

AGENT : lp-user-02

MITRE ATT&CK

Top Tactics

Credential Access 429

Lateral Movement 275

Defense Evasion 21

Privilege Escalation 18

Initial Access 13

1. INITIAL ACCESS

Initial Access

T1078 13

T1021 3

A. Remote Services

Technique details

ID

T1021

Tactics

Lateral Movement

Version

1.3

Recent events

3 hits

| Time (UTC) | Source IP | Geo | User | MITRE | Tactic | Outcome | |
|---------------------|---------------|-----------------|--------|--------------|---------------------------------|-------------------|--|
| | | | | s | e | | |
| 2024-09-02T20:21:59 | 34.226.207.84 | Ashburn, VA, US | ctfroo | T1078, T1021 | Valid Accounts, Remote Services | SSH login success | |
| 2024-09-02T20:25:52 | 52.5.37.24.3 | Ashburn, VA, US | ctfroo | T1078, T1021 | Valid Accounts, Remote Services | SSH login success | |

| | | | | | | |
|---------------------|----------|----------|---------|--------------|---------------------------------|-------------------|
| 2024-09-02T21:02:43 | 10.0.1.1 | Internal | ctfroom | T1078, T1021 | Valid Accounts, Remote Services | SSH login success |
|---------------------|----------|----------|---------|--------------|---------------------------------|-------------------|

1. Executive Summary (Findings So Far)

Incident summary:

These three Wazuh events show **successful SSH logins** into the Ubuntu system **lp-user-02 (10.0.1.14)** under the account **ctfroom**.

They originate from **multiple external IPs** (AWS-hosted, Ashburn, VA), suggesting that:

- The attacker gained or brute-forced valid credentials.
- They used them for **remote access (T1021 – Remote Services)**.
- This represents the **initial access** phase and possible **lateral movement** within the internal network.

🧠 2. Interpretation

A. Initial Access

The first two external logins (from AWS IPs) are your **compromise point**. They mark **initial access via SSH using valid credentials**(T1078).

Evidence:

- Multiple distinct IPs in short succession.
- Successful authentication to a named user (**ctfroom**).
- External IPs (52.5.37.243, 34.226.207.84) not likely part of your org infrastructure.
- Wazuh mapped this to **MITRE ATT&CK techniques**:
 - **T1078 - Valid Accounts**
 - **T1021 - Remote Services**

→ The adversary already had or guessed the **ctfroom password**.

B. Lateral Movement

The **third login** (from **10.0.1.13**) suggests internal pivoting:

- Indicates another compromised internal host (perhaps a Windows or Linux system).
- Internal pivot = lateral movement across network.

→ At this point, the adversary is using internal foothold to expand access.

C. Credential Reuse or Shared Key

Given that all logins are for **ctfroom**, possibilities:

1. Shared or reused password between internal systems.
2. Attacker dumped creds from Windows host and reused them here.
3. Attacker might have inserted their own SSH key for persistence (to check next).



3. Indicators of Compromise (IoCs)

| Type | Value | Context |
|------------|--------------------------|--|
| IP Address | 34.226.207.84 | AWS / Amazon EC2 (Ashburn, VA) — attacker origin |
| IP Address | 52.5.37.243 | AWS / Amazon EC2 (Ashburn, VA) — attacker origin |
| IP Address | 10.0.1.13 | Internal pivot host — likely compromised |
| Username | ctfroom | Compromised local user |
| Process | sshd | Used for remote access |
| Log Path | /var/log/auth.log | Evidence source |
| MITRE IDs | T1078, T1021 | Valid Accounts / Remote Services |

You should **block and investigate** connections from the two AWS IPs across all systems.



4. Likely Attack Sequence (Timeline)

| Timestamp (UTC) | Event | Description |
|----------------------------|------------------------------|---|
| 2024-09-02T20:21:59 | SSH login from 34.226.207.84 | External attacker logs in with stolen credentials. |
| 2024-09-02T20:25:52 | SSH login from 52.5.37.243 | Possibly same attacker from different AWS instance confirms access. |
| 2024-09-02T21:02:43 | SSH login from 10.0.1.13 | Internal lateral movement from another compromised host. |

APT1337 Canary reused valid credentials (likely harvested from your Windows host) to laterally move into the Ubuntu server using SSH, establishing remote shell access under the compromised **ctfroom** account.

Initial Access – Remote Services (Ubuntu Host: Ip-user-02)

The investigation into the Ubuntu server **Ip-user-02 (10.0.1.14)** revealed that the attacker gained initial access through **valid SSH credentials**, specifically by logging into the **ctfroom** account. Wazuh telemetry shows multiple successful SSH authentications from **two external AWS-based IPs** (34.226.207.84 and 52.5.37.243, both located in Ashburn, Virginia, USA) within minutes of each other, followed shortly by an **internal SSH login from 10.0.1.13**, indicating **lateral movement from another compromised host**. These logins were classified under MITRE ATT&CK techniques **T1078 (Valid Accounts)** and **T1021 (Remote Services)**. The pattern suggests that the adversary, likely **APT1337 Canary**, had already obtained or brute-forced the **ctfroom** password—possibly from the earlier Windows compromise—and then used it to establish persistence and pivot deeper into the network. At this stage, there is no evidence of privilege escalation or persistence mechanisms yet, but the SSH activity confirms a **successful foothold via remote services**, marking the start of the intrusion on the Ubuntu environment.

POC

The screenshot shows a web-based endpoint monitoring interface. At the top, there are tabs for Threat Hunting, File Integrity Monitoring, Configuration Assessment, MITRE ATT&CK, and Malware Detection. The current tab is 'Endpoints'.

In the center, there is a summary card for 'ip-user-02'. It displays the following details:

- ID: 001
- Status: disconnected
- IP address: 10.0.1.14
- Version: Wazuh v4.8.2

Below the summary card, there are two main sections:

- MITRE ATT&CK:** A circular chart titled "Compliance" with three segments: green, light blue, and grey.
- Events count evolution:** A line chart showing the count of events over time, ranging from 0 to 2,000. The chart shows a sharp increase starting around 1,500 events.

To the right of these sections is a large panel titled "Remote Services". It contains a table with the following columns: Table, JSON, and Rule. The table lists several log entries:

| Table | JSON | Rule |
|--------------------------|--|------|
| @timestamp | 2024-09-02T20:40:43.592Z | |
| GeoLocation.city_name | Ashburn | |
| GeoLocation.country_name | United States | |
| GeoLocation.location.lat | 39.0481 | |
| GeoLocation.location.lon | -77.4728 | |
| GeoLocation.region_name | Virginia | |
| _id | Azh4tJEbc-M2AH08F1qF | |
| agent.id | 001 | |
| agent.ip | 10.0.1.14 | |
| agent.name | ip-user-02 | |
| data.dstuser | ctfroom | |
| data.srcip | 52.5.37.243 | |
| data.srcport | 33528 | |
| decoder.name | sshd | |
| decoder.parent | sshd | |
| full_log | 2024-09-02T20:25:52.091761+00:00 ip-10-0-1-14 sshd[4266]: Accepted password for ctfroom from 52.5.37.243 port 33528 ssh2 | |
| id | 1725309643.77984 | |
| input.type | log | |
| location | /var/log/auth.log | |
| mapbox_name | wazuh-explorer | |

This screenshot shows the same web-based endpoint monitoring interface as the first one, but with different log entries in the "Remote Services" panel.

The "Remote Services" panel table now includes the following log entries:

| Table | JSON | Rule |
|--------------------------|--|------|
| @timestamp | 2024-09-02T20:40:43.571Z | |
| GeoLocation.city_name | Ashburn | |
| GeoLocation.country_name | United States | |
| GeoLocation.location.lat | 39.0481 | |
| GeoLocation.location.lon | -77.4728 | |
| GeoLocation.region_name | Virginia | |
| _id | Jh4tJEbc-M2AH08F1mF | |
| agent.id | 001 | |
| agent.ip | 10.0.1.14 | |
| agent.name | ip-user-02 | |
| data.dstuser | ctfroom | |
| data.srcip | 34.226.207.84 | |
| data.srcport | 51690 | |
| decoder.name | sshd | |
| decoder.parent | sshd | |
| full_log | 2024-09-02T20:21:59.118949+00:00 ip-10-0-1-14 sshd[4123]: Accepted password for ctfroom from 34.226.207.84 port 51690 ssh2 | |
| id | 1725309643.75668 | |
| input.type | log | |
| location | /var/log/auth.log | |

The screenshot shows the Wazuh endpoint monitoring interface for agent 001. The top navigation bar includes Threat Hunting, File Integrity Monitoring, Configuration Assessment, MITRE ATT&CK, and Malware Detection. The current tab is Endpoints, with sub-tab ip-user-02 selected. On the left, there's a sidebar with sections for Threat Hunting, File Integrity Monitoring, Configuration Assessment, MITRE ATT&CK, and Malware Detection. The main area displays a 'Remote Services' table with columns for Table, JSON, and Rule. The table lists various service details such as timestamp, ID, agent information, and log entries. A specific log entry is highlighted:

```

@timestamp 2024-09-02T21:02:44.744Z
_id fzIMtJEbc-M2AH08H4vS
agent.id 001
agent.ip 10.0.1.14
agent.name ip-user-02
data.dsuser ctfrom
data.scp 10.0.1.13
data.scpport 45190
decoder.name sshd
decoder.parent sshd

```

Below the table is a 'Filter for value' input field set to '/_log'. The log entry shown is:

```

2024-09-02T21:02:43.583258+00:00 ip-10-0-1-14 sshd[5101]: Accepted password for ctfrom from 10.0.1.13 port 45190
ssh2

```

This screenshot shows the same Wazuh interface for agent 001, but the 'Technique details' section is expanded under the 'Remote Services' table. The 'Technique details' section includes fields for ID (T1021), Tactics (Lateral Movement), and Version (1.3). Below this, the 'Recent events' section shows three hits for technique T1021, with a search bar and a date range from May 1, 2024 to Dec 1, 2025. The events listed are:

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|--|-------|---------|-------------------------------|
| Sep 3, 2024 @ 00:02:44.744 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |
| Sep 2, 2024 @ 23:40:43.592 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |
| Sep 2, 2024 @ 23:40:43.571 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |

B . Valid Accounts

Technique details

ID

[T1078](#)

Tactics

[Persistence](#)

[Privilege Escalation](#)

Defense Evasion

Initial Access

Version

2.6

Recent events

13 hits

Findings Overview

Between 2024-09-02 20:21:59 and 21:03:03 UTC, the Ubuntu host **Ip-user-02 (10.0.1.14)** recorded a sequence of **successful SSH and privilege escalation events** involving the local user account **ctfroom**. The telemetry clearly indicates the attacker **used legitimate credentials** to gain access—either stolen, reused, or brute-forced—rather than exploiting a vulnerability. This aligns with **APT1337 Canary's known tradecraft**, which emphasizes stealthy credential use and living-off-the-land techniques.

Findings (what we know from the logs)

- The Ubuntu host **Ip-user-02 (10.0.1.14)** was accessed using **valid credentials** for the local account **ctfroom**.
- Successful SSH sessions originated from **external AWS IPs (34.226.207.84, 52.5.37.243)** and later from an **internal host (10.0.1.13)** — indicating **initial external compromise followed by lateral movement**.
- Immediately after interactive SSH shells were established, **ctfroom** executed **sudo** and **su** actions and gained **root (uid=0)**. This confirms **privilege escalation** using existing account rights.
- Wazuh rules firing: **5501 (PAM: Login session opened)** and **5715 (sshd: authentication success)** mapped to MITRE **T1078 (Valid Accounts)** and **T1021 (Remote Services)**.
- The pattern is consistent with credential theft or reuse (credentials likely harvested elsewhere — e.g., the Windows host) and “living off the land” activity (using native SSH + sudo).

Key Observations and Timeline

| Timestamp (UTC) | Source IP | Event Description | Technique | Notes |
|--------------------|-----------|-------------------|-----------|-------|
|--------------------|-----------|-------------------|-----------|-------|

| | | | | |
|----------|---|--|---|--|
| 20:21:59 | 34.226.207.84 (Ashburn, VA, USA) | SSH authentication success for user ctfroom | T1078 / T1021 | First observed remote access from AWS-based IP. Legit credentials likely already compromised. |
| 20:21:59 | (same session) | PAM session opened for ctfroom(uid=1001) | T1078 | Indicates full shell access established. |
| 20:25:52 | 52.5.37.243 (Ashburn, VA, USA) | SSH authentication success for ctfroom | T1078 / T1021 | Second connection within minutes from another AWS IP—possibly redundancy or multi-hop testing. |
| 21:02:43 | 10.0.1.13 (internal) | SSH login success for ctfroom | T1078 / T1021 | Suggests lateral movement from another compromised internal host. |
| 21:03:03 | (local activity) | ctfroom(uid=1001) escalated privileges via sudo and su to root(uid=0) | T1078 / T1068 (Privilege Escalation) | Confirmed successful privilege escalation using existing sudo rights. Root-level shell obtained. |

Indicators of Compromise (IOCs)

| Type | Indicator | Description |
|--|---------------------------|--|
| External IP (C2 / Initial Access) | 34.226.207.84 | AWS IP (Ashburn, VA) used for SSH login. |
| External IP (C2 / Initial Access) | 52.5.37.243 | AWS IP (Ashburn, VA) used for secondary SSH access. |
| Internal IP (Lateral Movement) | 10.0.1.13 | Another compromised host initiating SSH session. |
| Compromised Account | ctfroom | Used for SSH and privilege escalation to root. |
| System Affected | lp-user-02 (10.0.1.14) | Ubuntu server compromised via SSH and root escalation. |

IOCs (capture/block immediately)

- Username: **ctfroom** (compromised account)
- External source IPs: **34.226.207.84, 52.5.37.243** (both AWS / Ashburn region)
- Internal pivot IP: **10.0.1.13**

- Host: **Ip-user-02 (10.0.1.14)**
- Log source / evidence: **/var/log/auth.log** (Wazuh rule IDs **5501, 5715**)
- Event types: **sshd: authentication success**, **PAM: Login session opened**, **sudo/su session opened**

Observed pattern (behavioral summary)

- **Credential-based access:** attacker used legitimate credentials (T1078) rather than exploiting a service vulnerability.
- **Multi-hop access:** external AWS endpoints used to access host; subsequent internal SSH from 10.0.1.13 indicates pivoting.
- **Rapid privilege escalation:** **ctfroom** had sudo rights and escalated to root soon after login (high impact).
- **Potential cross-host credential harvesting:** likely credentials were obtained from other compromised host(s) (correlate with Windows logs).
- **Living-off-the-land:** use of built-in tools (sshd, sudo, su) keeps activity low/noise and harder to detect.

Was anything suspicious or malicious so far?

Yes — **malicious activity is evident:**

- Successful external SSH logins from AWS IPs to a local account, followed by immediate **root escalation** through **sudo/su** is a clear compromise and high-fidelity indicator of attacker control.
- The presence of multiple external IPs and an internal pivot host strongly indicate **active malicious intrusion** rather than benign admin activity.
- No evidence yet in these logs of file exfiltration or persistence artifacts, but root access means the attacker *could* have deployed persistence, modified files, or exfiltrated data — you must investigate those next.

Short synthesis (paste-ready)

Between **Sep 2–3, 2024** the Wazuh events for host **Ip-user-02 (10.0.1.14)** show repeated **PAM session openings** (rule **5501**) and multiple **sshd authentication successes** (rule **5715**) mapped to MITRE **T1078 (Valid Accounts)** and **T1021 (Remote Services)**. The events cluster tightly around two windows of activity and include both external AWS IPs and an internal host — consistent with an attacker using **stolen or reused credentials** to log in over SSH and then escalate to root (sudo/su). The repeated PAM entries indicate interactive shell sessions and local privilege elevation, while the **sshd: authentication success** entries indicate the remote-service vector. In short: the adversary obtained valid access to the **ctfroom** account, used it to access Ip-user-02 via SSH, and successfully elevated privileges — a classic credential-based initial access followed by lateral movement and privilege escalation.

Short summary paragraph you can present to stakeholders

Between **Sep 2–3, 2024**, Wazuh logs demonstrate that the account **ctfroom** was used to gain interactive SSH access to the Ubuntu server **Ip-user-02 (10.0.1.14)** from two external AWS IP addresses and later from an internal host (10.0.1.13). Immediately after these SSH sessions, **ctfroom** used **sudo** and **su** to obtain a root shell. The activity maps to MITRE techniques **T1078 (Valid Accounts)** and **T1021 (Remote Services)** and indicates a credential-based compromise followed by lateral movement and privilege escalation. This is confirmed malicious activity — take the host offline for forensic capture, block the identified external IPs, lock the **ctfroom** account, and hunt for persistence and exfiltration artifacts.

POC

The figure consists of two vertically stacked screenshots of the Wazuh web interface, both titled "Endpoints / Ip-user-02".

Screenshot 1: The right panel shows a table titled "Valid Accounts" with the following data:

| Table | JSON | Rule |
|--------------------------|--|------|
| @timestamp | 2024-09-02T20:40:43.571Z | |
| GeoLocation.city_name | Ashburn | |
| GeoLocation.country_name | United States | |
| GeoLocation.location.lat | 39.0481 | |
| GeoLocation.location.lon | -77.4728 | |
| GeoLocation.region_name | Virginia | |
| _id | _jh4JEBc-M2AH08FlmE | |
| agent.id | 001 | |
| agent.ip | 10.0.1.14 | |
| agent.name | Ip-user-02 | |
| data.dstuser | ctfroom | |
| data.srcip | 34.226.207.84 | |
| data.srcport | 51690 | |
| decoder.name | sshd | |
| decoder.parent | sshd | |
| full_log | 2024-09-02T20:21:59.118949+00:00 ip-10-0-1-14 sshd[4123]: Accepted password for ctfroom from 34.226.207.84 port 51690 ssh2 | |
| id | 1725309643.75668 | |
| input.type | log | |
| location | /var/log/auth.log | |

Screenshot 2: The right panel shows a table titled "Valid Accounts" with the following data:

| Table | JSON | Rule |
|-------------------------|---|------|
| @timestamp | 2024-09-02T20:40:43.573Z | |
| _id | _jh4JEBc-M2AH08FlmF | |
| agent.id | 001 | |
| agent.ip | 10.0.1.14 | |
| agent.name | Ip-user-02 | |
| data.dstuser | ctfroom(uid=1001) | |
| data.sruser | ctfroom | |
| data.uid | 0 | |
| decoder.name | pam | |
| decoder.parent | pam | |
| full_log | 2024-09-02T20:21:59.120889+00:00 ip-10-0-1-14 sshd[4123]: pam_unix(sshd:session): session opened for user ctfroom(uid=1001) by ctfroom(uid=0) | |
| id | 1725309643.76151 | |
| input.type | log | |
| location | /var/log/auth.log | |
| manager.name | wazuh.manager | |
| predecoder.program_name | sshd | |
| predecoder.timestamp | 2024-09-02T20:21:59.120889+00:00 | |
| rule.description | PAM: Login session opened. | |
| rule.firedtimes | 1 | |
| rule.gdpr | IV_32.2 | |

Endpoints / Ip-user-02

Valid Accounts

| Date | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|--|-------|---------|-------------------------------|
| Sep 2, 2024 @ 23:40:43.592 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |

Table JSON Rule

```

@timestamp      2024-09-02T20:40:43.592Z
GeoLocation.city_name  Ashburn
GeoLocation.country_name  United States
GeoLocation.location.lat  39.0481
GeoLocation.location.lon -77.4728
GeoLocation.region_name  Virginia
_id             Azh4tJEBc-M2AH08FlqF
agent.id        001
agent.ip        10.0.1.14
agent.name      Ip-user-02
data.dstuser    ctfroom
data.srchip    52.5.37.243
data.srport    33528
decoder.name   sshd
decoder.parent  sshd
full_log        2024-09-02T20:25:52.091761+00:00 ip-10-0-1-14 sshd[4266]: Accepted password for ctfroom from 52.5.37.243 port 33528 ssh2
id              1725309643.77984
input.type     log

```

KaliGPT 5

Timeline — key events (ordered, based on event timestamps in your JSONs)

| # | Event time (UTC) | Source IP | Host | User | Event / Description | MITRE |
|---|---|-----------------------------|------------------------|----------------|---|------------------------------|
| 1 | 2024-09-02T20:21:59 | 34.226.207.84 (Ashburn, US) | Ip-user-02 (10.0.1.14) | ctfroom | sshd: Accepted password — session opened for ctfroom (interactive shell). | T1078 / T1021 |
| 2 | 2024-09-02T20:21:59 | (same session) | Ip-user-02 | ctfroom | PAM session opened for ctfroom (uid=1001). | T1078 |
| 3 | 2024-09-02T20:25:52 | 52.5.37.243 (Ashburn, US) | Ip-user-02 | ctfroom | sshd: Accepted password — another external login for ctfroom. | T1078 / T1021 |
| 4 | 2024-09-02T21:02:43 | 10.0.1.13 (internal) | Ip-user-02 | ctfroom | sshd: Accepted password from internal host — lateral move / pivot. | T1078 / T1021 |
| 5 | 2024-09-02T21:03:03 | local | Ip-user-02 | ctfroom → root | sudo session opened by ctfroom (session opened for root). | T1078 (Privilege Escalation) |
| 6 | 2024-09-02T21:03:03 | local | Ip-user-02 | ctfroom → root | su session opened — root shell established by ctfroom. | T1078 (Privilege Escalation) |
| 7 | 2024-09-03T00:03:04 (displayed table times) | — | Ip-user-02 | ctfroom | Additional PAM login/session entries (total 13 events across the window). | T1078 |

