SSH Brute-Force Detection & Analysis Dashboard in Splunk

Project Report

Prepared by

Roshinni Gandhi

Aspiring SOC Analyst

Date: September 2025

Table Of Contents

Executive Summary

This project focuses on analyzing SSH authentication logs using Splunk, with the goal of simulating a Security Operations Center (SOC) workflow. SSH login attempts are a frequent source of security alerts in enterprise environments due to brute-force attempts, misconfigurations, or insider misuse.

For this project, I collected a sample SSH log file from GitHub and ingested it into Splunk, running inside a Kali Linux virtual machine on VMware Workstation, hosted on Windows. After parsing the logs, I created a SOC-style dashboard that highlights failed login attempts, user activity patterns, and top source IPs.

Key outcomes include:

- A functional Splunk dashboard for SSH event monitoring.
- Identification of failed login trends, top users, and source IPs.
- Demonstration of how SOC analysts can use log analysis to investigate suspicious login activity.

This project showcases my ability to set up a SOC-style monitoring solution, even with static log files, and lays the foundation for extending into real-time log collection in future work.

Data Source, Ingestion & Assumptions

Log Source

- **File:** https: //www.secrepo.com/maccdc2012/ssh.log.gz
- **Events:** Login attempts (success/failure), user accounts, source IPs, timestamps

Ingestion Process

- **Method:** Add Data → Upload → Select Source → Set Source Type → Input Settings → Review
- **Index:** main
- **Sourcetype:** ssh

Field Extraction

- src_ip → Source IP address
- src_port → Source Port
- dest_ip → Destination IP
- dest_port → Destination Port
- action → Authentication Status (Success or Failure or Undetermined)
- timestamp → Event time
- data_direction → Dataflow Direction

Assumptions

- Sample logs ingested manually for this project.
- Failed Attempts > 20 times from one IP Address within 5 minutes = brute-force attack.

Dashboard Overview

The dashboard includes the following visualizations:

- Total Authentication Attempts
- Login Attempts: Success vs Failed
- Top Source IPs Generating Login Attempts
- Detected Brute-Force Attacks
- Total Successful Login Attempts by IPs
- Total Failed Login Attempts by IPs

