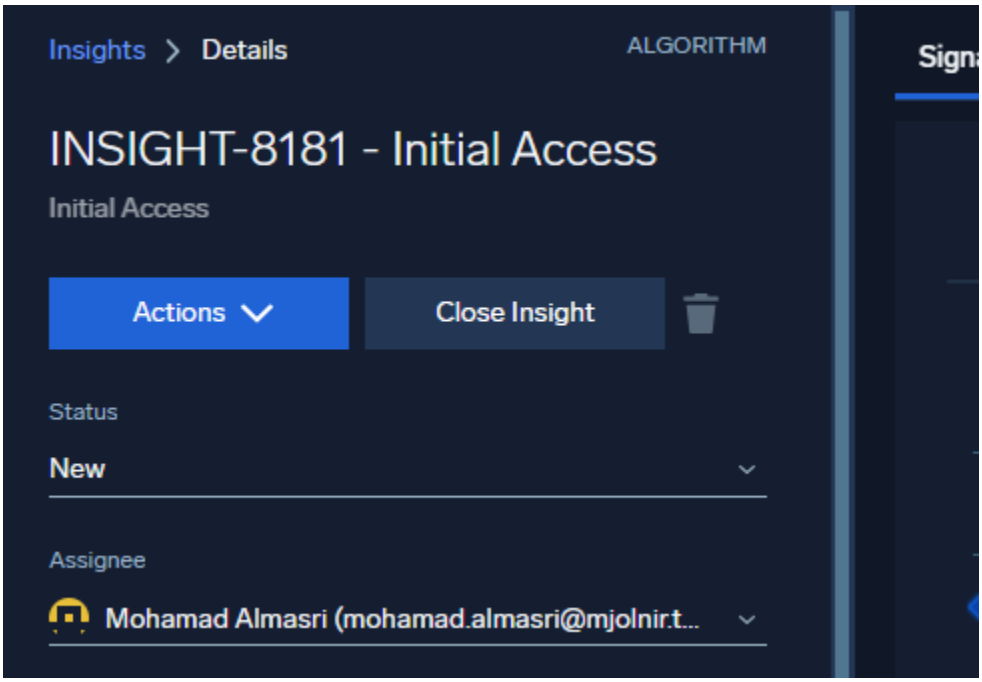
MOHAMAD ALMASRI ID: 101167438

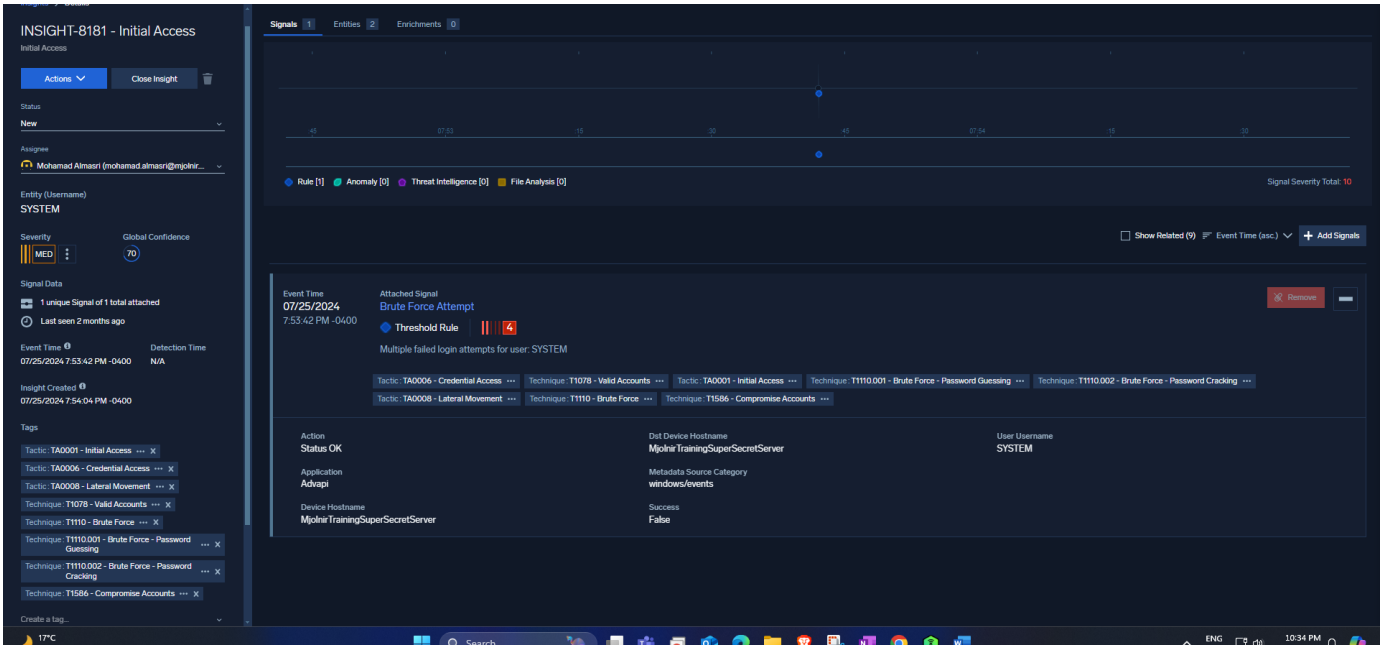
DIGITAL FORENSICS&INCID. RESP - COMP 4071

Homework Lab 1

Contents

