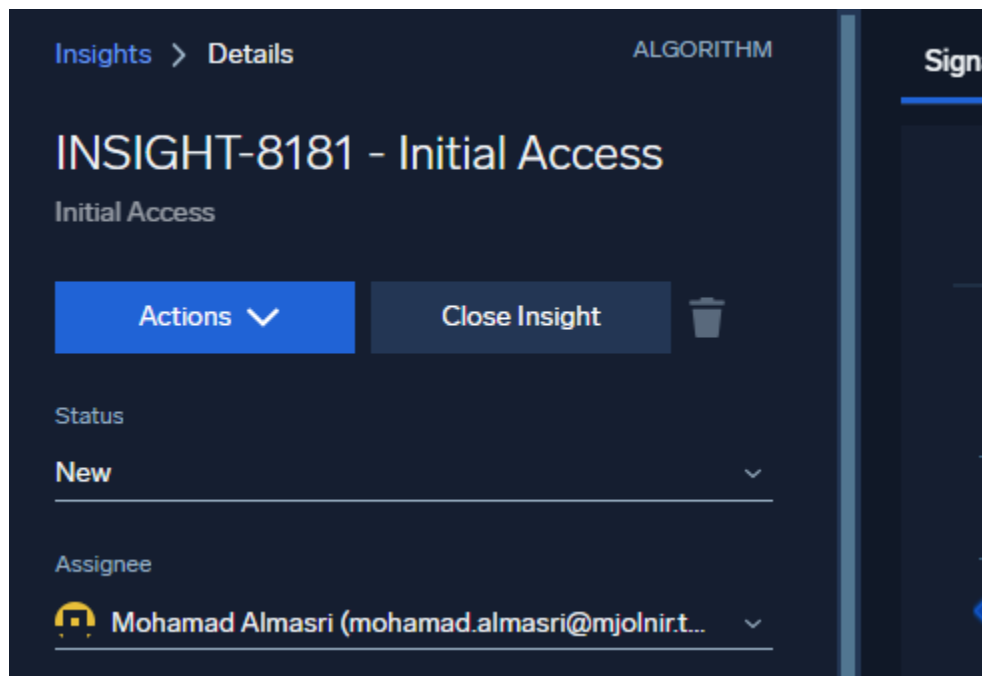
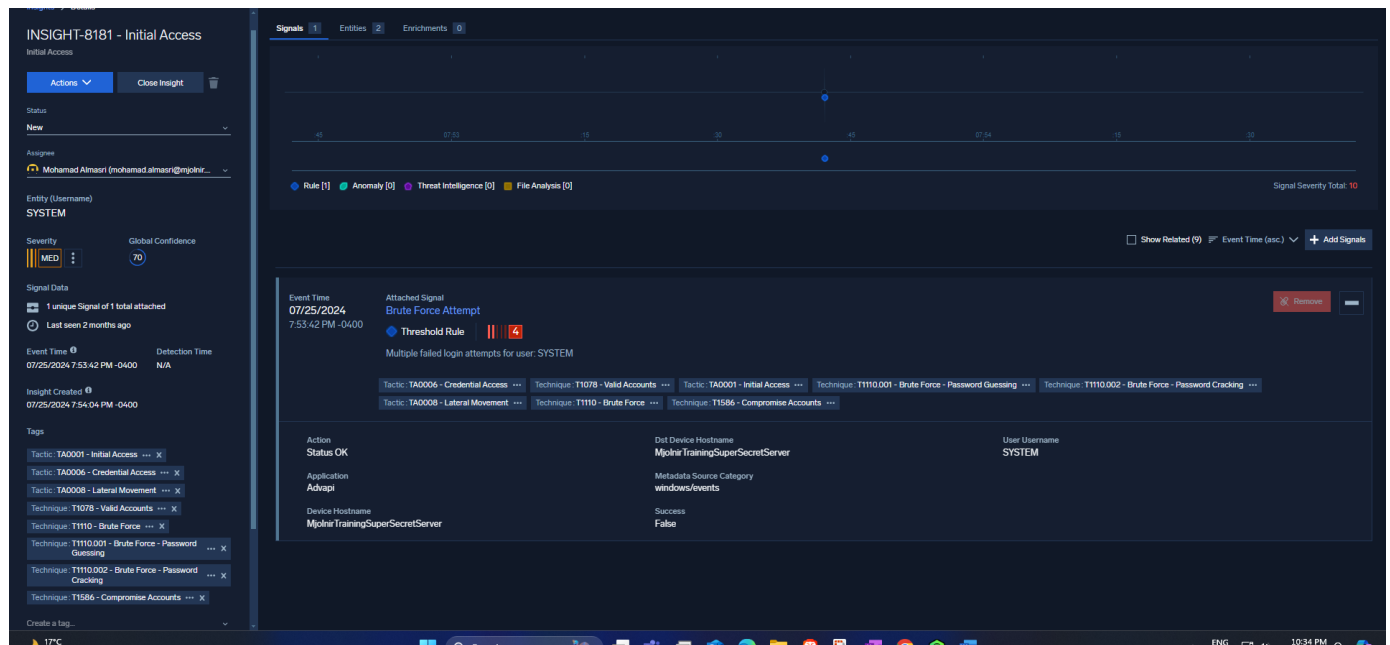


