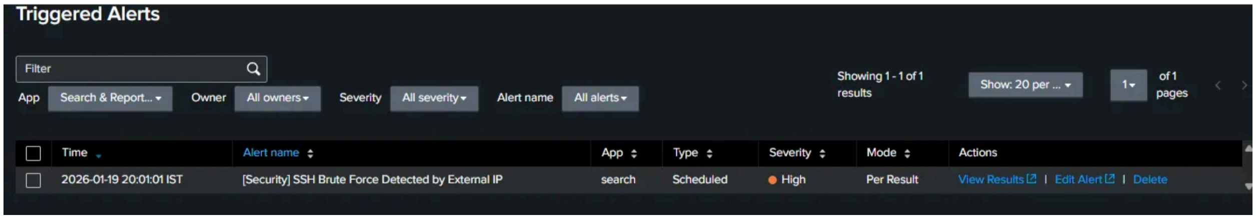
SOC INCIDENT REPORT (L1)

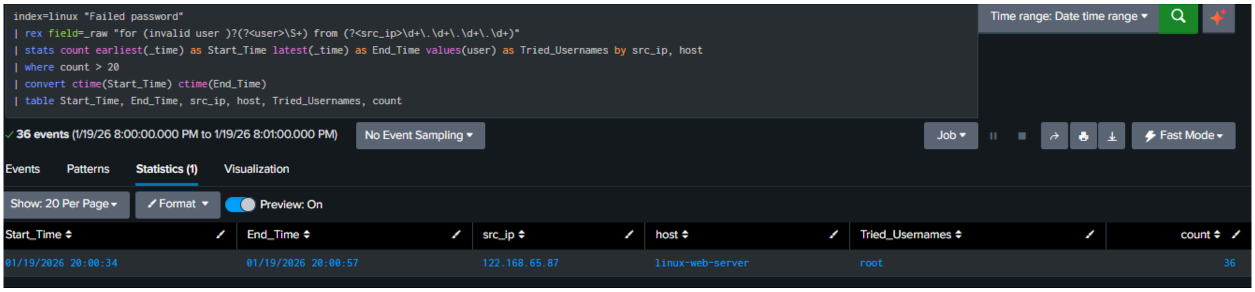
1. Incident Identification


Triggered Alerts

□	Time	Alert name	App	Type	Severity	Mode	Actions
□	2026-01-19 20:01:01 IST	[Security] SSH Brute Force Detected by External IP	search	Scheduled	● High	Per Result	View Results | Edit Alert | Delete

- **Incident ID:**
  SSH-2026-01-19
- **Alert ID / Event ID:**
  02
- **Detection Source:** (SIEM / EDR / IDS / Email Gateway / Firewall)
  SIEM
- **Detection Rule Name:**
  [Security] SSH Brute Force Detected by External IP
- **Severity Level:** (Low / Medium / High / Critical)
  High
- **Confidence Level:** (Low / Medium / High)
  High
- **Date & Time Detected (UTC):**
  2026-01-19 14:31:01 UTC
- **Reporting Analyst:**
  Shewag Bhattarai
- **Business Unit / Asset Owner:**
  Aayan

2. Incident Summary (Executive Overview)



```
index=linux "Failed password"
| rex field=_raw "for (invalid user )?(?<user>\S+) from (?<src_ip>\d+\.\d+\.\d+\.\d+)"
| stats count earliest(_time) as Start_Time latest(_time) as End_Time values(user) as Tried_Usernames by src_ip, host
| where count > 20
| convert ctime(Start_Time) ctime(End_Time)
| table Start_Time, End_Time, src_ip, host, Tried_Usernames, count
```

✓ **36 events** (1/19/26 8:00:00.000 PM to 1/19/26 8:01:00.000 PM)

