🔐 SIEM LOG ANALYSIS PROJECT REPORT

Name: Sai Kiran G
Tools Used: Python, Regex, Linux auth.log, Manual Log Parsing
Duration: August 2024
Dataset: Realistic Linux system logs from SSH authentication

🧭 Objective

To identify and analyze brute-force login attempts from Linux authentication logs. The project emulates a real-world SOC analyst's task in detecting threats using SIEM principles.

📁 Sample Log Entry

Jun 15 02:04:59 combo sshd(pam_unix)[20886]: authentication failure; logname= uid=0 euid=0 tty=NODEVssh ruser= rhost=220-135-151-1.hinet-ip.hinet.net user=root

🔍 Log Analysis Logic

- Parsed log lines for `authentication failure`.
- Extracted source IPs using regex.
- Counted failed attempts by each IP.
- Flagged IPs with more than 5 failures as **suspected brute-force attacks**.

🚨 Brute Force Detection Result

31 IP addresses were flagged for attempting more than **5 unauthorized SSH logins**, with the highest reaching **80 failures** from a single source.

	IP Address	Failed Attempts
0	150.183.249.110	80
1	n219076184117.netvigator.com	23
2	207.243.167.114	23
3	60.30.224.116	20
4	195.129.24.210	15
5	218.188.2.4	14
6	h64-187-1-131.gtconnect.net	13
7	220.117.241.87	13
8	220-135-151-1.hinet-ip.hinet.net	10
9	061092085098.ctinets.com	10
10	adsl-70-242-75-179.dsl.ksc2mo.swbell.net	10
11	65.166.159.14	10
12	ip-216-69-169-168.ip.secureserver.net	10
13	209.152.168.249	10
14	massive.merukuru.org	10
15	62-192-102-94.dsl.easynet.nl	10
16	csnsu.nsuok.edu	10
17	zummit.com	10
18	p15105218.pureserver.info	10
19	211.214.161.141	10
20	82.77.200.128	10
21	211.137.205.253	10
22	68.143.156.89.nw.nuvox.net	10
23	c51471f2c.cable.wanadoo.nl	10
24	211-76-104-65.ebix.net.tw	10
25	202.181.236.180	10
26	211.9.58.217	10
27	218.22.3.51	9
28	61.53.154.93	9
29	biblioteka.wsi.edu.pl	8
30	202-132-40-29.adsl.ttn.net	8
31	210.76.59.29	7
32	217.60.212.66	6

🛠️ Recommendations

- Configure `fail2ban` to block IPs with repeated failures.
- Disable root login over SSH (`PermitRootLogin no` in sshd_config).
- Use key-based authentication instead of passwords.
- Monitor logs continuously using tools like Splunk, ELK, or Graylog.