Official Incident Report

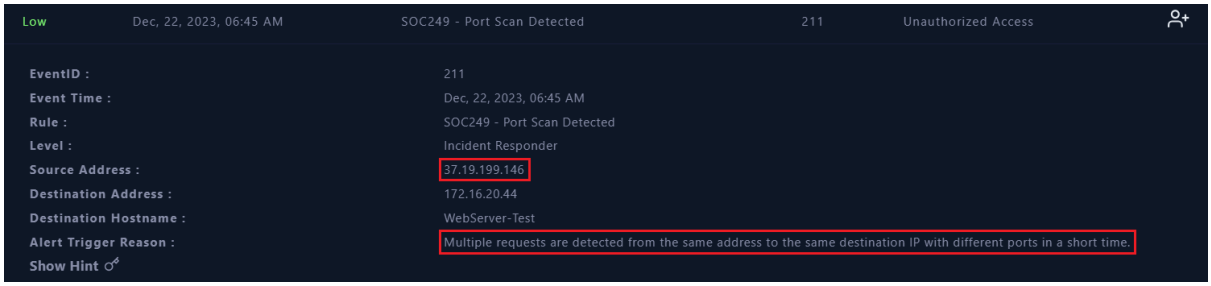
Event ID: 211

Rule Name: SOC249 - Port Scan Detected

Table of contents

Alert

The alert was triggered due to the requests seen from different ports in a short time over the USA located 37[.]19.199.146 IP.



Low	Dec, 22, 2023, 06:45 AM	SOC249 - Port Scan Detected	211	Unauthorized Access

EventID :	211
Event Time :	Dec, 22, 2023, 06:45 AM
Rule :	SOC249 - Port Scan Detected
Level :	Incident Responder
Source Address :	37.19.199.146
Destination Address :	172.16.20.44
Destination Hostname :	WebServer-Test
Alert Trigger Reason :	Multiple requests are detected from the same address to the same destination IP with different ports in a short time.
Show Hint	

First, the alert should be verified by checking the available logs, and then it should be determined whether the attack was successful or not.

Detection

Verify

You can search for Destination IP on Log Management to better understand the alert. As a result, both Firewall, proxy, and DNS logs for different years can be seen. To confirm the alert, examine all requests from the IP 37[.]19.199.146.

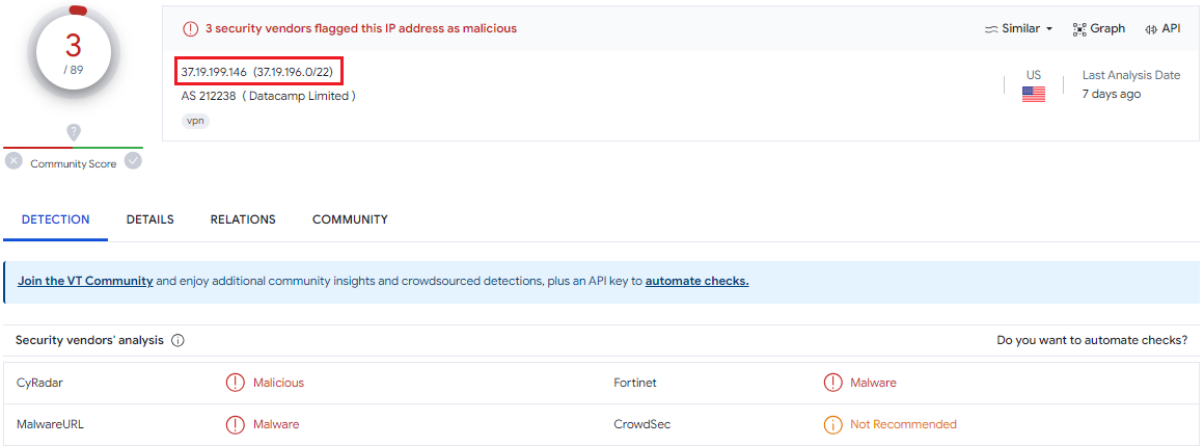
DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Dec, 22, 2023, 06:40 AM	Firewall	37.19.199.146	45012	172.16.20.44	21	
Dec, 22, 2023, 06:41 AM	Firewall	37.19.199.146	21345	172.16.20.44	22	
Dec, 22, 2023, 06:42 AM	Firewall	37.19.199.146	47023	172.16.20.44	23	
Dec, 22, 2023, 06:42 AM	Firewall	37.19.199.146	26435	172.16.20.44	25	
Dec, 22, 2023, 06:43 AM	Firewall	37.19.199.146	27089	172.16.20.44	53	
Dec, 22, 2023, 06:43 AM	Firewall	37.19.199.146	47056	172.16.20.44	80	
Dec, 22, 2023, 06:44 AM	Firewall	37.19.199.146	41078	172.16.20.44	110	
Dec, 22, 2023, 06:44 AM	Firewall	37.19.199.146	38079	172.16.20.44	443	
Dec, 22, 2023, 06:44 AM	Firewall	37.19.199.146	38043	172.16.20.44	8080	
Dec, 22, 2023, 06:44 AM	Firewall	37.19.199.146	29076	172.16.20.44	3389	