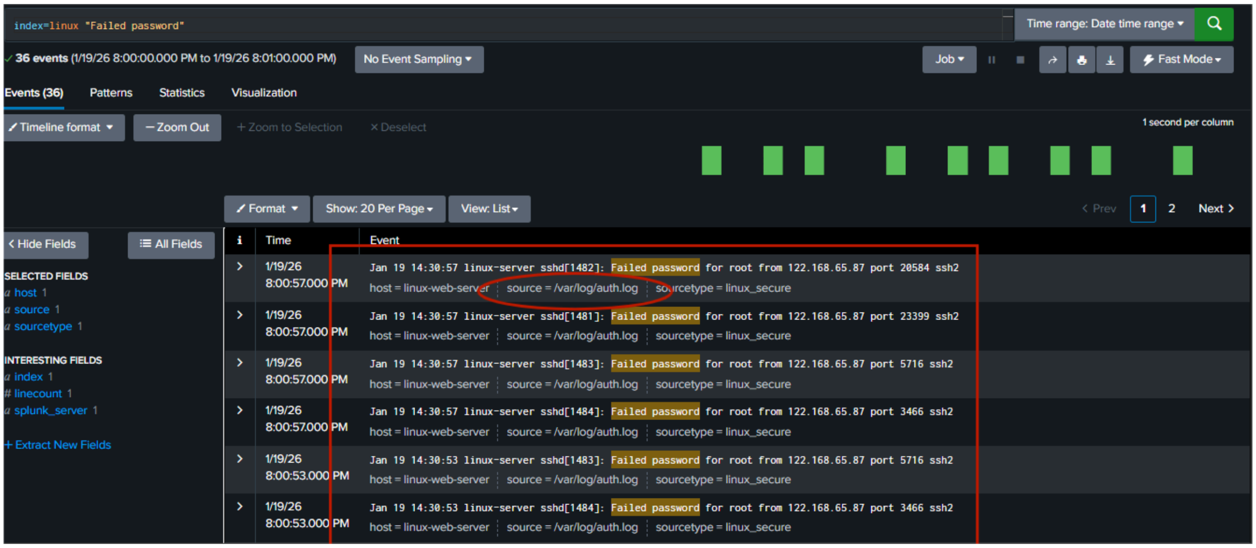
Start_Time	End_Time	src_ip	host	Tried_Usernames	count
01/19/2026 20:00:34	01/19/2026 20:00:57	122.168.65.87	linux-web-server	root	36

- **Incident Type:** (e.g., Phishing, Brute Force, Malware, Web Attack)
  SSH Brute Force
- **Initial Assessment:** (Suspected / Confirmed / Benign)
  Confirmed
- **Current Status:** (Open / Contained / Escalated / Closed)
  Closed
- **Impact Level:** (None / Low / Moderate / High)
  None

3. Affected Assets

Asset Type	Hostname / Identifier	IP Address	OS / Platform	Role
Web-Server	LIN-WEB-001	...*	Linux	Web-Admin

4. Detection Details



```
index=linux "Failed password"
```

✓ 36 events (1/19/26 8:00:00.000 PM to 1/19/26 8:01:00.000 PM)

```
i  Time                    Event
>  1/19/26                 Jan 19 14:30:57 linux-server sshd[1482]: Failed password for root from 122.168.65.87 port 20584 ssh2
   8:00:57.000 PM          host = linux-web-server   source = /var/log/auth.log   sourcetype = linux_secure
>  1/19/26                 Jan 19 14:30:57 linux-server sshd[1481]: Failed password for root from 122.168.65.87 port 23399 ssh2
   8:00:57.000 PM          host = linux-web-server   source = /var/log/auth.log   sourcetype = linux_secure
>  1/19/26                 Jan 19 14:30:57 linux-server sshd[1483]: Failed password for root from 122.168.65.87 port 5716 ssh2
   8:00:57.000 PM          host = linux-web-server   source = /var/log/auth.log   sourcetype = linux_secure
>  1/19/26                 Jan 19 14:30:57 linux-server sshd[1484]: Failed password for root from 122.168.65.87 port 3466 ssh2
   8:00:57.000 PM          host = linux-web-server   source = /var/log/auth.log   sourcetype = linux_secure
>  1/19/26                 Jan 19 14:30:53 linux-server sshd[1483]: Failed password for root from 122.168.65.87 port 5716 ssh2
   8:00:53.000 PM          host = linux-web-server   source = /var/log/auth.log   sourcetype = linux_secure
>  1/19/26                 Jan 19 14:30:53 linux-server sshd[1484]: Failed password for root from 122.168.65.87 port 3466 ssh2
   8:00:53.000 PM          host = linux-web-server   source = /var/log/auth.log   sourcetype = linux_secure
```

