LetsDefend

Official Incident Report

Event ID: 263

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

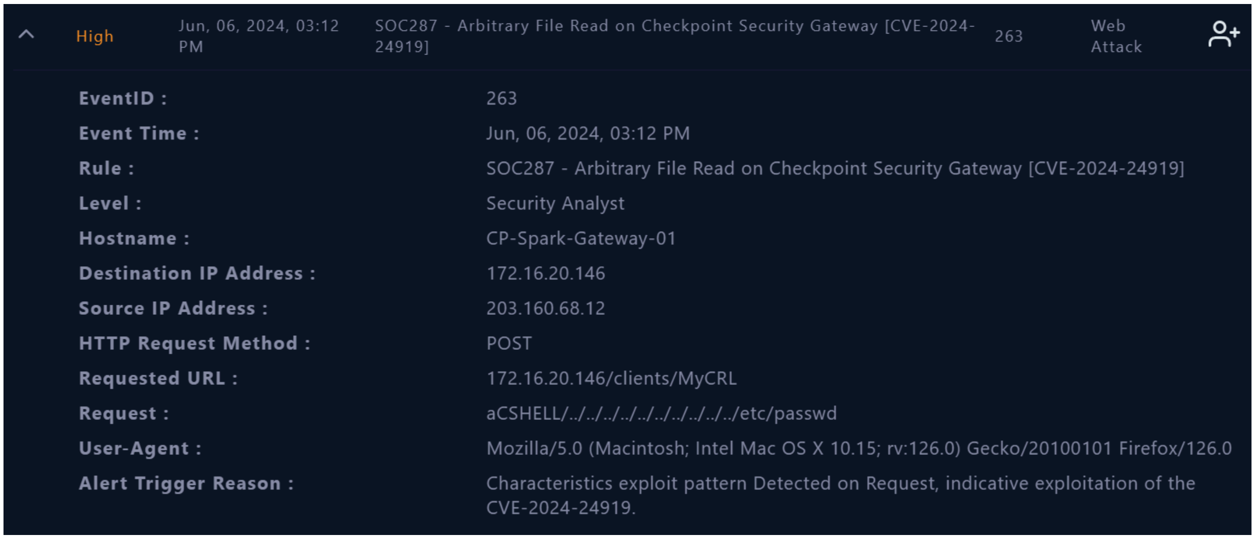
Table of Contents

Alert

Based on the information that the alert provided, it appears that there is a suspicious Web Attack detected on a server named "**CP-Spark-Gateway-01**" with an IP address of **172.16.20.146**. The Alert is triggered by the **SOC287** rule for **Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919]**.

CVE-2024-24919 is a zero-day arbitrary file read in Check Point Security Gateways with the IPSec VPN or Mobile Access blades enabled, and it is currently being actively exploited in the wild.

The device action is marked as "Allowed", indicating that no action was taken by the device to prevent or block the related activities.



High | Jun, 06, 2024, 03:12 PM | SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919] | 263 | Web Attack

EventID :	263
Event Time :	Jun, 06, 2024, 03:12 PM
Rule :	SOC287 - Arbitrary File Read on Checkpoint Security Gateway [CVE-2024-24919]
Level :	Security Analyst
Hostname :	CP-Spark-Gateway-01
Destination IP Address :	172.16.20.146
Source IP Address :	203.160.68.12
HTTP Request Method :	POST
Requested URL :	172.16.20.146/clients/MyCRL
Request :	aCSHELL/../../../../../../../../../../etc/passwd
User-Agent :	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0
Alert Trigger Reason :	Characteristics exploit pattern Detected on Request, indicative exploitation of the CVE-2024-24919.

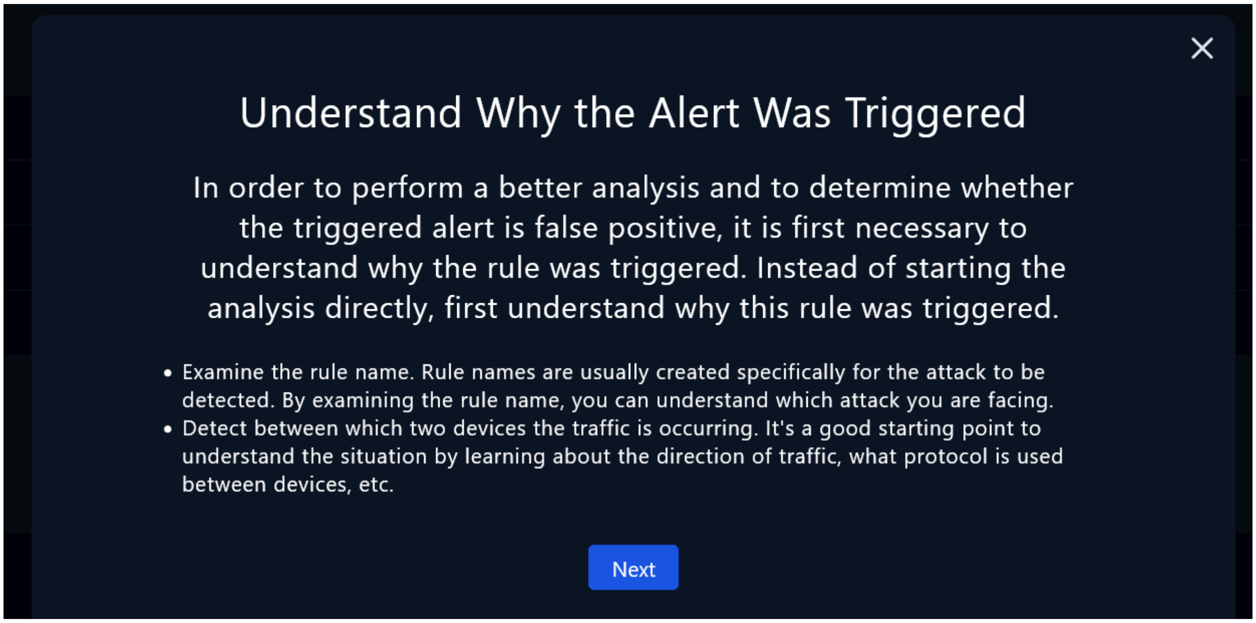
The **CP-Spark-Gateway-01** received a POST request from the IP address **203.160.68[.]12**. The requested URL is '**/clients/MyCRL**'. This activity was flagged as detection of Characteristics exploit pattern on request which indicates exploitation of the CVE-2024-24919, and led to the triggering of an alert.

The request contains "aCSHELL/../../../../../../../../../../etc/passwd". This could potentially allow for arbitrary file read on Check Point Security Gateway.

Detection

Verify

As the playbook suggests we can start investigating the alert by understanding why the alert was triggered.



Understand Why the Alert Was Triggered

In order to perform a better analysis and to determine whether the triggered alert is false positive, it is first necessary to understand why the rule was triggered. Instead of starting the analysis directly, first understand why this rule was triggered.

- Examine the rule name. Rule names are usually created specifically for the attack to be detected. By examining the rule name, you can understand which attack you are facing.
- Detect between which two devices the traffic is occurring. It's a good starting point to understand the situation by learning about the direction of traffic, what protocol is used between devices, etc.

Examine the rule name. Rule names are usually created specifically for the attack to be detected. By examining the rule name, you can understand which attack you are facing.

- The above instructions indicate that there has been a flagged anomalous activity involving suspicious activity for CVE-2024-24919 during a POST request on the CP-Spark-Gateway-01. This activity could potentially result in an arbitrary file read on the host. By understanding the rule name, it will be possible to determine the nature of the attack being faced.

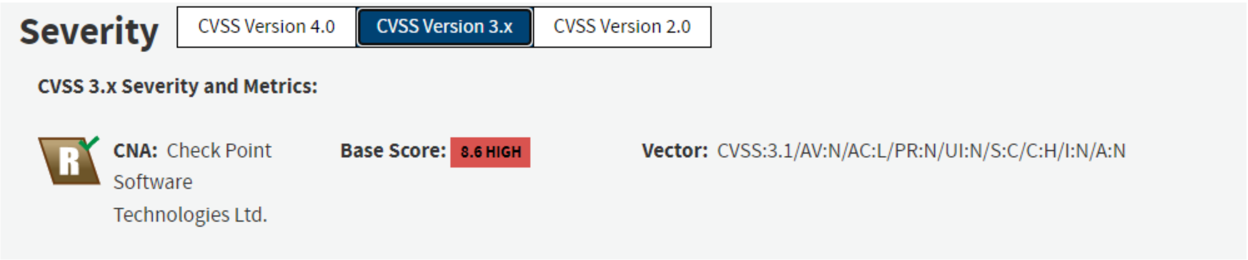
Detect between which two devices the traffic is occurring. It's a good starting point to understand the situation by learning about the direction of traffic, what protocol is used between devices, etc.

The alert details provide information about the source and destination IP addresses involved in the suspicious network traffic:

- Source IP Address: 203.160.68[.]12
- Destination IP Address (Hostname): 172.16.20.146 (CP-Spark-Gateway-01)

Severity & Affected Versions

Potentially allowing an attacker to read certain information on Check Point Security Gateways once connected to the internet and enabled with remote Access VPN or Mobile Access Software Blades. The severity for this vulnerability is **8.6** which is **HIGH**.

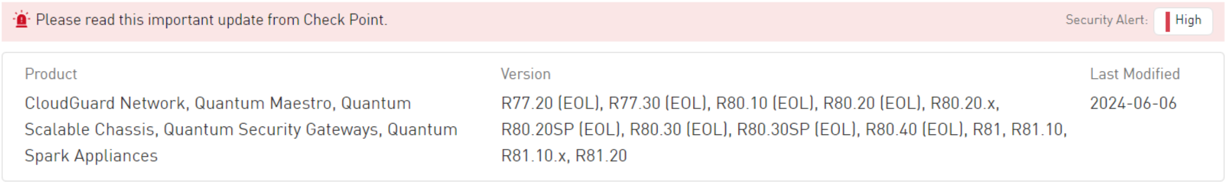


CVSS 3.x Severity and Metrics:

CNA: Check Point Software Technologies Ltd.