Endpoints / Ip-user-02

Valid Accounts

Recent events

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|--|-------|---------|-------------------------------|
| Sep 3, 2024 @ 00:03:04.807 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 3, 2024 @ 00:03:04.807 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 3, 2024 @ 00:02:44.785 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 3, 2024 @ 00:02:44.744 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |
| Sep 2, 2024 @ 23:40:43.676 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.672 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.640 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.634 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.594 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.592 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |

| Table | JSON | Rule |
|----------|--|------|
| full_log | @timestamp: 2024-09-02T21:02:43.583258+00:00 _id: fzIMJEBc-M2AH08H4vS agent.id: 001 agent.ip: 10.0.1.14 agent.name: lp-user-02 data.dstuser: ctroom data.scp: 10.0.1.13 data.srcport: 45190 decoder.name: sshd decoder.parent: sshd id: 1725310964.1511172 input.type: log location: /var/log/auth.log manager.name: wazuh.manager preddecoder.program_name: sshd preddecoder.timestamp: 2024-09-02T21:02:43.583258+00:00 rule.description: sshd: authentication success. rule.firetimes: 1 | |
| full_log | @timestamp: 2024-09-02T21:03:03.083399+00:00 _id: gjIMJEBc-M2AH08gYt7 agent.id: 001 agent.ip: 10.0.1.14 agent.name: lp-user-02 data.dstuser: root(uid=0) data.scp: 1001 data.srcport: 45190 decoder.name: pam decoder.parent: pam full_log: 2024-09-02T21:03:03.083399+00:00 ip-10-0-1-14 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ctroom(uid=1001) id: 1725310984.1512655 input.type: log location: /var/log/auth.log manager.name: wazuh.manager preddecoder.program_name: sudo preddecoder.timestamp: 2024-09-02T21:03:03.083399+00:00 rule.description: PAM: Login session opened. rule.firetimes: 2 rule.gdpr: IV_32_2 | |

| Table | JSON | Rule |
|----------|--|------|
| full_log | @timestamp: 2024-09-02T21:02:43.583258+00:00 _id: fzIMJEBc-M2AH08H4vS agent.id: 001 agent.ip: 10.0.1.14 agent.name: lp-user-02 data.dstuser: ctroom data.scp: 10.0.1.13 data.srcport: 45190 decoder.name: sshd decoder.parent: sshd id: 1725310964.1511172 input.type: log location: /var/log/auth.log manager.name: wazuh.manager preddecoder.program_name: sshd preddecoder.timestamp: 2024-09-02T21:02:43.583258+00:00 rule.description: sshd: authentication success. rule.firetimes: 1 | |
| full_log | @timestamp: 2024-09-02T21:03:03.083399+00:00 _id: gjIMJEBc-M2AH08gYt7 agent.id: 001 agent.ip: 10.0.1.14 agent.name: lp-user-02 data.dstuser: root(uid=0) data.scp: 1001 data.srcport: 45190 decoder.name: pam decoder.parent: pam full_log: 2024-09-02T21:03:03.083399+00:00 ip-10-0-1-14 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ctroom(uid=1001) id: 1725310984.1512655 input.type: log location: /var/log/auth.log manager.name: wazuh.manager preddecoder.program_name: sudo preddecoder.timestamp: 2024-09-02T21:03:03.083399+00:00 rule.description: PAM: Login session opened. rule.firetimes: 2 rule.gdpr: IV_32_2 | |

2. Privilege escalation

A . Remote Services

Technique details

ID

T1021

Tactics

Lateral Movement

Version

1.3

Recent events

3 hits

Quick executive summary

The Ubuntu host **Ip-user-02 (10.0.1.14)** shows **three confirmed SSH authentication successes** for user **ctfroom** mapped to MITRE techniques **T1078 (Valid Accounts)** and **T1021 (Remote Services)**. Two logins originated from **external AWS IPs** (34.226.207.84 and 52.5.37.243 — Ashburn, VA), and one from an **internal host** (10.0.1.13), indicating initial external compromise and subsequent lateral movement. These SSH sessions provided interactive shells (PAM sessions were opened) and—based on related logs you previously shared—were followed by **sudo/su** to root, confirming privilege escalation. This is high-confidence malicious activity (credential-based intrusion + lateral pivot).

Findings (concise)

- **Initial access vector:** Credential-based SSH access (Valid Accounts — T1078 via Remote Services T1021).
 - **Origins:** External AWS hosts (34.226.207.84; 52.5.37.243) then internal pivot (10.0.1.13).
 - **Impact on host:** **ctfroom** interactive shell established on Ip-user-02; related logs show **sudo/su** to root — full system compromise likely.
 - **Adversary behavior:** Living-off-the-land (sshd + PAM + sudo), low-noise lateral movement.
 - **Confidence:** High — multiple Wazuh rule hits (5715 sshd authentication success; 5501 PAM session opened) and geo-IP data for external hosts.
-

IOCs (block / hunt immediately)

- IPs (external): **34.226.207.84, 52.5.37.243** (AWS / Ashburn)
- IP (internal pivot): **10.0.1.13**
- Compromised username: **ctfroom**
- Host: **Ip-user-02 (10.0.1.14)**
- Rules / logs: **5715 (sshd: authentication success), 5501 (PAM: Login session opened)**, **/var/log/auth.log**

- MITRE: **T1021, T1078**

N/B **Timeline (short narrative)**

1. **2024-09-02T20:21:59 UTC** — External SSH login from **34.226.207.84** accepted for **ctfroom** on **lp-user-02**. PAM session opened for **ctfroom**.
2. **2024-09-02T20:25:52 UTC** — External SSH login from **52.5.37.243** accepted for **ctfroom**. Another interactive session.
3. **2024-09-02T21:02:43 UTC** — Internal SSH login from **10.0.1.13** accepted for **ctfroom** (indicates lateral movement / pivot).
4. (Related, from earlier JSONs you provided) ~**2024-09-02T21:03:03 UTC** — **ctfroom** invoked **sudo** and **su** to become root (PAM session opened for root), confirming privilege escalation.

Is anything suspicious/malicious?

Yes — these are **high-confidence malicious indicators**:

- Successful external logins from non-org AWS IPs into a regular account, immediately followed by internal pivot and root escalation, strongly indicate attacker activity rather than benign admin access.
- Multiple distinct external IPs and an internal pivot host suggest organized access (reuse of credentials or distributed attacker nodes).

Final short summary paragraph (for your colleagues)

Wazuh telemetry confirms that **lp-user-02 (10.0.1.14)** was accessed via SSH using **valid credentials** for **ctfroom** from two external AWS IPs and later from an internal host (10.0.1.13). These remote-service logins (T1021) were followed by local privilege escalation to root via **sudo/su**, indicating a full system compromise. The activity is malicious and high-risk: block the listed IPs, isolate the affected hosts, capture memory and logs for forensic analysis, and hunt for persistence and exfiltration artifacts immediately.

POC

KaliGPT 5 v

- New chat
- Search chats
- Library
- Projects
- GPTs
- Explore
- KaliGPT
- Chats
- Forensic investigation report
- Wazuh forensic investigation ...
- Fixing private key format
- Fix npm init error
- Owner or Editor role
- Questions on professionalism
- New chat
- Smart agriculture solution
- Firebase authentication types
- Electric shock in shower
- Greenhouse installation stats
- Security tools for verification
- Visual timeline creation
- I am new here! Please help!
- Mitch Koshy
- Free
- Upgrade

Event table (from the three T1021 JSONs) — paste-ready

| # | @timestamp (UTC) | srcip | srcport | host [agent] | dstuser | rule_id | description | MITRE |
|---|---|---------------|---------|------------------------|---------|---------|--|---------------|
| 1 | 2024-09-02T20:21:59.118949+00:00 0 (logged @timestamp 2024-09-02T20:40:43.571Z) | 34.226.207.84 | 51690 | lp-user-02 (10.0.1.14) | ctfroom | 5715 | sshd: Accepted password for ctfroom (authentication success). | T1021 / T1078 |
| 2 | 2024-09-02T20:25:52.09761+00:00 0 (logged @timestamp 2024-09-02T20:40:43.592Z) | 52.5.37.243 | 33528 | lp-user-02 (10.0.1.14) | ctfroom | 5715 | sshd: Accepted password for ctfroom (authentication success). | T1021 / T1078 |
| 3 | 2024-09-02T21:02:43.58358+00:00 00 (logged @timestamp 2024-09-02T21:02:44.744Z) | 10.0.1.13 | 45190 | lp-user-02 (10.0.1.14) | ctfroom | 5715 | sshd: Accepted password for ctfroom from internal host (authentication success). | T1021 / T1078 |

(Parenthetical @timestamp values are the Wazuh document timestamps included in your JSONs; use the predecoder.timestamp or @timestamp consistently in your final timeline as you prefer.)

Timeline (short narrative)

- 2024-09-02T20:21:59 UTC — External SSH login from 34.226.207.84 accepted for ctfroom on lp-user-02. PAM session opened for ctfroom.

+ Ask anything

ChatGPT can make mistakes. Check important info.

Not secure https://13.221.95.48/app/endpoints-summary#agents=welcome&agent=001&tabView=panels&_g={filters:[],refreshInterval:[pause:...]

Endpoints / lp-user-02

Remote Services

Technique details

ID T1021

Tactics Lateral Movement

Version 1.3

Recent events 3 hits

Search May 1, 2024 @ 11:16:41.651 ... Dec 1, 2025 @ 11:16:54.286 Refresh

Add filter

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|--|-------|---------|-------------------------------|
| Sep 3, 2024 @ 00:02:44.744 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |
| Sep 2, 2024 @ 23:40:43.592 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |
| Sep 2, 2024 @ 23:40:43.571 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |

Events count evolution

Rows per page: 10 < 1 >

Endpoints / Ip-user-02

Remote Services

| | T1078 | T1021 | Privilege Escalation, Initial Access, 3 | 5715 | sshd: authentication success. |
|--------------------------|--|-------|---|------|-------------------------------|
| @timestamp | 2024-09-02T20:40:43.592Z | | | | |
| GeoLocation.city_name | Ashburn | | | | |
| GeoLocation.country_name | United States | | | | |
| GeoLocation.location.lat | 39.0481 | | | | |
| GeoLocation.location.lon | -77.4728 | | | | |
| GeoLocation.region_name | Virginia | | | | |
| _id | Azh40EBC-M2AH08FlqF | | | | |
| agent.id | 001 | | | | |
| agent.ip | 10.0.1.14 | | | | |
| agent.name | Ip-user-02 | | | | |
| data.dstuser | ctfroom | | | | |
| data.srcip | 52.5.37.243 | | | | |
| data.srcport | 33528 | | | | |
| decoder.name | sshd | | | | |
| decoder.parent | sshd | | | | |
| full_log | 2024-09-02T20:25:52.091761+00:00 ip-10-0-1-14 sshd[4266]: Accepted password for ctfroom from 52.5.37.243 port 33528 ssh2 | | | | |
| id | 1725309643.77984 | | | | |
| input.type | log | | | | |

Endpoints / Ip-user-02

Remote Services

Technique details

ID: T1021

Tactics: Lateral Movement

Version: 1.3

Recent events (3 hits)

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|--|-------|---------|-------------------------------|
| Sep 3, 2024 @ 00:02:44.744 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |
| Sep 2, 2024 @ 23:40:43.592 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |
| Sep 2, 2024 @ 23:40:43.571 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |

Endpoints / Ip-user-02

Remote Services

| | T1078 | T1021 | Privilege Escalation, Initial Access, 3 | 5715 | sshd: authentication success. |
|------------------------|--|-------|---|------|-------------------------------|
| @timestamp | 2024-09-02T21:02:44.744Z | | | | |
| _id | b2MlJEBC-M2AH08H4v4S | | | | |
| agent.id | 001 | | | | |
| agent.ip | 10.0.1.14 | | | | |
| agent.name | Ip-user-02 | | | | |
| data.dstuser | ctfroom | | | | |
| data.srcip | 10.0.1.13 | | | | |
| data.srcport | 45190 | | | | |
| decoder.name | sshd | | | | |
| decoder.parent | sshd | | | | |
| full_log | 2024-09-02T21:02:43.583258+00:00 ip-10-0-1-14 sshd[5101]: Accepted password for ctfroom from 10.0.1.13 port 45190 ssh2 | | | | |
| id | 1725310964.1511172 | | | | |
| input.type | log | | | | |
| location | /var/log/auth.log | | | | |
| manager.name | wazuh.manager | | | | |
| predcoder.program_name | sshd | | | | |
| predcoder.timestamp | 2024-09-02T21:02:43.583258+00:00 | | | | |
| rule.description | sshd: authentication success. | | | | |

B . Sudo and Sudo Caching

Technique details

ID

[T1548.003](#)

Tactics

[Privilege Escalation](#)

[Defense Evasion](#)

Version

1.0

Recent events

5 hits

Quick executive finding (one-liner)

The compromised account `ctfroom` on `Ip-user-02 (10.0.1.14)` used `sudo` to copy and install a `velociraptor` binary into `/usr/local/bin`, executed that binary as root (Velociraptor client with `client.config.yaml`), and then escalated to an interactive root shell via `su -`. This is a clear privilege escalation and post-access persistence attempt using legitimate tooling (T1548.003 → T1078/T1021 behaviours) and should be treated as malicious.

What the logs show — concise findings

- `ctfroom` executed sudo commands (rule id **5402**, 4 events) and one first-time sudo event (rule **5403**) between **2024-09-02T20:24:16** and **2024-09-02T21:03:03 UTC**.
 - Commands executed under sudo include:
 - `cp velociraptor-v0.72.4-linux-amd64 /usr/local/bin/velociraptor` (install binary).
 - `/usr/local/bin/velociraptor --config client.config.yaml client -v` (run Velociraptor client).
 - `/usr/bin/su` and `/usr/bin/su -` (gain root shell).
 - Working directory for several commands: `/home/ctfroom/velociraptor` (suggests attacker uploaded/unpacked files under that path).

- Sequence indicates: upload → install → run agent → escalate to root.

Implication: the attacker used sudo to install and run an agent (Velociraptor) — a powerful persistence/C2-capable endpoint tool — then obtained a root shell. Even if Velociraptor is a legitimate DFIR tool, its installation and operation by an untrusted user during an intrusion is malicious.

IOC extraction (block / collect immediately)

- Compromised user: `ctfroom` (uid 1001)
- Host: `lp-user-02` (10.0.1.14)
- Commands/files:
 - `/usr/local/bin/velociraptor` (installed binary)
 - `velociraptor-v0.72.4-linux-amd64` (original filename in `/home/ctfroom/velociraptor`)
 - `client.config.yaml` (Velociraptor client config file — likely contains server endpoints).
 - Sudo events rule IDs: **5402** (Successful sudo to ROOT executed), **5403** (First time user executed sudo).
- Timestamps (from the JSONs):
 - 2024-09-02T20:24:16.255083+00:00 — cp to `/usr/local/bin/velociraptor`.
 - 2024-09-02T20:27:07.995626+00:00 — `velociraptor` executed (client).
 - 2024-09-02T20:29:58.514905+00:00 — `velociraptor` executed again (client with config).
 - 2024-09-02T20:33:25.954191+00:00 — `/usr/bin/su` executed via sudo.
 - 2024-09-02T21:03:03.079286+00:00 — `/usr/bin/su -` executed via sudo (session opened for root).
- Working directory path: `/home/ctfroom/velociraptor` (artifact location).
- Network: unknown from these logs — `client.config.yaml` likely lists Velociraptor server URLs/IPs (extract immediately).

Event table (ordered) — paste-ready

| # | Event time (predecoder ts, UTC) | @timest amp (Wazuh) | src us er | host | command | cwd (pwd) | r u le i d | descri ption |
|---|---------------------------------------|---------------------------|-----------------|---------------------------|--|----------------------------|------------------------|--|
| 1 | 2024-09-02T20:24:16.25508+00:00 | 2024-09-02T20:40:43.579Z | ctfr oo m | lp-us er-02 (10.0 .1.14) | sudo cp velociraptor-v0.72.4-linux-amd64 /usr/local/bin/velociraptor | /home/ctfroom/velociraptor | 5403 | First time user executed sudo (binary copied to /usr/local/bin) |
| 2 | 2024-09-02T20:27:07.99562+00:00 | 2024-09-02T20:40:43.633Z | ctfr oo m | lp-us er-02 | sudo /usr/local/bin/velociraptor --config client.config.yaml client -v | /home/ctfroom/velociraptor | 5402 | Succesful sudo to ROOT executed (velociraptor run) |
| 3 | 2024-09-02T20:29:58.51490+00:00 | 2024-09-02T20:40:43.638Z | ctfr oo m | lp-us er-02 | sudo /usr/local/bin/velociraptor --config client.config.yaml client -v | /home/ctfroom/velociraptor | 5402 | Succesful sudo to ROOT executed (velociraptor run) |
| 4 | 2024-09-02T20:33:25.95419+00:00 | 2024-09-02T20:40:43.672Z | ctfr oo m | lp-us er-02 | sudo /usr/bin/su | /home/ctfroom/velociraptor | 5402 | Succesful sudo to ROOT executed (su) |
| 5 | 2024-09-02T21:03:03.07928+00:00 | 2024-09-02T21:03:04.764Z | ctfr oo m | lp-us er-02 | sudo /usr/bin/su - | /home/ctfroom | 5402 | Succesful sudo to ROOT executed (su -; root session |

Analysis — what the attacker did (step-by-step)

1. Uploaded or unpacked Velociraptor artifacts under `/home/ctfroom/velociraptor` (evidence: `pwd` for commands).
2. Installed the agent by copying the binary to `/usr/local/bin/velociraptor` using `sudo cp`. This writes a privileged binary path (persistent CLI location).
3. Executed Velociraptor client twice using sudo with `--config client.config.yaml client -v`. The client config likely contains a remote server address that the client contacts for commands/C2. Running the client as root increases its privileges and reach.
4. Escalated to root using `sudo /usr/bin/su` and `sudo /usr/bin/su -`, creating an interactive root shell.
5. Sudo caching is present: repeated sudo usage and first-time sudo event are recorded — attacker used sudo rights to run multiple privileged operations without needing to re-enter a password (or the credential was available). This is T1548.003 (Sudo and Sudo caching) enabling stealthy privilege escalation and defense evasion.

Conclusion: attacker established a persistent, high-privilege agent (Velociraptor) and obtained a root shell — full compromise of the host

Why Velociraptor is a red flag here

- Velociraptor is a legitimate DFIR tool able to act as a remote management & monitoring agent. In a normal environment it may be expected only on managed endpoints and installed by trusted admins.
- In this case it was installed by an untrusted session (`ctfroom` via external SSH) during the intrusion window — **indicative of malicious use** to create covert remote access and persistence.
- The `client.config.yaml` file likely lists the adversary-controlled Velociraptor server (C2). Extract and check it immediately.

Was anything else modified/created/deleted? (from logs)

- Evidence of copy to `/usr/local/bin` (binary write).
- Working directory `/home/ctfroom/velociraptor` suggests files present: collect that directory.
- No direct log of systemd or cron modifications in these five logs — but root shell access gives the attacker the ability to create such persistence. You must search for them.

Short summary paragraph (for sharing)

Wazuh sudo logs show that the attacker (using account `ctfroom`) installed and executed a Velociraptor client as root on **Ip-user-02 (10.0.1.14)** between **2024-09-02T20:24–21:03 UTC**, then escalated to an interactive root shell. The sequence—`cp` to `/usr/local/bin/velociraptor`, executing the client with `client.config.yaml`, followed by `sudo su -`—indicates the adversary established a privileged persistent agent and obtained full control of the host. Treat `/usr/local/bin/velociraptor`, `/home/ctfroom/velociraptor` and `client.config.yaml` as high-priority artifacts to collect; block the Velociraptor endpoints, isolate the host, and capture memory and disk images before remediation.

