



Official incident report

Event ID: 263

Rule Name: SOC287 - Arbitrary File Read on Checkpoint
Security Gateway [CVE-2024-24919]

Table of contents

Official incident report	1
Event ID: 263	1
Rule Name: SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919]	1
Table of contents	2
Event Details	3
Network Information Details	3
Detection	4
Threat intelligence	4
Analysis	11
Log management	11
End Point Security	17
Conclusion	20

Event Details

Event ID:

263

Event Date and Time:

Jun, 06, 2024, 03:12 PM

Rule:

SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919]

Level:

Security Analyst

Description:

Characteristics exploit pattern Detected on Request, indicative exploitation of the CVE-2024-24919.

Network Information Details

Destination Address:

172.16.20.146

Source Address:

203.160.68.12

Internal / External Attack:

External attack

Detection:

Threat Intelligence Results

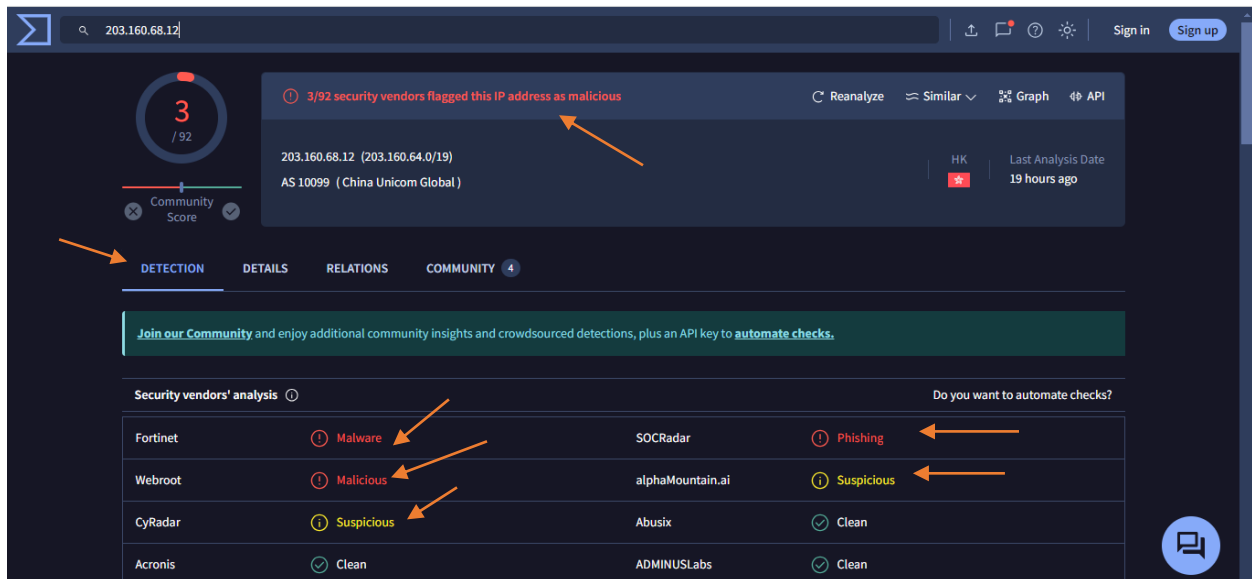
www.virustotal.com

Detection Section

According to the VirusTotal analysis, the IP address was flagged by 3 out of 93 security vendors as malicious. Below are the details:

- **Fortinet:** Malware
- **SOCradar:** Phishing
- **Webroot:** Malicious
- **alphaMountain.ai:** Suspicious
- **CyRadar:** Suspicious
- **Abusix:** Clean

For further reference, please see the attached photo.



203.160.68.12

3 / 92

Community Score

3/92 security vendors flagged this IP address as malicious

203.160.68.12 (203.160.64.0/19)
AS 10099 (China Unicom Global)

HK Last Analysis Date 19 hours ago

Reanalyze Similar Graph API

DETECTION DETAILS RELATIONS COMMUNITY 4

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Security vendors' analysis		Do you want to automate checks?	
Fortinet	Malware	SOCradar	Phishing
Webroot	Malicious	alphaMountain.ai	Suspicious
CyRadar	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

Details Section

Basic Properties:

- **Network:** 203.160.64.0/19
- **Autonomous System Number:** 10099
- **Autonomous System Label:** China Unicom Global
- **Regional Internet Registry:** APNIC
- **Country:** Hong Kong (HK)
- **Continent:** Asia (AS)

For detailed information, refer to the attached photo.

The screenshot shows a network security dashboard for the IP address 203.160.68.12. The interface is dark-themed with a top navigation bar containing a search bar, user profile (Ahmed Mansour), and various icons. A circular gauge on the left indicates a 'Community Score' of 3/93. A red banner at the top states '3/93 security vendors flagged this IP address as malicious'. Below this, the IP address is shown with its subnet (203.160.64.0/19) and the Autonomous System (AS 10099 - China Unicom Global). The 'DETAILS' tab is selected, showing a table of 'Basic Properties' with an orange arrow pointing to the 'Network' field. Below the properties table is a 'Whois Lookup' section showing the IP range and netname.

203.160.68.12

3/93 security vendors flagged this IP address as malicious

Reanalyze Similar Graph API

203.160.68.12 (203.160.64.0/19)

AS 10099 (China Unicom Global)

HK Last Analysis Date 14 hours ago

DETECTION DETAILS RELATIONS COMMUNITY 9

Basic Properties

Network	203.160.64.0/19
Autonomous System Number	10099
Autonomous System Label	China Unicom Global
Regional Internet Registry	APNIC
Country	HK
Continent	AS

Whois Lookup

inetnum: 203.160.64.0 - 203.160.95.255

netname: UNICOM-HK

descr: China Unicom (Hong Kong) Operations Limited

Community Section

There are two comments in the community section related to this IP address:

1. Comment by patricksvgrapi:

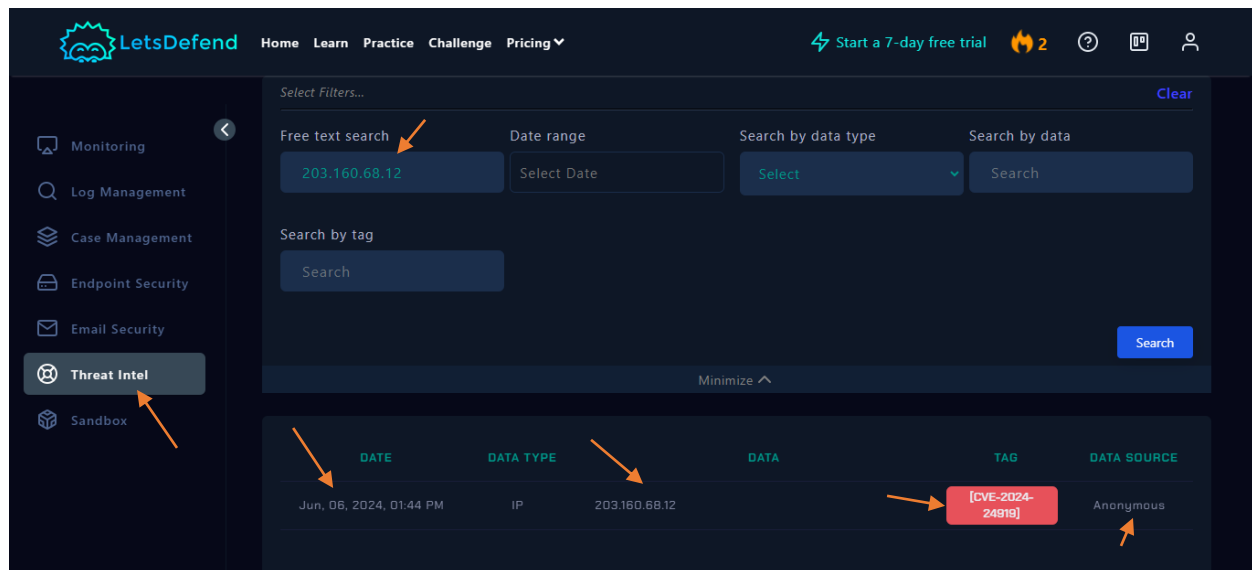
- *Description:* This indicator was mentioned in a report.
- *Title:* Advisory: Active exploitation of Check Point Remote Access VPN vulnerability (CVE-2024-24919)
- *Reference:* <https://www.mnemonic.io/resources/blog/advisory-check-point-remote-access-vpn-vulnerability-cve-2024-24919/>
- *Report Publish Date:* 2024-05-29
- *Reference ID:* [#4d0076650](#)

2. Comment by cdscybersoc:

- *Description:* Peaksys - Port Scan
- *Date:* 2024-05-30 16:04:00 UTC+01

Please refer to the attached photo for more details.





CVE-2024-24919: Overview

CVE-2024-24919 refers to a critical vulnerability affecting Check Point's Remote Access VPN products. This flaw allows for the possibility of unauthorized access due to inadequate validation of user credentials during the authentication process. Exploiting this vulnerability, an attacker could potentially gain unauthorized access to sensitive systems, bypass security controls, and escalate privileges. This vulnerability is particularly concerning because it targets a critical component of network security infrastructure, which is often used to protect sensitive corporate networks and data.

The exploitation of CVE-2024-24919 could lead to significant security breaches, data exfiltration, and the compromise of organizational assets. Organizations using affected Check Point VPN products are strongly advised to apply security patches and follow recommended security practices to mitigate the risk associated with this vulnerability. Additionally, monitoring network traffic for signs of exploitation and anomalous activity is crucial in preventing and detecting unauthorized access attempts.

www.abuseipdb.com

Result 1

IP Address: 203.160.68.12

- **Reports:** This IP address was reported twice in our database.
- **Confidence of Abuse:** 0%
- **ISP:** China Unicom (Hong Kong) Operations Limited
- **Usage Type:** Unknown
- **Domain Name:** chinaunicom.com.hk
- **Country:** Hong Kong
- **City:** Hong Kong, Hong Kong

For more detailed information, refer to the attached photo.

Check an IP Address, Domain Name, or Subnet
e.g. 156.197.32.19, microsoft.com, or 5.188.10.0/24

156.197.32.19

CHECK

203.160.68.12 was found in our database!

This IP was reported **2** times. Confidence of Abuse is **7%**.

7%

ISP China Unicom (Hong Kong) Operations Limited

Usage Type Unknown

Domain Name chinaunicom.com.hk

Country 🇭🇰 Hong Kong

City Hong Kong, Hong Kong

IP info including ISP, Usage Type, and Location provided by [IP2Location](#).
Updated monthly.

REPORT 203.160.68.12

WHOIS 203.160.68.12

Result 2


- Reporter: NSCA-ISEU
 - IoA Timestamp (UTC): 2024-06-01 07:31:52
 - Comment: Check Point VPN Information Disclosure (CVE-2024-24919)
 - VirusTotal: Malicious: 1, Suspicious: 0
 - AS Number: AS10099
 - ISP: China Unicom Global, China Unicom (Hong Kong) Operations Limited
 - Categories: Port Scan and Web App Attack
- Reporter: Cyber SOC
 - IoA Timestamp (UTC): 2024-05-30 15:04:32
 - Comment: Peaksys - 2024-05-30 16:04:00 UTC+01
 - Categories: Port Scan

For more detailed information, refer to the attached photo.

IP Abuse Reports for 203.160.68.12:

This IP address has been reported a total of 2 times from 2 distinct sources. 203.160.68.12 was first reported on May 30th 2024, and the most recent report was 2 months ago.