In the logs of 37[.]19.199.146 IP, requests to 10 different ports were seen in a short period of 4 minutes. The alert occurred because the requests here exceeded the threshold value in the rule. Thus, it can be said that the alert is True Positive.

Analysis

Reputation Check

It was detected in the first examinations that the IP "37[.]19.199.146" performed the port scan activity. Conduct reputation checks for the relevant IP.



hxxps://www.virustotal.com/gui/ip-address/37.19.199.146

IP Abuse Reports for 37.19.199.146:

This IP address has been reported a total of **23** times from 17 distinct sources. 37.19.199.146 was first reported on April 2nd 2023, and the most recent report was **3 months ago**.

Old Reports: The most recent abuse report for this IP address is from **3 months ago**. It is possible that this IP is no longer involved in abusive activities.

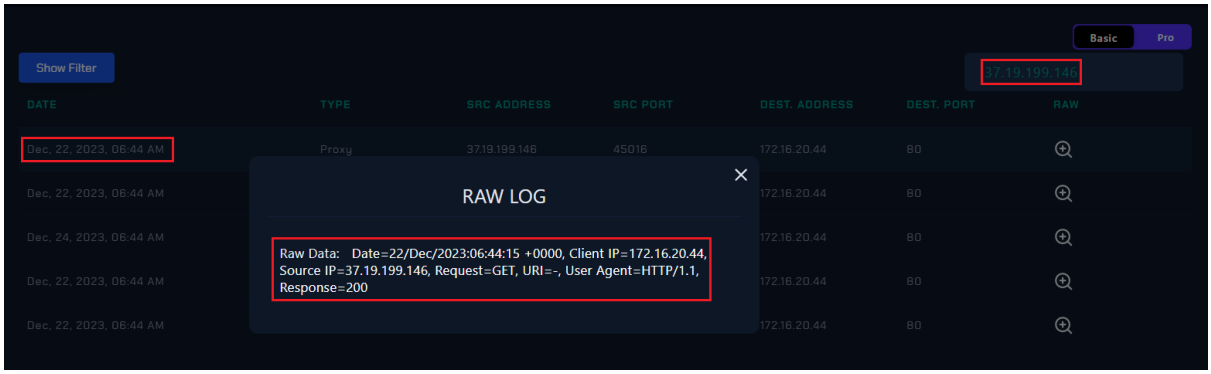
Reporter	IoA Timestamp	Comment	Categories
ThreatBook.io	2023-09-01 22:59:25 (3 months ago)	ThreatBook Intelligence: Zombie,Exploit more details on https://threatbook.io/ip/37.19.199.146 ... show more	Web App Attack
ThreatBook.io	2023-08-28 23:01:09 (3 months ago)	ThreatBook Intelligence: Zombie,Exploit more details on https://threatbook.io/ip/37.19.199.146 ... show more	Web App Attack
Anonymous	2023-06-06 12:39:19 (6 months ago)	Possible intrusion attempt from 37.19.199.146	Brute-Force
formality	2023-05-24 17:50:20 (7 months ago)	Invalid user admin from 37.19.199.146 port 13230	Brute-Force SSH
nicosqc	2023-05-24 17:39:01 (7 months ago)	Invalid user admin from 37.19.199.146 port 30373	Brute-Force SSH
nicosqc	2023-05-24 17:39:01 (7 months ago)	Invalid user admin from 37.19.199.146 port 30373	Brute-Force SSH
nicosqc	2023-05-24 17:39:01 (7 months ago)	Invalid user admin from 37.19.199.146 port 30373	Brute-Force SSH
nicosqc	2023-05-24 17:39:01 (7 months ago)	Invalid user admin from 37.19.199.146 port 30373	Brute-Force SSH
Anonymous	2023-05-24 16:00:01 (7 months ago)	Report: Unauthorised SSH/Telnet login attempt with use r "admin" at 2023-05-24T15:59:50Z	Brute-Force SSH
Lat31320	2023-05-24 13:28:37 (7 months ago)	debx - SSH brute force	Brute-Force SSH
sverre26	2023-05-24 13:21:21	Bruteforce detected by fail2ban	Brute-Force