DIGITAL FORENSICS&INCID. RESP - COMP 4071**Homework Lab 1****Contents**

1. INSIGHT-8181 - Initial Access	2
2. INSIGHT-8180 - Initial Access	4
3. INSIGHT-8163 – Discovery	5
4. INSIGHT-8164 - Discovery	5
5. INSIGHT-8165 - Discovery	5
6. INSIGHT-8166 - Discovery	5
7. INSIGHT-8167 - Discovery	5
8. INSIGHT-8168 - Discovery	5
9. INSIGHT-8170 - Discovery	5
10. INSIGHT-8171 - Defense Evasion.....	7
11. INSIGHT-8172 - Defense Evasion.....	7
12. INSIGHT-8334 - Credential Access	10
13. INSIGHT-8331 - Credential Access	10
14. INSIGHT-8179 - Initial Access	12
15. INSIGHT-8178 - Initial Access	14
16. INSIGHT-8175 - Initial Access	14
17. INSIGHT-8174 - Initial Access	14
18. INSIGHT-8173 - Initial Access	14
19. INSIGHT-8169 - Initial Access	14
20. INSIGHT-8161 - Initial Access	14

1. INSIGHT-8181 - Initial Access





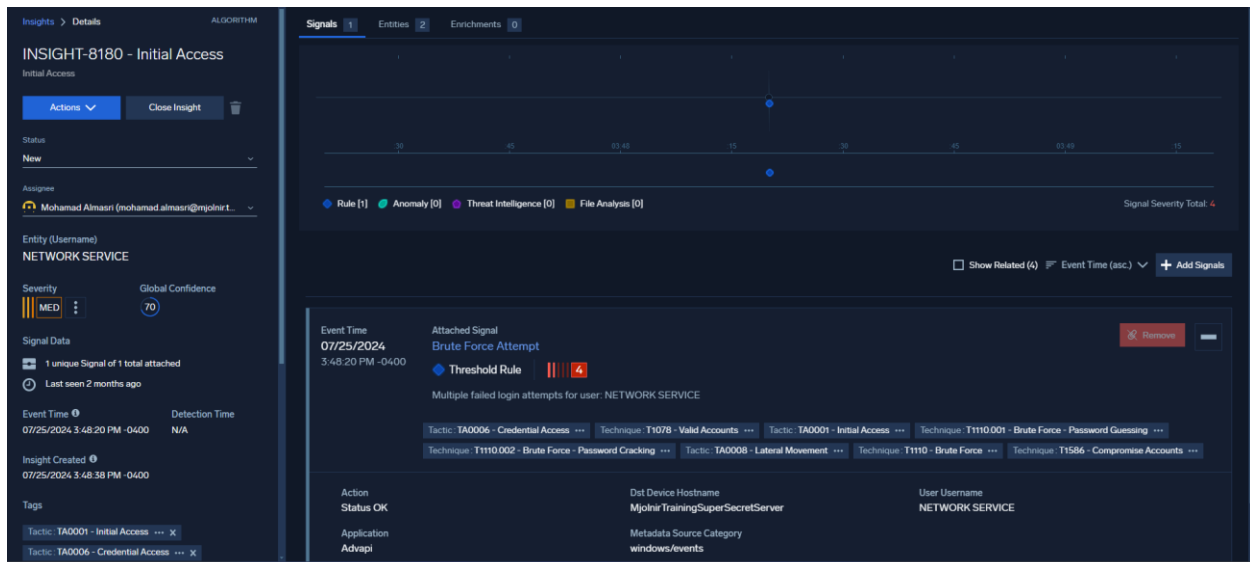
1. Name of insight and number:
2. INSIGHT-8181 - Initial Access
3. What is the insight about? Brute Force Attempt
4. What are the signals contained within and their descriptions in your own words (do not copy paste from what sumo says)?