Old Reports: The most recent abuse report for this IP address is from 2 months ago. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp in UTC	Comment	Categories
 NSCA-ISEU	2024-06-01 07:31:52 (2 months ago)	Check Point VPN Information Disclosure (CVE-2024-24919). VT: Malicious: 1 - Suspicious: 0. AS10099 China Unicom Global China Unicom (Hong Kong) Operations Limited show less	<div>Port Scan</div> <div>Web App Attack</div>
 Cyber SOC	2024-05-30 15:04:32 (2 months ago)	Peaksys - 2024-05-30 16:04:00 UTC+01	<div>Port Scan</div>

Showing 1 to 2 of 2 reports

feedback

Combined Analysis from VirusTotal, AbuseIPDB, and LetsDefend

VirusTotal

The IP address 203.160.68.12 has been flagged as malicious by 3 out of 92 security vendors. The issues identified include malware and phishing activities, with some vendors marking it as suspicious. However, not all vendors agree, as some did not flag it as malicious.

AbuseIPDB

This IP address appears in the AbuseIPDB database with only 2 reports and a low abuse confidence level of 7%. This suggests that while there have been some reports, the history of abuse or malicious activity associated with this IP is not strong.

LetsDefend

On LetsDefend, the IP address 203.160.68.12 is linked to [CVE-2024-24919], a specific vulnerability related to Check Point VPN Information Disclosure. The reference to this vulnerability is marked as "Anonymous," meaning the context or specific details about the CVE's relation to the IP are not fully clear.

Summary

The IP address 203.160.68.12 presents mixed results. While VirusTotal shows some reports of malicious activity, including malware and phishing, the reports on AbuseIPDB are minimal and have low confidence. Additionally, its association with [CVE-2024-24919] on LetsDefend adds a layer of concern, although the details are not fully transparent.

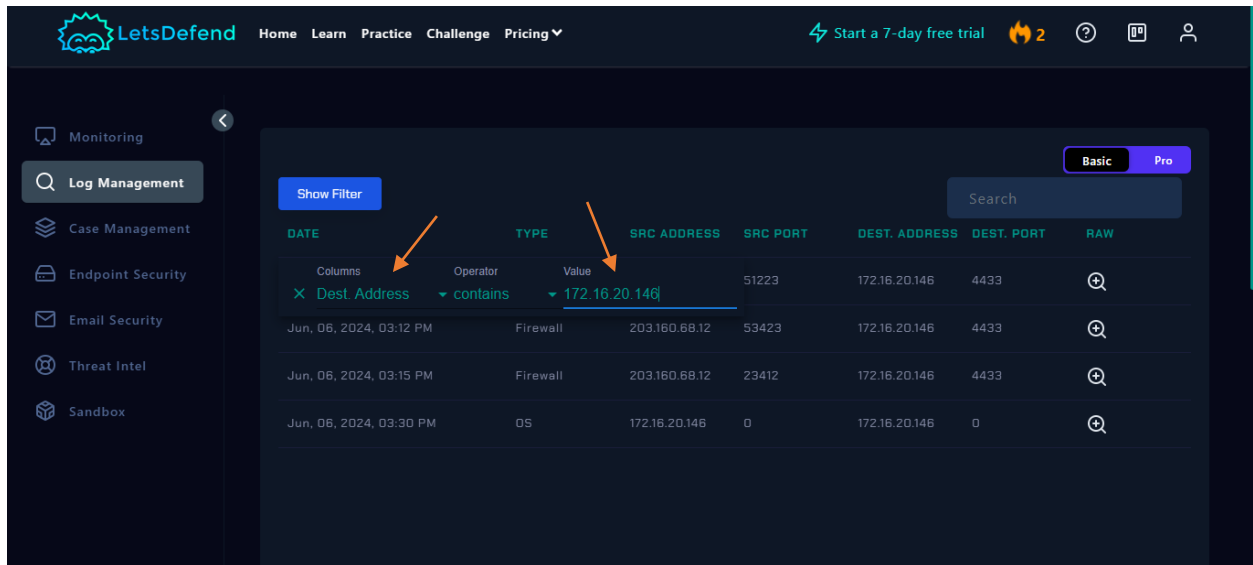
Overall, further investigation is necessary to determine the true nature of this IP address. Given its ties to known vulnerabilities and the mixed security assessments, caution and deeper analysis are advised.

Analysis:

Log Management

So, I jumped into the log management section, and to get the juicy details, I filtered the results. I did this by selecting the Destination address and then punching in the victim server's IP.

For more detailed information, refer to the attached photo

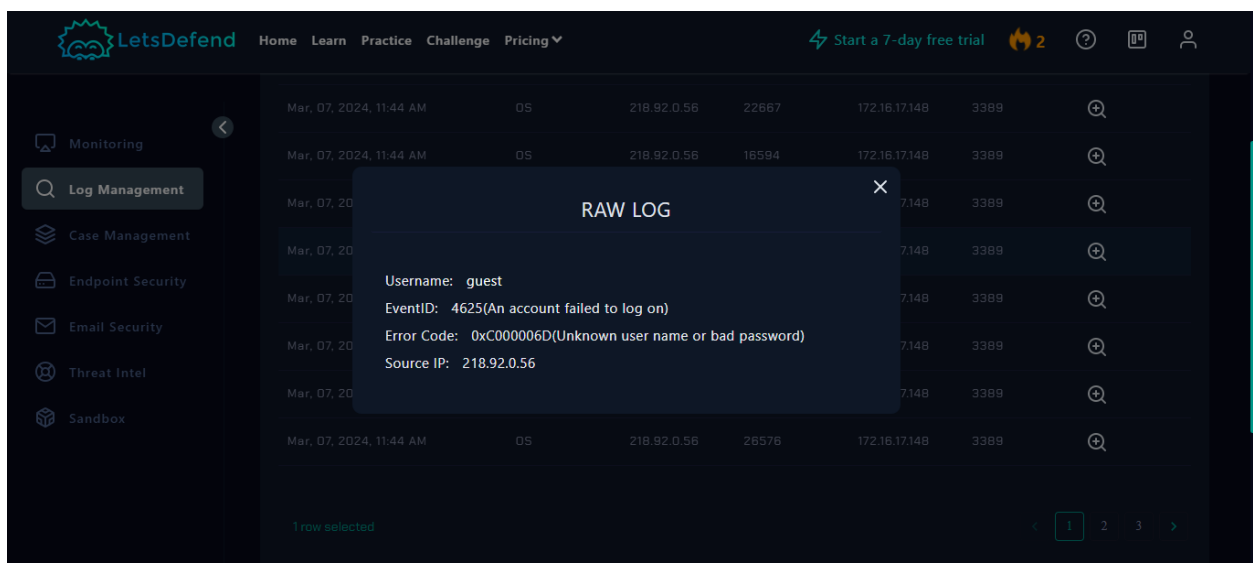


So, I checked out the logs, specifically the FIREWALL type, and found this gem:

- **Username:** guest
- **EventID:** 4625 (An account failed to log on)

Looks like someone might be trying a brute force attack to crack the login!