- **Log Source(s):**
  /var/log/auth.log
- **Index / Data Source:**
  linux-server
- **Timestamp Range Analyzed:**
  - **Start Time:** 2026-01-19 14:30:34 UTC
  - **End Time:** 2026-01-19 14:30:57 UTC
- **Trigger Condition:** SSH Brute Force Detected by External IP
- **Observed Behavior:**
  36 SSH failed login attempt for user root from external IP **122.168.65.87**

5. Threat Analysis

5.1 MITRE ATT&CK Mapping

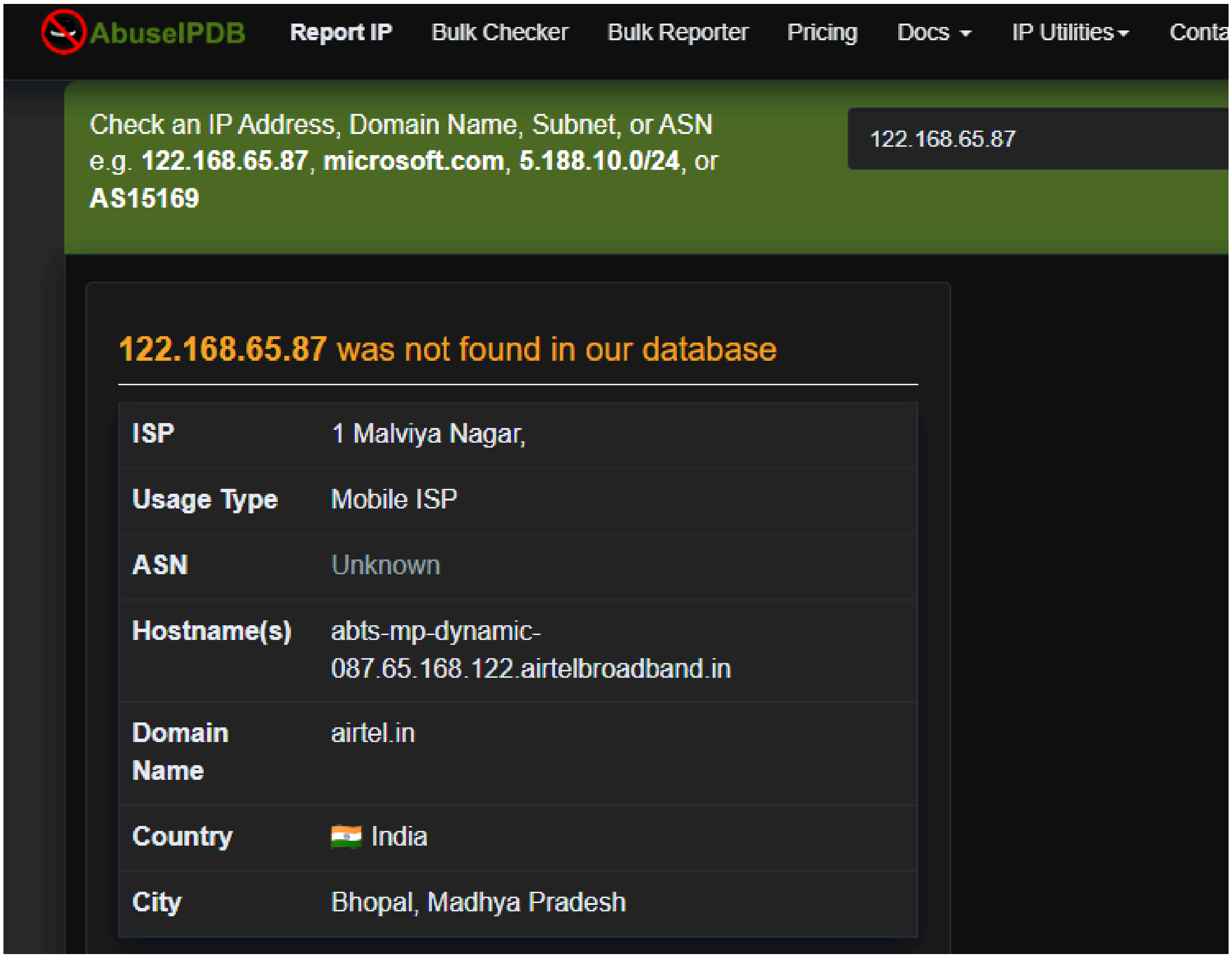
- **Tactic:**
  Credential Access
- **Technique ID:**
  T1110