hxxps://www.abuseipdb.com/check/37.19.199.146

The IP in question was reported as Malicious, Web Attack, and Brute Force in sources such as Virus Total and AbuseIPDB.

You should examine all transactions that the attacker IP performed on the system or on different systems after the port scan operation. For this, search for the relevant IP on Log Management.

The first log of the related IP is seen in the proxy. It is seen in the related log that the request sent to the address hosted at IP 172[.]16.20.44 received 200 (success status response code) on the proxy. This means that the related host is open to remote access.



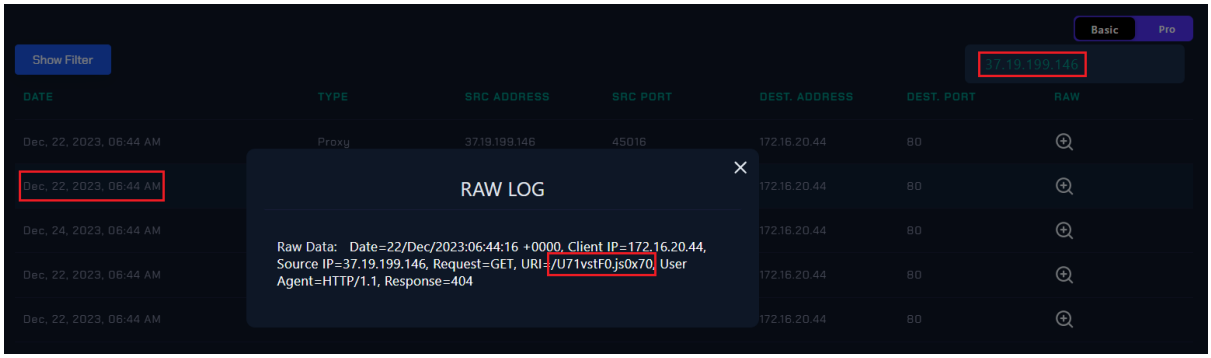
Response Code: **200**

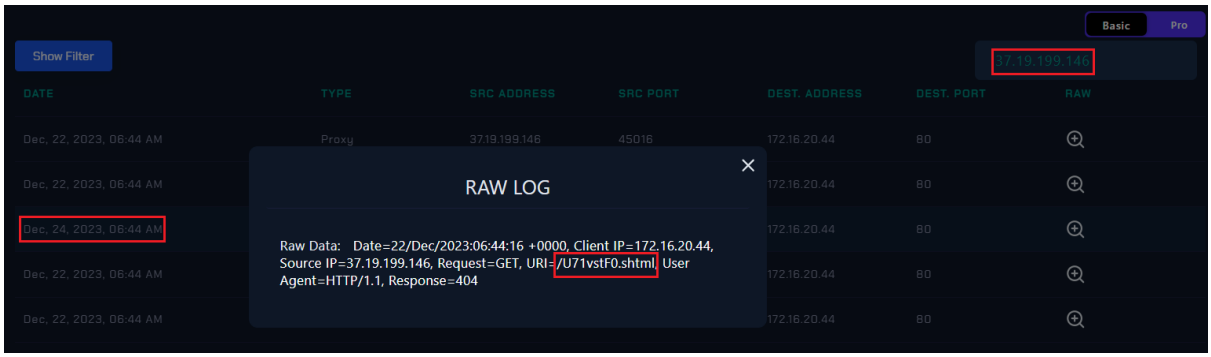
- The resource has been fetched and is transmitted in the message body.