Base Score: 8.6 HIGH

Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N



Please read this important update from Check Point.

Security Alert: High

Product	Version	Last Modified
CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways, Quantum Spark Appliances	R77.20 (EOL), R77.30 (EOL), R80.10 (EOL), R80.20 (EOL), R80.20.x, R80.20SP (EOL), R80.30 (EOL), R80.30SP (EOL), R80.40 (EOL), R81, R81.10, R81.10.x, R81.20	2024-06-06

Some of the information about CVE-2024-24919 are listed on Check Point website.

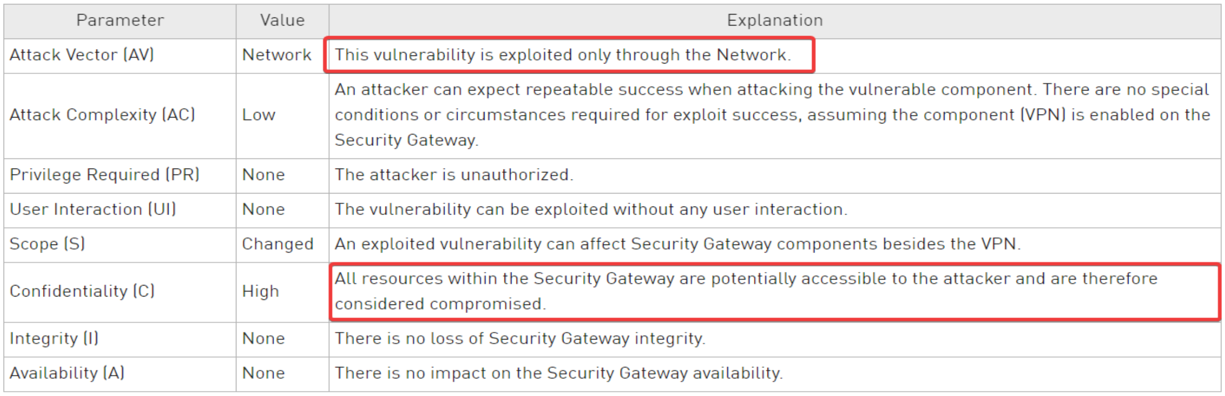
Affected Products:

- CloudGuard Network, Quantum Maestro, Quantum Scalable Chassis, Quantum Security Gateways, **Quantum Spark** Appliances

Affected Versions:

- **CVE-2024-24919:** PAN-OS 10.2, PAN-OS 11.0, and PAN-OS 11.1.

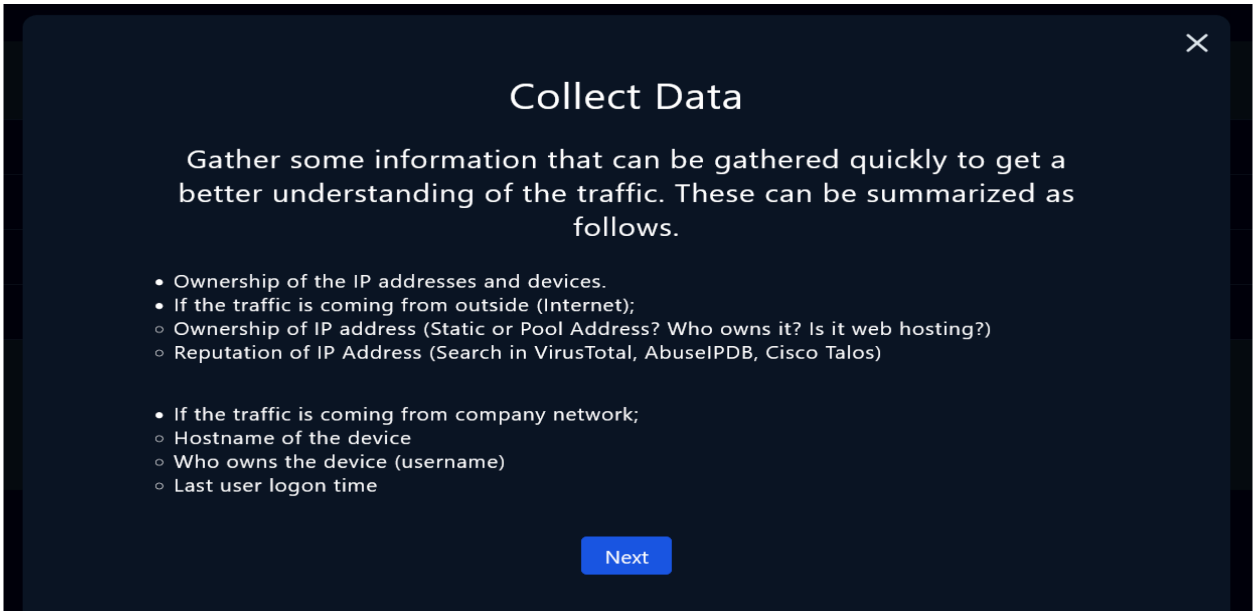
An unauthenticated remote attacker could leverage this vuln to read sensitive data like password hashes and complete network compromise under the right circumstances.



Parameter	Value	Explanation
Attack Vector (AV)	Network	This vulnerability is exploited only through the Network.
Attack Complexity (AC)	Low	An attacker can expect repeatable success when attacking the vulnerable component. There are no special conditions or circumstances required for exploit success, assuming the component (VPN) is enabled on the Security Gateway.
Privilege Required (PR)	None	The attacker is unauthorized.
User Interaction (UI)	None	The vulnerability can be exploited without any user interaction.
Scope (S)	Changed	An exploited vulnerability can affect Security Gateway components besides the VPN.
Confidentiality (C)	High	All resources within the Security Gateway are potentially accessible to the attacker and are therefore considered compromised.
Integrity (I)	None	There is no loss of Security Gateway integrity.
Availability (A)	None	There is no impact on the Security Gateway availability.

Collect Data

The next step in the playbook leads us to collect data and gather information about the relevant IP address.



Collect Data

Gather some information that can be gathered quickly to get a better understanding of the traffic. These can be summarized as follows.

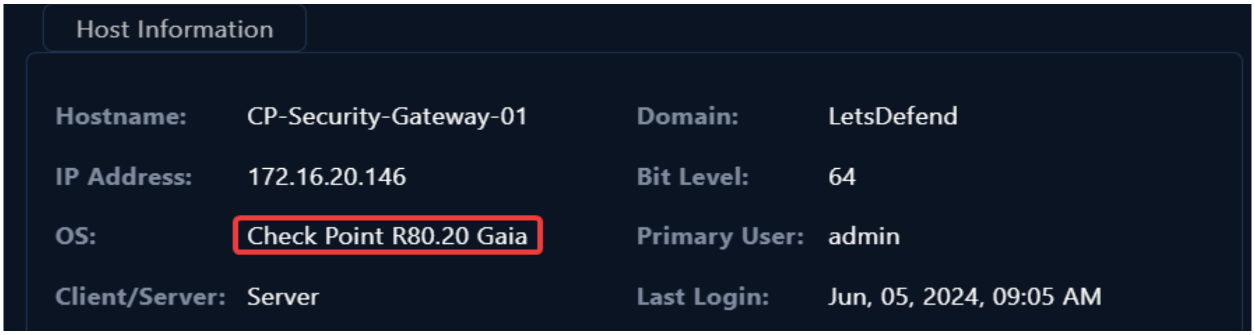
- Ownership of the IP addresses and devices.
- If the traffic is coming from outside (Internet);
  - Ownership of IP address (Static or Pool Address? Who owns it? Is it web hosting?)
  - Reputation of IP Address (Search in VirusTotal, AbuseIPDB, Cisco Talos)

- If the traffic is coming from company network;
  - Hostname of the device
  - Who owns the device (username)
  - Last user logon time

Examining whether the IP address or domain has been linked to prior malicious activities and ownership of the IP address can provide insights into the current activity.

Hostname:	CP-Spark-Gateway-01
IP Address:	172.16.20.146
Version:	Check Point R80.20 Gaia
Last Logon:	Jun, 05, 2024, 09:05 AM

When going through the technical details on the Check Point website to check the affected versions, it's noted that **CP-Spark-Gateway-01** with the IP address **172.16.20.146** is affected by this vulnerability because of version **R80.20** is affected.



