Official Incident Report

Event ID: 208

Rule Name: SOC246 - Forced Authentication Detected

Table of contents

Alert

The alert was triggered due to too many POST requests to the host “test-frontend.letsdefend.io” over the same IP in a short time. It was seen that the related alert hit the “SOC246 - Forced Authentication Detected” rule.

EventID :	208
Event Time :	Dec, 12, 2023, 02:15 PM
Rule :	SOC246 - Forced Authentication Detected
Level :	Security Analyst
Source IP :	120.48.36.175
Destination IP :	104.26.15.61
Host :	WebServer_Test
Request URL :	http://test-frontend.letsdefend.io/accounts/login
Request Method :	POST
Device Action :	Permitted
Alert Trigger Reason :	Multiple POST requests were soon seen from the same IP to the fixed URI "/accounts/login".
Show Hint	

First, the alert should be verified by checking the available logs, then the source of this traffic should be investigated and it should be confirmed whether it is legitimate or not.

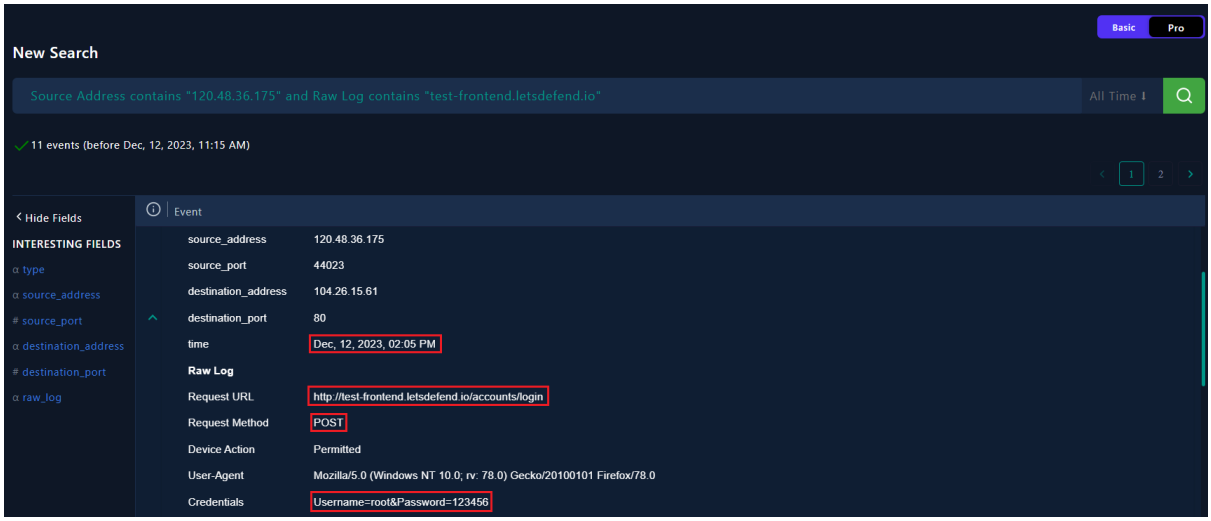
Detection

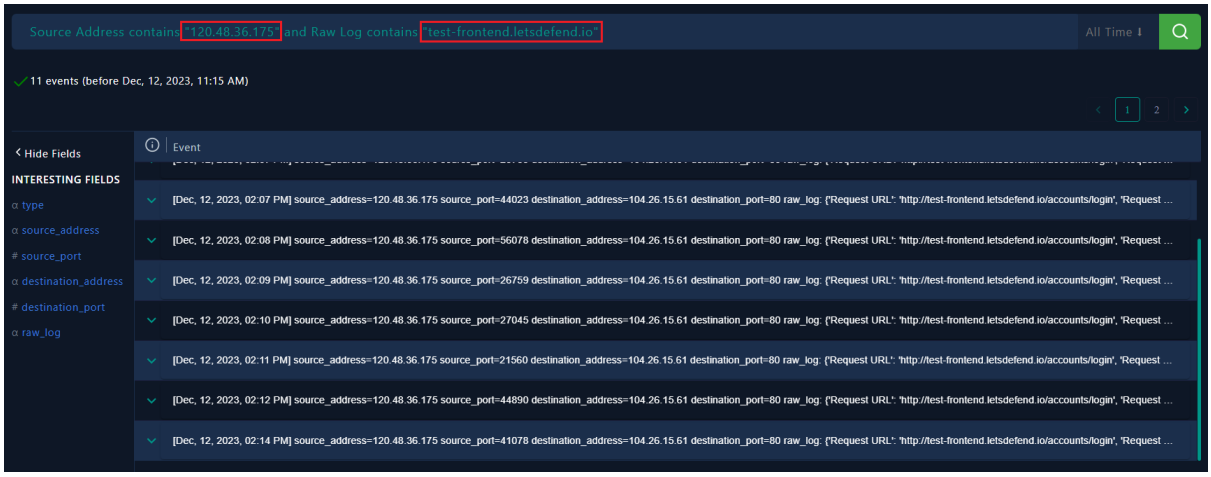
Verify