hxxps://developer.mozilla.org/en-US/docs/Web/HTTP/Status/200

The following logs show various requests to different URIs in the proxy. The response code in these requests was 404 (Not Found). This means that there is no such URI belonging to the requested host.

hxxps://developer.mozilla.org/en-US/docs/Web/HTTP/Status/404

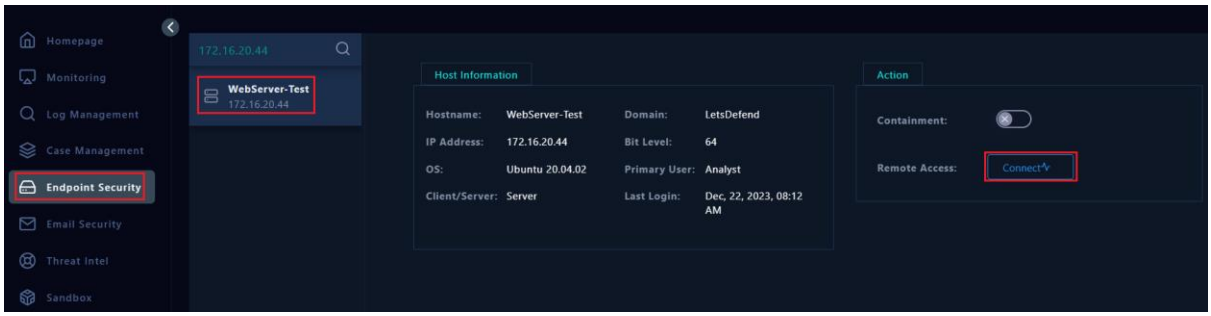




-URI-
/U71vstF0.js0x70
/U71vstF0.shtml
/U71vstF0.00RelNotes
/U71vstF0.bas:ShowVolume

Upon checking the URIs from which the requests were made, it is possible that they are random URIs or scans belonging to attack tools. Therefore, you should connect to the system and examine all requests belonging to the attacker. You should examine in detail which requests of the attacker were successful and which were unsuccessful.

Go to Endpoint Security to connect to the system using the "connect" button as below.



View the apache logs to see the incoming requests after connecting to the system. You should check the /var/log/apache2 file path for this.

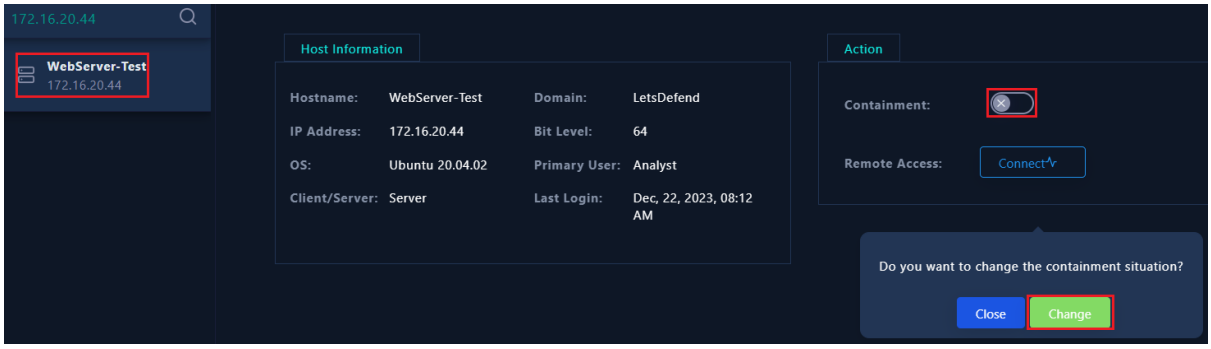
After connecting to the system, all access logs of the attacker IP can be seen as follows.

```
root@ip-172-31-29-181:/var/log/apache2# ls
access.log  access.log.1  error.log  error.log.1  other_vhosts_access.log
root@ip-172-31-29-181:/var/log/apache2# cat access.log.1 | grep "37.19.199.146"
```