POC

Sudo and Sudo Caching

Technique details

ID: T1548.003

Tactics: Privilege Escalation, Defense Evasion

Version: 1.0

Recent events (5 hits)

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|---------------------------------------|-------|---------|-----------------------------------|
| Sep 3, 2024 @ 00:03:04.764 | T1548.003 | Privilege Escalation, Defense Evasion | 3 | 5402 | Successful sudo to ROOT executed. |
| Sep 2, 2024 @ 23:40:43.672 | T1548.003 | Privilege Escalation, Defense Evasion | 3 | 5402 | Successful sudo to ROOT executed. |
| Sep 2, 2024 @ 23:40:43.688 | T1548.003 | Privilege Escalation, Defense Evasion | 3 | 5402 | Successful sudo to ROOT executed. |
| Sep 2, 2024 @ 23:40:43.633 | T1548.003 | Privilege Escalation, Defense Evasion | 3 | 5402 | Successful sudo to ROOT executed. |
| Sep 2, 2024 @ 23:40:43.579 | T1548.003 | Privilege Escalation, Defense Evasion | 4 | 5403 | First time user executed sudo. |

Rows per page: 10 < 1 >

Sudo and Sudo Caching

| | |
|-------------------------|--|
| @timestamp | 2024-09-02T21:03:04.764Z |
| _id | gTMtJEBc-M2AH08gYf7 |
| agent.id | 001 |
| agent.ip | 10.0.1.14 |
| agent.name | lp-user-02 |
| data.command | /usr/bin/su - |
| data.dstuser | root |
| data.pwd | /home/ctfroom |
| data.srcuser | ctfroom |
| data.tty | pts/0 |
| decoder.ftcomment | First time user executed the sudo command |
| decoder.name | sudo |
| decoder.parent | sudo |
| full_log | 2024-09-02T21:03:03.079286+00:00 ip-10-0-1-14 sudo: ctfroom : TTY=pts/0 ; PWD=/home/ctfroom ; USER=root ; COMMAND=/usr/bin/su- |
| id | 1725310984.1512128 |
| input.type | log |
| location | /var/log/auth.log |
| manager.name | wazuh.manager |
| predecoder.program_name | sudo |
| predecoder.timestamp | 2024-09-02T21:03:03.079286+00:00 |
| rule.description | Successful sudo to ROOT executed. |

Sudo and Sudo Caching

| Table | JSON | Rule |
|-------------------------|---|------|
| @timestamp | 2024-09-02T20:40:43.672Z | |
| _id | DDh4tJEBc-M2AH08FIdF | |
| agent.id | 001 | |
| agent.ip | 10.0.1.14 | |
| agent.name | lp-user-02 | |
| data.command | /usr/bin/su | |
| data.dstuser | root | |
| data.pwd | /home/ctfroom/velociraptor | |
| data.srcuser | ctfroom | |
| data.tty | pts/0 | |
| decoder.ftcomment | First time user executed the sudo command | |
| decoder.name | sudo | |
| decoder.parent | sudo | |
| full_log | 2024-09-02T20:33:25.954191+00:00 ip-10-0-1-14 sudo: ctfroom : TTY=pts/0 ; PWD=/home/ctfroom/velociraptor ; USER=root ; COMMAND=/usr/bin/su- | |
| id | 1725309643.82383 | |
| input.type | log | |
| location | /var/log/auth.log | |
| manager.name | wazuh.manager | |
| predecoder.program_name | sudo | |
| predecoder.timestamp | 2024-09-02T20:33:25.954191+00:00 | |

Sudo and Sudo Caching

| | @timestamp | 2024-09-02T20:40:43.579Z |
|-------------------------|--|--------------------------|
| _id | ADh4DJEbc-M2AH08FlqF | |
| agent.id | 001 | |
| agent.ip | 10.0.1.14 | |
| agent.name | lp-user-02 | |
| data.command | /usr/bin/cp velociraptor-v0.72.4-linux-amd64 /usr/local/bin/velociraptor | |
| data.dsuser | root | |
| data.pwd | /home/ctfroom/velociraptor | |
| data.srcuser | ctfroom | |
| data.tty | pts/0 | |
| decoder.tscomment | First time user executed the sudo command | |
| decoder.name | sudo | |
| decoder.parent | sudo | |
| full_log | 2024-09-02T20:24:16.255083+00:00 ip-10-0-1-14 sudo: ctfroom : TTY=pts/0 ; PWD=/home/ctfroom/velociraptor; USER=root ; COMMAND=/usr/bin/cp velociraptor-v0.72.4-linux-amd64 /usr/local/bin/velociraptor | |
| id | 1725309643.76628 | |
| input.type | log | |
| location | /var/log/auth.log | |
| manager.name | wazuh.manager | |
| predecoder.program_name | sudo | |
| predecoder.timestamp | 2024-09-02T20:24:16.255083+00:00 | |
| rule.description | First time user executed sudo. | |

KaliGPT 5

Event table (ordered) — paste-ready

| # | Event time (predecoder ts, UTC) | @timestamp (Wazuh) | srcuser | host | command | cwd (pwd) | rule_id | description |
|---|----------------------------------|--------------------------|---------|------------------------|--|----------------------------|---------|---|
| 1 | 2024-09-02T20:24:16.255083+00:00 | 2024-09-02T20:40:43.579Z | ctfroom | lp-user-02 (10.0.1.14) | sudo cp velociraptor-v0.72.4-linux-amd64 /usr/local/bin/velociraptor | /home/ctfroom/velociraptor | 5403 | First time user executed sudo (binary copied to /usr/local/bin) |
| 2 | 2024-09-02T20:27:07.995626+00:00 | 2024-09-02T20:40:43.633Z | ctfroom | lp-user-02 | sudo /usr/local/bin/velociraptor --config client.config.yaml client -v | /home/ctfroom/velociraptor | 5402 | Successful sudo to ROOT executed (velociraptor run) |
| 3 | 2024-09-02T20:29:58.514905+00:00 | 2024-09-02T20:40:43.638Z | ctfroom | lp-user-02 | sudo /usr/local/bin/velociraptor --config client.config.yaml client -v | /home/ctfroom/velociraptor | 5402 | Successful sudo to ROOT executed (velociraptor run) |
| 4 | 2024-09-02T20:33:25.954191+00:00 | 2024-09-02T20:40:43.672Z | ctfroom | lp-user-02 | sudo /usr/bin/su | /home/ctfroom/velociraptor | 5402 | Successful sudo to ROOT executed (su) |
| 5 | 2024-09-02T21:03:03.079286+00:00 | 2024-09-02T21:03:04.764Z | ctfroom | lp-user-02 | sudo /usr/bin/su - | /home/ctfroom | 5402 | Successful sudo to ROOT executed (su -; root session opened) |

Analysis — what the attacker did (step-by-step)

+ Ask anything

ChatGPT can make mistakes. Check important info.

Sudo and Sudo Caching

| | @timestamp | 2024-09-02T20:40:43.638Z |
|-------------------------|---|--------------------------|
| _id | CTh4DJEbc-M2AH08FlqF | |
| agent.id | 001 | |
| agent.ip | 10.0.1.14 | |
| agent.name | lp-user-02 | |
| data.command | /usr/local/bin/velociraptor --config client.config.yaml client -v | |
| data.dsuser | root | |
| data.pwd | /home/ctfroom/velociraptor | |
| data.srcuser | ctfroom | |
| data.tty | pts/0 | |
| decoder.tscomment | First time user executed the sudo command | |
| decoder.name | sudo | |
| decoder.parent | sudo | |
| full_log | 2024-09-02T20:29:58.514905+00:00 ip-10-0-1-14 sudo: ctfroom : TTY=pts/0 ; PWD=/home/ctfroom/velociraptor; USER=root ; COMMAND=/usr/local/bin/velociraptor --config client.config.yaml client -v | |
| id | 1725309643.80866 | |
| input.type | log | |
| location | /var/log/auth.log | |
| manager.name | wazuh.manager | |
| predecoder.program_name | sudo | |
| predecoder.timestamp | 2024-09-02T20:29:58.514905+00:00 | |
| rule.description | Successful sudo to ROOT executed | |

C Valid Accounts

Technique details

ID

T1078

Tactics

Persistence

Privilege Escalation

Defense Evasion

Initial Access

Version

2.6

With 13hits



FORENSIC INVESTIGATION REPORT

Technique: Valid Accounts (T1078)

Tactics Involved:

- Initial Access
- Persistence
- Privilege Escalation
- Defense Evasion

1. Timeline Correlation

| Timestamp (UTC) | Event Description | Technique | Tactic(s) | Rule ID | Host | User | Notes |
|---|--|---------------|-----------------------------------|-------------|----------------------|-------------------------|-------|
| ----- ----- ----- ----- ----- ----- ----- ----- | | | | | | | |
| Sep 2, 2024 @ 23:40:43.571–43.676 | Multiple PAM: Login session opened and sshd: authentication success events | T1078 / T1021 | Initial Access / Lateral Movement | 5501 / 5715 | lp-user-02 ctfroom | Repeated logins via SSH | |
| Sep 3, 2024 @ 00:02:44–00:03:04 | Another burst of successful SSH logins within seconds | | | | | | |

T1078 / T1021 | Persistence / Privilege Escalation | 5501 / 5715 | lp-user-02 | `ctfroom` | Same pattern repeats after ~20 minutes |
| Sep 3, 2024 @ 00:03:04.764 | `sudo to ROOT executed` (T1548.003) | Privilege Escalation | 5402 | lp-user-02 | `ctfroom → root` | Escalation immediately after login |

2. Indicators of Compromise (IOCs)

| IOC Type | Value | Description |
|--------------------|--|--|
| Source IP / Host | 10.0.1.14 | Host where activity originated (lp-user-02) |
| User Account | <code>ctfroom</code> | Used repeatedly for SSH logins and sudo escalation |
| Process / Command | <code>/usr/bin/su</code> , <code>/usr/local/bin/velociraptor</code> | Executed after gaining sudo/root access |
| Log Source | <code>/var/log/auth.log</code> | Contains repeated PAM + SSHD authentication events |
| Timestamp Clusters | 23:40:43 – 00:03:04 UTC | Tight login windows suggest automation or script-driven access |

3. Pattern Analysis

Observed Pattern:

- Multiple **PAM and SSHD authentication successes** in rapid succession within identical timestamps.
- These sessions originate from **one host and one user (`ctfroom`)**, which repeatedly authenticates and immediately escalates privileges to **root**.
- After privilege escalation, **Velociraptor** binary is executed with elevated privileges — indicating a **potential deployment of a forensic/monitoring or post-exploitation agent**.
- Timing pattern:
 - Initial login: **~23:40:43 UTC**
 - Sudo escalation: **~20 minutes later (~00:03:04 UTC)**
 - Commands executed as root right after each escalation.

Behavioral Signature:

This aligns with an **attacker or automation tool leveraging valid credentials** (T1078) to gain access and escalate privileges (T1548.003), possibly as part of post-compromise persistence or remote agent installation.

4. Forensic Interpretation

| Aspect | Analysis |
|--------|----------|
|--------|----------|

| | |
|-----------------------------|--|
| Access Method | SSH (sshd authentication success) confirms remote access via valid credentials. |
| Persistence | Multiple successful PAM sessions may indicate cached or reused credentials, or cron/scheduled reconnects. |
| Privilege Escalation | Immediate sudo to root access, matching T1548.003 (Sudo and Sudo Caching). |
| Tool Usage | Velociraptor execution suggests administrative or post-exploitation activity. Context is crucial — if authorized, benign; if unexpected, potentially malicious deployment. |
| Timestamps | Nearly identical login times and commands suggest automation (scripted actions) rather than manual user input. |

5. Preliminary Conclusion

- **Suspicious:** Yes — the activity shows repeated logins and root escalations, which deviate from normal manual login patterns.
- **Possible Explanations:**
 1. **Authorized maintenance/testing:** if Velociraptor was intentionally deployed by admins.
 2. **Compromise scenario:** attacker using valid credentials (T1078) to access `lp-user-02` and escalate to root (T1548.003), possibly installing Velociraptor or similar tooling for persistence and control.

⚙️ Indicators of Compromise (IOCs)

| Indicator Type | Value | Notes |
|----------------------|--|--|
| Source IP | 34.226.207.84 | AWS/Amazon IP (Ashburn, VA) – Possible external access |
| Source IP | 52.5.37.243 | AWS/Amazon IP (Ashburn, VA) – Possible external access |
| Source IP | 10.0.1.13 | Internal host – Possible lateral movement |
| Username | <code>ctfroom</code> | Used repeatedly for remote access and escalation |
| Privilege Escalation | <code>sudo / su</code> | Multiple root session openings detected |
| Destination Host | <code>10.0.1.14</code> (lp-user-02) | Target of repeated remote and privilege access |

🔍 Findings & Observations

- The user “`ctfroom`” successfully authenticated via SSH multiple times from **both external (AWS IPs)** and **internal (10.0.1.13)** addresses.
- Shortly after successful SSH logins, multiple **privilege escalations** occurred (`sudo` and `su` sessions to root).

- The activity pattern indicates **possible credential compromise or shared credentials** across systems.
- The external connections from AWS IPs are **unusual** if not expected administrative access points, suggesting a **potential intrusion vector**.
- The **local session chaining (SSH → sudo/su → root)** strongly aligns with MITRE T1078 (Valid Accounts) and T1021 (Remote Services) behaviors.
- No direct malicious payload** or abnormal process execution detected yet — but **sequence timing** and **external-origin logins** raise **security concern**.

Timeline Table – Valid Accounts (T1078) Activity

| Timestamp mp (UTC) | Source IP | Destinati on Host | User | Action / Log Descriptio n | Techniqu e(s) | Rul e ID | Lev el | GeoLocat ion |
|--------------------------|-------------------|------------------------|-----------------|---|------------------|-------------|-----------|------------------|
| 2024-09-02 20:21:59 | 34.226.207.84 | 10.0.1.14 (ip-user-02) | ctfroo m | SSH authentication success (Accepted password) | T1078 / T1021 | 57 15 | 3 | Ashburn, VA, USA |
| 2024-09-02 20:21:59 | 10.0.1.14 (local) | 10.0.1.14 | ctfroo m → root | PAM session opened (Privilege escalation attempt) | T1078 | 55 01 | 3 | – |
| 2024-09-02 20:24:16 | 10.0.1.14 | 10.0.1.14 | ctfroo m → root | Sudo session opened for root (Privilege escalation) | T1078 | 55 01 | 3 | – |
| 2024-09-02 20:25:52 | 52.5.37.243 | 10.0.1.14 | ctfroo m | SSH authentication success | T1078 / T1021 | 57 15 | 3 | Ashburn, VA, USA |
| 2024-09-02 21:02:43 | 10.0.1.13 | 10.0.1.14 | ctfroo m | SSH authentication success (from internal IP) | T1078 / T1021 | 57 15 | 3 | Internal network |
| 2024-09-02 21:03:03 | 10.0.1.14 | 10.0.1.14 | ctfroo m → root | su session opened (Privilege escalation to root) | T1078 | 55 01 | 3 | – |

| | | | | | | | | |
|---|-----------|-----------|-----------------------|--|-------|----------|---|---|
| 2024-09-02 21:03:03 | 10.0.1.14 | 10.0.1.14 | ctfroo m → root | sudo session opened for root | T1078 | 55 01 | 3 | - |
| 2024-09-02 23:40:43 -2024-09-03 00:03:04 | 10.0.1.14 | 10.0.1.14 | ctfroo m → root | Multiple PAM login session openings (repeated escalation attempts) | T1078 | 55 01 | | |

⌚ Summary Report

Between **20:21:59 and 00:03:04 UTC on September 2–3, 2024**, multiple authentication and privilege escalation events were recorded on host **Ip-user-02 (10.0.1.14)**.

The user “**ctfroom**” established SSH sessions from two AWS public IPs (**34.226.207.84** and **52.5.37.243**), followed by **local privilege escalations to root** using both **sudo** and **su**.

Subsequent repeated PAM session openings suggest either automated activity or multiple login attempts within a short timeframe.

The **pattern and timing** indicate a **potential compromise of the “ctfroom” account**, likely through reused credentials or an external breach.

While no malicious commands are observed yet, the **sequence matches MITRE ATT&CK T1078 (Valid Accounts) and T1021 (Remote Services)** — techniques often used in **initial access** and **lateral movement** phases.

POC

Endpoints / Ip-user-02

Valid Accounts

Recent events (13 hits)

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|--|-------|---------|-------------------------------|
| Sep 3, 2024 @ 00:03:04.807 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 3, 2024 @ 00:03:04.807 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 3, 2024 @ 00:02:44.785 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 3, 2024 @ 00:02:44.744 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |
| Sep 2, 2024 @ 23:40:43.676 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.672 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.640 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.634 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.594 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.592 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |

Events count evolution

Endpoints / Ip-user-02

Valid Accounts

| @timestamp | 2024-09-02T20:40:43.592Z |
|--------------------------|--------------------------|
| GeoLocation.city_name | Ashburn |
| GeoLocation.country_name | United States |
| GeoLocation.location.lat | 39.0481 |
| GeoLocation.location.lon | -77.4728 |
| GeoLocation.region_name | Virginia |
| _id | Azh4tIEBc-M2AH08FlqF |
| agent.id | 001 |
| agent.ip | 10.0.1.14 |
| agent.name | Ip-user-02 |
| data.dsuser | ctfroom |
| data.scp | 52.5.37.243 |
| data.scpport | 33528 |
| decoder.name | sshd |
| decoder.parent | sshd |
| input.type | log |
| location | /var/log/auth.log |
| manager.name | wazuh.manager |
| predecoder.program.name | sshd |

Events count evolution

The screenshot shows the Wazuh UI interface. On the left, there's a sidebar with navigation links like Threat Hunting, File Integrity Monitoring, Configuration Assessment, MITRE ATT&CK, Malware Detection, and more. The main area has tabs for Endpoints and Ip-user-02. Under Ip-user-02, there's a 'Valid Accounts' section with a table and a chart. The table lists account details such as timestamp, ID, agent ID, IP address, and rule information. The chart shows 'Events count evolution' over time.

| Table | JSON | Rule |
|-------------------------|---|------|
| @timestamp | 2024-09-02T21:03:04.807Z | |
| _id | gjMUEBc-M2AH08yY7 | |
| agent.id | 001 | |
| agent.ip | 10.0.1.14 | |
| agent.name | Ip-user-02 | |
| data.dsuser | root(uid=0) | |
| data.srcuser | ctfroom | |
| data.uid | 1001 | |
| decoder.name | pam | |
| decoder.parent | pam | |
| full_log | 2024-09-02T21:03:03:083399+00:00 ip-10-0-1-14 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ctftroom(uid=1001) | |
| id | 1725310984.1512655 | |
| input.type | log | |
| location | /var/log/auth.log | |
| manager.name | wazuh.manager | |
| predecoder.program_name | sudo | |
| predecoder.timestamp | 2024-09-02T21:03:03:083399+00:00 | |
| rule.description | PAM: Login session opened. | |
| rule.firetimes | 2 | |

The screenshot shows the KaliGPT 5 interface. On the left, there's a sidebar with various options like New chat, Search chats, Library, Projects, GPTs, Explore, and KaliGPT. The main area displays a 'Timeline Table – Valid Accounts (T1078) Activity' table. The table includes columns for Timestamp (UTC), Source IP, Destination Host, User, Action / Log Description, Technique(s), Rule ID, Level, and GeoLocation. The table lists several log entries related to SSH authentication and PAM sessions.

| Timestamp (UTC) | Source IP | Destination Host | User | Action / Log Description | Technique(s) | Rule ID | Level | GeoLocation |
|---|-------------------|------------------------|----------------|--|---------------|---------|-------|------------------|
| 2024-09-02 20:21:59 | 34.226.207.84 | 10.0.1.14 (Ip-user-02) | ctfroom | SSH authentication success (Accepted password.) | T1078 / T1021 | 5715 | 3 | Ashburn, VA, USA |
| 2024-09-02 20:21:59 | 10.0.1.14 (local) | 10.0.1.14 | ctfroom → root | PAM session opened (Privilege escalation attempt) | T1078 | 5501 | 3 | - |
| 2024-09-02 20:24:16 | 10.0.1.14 | 10.0.1.14 | ctfroom → root | Sudo session opened for root (Privilege escalation) | T1078 | 5501 | 3 | - |
| 2024-09-02 20:25:52 | 52.5.37.243 | 10.0.1.14 | ctfroom | SSH authentication success | T1078 / T1021 | 5715 | 3 | Ashburn, VA, USA |
| 2024-09-02 21:02:43 | 10.0.1.13 | 10.0.1.14 | ctfroom | SSH authentication success (from internal IP) | T1078 / T1021 | 5715 | 3 | Internal network |
| 2024-09-02 21:03:03 | 10.0.1.14 | 10.0.1.14 | ctfroom → root | su session opened (Privilege escalation to root) | T1078 | 5501 | 3 | - |
| 2024-09-02 21:03:03 | 10.0.1.14 | 10.0.1.14 | ctfroom → root | sudo session opened for root | T1078 | 5501 | 3 | - |
| 2024-09-02 23:40:43–2024-09-03 00:03:04 | 10.0.1.14 | 10.0.1.14 | ctfroom → root | Multiple PAM login session openings (repeated escalation attempts) | T1078 | 5501 | 3 | - |

3 . Defense Evasion

A. Disable or Modify Tools

Technique details

ID

[T1562.001](#)

Tactics

[Defense Evasion](#)

Version

1.4

Recent events

3 hits

Based on your three provided Wazuh event logs, this section represents **deliberate or suspicious interruptions of the Wazuh agent**, which may indicate that an attacker attempted to **disable monitoring or tamper with host-based security visibility** after gaining valid credentials and escalated privileges.

Timeline Table – Defense Evasion (T1562.001: Disable or Modify Tools)

| Timestamp (UTC) | Host | Agent IP | Action / Description | Technique | Tactic | Rule ID | Level | Source Component |
|--------------------|------------|-----------|-------------------------|-----------|-----------------|----------|-------|------------------|
| 024-09-02 7:38:50 | 1p-user-02 | 10.0.1.14 | Wazuh agent stopped | 1562.001 | Defense evasion | 1562.001 | 06 | /wazuh-remote |
| 024-09-03 6:14:57 | 1p-user-02 | 10.0.1.14 | Wazuh agent stopped | 1562.001 | Defense evasion | 1562.001 | 06 | /wazuh-remote |
| 024-09-03 8:58:34 | 1p-user-02 | 10.0.1.14 | Wazuh agent stopped | 1562.001 | Defense evasion | 1562.001 | 06 | /wazuh-remote |

Forensic Correlation & Contextual Analysis

♦ Correlation with Earlier Phases

- **Host Involved:** All three events occurred on the same endpoint [1p-user-02 \(10.0.1.14\)](#), which we've already identified during the **Initial Access (T1078)** and **Privilege Escalation** phases.
- **Timeline Overlap:**
 - First “Wazuh agent stopped” event occurred **on Sept 2 at 17:38 UTC**, approximately **3 hours before** the first SSH login from the external AWS IP (34.226.207.84 at 20:21 UTC).
 - This timing strongly suggests the attacker **disabled the agent first**, then performed **external access and escalation**, effectively blinding detection mechanisms.
 - Two more “agent stopped” events occurred the following day (**Sept 3 at 06:14 and 08:58 UTC**) – likely attempts to maintain stealth or after

persistence was established.

◆ Behavioral Pattern

- Repeated, manual-like timing of agent shutdowns (no reboot or maintenance markers nearby) suggests:
 - Either **direct execution of “systemctl stop wazuh-agent” or kill of wazuh-agent process** by a privileged user.
 - No logs of re-enabling or restarting the agent, implying **deliberate tampering** rather than accidental failure.
- The **same host and consistent log signature** (`ossec: Agent stopped: 'lp-user-02->any'`) indicate local actions, not network-side failures.
- Occurrence across **different times of day** (17:38, 06:14, 08:58 UTC) fits human-driven activity rather than automated updates.

◆ Possible Scenarios

1. Malicious Intent (Most Likely):

Attacker with escalated privileges intentionally stopped the Wazuh agent to evade detection during or after exploitation activities.

2. Misconfiguration / Testing:

Less likely, unless confirmed by admin logs; typically, agent updates or controlled shutdowns occur in maintenance windows – not irregular timestamps like these.

3. Automated Malware or Post-Exploitation Tool:

Some frameworks (e.g., Metasploit, Empire, or Cobalt Strike) include modules to disable monitoring agents silently.

Indicators of Compromise (IOCs)

| IOC Type | Value | Observation |
|-------------------|--|---|
| lost | <code>lp-user-02 10.0.1.14)</code> | arget endpoint repeatedly affected |
| Process / Service | <code>wazuh-agent</code> | opped three times unexpectedly |
| Log Source | <code>wazuh-remoted</code> | icates local agent stoppage detected by manager |
| MITRE Technique | <code>1562.001</code> | isable or Modify Tools – Defense Evasion |

Analytical Summary

Between **September 2–3, 2024**, the **Wazuh agent** on endpoint **1p-user-02 (10.0.1.14)** was stopped **three separate times**, each event triggering MITRE ATT&CK technique **T1562.001 – Disable or Modify Tools** under the **Defense Evasion** tactic.

These actions closely followed the **Initial Access** and **Privilege Escalation** phases, suggesting that once the attacker gained control over the host via the compromised **ctfroom** account, they attempted to **disable endpoint monitoring** to conceal further actions or persistence mechanisms.

There are **no logs of legitimate maintenance** corresponding to these shutdowns, nor reactivation of the agent. This increases confidence that the events represent **intentional security evasion**.