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)?

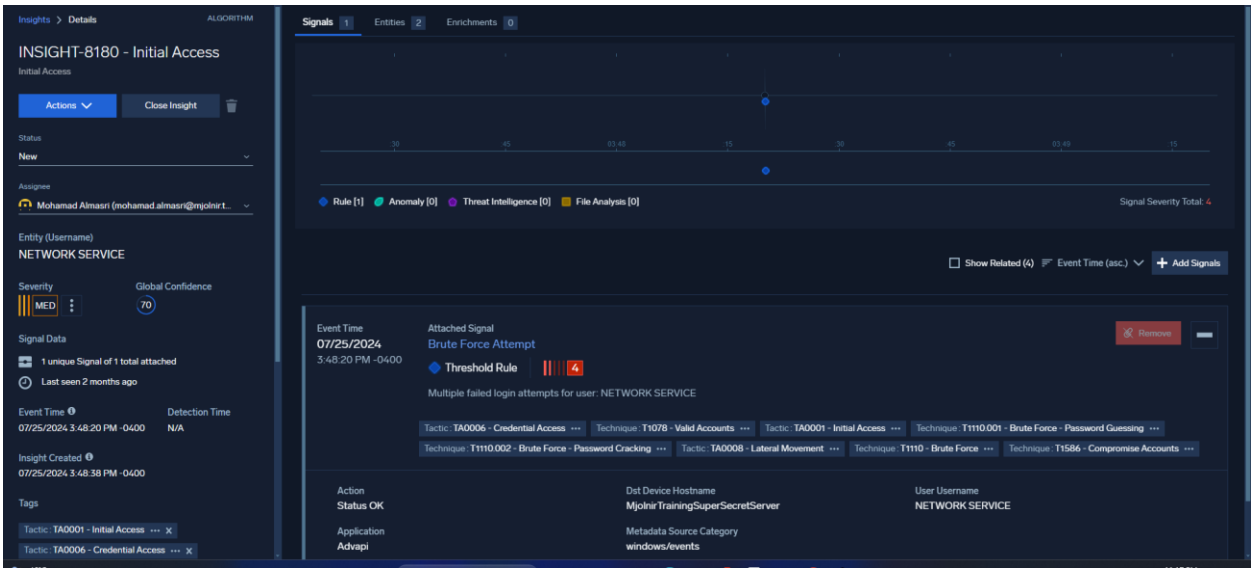
   Identifies several unsuccessful attempts to log in with the same username during a 24-hour period.