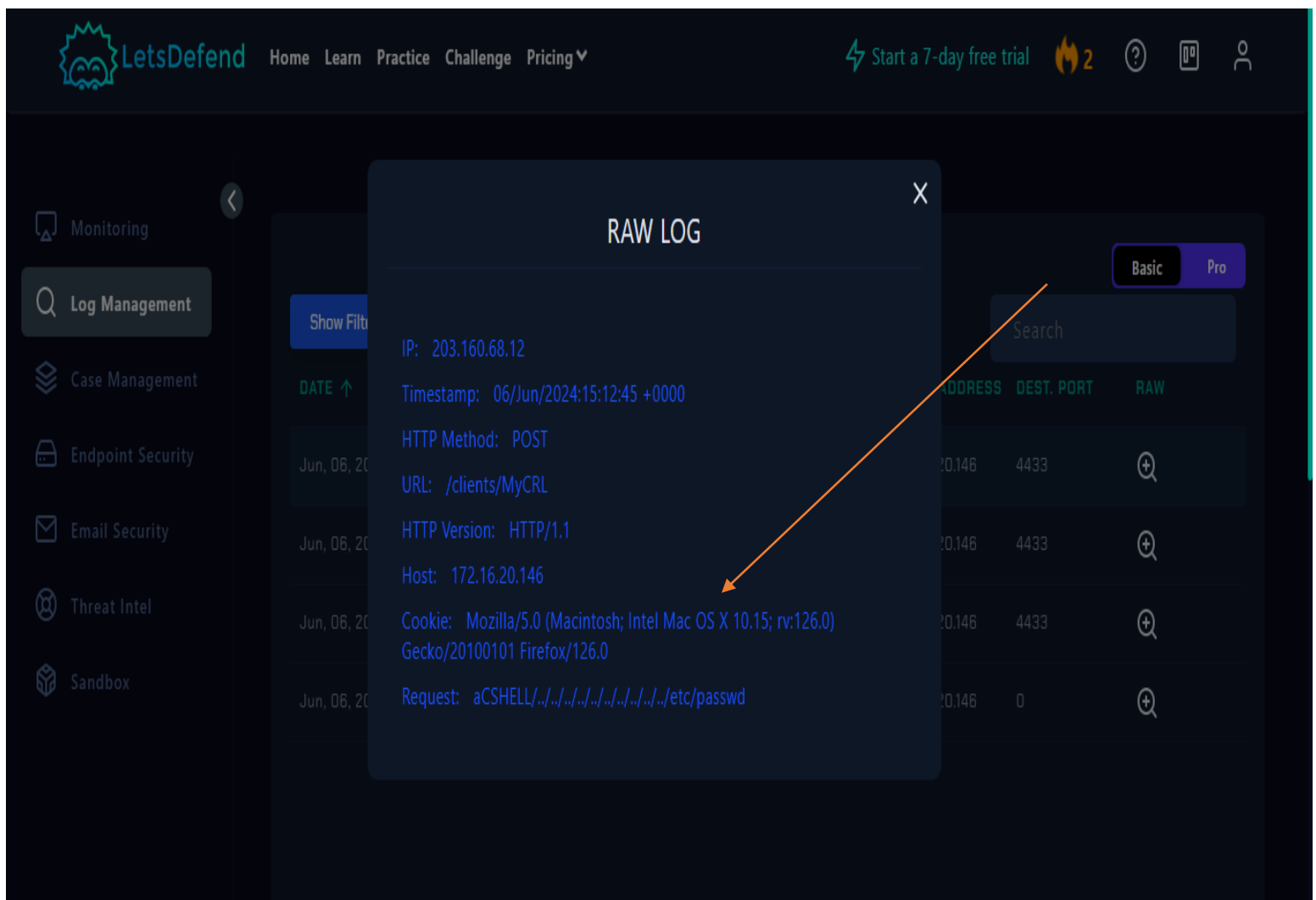
For more detailed information, refer to the attached photo



The log entry indicates a potentially malicious HTTP request targeting a specific server. Here's a breakdown of what's happening:

- **IP Address:** The request originated from 203.160.68.12.
- **Timestamp:** The activity occurred on June 6, 2024, at 15:12:45 UTC.
- **HTTP Method:** The request used the POST method.
- **URL:** The target endpoint is `/clients/MyCRL`.
- **HTTP Version:** The request was made using HTTP/1.1.
- **Host:** The targeted server's IP address is 172.16.20.146.
- **User-Agent:** The request header includes a user-agent string indicating the request was made using Firefox on a macOS system (Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0).

