Project: Incident Detection & Response with Splunk

Objective:

Detect brute-force login attempts using Splunk, respond with containment actions, and document the incident for future readiness.

Environment & Tools Used

- **Splunk Enterprise / Splunk Free** (SIEM platform)
- **Ubuntu Linux VM** (attacker simulation)
- **Windows Server VM** (target system)
- **Python** (for automation of log parsing & alert handling)

Step 1: Data Ingestion

- Configured Splunk to collect logs from Windows Event Viewer and Linux syslog.
- Normalized log data into a common schema for easier correlation.

Step 2: Detection Rule

- Created a Splunk search query to detect multiple failed login attempts within 5 minutes:

```
index=auth_logs sourcetype=linux_secure OR sourcetype=WinEventLog:Security
"failed password" OR "Login failed"
| stats count by user, src_ip
| where count > 5
```

- **Alert Configuration:** Set Splunk to trigger an alert when count > 5.

Step 3: Incident Response Simulation

1. **Detection:** Alert triggered for multiple failed login attempts from a suspicious IP.
2. **Analysis:** Verified IP address and user account activity in Splunk dashboard.
3. **Containment:** Blocked malicious IP on the firewall (simulated with iptables).
4. sudo iptables -A INPUT -s <malicious_IP> -j DROP
5. **Eradication:** Reset the compromised user password and disable the account temporarily.
6. **Recovery:** Monitored logs for further suspicious activity.

Step 4: Documentation (Incident Report)

Incident Title: Brute-Force Login Attempt Detected
Date& Time: 12 July 2024, 15:43 UTC
Detected By: Splunk SIEM (custom brute-force detection query)
Incident ID: INC-2024-07-001

Summary:
Splunk detected >10 failed login attempts from 192.168.10.45 targeting user admin. Alert escalated to CSIRT.

Impact:

- Targeted system: Windows Server 2019 (Domain Controller)
- No successful login observed
- Risk: Credential stuffing/brute-force attack

Actions Taken:

- Contained attack by blocking source IP.
- Reset targeted account password and enforced MFA.
- Conducted log review for lateral movement – none detected.

Lessons Learned:

- Added automated Splunk alert for excessive failed logins.
- Updated incident response playbook with brute-force containment steps.
- Recommended security awareness training for stronger password policies.

Outcome:

- Improved detection of brute-force attempts.
- Reduced MTTR (Mean Time to Respond) by using Splunk alerts and structured playbooks.
- Strengthened organizational readiness through documentation and simulation.