In Log Management, search for the source IP address (120[.]48.36.175) in the alert and examine the logs among the results. Thus, both Firewall, OS, and Proxy logs of the relevant IP are seen.

Since the alert was triggered by a repetitive behavior, you should examine all requests from the IP "120[.]48.36.175" to the host "test-frontend.letsdefend.io". Perform a search on Log Management to confirm the related logs.

As can be seen below, the relevant search result shows that the POST requests started at 02:05 PM and ended at 02:14 PM.



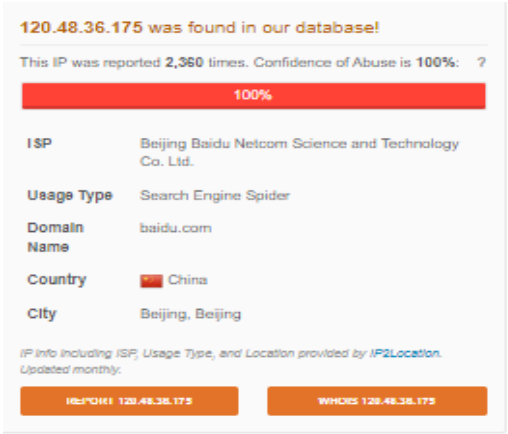


According to the logs in the screenshots above, it has been confirmed that the related alert is True Positive.

Analysis

Reputation Check

The IP “120[.]48.36.175” that sends post requests should be checked for reputability. As can be seen below, the relevant IP is located in China and has been reported in categories such as Malicious, Brute Force, and Phishing.



120.48.36.175 was found in our database!

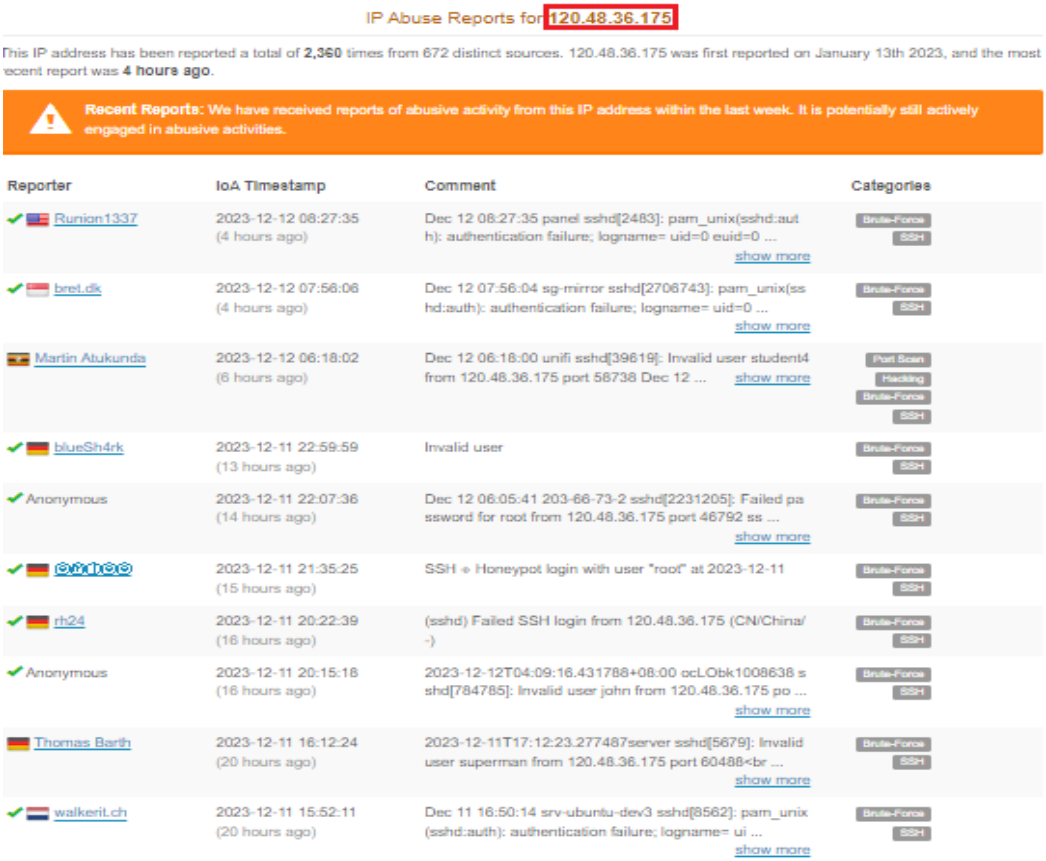
This IP was reported **2,360** times. Confidence of Abuse is **100%**: ?