Dashboard Panels & SPL Documentation

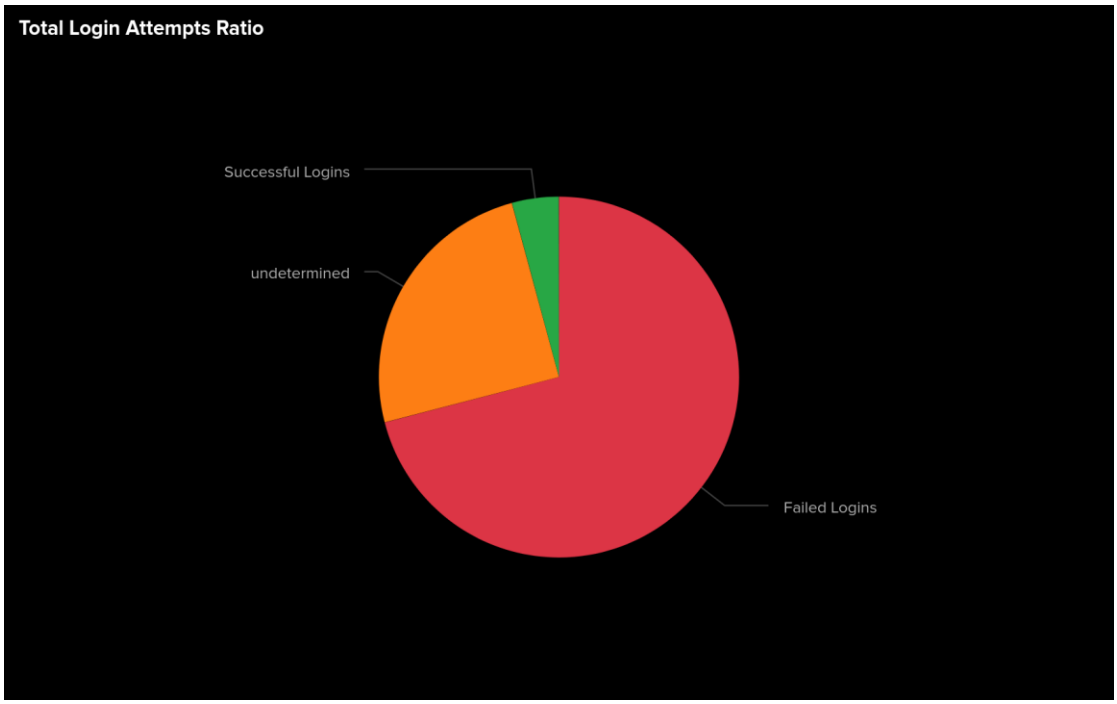
Panel 1: Total Login Attempts

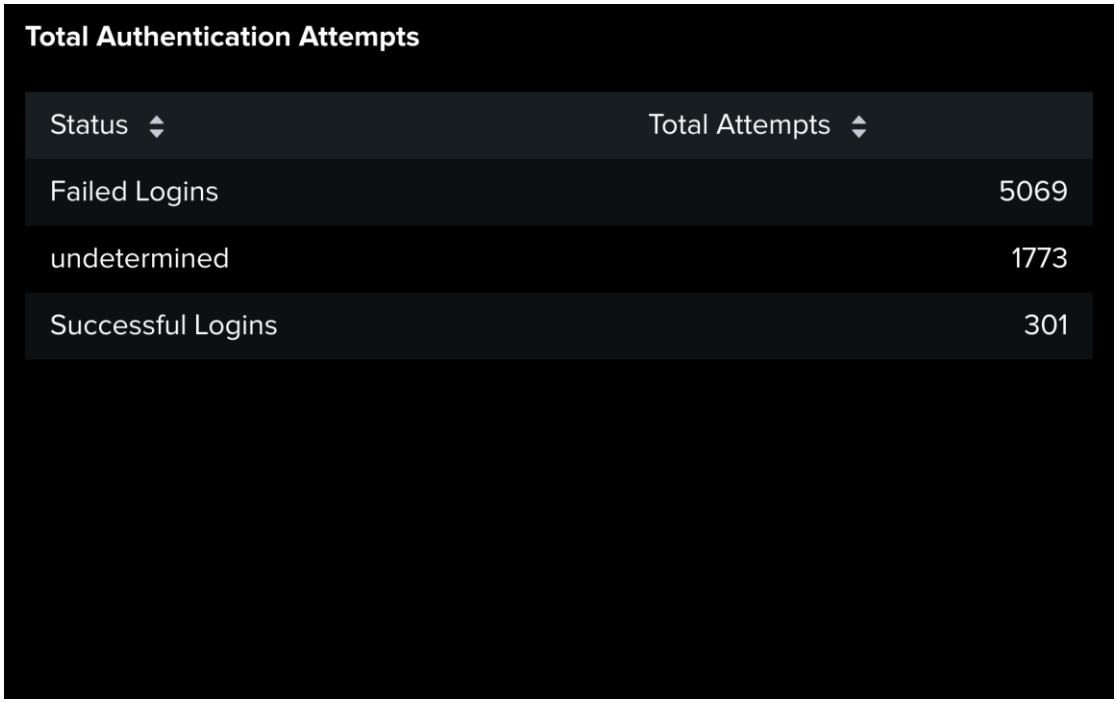
Shows the count and ratio of all type of authentication attempts such as Success, Failure and Undetermined.

SPL:

```
index=main sourcetype=ssh
| eval Status =
case(auth_status="success","Successful Logins",

auth_status="failure","Failed Logins",
                    1=1,auth_status)
| stats count AS "Total Attempts" by Status
| sort -"Total Attempts"
```



