Official Incident Report

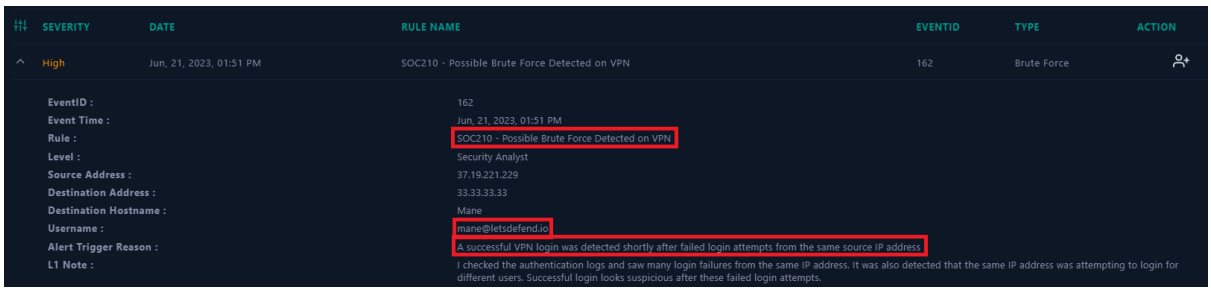
Event ID: 162

Rule Name: SOC210 - Possible Brute Force Detected on VPN

Table of contents

Alert

The alert was triggered due to a successful login from the same source IP address in a short period of time after failed login activities. When the L1 Analyst's note was analyzed, it was determined that there were attempts with different usernames from the same Source IP (37[.]19.221.229) and that it was successful with the user named Mane.



SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
High	Jun, 21, 2023, 01:51 PM	SOC210 - Possible Brute Force Detected on VPN	162	Brute Force	

EventID :	162
Event Time :	Jun, 21, 2023, 01:51 PM
Rule :	SOC210 - Possible Brute Force Detected on VPN
Level :	Security Analyst
Source Address :	37.19.221.229
Destination Address :	33.33.33.33
Destination Hostname :	Mane
Username :	mane@letsdefend.io
Alert Trigger Reason :	A successful VPN login was detected shortly after failed login attempts from the same source IP address
L1 Note :	I checked the authentication logs and saw many login failures from the same IP address. It was also detected that the same IP address was attempting to login for different users. Successful login looks suspicious after these failed login attempts.

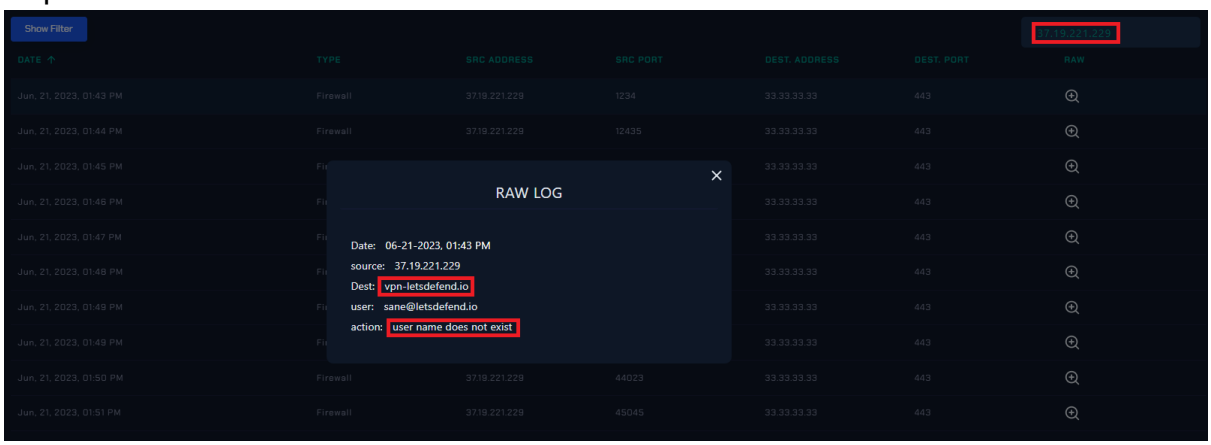
First, the alert should be verified by checking the available logs, and then it should be determined whether the attack was successful or not.