- **Technique Name:**
  Brute Force
- **Sub-Technique (if applicable):**
  T1110.003 – Password Spraying

5.2 Indicators of Compromise (IOCs)

IOC Type	Value	Source	Verdict
IPv4 Address	`122.168.65.87`	Splunk `(auth.log)`	Malicious
Targeted user	root	Splunk `(auth.log)`	Targeted

5.3 Threat Intelligence Correlation

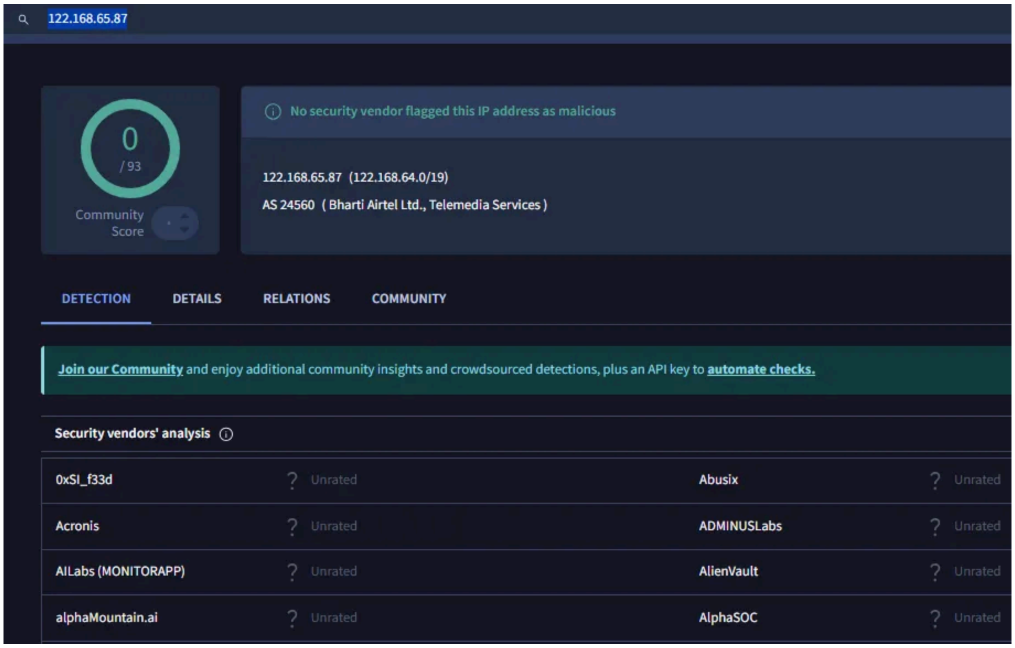


Check an IP Address, Domain Name, Subnet, or ASN
e.g. **122.168.65.87**, **microsoft.com**, **5.188.10.0/24**, or **AS15169**

122.168.65.87

122.168.65.87 was not found in our database

ISP	1 Malviya Nagar,
Usage Type	Mobile ISP
ASN	Unknown
Hostname(s)	abts-mp-dynamic-087.65.168.122.airtelbroadband.in
Domain Name	airtel.in
Country	India
City	Bhopal, Madhya Pradesh



No security vendor flagged this IP address as malicious

122.168.65.87 (122.168.64.0/19)
AS 24560 (Bharti Airtel Ltd., Telemedia Services)