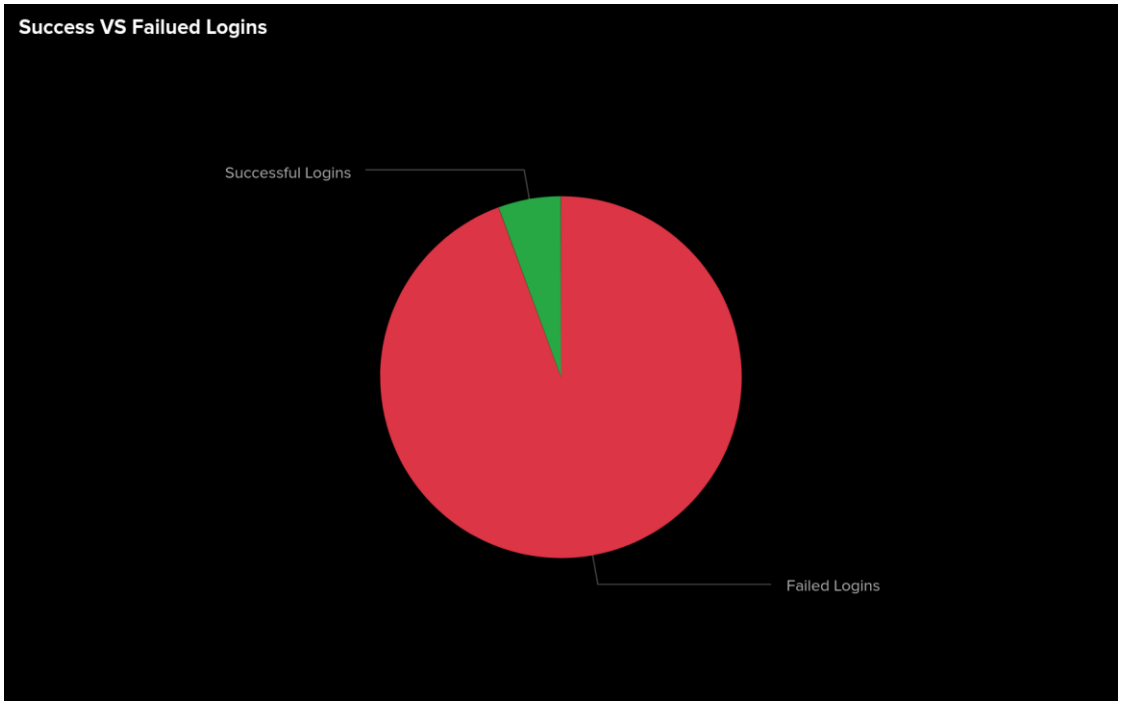


Panel 2: Success vs Failed Logins

Displays ratio of successful vs failed logins. A high failed ratio indicates possible brute-force attempts.

SPL:

```
index=main sourcetype=ssh (success OR failure)
| eval Status = case(auth_status="success","Successful Logins",
                     auth_status="failure","Failed Logins",
                     1=1,auth_status)
| stats count AS "Total Logins" by Status
| sort -"Total Logins"
```



