Prepared By: Gopi Gor

Date: 03/14/2024

User Security Monitoring

This report analyses 3 different parts of user security monitoring and plays a role in incident reporting. This report has been created using Sumologic for lab purposes. Previously parsed logs have been used to run the scripts. Considering a role of an SOC analyst, a report has been prepared for Brute Force Attacks, Password Spray techniques and Threat Intelligence along with business implications.

Brute Force Attacks

In the case of Brute Force Attacks, the attackers usually try about a list of passwords, using dictionaries, or commonly used words in passwords. The Brute Force technique is to constantly try different passwords one after another. As an SOC analyst investigating this alert, I would first try to filter out and parse the fields that give me important information about the users, their IP's and then the status on their login requests. Additionally, it would be necessary to allocate the status as "Failed" to be able to identify failed requests and then investigate them in detail. Following this, a filter would be needed to set the timespan in which these failed requests occur. It is nearly impossible for a human to fail 100 passwords in 10 minutes. According to the data collected, this count and timespan can be decided to understand the cause. With regards to the IP addresses, we can investigate the user device which is being targeted and analyze further details of the data on that computer. The criticality assigned to this alert would be **high** because brute force logins and failed attempts could mean unauthorized entry into the network, via just one endpoint. The dashboards that could be useful in the investigation of this alert which be user logons and logoffs, user failed attempts with counts, and dashboards like OneLogin which show the password changes made. The Enterprise Audit dashboard to deploy for User Activities could be helpful too.

There can be major business implications of brute force attacks on an organization. If an attacker manages entry into the endpoint, there could be loss of data and personal information and other linked passwords too. With regards to short-term risks, they include stealing of local files which may contain confidential information, and complete control of the network in no time. Once in a system, and if it does undetected, the user can install malicious payloads and applications on the endpoint, thereby opening up security issues for the whole network. Long-term risks involve financial losses, consuming of CPU resources, lack of trust in the brand itself and legal fines.

To remediate this, and prevent the occurrence of the same, an organization should make sure that there is a strong password policy and backend list of words that cannot be a part of the password. These lists can be defined on the basis of the wordlists that attackers use. Furthermore, not just multi-factor authentication but a fixed number of failed attempts (for example, 3) should result in a system lockout.

Password Spray

A password spray attack is the one where the user tries to spray one password to many different accounts. In this case, the commonly used passwords are tried on accounts instead of combinations on just one account. This allows just a bigger surface area to penetrate a network. Just one single point of entry is enough to gain access to the network. As an SOC analyst, it would be important to first failed failed attempts in the network logs, followed by checking the source IP addresses of the failed attempts. This would allow us to understand what the reasons for a failure of just one source IP address are trying to login to different accounts. For a detailed analysis, we can look at the messages, which tell us about the client details, authentication context, event type and outcome. All these headers can show different information about the failure. Additionally, we can add a where clause to define the failed attempts to show that more client ip's have been failing the requests. The severity assigned to this log can be defined as **medium** as this shows attempts to spray the passwords along different users. If any suspicious activity gets recorded, quick changes can be done to avoid it from further damage into the network. The dashboards that can be useful in this case could be the IP Address Dashboards, which show the current Source IP's trends in the logs. This could also have another tab which shows the Usernames of users that are targeted. A UEBA tool kind of dashboard can be used which as well show the severity of risk to the users with their current passwords. Additionally, general user monitoring dashboards can be used to show the failed login or logouts.

The short-term risks associated with this could mean unauthorized payments from a legitimate user's account, and also slow down all the operations in the organization. Private information stealing and crafting a new purchase can all be done. These short-term risks result in the long-term damages and risks to the organizational such as financial debt, loss of sensitive information, and lack of trust in all shareholders and customers. Additionally, recovering from all of this could take a really long time and it could mean a drop in revenue, and laying of employees.

To remediate this kind of an attack in the case it occurs, apart from the strong password policy, login detection can be setup beforehand so that system admins are notified in the alert that a user from one IP has logged into multiple locations or detecting this activity. Zero trust and biometrics can be implemented.