Detection

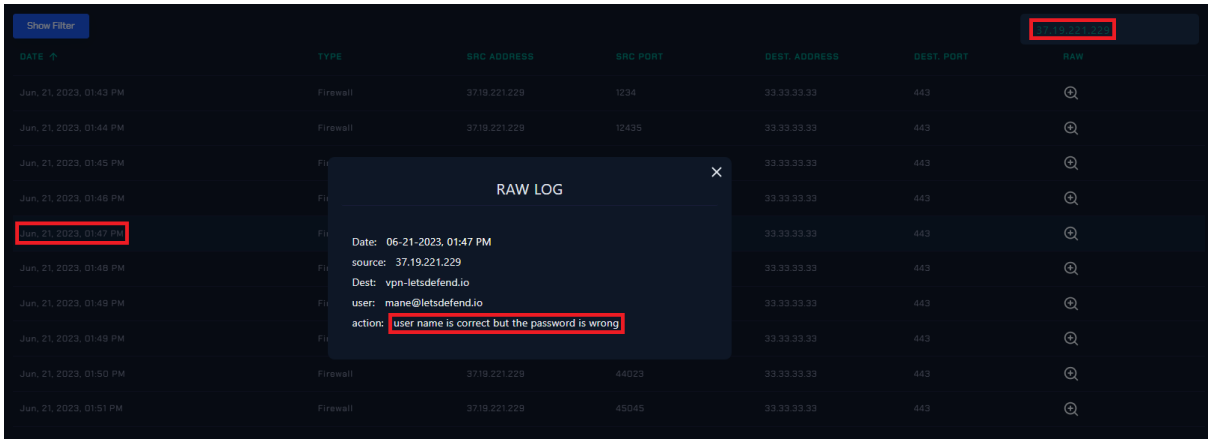
Verify

In Log Management, search for the source IP address (37[.]19.221.229) in the alert and examine the logs among the results. This way, all logs belonging to the attacker IP are seen. As a result, Firewall logs were seen.

When the traffic from 37[.]19.221.229 IP located in the USA was examined in detail, it was seen that "sane@letsdefend.io", "zane@letsdefend.io", "fane@letsdefend.io" and "tane@letsdefend.io" were used in incoming requests. It was seen that FW "user name does not exist" response was returned in these requests.



The request from the same IP at 01:47 PM returned the response "user name is correct but the password is wrong". With this information, the attacker has obtained that there is a user named "mane[@]letsdefend[.]io" in the "vpn-letsdefend.io" structure. Therefore, they will continue with different passwords over the username "mane[@]letsdefend[.]io" in their next requests.



The requests received with the username "mane[@]letsdefend[.]io" show that at 01:51 PM, the attacker received "Login Successful" action in FW. Thus, the alert can be called True Positive.

Analysis

IP Reputation

The attacker IP address is an external IP address. Therefore, the validity of the analysis can be strengthened by performing a reputation check.

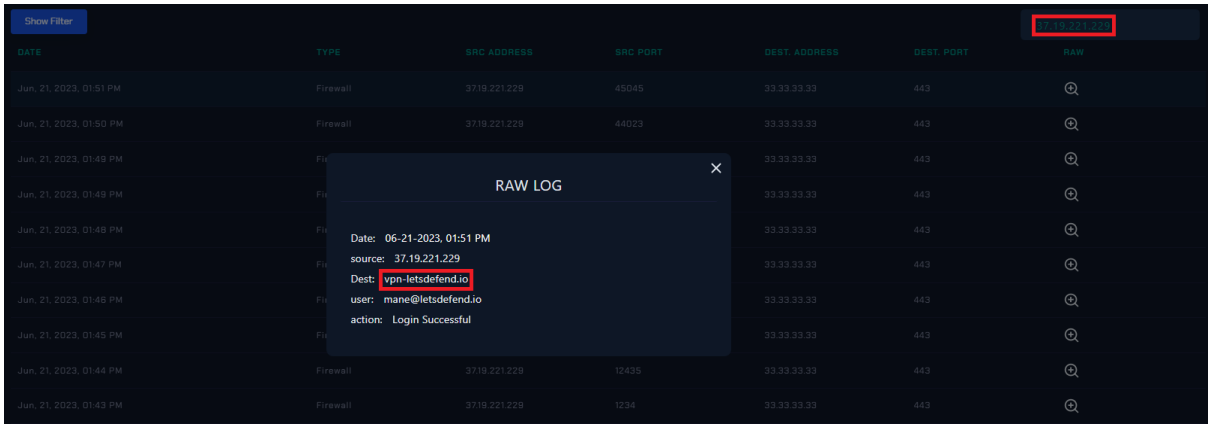
hxxps://www.virustotal.com/gui/ip-address/37.19.221.229

hxxps://www.abuseipdb.com/check/37.19.221.229

The query on Virus Total showed that the IP has been reported as both Suspicious and Malware by two different sources in the past. According to AbuseIPDB, it has a 20% risk record. It was reported by different sources in categories such as E-mail spam, phishing, and Brute Force.