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

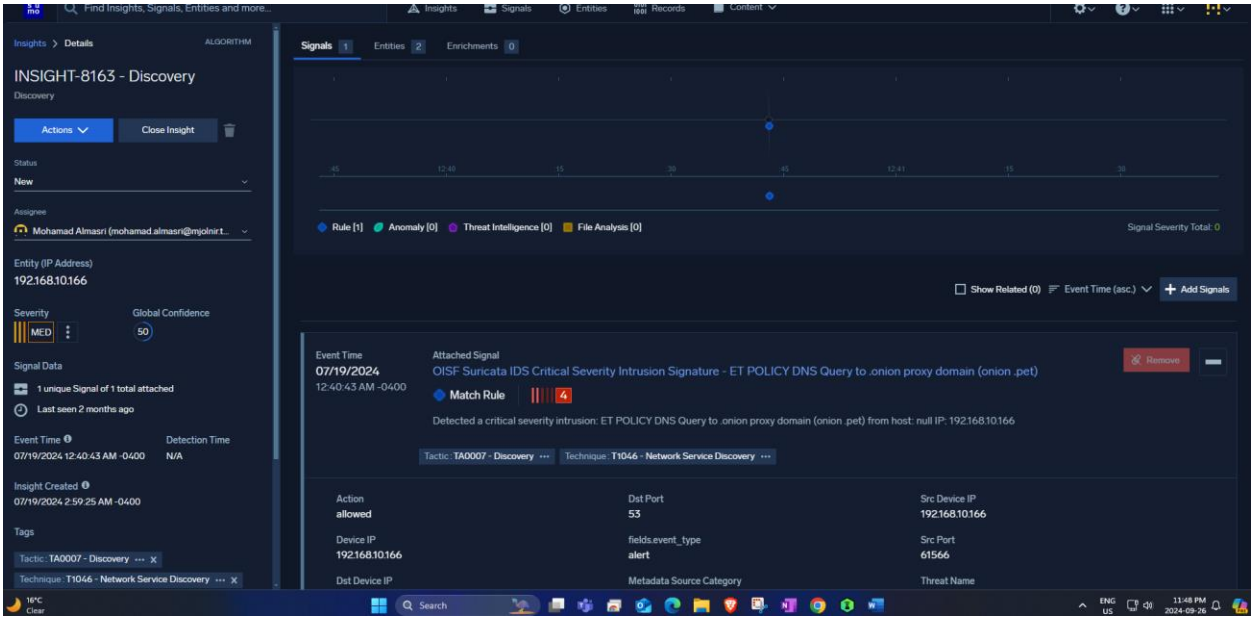
4. What is your analysis on the basis of the tags?

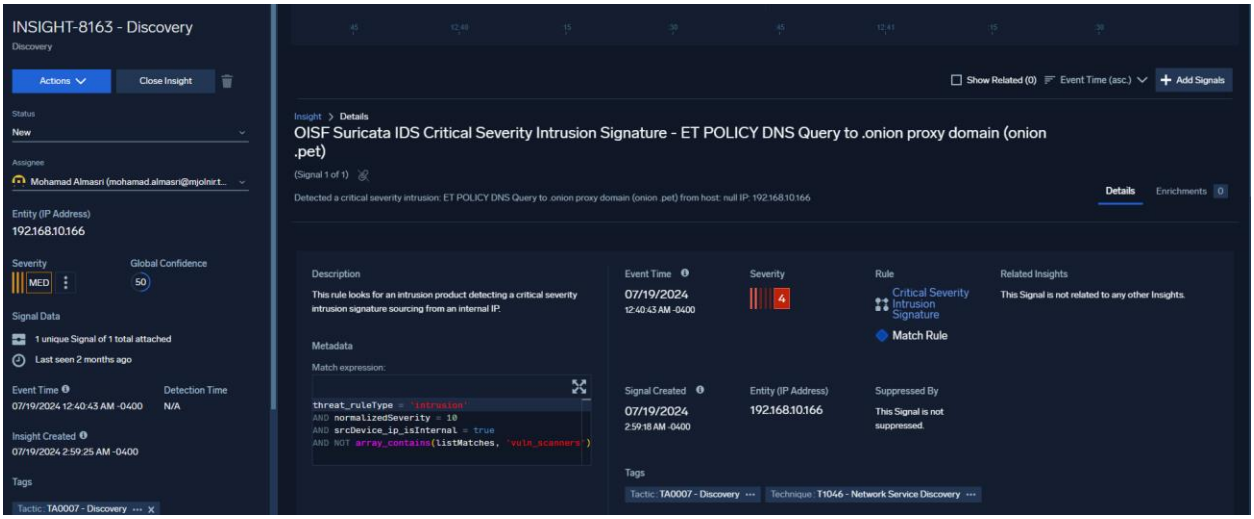
   The tags show that the attacker used compromised accounts for Credential Access and Social Engineering tactics. They likely obtained credentials through phishing, brute force,

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?