Threat Intelligence

Threat Intelligence in this case would mean to use threat intelligence methods and sources to detect unusual Azure AD logins. For investigating this alert, we need to first look for all activity that is related to sign-in attempts. This would filter out results for sign-ons and then we need to see if we can sort these and filter them by IP address to understand unusual logins. In organizations, domain computers have a defined Ip address associated with the user. Threat Intelligence sources can be set-up which then detect any other IPs or malicious IPs that are being used. Additionally, other sources can be used to verify the network activity and severity of the threat that is being currently examined. The severity of this threat or alert can be **high** and **medium** based on the data collected from the threat intelligence collected. The threat level and malicious actor type can give a lot of information on the type of entry performed. The dashboards that can be useful in this case would be one which displays malicious confidence along with IP address. Another one which can be used is a dashboard which sorts the data in highest severity to lowest severity along with CVE numbers.

In terms of business aspect, threat intelligence reports for malicious logins are very risky for an organization, because they go more in depth than usernames, IP addresses and login time. The short-term risks associated with this include complete control of the computer along with injection of malware via bot computers. This means stealing of passwords, data, continuous control and monitoring of the network. Over the long run, this means that the threat actor can launch a malicious payload and be an advanced persistent threat in the whole network. This results in constant leaking of data and persistence of an actor in the network. In conclusion, this would cause loss of data, loss of money and complete reinstallation of the network after a complete sanitization.

To remediate this kind of issue showing up in the organization's network, threat detection should be enabled on the network, with all local sources on the server which develop the log on the basis of these threat intelligence capabilities. All end-points should be included by default with end-point solutions and user awareness and training, incase something like this occurs. SOC operations should constantly monitor and set up alerts for any kind of threat actors that may be dangerous to the organization.

Appendix

1. Brute Force Attacks

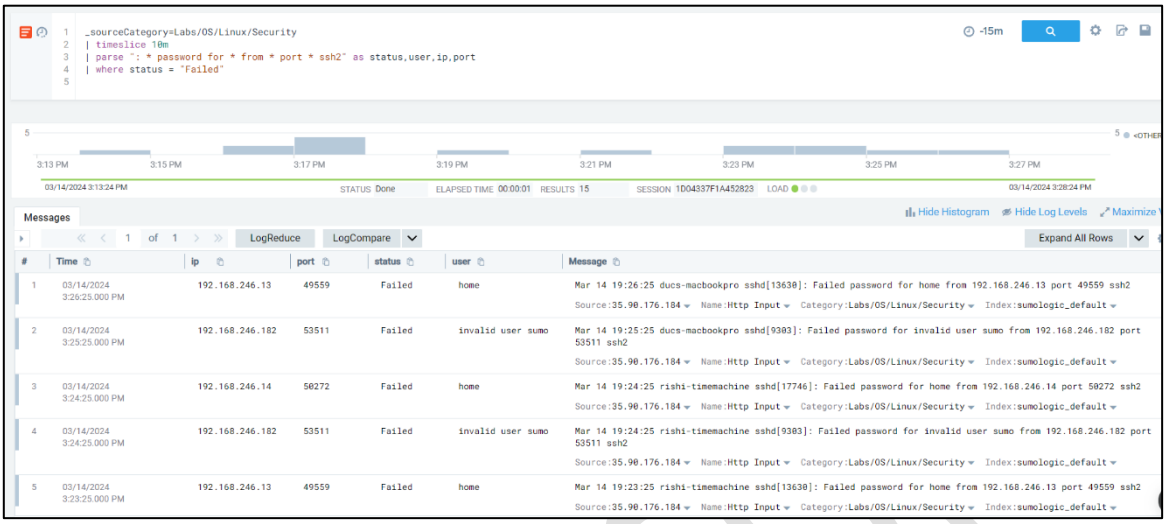


Fig: We can see the failed status for the requests made within the 10 minutes timeslice filter, and then further the user for which these password requests failed.

```
_sourceCategory=Labs/OS/Linux/Security
| timeslice 10m
| parse ": * password for * from * port * ssh2" as status,user,ip,port
| where status = "Failed"
| count by _timeslice, user,status,ip,port
| where _count > 100
| sort by _count
```

Fig: After this, we added where clause which showed no results in the current log source, but it is impossible for a human to make 100 requests within the span of 10 minutes. So that is we were looking for in this alert.

