



Capstone

**Bryant Aguirre
Gulnaz Mukanbetova
Josh Philip
Rishi Nalam**

CYB102 | Intermediate Cybersecurity

SSH Brute Force IP/User/Password

Attacks from the internet on an SSH server.



Data Card Code (1) Discussion (0) Suggestions (0)

About Dataset

Context

I set up an SSH server, enabled password SSH authentication, and exposed port 22 to the internet. This data is from a little bit under a week of activity, updated versions will be posted in the future.

Content

1. Username the attacker used to try and authenticate, most went for root.
2. Foreign IP address that the attack came from.
3. Date of the attack.
4. Passwords used.

Inspiration

This was an excellent read, but I wanted some more up to date data:
http://people.scs.carleton.ca/~paulv/papers/passwords_full.pdf

brute_force_data.json (4.83 MB)

About this file

This is data related to the widespread brute force attempts from the internet. The username is the user account that the ssh attempt tried to use. Foreign IP is the IP address the attempt came from, and passwords is an array of the passwords that the attacker used. Password fields include Unicode.

There were other attempts not included here, which broadly fell into two categories: attempts with a key, and attempts that entered no username or password. This dataset only includes attempts using password authentication.

The data set we have chosen to analyze for The Data Dig is...

This dataset comes from a user who set up an SSH server specifically to collect login activity for research.

The logs mainly capture network-based attacks, especially brute-force attempts where attackers try many username and password combinations to gain access. It was created to study how these attacks behave in real environments.

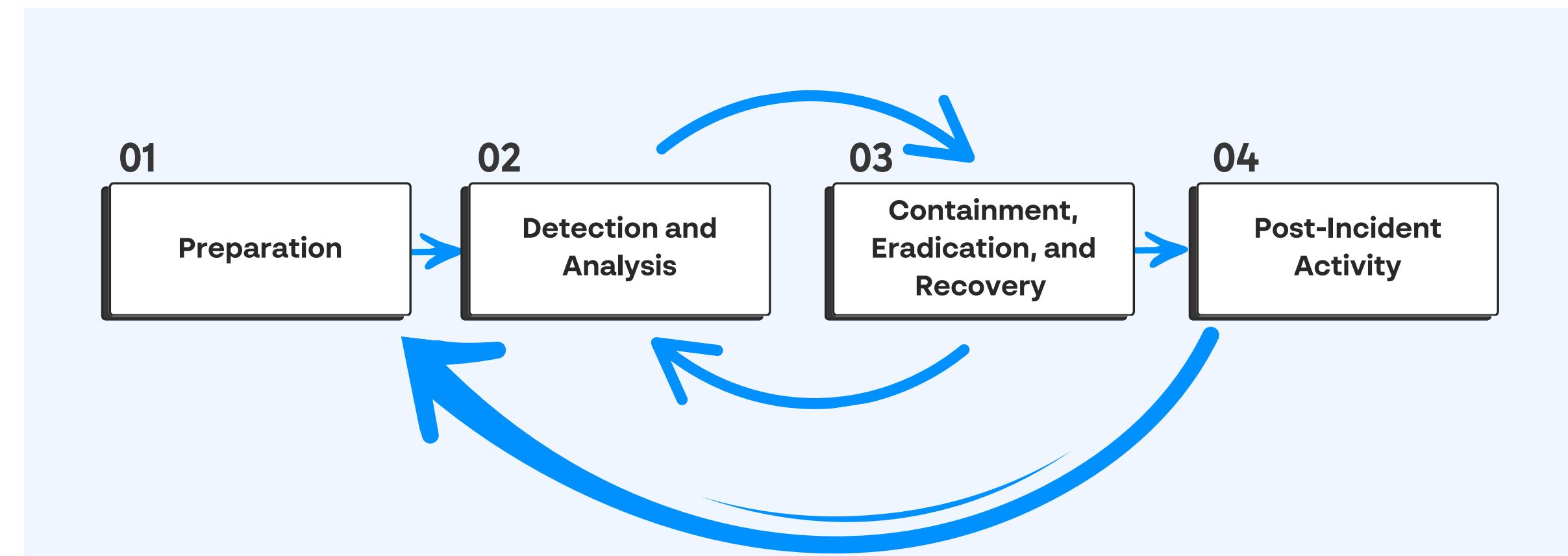


Tools Used

- Splunk
- Catalyst: to document all the findings with artefacts, so we can properly do step 4. Learn
- Virus Total



The playbook we have decided
to follow for The Data Dig is...



NIST Special Publication 800 NIST SP 800-61r3 Incident Response Recommendations
and Considerations for Cybersecurity Risk Management A CSF 2.0 Community Profile

What happened?