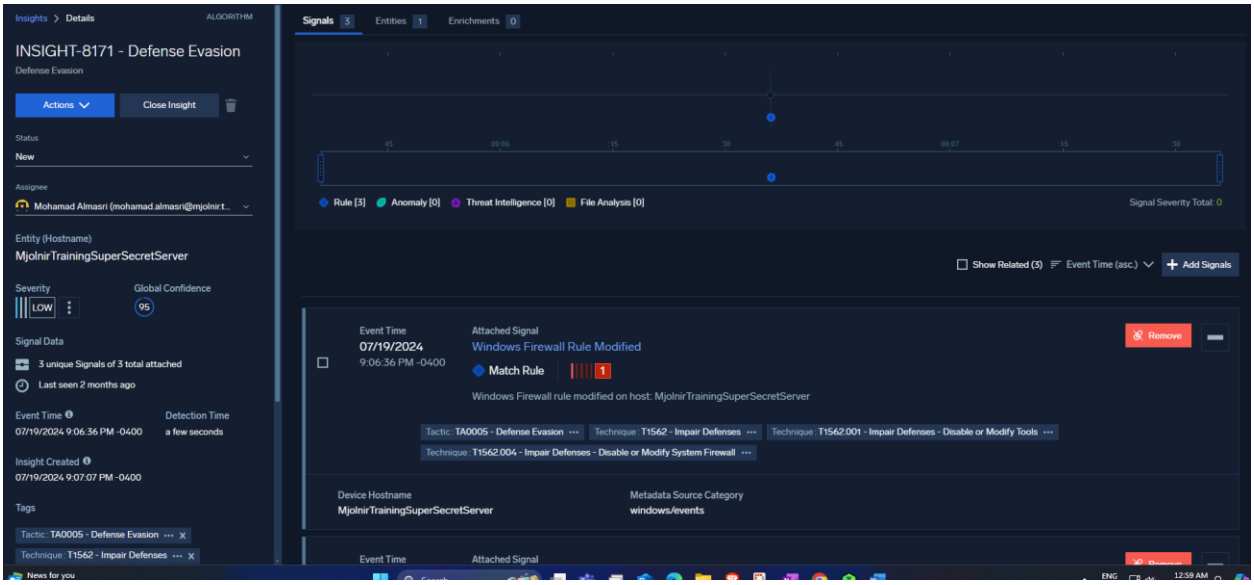
   The attack uses discovery techniques, meaning an adversary attempts to gather information about your system. DNS queries found in the onion proxy domain indicate either malicious intent or access to a hidden network.

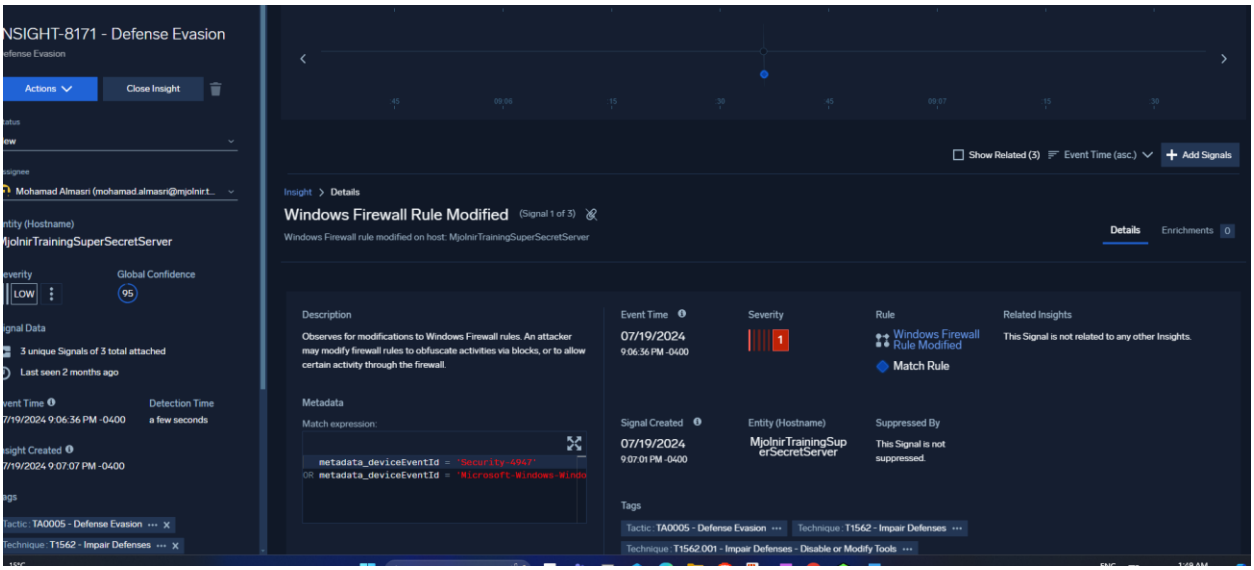
5. What is your recommendation?