Host Information

Hostname: CP-Security-Gateway-01

IP Address: 172.16.20.146

OS: Check Point R80.20 Gaia

Client/Server: Server

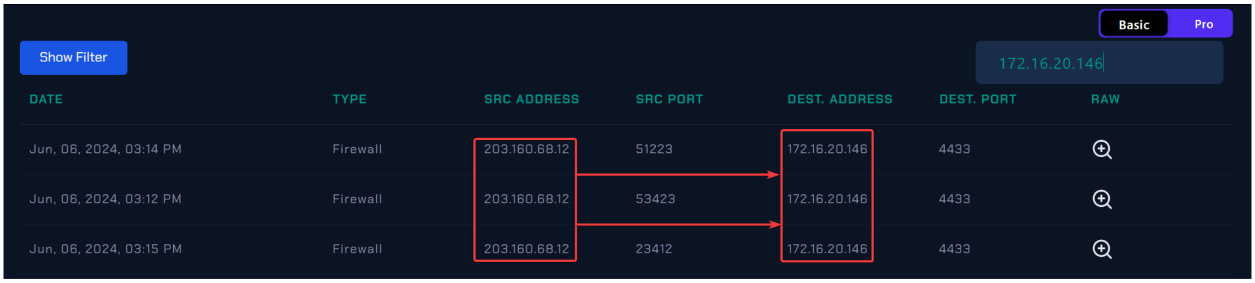
Domain: LetsDefend

Bit Level: 64

Primary User: admin

Last Login: Jun, 05, 2024, 09:05 AM

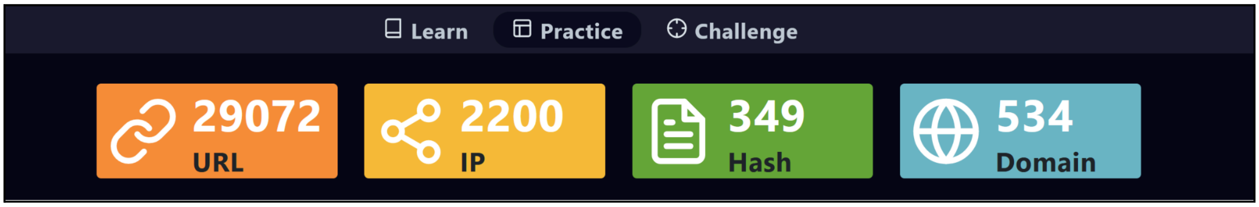
We can check if the traffic is inbound or outbound from the log management system by filtering the IP address of the host. As seen in the log management traffic is inbound. There is a suspicious IP address with **203.160.68[.]12** ip



172.16.20.146

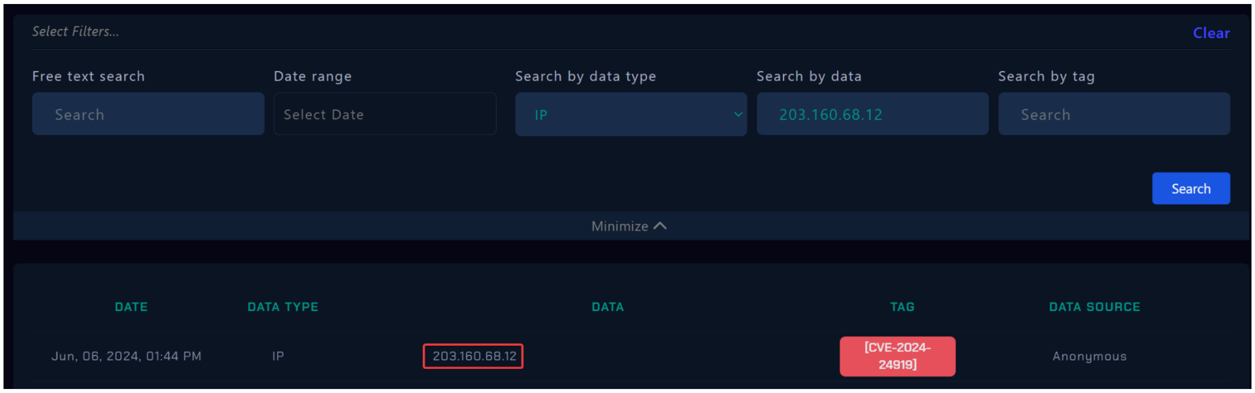
DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jun, 06, 2024, 03:14 PM	Firewall	203.160.68.12	51223	172.16.20.146	4433	
Jun, 06, 2024, 03:12 PM	Firewall	203.160.68.12	53423	172.16.20.146	4433	
Jun, 06, 2024, 03:15 PM	Firewall	203.160.68.12	23412	172.16.20.146	4433	

On the LetsDefend threat intel tab, you'll find a comprehensive database dedicated to cataloging maliciously used information, such as IP addresses, domains, and other indicators of compromise.



https://app.letsdefend.io/threath-intelligence-feed

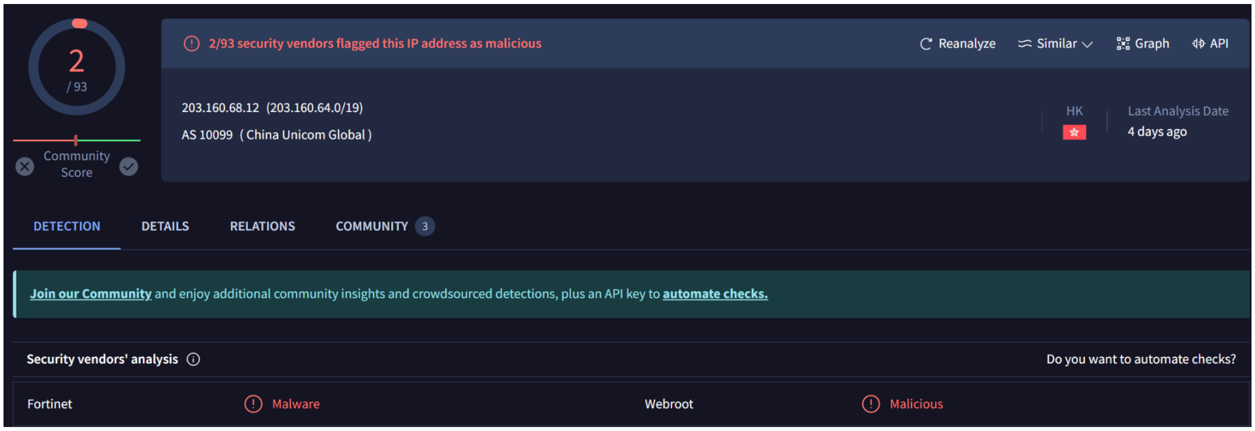
Upon cross-referencing the destination IP address discovered in the log management system with the Threat Intel tab, it was determined that the address had been categorized as [CVE-2024-24919].



Free text search: Search
Date range: Select Date
Search by data type: IP
Search by data: 203.160.68.12
Search by tag: Search

DATE	DATA TYPE	DATA	TAG	DATA SOURCE
Jun, 06, 2024, 01:44 PM	IP	203.160.68.12	[CVE-2024-24919]	Anonymous

By cross-referencing the IP address with threat intelligence platforms such as Abuseip or Virustotal, we discovered that the IP address is malicious and reported many times.



2/93 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
4 days ago

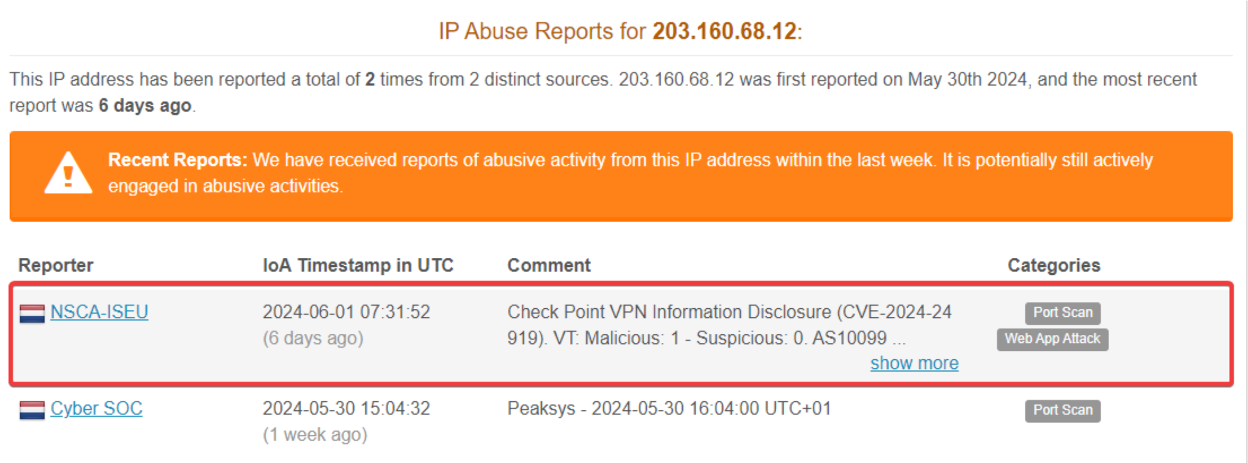
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

Fortinet	Malware	Webroot	Malicious

Based on the information provided by **VirusTotal**, the IP address has been flagged as malicious by **2** antivirus engines. Additionally, in the **AbuseIPDB**, it is seen that this IP is tagged as **Web App Attack - (CVE-2024-24919)**.



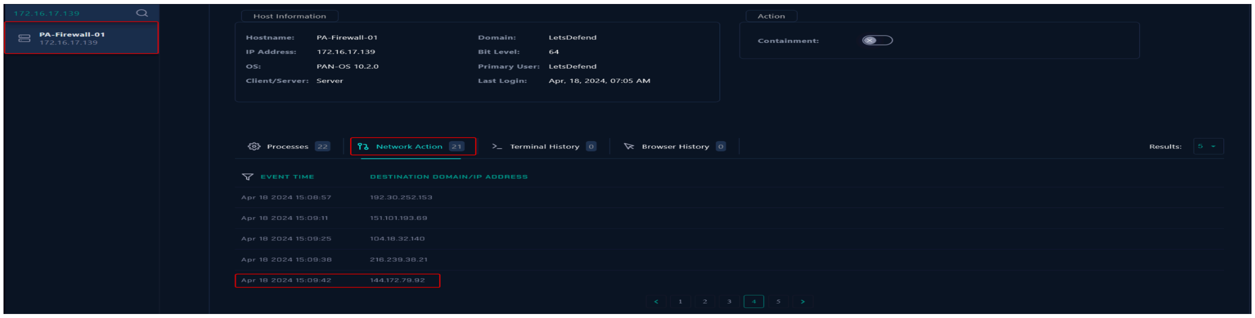
IP Abuse Reports for **203.160.68.12**:

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 **6 days ago**.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	IoA Timestamp in UTC	Comment	Categories
NSCA-ISEU	2024-06-01 07:31:52 (6 days ago)	Check Point VPN Information Disclosure (CVE-2024-24919). VT: Malicious: 1 - Suspicious: 0. AS10099 ... show more	Port Scan Web App Attack
Cyber SOC	2024-05-30 15:04:32 (1 week ago)	Peaksys - 2024-05-30 16:04:00 UTC+01	Port Scan

The IOC is also seen in the network action of the host machine.