Key Findings



Description of the incident

The screenshot shows a ticket management interface with the following details:

- Tickets / 8384**: The current ticket number is 8384.
- Incidents**: A dropdown menu showing the current selection.
- + NEW INCIDENT**: A button to create a new incident.
- CAQL**: A search bar with the query `status == 'open' AND (owner == 'admin' OR !owner)`.
- Search icon**: A magnifying glass icon.
- Table Headers**: Name, Status, Owner, Creation, Last Modification.
- Table Data**: One row for "Incident #8384: Brute Force Login Attempt Investigation" by owner "admin".
- Row Actions**: Open, Edit, Delete, Log, Details, and other icons.
- Rows per page**: Set to 10.
- Page Number**: 1-1 of 1.
- Incident Detail Page**:
 - Title**: Incident #8384: Brute Force Login Attempt Investigation
 - Status**: Open · Created: 2025-11-19 03:49:14 · Last Modified: 2025-11-19 03:53:59
 - Owner**: admin
 - Playbooks**: NIST 800-61 Incident Response Playbook
 - Description**: We are analyzing a brute-force authentication dataset as part of the CYB102 Data Dig project. The dataset contains login attempts (failed and successful). We will use Splunk to identify patterns, suspicious IPs, and potential compromise. After Splunk analysis, specific attacker IPs, usernames, and timestamps will be added.
 - Log**: Add a comment... (with a placeholder "CreateTicket - admin - today, 03:49 PM")
 - Save Details**: A button to save the incident details.
 - Severity**: Medium
 - TLP**: Green
 - Change Template**: A link to change the incident template.
 - Details**: A section for additional incident information.
 - References**: A section for references.
 - Artifacts**: A section for artifacts.
 - Related Tickets**: A section for related tickets.
 - Files**: A section for files.

We are analyzing a dataset that captures brute-force authentication activity against an SSH server. The data includes both failed and successful login attempts, allowing us to observe attacker behavior and login patterns. Splunk will be used to investigate the logs, identify suspicious IP addresses, detect targeted usernames, and determine whether any compromises occurred. Once the analysis is complete, we will add the specific attacker IPs, targeted accounts, and timestamps to this incident for full documentation.

First NIST Steps + Tools Used During Investigation

Identify → Detect → Analyze steps



Early Incident Analysis Results

Tickets / 8384

Incidents + NEW INCIDENT

CAQL status == 'open' AND (owner == 'admin' OR !owner)

Name	Status	Owner	Creation	Last Modification
Incident #8384: Brute Force Login Attempt Investigation	Open	admin	2025-11-19 03:49:14	2025-11-19 03:49:14

Rows per page: 10 1-1 of 1 < >

Incident #8384: Brute Force Login Attempt Investigation

Open · 2025-11-19 03:49:14 · 2025-11-19 04:24:47

Details CHANGE TEMPLATE

Severity TLP

Medium Green

Description

We are analyzing a brute-force authentication dataset as part of the CYB102 Data Dig project. The dataset contains login attempts (failed and successful). We will use Splunk to identify patterns, suspicious IPs, and potential compromise. After Splunk analysis, specific attacker IPs, usernames, and timestamps will be added.

SAVE DETAILS

Log

Add a comment... >

admin today, 04:20 PM DETECT & ANALYZE: Used Splunk to count attacks by foreign_ip. Identified top attacker IPs attempting multiple logins. Reviewing targeted usernames for patterns.

admin today, 04:20 PM DETECT & ANALYZE: Used Splunk to count attacks by foreign_ip. Identified top attacker IPs attempting multiple logins. Reviewing targeted usernames for patterns.

admin today, 04:17 PM IDENTIFY: Uploaded dataset into Splunk and confirmed successful ingestion. Initial review of events shows SSH login attempts with usernames, timestamps, and foreign IP addresses.

admin today, 03:58 PM IDENTIFY: We are reviewing authentication logs for suspicious login attempts.

DETECT & ANALYZE: We will use Splunk to search for failed logins, attacker IPs, and any successful brute-force patterns.