100%

ISP	Beijing Baidu Netcom Science and Technology Co. Ltd.
Usage Type	Search Engine Spider
Domain Name	baidu.com
Country	China
City	Beijing, Beijing

IP Info including ISP, Usage Type, and Location provided by IP2Location. Updated monthly.

REPORT 120.48.36.175 | WHOIS 120.48.36.175



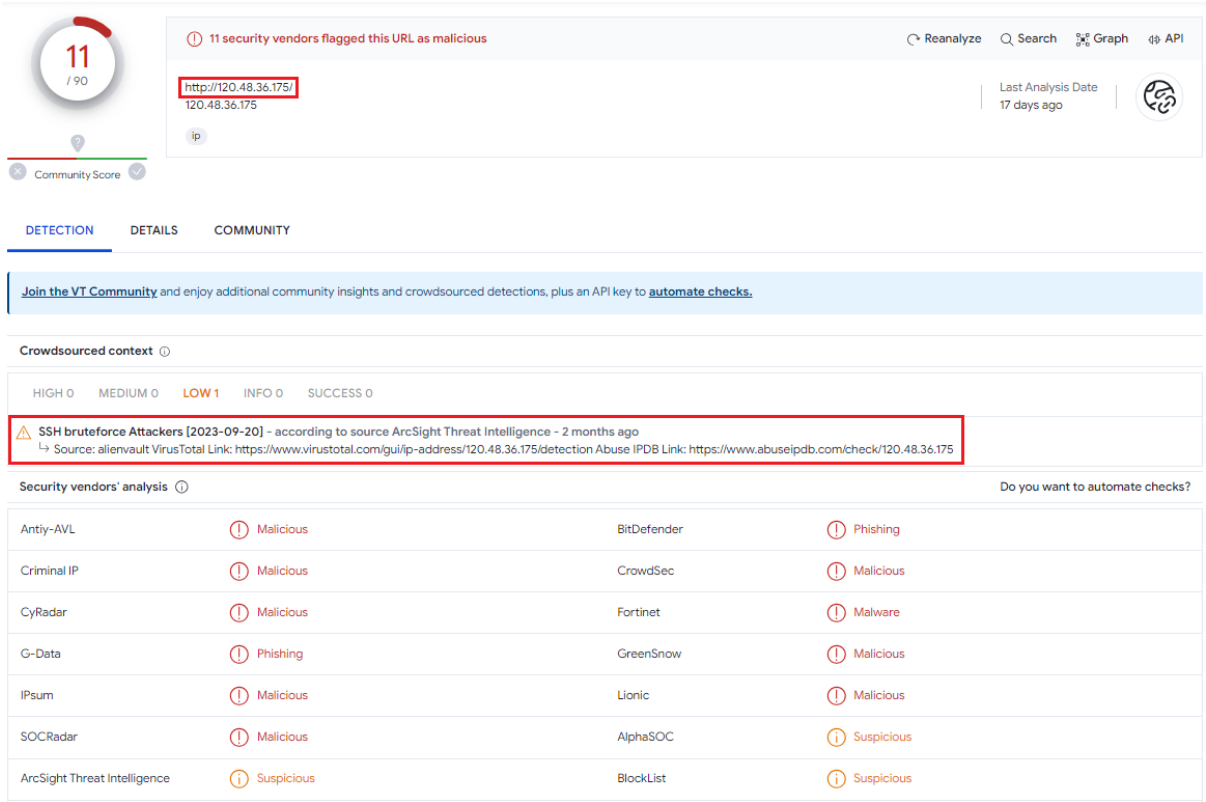
IP Abuse Reports for 120.48.36.175

This IP address has been reported a total of **2,360** times from 672 distinct sources. 120.48.36.175 was first reported on January 13th 2023, and the most recent report was **4 hours 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	Comment	Categories
Runion1337	2023-12-12 08:27:35 (4 hours ago)	Dec 12 08:27:35 panel sshd[2483]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 ... show more	Brute-Force, SSH
bret.dk	2023-12-12 07:56:06 (4 hours ago)	Dec 12 07:56:04 sg-mirror sshd[2706743]: pam_unix(sshd:auth): authentication failure; logname= uid=0 ... show more	Brute-Force, SSH
Martin Atukunda	2023-12-12 06:18:02 (6 hours ago)	Dec 12 06:18:00 unifi sshd[39619]: Invalid user student4 from 120.48.36.175 port 58738 Dec 12 ... show more	Port Scan, Hacking, Brute-Force, SSH
