Incident Report: Brute Force Activity Detection

Incident ID: IR-2025-005

Attack Type: Bruteforce - TryHackme

Date: Dec 21, 2025

Analyst: BALA KOTESWARA REDDY REDDYMALLI

Severity: High

Status: Closed - True Positive

1. Executive Summary

A brute force attack was performed against john.smith over SSH from source IP address 10.10.242.248. The brute force attempt was successful and the attacker escalated privileges as root user using the su command. The attacker created potentially a new backdoor account named "system-utm". The backdoor account is further added into the group named “users”.

2. Scenario Context

Scenario: You’ve just started your first shift as a SOC analyst at an MSSP. Only a few minutes have passed since an alert about a possible brute force attack appeared on the platform.
Alert Details:

- **Alert Name:** Brute Force Activity Detection
- **Time:** 17/09/2025 9:00:21 AM
- **Target Host:** tryhackme-2404
- **Source IP:** 10.10.242.248

Your job is to investigate this activity and decide whether it should be considered suspicious.

Environment	Details
Target System	tryhackme-2404
Source IP	10.10.242.248

3. Incident Timeline

Time	Event Description
17/09/2025 09:01:48 - 09:06:35	Attacker performed Bruteforce Activity against “john.smith” over SSH.

Time	Event Description
17/09/2025 09:07:25	Attacker succeeded by logging in as “John.smith” over SSH
17/09/2025 09:11:28	Attacker escalated privileges into root user using “su”
17/09/2025 09:12:10	Attacker created a new backdoor account named “system-utm”
17/09/2025 09:12:21	“System-utm” user account is added to group “users”
17/09/2025 09:12:33	Attacker ssh session of user john.smith was closed.

4. Investigation Methodology

My Approach:

1. Determining which user is compromised. (john.smith)
2. Investigating the events of the Compromised user (Start and End of Bruteforce, Source IP)
3. Search for any Privilege Escalation Attempts (sudo,su escalation)
4. Search for any Persistence attempts like creating Backdoor users.
5. Extracted IOCs for threat hunting

5. Technical Analysis

Detection queries(SPL):

Determining the user Compromised in bruteforce:

```
index="linux-alert" sourcetype=linux_secure 10.10.242.248
| search "sshd" AND ("Accepted password" OR "Failed password")
| stats values(action) as action values(process) as process count by user src
| table user src action count
```

Investigating the events of compromised User:

To determine the first and last event of Bruteforce activity:

```
index="linux-alert" sourcetype=linux_secure 10.10.242.248 user=john.smith
```

To determine the successful login time:

```
index="linux-alert" sourcetype=linux_secure 10.10.242.248 user=john.smith
| search "Accepted"
```

Search for Privilege Escalation Attempts:

```
index="linux-alert" sourcetype=linux_secure
| search "*su*" AND "*COMMAND*"
```

Search for Backdoor account activity:

```
index="linux-alert" sourcetype=linux_secure system-utm
```

Key Findings:

- Multiple Authentication failures observed for john.smith
- Escalated privileges as root user using su command
- Created a new backdoor account named “system-utm” and added it into group named “users”
- No further activity is observed for newly created backdoor account “system-utm”