Identifies several unsuccessful attempts to log in with the same username during a 24-hour period.

5. What is your analysis on the basis of the tags?

The tags indicate that the attack involved methods like initial Access and Credential Access suggesting adversaries used brute force to bet passwords.
6. What is your recommendation? Force Strengthen password policies with capital and special characters, use multi-factor authentication, monitor for multiple login failures

2. INSIGHT-8180 - Initial Access



1. Name of insight and number : **INSIGHT-8180 - Initial Access**
2. What is the insight about? **Brute Force Attempt Compromise Accounts**
3. What are the signals contained within and their descriptions in your own words (do not copy paste from what sumo says)?

Multiple failed login attempts for user: NETWORK SERVICE

4. What is your analysis on the basis of the tags?

The tags show that the attacker used compromised accounts for Credential Access and Social Engineering tactics. They likely obtained credentials through phishing, brute force,

5. What is your recommendation?

Implement strong multi-factor authentication, monitor for unusual account activities like login, and logout, time, and locations, and educate the employees about phishing risks.

3. INSIGHT-8163 – Discovery

4. INSIGHT-8164 - Discovery

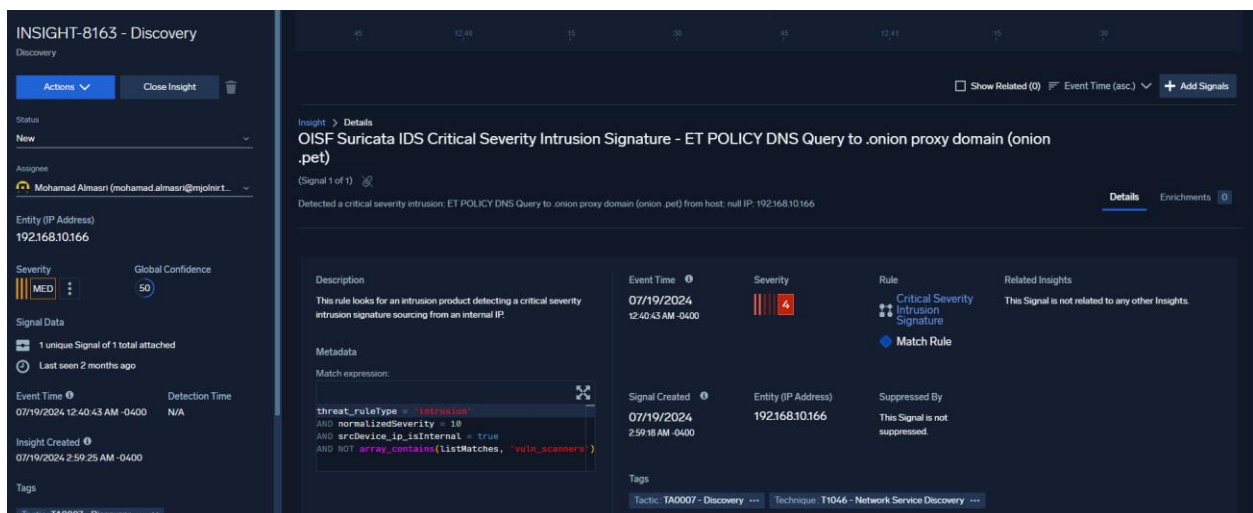
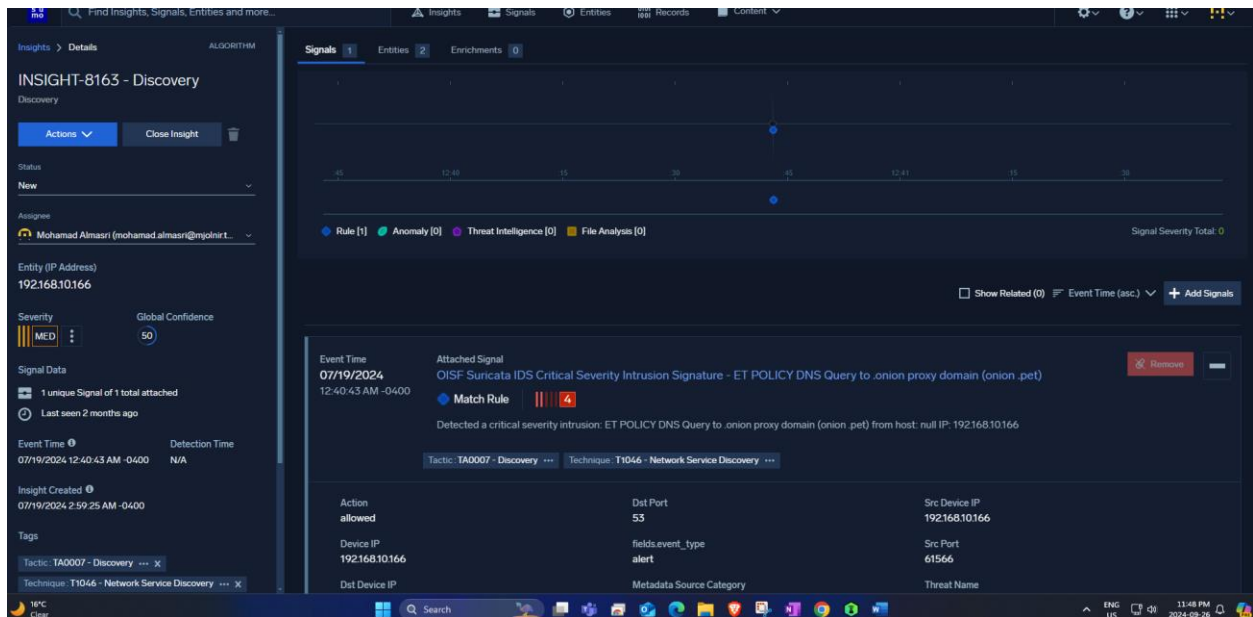
5. INSIGHT-8165 - Discovery