Host Information

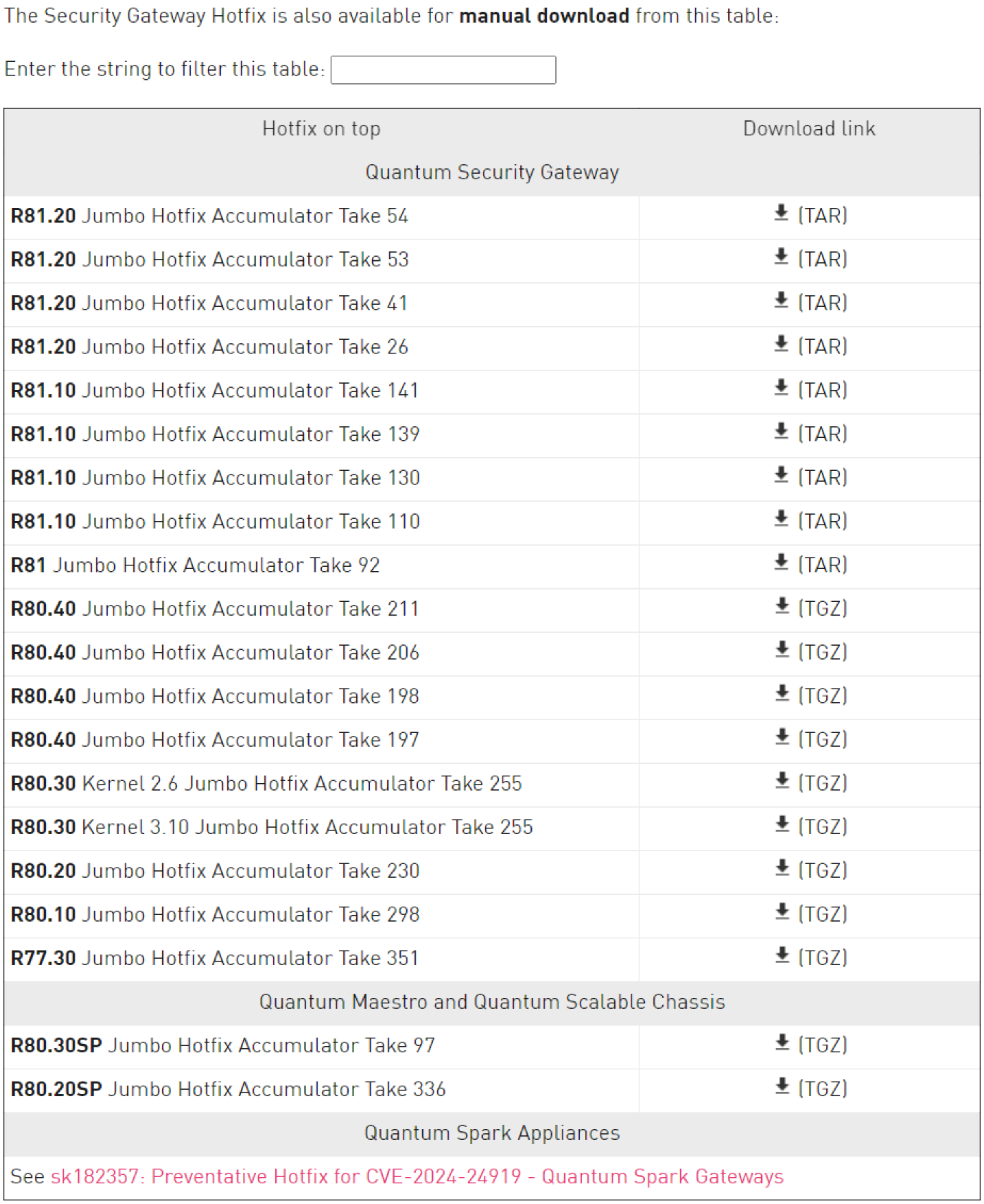
Hostname:	PA-Firewall-01	Domain:	LetsDefend
IP Address:	172.16.17.139	Bit Level:	64
OS:	PAN-OS 10.2.0	Primary User:	LetsDefend
Client/Server:	Server	Last Login:	Apr, 18, 2024, 07:05 AM

Containment: ○

Results: 5

EVENT TIME	DESTINATION DOMAIN/IP ADDRESS
Apr 18 2024 15:08:57	192.30.252.153
Apr 18 2024 15:09:11	151.101.193.69
Apr 18 2024 15:09:25	104.18.32.140
Apr 18 2024 15:09:38	216.239.38.21
Apr 18 2024 15:09:42	144.172.79.92

By visiting the Check Point website we see there is a hotfix released for this vulnerability. It is highly recommended to patch the systems.



The Security Gateway Hotfix is also available for **manual download** from this table:

Enter the string to filter this table:

Hotfix on top	Download link
Quantum Security Gateway	
R81.20 Jumbo Hotfix Accumulator Take 54	⬇ (TAR)
R81.20 Jumbo Hotfix Accumulator Take 53	⬇ (TAR)
R81.20 Jumbo Hotfix Accumulator Take 41	⬇ (TAR)
R81.20 Jumbo Hotfix Accumulator Take 26	⬇ (TAR)
R81.10 Jumbo Hotfix Accumulator Take 141	⬇ (TAR)
R81.10 Jumbo Hotfix Accumulator Take 139	⬇ (TAR)
R81.10 Jumbo Hotfix Accumulator Take 130	⬇ (TAR)
R81.10 Jumbo Hotfix Accumulator Take 110	⬇ (TAR)
R81 Jumbo Hotfix Accumulator Take 92	⬇ (TAR)
R80.40 Jumbo Hotfix Accumulator Take 211	⬇ (TGZ)
R80.40 Jumbo Hotfix Accumulator Take 206	⬇ (TGZ)
R80.40 Jumbo Hotfix Accumulator Take 198	⬇ (TGZ)
R80.40 Jumbo Hotfix Accumulator Take 197	⬇ (TGZ)
R80.30 Kernel 2.6 Jumbo Hotfix Accumulator Take 255	⬇ (TGZ)
R80.30 Kernel 3.10 Jumbo Hotfix Accumulator Take 255	⬇ (TGZ)
R80.20 Jumbo Hotfix Accumulator Take 230	⬇ (TGZ)
R80.10 Jumbo Hotfix Accumulator Take 298	⬇ (TGZ)
R77.30 Jumbo Hotfix Accumulator Take 351	⬇ (TGZ)
Quantum Maestro and Quantum Scalable Chassis	
R80.30SP Jumbo Hotfix Accumulator Take 97	⬇ (TGZ)
R80.20SP Jumbo Hotfix Accumulator Take 336	⬇ (TGZ)
Quantum Spark Appliances	
See sk182357: Preventative Hotfix for CVE-2024-24919 - Quantum Spark Gateways	

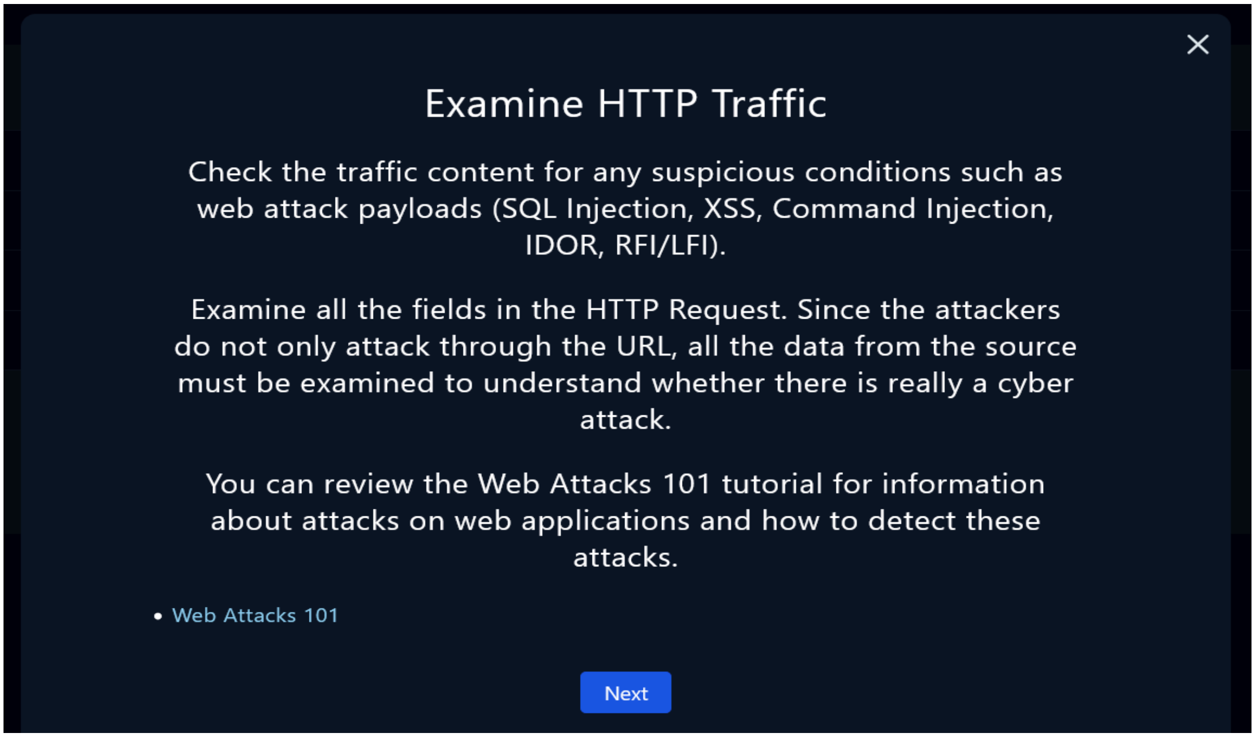
https://support.checkpoint.com/results/sk/sk182336

Analysis

The next step is Investigating the access logs. Focusing on IP addresses, user-agents, paths, HTTP status codes and timestamps will help us identify any suspicious or malicious activity.

