

Security Incident Report

DVWA System Incident

Executive Summary

On June 30, 2025 at 5:00 PM (UTC -03:00), the organization became aware of multiple login attempts and web directory enumeration against the DVWA system. The incident, considered of medium severity, was detected in real time by the monitoring software (Splunk Enterprise) and quickly mitigated without data compromise

Affected Systems and Tools Used

Type of attack: SSH Brute-force and e Web Directory Fuzzing

Tools involved: Hydra, Dirb, Splunk

Affected services: SSH and Web Server

Timeline

Incident Date: 2025-06-30T17:00:00.000-0300

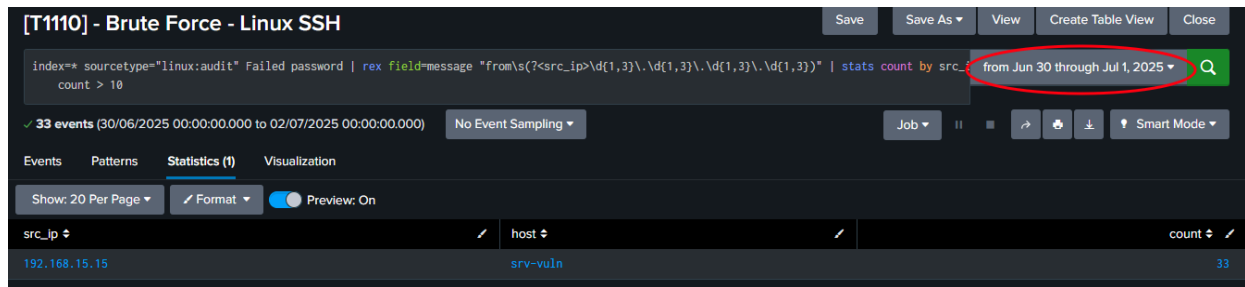
Incident Acknowledgment: 2025-06-30T17:04:00.000-0300

Actions taken:

- **Attacker IP blocked via firewall:** 2025-06-30T17:05:00.000-0300
- **Password reset for targeted account:** 2025-06-30T17:09:00.000-0300
- **System accessed for audit and data integrity verification:**
2025-06-30T17:15:00.000-0300
- **Team leader notified via email:** 2025-06-30T17:42:00.000-0300

Incident Evidence

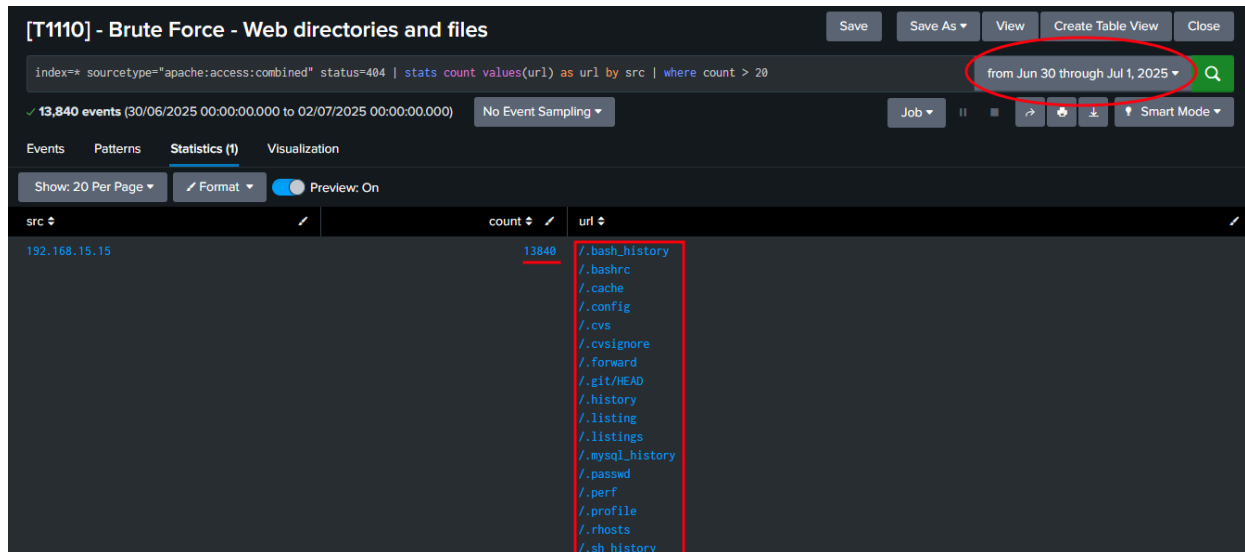
Splunk logs confirmed 33 SSH login attempts from source IP **192.168.15.15** targeting the **srv-vuln** host



The screenshot shows a Splunk search interface for the title "[T1110] - Brute Force - Linux SSH". The search bar contains the query: `index=* sourcetype="linux:audit" Failed password | rex field=message "from\s(<src_ip>\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3})" | stats count by src_ip where count > 10`. The time range is set to "from Jun 30 through Jul 1, 2025". The results show 33 events. Below the search bar, there are tabs for "Events", "Patterns", "Statistics (1)", and "Visualization". The "Statistics (1)" tab is selected, showing a table with columns "src_ip", "host", and "count".

src_ip	host	count
192.168.15.15	srv-vuln	33

Splunk also detected over 13,000 HTTP requests resulting in 404 status codes, along with several numbered directory patterns, indicating a high probability of automated fuzzing activity targeting web directories.



The screenshot shows a Splunk search interface for the title "[T1110] - Brute Force - Web directories and files". The search bar contains the query: `index=* sourcetype="apache:access:combined" status=404 | stats count values(url) as url by src | where count > 20`. The time range is set to "from Jun 30 through Jul 1, 2025". The results show 13,840 events. Below the search bar, there are tabs for "Events", "Patterns", "Statistics (1)", and "Visualization". The "Statistics (1)" tab is selected, showing a table with columns "src", "count", and "url".

src	count	url
192.168.15.15	13840	<ul style="list-style-type: none">/.bash_history/.bashrc/.cache/.config/.cvs/.cvsignore/.forward/.git/HEAD/.history/.listing/.listings/.mysql_history/.passwd/.perf/.profile/.rhosts/.sh_history

Impact Assessment

Medium severity incident. No systems were compromised. All attempts were successfully blocked

Root Cause

Automated attacks using Hydra and Dirb exploiting weak authentication and predictable directory structures.

Response actions

Containment

- Attacker IP blocked via firewall

Eradication

- Password reset for targeted user
- Removal of unnecessary public files from the web server.

Recovery

- Implementation of enhanced authentication (SSH key + 2FA).
- Firewall rule validation and analysis of new access attempts

Recommendation and Post-Incident Activities

- Full documentation of the incident and response actions
- Enable rate limiting on the web application
- Recommend starting development of automated playbooks via SOAR
- Update password complexity policy

The incident was successfully closed and reinforced the importance of a structured response process.