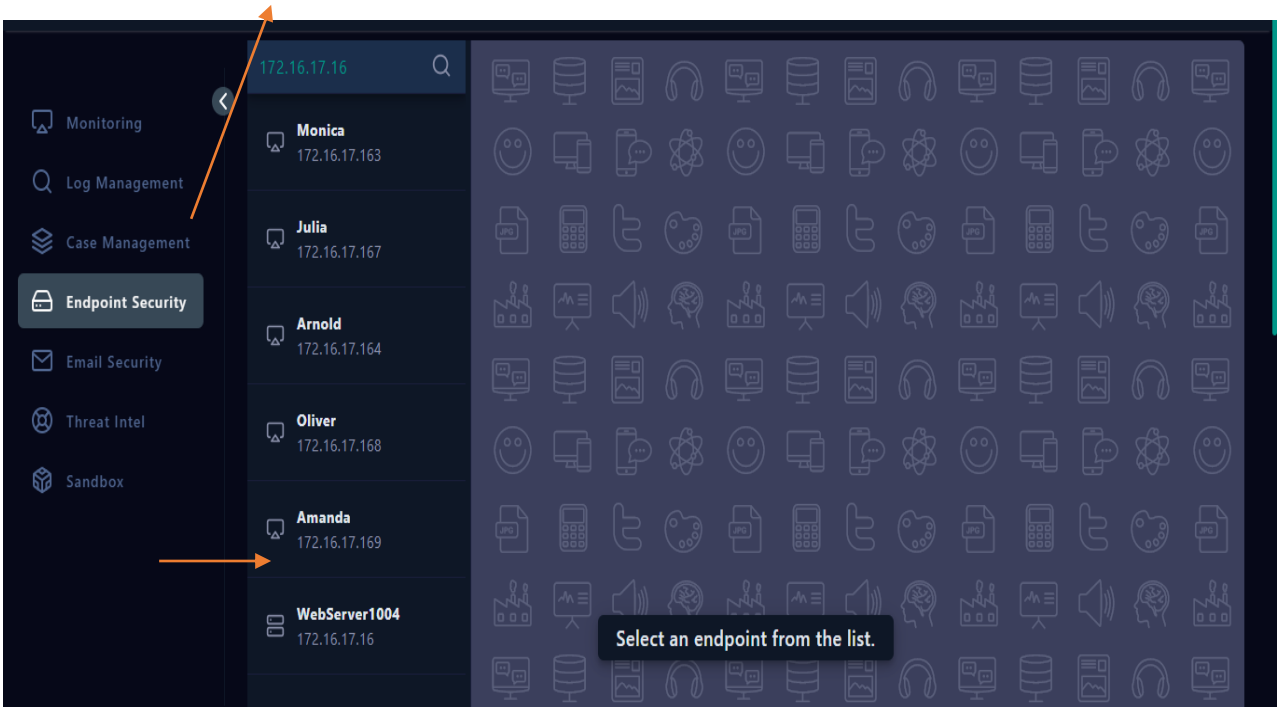
5. **Do You Need Tier 2 Escalation?**

    Yes, Tier 2 escalation is required due to the successful execution of the attack. This escalation is necessary to address the security breach and mitigate any further risks.

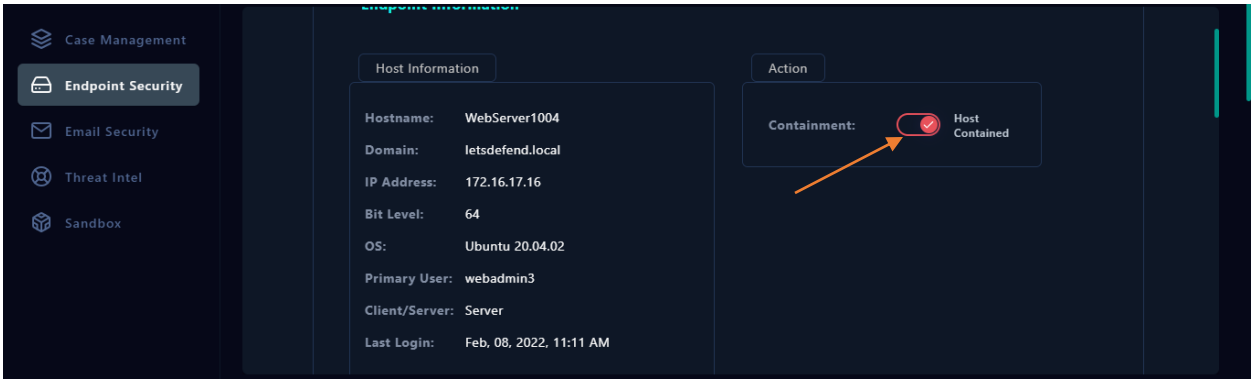
Endpoint Security

We will enter either the Destination IP to contain the server.

Refer to the attached image for further details.



We need to contain the server because the attack is successful.



The device contained successfully

Conclusion

On February 28, 2022, at 04:12 AM, our security monitoring systems flagged a significant event (Event ID 118) involving a Command Injection Attack on WebServer1004. The attack was initiated by an external IP address, 61.177.172.87, which exploited a vulnerability on the server via POST requests to `https://172.16.17.16/video/`.

Incident Summary:

The attack unfolded through a series of malicious POST requests containing command injection parameters. Each request executed commands with the following results:

1. **Log 1:** The `?c=whoami` command identified the user, with a response size of 912 bytes.
2. **Log 2:** The `?c=ls` command successfully listed directory contents, with a response size of 1021 bytes.
3. **Log 3:** The `?c=uname` command retrieved system information, with a response size of 910 bytes.
4. **Log 4:** The `?c=cat /etc/passwd` command accessed user account details, with a response size of 1321 bytes.
5. **Log 5:** The `?c=cat /etc/shadow` command retrieved encrypted password data, with a response size of 1501 bytes.

Each command was executed successfully, as indicated by the consistent HTTP status 200 and the corresponding output sizes. This confirms that the server was compromised and sensitive information was accessed.

Malicious Traffic Confirmation: Our thorough analysis confirmed that the traffic was indeed malicious. The attack was not part of a planned test, as verified by the email security review.

Attack Type and Impact: The attack was identified as a Command Injection Attack. The successful execution of commands targeting critical system files, such as `/etc/passwd` and `/etc/shadow`, demonstrates the severity of the breach.

Recommendations: Immediate Tier 2 escalation is essential to address and mitigate the impact of this security incident. The attack's success necessitates a comprehensive response to enhance security measures and prevent future occurrences.

Additional Actions: The affected server has been contained to prevent further exploitation. For a detailed review, please refer to the attached images and VirusTotal analysis, which confirm the malicious nature of the source IP address.

This incident highlights the need for urgent and enhanced security protocols to safeguard against sophisticated attacks.