There are many logs as a result of the relevant search. It will take a lot of time to examine them one by one. You can search according to response code 200 to lighten the workload. The following command can be used for this.

Command : cat access.log.1 | grep "37.19.199.146" | grep "\s200\s"

The result of the related search again shows a high number of different logs. From this, it can be understood that the attacker succeeded in some attacks on the target system. Therefore, it is recommended to isolate the target system from the network. For this, go to Endpoint security and isolate the system as follows.



The above logs of the attacker were taken to my own system for easier analysis. As shown in the screenshot below, it was seen that the attacker made various web attacks from a specific attack location. They also tried CVE-2014-6271 and CVE-2014-6278 in case the system was vulnerable. Therefore, it can be said that Active Scanning: Vulnerability Scanning technique was used.

```
37.19.199.146 - - [22/Dec/2023:06:46:54 +0000] "GET / HTTP/1.1" 200 1915 "() { _; } >_[$($())] { echo 93e4r0-CVE-2014-6278: true; echo;echo; }" "() { :; }; echo 93e4r0-CVE-2014-6271:
true;echo;echo;"
37.19.199.146 - - [22/Dec/2023:06:46:54 +0000] "GET / HTTP/1.1" 200 1915 "() { _; } >_[$($())] { echo 93e4r0-CVE-2014-6278: true; echo;echo; }" "() { :; }; echo 93e4r0-CVE-2014-6271:
true;echo;echo;"
37.19.199.146 - - [22/Dec/2023:06:46:58 +0000] "GET /index.php HTTP/1.1" 200 1915 "() { _; } >_[$($())] { echo 93e4r0-CVE-2014-6278: true; echo;echo; }" "() { :; }; echo
93e4r0-CVE-2014-6271: true;echo;echo;"
37.19.199.146 - - [22/Dec/2023:06:47:06 +0000] "GET / HTTP/1.1" 200 1915 "() { _; } >_[$($())] { echo 93e4r0-CVE-2014-6278: true; echo;echo; }" "() { :; }; echo 93e4r0-CVE-2014-6271:
```

```
37.19.199.146 - - [22/Dec/2023:06:48:35 +0000] "GET /index.php?download=/windows/win.ini HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:48:35 +0000] "GET /index.php?download=/etc/passwd HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:48:35 +0000] "GET /index.php?|=../../../../../../../../../etc/passwd HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:48:35 +0000] "GET /index.php?page=../../../../../../../../../etc/passwd HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:48:35 +0000] "GET /index.php?page=../../../../../../../../../boot.ini HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:48:36 +0000] "GET /index.php?l=forum/view.php&topic=../../../../../../../../../etc/passwd HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:48:47 +0000] "GET /index.php?module=My_eGallery&do=showpic&pid=-1/**/AND/**/1=2/**/UNION/**/ALL/**/SELECT/**/0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,concat(
0x3C7230783E,pn_uname,0x3a,pn_pass,0x3C7230783E),0,0,0/**/FROM/**/md_users/**/WHERE/**/pn_uid=$id/* HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:48:48 +0000] "GET /index.php?option=search&searchword=<script>alert(document.cookie);</script> HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:48:50 +0000] "GET /index.php?dir=<script>alert('Vulnerable')</script> HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:49:17 +0000] "GET /index.php?top_message=&lt;script&gt;alert(document.cookie)&lt;/script&gt; HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:49:17 +0000] "GET /index.php?file=Liens&op=\\\"><script>alert('Vulnerable');</script> HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:49:17 +0000] "GET /index.php?catid=&lt;script&gt;alert('Vulnerable')&lt;/script&gt; HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:49:17 +0000] "GET /index.php?action=storenew&username=<script>alert('Vulnerable')</script> HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:49:18 +0000] "GET /index.php?action=search&searchFor=\\\"><script>alert('Vulnerable')</script> HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64;
x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:49:18 +0000] "GET /index.php/\\\"><script><script>alert(document.cookie)</script>< HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:49:18 +0000] "GET /index.php/content/search/?SectionID=3&SearchText=<script>alert(document.cookie)</script> HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT
10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:49:19 +0000] "GET /index.php/content/advancedsearch/?SearchText=<script>alert(document.cookie)</script>&PhraseSearchText=<script>alert(
document.cookie)</script>&SearchContentClassID=-1&SearchSectionID=-1&SearchDate=-1&SearchButton=Search HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (
KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:49:27 +0000] "GET /?mod=<script>alert(document.cookie)</script>&op=browse HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:49:33 +0000] "GET /?sql_debug=1 HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:49:37 +0000] "GET /index.php?sql_debug=1 HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/
74.0.3729.169 Safari/537.36"
37.19.199.146 - - [22/Dec/2023:06:50:00 +0000] "GET /// HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/
537.36"
37.19.199.146 - - [22/Dec/2023:06:50:03 +0000] "GET /index.php?rep=<script>alert(document.cookie)</script> HTTP/1.1" 200 1914 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/
537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"
```