blueSh4rk	2023-12-11 22:59:59 (13 hours ago)	Invalid user	Brute-Force, SSH
Anonymous	2023-12-11 22:07:36 (14 hours ago)	Dec 12 06:05:41 203-66-73-2 sshd[2231205]: Failed password for root from 120.48.36.175 port 46792 ss ... show more	Brute-Force, SSH
[illegible]	2023-12-11 21:35:25 (15 hours ago)	SSH + Honeypot login with user "root" at 2023-12-11	Brute-Force, SSH
rh24	2023-12-11 20:22:39 (16 hours ago)	(sshd) Failed SSH login from 120.48.36.175 (CN/China/-)	Brute-Force, SSH
Anonymous	2023-12-11 20:15:18 (16 hours ago)	2023-12-12T04:09:16.431788+08:00 ocLObk1008638 sshd[784785]: Invalid user john from 120.48.36.175 po ... show more	Brute-Force, SSH
Thomas Barth	2023-12-11 16:12:24 (20 hours ago)	2023-12-11T17:12:23.277487server sshd[5679]: Invalid user superman from 120.48.36.175 port 60488<br ... show more	Brute-Force, SSH
walkerit.ch	2023-12-11 15:52:11 (20 hours ago)	Dec 11 16:50:14 srv-ubuntu-dev3 sshd[8562]: pam_unix(sshd:auth): authentication failure; logname= ui ... show more	Brute-Force, SSH