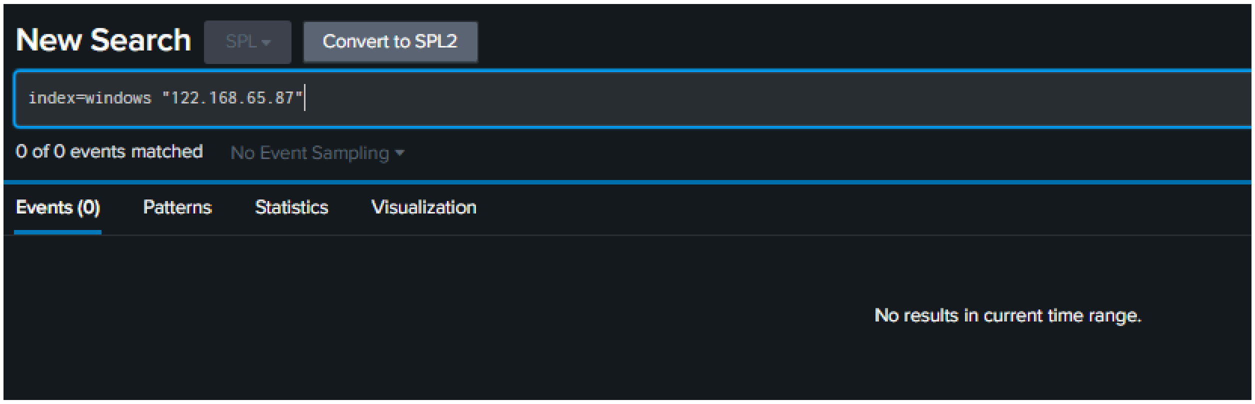
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

0xSI_f33d	? Unrated	Abusix	? Unrated
Acronis	? Unrated	ADMINUSLabs	? Unrated
AILabs (MONITORAPP)	? Unrated	AlienVault	? Unrated
alphaMountain.ai	? Unrated	AlphaSOC	? Unrated

- **Reputation Checks Performed:** (Yes / No)
  yes
- **Sources Used:** (VirusTotal / AbuseIPDB / Talos / Internal TI)
  VirusTotal / AbuseIPDB
- **Result Summary:**
  Malicious(This is just a demo report, the source IP belongs to myself.)

6. Investigation Findings

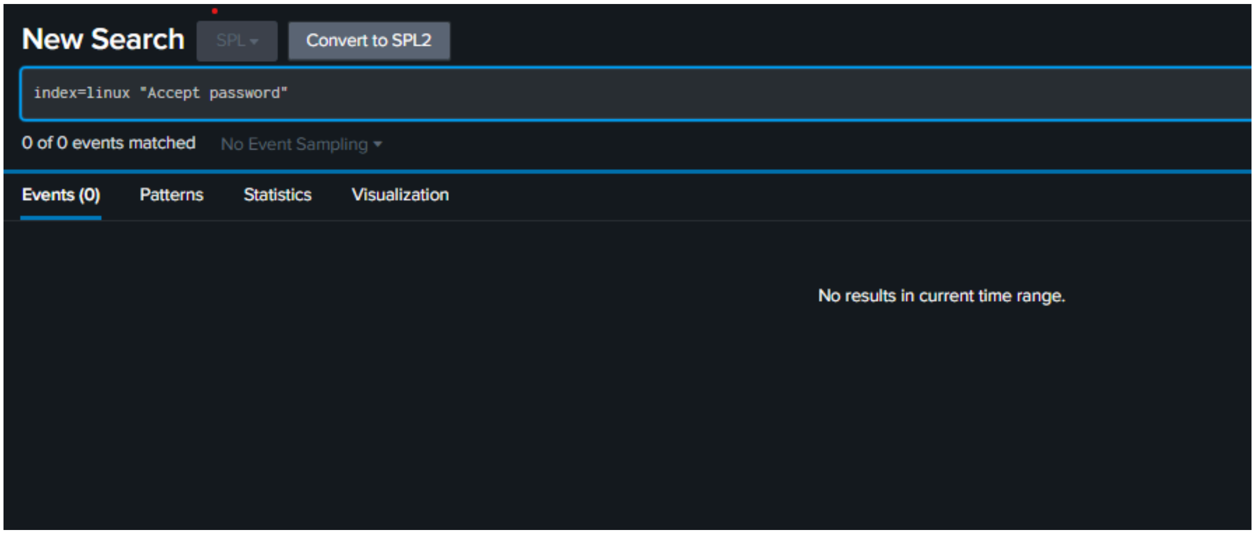


```
index=windows "122.168.65.87"
```

0 of 0 events matched

No results in current time range.