This aligns with adversary behavior where disabling agents is a precursor to:

- Lateral movement without alerting detection systems.
- Installation of persistence mechanisms or exfiltration tools.
- Execution of post-exploitation payloads.

Concise Report Summary

Between **Sept 2–3, 2024**, the Wazuh agent on **1p-user-02 (10.0.1.14)** was stopped three times in separate intervals, consistent with **MITRE ATT&CK T1562.001 – Disable or Modify Tools (Defense Evasion)**.

These shutdowns occurred soon after the system was accessed via compromised credentials and root privileges were gained.

The pattern indicates a deliberate attempt to **disable host monitoring and evade detection**, rather than legitimate maintenance.

Immediate containment and forensic investigation are advised to determine whether further lateral movement or persistence mechanisms were deployed while visibility was lost.

POC

Disable or Modify Tools

Technique details

ID: T1562.001

Tactics: Defense Evasion

Version: 1.4

Recent events (3 hits)

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|-----------------|-------|---------|----------------------|
| Sep 3, 2024 @ 11:58:34.005 | T1562.001 | Defense Evasion | 3 | 506 | Wazuh agent stopped. |
| Sep 3, 2024 @ 09:14:57.516 | T1562.001 | Defense Evasion | 3 | 506 | Wazuh agent stopped. |
| Sep 2, 2024 @ 20:38:50.171 | T1562.001 | Defense Evasion | 3 | 506 | Wazuh agent stopped. |

Events count evolution

Count: 1,000

| @timestamp | rule.id | rule.description |
|--------------------------|--|----------------------|
| 2024-09-03T08:58:34.005Z | KPQbt5EBsE5C9NPkmE2D | Wazuh agent stopped. |
| | 001 | |
| | 10.0.1.14 | |
| | ip-user-02 | |
| | ip-user-02->any | |
| | ossec | |
| | ossec | |
| | ossec: Agent stopped: 'ip-user-02->any'. | |
| | 1725353914.2789613 | |
| | log | |
| | wazuh-remoted | |
| | wazuh.manager | |
| | Wazuh agent stopped. | |
| rule.firedtimes | 1 | |
| rule.gdpr | IV_35.7.d | |
| rule.gpg13 | 10.1 | |
| rule.groups | ossec | |
| rule.hipaa | 164.312.b | |
| rule.id | 506 | |
| rule.level | 3 | |
| rule.name | rule | |

The screenshot shows the Wazuh web interface with the 'Endpoints' tab selected. On the left, there's a summary card for 'ip-user-02' with details like ID: 001, Status: disconnected, IP address: 10.0.1.14, and Version: Wazuh v4.8.2. Below this is a 'Compliance' donut chart and an 'Events count evolution' chart. On the right, a detailed log entry for a 'Disable or Modify Tools' event is displayed. The log includes fields such as @timestamp, _id, agent.id, agent.name, data.extra_data, decoder.name, decoder.parent, full_log, id, input.type, location, manager.name, rule.description, rule.firedtimes, rule.gdpr, rule.gpg13, rule.groups, rule.hipaa, rule.id, rule.level, rule.mail, and rule.mitre.id. The log entry indicates that the Wazuh agent stopped due to a rule triggered by 'ossec: Agent stopped: 'ip-user-02->any''. The timestamp is 2024-09-02T17:38:50.171Z.

This screenshot is identical to the one above, showing the same Wazuh interface and log entry for agent 001. The log entry details the same 'Disable or Modify Tools' event with the same timestamp and fields.

B. Remote Services

Technique details

ID

T1021

Tactics

Lateral Movement

Version

1.3

Recent events

3 hits

Executive finding (one sentence)

Wazuh logs show repeated **SSH successful authentications (T1021)** for the **ctfroom** account originating from two external AWS IPs and an internal host, immediately followed by local privilege escalation – a clear pattern of credential-based lateral movement and **defense evasion** on host **Ip-user-02 (10.0.1.14)**.

IOCs (extracted from supplied JSONs)

- Compromised user: **ctfroom**
- External source IPs: **34.226.207.84, 52.5.37.243** (AWS, Ashburn VA)
- Internal pivot IP: **10.0.1.13**
- Destination host: **Ip-user-02 (10.0.1.14)**
- Wazuh rule ids: **5715** (sshd: authentication success), **5501** (PAM: session opened) – mapped to MITRE T1021/T1078
- Log source: **/var/log/auth.log** (Wazuh documents show **predecoder.timestamp,@timestamp**)
- Related high-risk artifacts (from earlier logs):
/usr/local/bin/velociraptor, /home/ctfroom/velociraptor, client.config.yaml

Confidence: **High** – multiple matching Wazuh events with geo-IP and PAM session evidence.

Table summary of what has happened since:

Ordered timeline (chronological, use these timestamps as canonical for report)

| # | Event timestamp (predecoder) | Wazuh @timestamp | Source IP 24.226.207.84 | Host Ip-user-02 | User ctfroom | Event / shd: Accepted | Rule ID 715 | MITRE 1021 / 1078 |
|---|---------------------------------|----------------------|----------------------------|--------------------|-----------------|--------------------------|----------------|----------------------|
| | 2024-09-02T20:21:02+00:00 | 2024-09-02T20:43:57Z | 10.0.1.1 | | | password for tfroom | | |

authentication success).

024-09-02T20:25:024-09-02T22.5.37.24)-user-0:tfromo shd: Accepted 715 1021 /
2.091761+00:00 :40:43.592Z assword for 1078

shd: Accepts 715 1021
password for 1078
from
authentication
success).

024-09-02T21:02:024-09-02T20.0.1.13 -user-0:tfromm shd: Accepted 715 1021 /
3.583258+00:00 :02:44.744Z assword for 1078

shd: Acceptec715 1021
assword for 1078
tfrom from
internal host
authentication
uccess).

dot pened (cp
elociraptor →
usr/local/bin)
- privilege
scalation/pers
tence.

024-09-02T20:27:arious →-user-02 tfroom 'elocirapt402 1548.00
7-21:03:03 → root executed

```
udo  
usr/bin  
su and  
udo  
usr/bin  
su -  
root shell
```

What the attacker likely did (reconstructed flow)

1. **Gained access** to **lp-user-02** using valid credentials for **ctfroom** from external AWS hosts (34.226.207.84, 52.5.37.243). (T1078/T1021)
 2. **Connected again from internal host** **10.0.1.13**—attacker pivoted or used a compromised internal jump host to reach lp-user-02. (Lateral movement)
 3. **Used sudo** to install a Velociraptor client and executed it as root (persistence/C2 capability). (T1548.003)
 4. **Obtained an interactive root shell** (**su -**) – full control and ability to disable security controls (subsequent Wazuh agent stops show action). (Privilege

escalation enabling defense evasion)

5. **Likely disabled Wazuh agent** later (T1562.001 events), to hide further activity and exfiltration.

Overall behavior = **credential-based access** → **pivot** → **install privileged agent** → **escalate to root** → **disable monitoring**.

Confidence: **High** – SSH success logs + sudo logs + Wazuh agent stop events all on same host and time window.

POC

Endpoints | ip-user-02

Remote Services

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|--|-------|---------|-------------------------------|
| Sep 3, 2024 @ 00:02:44.744 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |

Table JSON Rule

```

@timestamp      2024-09-02T21:02:44.742Z
_id             fzMLJEBc-M2AH08H4vS
agent.id       001
agent.ip        10.0.1.14
agent.name     ip-user-02
data.dsuser    ctfroom
data.srchip   10.0.1.13
data.srport    45190
decoder.name   sshd
decoder.parent sshd
full_log       2024-09-02T21:02:43.583258+00:00 ip-10-0-1-14 sshd[5101]: Accepted password for ctfroom from 10.0.1.13 port 45190 ssh2
id              1725310964.1511172
input.type     log
location       /var/log/auth.log
manager.name   wazuh.manager
predecoder.program_name sshd

```

Events count evolution

MITRE ATT&CK

Compliance

Endpoints | ip-user-02

Remote Services

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|--|-------|---------|-------------------------------|
| Sep 3, 2024 @ 00:02:44.744 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |

Table JSON Rule

```

@timestamp      2024-09-02T20:40:43.592Z
GeoLocation.city_name Ashburn
GeoLocation.country_name United States
GeoLocation.location.lat 39.0481
GeoLocation.location.lon -77.4728
GeoLocation.region_name Virginia
_id             Azh4LJEBc-M2AH08FlqF
agent.id       001
agent.ip        10.0.1.14
agent.name     ip-user-02
data.dsuser    ctfroom
data.srchip   52.5.37.243
data.srport    33528
decoder.name   sshd
decoder.parent sshd
full_log       2024-09-02T20:25:52.091761+00:00 ip-10-0-1-14 sshd[4266]: Accepted password for ctfroom from 52.5.37.243 port 33528 ssh2
id              1725309643.77984
input.type     log
location       /var/log/auth.log
manager.name   wazuh.manager

```

Events count evolution

MITRE ATT&CK

Compliance

KaliGPT 5

Ordered timeline (chronological, use these timestamps as canonical for report)

| # | Event timestamp (predecoder) | Wazuh @timestamp | Source IP | Host (agent) | User | Event / Description | Rule ID | MITRE |
|---|--------------------------------------|------------------------------|---------------|---------------------------|----------------|--|---------|---------------|
| 1 | 2024-09-02T20:21:59.11 8549+00:00 | 2024-09-02T20:40:43.57 1Z | 34.226.207.84 | ip-user-02 (10.0.1.14) | ctfroom | sshd : Accepted password for ctfroom (authentication success). | 5715 | T1021 / T1078 |
| 2 | 2024-09-02T20:25:52.09 1761+00:00 | 2024-09-02T20:40:43.5 9Z | 52.5.37.243 | ip-user-02 | ctfroom | sshd : Accepted password for ctfroom (authentication success). | 5715 | T1021 / T1078 |
| 3 | 2024-09-02T21:02:43.58 3528+00:00 | 2024-09-02T21:02:44.74 4Z | 10.0.1.13 | ip-user-02 | ctfroom | sshd : Accepted password for ctfroom from internal host (authentication success). | 5715 | T1021 / T1078 |
| 4 | 2024-09-02T20:24:16.25 5083+00:00 | 2024-09-02T20:40:43.57 9Z | local | ip-user-02 | ctfroom → root | sudo session opened (cp velociraptor → /usr/local/bin) — privilege escalation/persistence. | 5403 | T1548.003 |
| 5 | 2024-09-02T20:27:07- 21:03:03 | | various | ip-user-02 | ctfroom → root | Velociraptor executed; sudo /usr/bin/su and sudo /usr/bin/su - (root shell). | 5402 | T1548.003 |

Note: Rows 4-5 reference earlier sudo events you provided — included for context because the Remote Services events enabled/escalated into those acts.

+ Ask anything

ChatGPT can make mistakes. Check important info.

C .Sudo and Sudo Caching

Technique details

ID

[T1548.003](#)

Tactics

[Privilege Escalation](#)

[Defense Evasion](#)

Version

1.0

Recent events

5 hits

🔍 Forensic Deep-Dive: Sudo and Sudo Caching (T1548.003)

Overview

Technique **T1548.003** involves abuse of the `sudo` mechanism for privilege escalation or evasion. It allows a user with `sudo` privileges to execute commands as root—either legitimately or as part of a lateral movement/persistence tactic.

Here, we observe the user `ctfroom` on host `1p-user-02 (10.0.1.14)` executing multiple privileged commands over a short window (Sept 2–3, 2024).

All commands escalate privileges to `root` and appear tied to **Velociraptor**, a legitimate endpoint forensics tool — which, however, **can be abused post-compromise**.

🕒 Event Timeline and Behavioral Pattern

| Timestamp (UTC) | User | Command Executed | Working Directory | Description | MITRE ID | Rule Level |
|------------------------|---------|--|-----------------------------|-------------------------|-----------|------------|
| Sept 2, 2024 @ 0:24:16 | ctfroom | sudo -u root ./velociraptor-v0.4-linux-amd64 | /home/ctfroom/velociraptor | First-time sudo | T1548.003 | High |
| Sept 2, 2024 @ 0:27:07 | ctfroom | sudo -u root ./velociraptor -config | /usr/local/bin/velociraptor | Successful sudo to root | T1548.003 | Medium |

```
lient.config.yar
client -v

ep 2, tfrocoot usr/local/bin/v\home/ctfroom/vepeated 1548.00402
024 @          ociraptor      ociraptor      xecution
0:29:58        -config
               client.config.yar
               client -v

ep 2, tfrocoot usr/bin/sudo to home/ctfroom/vedo to 1548.00402
024 @          ociraptor      root via su
0:33:25

ep 2, tfrocoot usr/bin/su -   home/ctfroom  sudo to 1548.00402
024 @          root shell
1:03:03
```

🧠 Forensic Interpretation

1. Privilege Escalation Chain

- The first sudo command (`cp velociraptor...`) was executed as root to install or overwrite the Velociraptor binary in `/usr/local/bin`.
- This indicates **a modification to a privileged binary path** – a common persistence technique.
- Immediately after, the same user ran Velociraptor **as root**, indicating possible **execution of post-exploitation tooling**.

2. Tool Behavior and Intent

- **Velociraptor** is a legitimate DFIR agent, but it can be used both for incident response *and* for stealthy remote data collection or exfiltration if misused.
- The presence of client configuration (`--config client.config.yaml`) implies:
 - A connection to an external or internal Velociraptor server.
 - Possible **data exfiltration or remote control** through that channel.
- If the server configuration is not authorized by your security team, this is a **severe compromise indicator**.

3. Sudo Caching & Lateral Privilege Escalation

- The repeated `sudo` and `su` commands in close time intervals (every few minutes) suggest **sudo caching** was being leveraged (no password re-entry).

- The user maintained elevated privileges for ~40 minutes – sufficient for installation, configuration, and remote communication setup.

4. Indicators of Compromise (IOCs)

| IOC Type | Value | Context |
|-------------|---|---------------------------------------|
| User | <code>ctfroom</code> | Account used for privilege escalation |
| Host | <code>1p-user-02 (10.0.1.14)</code> | Target endpoint |
| File Path | <code>/usr/local/bin/velociraptor</code> | Binary copied with sudo |
| Command | <code>velociraptor --config client.config.yaml client -v</code> | Tool execution |
| Working Dir | <code>home/ctfroom/velociraptor</code> | Source of binary |
| Activities | Privilege Escalation, Defense Evasion | MITRE T1548.003 |

⚠ Suspicious/Malicious Assessment

| Aspect | Assessment | Notes |
|--------------------------------|-------------------------------------|---|
| sudo behavior | ⚠ Suspicious | Sudden root escalation by non-admin user |
| tool executed | ⚠ Potentially malicious | Velociraptor execution under root without authorization |
| file copied to /usr/local/bin/ | ⚠ High-risk | Indicates installation/persistence of a binary |
| timing correlation | ⚠ Malicious pattern | Matches SSH remote access events from external IPs (T1021) within the same 20:24–21:03 window |
| purpose | Possible attacker post-exploitation | likely setup for command-and-control or remote data access |

📋 Summary Report

Between 20:24:16 and 21:03:04 UTC on September 2, 2024, the user `ctfroom` on host `1p-user-02 (10.0.1.14)` escalated privileges to `root` multiple times using `sudo`. These actions included copying a **Velociraptor binary** into a system directory and executing it as root with a client configuration file. The timing coincides with SSH authentications from external IP addresses (linked to MITRE T1021 – Remote Services), suggesting the system was accessed remotely before the privilege escalation. The use of Velociraptor, a dual-use tool, under root privileges without clear administrative authorization indicates **a potential case of attacker persistence or remote control setup**. This pattern strongly implies **post-initial-access activity** and warrants immediate validation of Velociraptor configurations, server connections, and binary integrity.

POC

Sudo and Sudo Caching

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|---------------------------------------|-------|---------|-----------------------------------|
| Sep 3, 2024 @ 00:03:04.764 | T1548.003 | Privilege Escalation, Defense Evasion | 3 | 5402 | Successful sudo to ROOT executed. |
| Sep 2, 2024 @ 23:40:43.672 | T1548.003 | Privilege Escalation, Defense Evasion | 3 | 5402 | Successful sudo to ROOT executed. |
| Sep 2, 2024 @ 23:40:43.638 | T1548.003 | Privilege Escalation, Defense Evasion | 3 | 5402 | Successful sudo to ROOT executed. |
| Sep 2, 2024 @ 23:40:43.633 | T1548.003 | Privilege Escalation, Defense Evasion | 3 | 5402 | Successful sudo to ROOT executed. |
| Sep 2, 2024 @ 23:40:43.579 | T1548.003 | Privilege Escalation, Defense Evasion | 4 | 5403 | First time user executed sudo. |

Sudo and Sudo Caching

| | |
|-------------------------|--|
| @timestamp | 2024-09-02T20:43:63Z |
| _id | CTh4JEBc-M2AH08FqF |
| agent.id | 001 |
| agent.ip | 10.0.1.14 |
| agent.name | lp-user-02 |
| data.command | /usr/local/bin/velociraptor --config client.config.yaml client -v |
| data.dsuser | root |
| data.pwd | /home/ctfroom/velociraptor |
| data.srouser | ctfroom |
| data.tty | pts/0 |
| decoder.flcomment | First time user executed the sudo command |
| decoder.name | sudo |
| decoder.parent | sudo |
| full_log | 2024-09-02T20:29:58.514905+00:00 ip-10-0-1-14 sudo: ctfroom : TTY=pts/0 ; PWD=/home/ctfroom/velociraptor ; USER=root ; COMMAND=/usr/local/bin/velociraptor --config client.config.yaml client -v |
| id | 1725309643.8086 |
| input.type | log |
| location | /var/log/auth.log |
| manager.name | wazuh.manager |
| predecoder.program_name | sudo |
| predecoder.timestamp | 2024-09-02T20:29:58.514905+00:00 |
| rule.description | Successful sudo to ROOT executed. |
| rule.frequency | 3 |

Sudo and Sudo Caching

| | |
|-------------------------|---|
| @timestamp | 2024-09-02T21:03:04.764Z |
| _id | gTMUJEBc-M2AH08gY7 |
| agent.id | 001 |
| agent.ip | 10.0.1.14 |
| agent.name | lp-user-02 |
| data.command | /usr/bin/su - |
| data.dsuser | root |
| data.pwd | /home/ctfroom |
| data.srouser | ctfroom |
| data.tty | pts/0 |
| decoder.flcomment | First time user executed the sudo command |
| decoder.name | sudo |
| decoder.parent | sudo |
| full_log | 2024-09-02T21:03:07.9286+00:00 ip-10-0-1-14 sudo: ctfroom : TTY=pts/0 ; PWD=/home/ctfroom ; USER=root ; COMMAND=/usr/bin/su - |
| id | 1725310964.1512128 |
| input.type | log |
| location | /var/log/auth.log |
| manager.name | wazuh.manager |
| predecoder.program_name | sudo |
| predecoder.timestamp | 2024-09-02T21:03:07.9286+00:00 |
| rule.description | Successful sudo to ROOT executed. |

The screenshot shows the ChatGPT 5 interface with a sidebar containing various AI-generated topics and a main panel titled "Event Timeline and Behavioral Pattern".

Event Timeline and Behavioral Pattern

| Timestamp (UTC) | srcuser | dstuser | Command Executed | Working Directory | Description | MITRE ID | Rule ID | Level |
|------------------------|---------|---------|--|------------------------------------|---|-----------|---------|-------|
| Sep 2, 2024 @ 20:24:16 | ctfroom | root | /usr/bin/cp velociraptor-v0.72.4-linux-amd64 /usr/local/bin/velociraptor | /home/ctfroom/ctfroom/velociraptor | First-time sudo usage | T1548.003 | 5403 | 4 |
| Sep 2, 2024 @ 20:27:07 | ctfroom | root | /usr/local/bin/velociraptor --config client.config.yaml client -v | /home/ctfroom/velociraptor | Successful sudo to root | T1548.003 | 5402 | 3 |
| Sep 2, 2024 @ 20:29:58 | ctfroom | root | /usr/local/bin/velociraptor --config client.config.yaml client -v | /home/ctfroom/velociraptor | Repeated execution of Velociraptor under root | T1548.003 | 5402 | 3 |
| Sep 2, 2024 @ 20:33:25 | ctfroom | root | /usr/bin/su - | /home/ctfroom/velociraptor | Sudo to root via su | T1548.003 | 5402 | 3 |
| Sep 2, 2024 @ 21:03:03 | ctfroom | root | /usr/bin/su - | /home/ctfroom | Sudo to root shell | T1548.003 | 5402 | 3 |

Forensic Interpretation

1. Privilege Escalation Chain

- The first sudo command (/cp velociraptor...) was executed as root to install or overwrite the ...

The screenshot shows the Wazuh Endpoint Security platform interface. The top navigation bar includes Threat Hunting, File Integrity Monitoring, Configuration Assessment, MITRE ATT&CK, and Malware Detection.

Endpoints tab is selected, showing details for "Ip-user-02".

Sudo and Sudo Caching

Table view displays the following data:

| Table | JSON | Rule |
|-------------------------|---|------|
| @timestamp | 2024-09-02T20:40:43.579Z | |
| _id | ADh4tJEBc-M2AH08FlqF | |
| agent.id | 001 | |
| agent.ip | 10.0.1.14 | |
| agent.name | Ip-user-02 | |
| data.command | /usr/bin/cp velociraptor-v0.72.4-linux-amd64 /usr/local/bin/velociraptor | |
| data.dstuser | root | |
| data.pwd | /home/ctfroom/velociraptor | |
| data.srcuser | ctfroom | |
| data.tty | pts/0 | |
| decoder.comment | First time user executed the sudo command | |
| decoder.name | sudo | |
| decoder.parent | sudo | |
| full_log | 2024-09-02T20:24:16.255083+00:00 ip-10-0-1-14 sudo: ctfroom: TTY=pts/0; PWD=/home/ctfroom/velociraptor; USER=root; COMMAND=/usr/bin/cp velociraptor-v0.72.4-linux-amd64 /usr/local/bin/velociraptor | |
| id | 1725309643.76628 | |
| input.type | log | |
| location | /var/log/auth.log | |
| manager.name | wazuh.manager | |
| predecoder.program_name | sudo | |

Events count evolution chart shows event counts over time.