hxxps://www.abuseipdb.com/check/120.48.36.175

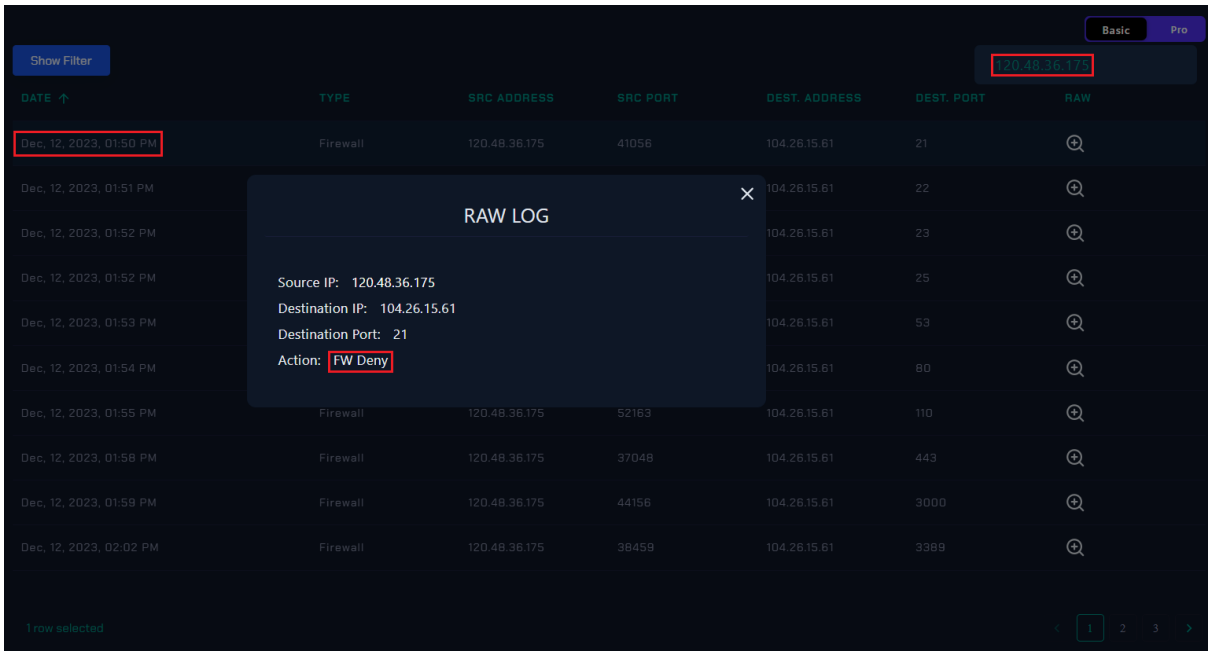


hxxps://www.virustotal.com/gui/url/1328ffa43058b82b82d01e59d3f3fba1760b180289b7501e3ba9c63c1d90a3ee

You should look at all traffic belonging to the attacker IP after performing the reputation check. If there are any logs of the attacker IP before the alert, they can be checked. The relevant search result shows the logs on the Firewall.

DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Dec, 12, 2023, 01:50 PM	Firewall	120.48.36.175	41056	104.26.15.61	21	
Dec, 12, 2023, 01:52 PM	Firewall	120.48.36.175	29078	104.26.15.61	23	
Dec, 12, 2023, 01:52 PM	Firewall	120.48.36.175	27089	104.26.15.61	25	
Dec, 12, 2023, 01:53 PM	Firewall	120.48.36.175	54012	104.26.15.61	53	
Dec, 12, 2023, 01:51 PM	Firewall	120.48.36.175	15026	104.26.15.61	22	
Dec, 12, 2023, 01:54 PM	Firewall	120.48.36.175	29078	104.26.15.61	80	
Dec, 12, 2023, 01:55 PM	Firewall	120.48.36.175	52163	104.26.15.61	110	
Dec, 12, 2023, 01:58 PM	Firewall	120.48.36.175	37048	104.26.15.61	443	
Dec, 12, 2023, 01:59 PM	Firewall	120.48.36.175	44156	104.26.15.61	3000	
Dec, 12, 2023, 02:02 PM	Firewall	120.48.36.175	38459	104.26.15.61	3389	