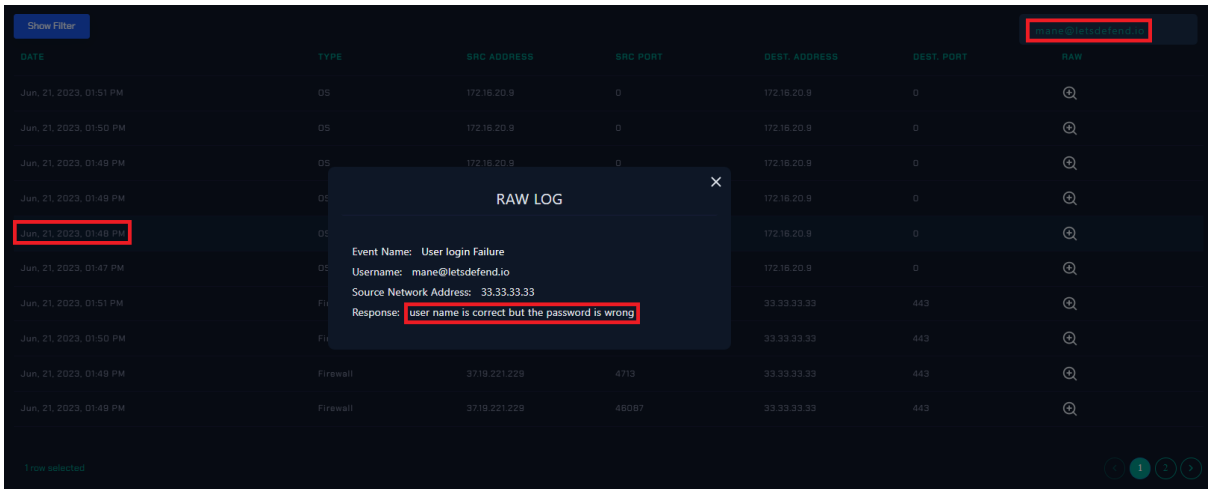
Initial Access

When the logs of the attacker IP 37[.]19.221.229 were analyzed in Log Management, requests to the address "vpn-letsdefend.io" were seen. The system was logged in to the relevant address with Brute Force with multiple users. Thus, it can be said that "External Remote Services(T1133)" technique was used for initial access.