Owner admin

Playbooks

NIST 800-61 Incident Response Playbook

Identify — Gather Initial Information
Detect & Analyze — Investigate Indicators
Contain — Limit Damage and Prevent Spread

References

Artifacts

116.31.116.42
Unknown ?
Username targeted the most - root #14007
Unknown ?

Related Tickets

Files

X CLOSE HANDBOOK

Using Splunk, we were able to identify the attacker's IP address, the targeted username, and confirm that this specific IP was repeatedly attempting to log in to that user account.

splunk>enterprise Apps ▾

Messages ▾ Settings ▾ Activity ▾ Help ▾ Q Find

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

New Search

Save As ▾ Create Table View Close

```
1 index=main
2 | stats count by foreign_ip
3 | sort - count
```

All time ▾

67,043 events (before 11/19/25 4:18:25.000 PM) No Event Sampling ▾

Job ▾ II ⌂ ⌄ ⌅ ⌆ ⌇ Smart Mode ▾

Events Patterns Statistics (303) Visualization

20 Per Page ▾ Format Preview ▾

foreign_ip ▾ 1 2 3 4 5 6 7 8 ... Next >

foreign_ip	count
116.31.116.42	2805

splunk>enterprise Apps ▾

Messages ▾ Settings ▾ Activity ▾ Help ▾ Q Find

Search Analytics Datasets Reports Alerts Dashboards > Search & Reporting

New Search

Save As ▾ Create Table View Close

```
1 index=main
2 | stats count by username
3 | sort - count
```

All time ▾

67,043 events (before 11/19/25 4:23:33.000 PM) No Event Sampling ▾

Job ▾ II ⌂ ⌄ ⌅ ⌆ ⌇ Smart Mode ▾

Events Patterns Statistics (441) Visualization

20 Per Page ▾ Format Preview ▾

username ▾ 1 2 3 4 5 6 7 8 ... Next >

username	count
root	14007

New Search

Save As ▾ Create Table View Close

```
1 index=main
2 | stats count by foreign_ip username
3 | sort - count
```

All time ▾

67,043 events (before 11/19/25 4:28:17.000 PM) No Event Sampling ▾

Job ▾ II ⌂ ⌄ ⌅ ⌆ ⌇ Smart Mode ▾

Events Patterns Statistics (812) Visualization

20 Per Page ▾ Format Preview ▾

foreign_ip ▾ username ▾ 1 2 3 4 5 6 7 8 ... Next >

foreign_ip	username	count
116.31.116.42	root	2805

VirusTotal Screenshot of the Attacker IP

The screenshot shows the VirusTotal analysis interface for the IP address 116.31.116.42. The main header bar includes a search input, a file upload icon, and various navigation and account options. The main content area displays a summary card with a community score of 0/95, a note that no security vendor flagged the IP as malicious, and details about the IP (116.31.116.42, AS 4134, China). Below this is a navigation bar with tabs: DETECTION (selected), DETAILS, RELATIONS, and COMMUNITY. A green banner encourages joining the community for additional insights. The main table lists 25 security vendors' analysis results, all marked as unrated.

Security vendors' analysis		Do you want to automate checks?	
0xSl_f33d	? Unrated	Abusix	? Unrated
Acronis	? Unrated	ADMINUSLabs	? Unrated
AI Labs (MONITORAPP)	? Unrated	AlienVault	? Unrated
alphaMountain.ai	? Unrated	AlphaSOC	? Unrated
Antiy-AVL	? Unrated	ArcSight Threat Intelligence	? Unrated
AutoShun	? Unrated	Axur	? Unrated
benkow.cc	? Unrated	Bfore.Ai PreCrime	? Unrated
BitDefender	? Unrated	Bkav	? Unrated
Blueliv	? Unrated	Certego	? Unrated
ChainPatrol	? Unrated	Chong Lua Dao	? Unrated
CINS Army	? Unrated	Cluster25	? Unrated
CMC Threat Intelligence	? Unrated	CRDF	? Unrated
Criminal IP	? Unrated	CSIS Security Group	? Unrated
Cyan	? Unrated	Cyble	? Unrated
CyRadar	? Unrated	desenmascara.me	? Unrated
DNS8	? Unrated	Dr.Web	? Unrated
EmergingThreats	? Unrated	Emsisoft	? Unrated

Containment, eradication and recovery

CONTAINMENT:

We blocked the attacker IPs to stop more login attempts. We also locked the user accounts that were being targeted and added limits on how many login attempts can happen in a short time. These actions helped stop the brute-force attack and prevented any further damage.

ERADICATION:

We would reset passwords and change our password policies to make them stronger. We would turn on MFA (Multifactor Authentication to make logins more secure. We would also nullify any unauthorized sessions accessed by the attacker.

To enhance network security, we would update firewall rules to block any malicious IP address ranges and make sure no suspicious SSH keys, accounts, or settings were left behind. This ensures the attacker is fully removed from the system.

RECOVERY:

After removing the attacker and securing the accounts, we would restore normal access for users. Any locked accounts would be unlocked once passwords were reset and MFA was enabled. We would keep monitoring Splunk for any new suspicious login attempts to make sure the attack doesn't return.