For more detailed information, refer to the attached photo

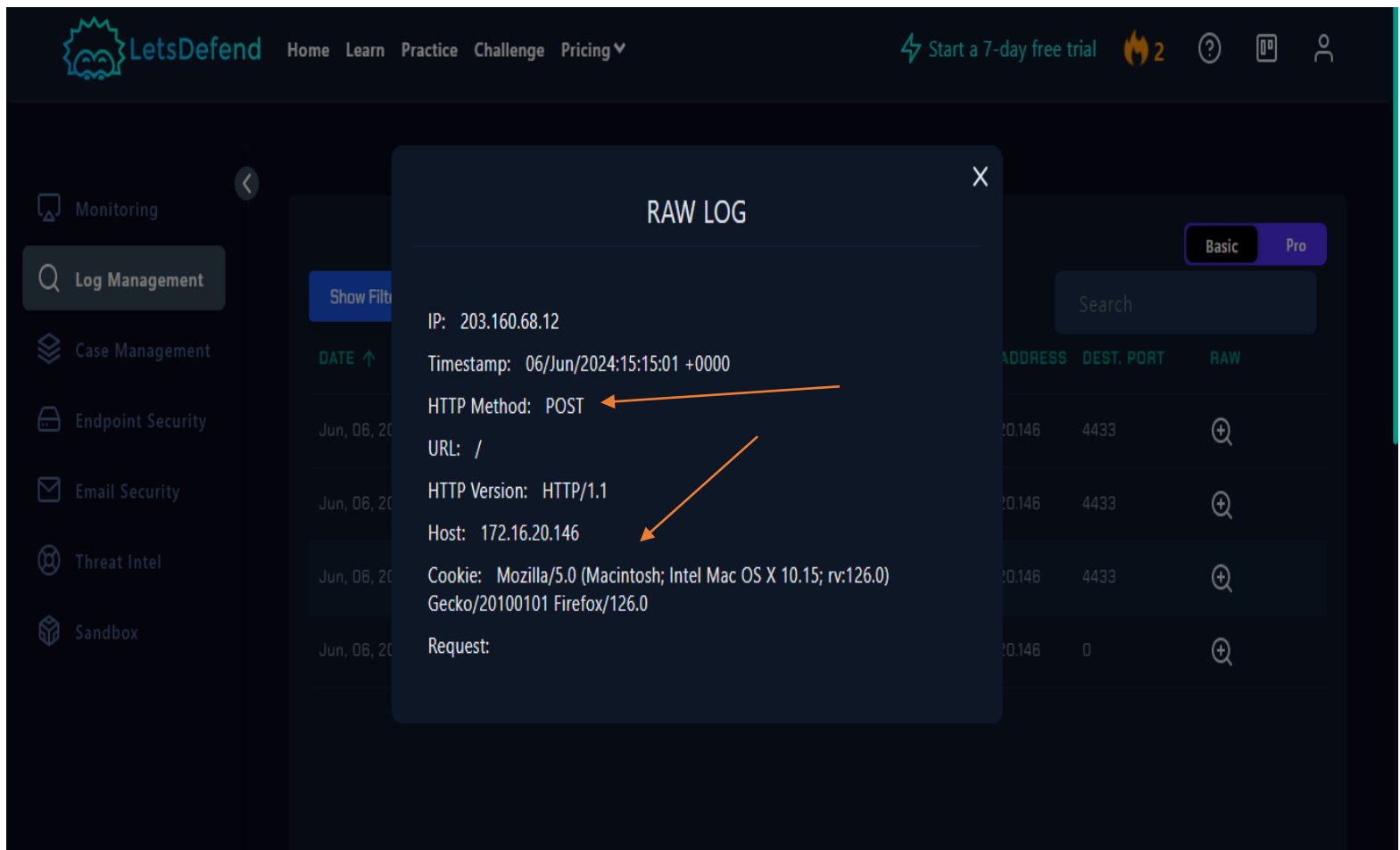


The log entry provides information about an HTTP request that could potentially indicate malicious activity. Here's a detailed breakdown:

Log Details

- **IP Address:** The request originated from 203.160.68.12.
- **Timestamp:** The request was made on June 6, 2024, at 15:15:01 UTC.
- **HTTP Method:** The method used for the request is POST, which is typically used to send data to the server.
- **URL:** The request was made to the root endpoint / of the server.
- **HTTP Version:** The request was made using HTTP/1.1.
- **Host:** The target server's IP address is 172.16.20.146.
- **User-Agent:** The request header includes a user-agent string indicating it was made using Firefox on a macOS system (Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0).

For more detailed information, refer to the attached photo



This log file from `/var/log/access.log` provides a snapshot of web server activity, highlighting several HTTP requests from various IP addresses. Let's analyze the key entries, focusing on the potential malicious activities:

Notable Entries

1. IP: 203.160.68.12

- **Timestamp:** 06/Jun/2024:15:12:43 +0000
- **Request:** GET /clients/MyCRL HTTP/1.1
- **Response:** 200 (OK)
- **User-Agent:** "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0"

Description: This entry indicates a successful GET request to the `/clients/MyCRL` endpoint, with a standard user-agent string. The response code 200 signifies a successful request.

2. IP: 203.160.68.12

- **Timestamp:** 06/Jun/2024:15:12:45 +0000
- **Request:** POST /clients/MyCRL HTTP/1.1
- **Response:** 200 (OK)
- **Request Body:** "aCSHELL/////////etc/passwd"
- **User-Agent:** "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0"

Description: This POST request is attempting a directory traversal attack, specifically targeting the `/etc/passwd` file. The attempt to access this file is typically an effort to retrieve sensitive system information, such as user details. The response code 200 indicates the server processed the request, raising concerns about potential data exposure.

3. IP: 192.168.1.100

- **Timestamp:** 06/Jun/2024:15:13:01 +0000
- **Request:** GET / HTTP/1.1
- **Response:** 404 (Not Found)
- **User-Agent:** "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36"

Description: This request resulted in a 404 error, indicating the requested resource was not found on the server. This could be a legitimate user error or a part of reconnaissance activities.