When the logs are analyzed, it is seen that the attacker tried to access "/etc/passwd" address with different requests. The purpose of the request that appears in this log entry is a “Directory Traversal” attack. The attacker tried to access a specific file via URL. The “topic=../../../../../../../../../../etc/passwd” section in the request indicates that the attacker attempted to access the “/etc/passwd” file.

37[.]19.199.146 - - [22/Dec/2023:06:48:36 +0000] "GET /index.php?l=forum/view.php&topic=../../../../../../../../../etc/passwd HTTP/1.1" 200

1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"

This attack is an example of a SQL injection attack. It is understood that the attacker tried to add another query to the result of the original query as the `-1 AND 1=2` condition was achieved by using a SQL UNION query. This added query is intended to extract the `pn_uname` and `pn_pass` fields from the `md_users` table. If it succeeds, the attacker can obtain the usernames and passwords on the target system.

*37[.]19.199.146 - - [22/Dec/2023:06:48:47 +0000] "GET /index.php?module=My_eGallery&do=showpic&pid=-1/**/AND/**/1=2/**/UNION/**/ALL/**/SELECT/**/0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,concat(0x3C7230783E,pn_uname,0x3a,pn_pass,0x3C7230783E),0,0,0/**/FROM/**/md_users/**/WHERE/**/pn_uid=$id/* HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"*

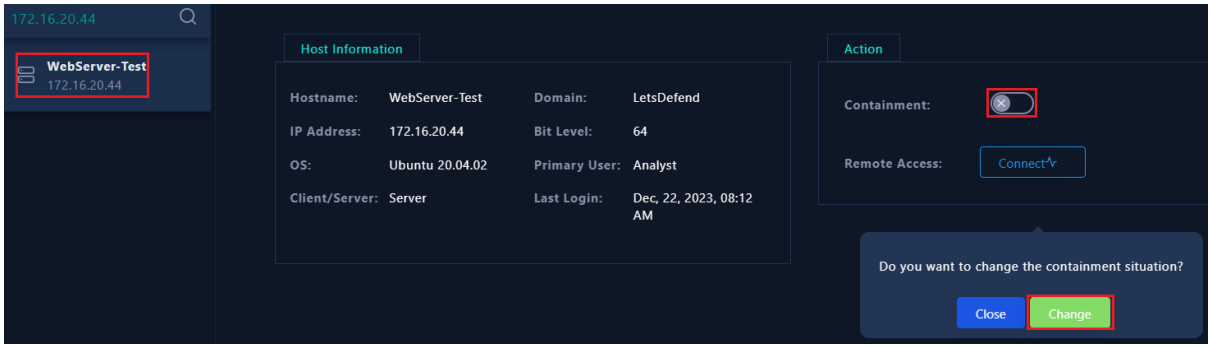
The following log is an example of a Cross-Site Scripting (XSS) attack. The attacker tried to send a GET request to the web application with a parameter containing a text in the following form <script>alert('Vulnerable')</script>.
37[.]19.199.146 - - [22/Dec/2023:06:48:50 +0000] "GET /index.php?dir=<script>alert('Vulnerable')</script> HTTP/1.1" 200 1915 "-" "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/74.0.3729.169 Safari/537.36"