6. Indicators of Compromise (IOCs)

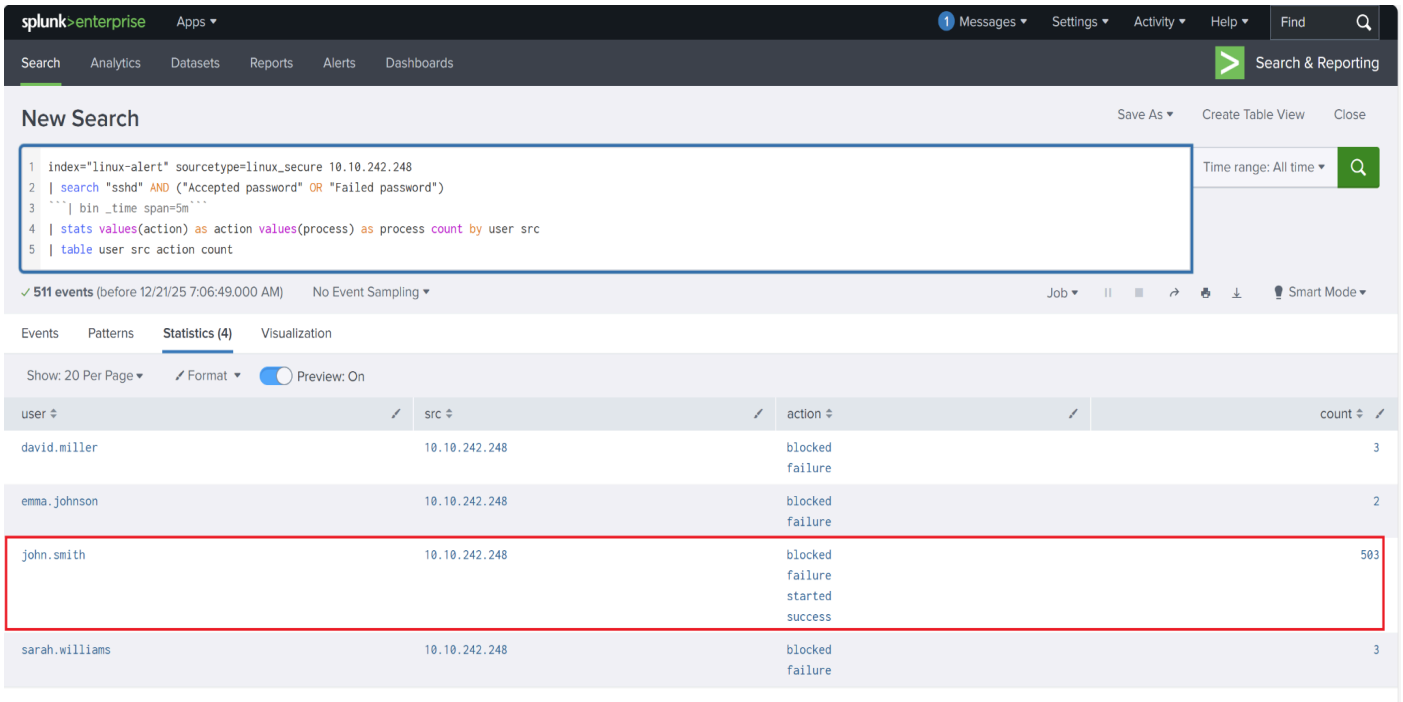
Indicator Type	Value	Context
IP Address	10.10.242.248	Attacker IP
User	john.smith	Compromised User Account
New User	system-utm	Backdoor user created
Group Modification	users	System-utm is added to the users group

