**──────────────────────────────────────────────**

**🧠 Brute Force Attack Detection & Mitigation using Splunk & Wireshark**

**──────────────────────────────────────────────**

**📌 Overview:**

**This project demonstrates how to detect, analyze, and mitigate brute-force attack attempts using Splunk for log analysis and Wireshark for network packet inspection.**

**The purpose is to showcase a real-world SOC (Security Operations Center) incident response workflow.**

**──────────────────────────────────────────────**

**🎯 Objective:**

**Identify brute-force login attempts on a Windows host, investigate their source, and implement preventive measures to stop further attacks.**

**──────────────────────────────────────────────**

**🧰 Tools Used:**

**- Splunk Enterprise – Log analysis and correlation**

**- Wireshark – Network packet capture and inspection**

**- Nmap – Port and service scanning**

**- Windows Event Viewer – Authentication logs (Event ID 4625)**

**──────────────────────────────────────────────**

**🧩 Methodology:**

**1. Collect Logs in Splunk**

**• Configured Splunk to ingest Windows Security Event Logs.**

**• Focused on Event ID 4625 (Failed Logon Attempts).**

**2. Run Query to Identify Brute Force Activity**

**SPL Query:**

**index="soc\_lab" EventCode=4625**

**| stats count by Account\_Name, IPAddress**

**| where count > 5**

**| sort -count**

**3. Analyze Logs**

**• Identified multiple failed login attempts from the same IP.**

**• Observed suspicious login patterns within short time intervals.**

**4. Verify with Wireshark**

**• Captured packets for suspicious source IP.**

**• Observed repeated TCP connection attempts to port 3389 (RDP).**

**5. Validate via Nmap**

**• Performed service scan on attacker IP:**

**nmap -sV <attacker\_ip>**

**• Confirmed open ports and possible attack vector.**

**6. Mitigation Steps**

**• Blocked IP using Windows Firewall.**

**• Enforced Account Lockout Policy.**

**• Implemented MFA (Multi-Factor Authentication).**

**• Created detection rule for repeated 4625 events.**

**──────────────────────────────────────────────**

**📊 Findings:**

**- Repeated failed logon attempts from a single IP confirmed Brute Force Attack.**

**- Attack targeted Administrator account via RDP service.**

**- Quick mitigation prevented further unauthorized access.**

**──────────────────────────────────────────────**

**🔐 Outcome:**

**✅ Detected and mitigated brute-force attempt successfully.**

**✅ Enhanced security monitoring through custom Splunk alerts.**

**✅ Strengthened authentication and firewall policies.**

**──────────────────────────────────────────────**

**📎 Folder Structure:**

**Brute-Force-Attack-Case-Study/**

**│**

**├── README.md**

**├── Brute Force Attack Detection.docx**

**──────────────────────────────────────────────**

**👨‍💻 Author:**

**Sahil Rajesh Koli**

**🛡️ Cybersecurity Analyst | CEH (v13) | CompTIA Security+ | CISSP Trained**

**LinkedIn: https://www.linkedin.com/in/sahil-koli-8ba0792b8/**

**GitHub: https://github.com/jokersk551**

**──────────────────────────────────────────────**

**⚡ Fun Fact:**

**Every failed logon attempt has a story — find it before the attacker does.**

**──────────────────────────────────────────────**