   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.

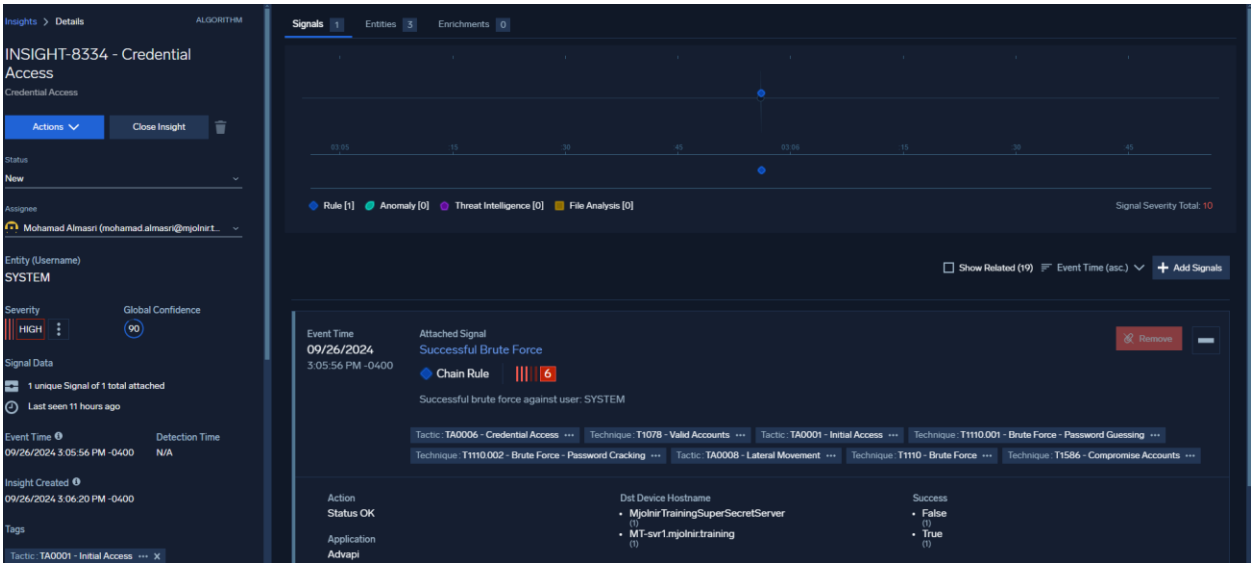
4. What is your analysis on the basis of the tags?