6. INSIGHT-8166 - Discovery

7. INSIGHT-8167 - Discovery

8. INSIGHT-8168 - Discovery

9. INSIGHT-8170 - Discovery



1. Name of insight and number:

INSIGHT-8163 – Discovery

INSIGHT-8164 - Discovery

INSIGHT-8165 - Discovery

INSIGHT-8166 - Discovery

INSIGHT-8167 - Discovery

INSIGHT-8168 - Discovery

INSIGHT-8170 - Discovery

2. What is the insight about?

OISF Suricata IDS Critical Severity Intrusion Signature - ET POLICY DNS Query to onion proxy domain (onion .pet)

3. What are the signals contained within and their descriptions in your own words (do not copy paste from what sumo says)?

When the Suricata IDS device discovered that a likely SSH scan changed into being sent out from the inner IP cope with 192.168.10.143, it sent a excessive-severity alert. This suggests that the device is probably engaging in questionable behavior, such as seeking out protection holes in different systems.

4. What is your analysis on the basis of the tags?

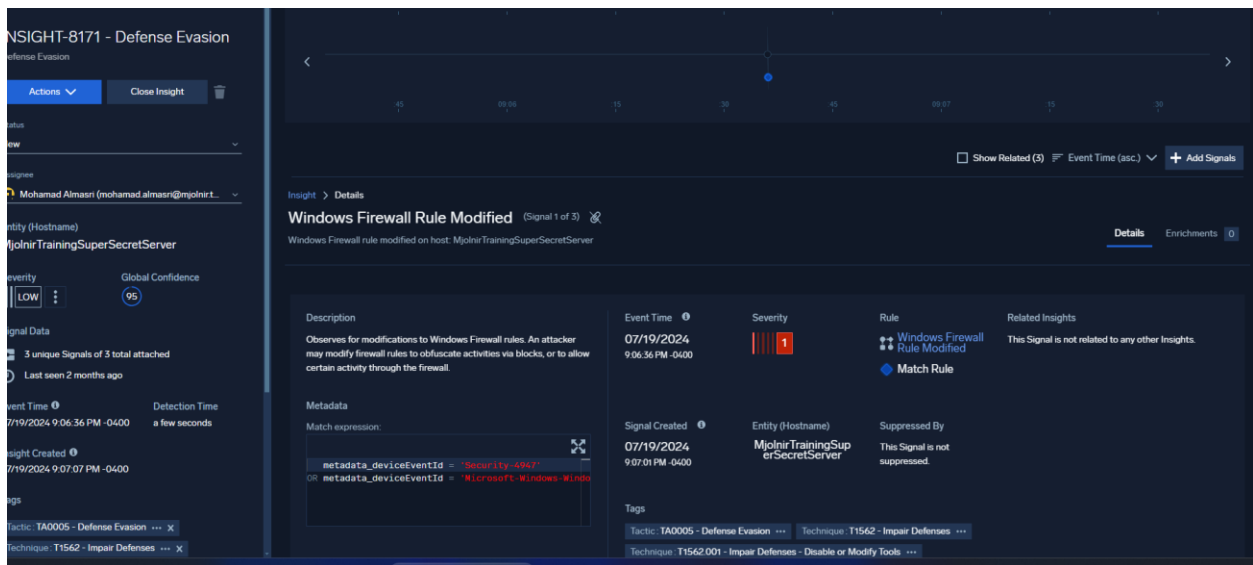
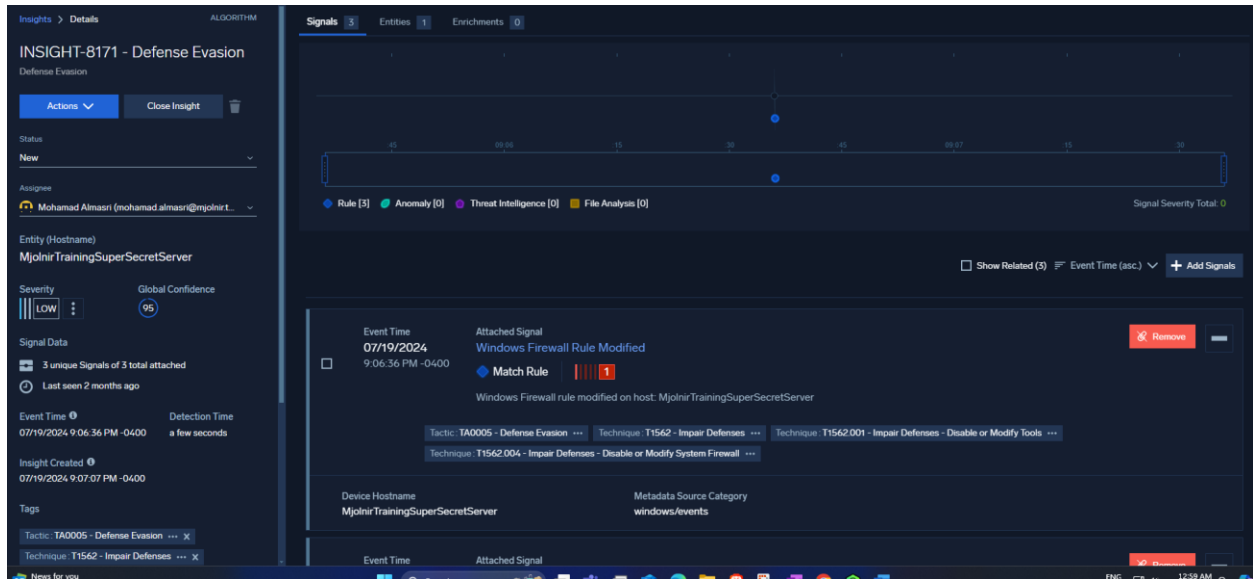
The attack uses discovery techniques, meaning an adversary attempts to gather information about your system. DNS queries found in the onion proxy domain indicate either malicious intent or access to a hidden network.

5. What is your recommendation?

Block all DNS you do not trust , especially on onion domains. Analyze the source IP 192.168.10.166 for each unique user and enable the firewall rule and antivirus .

10. INSIGHT-8171 - Defense Evasion

11. INSIGHT-8172 - Defense Evasion



1. Name of insight and number:

INSIGHT-8171 - Defense Evasion

INSIGHT-8172 - Defense Evasion

2. What is the insight about?

Defense Evasion, Windows Firewall Rule Modified

3. What are the signals contained within and their descriptions in your own words (do not copy paste from what sumo says)?

Tactic: TA0005 - Defense Evasion

Technique: T1562 - Impair Defenses

Technique: T1562.001 - Impair Defenses - Disable or Modify Tools

Technique: T1562.004 - Impair Defenses - Disable or Modify System Firewall

keeps an eye out for changes to Windows Firewall rules. An attacker may modify firewall rules to either permit specific operations via the firewall or hide actions using blocks.

4. What is your analysis on the basis of the tags?

The tags show that an attacker is probably trying to get around security with the aid of converting firewall guidelines. This could allow terrible visitors pass through or stop some gear from watching, making it tougher to identify dangerous movements. In short, the tags factor to suspicious activity where someone is messing with the firewall, which will be a signal of a protection breach or bad conduct.