Examine The Traffic

The next step of the playbook involves examining the traffic.This step is crucial in identifying any suspicious or malicious activities and understanding the overall network behavior. Additionally, examining the traffic can provide valuable information for further investigation and potential security enhancements.



Examine HTTP Traffic

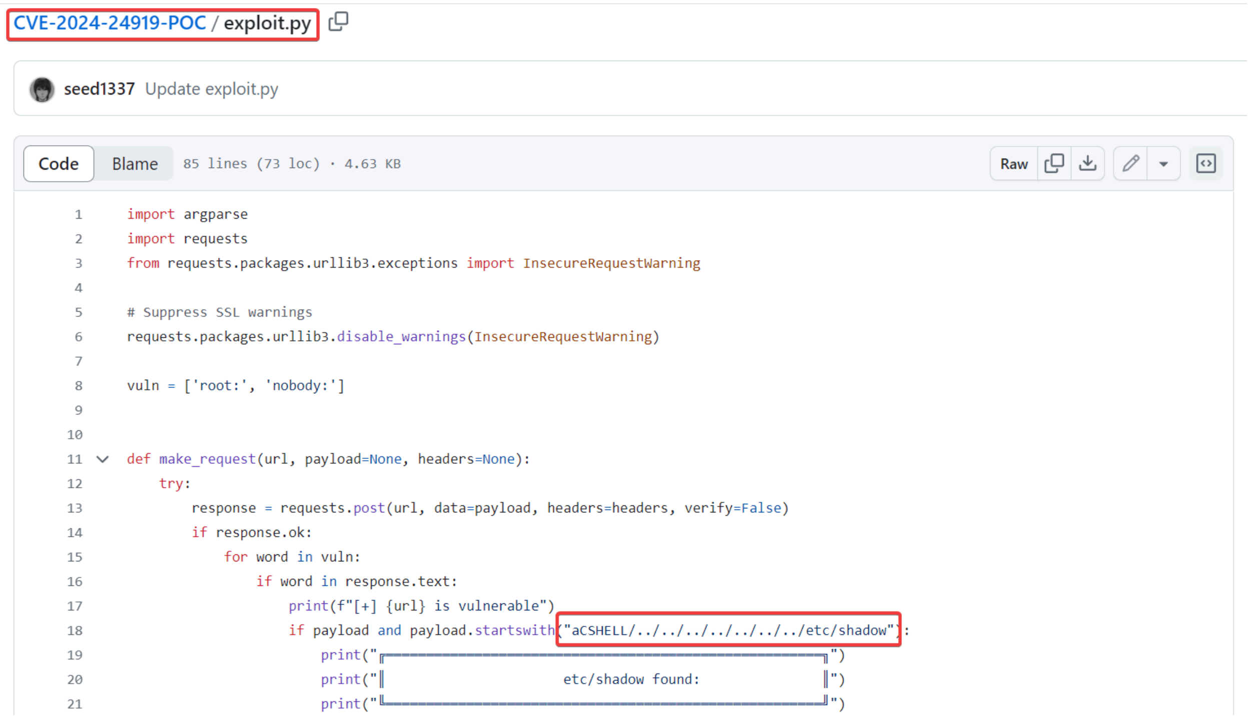
Check the traffic content for any suspicious conditions such as web attack payloads (SQL Injection, XSS, Command Injection, IDOR, RFI/LFI).

Examine all the fields in the HTTP Request. Since the attackers do not only attack through the URL, all the data from the source must be examined to understand whether there is really a cyber attack.

You can review the Web Attacks 101 tutorial for information about attacks on web applications and how to detect these attacks.

- Web Attacks 101

Before examining HTTP traffic, it is crucial to investigate the payloads used in exploiting the relevant vulnerability. There are public POCs in the wild of [CVE-2024-24919].
By checking Github we can find many public POC of [CVE-2024-24919].



CVE-2024-24919-POC / exploit.py

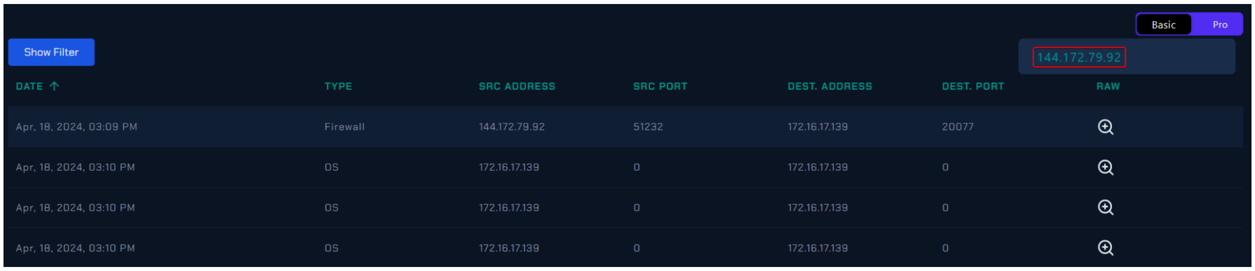
seed1337 Update exploit.py

85 lines (73 loc) · 4.63 KB

```
import argparse
import requests
from requests.packages.urllib3.exceptions import InsecureRequestWarning

# Suppress SSL warnings
requests.packages.urllib3.disable_warnings(InsecureRequestWarning)

vuln = ['root:', 'nobody:']


def make_request(url, payload=None, headers=None):
    try:
        response = requests.post(url, data=payload, headers=headers, verify=False)
        if response.ok:
            for word in vuln:
                if word in response.text:
                    print(f"[+] {url} is vulnerable")
                    if payload and payload.startswith("aCSHELL/../../../../../../../etc/shadow"):
                        print("╔══════════════════════════════════════════════════╗")
                        print("║                 etc/shadow found:                ║")
                        print("╚══════════════════════════════════════════════════╝")
```

https://github.com/seed1337/CVE-2024-24919-POC/blob/main/exploit.py

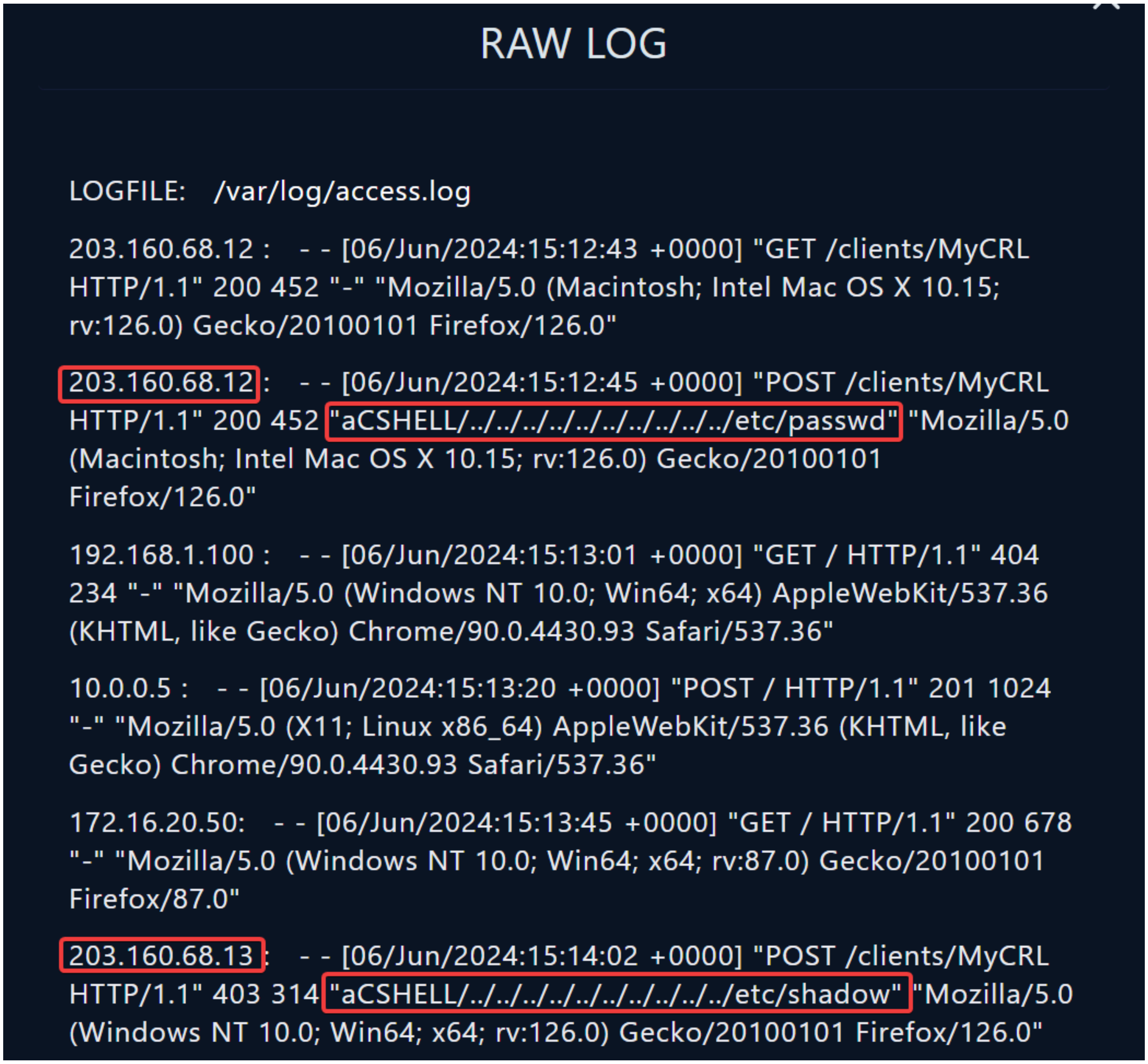
Considering that this attack involves a 0-day exploit targeting the CP-Spark-Gateway-01, we can use the time when the alert was triggered as a reference point for analysis. Filtering the CP-Spark-Gateway-01 IP address in log management allows us to view the logs.