You should also review all the authentication processes on the system at the end of the investigations. Check the /var/log/auth.log file for the relevant checks. It should be checked in three different ways as follows because the attacker may appear with a different IP or there may be a Brute Force attempt. At the end of all these, there was no log showing that the system was accessed by the attacker.

```
root@ip-172-31-29-181:/var/log# ls
Xorg.0.log              apport.log.2.gz  cloud-init-output.log  dpkg.log.2.gz    kern.log           syslog
Xorg.0.log.old          apport.log.3.gz  cloud-init.log         dpkg.log.3.gz    kern.log.1         syslog.1
alternatives.log        apport.log.4.gz  cups                   dpkg.log.4.gz    kern.log.2.gz      syslog.3.gz
alternatives.log.1      apport.log.5.gz  dist-upgrade           dpkg.log.5.gz    kern.log.3.gz      syslog.4.gz
alternatives.log.2.gz   apport.log.6.gz  dmesg                  dpkg.log.6.gz    kern.log.4.gz      syslog.5.gz
alternatives.log.3.gz   apt              dmesg.0                dpkg.log.7.gz    landscape          syslog.6.gz
alternatives.log.4.gz   auth.log         dmesg.1.gz             dpkg.log.8.gz    lastlog            syslog.7.gz
alternatives.log.5.gz   auth.log.2.gz    dmesg.2.gz             fontconfig.log   lightdm            ubuntu-advantage.log
amazon                  auth.log.3.gz    dmesg.3.gz             gdm3             nginx              ubuntu-advantage.log.1
apache2                 auth.log.4.gz    dmesg.4.gz             gpu-manager.log  openvpn            ubuntu-advantage.log.2.gz
apport.log              btmp             dpkg.log               hp               private            unattended-upgrades
apport.log.1            btmp.1           dpkg.log.1             journal          speech-dispatcher  wtmp
root@ip-172-31-29-181:/var/log# cat auth.log | grep "37.19.199.146"
root@ip-172-31-29-181:/var/log# cat auth.log | grep "fail"
root@ip-172-31-29-181:/var/log# cat auth.log | grep "succes"
root@ip-172-31-29-181:/var/log#
```

Containment

It is understood from the logs on the system that the attacker tried many web attacks on the target system, especially SQL injection, XSS and Directory Traversal. Most of these requests received 200 as response code on the target system. It can be said that the target system is a compromised host. Therefore, it is recommended to isolate the system from the network. For the relevant process, go to Endpoint Security and isolate the system as below.



Lesson Learned

- Hosts should not be opened to remote access or unauthorized users unless necessary, even in test environments.
- If there are authentication structures on remote hosts, measures should be taken against Brute Force attacks in the system. For instance, MFA or recaptcha structure should be activated.
- In order not to be affected by vulnerabilities, structures open to remote access must be Up-to-Date.
- In structures open to remote access, various security products should be used to detect web attacks and protect the system against them, and their signatures/rules must be up to date.

Appendix

MITRE

MITRE Tactics	MITRE Techniques
Reconnaissance	• Active Scanning: Vulnerability Scanning
Initial Access	• Exploit Public-Facing Application
Credential Access	• Unsecured Credentials: Credentials In Files

Artifacts

Field	Value
IPs	• 172.16.20.44 • 37[.]19.199.146
Host	• WebServer-Test