5. What is your recommendation?

Monitor firewall changes, conduct regular audits, and educate employees on security, and set up alerts for unusual activity, and use strong security measures like multi-factor authentication.

12. INSIGHT-8334 - Credential Access

13. INSIGHT-8331 - Credential Access

Created

09/26/2024

3:06:20 PM -0400

Detection time is N/A

Age is a day

New

INSIGHT-8334 - Credential Access

Credential Access

90 Global Confidence

Mohamad Almasri

Severity

HIGH

Entity

SYSTEM

Signal Data

1 unique signal of 1 total

Last seen a day ago

Tactic: TA0001 - Initial Access

Tactic: TA0006 - Credential Access

Tactic: TA0008 - Lateral Movement

Technique: T1078 - Valid Accounts

Technique: T1110 - Brute Force

Technique: T1110.001 - Brute Force - Password Guessing

Technique: T1110.002 - Brute Force - Password Cracking

Technique: T1586 - Compromise Accounts

Insights > Details

ALGORITHM

INSIGHT-8334 - Credential Access

Credential Access

Actions

Close Insight

Status

New

Assignee

Mohamad Almasri (mohamad.almasri@mjolnir.t...)

Entity (Username)

SYSTEM

Severity

HIGH

Global Confidence

90

Signal Data

1 unique Signal of 1 total attached

Last seen 11 hours ago

Event Time

09/26/2024 3:05:56 PM -0400

Detection Time

N/A

Insight Created

09/26/2024 3:06:20 PM -0400

Tags

Tactic: TA0001 - Initial Access

Signals 1

Entities 5

Enrichments 0

Signal Severity Total: 10

Show Related (19)

Event Time (asc)

Add Signals

Event Time

09/26/2024

Attached Signal

Successful Brute Force

Chain Rule

6

Successful brute force against user: SYSTEM

Tactic: TA0006 - Credential Access

Technique: T1078 - Valid Accounts

Tactic: TA0001 - Initial Access

Technique: T1110.001 - Brute Force - Password Guessing

Technique: T1110.002 - Brute Force - Password Cracking

Tactic: TA0008 - Lateral Movement

Technique: T1110 - Brute Force

Technique: T1586 - Compromise Accounts

Action

Status OK

Dst Device Hostname

MjolnirTrainingSuperSecretServer

Success

False

Application

MT-svr1.mjolnir.training

True

Advapi

The screenshot displays the Microsoft Sentinel console. On the left, a sidebar shows the 'INSIGHT-8334 - Credential Access' insight. The main pane shows the details of this insight, which is titled 'Successful Brute Force' (Signal 1 of 1). The insight is categorized under 'Credential Access' and has a severity of 'HIGH'. The description states: 'Detects a series of failed logins followed by a successful login. This could indicate that an attacker was successful in guessing a user's password and has compromised their account. This rule does not leverage authentication logs with a normalizedAction of domainLogon and does not have a Domain version, meaning that Windows workstation logging is required to achieve full visibility.' The event time is 09/26/2024 3:05:56 PM -0400. The signal was created on 09/26/2024 3:06:12 PM -0400. The insight is associated with the entity 'SYSTEM'. The rule is 'Successful Brute Force' with a chain rule. The insight is not suppressed. The tags include: TA0006 - Credential Access, T1078 - Valid Accounts, TA0001 - Initial Access, T1110.001 - Brute Force - Password Guessing, T1110.002 - Brute Force - Password Cracking, TA0008 - Lateral Movement, T1110 - Brute Force, and T1586 - Compromise Accounts.

1. Name of insight and number?

INSIGHT-8334 - Credential Access

INSIGHT-8331 - Credential Access

2. What is the insight about?

Credential Access, Successful brute force against user: SYSTEM

3. What are the signals contained within and their descriptions in your own words (do not copy paste from what sumo says)?

TA0006 - Credential Access

Technique: T1078 - Valid Accounts

Tactic: TA0001 - Initial Access

Technique: T1110.001 - Brute Force - Password Guessing

Technique: T1110.002 - Brute Force - Password Cracking

Tactic: TA0008 - Lateral Movement

Technique: T1110 - Brute Force

Technique: T1586 - Compromise Accounts

It recognizes when a login attempt is made unsuccessfully and then being successful. This could mean that the user's account has been compromised by an attacker who has guessed the password correctly. This rule does not leverage authentication logs.