144.172.79.92

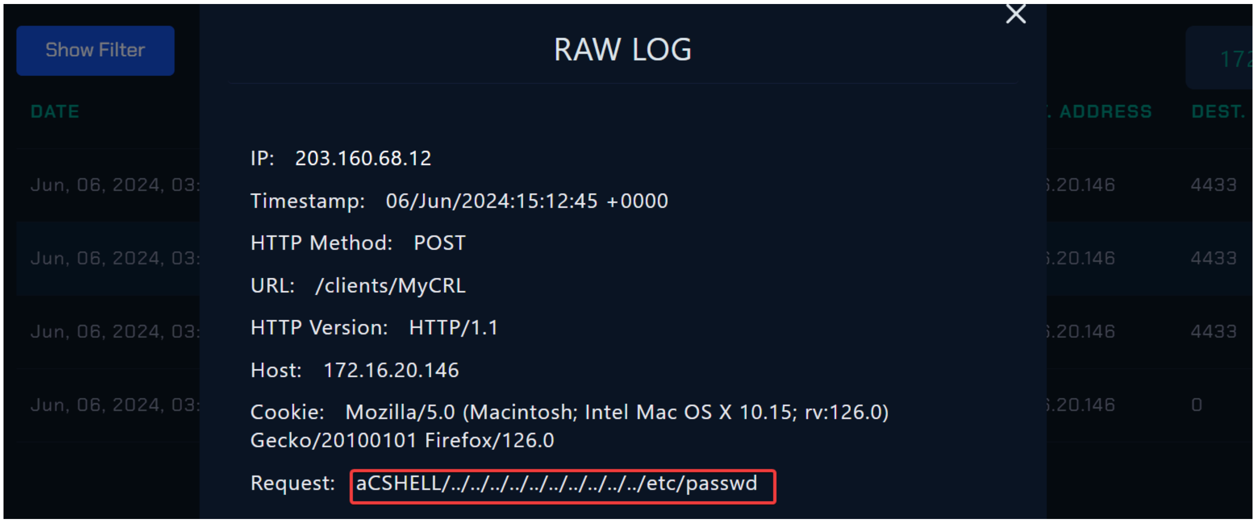
DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Apr, 18, 2024, 03:09 PM	Firewall	144.172.79.92	51232	172.16.17.139	20077	🔍
Apr, 18, 2024, 03:10 PM	OS	172.16.17.139	0	172.16.17.139	0	🔍
Apr, 18, 2024, 03:10 PM	OS	172.16.17.139	0	172.16.17.139	0	🔍
Apr, 18, 2024, 03:10 PM	OS	172.16.17.139	0	172.16.17.139	0	🔍

Firewall logs for the date of Jun 6th are available. These logs are essential for monitoring and analyzing network traffic and security events on that specific date.



RAW LOG

```
LOGFILE:   /var/log/access.log

203.160.68.12 :   - - [06/Jun/2024:15:12:43 +0000] "GET /clients/MyCRL
HTTP/1.1" 200 452 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
rv:126.0) Gecko/20100101 Firefox/126.0"

203.160.68.12 :   - - [06/Jun/2024:15:12:45 +0000] "POST /clients/MyCRL
HTTP/1.1" 200 452 "aCSHELL/../../../../../../../../../../etc/passwd" "Mozilla/5.0
(Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101
Firefox/126.0"

192.168.1.100 :   - - [06/Jun/2024:15:13:01 +0000] "GET / HTTP/1.1" 404
234 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36
(KHTML, like Gecko) Chrome/90.0.4430.93 Safari/537.36"

10.0.0.5 :   - - [06/Jun/2024:15:13:20 +0000] "POST / HTTP/1.1" 201 1024
"-" "Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/90.0.4430.93 Safari/537.36"

172.16.20.50:   - - [06/Jun/2024:15:13:45 +0000] "GET / HTTP/1.1" 200 678
"-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:87.0) Gecko/20100101
Firefox/87.0"

203.160.68.13 :   - - [06/Jun/2024:15:14:02 +0000] "POST /clients/MyCRL
HTTP/1.1" 403 314 "aCSHELL/../../../../../../../../../../etc/shadow" "Mozilla/5.0
(Windows NT 10.0; Win64; x64; rv:126.0) Gecko/20100101 Firefox/126.0"
```



RAW LOG

IP: 203.160.68.12

Timestamp: 06/Jun/2024:15:12:45 +0000

HTTP Method: POST

URL: /clients/MyCRL

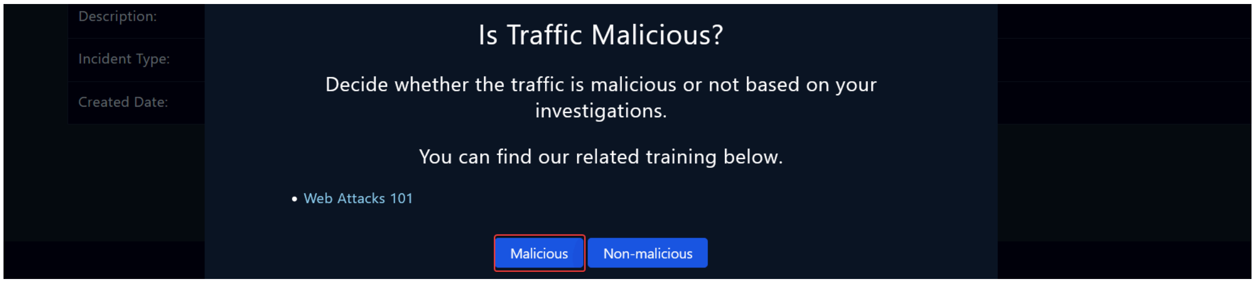
HTTP Version: HTTP/1.1

Host: 172.16.20.146

Cookie: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0

Request: aCSHELL/../../../../../../../../../../etc/passwd

As seen in the raw log the request contains: **“aCSHELL/../../../../../../../../../../etc/passwd”** and the URL is **/clients/MyCRL**.



Description:

Incident Type:

Created Date:

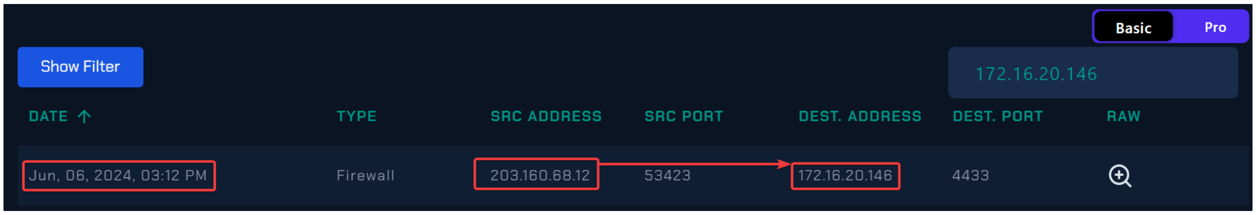
Is Traffic Malicious?

Decide whether the traffic is malicious or not based on your investigations.

You can find our related training below.

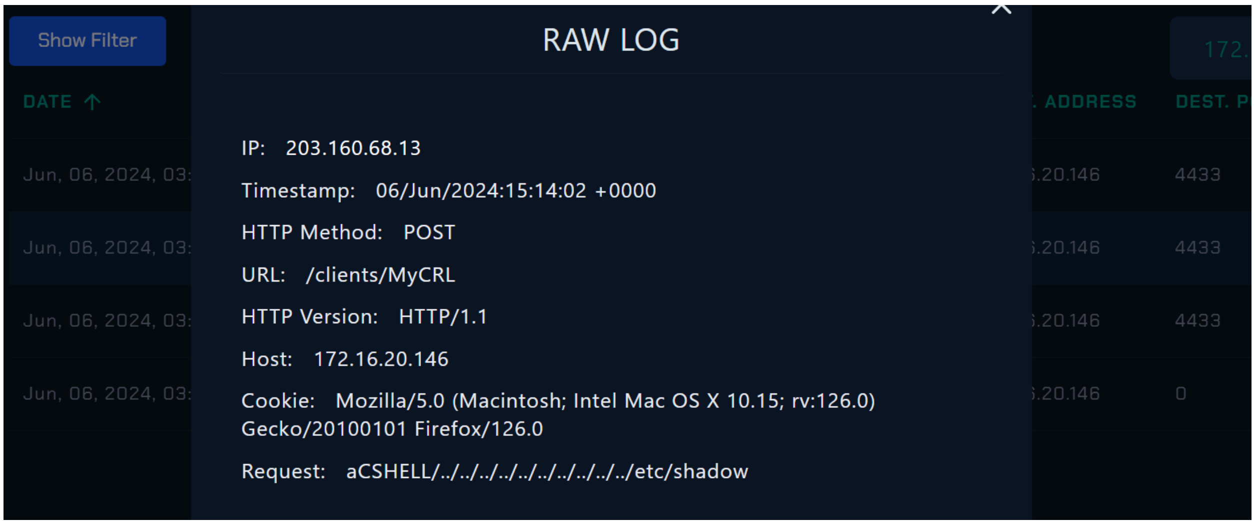
- Web Attacks 101

The traffic originating from **203.160.68[.]12** is malicious.