4. IP: 203.160.68.13

- **Timestamp:** 06/Jun/2024:15:14:02 +0000
- **Request:** POST /clients/MyCRL HTTP/1.1
- **Response:** 403 (Forbidden)
- **Request Body:** "aCSHELL/////////etc/shadow"

- **User-Agent:** "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0"

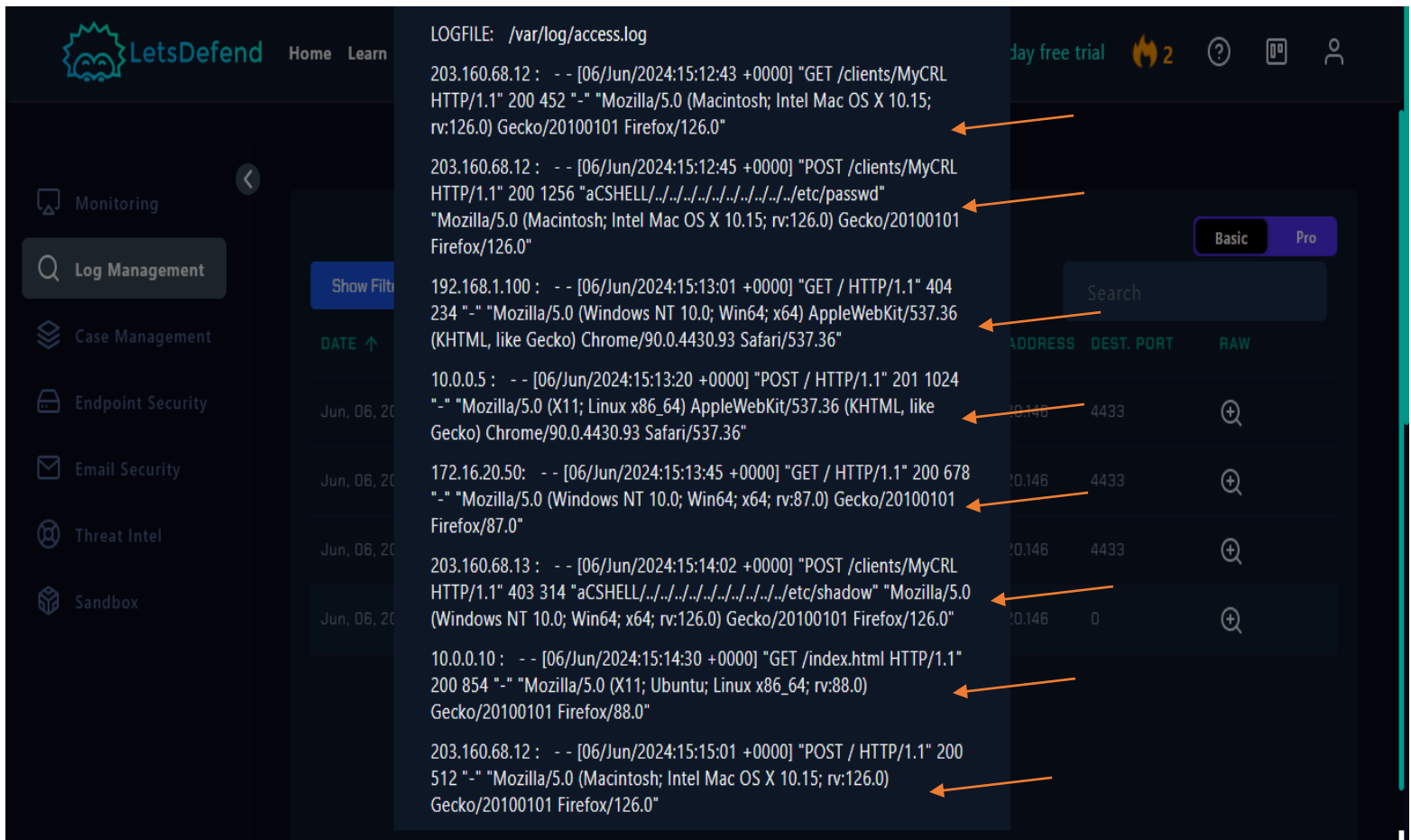
Description: Similar to the previous attack, this POST request attempts to access the `/etc/shadow` file, which contains encrypted passwords. The server responded with a 403 Forbidden status, indicating that the request was blocked, which is a positive security response.

5. IP: 203.160.68.12

- **Timestamp:** 06/Jun/2024:15:15:01 +0000
- **Request:** POST / HTTP/1.1
- **Response:** 200 (OK)
- **User-Agent:** "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0"

Description: This POST request to the root endpoint / returned a 200 OK response. The absence of a specific resource path suggests a possible probe or attempt to interact with the server without a clear objective. The consistent use of the same user-agent string across requests might indicate automation or script usage.

For more detailed information, refer to the attached photo



The analysis of the provided logs reveals a series of suspicious activities that indicate potential security incidents:

1. Brute Force Login Attempt:

- The log entry indicating a failed login attempt for the username 'guest' with EventID: 4625 suggests a possible brute force attack. This pattern of failed logins is often an indicator of unauthorized attempts to access an account by guessing the password.

2. Directory Traversal Attack:

- The repeated POST requests from IP address 203.160.68.12, particularly to `/clients/MyCRL`, demonstrate an attempt to exploit a directory traversal vulnerability. The request trying to access the sensitive `/etc/passwd` file, as well as subsequent attempts on other endpoints, indicates an effort to gather critical system information. The use of a crafted payload (`aCSHELL/../../../../../../../../../../../../../../../../etc/passwd`) aims to traverse directories and access unauthorized files.

3. Inconsistent HTTP Requests:

- Additional log entries, including a GET request that resulted in a 404 error, further suggest probing or reconnaissance activities. These requests are attempts to identify valid endpoints or vulnerabilities in the server.

4. Response Codes and User Agents:

- The 200 OK and 403 Forbidden response codes, along with varying user-agent strings, indicate that the attacker is using multiple methods and tools to evade detection and bypass security controls.