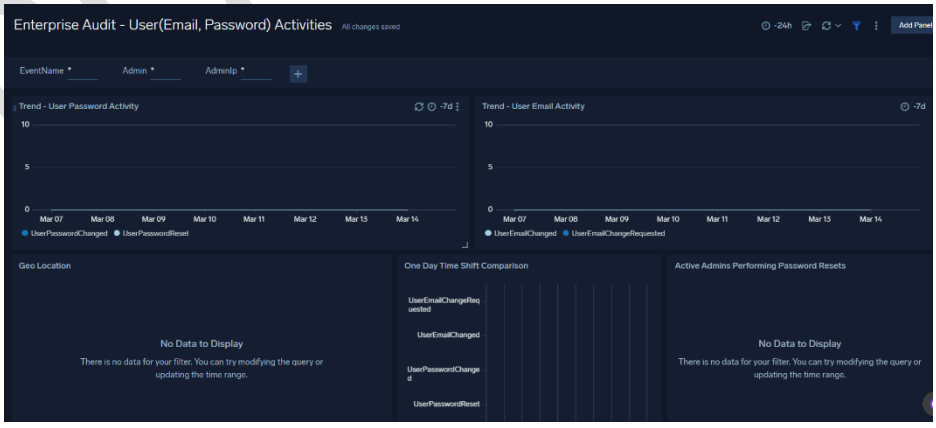


Fig: An example of a dashboard that could be useful for keeping track of user activities regarding passwords and logins.

2. Password Spray

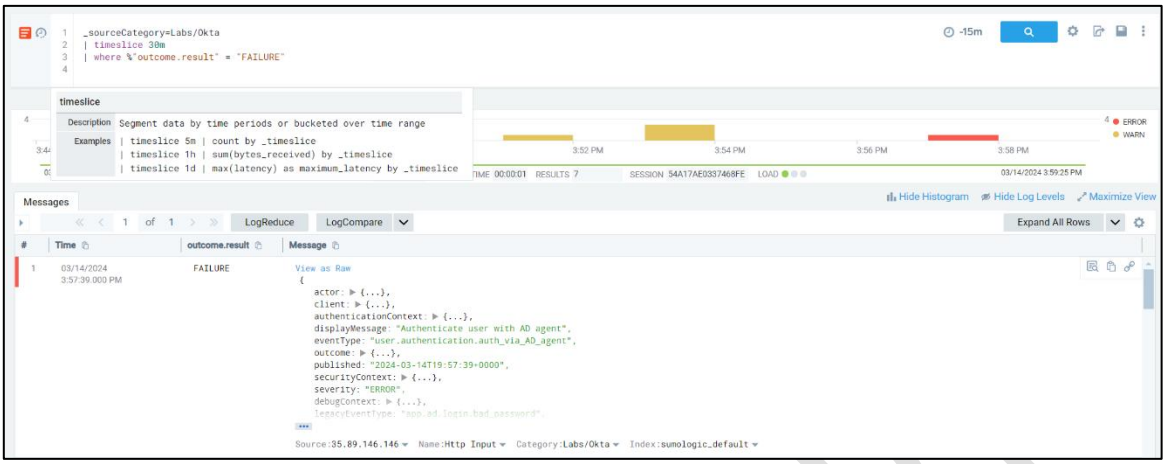


Fig: We looked for failed attempts and see the message details in this. We set a time slice of 30 minutes to collect data.