DATE ↑	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jun, 06, 2024, 03:12 PM	Firewall	203.160.68.12	53423	172.16.20.146	4433	⊕

We also see that the attacker accessed the **/etc/shadow**



RAW LOG

IP: 203.160.68.13

Timestamp: 06/Jun/2024:15:14:02 +0000

HTTP Method: POST

URL: /clients/MyCRL

HTTP Version: HTTP/1.1

Host: 172.16.20.146

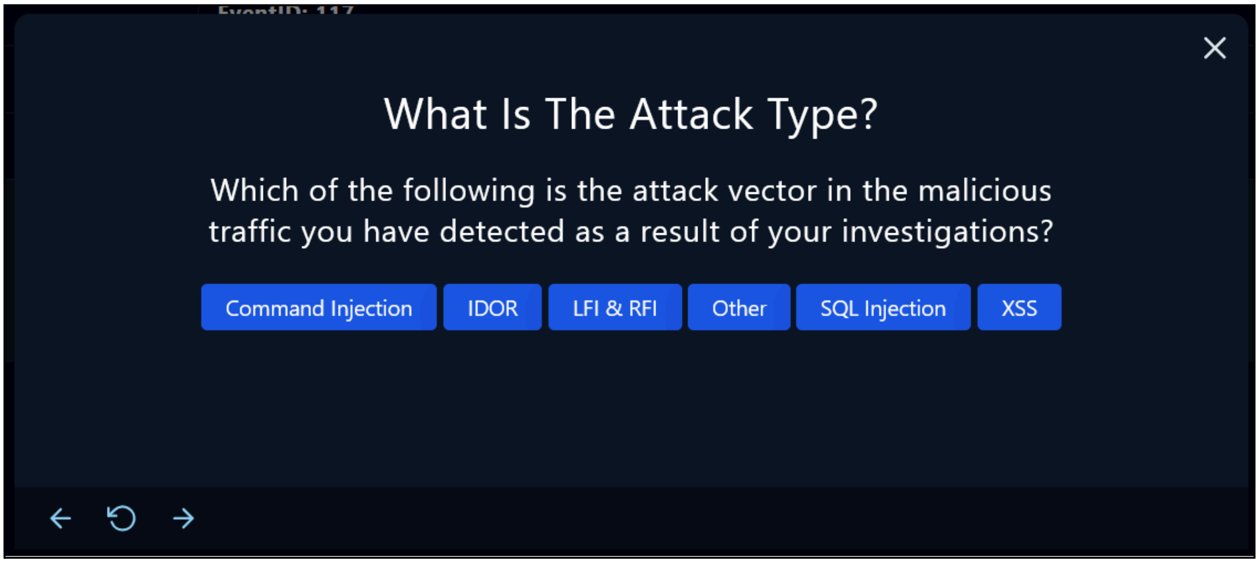
Cookie: Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101 Firefox/126.0

Request: aCSHELL/../../../../../../../../../../etc/shadow

The attacker accessed the host by sending a malicious POST request.

Based on our analysis, we have confirmed that the traffic is **malicious.**

The next playbook step requires us to find the attack type. The analysis confirms that the relevant attack type is both other and LFI & RFI Vulnerability (CVE-2024-24919). The answer for the attack type is both **other** and **LFI & RFI**.

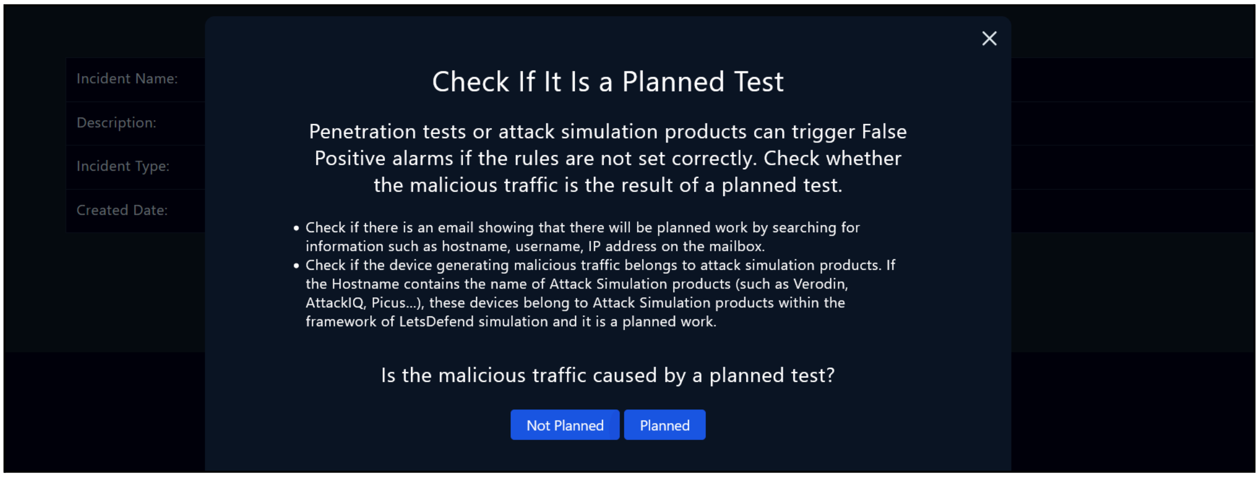


EventID: 117

What Is The Attack Type?

Which of the following is the attack vector in the malicious traffic you have detected as a result of your investigations?

When examining the relevant web traffic, it has been observed that the IP address associated with the attacker is listed as an Indicator of Compromise (IOC) in global resources. Furthermore, no evidence suggesting that the respective attack was conducted for testing purposes has been identified in email records or any other section of the investigation.



Incident Name:

Description:

Incident Type:

Created Date:

Check If It Is a Planned Test

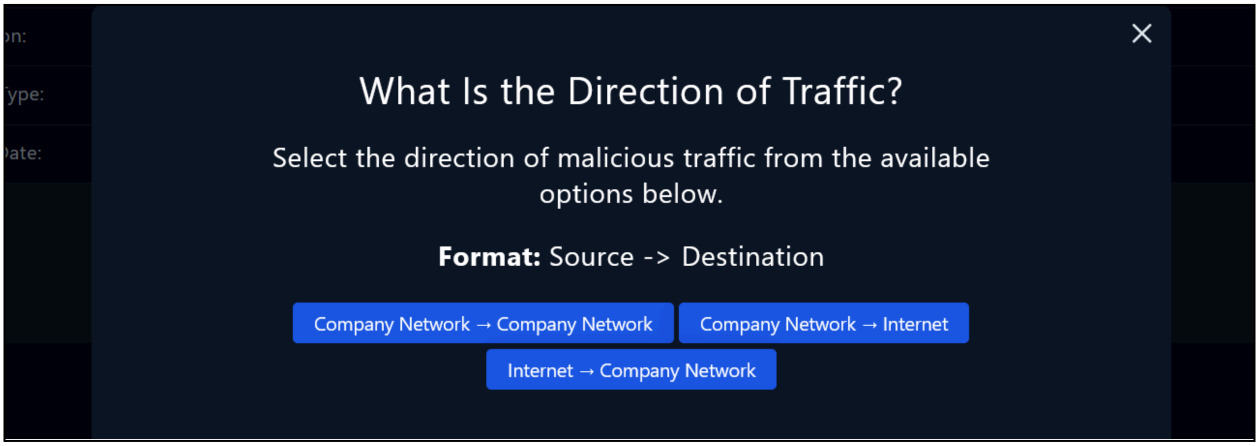
Penetration tests or attack simulation products can trigger False Positive alarms if the rules are not set correctly. Check whether the malicious traffic is the result of a planned test.

- Check if there is an email showing that there will be planned work by searching for information such as hostname, username, IP address on the mailbox.
- Check if the device generating malicious traffic belongs to attack simulation products. If the Hostname contains the name of Attack Simulation products (such as Verodin, AttackIQ, Picus...), these devices belong to Attack Simulation products within the framework of LetsDefend simulation and it is a planned work.

Is the malicious traffic caused by a planned test?

The IP and hostname information of the relevant hostname were searched within the emails received during the specified dates. However, no evidence related to a planned activity has been observed through this investigation.

The answer for this step is “**Not Planned**” The Next step of the playbook involves examining the direction of the traffic.

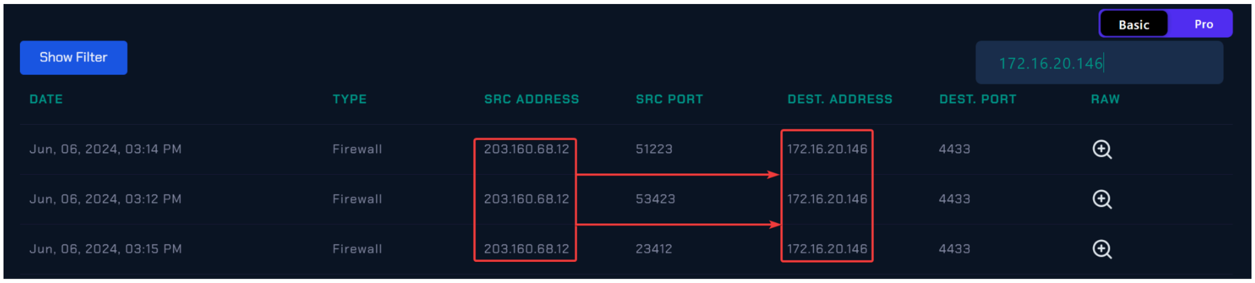

n:
ype:
ate:
Company Network → Company Network
Company Network → Internet
Internet → Company Network

What Is the Direction of Traffic?

Select the direction of malicious traffic from the available options below.