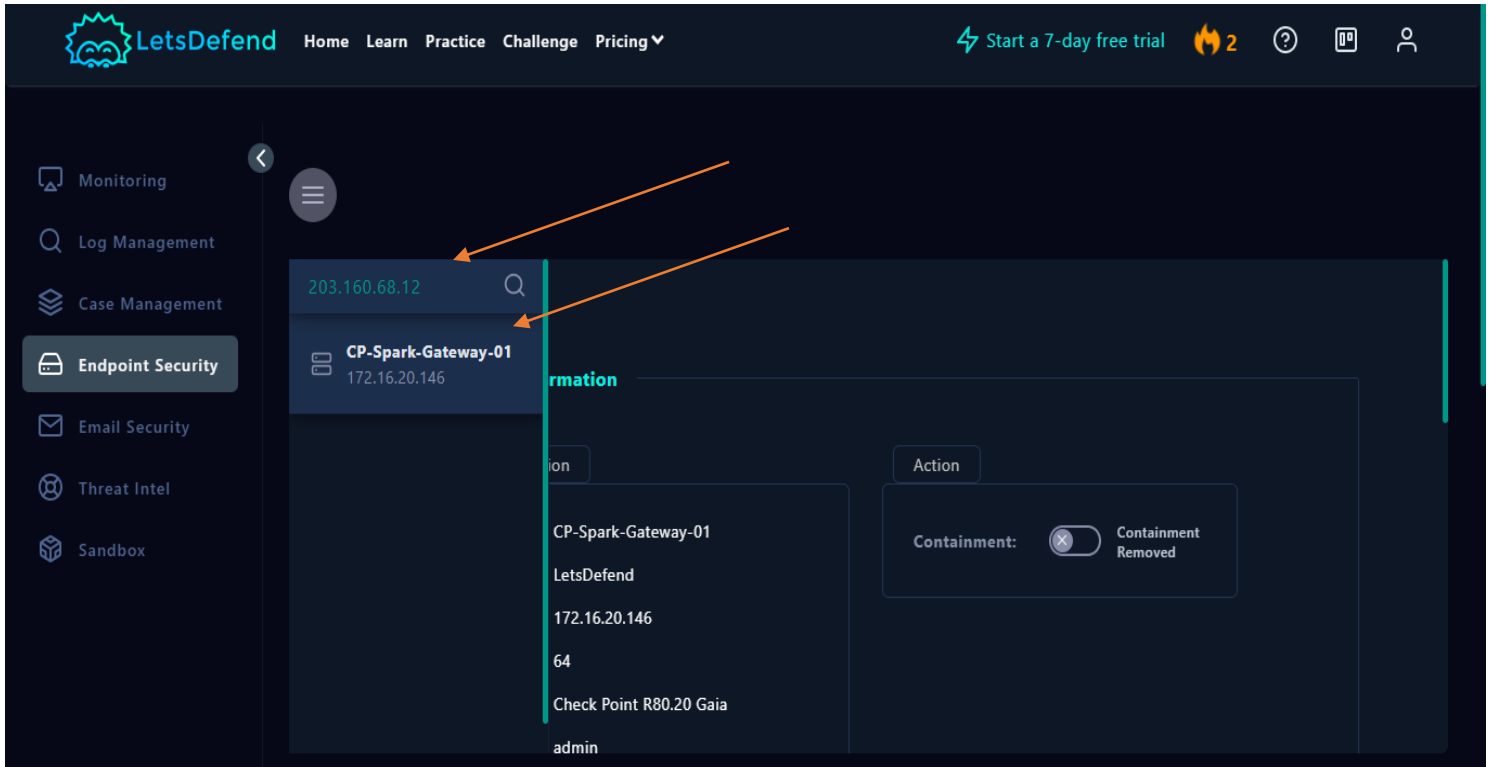
Assessment and Recommendations

The observed activities from IP addresses 203.160.68.12 and 203.160.68.13 raise significant security concerns, particularly the attempt to exploit potential vulnerabilities in the server. The successful response to directory traversal attacks suggests a lack of sufficient security controls, such as input validation and proper sanitization.

Endpoint Security

To conduct a thorough analysis, I entered the attacker's IP address into our monitoring system to review the associated data. The investigation covered several critical areas, including Processes, Network Actions, Terminal History, and Browser History.

For more detailed information, refer to the attached photo



Upon conducting a comprehensive review using the attacker's IP address, we found pertinent results solely from the Network Action analysis. This data provides crucial insights into the network behaviors and interactions associated with the IP, highlighting specific patterns and actions taken during the observed time frame. Further analysis is required for a complete assessment.

For more detailed information, refer to the attached photo

The screenshot displays the LetsDefend web application interface. The top navigation bar includes the LetsDefend logo, links for Home, Learn, Practice, Challenge, and Pricing, and a search bar containing the IP address 203.160.68.12. The left sidebar lists various security modules: Monitoring, Log Management, Case Management, Endpoint Security (highlighted), Email Security, Threat Intel, and Sandbox. The main content area shows a list of network actions. The 'Network Action' tab is selected, displaying 54 results. The table has two columns: 'EVENT TIME' and 'DESTINATION DOMAIN/IP ADDRESS'. Two rows are highlighted with orange arrows pointing to the IP address 203.160.68.12.

EVENT TIME	DESTINATION DOMAIN/IP ADDRESS
Jun 6 2024 15:12:43	203.160.68.12
Jun 6 2024 15:12:45	203.160.68.12
Jun 6 2024 15:12:48	203.160.68.13
Jun 6 2024 15:13:00	172.16.20.50

Brute Force Login Attempt:

The log shows a failed login attempt for the username 'guest' with EventID: 4625, suggesting a potential brute force attack. This pattern of unsuccessful login attempts typically indicates unauthorized efforts to access an account by guessing passwords.

Directory Traversal Attack:

Repeated POST requests from IP address 203.160.68.12, specifically targeting the `/clients/MyCRL` endpoint, indicate an attempt to exploit a directory traversal vulnerability. The request aimed at accessing the sensitive `/etc/passwd` file, along with subsequent efforts on other endpoints, demonstrates an attempt to gather critical system information. The crafted payload (`acSHELL/../../../../../../../../../../../../../../../../etc/passwd`) was intended to traverse directories and access unauthorized files.