- **Root Cause Analysis:**
  SSH port was open to internet AND Password Authentication was enabled in `/etc/ssh/sshd_config`
- **Attack Vector:External Remote Services (T1133).** The attacker targeted an exposed public-facing service (SSH) from the internet.
- **Lateral Movement Observed:** (Yes / No)
  No. (The attack consisted of *failed* login attempts. Since they did not successfully log in, they could not move to other machines)



```
index=linux "Accept password"
```

0 of 0 events matched

No results in current time range.

- **Privilege Escalation Observed:** (Yes / No)
  No. (They attempted to guess the `root` password, but failed).
- **Data Access / Exfiltration:** (None / Suspected / Confirmed)
  None. (No session was established, so no data could be touched).

---

7. Impact Assessment (NIST SP 800-61)

- **Confidentiality Impact:** (None / Low / Moderate / High)
  None*Reasoning:* The attacker failed to authenticate. No sensitive information was disclosed or accessed.
- **Integrity Impact:** (None / Low / Moderate / High)
  None*Reasoning:* No files or configurations were modified because the attacker never gained entry.

- **Availability Impact:** (None / Low / Moderate / High)
  None (or **Low**)
  Reasoning: The SSH service remained active and accessible to legitimate users. The attack did not cause a Denial of Service (DoS).

8. Containment Actions (If Any)

Action Taken	Timestamp	Performed By
Removed Firewall Rule (allow-ssh-danger)	2026-01-19 23:20 IST	L1 Analyst
Disabled SSH Password Auth (`sshd_config`)	2026-01-19 23:25 IST	L1 Analyst
Restarted SSH Service	2026-01-19 23:26 IST	L1 Analyst

9. Escalation Decision

- **Escalated to L2 / IR Team:** (Yes / No)
  No
- **Reason for Escalation:**
  - Not applicable. The incident was successfully contained at the L1 level. The attack was unsuccessful (no login occurred), and the vulnerability was remediated by disabling password authentication.
- **Escalation Time:**
  N/A

10. Incident Classification

- **True Positive / False Positive:**
  True Positive
- **Attack Success:** (Failed / Partial / Successful)
  Failed
- **Policy Violation:** (Yes / No)
  Yes

11. Recommendations

- **Immediate Remediation Actions:**
  - Ensure `PasswordAuthentication` remains disabled in `/etc/ssh/sshd_config`.
  - Maintain the firewall block on the attacker IP (`122.168.65.87`) for 30 days.
- **Preventive Controls Suggested:**
  - **Implement Fail2Ban:** Automated tool to ban IPs after 3 failed login attempts.
  - **VPN / Bastion Host:** Restrict SSH access so it is only accessible via a private VPN, removing it from the public internet.
- **Detection Gaps Identified:**
  N/A

12. Closure Summary

- **Final Verdict:**
  True Positive - Mitigated
- **Business Risk Post-Incident:** (Low / Medium / High)
  `Low`
  - *(Reason: The vulnerability was patched, and no successful access occurred.)*
- **Incident Closed By:**
  L1 Analyst
- **Closure Date & Time (UTC):**
  2026-01-19 17:55 UTC

13. Evidence & Artifacts

Artifact Type	Description	Location / Reference
Splunk Logs	CSV export of the 62 failed authentication attempts.	auth_logs_export.csv

Artifact Type	Description	Location / Reference
Screenshot	Dashboard showing the spike in traffic from 122.168.65.87.	dashboard_spike.png

14. Compliance & Framework Alignment

- **NIST Incident Response Phase:** (Preparation / Detection / Analysis / Containment / Eradication / Recovery)
  Detection / Analysis / Containment / Eradication / Recovery
- **MITRE ATT&CK Coverage Confirmed:** (Yes / No)
  Yes
- **Internal SOC Playbook Referenced:** (Yes / No)
  Yes