Login Attempts: Success VS Failed

Status	Total Logins
Failed Logins	5069
Successful Logins	301

Panel 3: Top Sources Generating Login Attempts

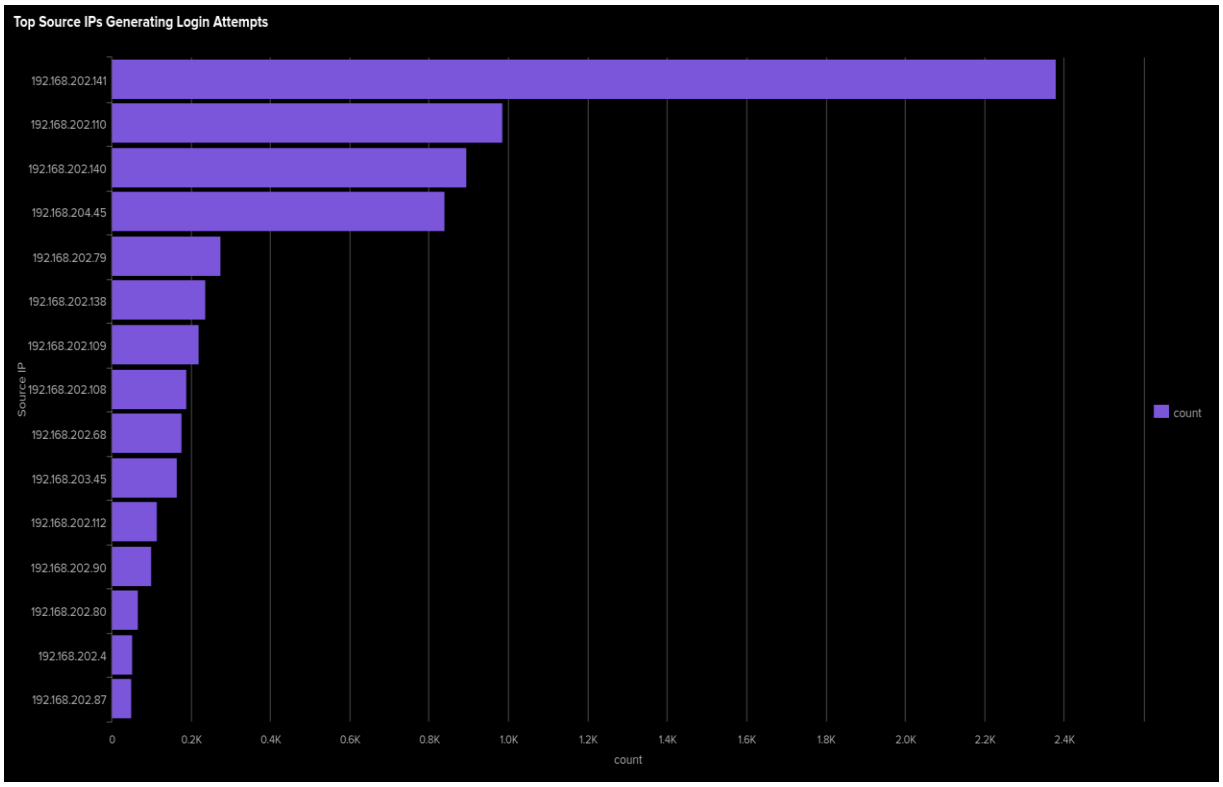
Identifies 15 IPs with the most login attempts (regardless of outcome). Useful for spotting high-volume sources.

SPL:

```
index=main sourcetype=ssh
 | rename src_ip AS "Source IP"
 | stats count  by "Source IP"
 | sort -count
 | head 15
```

Top Source IPs by Number of Login Attempts

Source IP	count
192.168.202.141	2380
192.168.202.110	986
192.168.202.140	894
192.168.204.45	839
192.168.202.79	274
192.168.202.138	237
192.168.202.109	220
192.168.202.108	189
192.168.202.68	176
192.168.203.45	166
192.168.202.112	116
192.168.202.90	101
192.168.202.80	66
192.168.202.4	52
192.168.202.87	51