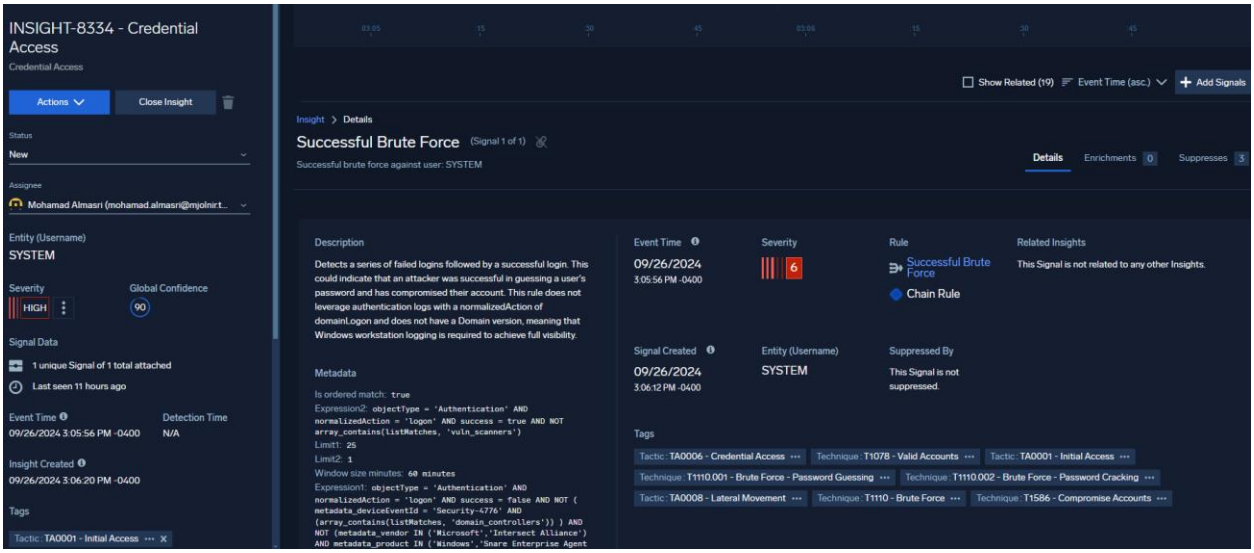
   The tags show that an attacker is probably trying to get around security with the aid of converting firewall guidelines. This could allow terrible visitors pass through or stop some gear from watching, making it tougher to identify dangerous movements. In short, the tags factor to suspicious activity 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





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.

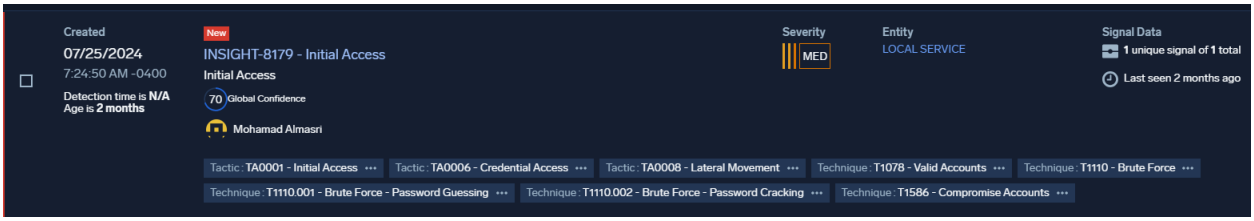
4. What is your analysis on the basis of the tags?

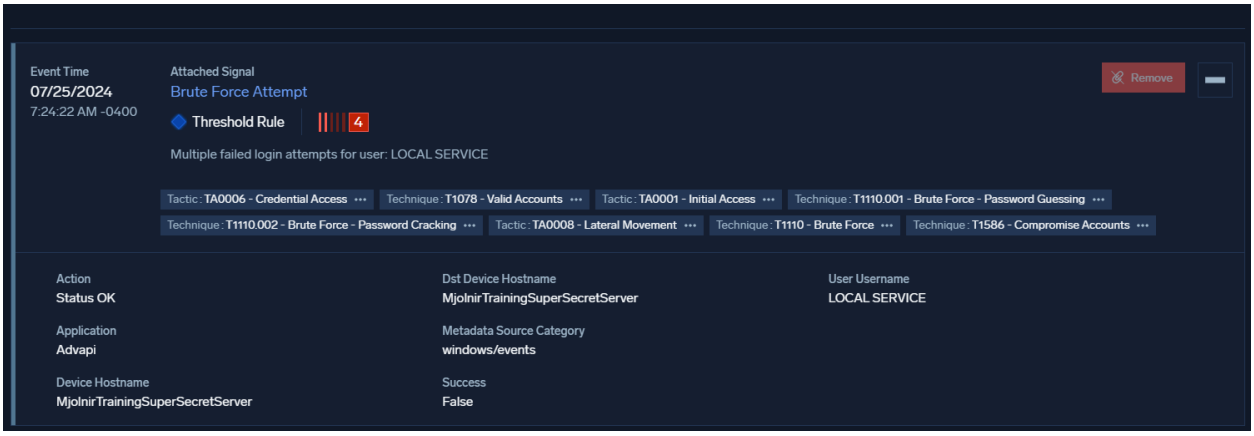
   According to Mitre& ATT&CKcon the tags, the adversary is attempting to obtain passwords and usernames. To do this, they might use methods like keylogging or credential dumping, which would give them access and enable them to move around covertly.