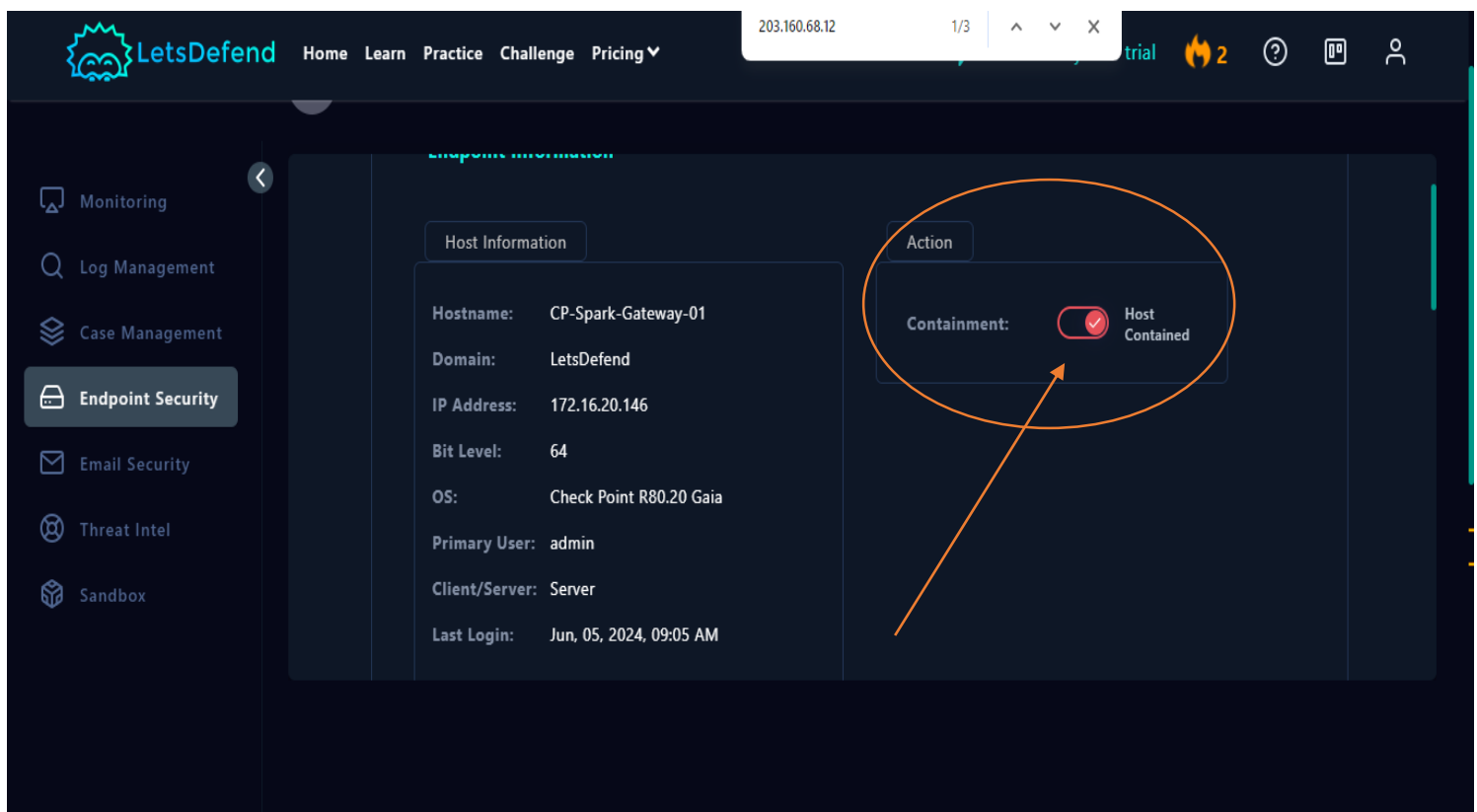
Inconsistent HTTP Requests:

Additional log entries, including a GET request that resulted in a 404 error, suggest reconnaissance activities. These attempts appear to be probing for valid endpoints or server vulnerabilities.

Response Codes and User Agents:

The presence of both 200 OK and 403 Forbidden response codes, along with a variety of user-agent strings, indicates that the attacker is employing multiple methods and tools to evade detection and circumvent security controls.

Based on our detection and analysis, the server has been secured and containment measures have been implemented to prevent further unauthorized access.



Conclusion

Overview: The security incident involved multiple malicious activities, primarily targeting the server at IP address 172.16.20.146. The attacks originated from the external IP address 203.160.68.12, which has been associated with various malicious behaviors, including brute force attempts and directory traversal attacks.

Key Findings:

1. **Brute Force Login Attempt:**
 - **Event Detected:** Failed login attempts for the username 'guest' were logged with EventID: 4625.
 - **Implication:** The pattern suggests a potential brute force attack, where unauthorized users attempt to gain access by systematically guessing passwords.
2. **Directory Traversal Attack:**
 - **Activity Observed:** Repeated POST requests from IP 203.160.68.12 targeted the endpoint /clients/MyCRL.
 - **Exploitation Attempt:** The crafted payload (e.g., `aCSHELL/../../../../../../../../../../../../etc/passwd`) indicates an attempt to exploit a directory traversal vulnerability to access sensitive system files.
3. **Reconnaissance Activities:**
 - **Behavior:** Inconsistent HTTP requests, including a GET request resulting in a 404 error, suggest probing actions to discover valid endpoints or vulnerabilities.
 - **User Agents:** The use of varying user-agent strings and different response codes (200 OK and 403 Forbidden) indicates the attacker employed diverse methods to evade detection and explore the system's defenses.
4. **Threat Intelligence Correlation:**
 - **IP Analysis:** The IP address 203.160.68.12 was flagged as malicious by multiple security vendors, including Fortinet, SOCRadar, and Webroot, for activities such as malware distribution and phishing.
 - **Contextual Insight:** The IP address is linked to the CVE-2024-24919 vulnerability, a known issue in Check Point's Remote Access VPN products, allowing unauthorized access through improper credential validation.

Action Taken:

- **Containment:** Immediate containment measures were implemented to secure the affected server and prevent further unauthorized access.
- **Mitigation:** Enhanced monitoring and logging mechanisms have been activated to track and respond to any additional suspicious activities.

Recommendations:

- **Patch Management:** Apply the latest security patches, particularly for vulnerabilities like CVE-2024-24919.
- **Security Posture Review:** Conduct a comprehensive review of security controls and policies to strengthen defenses against similar attacks.
- **Continuous Monitoring:** Maintain vigilant monitoring of network traffic and server logs to detect and respond to future threats promptly.