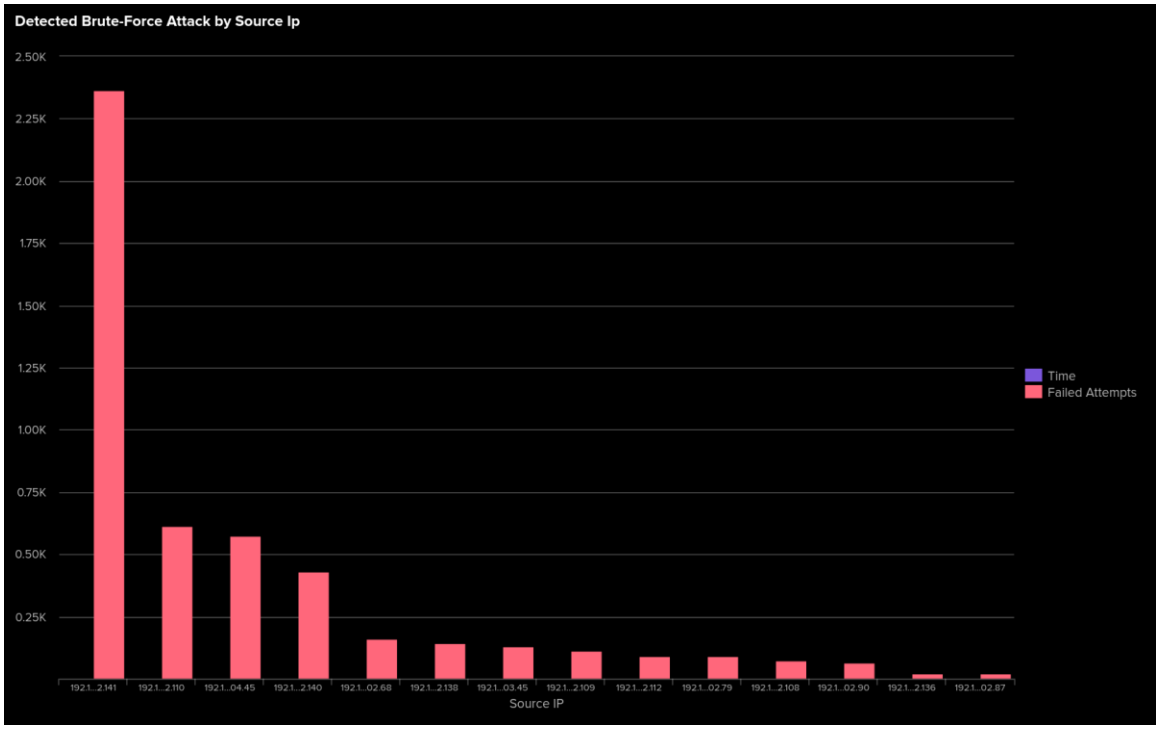


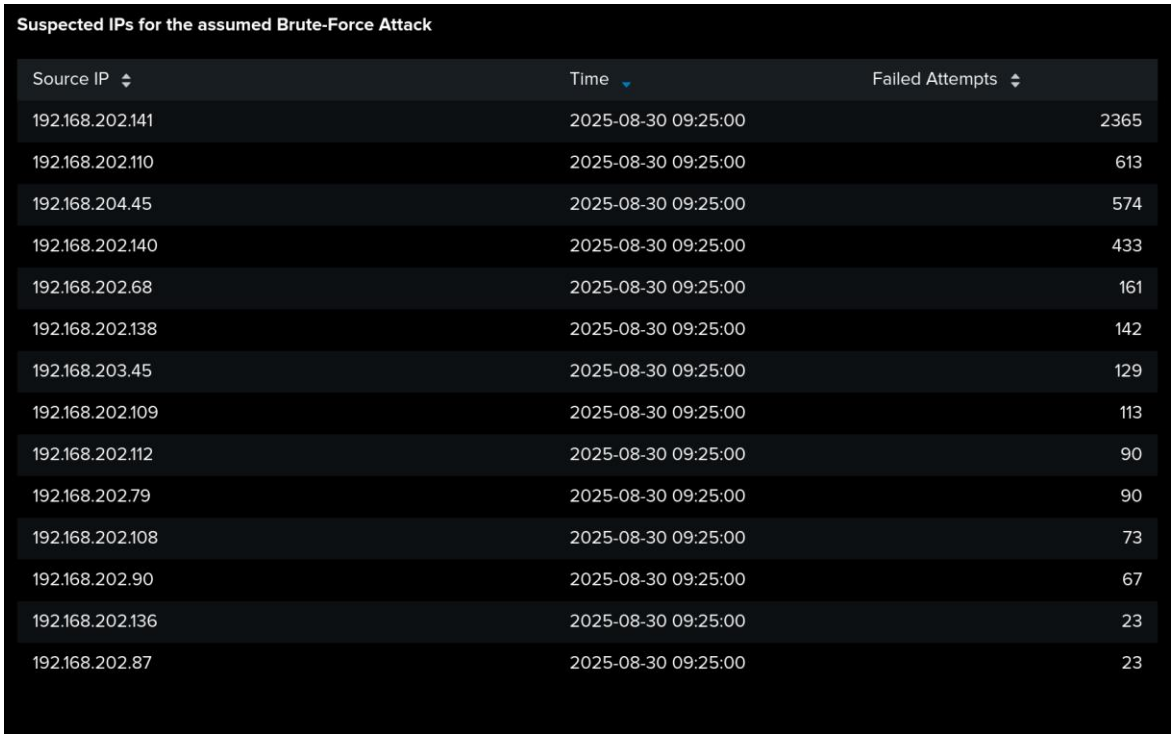
Panel 4: Detecting Brute-Force Attempt by Monitoring Login Attempts by Source IPs

Flags IPs exceeding the brute-force threshold (>20 failures) within 5 minutes. These should be escalated.