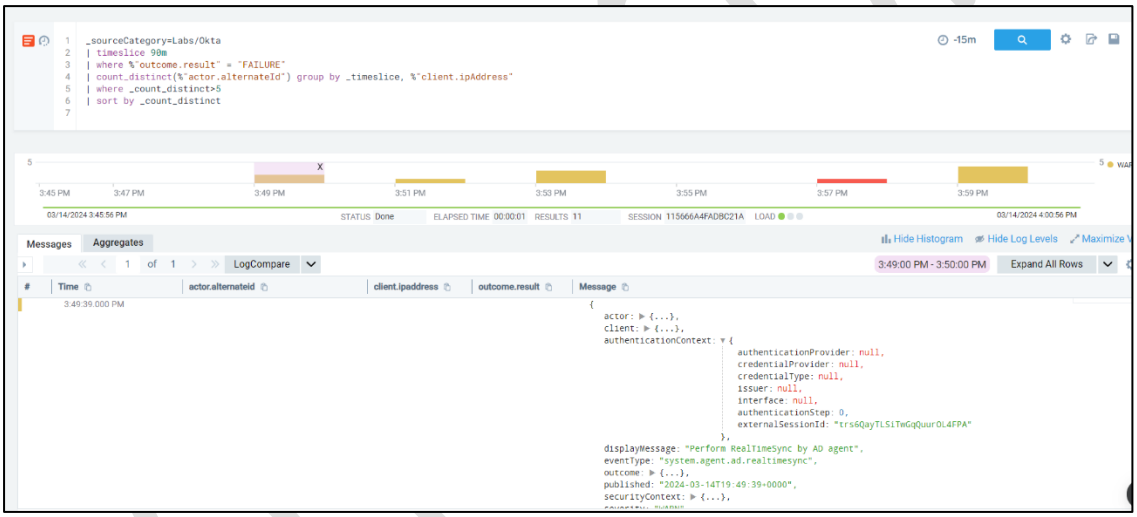
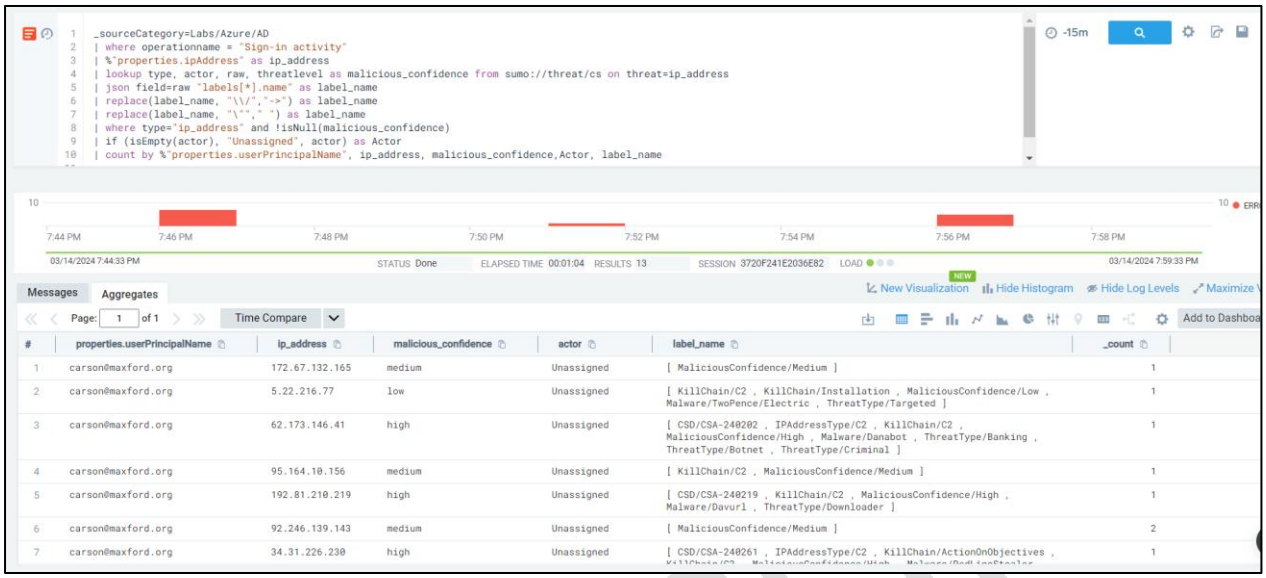


Fig: Here, we added a count for the requests and then sorted it to see the results. If we look at the message column, we can see a random string under the external session id.