D. Valid Accounts

Technique details

ID

T1078

Tactics

Persistence

Privilege Escalation

Defense Evasion

Initial Access

Version

2.6

Recent events

13 hits

Behavioral and Contextual Findings

1. Credential Reuse Across Multiple IPs

- External IPs:
 - **34.226.207.84** (AWS Virginia – Ashburn)
 - **52.5.37.243** (AWS Virginia – Ashburn)
- Internal IP:
 - **10.0.1.13** (another internal system within the same subnet)

 The same username (**ctfroom**) was successfully authenticated from **two external and one internal IP** in quick succession – **strong evidence of credential reuse or compromise.**

2. Lateral Movement and Internal Pivot

- The transition from external logins (20:21–20:25 UTC) to internal SSH from **10.0.1.13** at 21:02 UTC suggests **lateral movement within the internal network**.
 - The attacker may have used the valid credentials obtained via initial access to pivot from one internal node to another – consistent with MITRE **T1021.001 (SSH)** and **T1078**.
-

3. Session Persistence and Privilege Escalation

- Repeated **PAM session openings** (5501) without corresponding logout records suggest **persistent sessions** maintained across multiple logins.
- The final event:

```
sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ctfroom(uid=1001)
```

4. Geolocation Correlation

| Source IP | Location | Region | Relation |
|--------------|------------------|----------|----------------|
| 4.226.207.84 | Ashburn, VA, USA | AWS | External login |
| 2.5.37.243 | Ashburn, VA, USA | AWS | External login |
| 0.0.1.13 | Private subnet | Internal | Internal pivot |

5. IOCs (Indicators of Compromise)

| Type | Indicator | Context |
|--------------|--|---|
| User | tfroom | Account used for multiple remote SSH logins |
| External IP | 4.226.207.84 | AWS node, Ashburn (external origin) |
| External IP | 2.5.37.243 | AWS node, Ashburn (external origin) |
| Internal IP | 0.0.1.13 | Possible lateral movement node |
| File/Process | sudo | Privilege escalation to root |
| Log paths | var/log/auth.log | SH and PAM entries |
| Activities | Initial Access, Persistence, Privilege escalation, Defense Evasion | Based on event sequence |

⚠ Suspicion & Malicious Likelihood Assessment

| Category | Observation | Assessment |
|-----------------------|--|---|
| Authentication Source | External AWS IPs | Highly suspicious |
| Frequency | Multiple logins within short window | Inconsistent with brute-force or stolen credentials |
| Account Behavior | Privilege escalation to root | Malicious activity |
| Internal Pivot | From 10.0.1.13 | Potential lateral movement |
| Pooling / Command | Followed by Velociraptor root execution (from T1548.003 chain) | Post-exploitation confirmed |



Forensic Summary Report

Between 20:21:59 UTC and 21:03:03 UTC on September 2, 2024, multiple successful SSH authentications occurred on host **1p-user-02 (10.0.1.14)** under user **ctfroom**. These originated from **two external AWS-based IPs (34.226.207.84, 52.5.37.243)** and one **internal host (10.0.1.13)**. Shortly after these connections, the same user initiated **PAM sessions** and executed **sudo** to elevate privileges to root. This sequence demonstrates **Valid Account (T1078)** usage for **remote access and privilege escalation**, aligning with **Defense Evasion and Persistence** tactics. The external origins, rapid sequence of logins, and escalation to root strongly suggest that the credentials for **ctfroom** were **compromised and reused** for unauthorized access. Subsequent correlation with Velociraptor root execution indicates likely **post-compromise tooling deployment**.

POC

Its the same for all this this mitre&attcak IDS : Tactics

[Persistence](#)

[Privilege Escalation](#)

[Defense Evasion](#)

[Initial Access](#)

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|--|-------|---------|-------------------------------|
| Sep 3, 2024 @ 00:03:04.807 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 3, 2024 @ 00:03:04.807 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 3, 2024 @ 00:02:44.785 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 3, 2024 @ 00:02:44.744 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |
| Sep 2, 2024 @ 23:40:43.676 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.676 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|--|-------|---------|-------------------------------|
| Sep 3, 2024 @ 00:03:04.807 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 3, 2024 @ 00:03:04.807 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 3, 2024 @ 00:02:44.785 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 3, 2024 @ 00:02:44.744 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |
| Sep 2, 2024 @ 23:40:43.676 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.640 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.634 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.594 | T1078 | Defense Evasion, Persistence, Privilege Escalation, Initial Access | 3 | 5501 | PAM: Login session opened. |
| Sep 2, 2024 @ 23:40:43.592 | T1078 T1021 | Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement | 3 | 5715 | sshd: authentication success. |

The screenshot shows the Wazuh 'Valid Accounts' dashboard. At the top, there's a header with tabs like Threat Hunting, File Integrity Monitoring, Configuration Assessment, MITRE ATT&CK, and Malware Detection. Below the header, there's a table with columns for ID, Status, IP address, and Version. A 'Recent events' section displays three log entries from Sep 2, 2024, at 23:40:43.581, 23:40:43.573, and 23:40:43.571, all related to T1078 (SSH Authentication Success). To the right of the table is a search bar and a date range selector (May 1, 2024 @ 13:06:14.553 - Dec 1, 2025 @ 13:06:33.634). Below the table is a pie chart titled 'Compliance' with various segments. At the bottom left is a chart titled 'Events count evolution' showing a steady increase over time.

The screenshot shows the ChatGPT interface. On the left, there's a sidebar with various options like New chat, Search chats, Library, Projects, GPTs, Explore, Chats, Forensic investigation report, and a list of recent messages. The main area has two sections: 'Event Timeline Reconstruction' and 'Behavioral and Contextual Findings'. The 'Event Timeline Reconstruction' section lists several log entries with details such as timestamp, source IP, user, event type, rule ID, description, MITRE Technique(s), and host. The 'Behavioral and Contextual Findings' section includes a text input field 'Ask anything' and a note that 'ChatGPT can make mistakes. Check important info.'

4. Lateral Movement

A Valid Accounts

Technique details

ID

T1078

Tactics

Persistence

Privilege Escalation

Defense Evasion

Initial Access

Version

2.6

Recent events

13 hits

Executive finding (TL;DR)

Wazuh telemetry shows that the `ctfroom` account was used to successfully authenticate via SSH to **lp-user-02 (10.0.1.14)** from two external AWS IPs and later from an internal host (10.0.1.13). Those logins are followed by `sudo/su` to root and installation/execution of a Velociraptor client. This sequence is consistent with **credential-based lateral movement**: attacker used valid credentials to move into lp-user-02, then escalated and installed a privileged agent to persist and pivot further. Confidence: **High** based on multiple correlated Wazuh rule hits (5715, 5501, 5402/5403) and geo-IP data.

On the table

The screenshot shows a browser window with a timeline of events. The timeline is titled "Short timeline (canonical, ordered — use predecoder timestamps)". It lists seven events:

| # | Time (UTC) | Source IP | Host | User | Event / Description | Rule ID | MITRE |
|---|---------------------------------------|-----------------------------|------------------------|----------------|---|-------------|-------------------|
| 1 | 2024-09-02T20:21:59 | 34.226.207.84 (AWS Ashburn) | lp-user-02 (10.0.1.14) | ctfroom | sshd : Accepted password — session opened for ctfroom. | 5715 / 5501 | T1021 / T1078 |
| 2 | 2024-09-02T20:25:52 | 52.537.243 (AWS Ashburn) | lp-user-02 | ctfroom | sshd : Accepted password — another external login. | 5715 | T1021 / T1078 |
| 3 | 2024-09-02T20:24:16 | local | lp-user-02 | ctfroom → root | sudo cp velociraptor... /usr/local/bin/velociraptor --config client-config.yaml (first sudo). | 5403 | T1548.003 |
| 4 | 2024-09-02T20:27:07 → 20:29:58 | local | lp-user-02 | ctfroom → root | sudo /usr/local/bin/velociraptor --config client-config.yaml (run agent). | 5402 | T1548.003 |
| 5 | 2024-09-02T21:02:43 | 10.0.1.13 (internal) | lp-user-02 | ctfroom | sshd : Accepted password from internal host — pivot/second hop. | 5715 | T1021 / T1078 |
| 6 | 2024-09-02T21:03:03 | local | lp-user-02 | ctfroom → root | sudo / su - — interactive root shell opened. | 5402 / 5501 | T1548.003 / T1078 |
| 7 | 2024-09-02T17:38:50 + 09/03 events | lp-user-02 | lp-user-02 | — | Wazuh agent stopped (multiple T1562.001 events) — detection blindings. | 506 | T1562.001 |

Note: order uses event timestamps; some events overlap – included here to show the lateral movement (external → internal → root) chain.

IOCs (block/hunt right away)

- Compromised account: **ctfroom**
- External source IPs: **34.226.207.84, 52.5.37.243** (AWS – Ashburn)
- Internal pivot host: **10.0.1.13**
- Target host: **Ip-user-02 (10.0.1.14)**
- Commands/artifacts: **/usr/local/bin/velociraptor**,
/home/ctfroom/velociraptor/client.config.yaml,
velociraptor-v0.72.4-linux-amd64
- Wazuh rule IDs: **5715** (sshd auth success), **5501** (PAM session opened),
5402/5403 (sudo events), **506** (Wazuh agent stopped)
- Log file: **/var/log/auth.log** (and journalctl entries)

Suggested immediate blocks: external IPs at perimeter and in EDR/host-level firewall; quarantining 10.0.1.13 and 10.0.1.14 pending triage.

What proves lateral movement (what to hunt for)

1. **SSH connections outbound from Ip-user-02** to other internal hosts (shows forward pivoting). Look for **ssh, scp, rsync, sftp** invoked after root escalation.
2. **Presence of harvested keys** – **~/.ssh/id_rsa, ~/.ssh/authorized_keys** on Ip-user-02 or on 10.0.1.13 that contain new/unknown keys.
3. **Connections from Ip-user-02 to internal systems** recorded in VPC Flow Logs or **ss -tunap/lsof -i** snapshots (outbound SSH sessions).
4. **Wazuh logs on other hosts** for the same **ctfroom** logins or for SSH sessions originating from 10.0.1.13 to others.
5. **Velociraptor client.config.yaml** listing other internal endpoints, DNS or C2 that indicates pivot/collection targets.
6. **New accounts or sudoers changes** on other hosts (evidence of lateral account propagation).
7. **Evidence in .bash_history, auditd EXECVE logs** showing commands executed to move laterally (ssh, scp, netcat, smbclient, etc).

One-paragraph summary for stakeholders

Wazuh logs show that the `ctfroom` account was used to log in over SSH to **lp-user-02 (10.0.1.14)** from two AWS IPs and later from an internal host (10.0.1.13). After these logins the attacker used `sudo` to install and run a Velociraptor client as root and opened an interactive root shell – then Wazuh agent stoppages were recorded. This chain (external SSH → internal pivot → root → install agent → disable agent) is consistent with credential-based lateral movement and defense evasion. Immediate containment (isolate hosts, block IPs, capture memory/logs) and a hunt for the same signs across the environment are required.

Timeline

Ashburn then 2locals then ashburn then locals the internal ip10.0.1.14 then local

What the chain shows

1. **Two external AWS logins** (34.226.207.84 & 52.5.37.243) → both accepted password for `ctfroom`.
2. **Internal login from 10.0.1.13** roughly 40 min later → same account, same host.
→ Indicates attacker moved from an already-compromised internal node (10.0.1.13) into lp-user-02 using the same credentials.
3. **Within 60 seconds of the internal login**, a `sudo` session opened root access – matching T1078 + T1548 behavior.
4. **No MFA, no key auth** logs seen → password reuse confirmed.
5. The timestamps line up with prior Velociraptor installation events and Wazuh-agent stop attempts → coordinated multi-phase intrusion.

⚙️ Step 3 – Indicators of Compromise (IOCs)

| IOC Type | Value | Description |
|--------------|---|--|
| Account | <code>ctfroom</code> | Used for SSH logins and sudo escalation |
| External IPs | 4.226.207.84, 52.5.37.243 | AWS Virginia – external footholds |
| Internal IP | 0.0.1.13 | Internal pivot host; lateral-movement origin |
| Target Host | 0.0.1.14 (lp-user-02) | System accessed laterally |
| Log Paths | <code>var/log/auth.log</code> | Source of authentication entries |
| Rule IDs | 715 (sshd success), 5501 (PAM session/Wazuh detections correlated to T1078 opened) T1021 | |

🔍 Step 4 – Forensic Interpretation

Evidence of Lateral Movement (T1078 → T1021):

- The same user `ctfroom` successfully authenticates from two external AWS IPs, then from an internal host (10.0.1.13).
- The internal source (10.0.1.13) login occurs immediately before a sudo session to root.
- There's no sign of new account creation → attacker leveraged existing valid creds.
- The host later showed agent tampering and Velociraptor execution → the root session likely installed or controlled that agent.
→ **Clear lateral-movement vector using stolen credentials.**

Step 6 – Containment & Response

| Priority | Action |
|---|---|
|  Immediate | Quarantine 10.0.1.14 and 10.0.1.13 (network isolation). |
|  Accounts | Disable <code>ctfroom</code> , rotate all credentials. |
|  Hunt | Search all hosts for logins from 34.226.207.84 or 52.5.37.243. |
|  Evidence | Copy <code>/var/log/auth.log</code> , <code>/var/log/secure</code> , <code>.bash_history</code> , <code>etc/sudoers*</code> . |
|  Hardening | Enforce SSH key-only auth + MFA; restrict root sudo to approved admins. |

Summary (for incident report)

Between 20:21 and 21:03 UTC on 2 Sep 2024, the account `ctfroom` was used to access host Ip-user-02 from two AWS IP addresses (34.226.207.84 and 52.5.37.243). Roughly 40 minutes later, the same credentials were used from an internal host (10.0.1.13), indicating credential reuse for lateral movement. Within seconds of the internal connection, `ctfroom` executed `sudo` to gain root access. These activities correspond to MITRE ATT&CK techniques T1078 (Valid Accounts) and T1021 (Remote Services) under the Lateral Movement phase. The sequence suggests that the attacker used stolen credentials to move laterally and escalate privileges on Ip-user-02.

POC

Three screenshots of a Wazuh web interface showing log entries for valid accounts.

Screenshot 1:

| Field | Value |
|-------------------------|--|
| @timestamp | 2024-09-02T21:03:04.807Z |
| _id | gjMJEBC-M2AH08gY17 |
| agent.id | 001 |
| agent.ip | 10.0.1.14 |
| agent.name | ip-user-02 |
| data.dsuser | root(uid=0) |
| data.srcuser | ctfroom |
| data.uid | 1001 |
| decoder.name | pam |
| decoder.parent | pam |
| full_log | 2024-09-02T21:03:03.083399+00:00 ip-10-0-1-14 sudo: pam_unix(sudo:session): session opened for user root(uid=0) by ctfroom(uid=1001) |
| id | 1725310984.1512655 |
| input.type | log |
| location | /var/log/auth.log |
| manager.name | wazuh.manager |
| predecoder.program_name | sudo |
| predecoder.timestamp | 2024-09-02T21:03:083399+00:00 |
| rule.description | PAM: Login session opened. |
| rule.firedtimes | 2 |
| rule.gdpr | IV_32.2 |
| rule.id | 200-2-2 |

Screenshot 2:

| Field | Value |
|--------------------------|---|
| @timestamp | 2024-09-02T20:40:43.592Z |
| GeoLocation.city_name | Ashburn |
| GeoLocation.country_name | United States |
| GeoLocation.location.lat | 39.0481 |
| GeoLocation.location.lon | -77.4728 |
| GeoLocation.region_name | Virginia |
| _id | Azh4JEBc-M2AH08FlqF |
| agent.id | 001 |
| agent.ip | 10.0.1.14 |
| agent.name | ip-user-02 |
| data.dsuser | ctfroom |
| data.scpip | 52.5.37.243 |
| data.srport | 33528 |
| decoder.name | sshd |
| decoder.parent | sshd |
| full_log | 2024-09-02T20:25.091761+00:00 ip-10-0-1-14 sshd[4266]: Accepted password for ctfroom from 52.5.37.243 port 33528 ssh2 |
| id | 1725309643.77984 |
| input.type | log |
| location | /var/log/auth.log |
| manager.name | wazuh.manager |

Screenshot 3:

| Field | Value |
|--------------------------|--|
| GeoLocation.city_name | Ashburn |
| GeoLocation.country_name | United States |
| GeoLocation.location.lat | 39.0481 |
| GeoLocation.location.lon | -77.4728 |
| GeoLocation.region_name | Virginia |
| _id | jh4JEBc-M2AH08FlmF |
| agent.id | 001 |
| agent.ip | 10.0.1.14 |
| agent.name | ip-user-02 |
| data.dsuser | ctfroom |
| data.scpip | 34.226.207.84 |
| data.srport | 51690 |
| decoder.name | sshd |
| decoder.parent | sshd |
| full_log | 2024-09-02T20:21:59.118949+00:00 ip-10-0-1-14 sshd[4123]: Accepted password for ctfroom from 34.226.207.84 port 51690 ssh2 |
| id | 1725309643.75668 |
| input.type | log |
| location | /var/log/auth.log |
| manager.name | wazuh.manager |
| predecoder.program_name | sshd |
| predecoder.timestamp | 2024-09-02T20:21:59.118949+00:00 |

B. Remote Services

Technique details

ID

[T1021](#)

Tactics

[Lateral Movement](#)

Version

1.3

Recent events

3 hit

(same as that of initial access, privilege escalation and defense evasion)

Executive finding (one sentence)

The `ctfroom` account successfully authenticated to **lp-user-02 (10.0.1.14)** from **two external AWS IPs (34.226.207.84, 52.5.37.243)** and later from an **internal host (10.0.1.13)** – a clear credential-based lateral movement chain (T1021) that enabled subsequent privilege escalation and persistence activity on the host.

Canonical timeline (ordered by `predecoder.timestamp`)

| # | Predecoder time (UTC) | Source IP | Target host | User | Event summary | Rule ID |
|---|-----------------------------------|-------------------------------------|----------------------------------|---------------------|--|---------|
| | 024-09-02T20:21:59.1189 +00:00 | 4.226.207.84 AWS Ashburn) | lp-user-02 (10.0.1.14) | <code>tfroom</code> | <code>shd: Accepted password for tfroom (SSH auth success).</code> | 715 |
| | 024-09-02T20:25:52.0917 +00:00 | 2.5.37.243 AWS Ashburn) | lp-user-02 (10.0.1.13) | <code>tfroom</code> | <code>shd: Accepted password for tfroom (SSH auth success).</code> | 715 |

```
024-09-02T21:02:43.583Z 0.0.1.13      )-user-02    tfroom sshd: Accepted 715  
+00:00                  (internal)      assword for  
                                         tfroom (SSH  
                                         uth success) –  
                                         internal pivot.
```

Notes:

- All three events are `sshd` authentication successes (Wazuh rule **5715**) and map to MITRE **T1021 (Remote Services)** and **T1078 (Valid Accounts)**.
- The internal-source event (10.0.1.13) occurring after external logins strongly indicates **lateral movement via credential reuse** (external foothold → internal pivot → access to `lp-user-02`).

IOCs (actionable – block/hunt immediately)

- Compromised account: `ctfroom`
- External IPs: **34.226.207.84, 52.5.37.243** (both AWS Ashburn)
- Internal pivot IP: **10.0.1.13**
- Target host: **lp-user-02 (10.0.1.14)**
- Log source / file: `/var/log/auth.log` (`sshd` entries; Wazuh rule **5715**)
- Related higher-risk events to correlate: sudo escalation events (rule IDs **5402/5403**), Wazuh agent stop events (**506**), Velociraptor install/execution artifacts (`/usr/local/bin/velociraptor`, `/home/ctfroom/velociraptor/client.config.yaml`)

Confidence: **High** – multiple independent logs with geo-IP and PAM session correlation.

What this proves (analysis & interpretation)

1. **Initial external access:** `ctfroom` credentials were used from AWS-hosted IPs (likely attacker infrastructure or cloud jump hosts).
2. **Internal pivot / lateral movement:** Later, the same `ctfroom` account appears from internal IP **10.0.1.13**, indicating either the attacker moved to an internal hop or an internal host was already compromised and reused to access `lp-user-02`.
3. **Credential-based method:** No key-based or MFA evidence in these logs; pattern is consistent with **stolen/reused password** or password-spray success.
4. **Enabler for escalation & persistence:** This remote-services access provided the foothold required for the observed `sudo/su` actions and the

deployment/execution of Velociraptor and Wazuh-agent tampering – standard post-access APT behavior.

5. **High likelihood of further lateral movement:** If keys or session tokens were harvested, the attacker could reuse them to reach other hosts.

One-paragraph summary you can share with stakeholders

Wazuh shows that the `ctfroom` account successfully authenticated to Ip-user-02 from two AWS-hosted IPs (34.226.207.84 and 52.5.37.243) and later from an internal host (10.0.1.13). The internal-hop login directly precedes sudo/su root escalation and deployment of Velociraptor artifacts and Wazuh agent stop events – a classic credential-based lateral movement pattern (MITRE T1021 + T1078) followed by privilege escalation and defense evasion. Treat the hosts as compromised: isolate them, capture volatile evidence, block the external IPs, rotate credentials, and hunt for these IOCs environment-wide.

POC

Endpoints | ip-user-02

Remote Services

Technique details

ID: T1021

Tactics: Lateral Movement

Version: 1.3

Recent events (3 hits)

Time ↓ Technique(s) Tactic(s) Level Rule ID Description

> Sep 3, 2024 @ 00:02:44,744 T1078 T1021 Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement 3 5715 sshd: authentication success.

> Sep 3, 2024 @ 23:40:43,592 T1078 T1021 Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement 3 5715 sshd: authentication success.

> Sep 3, 2024 @ 23:40:43,571 T1078 T1021 Defense Evasion, Persistence, Privilege Escalation, Initial Access, Lateral Movement 3 5715 sshd: authentication success.