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





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

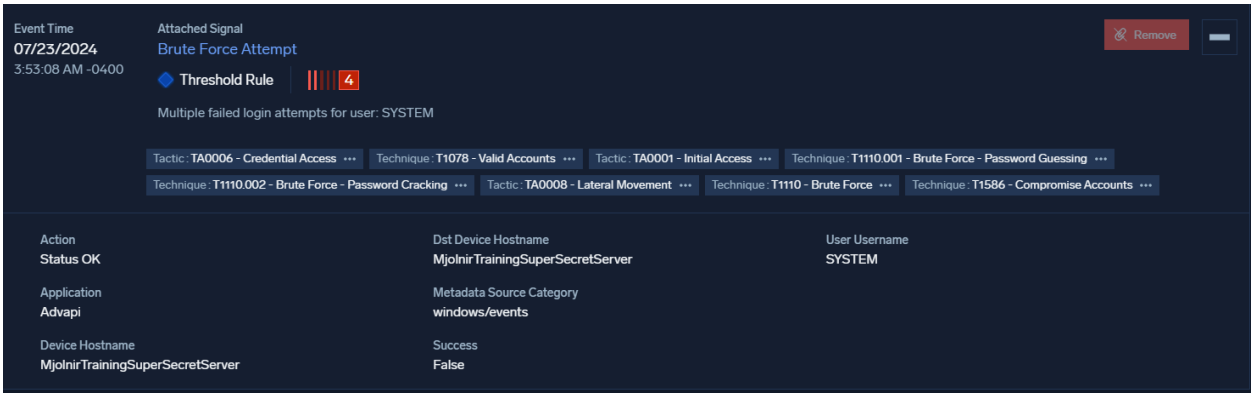
16. INSIGHT-8175 - Initial Access

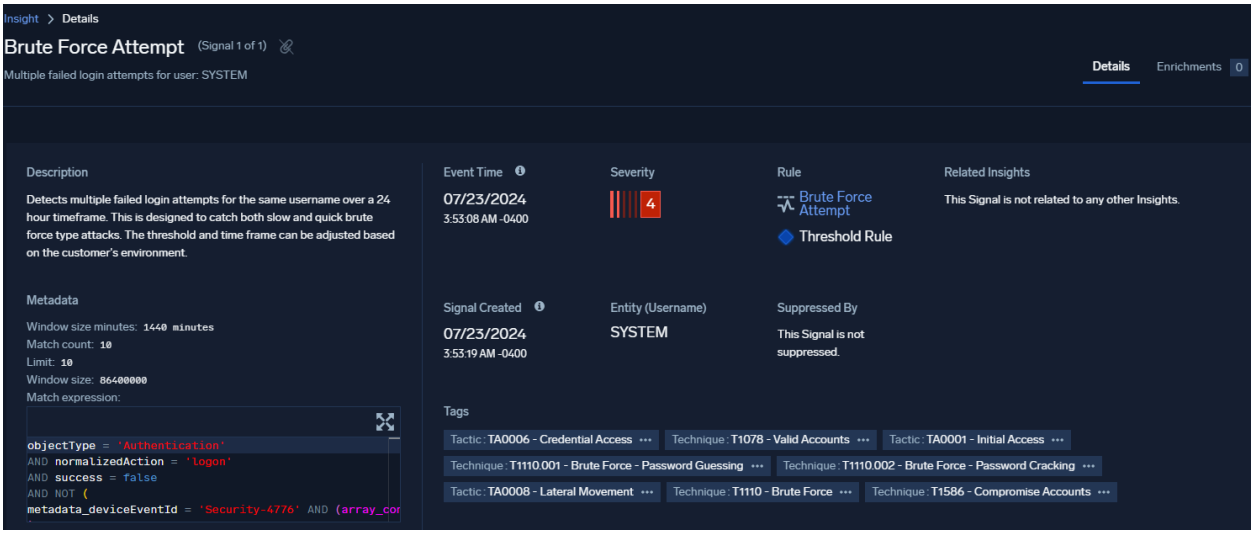
17. INSIGHT-8174 - Initial Access

18. INSIGHT-8173 - Initial Access

19. INSIGHT-8169 - Initial Access

20. INSIGHT-8161 - Initial Access





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 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.

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.