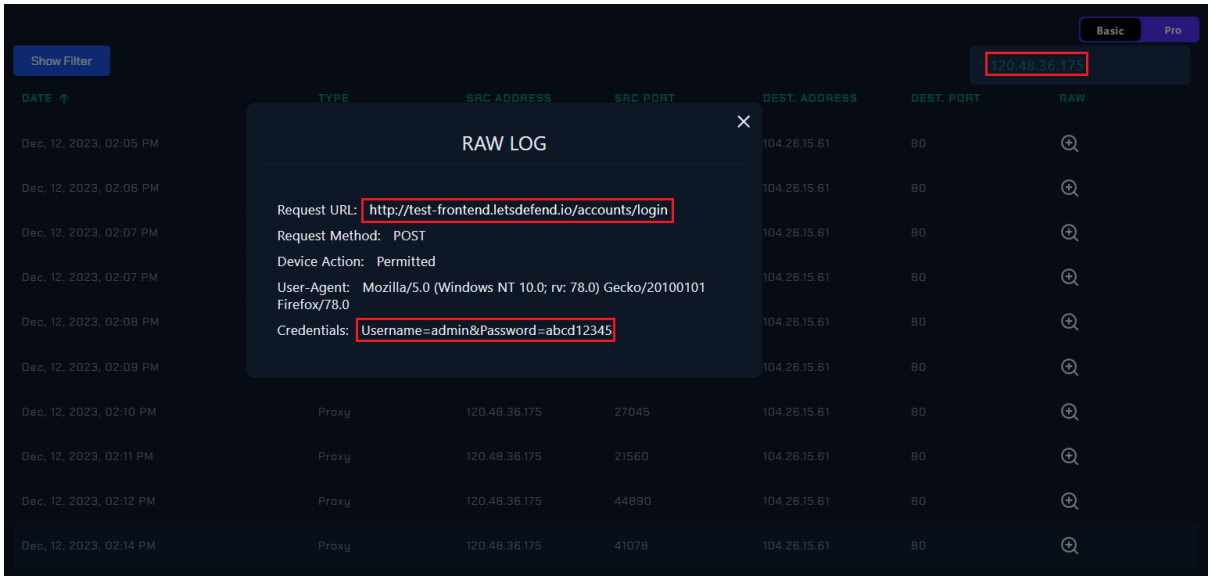
It is understood from the logs above that the attacker performed a port scan on the target system before attacking the system. Here, examine the details of the logs to better understand the port scan.



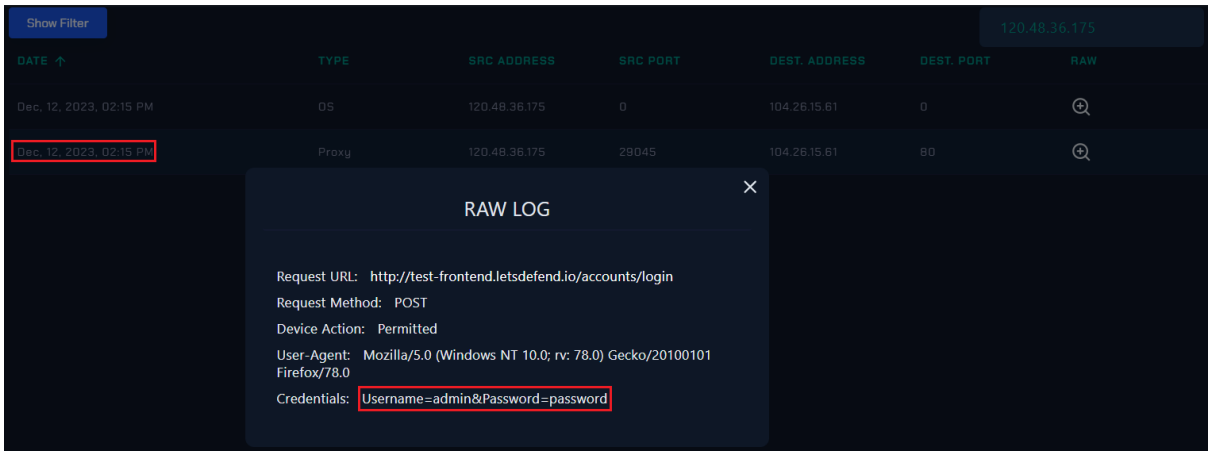
It was seen in the details of the firewall logs that it received "Firewall Deny" except for ports 80 and 3000. It can be said that “Active Scanning: Scanning IP Blocks” was used as the Mitre technique for this situation.