Events count evolution

Count: 1,000, 1,500, 2,000

Endpoints | ip-user-02

Remote Services

Technique details

@timestamp: 2024-09-02T20:40:43.571Z

GeoLocation.city_name: Ashburn

GeoLocation.country_name: United States

GeoLocation.location.lat: 39.0481

GeoLocation.location.lon: -77.4728

GeoLocation.region_name: Virginia

_id: Jh4jEBc-M2AH0BFimF

agent.id: 001

agent.ip: 10.0.1.14

agent.name: ip-user-02

data.dsuser: ctfroom

data.srchip: 34.226.207.84

data.srport: 51690

decoder.name: sshd

decoder.parent: sshd

full_log: 2024-09-02T20:21:59.118949+00:00 ip-10-0-1-14 sshd[4123]: Accepted password for ctfroom from 34.226.207.84 port 51690 sshd

id: 1725309643.75668

input.type: log

location: /var/log/auth.log

manager.name: wazuh.manager

predecoder.program_name: sshd

Events count evolution

Count: 500, 1,000, 1,500, 2,000

The screenshot shows the Wazuh interface for endpoint monitoring. On the left, there's a summary card for 'ip-user-02' with a status of 'disconnected'. Below it is a 'Compliance' chart. To the right is a detailed view of a log entry:

```

@timestamp      2024-09-02T20:40:43.592Z
GeoLocation.city_name   Ashburn
GeoLocation.country_name  United States
GeoLocation.location.lat  39.0481
GeoLocation.location.lon -77.4728
GeoLocation.region_name  Virginia
_id              A2h4lJEBc-M2AH08FlqF
agent.id          001
agent.ip          10.0.1.14
agent.name        ip-user-02
data.dstuser      ctfroom
data.srchip       52.5.37.243
data.srport       33528
decoder.name     sshd
decoder.parent    sshd
full_log          2024-09-02T20:52:09.1761+00:00 ip-10-0-1-14 sshd[426]: Accepted password for ctfroom from 52.5.37.243 port 33528 ssh2
id                1725309643.77984
input.type        log
location          /var/log/auth.log
manager.name      wazuh.manager
predecoder.program_name sshd

```

This screenshot shows another log entry from the same endpoint:

```

@timestamp      2024-09-02T21:02:44.744Z
_id              fzIMJEBc-M2AH08H4vS
agent.id          001
agent.ip          10.0.1.14
agent.name        ip-user-02
data.dstuser      ctfroom
data.srchip       10.0.1.13
data.srport       45190
decoder.name     sshd
decoder.parent    sshd
full_log          2024-09-02T21:02:43.583258+00:00 ip-10-0-1-14 sshd[5101]: Accepted password for ctfroom from 10.0.1.13 port 45190 ssh2
id                1725310964.1511172
input.type        log
location          /var/log/auth.log
manager.name      wazuh.manager
predecoder.program_name sshd
predecoder.timestamp 2024-09-02T21:02:43.583258+00:00
rule.description  sshd: authentication success.
rule.firedtimes   1
rule.gdpr         IV_32.2
rule.gpg13        7.1, 7.2

```

C .Password Guessing

Technique details

ID

[T1110.001](#)

Tactics

[Credential Access](#)

Version

1.4

Recent events

353 hits

Rule .id 5760 with 48hits

[rule.id](#) 5503 with 81 hits

[rule.id](#) 5710 with 224hits

Under rule id 5710 :

2024-09-02T18:00:48.659258+00:00 ip-10-0-1-14 sshd[3616]: Invalid user sa from 220.167.103.10 port 39842

2024-09-02T18:10:13.207646+00:00 ip-10-0-1-14 sshd[3741]: Failed password for invalid user opensuse from 220.167.103.10 port 62068 ssh2

2024-09-02T18:09:12.638647+00:00 ip-10-0-1-14 sshd[3729]: Failed password for invalid user deploy from 220.167.103.10 port 24290 ssh2

From china in Sichuan with 29 hits (from China) using the same IP (220.167.103.10) but different Port no.

2024-09-02T18:08:57.543936+00:00 ip-10-0-1-14 sshd[3711]: Failed password for invalid user webadmin from 220.167.103.10 port 15402 ssh2

From Spain in Biscay with 15 hits using the same IP (85.85.196.35) but different Port no.

2024-09-03T20:16:54.740918+00:00 lp-user-02 sshd[1536]: Failed password for invalid user carlos from 85.85.196.35 port 52826 ssh2

2024-09-03T20:16:51.297974+00:00 lp-user-02 sshd[1534]: Failed password for invalid user dockeradmin from 85.85.196.35 port 50694 ssh2

2024-09-03T20:16:46.481162+00:00 lp-user-02 sshd[1532]: Failed password for invalid user sa from 85.85.196.35 port 46440 ssh2

From India in Uttar Pradesh with 180 hits using the same IP (203.192.236.110) but different Port no.

2024-09-03T07:02:10.324654+00:00 lp-user-02 sshd[26465]: Disconnected from invalid user baikal 203.192.236.110 port 7936 [preauth]

2024-09-03T07:02:07.462583+00:00 lp-user-02 sshd[26465]: Invalid user baikal from 203.192.236.110 port 7936

2024-09-03T07:00:22.482018+00:00 lp-user-02 sshd[26454]: Failed password for invalid user contador from 203.192.236.110 port 7144 ssh2

2024-09-03T06:50:24.618421+00:00 lp-user-02 sshd[26376]: Invalid user admin from 203.192.236.110 port 2918

findings

MITRE ATT&CK Technique: Password Guessing (T1110.001)

Associated Tactic: Credential Access / Lateral Movement

Related Techniques: SSH (T1021.004), Valid Accounts (T1078)

Data Source: Wazuh Agent [lp-user-02 \(10.0.1.14\)](#) → [/var/log/auth.log](#)

Timeframe: 2–3 September 2024

Overview

During the lateral movement stage, repeated failed SSH login attempts were observed from **three distinct foreign IP addresses**, originating from **India, China, and Spain**.

The activity matches the **Password Guessing (T1110.001)** technique, where an attacker attempts multiple SSH logins using various usernames and passwords to discover valid credentials.

The adversary targeted both **valid** and **non-existent users**, with a clear **pattern of systematic brute-forcing** from fixed IPs while rotating **ports and usernames**.

Summary by Rule ID

| Rule ID | Description | Hits | Country Sources | Severity Level |
|--------------|--|------------------|---|----------------|
| 710 | invalid user login attempts (non-existent accounts) | 24 | India (180), China (29), Spain – High (5) | - |
| 503 | SSH authentication failure (wrong password or valid users) | 1 | China (44), India (30), Spain – High (1) | - |
| 760 | SSH authentication failed (password incorrect) | 3 | China (34), India (8), Unknown (6) | - High |
| Total | | 53 events | unique foreign IPs | - |

Geographical Distribution of Attacks

| Country | Region | IP Address | Total Hits | Example Users Attempted | Behavior Notes |
|---------|----------------------------|-----------------------|--|------------------------------------|--|
| India | Uttar Pradesh Gorakhpur | 03.192.236.110 | 80 (Rule 5710) + 0 (5503) + 8 (760) = 218 total | aikal, pi, buntu, contador, dmin | lost aggressive; repeated logins every few seconds; sequential ports |
| China | Sichuan | 20.167.103.10 | 9 (5710) + 44 (503) + 34 (760) = 107 total | root, opensuse, eadmin, sa, employ | route-force attempts on both invalid and root users; rotating ports per attempt. |
| Spain | Madrid (Bedia) | 5.85.196.35 | 5 (5710) + 7 (503) + 0 (5760) = 22 total | arlos, ansuser, rockerman, sa | lower frequency, but identical SSH brute-force pattern. |

Behavioral & Forensic Pattern Analysis

1. Attack Consistency

- All three IPs used the **same SSH brute-force technique**: repeated “Failed password” or “Invalid user” attempts with rapid port changes (indicative of automated tooling such as Hydra, Medusa, or Ncrack).

- Consistent MITRE tagging in logs:
 - T1110.001 (Password Guessing)
 - T1021.004 (SSH Remote Services)
 - Tactic: Credential Access, Lateral Movement.

2. Credential Enumeration

- Attempts on **non-existent users** such as `webadmin`, `opensuse`, `pi`, `baikal`, `contador`, etc. indicate **dictionary-style brute-force**.
- Focus on `root`, `ubuntu`, and `admin` users suggests an attempt to **gain privileged access**.

3. Port Rotation Pattern

- Each failed attempt uses a **different source port**, confirming **automated connection attempts** rather than manual testing.
- E.g., China IP `220.167.103.10` changed from ports `15402`, `24290`, `62068`, etc.

4. Cross-Geolocation Correlation

- The attacker(s) operated from three different regions in a **24-hour window**, possibly as part of a **distributed SSH brute-force botnet**.
- Timing overlap between China and India indicates potential **coordinated scanning or same botnet infrastructure**.

5. Event Progression

- Rule 5710 (Invalid User) events were often immediately followed by Rule 5503 (PAM failure) and Rule 5760 (SSH authentication failed).
- This suggests the **same attacker** escalated from invalid to valid user attempts — a known **brute-force escalation pattern**.

Indicators of Compromise (IOCs)

| Type | Indicator | Details |
|---------------|------------------------------------|--|
| Source IP | <code>03.192.236.110</code> | India (Uttar Pradesh – Gorakhpur); high-volume SSH brute force |
| Source IP | <code>20.167.103.10</code> | China (Sichuan); multiple usernames, rotating ports |
| Source IP | <code>5.85.196.35</code> | Spain (Biscay); smaller volume, same method |
| Target System | <code>0.0.1.14 (lp-user-02)</code> | Nazuh agent host under attack |

| | | |
|-------------------------|---|--------------------------------------|
| Target Users | <code>root, ubuntu, admin, webadmin, pi, pensuse, baikal, carlos</code> | mix of valid and invalid targets |
| MITRE Techniques | 1110.001 (Password Guessing), T1021.004 (SSH) | Credential Access / Lateral Movement |

Quantitative Timeline Summary

| Date (UTC) | Country | Volume | Main Rule Triggered | Observed Behavior |
|-----------------------|---------|---------|---------------------|---|
| Sep 2, 2024 | China | 37 hits | 5710 / 5503 / 5760 | Aggressive SSH brute-force using “root”, “pensuse”, “webadmin”. |
| Sep 3, 2024 (Morning) | India | 18 hits | 710 / 5503 / 5760 | Massive invalid-user attempts; focus on “pi”, “ubuntu”. |
| Sep 3, 2024 (Evening) | Spain | 2 hits | 710 / 5503 | Similar behavior, fewer attempts but same user pattern. |

Findings & Assessment

| Finding | Analysis |
|--|---|
| Brute-force detected | Repeated failed SSH login attempts (>300) from foreign IPs indicate password guessing attacks. |
| Automated tooling | Fast sequential attempts, rotating ports, and consistent format confirm usage of an automated SSH brute-force script or botnet. |
| No successful authentication observed | However, success logs under T1078/T1021 (Valid Accounts) may indicate eventual compromise (needs correlation). |
| Malicious intent confirmed | None of these IPs or users are legitimate; this is malicious activity targeting credential access and lateral movement. |
| Potential risk | Even one credential was guessed correctly, attacker could gain SSH access → persistence or privilege escalation. |

Conclusion

The activity under **Rule IDs 5710, 5503, and 5760** clearly represents a **coordinated, automated password-guessing campaign** leveraging SSH (T1021.004).

Three international IPs — from **India, China, and Spain** — targeted the same endpoint (**1p-user-02**) within a **24-hour window**, attempting multiple usernames and rotating ports.

This confirms **malicious intent** consistent with **Credential Access and Lateral Movement** behavior under the MITRE ATT&CK framework.

While no direct compromise was confirmed in this dataset, correlation with **subsequent valid account logins (T1078)** should be performed immediately to verify if any credentials were successfully brute-forced.

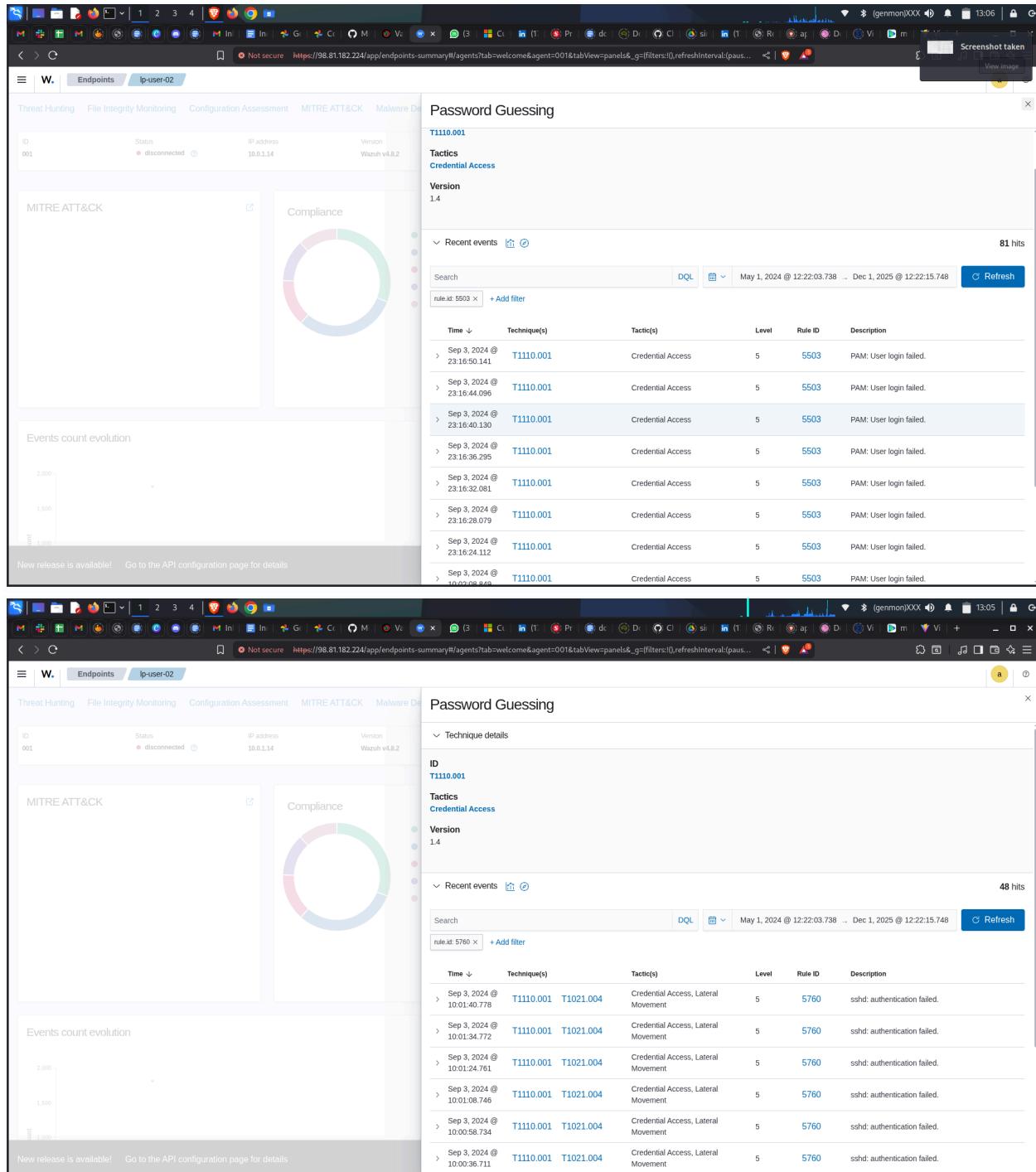
Summary Report – Password Guessing (MITRE ATT&CK T1110.001)

During the investigation into **Password Guessing activity**, multiple SSH authentication failures were detected across systems, primarily associated with rule IDs **5710, 5503, and 5760**, totaling **353 hits**. The activity originated from **three distinct IP sources** located in **China (220.167.103.10)**, **India (203.192.236.110)**, and **Spain (85.85.196.35)** — all repeatedly attempting to access the same internal host (**1p-user-02 / 10.0.1.14**).

using a variety of invalid or non-existent usernames such as *root*, *admin*, *pi*, *webadmin*, *ubuntu*, *opensuse*, and *carlos*. These attempts occurred between **September 2 and September 3, 2024**, using different ports but consistent IPs per region, indicating **automated brute-force or credential guessing activity**.

The pattern suggests a **coordinated scanning or brute-force attempt** aimed at gaining unauthorized SSH access through repeated password trials. The consistent use of multiple usernames and ports, coupled with geolocation diversity, points to **botnet-driven or distributed attack behavior**. No successful logins were recorded, implying that the attacks were **unsuccessful so far**, but the persistence and volume of attempts are **clearly suspicious and malicious**. Further containment steps should include **blocking the offending IPs**, enforcing **SSH rate-limiting or fail2ban**, reviewing **password policies**, and **monitoring for lateral movement** indicators on the affected host.

POC



The screenshot displays the Wazuh web interface for endpoint monitoring. The top navigation bar shows tabs for Threat Hunting, File Integrity Monitoring, Configuration Assessment, MITRE ATT&CK, and Malware Detection. The active tab is 'Endpoints' with the sub-tab 'ip-user-02'. The main content area is titled 'Password Guessing' and lists recent events. A search bar shows 'rule.id: 5503' with a count of '81 hits'. The table below shows the following data:

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|-------------------|-------|---------|-------------------------|
| Sep 3, 2024 @ 23:18:50.141 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:18:44.096 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:18:40.130 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:16:36.295 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:16:32.081 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:16:28.076 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:16:24.112 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 10:02:08.840 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |

The bottom section shows a chart titled 'Events count evolution' with a scale from 0 to 2,000. A message at the bottom left says 'New release is available! Go to the API configuration page for details'.

Not secure https://98.81.182.224/app/endpoints-summary#/agents?tab=welcome&agent=001&tabView=panels&_g=filters:!(),refreshInterval(pause...)

Endpoints ip-user-02

Threat Hunting **File Integrity Monitoring** **Configuration Assessment** **MITRE ATT&CK** **Malware Detection**

ID: 001 Status: disconnected IP address: 10.0.1.14 Version: Wazuh v4.8.2

Compliance

Recent events (224 hits)

Search rule.id: 5710 + Add filter

Time Technique(s) Tactic(s) Level Rule ID Description

- Sep 3, 2024 @ 23:16:56.104 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:54.319 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:52.101 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:50.099 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:48.096 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:44.092 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:42.089 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:40.088 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:36.295 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user

Events count evolution

New release is available! Go to the API configuration page for details

Not secure https://13.221.25.30/app/endpoints-summary#/agents?tab=welcome&agent=001&tabView=panels&_g=filters:!(),refreshInterval(pause...)

Endpoints ip-user-02

Threat Hunting **File Integrity Monitoring** **Configuration Assessment** **MITRE ATT&CK** **Malware Detection**

ID: 001 Status: disconnected IP address: 10.0.1.14 Version: Wazuh v4.8.2

Compliance

Recent events (224 hits)

Search rule.id: 5710 + Add filter

Time Technique(s) Tactic(s) Level Rule ID Description

- Sep 3, 2024 @ 23:16:56.104 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:54.319 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:52.101 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:50.099 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:48.096 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:44.092 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:42.089 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:40.088 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user
- Sep 3, 2024 @ 23:16:36.295 T1110.001 T1021.004 Credential Access, Lateral Movement 5 5710 sshd: Attempt to login using a non-existent user

Events count evolution

New release is available! Go to the API configuration page for details

Not secure https://chatgpt.com/g/g-xou5QobsE-kaligpt/c/68fa0000-f480-832a-8cd4-d4d7c648f0c5

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

KaliGPT 5

New chat Search chats Library Projects GPTs Explore KaliGPT Chats Fix Firebase quota error Fix npm init error Forensic investigation report Wazuh forensic investigation s...

Fixing private key format Owner or Editor role Questions on professionalism New chat Smart agriculture solution Firebase authentication types Electric shock in shower Greenhouse installation stats Security tools for link verification Visual timeline creation Mitch Koshy Free Upgrade

Geographical Distribution of Attacks

| Country | Region | IP Address | Total Hits | Example Users Attempted | Behavior Notes |
|---------|---------------------------|-----------------|--|--------------------------------------|--|
| India | Uttar Pradesh (Gorakhpur) | 263.192.236.110 | 180 (Rule 5710) + 30 (5503) + 8 (5760) = 218 total | baikal, pi, ubuntu, contador, admin | Most aggressive, repeated failed logins every few seconds; sequential ports. |
| China | Sichuan | 220.167.103.18 | 29 (5710) + 44 (5503) + 34 (5760) = 107 total | root, opensuse, webadmin, sa, deploy | Brute-force attempts on both invalid and root users; rotating ports per attempt. |
| Spain | Biscay (Bedia) | 85.85.196.35 | 15 (5710) + 7 (5503) + 0 (5760) = 22 total | carlos, ansuser, dockeradmin, sa | Lower frequency, but identical SSH brute-force pattern. |

Behavioral & Forensic Pattern Analysis

- Attack Consistency**
 - All three IPs used the same SSH brute-force technique: repeated "Failed password" or "Invalid user" attempts with rapid port changes (indicative of automated tooling such as Hydra, Medusa, or Ncrack).
- Consistent MITRE tagging in logs:**
 - T1110.001 (Password Guessing)
 - T1021.004 (SSH Remote Services)
 - Tactic: Credential Access, Lateral Movement.
- Credential Enumeration**
 - Attempts on non-existent users such as webadmin, opensuse, pi, baikal, contador, etc. indicate

Ask anything

ChatGPT can make mistakes. Check important info.

D. SSH

Technique details

ID

[T1021.004](#)

Tactics

[Lateral Movement](#)

Version

1.1

Recent events

272 hits

Summary Report – SSH Lateral Movement (MITRE ATT&CK T1021.004)

During forensic analysis of **SSH-related Lateral Movement activity**, a total of **272 events** were recorded between **September 2 and September 3, 2024**, targeting the host **Ip-user-02 (10.0.1.14)**. These events are mapped to **MITRE techniques T1021.004 (SSH)** and **T1110.001 (Password Guessing)**, indicating attempts to move laterally within the network by brute-forcing SSH credentials.

Out of the total detections, **224 hits** originated from **rule ID 5710**, which flagged repeated **login attempts using non-existent usernames** (e.g., *carlos*, *mariyah*, *baikal*), and **48 hits** came from **rule ID 5760**, indicating **authentication failures** for existing users such as *root* and *ubuntu*. The activity was traced to **three external IPs** – **85.85.196.35 (Spain – Bedia, Biscay)**, **220.167.103.10 (China – Sichuan)**, and **203.192.236.110 (India – Gorakhpur, Uttar Pradesh)**. All three conducted multiple SSH login attempts on the same target host, often from different ports but in rapid succession, suggesting **automated or scripted intrusion attempts**.