SPL:

```
index=main sourcetype=ssh auth_status=failure
| bin _time span=5m
| stats count AS "Failed Attempts" by src_ip, _time
| where 'Failed Attempts' > 20
| rename src_ip AS "Source IP"
| eval Time=strftime(_time, "%Y-%m-%d %H:%M:%S")
| table "Source IP", Time, "Failed Attempts"
| sort -"Failed Attempts"
```





Suspected IPs for the assumed Brute-Force Attack

Source IP	Time	Failed Attempts
192.168.202.141	2025-08-30 09:25:00	2365
192.168.202.110	2025-08-30 09:25:00	613
192.168.204.45	2025-08-30 09:25:00	574
192.168.202.140	2025-08-30 09:25:00	433
192.168.202.68	2025-08-30 09:25:00	161
192.168.202.138	2025-08-30 09:25:00	142
192.168.203.45	2025-08-30 09:25:00	129
192.168.202.109	2025-08-30 09:25:00	113
192.168.202.112	2025-08-30 09:25:00	90
192.168.202.79	2025-08-30 09:25:00	90
192.168.202.108	2025-08-30 09:25:00	73
192.168.202.90	2025-08-30 09:25:00	67
192.168.202.136	2025-08-30 09:25:00	23
192.168.202.87	2025-08-30 09:25:00	23

Panel 5: Successful and Failed Logins by Source IP

Shows frequent 15 IPs for successful and failed logged ins. Helps identify if brute-force attempts resulted in compromise.

SPL:

For Successful Logins

```
index=main sourcetype=ssh auth_status=success
| rename src_ip AS "Source IP"
| stats count by "Source IP"
| sort -count
| head 15
```

Total Successful Login Attempts by IPs

Source IP	count
192.168.202.109	88
192.168.202.80	40
192.168.202.90	30
192.168.202.95	25
192.168.202.112	22
192.168.203.45	18
192.168.202.103	12
192.168.202.87	10
192.168.202.138	7
192.168.202.110	6
192.168.202.68	6
192.168.202.76	6
192.168.202.98	5
192.168.202.108	4
192.168.202.88	4

For Failed Logins

```
index=main sourcetype=ssh auth_status=failure
| rename src_ip AS "Source IP"
| stats count by "Source IP"
| sort -count
| head 15
```

Total Failed Login Attempts by IPs

Source IP	count
192.168.202.141	2365
192.168.202.110	613
192.168.204.45	574
192.168.202.140	433
192.168.202.68	161
192.168.202.138	142
192.168.203.45	129
192.168.202.109	113
192.168.202.112	90
192.168.202.79	90
192.168.202.108	73
192.168.202.90	67
192.168.202.136	23
192.168.202.87	23
192.168.202.80	17

Final Dashboard

SSH Brute-Force Detection and Authentication Monitoring

This dashboard provides real-time visibility into SSH login attempts, helping SOC teams detect brute-force attacks, analyze authentication trends, and identify malicious IPs. It enables proactive defense by correlating failed logins, source IP reputation, and brute-force attack patterns.

Global Time Ran...