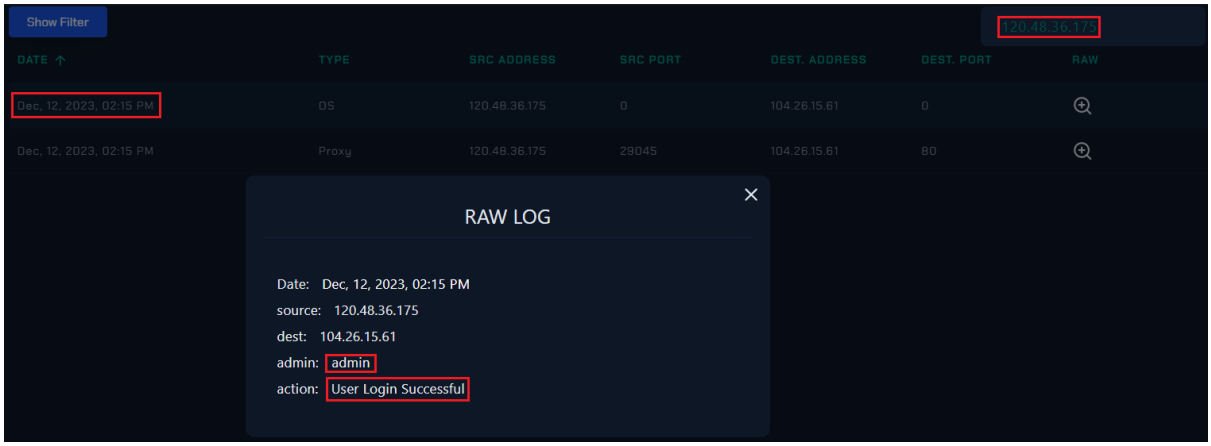
In the following examinations, you should examine the actions of the attacker after the port scan activity. To do this, you should analyze the logs of the attacker IP on Log Management according to time.

In the following logs of the attacker IP, there are many proxy logs. The common point in the proxy logs is that the attacker made all requests to the “hxxp://test-frontend.letsdefend.io/accounts/login” address. Another point to note is that the attacker entered “username” and “password”. However, the “username” and “password” in these logs are constantly changing. This type of attack can be called a dictionary attack. Since there would not be other attempts if the attacker had obtained a successful username and password in the first attempts, you should examine the last log. You should determine whether the attack was successful or the attacker terminated the attack.



When the last proxy log was checked by time, an OS log was also seen in the same minute.





As can be seen above, the last request was successful with the “admin” user. In other words, the attacker successfully accessed the target server with “username=admin” and “password=password”.

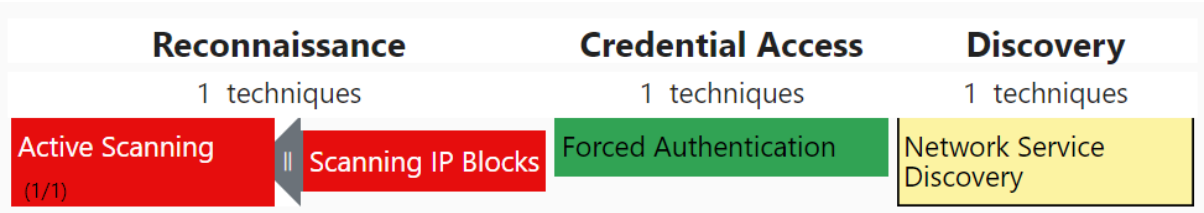
To summarize the alert, it was detected that the attacker attempted a dictionary attack towards the target host. Here, both the users and passwords used by the attacker can be called "most common usernames and passwords". It is another problem in the system that the attacker was successful with these users and passwords. The weak credentials of the host, when exposed to the remote structure, are among the shortcomings of the system. Another point is that there is no MFA in the structure.

Lesson Learned

- Hosts should not be opened to remote or unauthorized users unless necessary, even in test environments.
- Precautions should be taken against brute force attacks if there are authentication structures on remote hosts. For instance, MFA or recaptcha structure should be activated.
- Password policy should be applied for users in structures against attacks such as brute force or forced authentication.
- Lock policy should be applied in structures against attacks such as brute force or forced authentication.

Appendix

MITRE



MITRE Tactics	MITRE Techniques
Reconnaissance	• Active Scanning: Scanning IP Blocks
Credential Access	• Forced Authentication
Persistence	• Scheduled Task/Job
Discovery	• INetwork Service Discovery

Artifacts

Field	Value
IPs	• 120[.]48.36.175
User	• admin
URL	• hxxp://test-frontend.letsdefend.io/accounts/login