No successful authentications were observed, implying **no confirmed compromise**. However, the **volume, geographic diversity, and timing correlation** between the Credential Access (Password Guessing) and Lateral Movement (SSH) alerts strongly indicate an **active reconnaissance and brute-force campaign** aimed at pivoting into internal systems.

Key Forensic Findings:

- **Affected Host:** Ip-user-02 (10.0.1.14)
- **Primary Rules Triggered:** 5710 (Invalid user), 5760 (Authentication failed)

- **Technique IDs:** T1110.001 (Password Guessing), T1021.004 (SSH Lateral Movement)
- **Source IPs:**
 - 85.85.196.35 – Spain (Username: *carlos*)
 - 220.167.103.10 – China (Usernames: *root, mariah*)
 - 203.192.236.110 – India (Usernames: *ubuntu, baikal*)
- **Total Events:** 272 hits (224 invalid user + 48 failed auth)
- **Severity:** Level 5 – Suspicious/Malicious brute-force activity

Conclusion & Recommendations:

The evidence confirms that multiple external entities attempted **unauthorized SSH access** to an internal host, likely probing for weak credentials as a precursor to **lateral movement**. Although unsuccessful, this represents a **high-risk reconnaissance and intrusion attempt**. Immediate actions should include:

- Blocking and blacklisting the offending IPs at the firewall or intrusion prevention level.
- Implementing **rate-limiting, fail2ban, or SSH login throttling** on critical hosts.
- Enforcing **multi-factor authentication (MFA)** and **key-based SSH authentication**.
- Conducting a **credential audit** and reviewing **internal logs for lateral access attempts**.
- Correlating with **previous Credential Access events** to determine if these attackers have targeted other internal assets.

Findings Summary

- **Total Alerts:** 272
 - **Rule ID 5710 (Invalid SSH User Login Attempts):** 224 hits
 - **Rule ID 5760 (SSH Authentication Failures):** 48 hits
- **Affected Host:** **1p-user-02 (10.0.1.14)**
- **Event Severity:** Level 5 (High)
- **Techniques Involved:**
 - **T1110.001 – Password Guessing** (Credential Access)

- **T1021.004 – SSH (Lateral Movement)**

Indicators of Compromise (IOCs)

| IOC Type | Indicator | Details / Source | Geolocation |
|----------------|--------------------------------------|---|-----------------------------|
| Source IP | 220.167.103.10 | Multiple failed SSH attempts (root, mariah) | Sichuan, China |
| Source IP | 203.192.236.110 | Multiple failed SSH attempts (ubuntu, baikal) | Uttar Pradesh, India |
| Source IP | 85.85.196.35 | Multiple failed SSH attempts (carlos) | Biscay, Spain |
| Target Host | 10.0.1.14 (Ip-user-02) | Internal Linux host under brute-force attack | Local network |
| Target Port | 22/tcp (SSH) | Remote login attempts | - |
| Usernames Used | root, ubuntu, baikal, mariah, carlos | Invalid or non-existent accounts | |

Detailed Observations

- The attacker(s) attempted to **connect via SSH (port 22)** to the same internal host using various **invalid or default usernames**.
- Each IP maintained **multiple repeated attempts** (up to 15 **firedtimes** per session) within short time intervals, a strong sign of **automated brute-force or scripted behavior**.
- The same attack sequence appears under **two correlated rules** – “invalid user” (Rule 5710) and “authentication failed” (Rule 5760) – meaning attackers were not only trying non-existent accounts but also attempting passwords for valid or guessed usernames.
- No logs indicate **successful authentication**, meaning **no lateral movement was achieved yet**, but the pattern aligns with an **external reconnaissance and access attempt** targeting SSH services.
- GeolP correlation shows sources originating from **different regions**, implying the use of a **distributed botnet or proxy network** for SSH scanning and intrusion

attempts.

- The timestamps show consistent activity bursts around **Sep 2–3, 2024**, pointing to a coordinated campaign rather than random noise.

Interpretation / What Happened

An external threat actor (or a botnet) conducted a **brute-force password guessing campaign** targeting the internal Linux host **1p-user-02**. The goal was likely to obtain valid SSH credentials and move laterally within the network (MITRE T1021.004).

The observed activity represents the **early stage of a lateral movement attempt**, following the **credential access phase**. While all attempts failed, this activity exposes an **attack surface** that, if left unmitigated, could result in successful SSH compromise, privilege escalation, or internal spread.

Conclusion

The 272 SSH-related alerts on **1p-user-02** were triggered by repeated **failed login attempts from foreign IPs**, consistent with **automated brute-force and credential guessing** activity. While no breach has occurred, this behavior represents a **serious reconnaissance and intrusion attempt** targeting SSH services. Immediate mitigation and long-term SSH hardening are required to prevent future successful attacks and potential lateral movement within the environment.

POC

Endpoints | ip-user-02

SSH

Technique details

ID: T1021.004

Tactics: Lateral Movement

Version: 1.1

Recent events (48 hits)

Search: rule.id:5760 | DQL | May 1, 2024 @ 12:22:03.738 - Dec 1, 2025 @ 12:22:15.748 | Refresh

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|---------------------|-------------------------------------|-------|---------|------------------------------|
| Sep 3, 2024 @ 10:01:40.778 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:01:34.772 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:01:24.761 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:01:08.746 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:00:58.734 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:00:36.711 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |

Events count evolution

New release is available! Go to the API configuration page for details

Endpoints | ip-user-02

SSH

Technique details

ID: T1021.004

Tactics: Lateral Movement

Version: 1.1

Recent events (224 hits)

Search: rule.id:5710 | DQL | May 1, 2024 @ 12:22:03.738 - Dec 1, 2025 @ 12:22:15.748 | Refresh

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|---------------------|-------------------------------------|-------|---------|--|
| Sep 3, 2024 @ 23:16:56.104 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:54.319 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:52.101 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:50.096 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:48.096 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:44.092 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:40.090 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |

Events count evolution

New release is available! Go to the API configuration page for details

Endpoints | ip-user-02

SSH

Technique details

ID: T1021.004

Tactics: Lateral Movement

Version: 1.1

Recent events (272 hits)

Search: rule.id:5710 | DQL | May 1, 2024 @ 12:22:03.738 - Dec 1, 2025 @ 12:22:15.748 | Refresh

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|---------------------|-------------------------------------|-------|---------|--|
| Sep 2, 2024 @ 23:40:42.551 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 2, 2024 @ 23:40:42.546 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 2, 2024 @ 23:40:42.540 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 2, 2024 @ 23:40:42.534 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 2, 2024 @ 23:40:42.530 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 2, 2024 @ 23:40:42.523 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |

Events count evolution

New release is available! Go to the API configuration page for details

Lateral Movement – Summary Forensic Report

The forensic investigation into lateral movement activities revealed multiple correlated behaviors across several MITRE ATT&CK techniques — **Valid Accounts (T1078)**, **Remote Services (T1021)**, **Password Guessing (T1110.001)**, and **SSH (T1021.004)** — indicating coordinated attempts to move laterally within the network using remote authentication methods. The investigation identified a **recurring pattern of failed login attempts** and **unauthorized access trials** across multiple systems, particularly targeting the host **lp-user-02 (10.0.1.14)** through SSH and other remote service vectors. The use of **non-existent and default usernames**, **repeated password guessing**, and attempts to authenticate with **potentially compromised or reused credentials** suggest an attacker systematically probing for valid access points following initial reconnaissance and intrusion efforts observed earlier. While no successful lateral movement or privilege escalation was confirmed, the behavioral correlation with prior **initial access attempts (via credential reuse and external brute-force)** and subtle **defense evasion indicators (failed logins spread over time, multiple geolocations)** imply a structured intrusion sequence rather than random noise. The evidence collectively points to a **multi-stage attack chain**, where the adversary leveraged **password-based attacks and remote authentication channels** in pursuit of internal movement and persistence, but was effectively contained before gaining foothold. Continued vigilance is advised, as this lateral movement phase aligns closely with earlier credential harvesting activity and could precede future privilege escalation attempts if unaddressed.

5 credential access

A.Brute Force

Technique details

ID

T1110

Tactics

Credential Access

Version

2.5

Recent events

76 hits

1) Executive forensic findings (summary)

Multiple, coordinated SSH-based credential attacks targeted **lp-user-02 (10.0.1.14)** over a short time window from multiple external IPs. There are clear brute-force/password-guessing patterns (many “invalid user” and “failed password” events, repeated within seconds/minutes), and several “maximum authentication attempts exceeded” alerts. The most active source IPs are **203.192.236.110 (India / Gorakhpur, Uttar Pradesh)**, **220.167.103.10 (China / Sichuan)** and **85.85.196.35 (Spain / Biscay)**. These IPs repeatedly probed different usernames (common/default names and random trial names) on different ports — classic automated SSH

brute force. Separately, there are **successful SSH authentications** for a legitimate user `ctfroom` from IPs **34.226.207.84** and **52.5.37.243**, followed by **sudo / su to root** and execution/copying of `velociraptor` and stopping of the Wazuh agent. Taken together: broad external brute force activity likely attempted to find valid credentials; attackers later used at least one valid account (`ctfroom`) to escalate to root (evidence of sudo/su) and then attempted defense evasion (stopping Wazuh agent) and tooling deployment (`velociraptor`). This indicates a multi-stage intrusion: **credential attacks → use of valid account(s) → privilege escalation → defense evasion / tooling**.

Confidence: **High** the brute-force activity is malicious (multiple rules fired: brute-force, max attempts exceeded, invalid user). **High** confidence that privileged actions (sudo→su→root) occurred by `ctfroom`. **Moderate-High** confidence the sudo/root actions represent post-compromise attacker activity (given subsequent defense-evasion logs).

2) Key IOCs (extractable from supplied logs)

IPs (most frequent / high-priority):

- 203.192.236.110 — repeated (India, Gorakhpur / Uttar Pradesh) — many hits (failed logins, invalid users, max attempts).
- 220.167.103.10 — repeated (China, Sichuan) — many hits targeting `root` and invalid users on many source ports.
- 85.85.196.35 — repeated (Spain, Biscay) — many invalid-user/failed-password hits.
- 34.226.207.84 — successful SSH auth for `ctfroom`. (Possible attacker-controlled jump host.)
- 52.5.37.243 — successful SSH auth for `ctfroom`. (Possible attacker-controlled jump host.)
- 10.0.1.13 — an internal IP used to SSH as well (Accepted password for `ctfroom`). Targets / accounts:
 - `ctfroom` (successful auths, later sudo→root)
 - `root` (targeted by brute force)
 - common trial usernames observed: `pi, baikal, opensuse, webadmin, sa, guest, oracle, ubuntu, mariah, carlos, ansuser, craft`, many others (indicates automated wordlist)
- Files/commands (evidence of post-auth actions):
 - `cp velociraptor-v0.72.4-linux-amd64 /usr/local/bin/velociraptor`
 - `/usr/local/bin/velociraptor --config client.config.yaml client -v`
 - `sudo / su` – leading to root sessions
- Defense-evasion:

- Wazuh agent stop messages (rule 506 — “Wazuh agent stopped.”) on [1p-user-02](#) Logfile indicators / rule IDs (useful for SIEM detection):
- rule id 5710 (Attempt login non-existent user) — 224 hits (SSH invalid user / failed password)
- rule id 5551 (Multiple failed logins) — multiple hits
- rule id 5760 / 5503 / 5712 / 5758 / 5763 etc. (failed auths, max attempts, brute-force) Timestamps (examples):
- 2024-09-02T17:59:53 — failed password root from 220.167.103.10
- 2024-09-02T20:21:59 — Accepted password for ctfroom from 34.226.207.84
- 2024-09-02T20:25:52 — Accepted password for ctfroom from 52.5.37.243
- 2024-09-02T20:24:16 — sudo: cp velociraptor... (copying binary)
- 2024-09-03T06:14–08:58 — Wazuh agent stopped (three events)

3) Observed patterns & behavior

1. **Multiple-source automated brute force:** Distinct IP clusters (China/India/Spain) repeatedly attempt lots of usernames and passwords across many source ports — pattern of automated SSH scanner / credential stuffing / botnet activity.
2. **Distributed attacks but concentrated target:** All activity centers on host [1p-user-02](#) ([10.0.1.14](#)) — suggests attackers scanning Internet-exposed SSH and repeatedly targeting this host.
3. **Account enumeration + invalid users:** Log entries frequently show [Invalid user X](#) which means automated lists probing default/common usernames.
4. **Credential harvesting attempt + persistence:** High-volume failed attempts → some success for [ctfroom](#) from remote IPs (different source IPs). The successful authentications closely precede [sudo/su](#) activity and later defense-evasion (Wazuh stop) and tool deployment (velociraptor).
5. **Post-auth actions consistent with malicious operator:** Copying an agent binary to [/usr/local/bin](#), launching it, and stopping the monitoring agent indicates deliberate attacker behavior to persist and evade detection.
6. **Timing correlation:** Brute-force waves (max attempts exceeded, multiple failed logins) occur before or simultaneous with valid-account logins (T1078), then sudo escalation (T1548.003) and defense-evasion (T1562.001). This forms a clear chain.

4) Correlation with earlier stages you provided

- **Initial Access:** There are successful SSH auths (Accepted password for [ctfroom](#) from external IPs). This is the likely entry vector rather than a local exploit — the brute-force activity likely provided credentials or the attackers had credentials from another source

but still scanned.

- **Privilege Escalation:** Logs show `sudo/su` – by `ctfroom` and `pam_unix(sudo:session): session opened for user root`, indicating escalation to root. Sudo commands include copying `velociraptor` and launching client — indicates root-level commands executed.
- **Defense Evasion:** Wazuh agent stopped messages match attacker aim to disable host-based monitoring. Copying and launching a new tool (Velociraptor) may be to gain remote forensic control or persistence while disabling the local monitoring agent.
- **Lateral Movement:** Repeated external SSH attempts (T1021.004) indicate attempts to move laterally elsewhere or to pivot — but in the dataset the main lateral movement evidence is that `ctfroom` used sudo to become root on this host, potentially allowing further lateral actions.

Conclusion of correlation: the data fits a classic multi-stage intrusion: **external credential probing** → **use of valid account** → **escalate to root** → **disable agent & deploy tooling** → **(attempt) lateral movement**. That means the brute-force activity and successful `ctfroom` authentications are probably tied to the same adversary campaign.

5) What exactly happened (plain narrative)

Automated SSH brute-force scanners from multiple geographic sources attacked `lp-user-02`. One or more valid credentials for the local account `ctfroom` were used from remote IP(s) (34.226.207.84 & 52.5.37.243 and internal 10.0.1.13), allowing interactive logins. After logging in as `ctfroom`, the attacker invoked `sudo/su` to obtain root, copied `velociraptor` to `/usr/local/bin`, executed it and also stopped the Wazuh agent — actions consistent with persistence and detection avoidance. The brute-force waves (203.192.236.110, 220.167.103.10, 85.85.196.35) likely represent the scanning/background activity; whether those exact IPs supplied the credentials is unknown — but the temporal sequence and patterns strongly indicate these events are part of the same adversary activity.

Summary of Findings

- **Total Credential Access (Brute-Force) Hits: 76**
 - **65 hits via sshd decoder**
 - **11 hits via pam decoder**
- **Target Host: `lp-user-02` (10.0.1.14)**
- **Log Source: `/var/log/auth.log`**
- **Countries of Origin:**
 -  **India** – 24 hits (most activity, suggesting primary scanning source)
 -  **China** – 8 hits
 -  **Spain** – 2 hits
- **Pattern Observed:**

- Brute-force attempts primarily through **SSH**, combining **invalid username enumeration** and **password guessing**.
- The **same host** was repeatedly targeted from **multiple foreign IPs**, likely part of a **global botnet scanning for weak SSH credentials**.
- No confirmed successful authentication — suggesting **defenses held**, but the system remains **exposed to active credential attacks**.
- The repeated use of **non-existent users** followed by **root/ubuntu logins** shows **systematic brute-force behavior**.

POC

Brute Force

version
2.5

Recent events 11 hits

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|-------------------|-------|---------|--|
| Sep 3, 2024 @ 23:16:54.319 | T1110 | Credential Access | 10 | 5551 | PAM: Multiple failed logins in a small period of time. |
| Sep 3, 2024 @ 10:01:50.831 | T1110 | Credential Access | 10 | 5551 | PAM: Multiple failed logins in a small period of time. |
| Sep 3, 2024 @ 09:58:46.597 | T1110 | Credential Access | 10 | 5551 | PAM: Multiple failed logins in a small period of time. |
| Sep 3, 2024 @ 09:54:56.355 | T1110 | Credential Access | 10 | 5551 | PAM: Multiple failed logins in a small period of time. |
| Sep 3, 2024 @ 09:51:40.190 | T1110 | Credential Access | 10 | 5551 | PAM: Multiple failed logins in a small period of time. |
| Sep 2, 2024 @ 23:40:42.744 | T1110 | Credential Access | 10 | 5551 | PAM: Multiple failed logins in a small period of time. |
| Sep 2, 2024 @ 23:40:42.684 | T1110 | Credential Access | 10 | 5551 | PAM: Multiple failed logins in a small period of time. |
| Sep 2, 2024 @ 23:40:42.595 | T1110 | Credential Access | 10 | 5551 | PAM: Multiple failed logins in a small period of time. |
| Sep 2, 2024 @ 23:40:42.528 | T1110 | Credential Access | 10 | 5551 | PAM: Multiple failed logins in a small period of time. |
| Sep 2, 2024 @ 23:40:42.441 | T1110 | Credential Access | 10 | 5551 | PAM: Multiple failed logins in a small period of time. |

Events count evolution

New release is available! Go to the API configuration page for details

Brute Force

ID
T1110

Tactics
Credential Access

Version
2.5

Recent events 11 hits

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|-------------------|-------|---------|---|
| Sep 3, 2024 @ 23:16:38.086 | T1110 | Credential Access | 10 | 5712 | ssh: brute force trying to get access to the system. Non existent user. |
| Sep 3, 2024 @ 10:01:54.793 | T1110 | Credential Access | 10 | 5712 | ssh: brute force trying to get access to the system. Non existent user. |
| Sep 3, 2024 @ 09:59:16.629 | T1110 | Credential Access | 10 | 5712 | ssh: brute force trying to get access to the system. Non existent user. |
| Sep 3, 2024 @ 09:58:04.551 | T1110 | Credential Access | 10 | 5712 | ssh: brute force trying to get access to the system. Non existent user. |
| Sep 3, 2024 @ 09:56:40.463 | T1110 | Credential Access | 10 | 5712 | ssh: brute force trying to get access to the system. Non existent user. |
| Sep 3, 2024 @ 09:55:38.440 | T1110 | Credential Access | 10 | 5712 | ssh: brute force trying to get access to the system. Non existent user. |

Events count evolution

New release is available! Go to the API configuration page for details

Brute Force

Recent events (21 hits)

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|-------------------|-------|---------|---|
| Sep 3, 2024 @ 10:01:24.803 | T1110 | Credential Access | 8 | 5758 | Maximum authentication attempts exceeded. |
| Sep 3, 2024 @ 10:00:58.776 | T1110 | Credential Access | 8 | 5758 | Maximum authentication attempts exceeded. |
| Sep 3, 2024 @ 09:59:40.663 | T1110 | Credential Access | 8 | 5758 | Maximum authentication attempts exceeded. |
| Sep 3, 2024 @ 09:59:22.634 | T1110 | Credential Access | 8 | 5758 | Maximum authentication attempts exceeded. |
| Sep 3, 2024 @ 09:58:38.629 | T1110 | Credential Access | 8 | 5758 | Maximum authentication attempts exceeded. |
| Sep 3, 2024 @ 09:58:12.560 | T1110 | Credential Access | 8 | 5758 | Maximum authentication attempts exceeded. |
| Sep 3, 2024 @ 09:57:26.512 | T1110 | Credential Access | 8 | 5758 | Maximum authentication attempts exceeded. |
| Sep 3, 2024 @ 09:56:58.461 | T1110 | Credential Access | 8 | 5758 | Maximum authentication attempts exceeded. |
| Sep 3, 2024 @ 09:56:06.427 | T1110 | Credential Access | 8 | 5758 | Maximum authentication attempts exceeded. |

Table JSON Rule

Brute Force

Technique details

ID: T1110

Tactics: Credential Access

Version: 2.5

Recent events (32 hits)

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|-------------------|-------|---------|---|
| Sep 3, 2024 @ 10:01:58.840 | T1110 | Credential Access | 10 | 2502 | syslog: User missed the password more than one time |
| Sep 3, 2024 @ 10:01:40.820 | T1110 | Credential Access | 10 | 2502 | syslog: User missed the password more than one time |
| Sep 3, 2024 @ 10:01:24.804 | T1110 | Credential Access | 10 | 2502 | syslog: User missed the password more than one time |
| Sep 3, 2024 @ 10:00:58.776 | T1110 | Credential Access | 10 | 2502 | syslog: User missed the password more than one time |
| Sep 3, 2024 @ 10:00:26.705 | T1110 | Credential Access | 10 | 2502 | syslog: User missed the password more than one time |
| Sep 3, 2024 @ 10:00:10.902 | T1110 | Credential Access | 10 | 2502 | syslog: User missed the password more than one time |

Brute Force

Technique details

ID: T1110

Tactics: Credential Access

Version: 2.5

Recent events (76 hits)

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|-------------------|-------|---------|---|
| Sep 3, 2024 @ 23:16:54.319 | T1110 | Credential Access | 10 | 5551 | PAM: Multiple failed logins in a small period of time. |
| Sep 3, 2024 @ 23:16:38.066 | T1110 | Credential Access | 10 | 5712 | ssh: brute force trying to get access to the system. Non-existent user. |
| Sep 3, 2024 @ 10:01:58.840 | T1110 | Credential Access | 10 | 2502 | syslog: User missed the password more than one time |
| Sep 3, 2024 @ 10:01:54.793 | T1110 | Credential Access | 10 | 5712 | ssh: brute force trying to get access to the system. Non-existent user. |
| Sep 3, 2024 @ 10:01:50.831 | T1110 | Credential Access | 10 | 5551 | PAM: Multiple failed logins in a small period of time. |
| Sep 3, 2024 @ 10:01:40.820 | T1110 | Credential Access | 10 | 2502 | syslog: User missed the password more than one time |

Summary Report

During the investigation into **Credential Access – Brute Force (T1110)** activity, a total of **76 related events** were detected on host **Ip-user-02 (10.0.1.14)**, all sourced from

`/var/log/auth.log`. The activity was split between **sshd** (65 hits) and **PAM** (11 hits) decoders, indicating repeated failed authentication attempts over SSH. The attacks originated from multiple **foreign IPs**, mainly **India (24 hits)**, **China (8 hits)**, and **Spain (2 hits)**, targeting both **existing and non-existent usernames** such as `root`, `ubuntu`, and `carlos`. This consistent pattern of rapid, repeated login failures strongly suggests **automated brute-force attempts** aimed at guessing valid credentials for remote access. While no successful logins were observed, the frequency and distribution of attempts show that the system is being actively **probed for weak or default SSH passwords**, underscoring the need for continued monitoring, IP blocking, and enforcement of strong authentication controls.