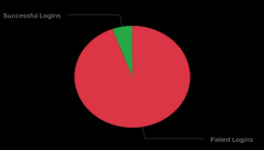
Last 24 hours

Total Authentication Attempts

Stat...	Total
Failed Logins	5069
undetermined	1773
Successful Logins	301

Total Login Attempts Ratio

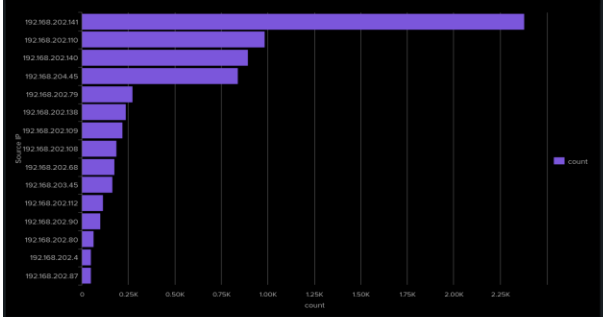
Success VS Failued Logins



Login Attempts: Success VS Failed

Stat...	Total
Failed Logins	5069
Successful Logins	301

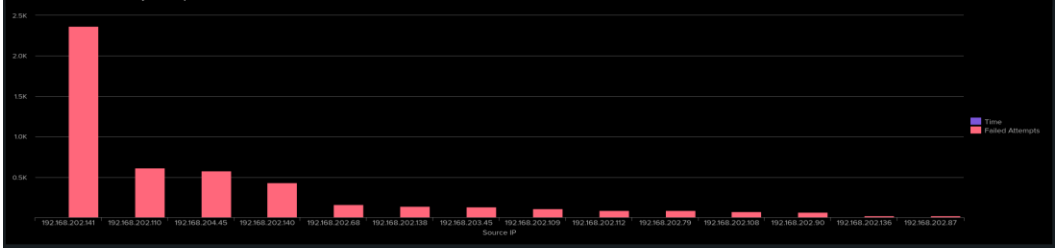
Top Source IPs Generating Login Attempts



Top Source IPs by Number of Login Attempts

Source IP	count
192.168.202.141	2380
192.168.202.110	986
192.168.202.140	894
192.168.204.45	839
192.168.202.79	274
192.168.202.138	237
192.168.202.109	220
192.168.202.108	189
192.168.202.68	176
192.168.203.45	166
192.168.202.112	116
192.168.202.90	101
192.168.202.80	66
192.168.202.4	52
192.168.202.87	51

Detected Brute-Force Attack by Source Ip



Suspected IPs for the assumed Brute-Force Attack

Source IP	Time	Failed
192.168.202.141	2025-08-30 09:25:00	2365
192.168.202.110	2025-08-30 09:25:00	613
192.168.204.45	2025-08-30 09:25:00	574
192.168.202.140	2025-08-30 09:25:00	433
192.168.202.68	2025-08-30 09:25:00	161
192.168.202.138	2025-08-30 09:25:00	142
192.168.203.45	2025-08-30 09:25:00	129
192.168.202.109	2025-08-30 09:25:00	113
192.168.202.112	2025-08-30 09:25:00	90
192.168.202.79	2025-08-30 09:25:00	90
192.168.202.108	2025-08-30 09:25:00	73
192.168.202.90	2025-08-30 09:25:00	67
192.168.202.136	2025-08-30 09:25:00	23
192.168.202.87	2025-08-30 09:25:00	23

Total Failed Login Attempts by IPs

Source IP	count
192.168.202.141	2365
192.168.202.110	613
192.168.204.45	574
192.168.202.140	433
192.168.202.68	161
192.168.202.138	142
192.168.203.45	129
192.168.202.109	113
192.168.202.112	90
192.168.202.79	90
192.168.202.108	73
192.168.202.90	67
192.168.202.136	23
192.168.202.87	23
192.168.202.80	17

Total Successful Login Attempts by IPs

Source IP	count
192.168.202.109	88
192.168.202.80	40
192.168.202.90	30
192.168.202.95	25
192.168.202.112	22
192.168.203.45	18
192.168.202.103	12
192.168.202.87	10
192.168.202.138	7
192.168.202.110	6
192.168.202.68	6
192.168.202.76	6
192.168.202.98	5
192.168.202.108	4
192.168.202.88	4

SOC Use Cases & Incident Response

- **Detection:** Monitor high failed login ratios & threshold breaches.
- **Response:** Block malicious IPs via firewall / IDS.
- **Investigation:** Correlate targeted usernames and IP reputation.
- **Forensics:** Check if suspicious IPs had successful logins → possible compromise.
- **Prevention:** Apply MFA, disable root login, configure fail2ban.

Future Improvements

- Add **Geo-IP visualization** (map attackers by country).
- Integrate with **Threat Intelligence Feeds** (check IP reputation).
- Build **SOAR automation** for blocking suspicious IPs.
- Create **Splunk Alerts** for brute-force thresholds.

Conclusion

This project demonstrates practical SOC dashboarding for SSH brute-force detection using Splunk. It highlights both technical skill (SPL, dashboards, ingestion) and security analysis skill (attack detection, response).