4. What is your analysis on the basis of the tags?

According to Mitre& ATT&CKcon the tags, the adversary is attempting to obtain passwords and usernames. To do this, they might use methods like keylogging or credential dumping, which would give them access and enable them to move around covertly.

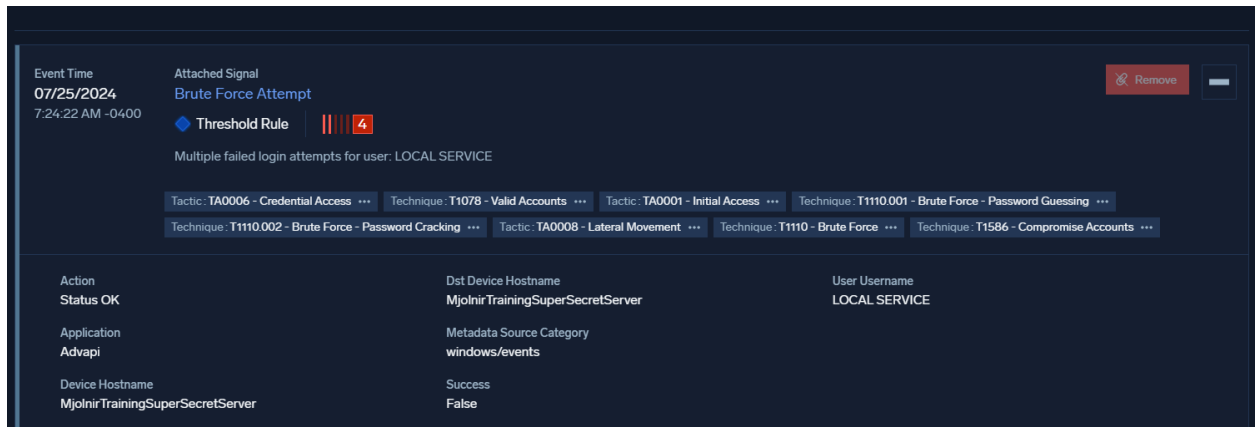
5. What is your recommendation?

Make sure your passwords are strong and unique, and turn on multi-factor authentication (MFA). Keep an eye out for unusual login behavior and set a limit on the quantity of unsuccessful login attempts

14. INSIGHT-8179 - Initial Access

The screenshot displays the MITRE ATT&CK framework interface for the tactic 'Initial Access' (INSIGHT-8179). The interface is dark-themed and includes the following elements:

- Created:** 07/25/2024, 7:24:50 AM -0400. Detection time is N/A, Age is 2 months.
- Severity:** MED (Medium).
- Entity:** LOCAL SERVICE.
- Signal Data:** 1 unique signal of 1 total. Last seen 2 months ago.
- Global Confidence:** 70.
- Author:** Mohamad Almasri.
- Tactics:** TA0001 - Initial Access, TA0006 - Credential Access, TA0008 - Lateral Movement.
- Techniques:** T1078 - Valid Accounts, T1110 - Brute Force, T1110.001 - Brute Force - Password Guessing, T1110.002 - Brute Force - Password Cracking, T1586 - Compromise Accounts.



1. Name of insight and number?

INSIGHT-8179 - Initial Access

2. What is the insight about?

Multiple failed login attempts for user: LOCAL SERVICE

3. What are the signals contained within and their descriptions in your own words (do not copy paste from what sumo says)?

Identifies several unsuccessful attempts to log in with the same username during a 24-hour period.

TA0006 - Credential Access

Technique: T1078 - Valid Accounts

Tactic: TA0001 - Initial Access

Technique: T1110.001 - Brute Force - Password Guessing

Technique: T1110.002 - Brute Force - Password Cracking

Tactic: TA0008 - Lateral Movement

Technique: T1110 - Brute Force

Technique: T1586 - Compromise Account

4. What is your analysis on the basis of the tags?
5. means the different ways an attacker might first get yo a system. They could accomplish this via using spearphishing, that's the practice of sending phony emails to lie to someone into granting get entry to, or by exploiting

vulnerabilities in websites. Once internal, they could use faraway get right of entry to or actual accounts to go back at will, however occasionally their get entry to will be terminated because of factors like password adjustments.

What is your recommendation?

Train employees on phishing awareness, regularly update web servers, implement multi-factor authentication, monitor for unusual activity, and limit access to critical systems.