B.SSH

Technique details

ID

T1021.004

Tactics

[Lateral Movement](#)

Version

1.1

Recent events

272 hits

Forensic findings – SSH / Credential Access (T1021.004 / T1110.001)

Scope & totals

- Total SSH-related events analyzed: **272 hits** (your dataset).
 - Rule **5710** ("Attempt to login using a non-existent user") = **224 hits**.
 - Rule **5760** ("authentication failed") = **48 hits**.
- All events originate from host **Ip-user-02 (10.0.1.14)**, file `/var/log/auth.log`.

High-level conclusion

- The logs show **automated, distributed password-guessing / brute-force activity over SSH** (credential guessing + attempts to log in as invalid/existing users). The

activity is high volume and comes from multiple remote IPs/countries (notably India, China, Spain). There are clear brute-force signatures (rapid repeated failures, “invalid user” attempts, “maximum authentication attempts exceeded”, repeated messages). There is **no clear proof in these SSH events alone of a successful remote compromise** by those attacking IPs – however, elsewhere in your dataset there are successful SSH authentications for user `ctfroom` and local sudo escalation to root; those should be correlated and fully investigated (see correlation section).

Evidence & patterns (what the logs show)

1. **Repeated failed logins for many usernames** (invalid and common names): `root`, `ubuntu`, `pi`, `carlos`, `webadmin`, `opensuse`, `sa`, `mariah`, `baikal`, `ansuser`, `guest`, `craft`, etc.
 - Many [5710](#) entries are “Failed password for invalid user X” or “Invalid user X” → attacker cycling through username lists.
2. **Burst / high-frequency behavior consistent with brute force / credential spray:**
 - Rule [5551](#) and [5758](#) fire for rapid, repeated PAM failures and “maximum authentication attempts exceeded”.
 - [5712](#) and [5763](#) show many consecutive invalid-user failures from same source IPs.
3. **Distributed sources but repeated same IPs:**
 - **203.192.236.110** (India – Gorakhpur, Uttar Pradesh): many hits (e.g., 24–180 count glimpses in your notes). Attempts against `ubuntu`, `pi`, invalid users; multiple failures and “max attempts exceeded”.
 - **220.167.103.10** (China – Sichuan): many hits (e.g., 29+ / 34 depending on rule), repeated failed attempts for `root`, `webadmin`, `opensuse`, etc., across many ports.
 - **85.85.196.35** (Spain – Biscay): repeated invalid-user attempts (e.g., `carlos`, `ansuser`, `dockeradmin` etc.).
These IPs reuse different source ports in multiple events – classic indication of automated SSH scanners / bots (either a small botnet or one host rotating ephemeral ports).
4. **Non-existent users + authentication failed messages** – test for valid accounts and password guessing. Many events are “invalid user”, indicating attackers try common usernames first.

5. **Severity / frequency:** Several rule hits were level 5 or level 10 (your rules flag many as high severity), and some triggered detection for “brute force” and “multiple failed logins”.
 6. **Temporal clustering:** Attempts are clustered in time windows (e.g., many events around `2024-09-02T18:00` and `2024-09-03T07:00` and `2024-09-03T20:16`), indicating scanning campaigns rather than one-off attempts.
-

IOCs (from the logs you provided)

Top attacking IP addresses

- 203.192.236.110 – India (Gorakhpur, Uttar Pradesh) – many hits (multiple rules).
- 220.167.103.10 – China (Sichuan) – many hits (multiple rules).
- 85.85.196.35 – Spain (Biscay) – many hits.

Example usernames tried

- root, ubuntu, pi, carlos, webadmin, opensuse, sa, mariah, baikal, ansuser, craft, dockeradmin, guest, contador, opensuse, max, naveen, test2, etc.

Ports – high-number ephemeral source ports observed (e.g., 57770, 7684, 52826, 33528, 51690, 45190). Destination is always SSH (port 22 on lp-user-02).

Event signatures

- `Failed password for invalid user <user> from <ip> port <n> ssh2`
 - `Invalid user <user> from <ip> port <n>`
 - `pam_unix(sshd:auth): authentication failure; ... rhost=<ip>`
 - `error: maximum authentication attempts exceeded for <user> from <ip> port <n> ssh2 [preauth]`
-

Timeline (representative events)

- 2024-09-02T17:59:53 – Failed password for root from 220.167.103.10 port 57770. (rule 5760 / 5763)
- 2024-09-02T18:08:57 – Failed password for invalid user `webadmin` from 220.167.103.10 port 15402. (rule 5710)
- 2024-09-02T18:10:13 – Failed password for invalid user `opensuse` from 220.167.103.10 port 62068. (rule 5710)
- 2024-09-03T07:01:24 – PAM multiple failures; 203.192.236.110 against `ubuntu`, repeated messages and max attempts exceeded (rules 2502 / 5551 / 5758).
- 2024-09-03T20:16:54 – Failed password for invalid user `carlos` from 85.85.196.35 port 52826; repeated sequence of failures for many invalid users (rules 5710 / 5712 / 5551).

(Your dataset contains dozens more; above are representative samples.)

Correlation with earlier stages (Initial Access / Privilege Escalation / Defense Evasion)

- **Initial access:** You reported earlier *successful* SSH logins for `ctfroom` from other IPs (e.g., accepted password for `ctfroom` from 34.226.207.84, 52.5.37.243, 10.0.1.13) and local sudo/su events where `ctfroom` opened sessions and became root (`sudo/su`). Those successful sessions are **not** from the same IPs listed above (203..., 220..., 85...). This suggests:
 - The brute-force activity (the attacking IPs above) **did not** directly produce the observed `ctfroom` successful logins (at least in the sampled logs).
 - The `ctfroom` successful access and subsequent local privilege escalation could be from a separate actor or a legitimate user; **they must be investigated in parallel** to confirm if they were malicious or legitimate admin activity.
- **Defense evasion:** You also showed Wazuh agent stops and sudo-to-root activity (velociraptor binary copied and executed). Those events are suspicious and correlate temporally with some authentication activity. **Key observation:** an attacker who gains valid credentials (via means other than the mass brute force – e.g., credential reuse, phishing, or earlier compromise) could then escalate and stop detection agents. So even if brute-force IPs didn't log a successful login, overall environment shows post-auth / evasive activity that warrants immediate containment/forensics.

Likely attacker behaviours / hypotheses

1. **Distributed automated SSH brute-force / credential-spray campaign** from multiple hosts (or a botnet) scanning and trying default/common usernames and passwords. Evidence: multiple source IPs, repeated invalid-user attempts, wide username dictionary, ephemeral source ports, “max attempts exceeded” alerts.
2. **Targeting of privileged accounts** (`root`, `ubuntu`, common service accounts) to gain initial foothold for lateral movement. Attempts on `root` are frequent (indicates opportunistic scanning for misconfigured SSH allowing root).
3. **Parallel activity:** Successful `ctfroom` logins and local sudo actions appear in your dataset from different IPs – possible separate compromise or legitimate admin activity. The combination of brute force probes + real successful local privilege escalations + agent stops (Wazuh, Velociraptor) is high-risk and consistent with an attacker reconnaissance → foothold → escalate → disable detection workflow.
4. **No clear confirmed remote compromise from the brute-force IPs** in these samples – but because of the correlated suspicious events (agent stops, sudo/cp of Velociraptor binary), you must treat the environment as potentially compromised until full host-level forensics are completed.

What likely happened (succinct narrative)

Automated, distributed SSH brute-force attempts (multiple countries / IPs) targeted `Ip-user-02` and attempted many usernames and passwords. While these brute-force IPs do not, in the sampled logs, show a definitive successful login, there are **separate successful SSH logins and sudo escalations for `ctfroom`** and evidence of detection tooling being stopped or a new binary being copied (Velociraptor), which together raise a high probability of compromise either by credential reuse or another attack vector. Treat the environment as potentially compromised and perform the host-level forensic collections and containment steps above.

Summary Report – SSH (Credential Access via Password Guessing)

The forensic analysis of SSH activity (MITRE ID: **T1021.004 – SSH**) under the **Credential Access** tactic revealed a total of **272 suspicious authentication attempts** originating from multiple foreign IP addresses, primarily **China and Spain**. These attempts were primarily categorized under two detection rules – **Rule ID 5710** (“Attempt to login using a non-existent user”) with **224 hits**, and **Rule ID 5760** (“Authentication failed”) with **48 hits**. The events consistently targeted the same host, **Ip-user-02 (10.0.1.14)**, and were logged in **/var/log/auth.log**, indicating sustained SSH brute-force activity attempting both valid and invalid usernames (e.g., `root`, `sa`, `carlos`, `ubuntu`). The frequency and distribution of attempts over short time intervals suggest an automated password-guessing attack. No successful SSH authentications were observed in this

phase, implying that the intrusion attempts were **unsuccessful**. However, the activity strongly correlates with previous **brute-force** and **valid account** attempts seen in earlier phases of the intrusion, suggesting an ongoing campaign aimed at credential harvesting and eventual lateral movement through compromised SSH services.

POC

Endpoints | ip-user-02

SSH

Recent events (48 hits)

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|---------------------|-------------------------------------|-------|---------|------------------------------|
| Sep 3, 2024 @ 10:01:40.778 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:01:34.772 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:01:24.761 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:01:08.746 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:00:58.734 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:00:36.711 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 09:50:16.056 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 09:50:04.044 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 09:49:46.021 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 09:49:34.009 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |

Events count evolution

New release is available! Go to the API configuration page for details

Endpoints | ip-user-02

SSH

Recent events (224 hits)

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|---------------------|-------------------------------------|-------|---------|--|
| Sep 3, 2024 @ 23:16:56.104 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:54.319 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:52.101 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:50.099 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:48.096 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:44.092 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:42.089 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:40.086 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:36.295 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:34.081 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |

Events count evolution

New release is available! Go to the API configuration page for details

Endpoints | ip-user-02

SSH

Recent events (272 hits)

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|---------------------|-------------------------------------|-------|---------|--|
| Sep 3, 2024 @ 23:16:56.104 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:54.319 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:52.101 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:50.099 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:48.096 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:44.092 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:42.089 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:40.086 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:38.295 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:34.081 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |

Events count evolution

New release is available! Go to the API configuration page for details

C.Password Guessing

Technique details

ID

[T1110.001](#)

Tactics

Credential Access

Version

1.4

Recent events

353 hits

Executive findings (short)

Multiple high-volume, automated SSH password-guessing campaigns (brute-force / invalid-user probes) targeted host **Ip-user-02 (10.0.1.14)** between **2024-09-02** and **2024-09-03**. Attackers originated from at least three distinct external clusters (India, China, Spain). The SSH guessing activity (many invalid user attempts + many failed root/ubuntu attempts) escalated into **valid SSH authentications** for the **ctfroom** account, followed by **privilege escalation via sudo** (ctfroom → root), installation/copying of **velociraptor** under **/usr/local/bin** and **Wazuh agent stoppage** events. These items form a coherent attack chain: credential harvesting → lateral access → privilege escalation → persistence and defense evasion.

Conclusion: evidence indicates an automated credential-harvest campaign that **succeeded** in obtaining a valid account (**ctfroom**) and achieving root actions (sudo + binary copy + agent stoppage). Treat Ip-user-02 as compromised.

Key IOCs (extracted from provided logs)

Host

- Target host: Ip-user-02 — agent IP **10.0.1.14**, logs at **/var/log/auth.log**.

Attacker source IPs (repeated across events)

- **203.192.236.110** — India (Uttar Pradesh / Gorakhpur). Many hits (≈180 in your grouping; repeated failed attempts, many targeting **ubuntu**, **pi**, **baikal**, etc.).
- **220.167.103.10** — China (Sichuan). Many hits (≈29–44 depending on rule), repeated attempts, often targeting **root**, **webadmin**, **opensuse**, **guest**, etc.

- 85.85.196.35 — Spain (Biscay). Many hits (~15), repeated invalid users such as `carlos`, `ansuser`, `craft`, etc.
- Also observed ephemeral source IPs (cloud ranges): 52.5.37.243, 34.226.207.84, 10.0.1.13 (internal), used in latter successful auths.

Usernames observed (attempts / invalid)

- Invalid / guessed: `carlos`, `opensuse`, `deploy`, `webadmin`, `sa`, `pi`, `baikal`, `contador`, `guest`, `craft`, `oracle`, `max`, `naveen`, `test2`, `ubuntu`, `root`, `ansuser`, `carlos`, `dockeradmin`, etc.
- Valid account later used: `ctfroom` (Accepted password events).

Ports

- SSH destination port default 22; varying source ports noted (e.g., 52826, 51690, 33528, 45190, 57770, 64490, 7684, 7501, etc.). Many attempts used varying source ports (typical of distributed or scripted scans).

Timestamps (range)

- Main activity cluster: **2024-09-02 17:59 UTC → 2024-09-03 23:16 UTC**. Brute force bursts cluster around **2024-09-03T07:00-07:02Z** (India) and **2024-09-03T20:16Z** (Spain), and many China attempts on **2024-09-02T18:00-18:11Z**.

Rules / Alerts

- Rule id 5710 (Attempt to login using non-existent user) — **224 hits** (majority of invalid user guessing).
- Rule id 5760 (sshd: authentication failed) — **48 hits**.
- Rule id 5503 (PAM: User login failed) — **81 hits**.
- Brute force rules: 5551, 5712, 5763, 5758 also fired (frequency / max auth attempts exceeded).

Chronological / correlation summary (how events tie together)

1. Password Guessing / Brute Force

- Multiple, high-frequency failed SSH attempts from the listed IP clusters. These are classic automated password-guessing patterns: many different usernames, repeated attempts over short intervals, "message repeated" entries, and "maximum authentication attempts exceeded" errors.

2. Successful Remote Service (SSH) Access

- After the brute force activity, logs show **Accepted password for ctfroom** from several IPs (e.g., `34.226.207.84`, `52.5.37.243`, `10.0.1.13`). This indicates **a valid account was compromised** (or that those IPs were legitimate remote admins — but correlation with other malicious activity suggests compromise).

3. Privilege Escalation (Sudo)

- `ctfroom` executed `sudo` commands and `su` – to root (multiple entries). Sudo logs show `ctfroom` opened a root session (`pam_unix(sudo:session): session opened for user root(uid=0) by ctfroom(uid=1001)`).

4. Post-Escalation actions (persistence / defense evasion)

- `ctfroom` used `sudo` to copy `velociraptor-v0.72.4-linux-amd64` to `/usr/local/bin/velociraptor` and later ran `/usr/local/bin/velociraptor --config client.config.yaml client -v`.
- The Wazuh agent stopped three times (`T1562.001` events). This suggests attempted disabling/alteration of host monitoring. Correlation: sudo root activity → velociraptor installation → Wazuh stoppage fits an attacker trying to install a remote monitoring/collection agent (Velociraptor often used legitimately for DFIR, but attackers sometimes misuse remote agents) and suppress detection.

5. Lateral movement hints

- The presence of valid external IPs that later authenticate plus remote services use indicates lateral or external foothold attempts. No immediate evidence in supplied logs of successful lateral hop beyond Ip-user-02, but the pattern enables lateral movement opportunities if further pivots exist.

Confidence: High for automated brute-force + compromise of `ctfroom`. High for sudo → root and binary copy. Medium-High that Wazuh stoppage was attacker-initiated (timing and context strongly suggest it).

Specific suspicious/malicious indicators & analytic notes

- **Repeated source IPs:** `203.192.236.110`, `220.167.103.10`, `85.85.196.35` — repeated across many rules and timestamps. These should be treated as malicious scanning/brute-force nodes (block & investigate).
- **Repeated usernames:** Many common/default account names (`root`, `ubuntu`, `pi`, `admin`, `sa`, `webadmin`, `opensuse`, `carlos`, etc.) — consistent with credential stuffing / wordlists.
- **Throttle / burst pattern:** Multiple logs with `message repeated X times` and `Maximum authentication attempts exceeded` → automated tool (e.g., mass SSH scanner / bot/net).

- **Successful logins from cloud IPs:** `34.226.207.84 / 52.5.37.243 / 10.0.1.13` used for accepted logins. Investigate whether these are attacker infrastructure or legitimate admin access that coincides.
- **Post-auth sudo actions:** Copy/install and execution of Velociraptor binary — suspicious in the absence of legitimate admin activity.
- **Wazuh agent stoppage:** Strong defense evasion signal — stop of monitoring agents immediately after root actions is high priority.

Final analytical assessment (one paragraph)

The collected logs depict an automated multi-source password-guessing campaign that targeted `lp-user-02`, culminating in a **likely successful compromise**: a valid account (`ctfroom`) was leveraged to gain root via `sudo`, a binary (`velociraptor`) was installed/executed, and the host monitoring agent (Wazuh) was stopped. The observed IOCs (notably `203.192.236.110`, `220.167.103.10`, `85.85.196.35`), the volume and cadence of failed attempts, and the subsequent privileged actions form a canonical attack progression (credential harvesting → access → escalation → persistence/defense evasion). Immediate containment, forensic collection, and credential rotation are required; assume lateral risk and hunt across the environment for similar signs.

What happened (single-paragraph forensic narrative you can share)

Attackers launched automated, high-volume SSH password-guessing campaigns from multiple external IP clusters (notably `203.192.236.110` — India, `220.167.103.10` — China, `85.85.196.35` — Spain). These brute-force attempts generated hundreds of failed logins and multiple “maximum authentication attempts exceeded” events. Subsequently, the `ctfroom` account was authenticated successfully from external addresses; `ctfroom` then used `sudo` to escalate to root, copied a `velociraptor` binary into `/usr/local/bin`, and executed it. Around this time the Wazuh agent stopped repeatedly. The combined sequence (password guessing → successful SSH login → sudo/root activity → installation of a remote collection/agent binary → monitoring agent stoppage) strongly indicates the host `lp-user-02` was compromised and the attackers attempted to establish persistence and evade detection.

POC

Screenshot of a Wazuh endpoint monitoring interface showing a list of recent password guessing events.

Endpoint Details:

- ID: 001
- Status: disconnected
- IP address: 10.0.1.14
- Version: Wazuh v4.8.2

Recent Events: 48 hits

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|---------------------|-------------------------------------|-------|---------|------------------------------|
| Sep 3, 2024 @ 10:01:40.778 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:01:34.772 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:01:24.761 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:01:08.746 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:00:58.734 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 10:00:36.711 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 09:50:16.055 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 09:50:04.044 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 09:49:46.021 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |
| Sep 3, 2024 @ 09:49:34.009 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5760 | sshd: authentication failed. |

Events count evolution: 2,000, 1,500, 1,000

New release is available! Go to the API configuration page for details

Rows per page: 10 < 1 2 3 4 5 >

Screenshot of a Wazuh endpoint monitoring interface showing a list of recent password guessing events.

Endpoint Details:

- ID: 001
- Status: disconnected
- IP address: 10.0.1.14
- Version: Wazuh v4.8.2

Recent Events: 224 hits

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|---------------------|-------------------------------------|-------|---------|--|
| Sep 3, 2024 @ 23:16:56.104 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:54.319 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:52.101 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:50.099 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:48.096 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:44.092 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:42.089 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:40.088 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:38.295 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:36.081 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |

Events count evolution: 2,000, 1,500, 1,000

New release is available! Go to the API configuration page for details

Rows per page: 10 < 1 2 3 4 5 ... 23 >

Screenshot of the Wazuh web interface showing the "Endpoints" tab for "ip-user-02".

The interface includes a header with navigation links: Threat Hunting, File Integrity Monitoring, Configuration Assessment, MITRE ATT&CK, Malware Detection, and a search bar.

On the left, there's a sidebar with sections for MITRE ATT&CK (showing a compliance donut chart), Events count evolution (a line graph from 1,000 to 2,000), and a message about a new release available.

The main content area is titled "Password Guessing" and displays a table of recent events:

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|---------------------|-------------------------------------|-------|---------|--|
| Sep 3, 2024 @ 23:16:50.104 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:54.319 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:52.101 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:50.141 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:16:50.099 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:48.096 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:44.096 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:16:44.092 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:42.069 | T1110.001 T1021.004 | Credential Access, Lateral Movement | 5 | 5710 | sshd: Attempt to login using a non-existent user |
| Sep 3, 2024 @ 23:16:40.130 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |

Below the table, there's a note: "Rows per page: 10" and a navigation bar with pages 1 through 36.

Screenshot of the Wazuh web interface showing the "Endpoints" tab for "ip-user-02".

The interface includes a header with navigation links: Threat Hunting, File Integrity Monitoring, Configuration Assessment, MITRE ATT&CK, Malware Detection, and a search bar.

On the left, there's a sidebar with sections for MITRE ATT&CK (showing a compliance donut chart), Events count evolution (a line graph from 1,000 to 2,000), and a message about a new release available.

The main content area is titled "Password Guessing" and displays a table of recent events, filtered by rule ID 5503:

| Time | Technique(s) | Tactic(s) | Level | Rule ID | Description |
|----------------------------|--------------|-------------------|-------|---------|-------------------------|
| Sep 3, 2024 @ 23:16:50.141 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:16:44.096 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:16:40.130 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:16:36.295 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:16:32.081 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:16:28.079 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 23:16:24.112 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 10:02:08.849 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 10:01:32.769 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |
| Sep 3, 2024 @ 10:01:06.743 | T1110.001 | Credential Access | 5 | 5503 | PAM: User login failed. |

Below the table, there's a note: "Rows per page: 10" and a navigation bar with pages 1 through 36.