7. MITRE ATT&CK Mapping

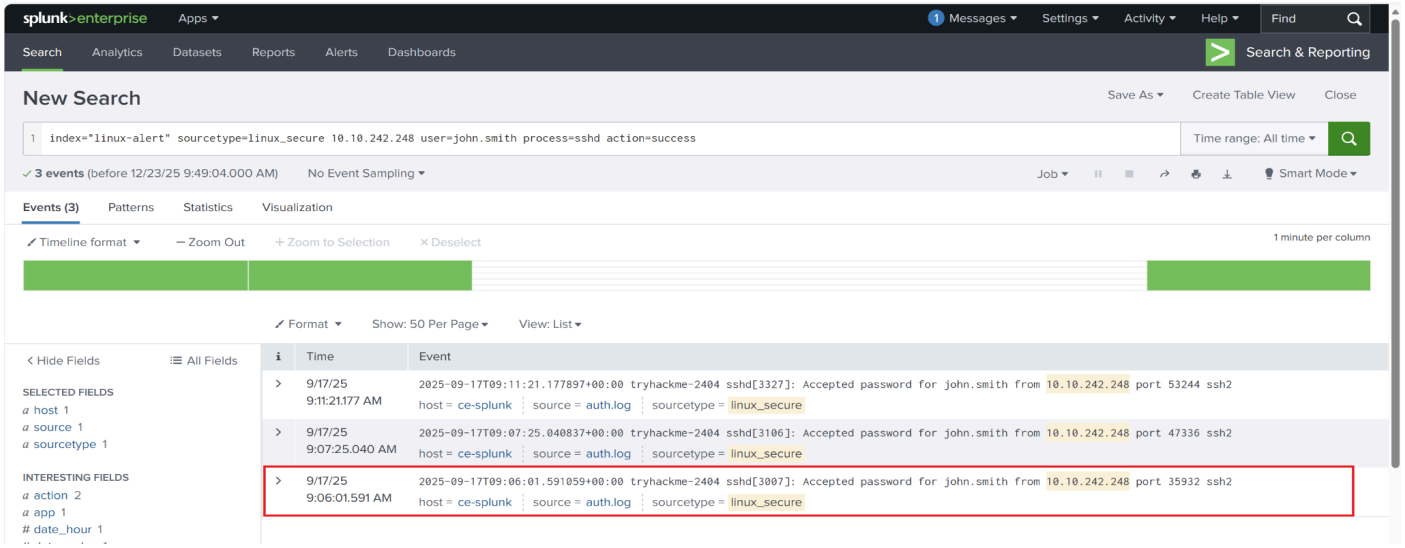
- **T1110 (Bruteforce):** The attacker performed a brute force attack against john.smith over SSH.
- **T1136 (Create Account):** The attacker created the backdoor account system-utm.
- **T1098 (Account Manipulation):** Adding system-utm to the users group.

8. Evidence Screenshots

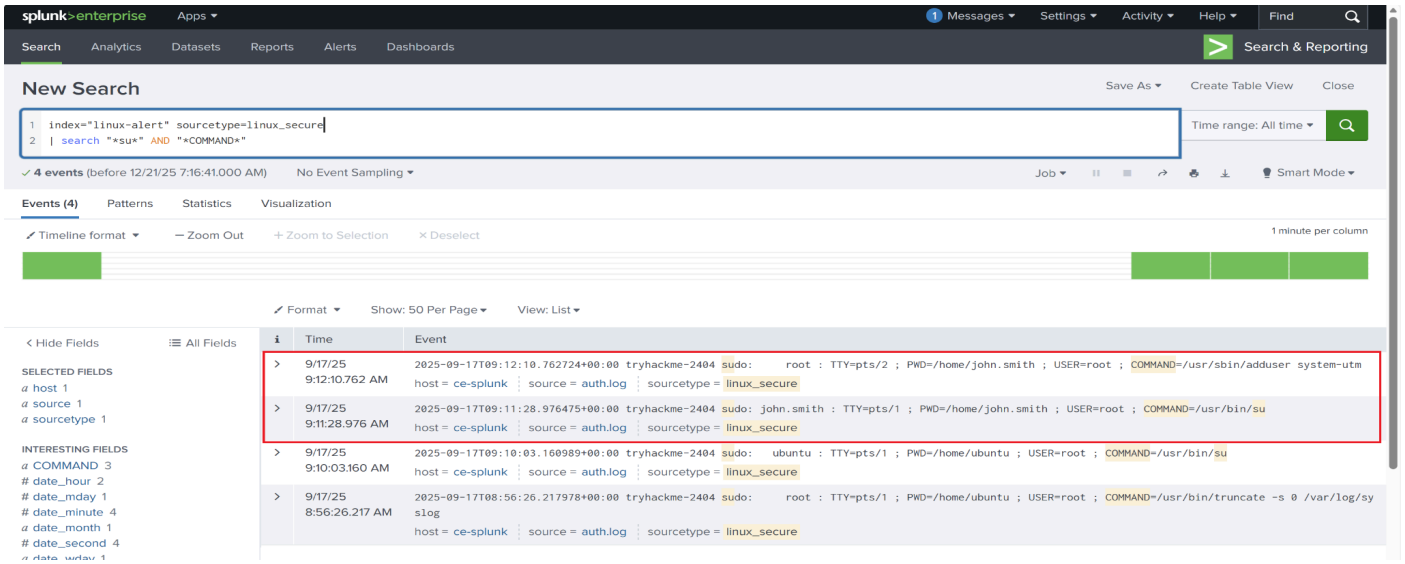
Splunk query determining the compromised user:



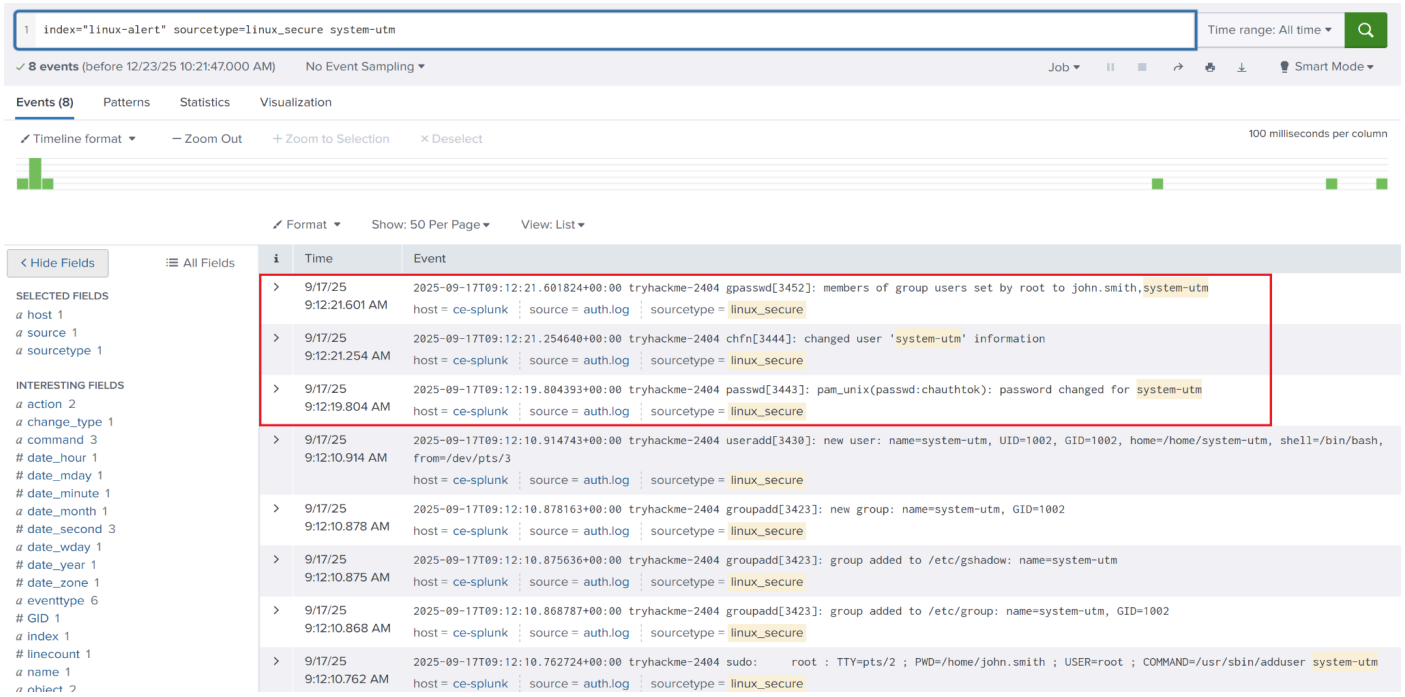
Splunk query showing the successful compromised user(john.smith) login:



Splunk query showing Privilege Escalation Attempts and New Backdoor user creation:



Splunk query showing Backdoor account modifications:



8. Recommendations & Remediation

- Isolate tryhackme-2404 from network
- Reset Credentials for the user “john.smith”
- Delete the newly created backdoor user named “system-utm”
- Hunt for Attacker IP across all systems using EDR
- Block the Attacker IP 10.10.242.248 in the firewall.