3. Threat Intelligence



```
_sourceCategory=Labs/Azure/AD
| where operationname = "Sign-in activity"
| %"properties.ipAddress" as ip_address
| lookup type, actor, raw, threatlevel as malicious_confidence from sumo://threat/cs on threat=ip_address
| json field=raw "labels[*].name" as label_name
| replace(label_name, "\\/","->") as label_name
| replace(label_name, "\"","") as label_name
| where type="ip_address" and !isNull(malicious_confidence)
| if (isEmpty(actor), "Unassigned", actor) as Actor
| count by %"properties.userPrincipalName", ip_address, malicious_confidence,Actor, label_name
```

-15m

7:44 PM 7:46 PM 7:48 PM 7:50 PM 7:52 PM 7:54 PM 7:56 PM 7:58 PM

03/14/2024 7:44:33 PM STATUS Done ELAPSED TIME 00:01:04 RESULTS 13 SESSION 3720F241E2036E82 LOAD 03/14/2024 7:59:33 PM

Messages Aggregates

New Visualization Hide Histogram Hide Log Levels Maximize

Page: 1 of 1 Time Compare Add to Dashboa

#	properties.userPrincipalName	ip_address	malicious_confidence	actor	label_name	_count
1	carson@maxford.org	172.67.132.165	medium	Unassigned	[MaliciousConfidence/Medium]	1
2	carson@maxford.org	5.22.216.77	low	Unassigned	[KillChain/C2 , KillChain/Installation , MaliciousConfidence/Low , Malware/TwoPence/Electric , ThreatType/Targeted]	1
3	carson@maxford.org	62.173.146.41	high	Unassigned	[CSD/CSA-240202 , IPAddressType/C2 , KillChain/C2 , MaliciousConfidence/High , Malware/Danabot , ThreatType/Banking , ThreatType/Botnet , ThreatType/Criminal]	1
4	carson@maxford.org	95.164.10.156	medium	Unassigned	[KillChain/C2 , MaliciousConfidence/Medium]	1
5	carson@maxford.org	192.81.210.219	high	Unassigned	[CSD/CSA-240219 , KillChain/C2 , MaliciousConfidence/High , Malware/Davurl , ThreatType/Downloader]	1
6	carson@maxford.org	92.246.139.143	medium	Unassigned	[MaliciousConfidence/Medium]	2
7	carson@maxford.org	34.31.226.230	high	Unassigned	[CSD/CSA-240261 , IPAddressType/C2 , KillChain/ActionOnObjectives ,	1

Fig: We can see that based on the method used and query set up, we can see the different kind of labels that have been collected and Ip addresses along with actor type.

#	properties.userPrincipalName	ip_address	malicious_confidence	actor	label_name	_count
					ThreatType/InformationStealer , ThreatType/RAT]	
8	carson@maxford.org	185.237.206.77	low	Unassigned	[CSD/CSIT-24031 , KillChain/C2 , MaliciousConfidence/Low , Malware/Socks5Systemz , ThreatType/Commodity , ThreatType/Criminal , ThreatType/Proxy]	1
9	carson@maxford.org	152.89.198.214	low	Unassigned	[CSD/CSIT-24031 , KillChain/C2 , MaliciousConfidence/Low , Malware/Socks5Systemz , ThreatType/Commodity , ThreatType/Criminal , ThreatType/Proxy]	1
10	carson@maxford.org	174.207.39.190	medium	SCATTEREDSPIDER	[Actor/SCATTEREDSPIDER , MaliciousConfidence/Medium , ThreatType/Criminal , ThreatType/Targeted , ThreatType/TargetedCrimeware]	1
11	carson@maxford.org	185.16.39.253	high	Unassigned	[CSD/CSIT-24059 , IPAddressType/C2 , KillChain/ActionOnObjectives , KillChain/C2 , MaliciousConfidence/High , Malware/Quasar , Malware/RaccoonStealer , ThreatType/Commodity , ThreatType/Criminal	1

Fig: This image shows us the different kind of actors and threat type along with malicious confidence levels. The scattered spider for example has a criminal threat type and it is a targeted threat.

References

1. https://www.splunk.com/en_us/blog/learn/brute-force-attacks.html
2. https://www.kaspersky.com/resource-center/definitions/what-is-password-spraying
3. https://learn.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection
4. https://jeffreyappel.nl/azure-ad-identity-protection-user-risk-and-sign-in-risk-protection-with-automation/