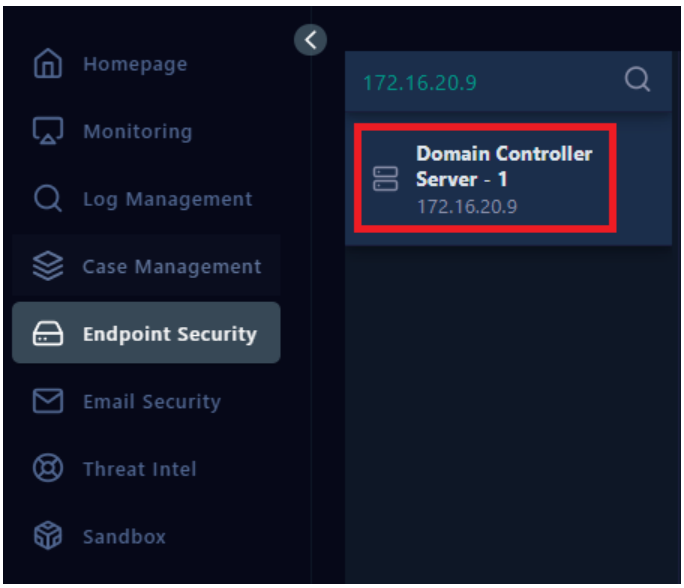


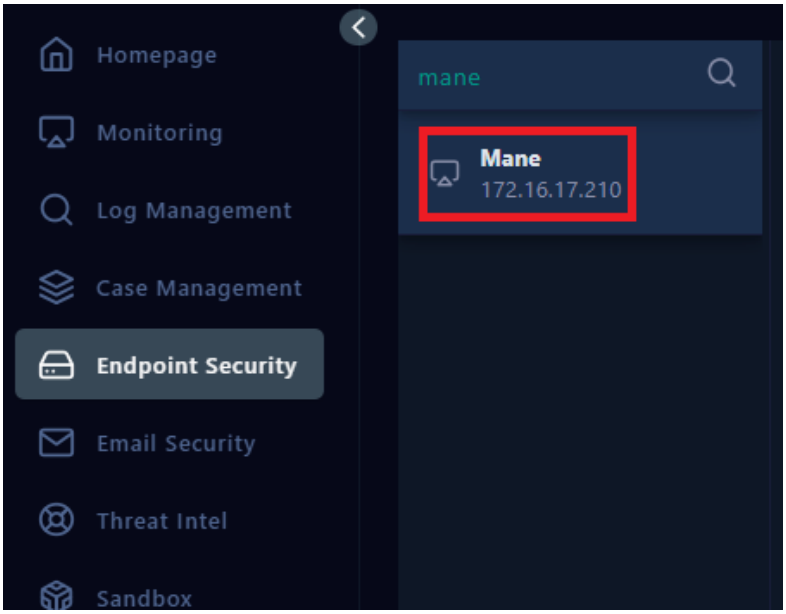
The analysis so far has been made on the IP belonging to the attacker. If you search victim(mane[@]letsdefend[.]io) on Log Management, you can see OS logs as well as FW logs.

You should examine the OS logs in detail to deepen the analysis. The source IP appears as 172[.]16.20.9 in OS logs. You can search on Endpoint Security to get information about the related IP.

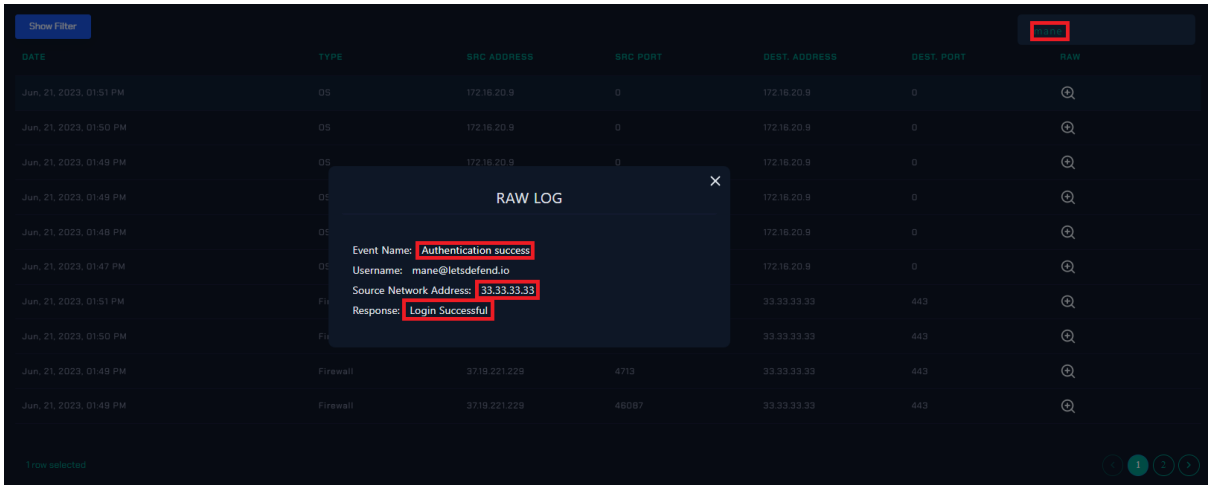


As a result of the search, it was seen that the relevant IP belongs to the Domain Controller. So what is the IP information of the user named "mane[@]letsdefend[.]io"? For this, you can make a search on Endpoint Security. As a result of the search, it was seen that the IP information of the relevant User was 172[.]16.17.210.





Upon further examination on Log Management, it was seen that the OS logs belong to the Domain Controller. As seen in the screenshot below, the Source Network Address information can be used to determine from which address this request was made to the Domain Controller. Previously, it was observed in the firewall logs that the IP address 33[.]33.33.33 belonged to vpn.letsdefend.io.



The above log shows that the Domain Controller received a successful response for the login request for mane[@]letsdefend[.]io via VPN. This proved that the attacker successfully VPN logged into the system via mane[@]letsdefend[.]io. So why was a second check done here? The reason for this is to check whether there is MFA (Multi-factor authentication) in the structure.

#Multi-factor authentication (MFA), also known as two-factor authentication (2FA) or strong authentication, is a security mechanism that requires users to provide multiple forms of identification or credentials to verify their identity when

accessing a system, service, or application. It adds an extra layer of protection beyond just using a username and password combination.