We'd also confirm that the updated firewall rules, stronger authentication settings, and system changes are working correctly. Once everything is stable and no new threats appear, the system can safely return to normal operation.

We would also begin a series of mandatory seminars to educate employees on proper security hygiene and identifying suspicious behavior effective immediately. Afterall, security is maximized when technology, process and PEOPLE are all functioning cohesively.

STEPS DONE IN CATALYST

The screenshot displays the Catalyst platform's incident management interface. On the left, a sidebar shows a list of incidents, with one specific entry highlighted: "Incident #8384: Brute Force Login Attempt Investigation". The main panel shows the details of this incident.

Incident Details:

- Name:** Incident #8384: Brute Force Login Attempt Investigation
- Status:** Open
- Owner:** admin
- Creation:** 2025-11-19 03:49:14
- Last Modification:** 2025-11-19 04:37:23

Description:

We are analyzing a brute-force authentication dataset as part of the CYB102 Data Dig project. The dataset contains login attempts (failed and successful). We will use Splunk to identify patterns, suspicious IPs, and potential compromise. After Splunk analysis, specific attacker IPs, usernames, and timestamps will be added.

Log:

Add a comment...

admin today, 04:37 PM

RECOVER:

After removing the attacker and securing the accounts, we would restore normal access for users. Any locked accounts would be unlocked once passwords were reset and MFA was enabled. We would keep monitoring Splunk for any new suspicious login attempts to make sure the attack doesn't return. We'd also confirm that the updated firewall rules, stronger authentication settings, and system changes are working correctly. Once everything is stable and no new threats appear, the system can safely return to normal operation.

Owner: admin

Playbooks:

- NIST 800-61 Incident Response Playbook
 - Identify — Gather Initial Information
 - Detect & Analyze — Investigate Indicators
 - Contain — Limit Damage and Prevent Spread
 - Eradicate — Remove the Threat
 - Recover — Restore Normal Operations
 - Post-Incident — Lessons Learned

References:

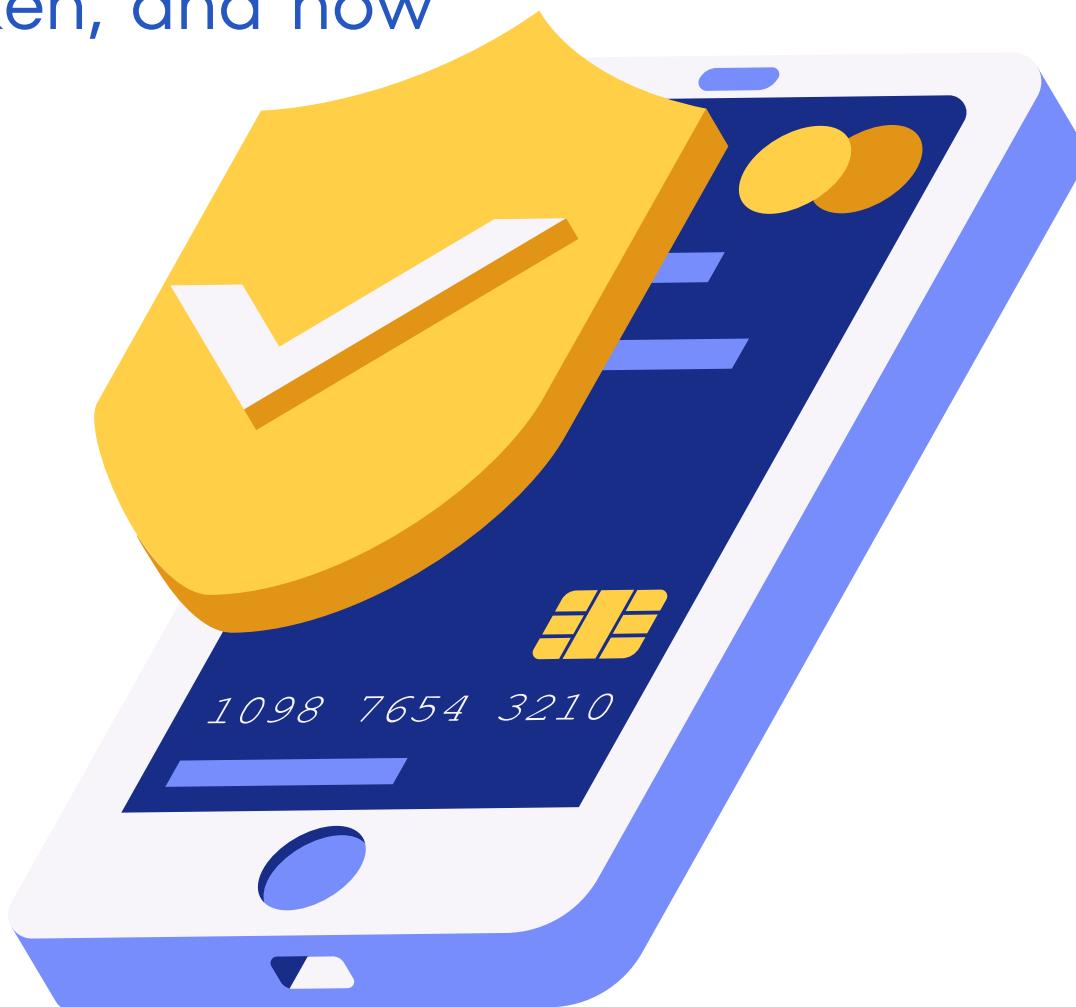
- 116.31.116.42
- Unknown ?
- Username targeted the most - root #14007
- Unknown ?
- IP: 16.31.116.42 Target; root # of attacks: 2805
- Unknown ?