15. INSIGHT-8178 - Initial Access

16. INSIGHT-8175 - Initial Access

17. INSIGHT-8174 - Initial Access

18. INSIGHT-8173 - Initial Access

19. INSIGHT-8169 - Initial Access

20. INSIGHT-8161 - Initial Access

Created
07/23/2024
3:53:24 AM -0400
Detection time is N/A
Age is 2 months

New

INSIGHT-8178 - Initial Access

Initial Access

75 Global Confidence

Mohamad Almasri

Severity

MED

Entity

SYSTEM

Signal Data

1 unique signal of 1 total

Last seen 2 months ago

Tactic: TA0001 - Initial Access ...

Tactic: TA0006 - Credential Access ...

Tactic: TA0008 - Lateral Movement ...

Technique: T1078 - Valid Accounts ...

Technique: T1110 - Brute Force ...

Technique: T1110.001 - Brute Force - Password Guessing ...

Technique: T1110.002 - Brute Force - Password Cracking ...

Technique: T1586 - Compromise Accounts ...

Event Time
07/23/2024
3:53:08 AM -0400

Attached Signal

Brute Force Attempt

Threshold Rule

4

Multiple failed login attempts for user: SYSTEM

Remove

Tactic: TA0006 - Credential Access ...

Technique: T1078 - Valid Accounts ...

Tactic: TA0001 - Initial Access ...

Technique: T1110.001 - Brute Force - Password Guessing ...

Technique: T1110.002 - Brute Force - Password Cracking ...

Tactic: TA0008 - Lateral Movement ...

Technique: T1110 - Brute Force ...

Technique: T1586 - Compromise Accounts ...

Action	Dst Device Hostname	User Username
Status OK	MjolnirTrainingSuperSecretServer	SYSTEM
Application	Metadata Source Category	
Advapi	windows/events	
Device Hostname	Success	
MjolnirTrainingSuperSecretServer	False	

Insight > Details

Brute Force Attempt (Signal 1 of 1)

Multiple failed login attempts for user: SYSTEM

Details

Enrichments 0

Description

Detects multiple failed login attempts for the same username over a 24 hour timeframe. This is designed to catch both slow and quick brute force type attacks. The threshold and time frame can be adjusted based on the customer's environment.

Metadata

Window size minutes: 1440 minutes

Match count: 10

Limit: 10

Window size: 86400000

Match expression:

objectType = 'Authentication'

AND normalizedAction = 'login'

AND success = false

AND NOT (

metadata_deviceEventId = 'Security-4776' AND (array_cor

Event Time

07/23/2024
3:53:08 AM -0400

Severity

4

Rule

Brute Force Attempt

Threshold Rule

Related Insights

This Signal is not related to any other Insights.

Signal Created

07/23/2024
3:53:19 AM -0400

Entity (Username)

SYSTEM

Suppressed By

This Signal is not suppressed.

Tags

Tactic: TA0006 - Credential Access ...

Technique: T1078 - Valid Accounts ...

Tactic: TA0001 - Initial Access ...

Technique: T1110.001 - Brute Force - Password Guessing ...

Technique: T1110.002 - Brute Force - Password Cracking ...

Tactic: TA0008 - Lateral Movement ...

Technique: T1110 - Brute Force ...

Technique: T1586 - Compromise Accounts ...

1. Name of insight and number:

INSIGHT-8178 - Initial Access

INSIGHT-8175 - Initial Access

INSIGHT-8174 - Initial Access

INSIGHT-8173 - Initial Access

INSIGHT-8169 - Initial Access

INSIGHT-8161 - Initial Access

2. What is the insight about?

Multiple failed logins attempts for user: LOCAL SERVICE

3. What are the signals contained within and their descriptions in your own words (do not copy paste from what sumo says)?

It detects when someone tries to log in with the same username multiple times in 24 hours but keeps failing. This helps spot both slow and fast attempts to guess the password. You can change how many tries are allowed and the time limit to fit your needs.

4. What is your analysis on the basis of the tags?

means the different ways an attacker might first get into a system. They could accomplish this via using spearphishing, that's the practice of sending phony emails to lie to someone into granting get entry to, or by exploiting vulnerabilities in websites. Once internal, they could use faraway get right of entry to or actual accounts to go back at will, however occasionally their get entry to will be terminated because of factors like password adjustments.

5. What is your recommendation?

Train employees on phishing awareness, regularly update web servers, implement multi-factor authentication, monitor for unusual activity, and limit access to critical systems.