Format: Source -> Destination

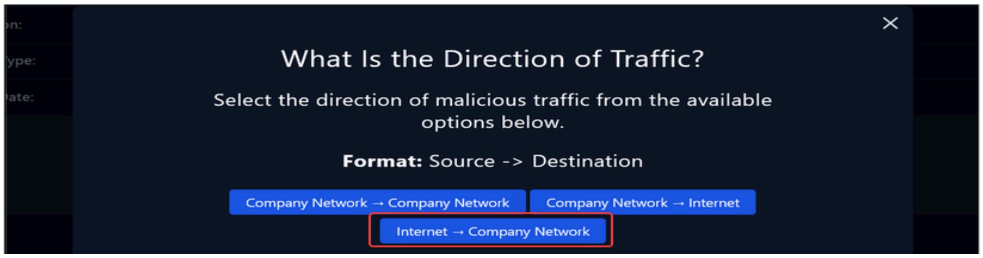
To determine the direction of traffic, we will review the all logs we gathered from our security products on the log management page. The alert creation time will be a key reference for us to investigate the incident.



172.16.20.146

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Jun, 06, 2024, 03:14 PM	Firewall	203.160.68.12	51223	172.16.20.146	4433	🔍
Jun, 06, 2024, 03:12 PM	Firewall	203.160.68.12	53423	172.16.20.146	4433	🔍
Jun, 06, 2024, 03:15 PM	Firewall	203.160.68.12	23412	172.16.20.146	4433	🔍

In the log management page, all of the malicious traffic is from the Internet -> Company Network.


n:
ype:
ate:
Company Network → Company Network
Company Network → Internet
Internet → Company Network

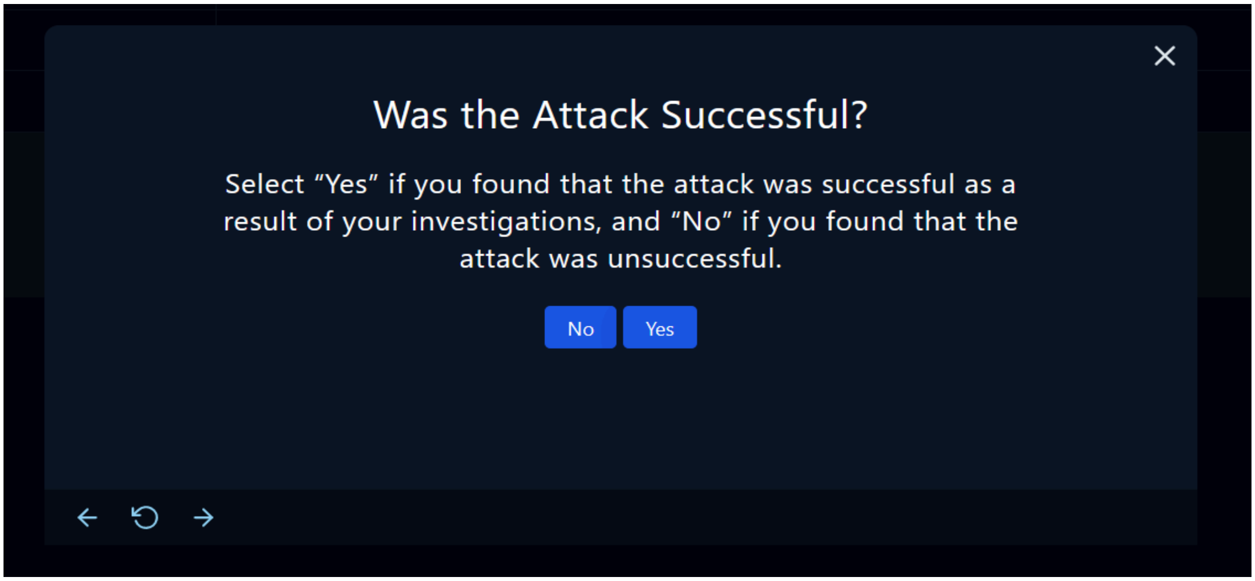
What Is the Direction of Traffic?

Select the direction of malicious traffic from the available options below.

Format: Source -> Destination

The source address is **203.160.68[.]12** and the destination address is **172.16.20.146**. So the answer for this playbook step is **Internet -> Company Network**.

The next step in the playbook is to assess whether the attack was successful. This involves analyzing the impact of the attacker's actions and determining if they were able to achieve their objectives.

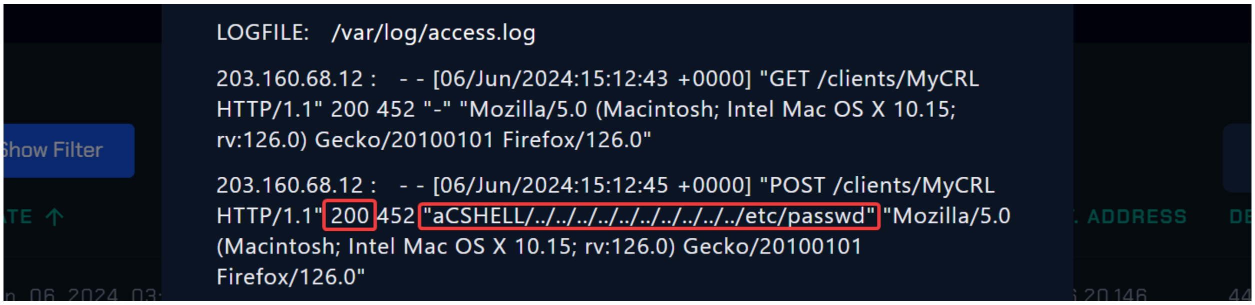


Was the Attack Successful?

Select “Yes” if you found that the attack was successful as a result of your investigations, and “No” if you found that the attack was unsuccessful.

Analyzing the responses enables us to ascertain whether a malicious implant has been detected on the system, thus providing insights into the system's security compromised status.

Let's filter the IP address of the machine (172.16.20.146) that initiated these requests on the log management system.

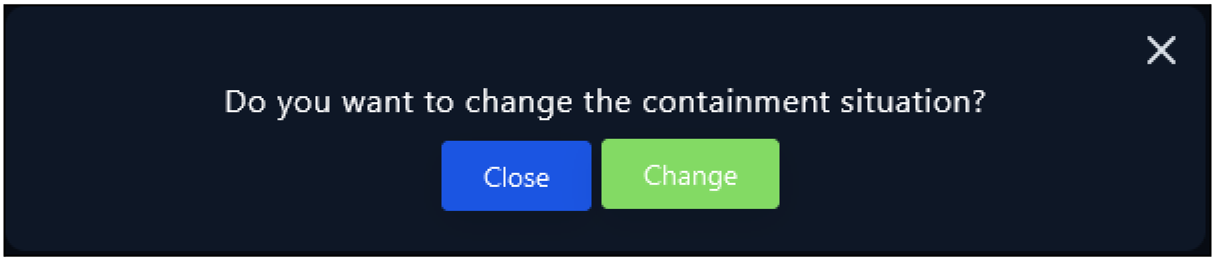


```
LOGFILE:  /var/log/access.log

203.160.68.12 :  - - [06/Jun/2024:15:12:43 +0000] "GET /clients/MyCRL
HTTP/1.1" 200 452 "-" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15;
rv:126.0) Gecko/20100101 Firefox/126.0"

203.160.68.12 :  - - [06/Jun/2024:15:12:45 +0000] "POST /clients/MyCRL
HTTP/1.1" 200 452 "aCSHELL/../../../../../../../../../../etc/passwd" "Mozilla/5.0
(Macintosh; Intel Mac OS X 10.15; rv:126.0) Gecko/20100101
Firefox/126.0"
```

Based on the 200 successfull HTTP response status code in the access log, it appears that the request to **172.16.20.146/clients/MyCRL** which contains malicious payload was successful. Through log analysis, we have confirmed that **the attack was successful**.

Containment

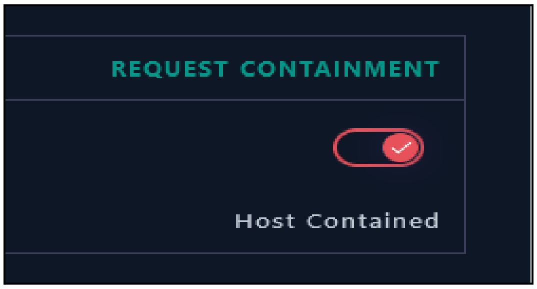
Based on the information gathered during the investigation, it is highly likely that the system has been compromised. To prevent further data loss or unauthorized access, it is recommended to isolate the system from the network immediately.



Do you want to change the containment situation?

Isolation of the host can be made from the endpoint security tab.

Hostname	CP-Spark-Gateway-01
IP Address	172.16.20.146



Host Contained

After the containment, we can close the alert from the investigation channel.

Lesson Learned

- Timely threat intelligence is crucial for identifying and responding to emerging vulnerabilities and exploits.

- Monitoring for specific indicators of compromise (IOCs) helps detect potential security threats, but they should be supplemented with in-depth analysis.

- Effective threat hunting and detailed investigation are essential to understand the scope of an attack and its potential impact on the organization.

- Staying informed about vulnerabilities and applying patches or mitigations is vital for system security.

- Enabling and collecting logs from various operating systems can significantly enhance visibility into your network's security posture.

Remediation Actions

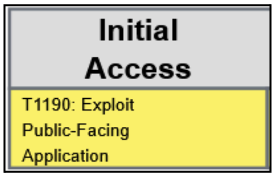
- Apply security patches or updates to address the CVE-2024-24919 vulnerability in the CP-Spark-Gateway-01 to eliminate the attack vector.

- Isolate the compromised machine from the network to prevent the attacker from accessing other resources and systems within the organization.

- If a Security Gateway / Cluster is configured to use an LDAP Account Unit, it is recommended to change the password of the LDAP account.

Appendix

MITRE ATT&CK



Initial Access

T1190: Exploit Public-Facing Application

MITRE Tactics	MITRE Techniques
Initial Access	T1190: Exploit Public-Facing Application

Artifacts

IOC TYPE	VALUE
IPv4	203.160.68[.]12
URI	172.16.20.146/clients/MyCRL
Request	aCSHELL/../../../../../../../../../../etc/passwd