Post-Incident Documentation & Remediation

After the incident was contained and the user's account was secured, we would review everything that happened and document the full timeline of events. This includes the attacker IP, the attempted logins, what actions were taken, and how the account was restored.

What could be improved:

- adding stronger lockout policies,
- enabling MFA by default,
- improving monitoring alerts for repeated failed logins.



Final Steps in Catalyst

Tickets / 8384

Incidents + NEW INCIDENT

CAQL status == 'open' AND (owner == 'admin' OR !owner)

Name	Status	Owner	Creation	Last Modification
Incident #8384: Brute Force Login Attempt Investigation	Open	admin	2025-11-19 03:49:14	2025-11-19 04:39:50

Rows per page: 10 1-1 of 1 < >

Incident #8384: Brute Force Login Attempt Investigation

Closed · 2025-11-19 03:49:14 · 2025-11-19 04:39:50

Details CHANGE TEMPLATE

Severity TLP
Medium Green

Description

We are analyzing a brute-force authentication dataset as part of the CYB102 Data Dig project. The dataset contains login attempts (failed and successful). We will use Splunk to identify patterns, suspicious IPs, and potential compromise. After Splunk analysis, specific attacker IPs, usernames, and timestamps will be added.

SAVE DETAILS

Log

Add a comment...

admin today, 04:38 PM

POST-INCIDENT:

After the incident was contained and the user's account was secured, we would review everything that happened and document the full timeline of events. This includes the attacker IP, the attempted logins, what actions were taken, and how the account was restored. We would also note what worked well and what could be improved, such as adding stronger lockout policies, enabling MFA by default, and improving monitoring alerts for repeated failed logins. These lessons help prevent similar brute-force attacks in the future and strengthen the overall security of the system.

admin today, 04:37 PM

RECOVER:

After removing the attacker and securing the accounts, we would restore normal access for users. Any locked accounts would be unlocked once passwords were reset and MFA was enabled. We would keep monitoring Splunk for any new suspicious login attempts to make sure the attack doesn't return. We'd also confirm that the updated firewall rules, stronger authentication settings, and system changes are working correctly. Once everything is stable and no new threats appear, the system can safely return to normal operation.

admin today, 04:35 PM

ERADICATE:

We would reset passwords for all affected accounts and require stronger passwords. We would turn on MFA to make logins more secure. We'd also clear out any unauthorized sessions or access the attacker might have gained. On the network side, we would update firewall rules to block any related malicious IP ranges and make sure no suspicious SSH keys, accounts, or settings were left behind. This ensures the attacker is fully removed from the system.

Owner admin

Playbooks

NIST 800-61 Incident Response Playbook

Gather Initial Information → Detect & Analyze → Investigate Indicators → Contain → Limit Damage and Prevent Spread → Eradicate → Remove the Threat → Recover → Restore Normal Operations → Post-Incident → Lessons Learned → Finish the Incident

Identify — Gather Initial Information

Detect & Analyze — Investigate Indicators

Contain — Limit Damage and Prevent Spread

Eradicate — Remove the Threat

Recover — Restore Normal Operations

Post-Incident — Lessons Learned

Finish the Incident

References

Artifacts

116.31.116.42

Unknown ?

Username targeted the most - root #14007

Unknown ?

IP: 16.31.116.42 Target; root # of attacks: 2805

Unknown ?

Related Tickets

Files



Thank You!

Pod 79