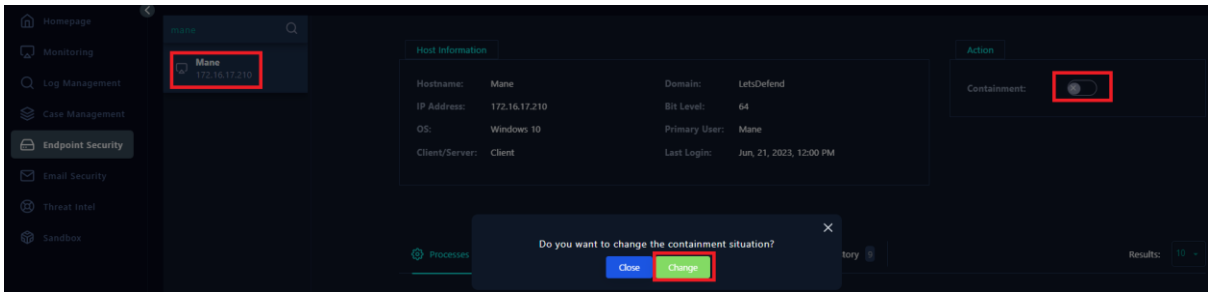
If there was MFA in the structure, even if the attacker managed to pass the password of mane[@]letsdefend[.]io with a brute force attack, they would not be able to access the system because there would need to be a second authentication. Since the second authentication here would be transmitted to the user by OTP (one-time passwords) via message/email, the attacker would not be able to access the system because they would not be able to enter this password. Of course, this applies to the case where the information of the structure in the second verification method does not fall into the hands of the attacker.

It was observed that the attacker received a "user name does not exist" response for users with which they tried to log in before the mane[@]letsdefend[.]io user. Can this be confirmed from the platform? You can make a search on Endpoint Security for this. As a result of the search, it was seen that there were no results for all four users.

"sane@letsdefend.io"
"zane@letsdefend.io"
"fane@letsdefend.io"
"tane@letsdefend.io"

Containment

The relevant host should be isolated from the network since it is certain that the attacker successfully logged into the system. To do this, go to the host named Mane via Endpoint Security and click on "containment". An example is shared below.

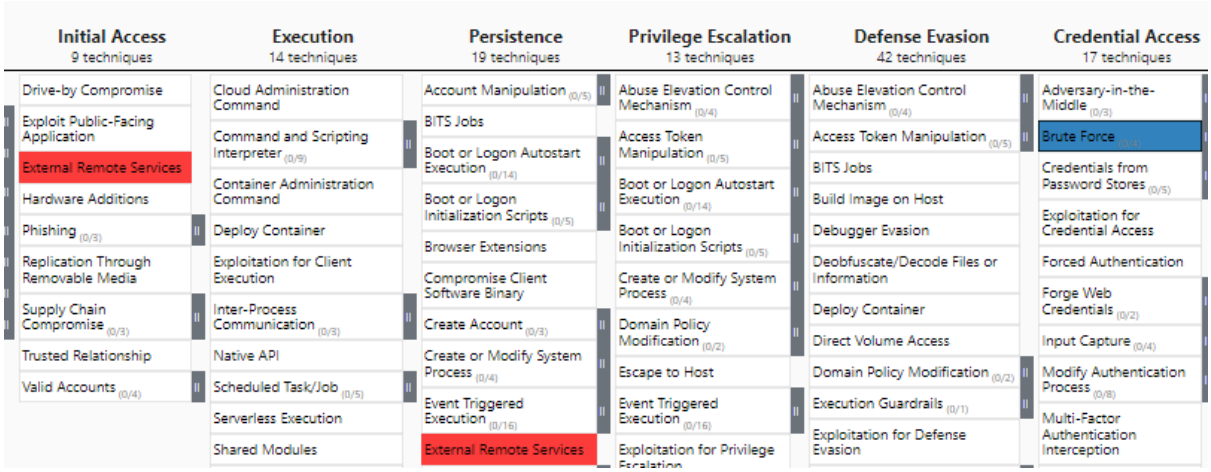


Lesson Learned

- Especially in structures open to the outside world, MFA (Multi-Factor Authentication) must be active.
- It is recommended to set a strong password policy on clients and servers.
- End users should be trained periodically to raise awareness on information security.

Appendix

MITRE



MITRE Tactics	MITRE Techniques
Initial Access	Valid Accounts(T1078)
Credential Access	Brute Force(T1110)

Artifacts

Field	Value
Attacker IP Address	37[.]19.221.229
User	mane[@]letsdefend[.]io