CYBERSECURITY PORTFOLIO – LAB ENVIRONMENT

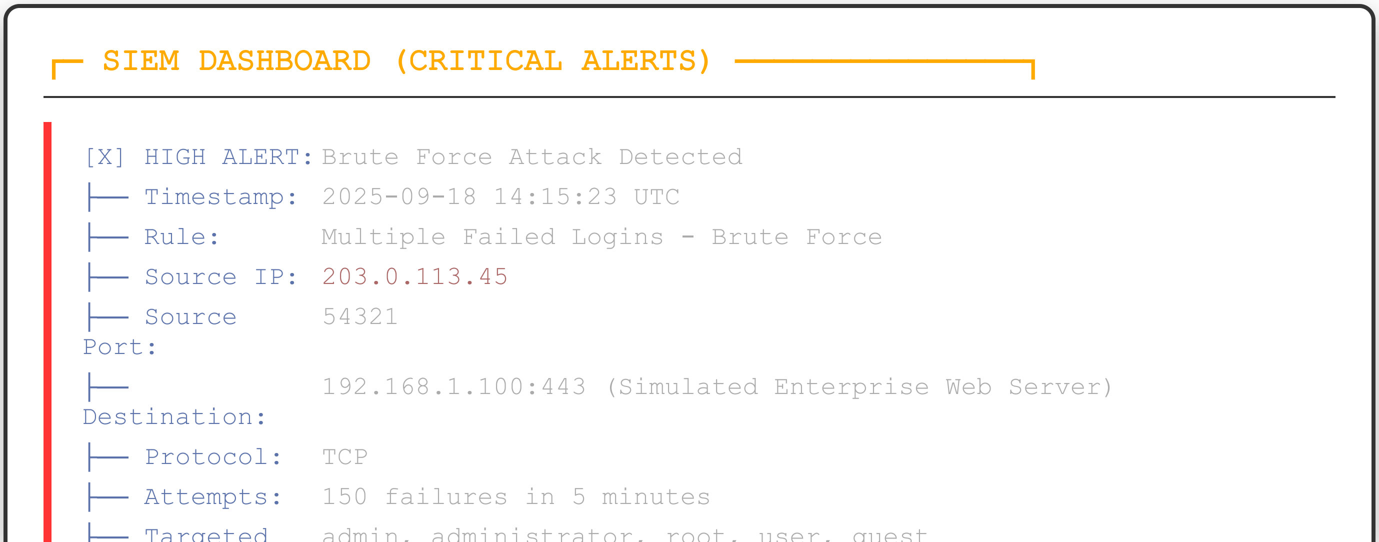
SECURITY INCIDENT REPORT

Report Reference:	IR-2025-09-18-001 (Lab Simulation)
Incident Date:	18 September 2025
Incident Time:	14:15 UTC
Report Date:	18 September 2025
Prepared by:	**Chieb Mohamed Anouar** (SOC Analyst)
Environment:	LAB ENVIRONMENT - SIMULATED

1. EXECUTIVE SUMMARY

On **18 September 2025** at **14:15 UTC**, the Security Information and Event Management (SIEM) system generated a HIGH severity alert regarding a simulated brute-force attack attempt against a lab enterprise web server. The attack, originating from IP address **203.0.113.45**, was automatically blocked by the firewall. This simulation demonstrates detection and response capabilities in a controlled lab environment. No real production assets were affected.

2. SIEM TOOL SCREENSHOT



```
┌ SIEM DASHBOARD (CRITICAL ALERTS) ──────────────┐

[X] HIGH ALERT: Brute Force Attack Detected
├── Timestamp:  2025-09-18 14:15:23 UTC
├── Rule:       Multiple Failed Logins - Brute Force
├── Source IP:  203.0.113.45
├── Source      54321
Port:
├──             192.168.1.100:443 (Simulated Enterprise Web Server)
Destination:
├── Protocol:   TCP
├── Attempts:   150 failures in 5 minutes
├── Targeted    admin, administrator, root, user, guest
```

```
│  Targeted    admin, administrator, root, user, guest
   Accounts:
└── Status:     ✅ Blocked (Firewall at 14:20 UTC)

[ ] INFO:      Port Scan Detected from 10.0.0.25 (Lab Network)
[ ] LOW:       Failed Login - Simulated User jdoe
```

3. EVENT TIMELINE

14:10:00	Start of failed login attempt sequence (simulated attack)	*Web Server Logs*
14:15:23	SIEM alert triggered (threshold of 150 failures reached)	*SIEM*
14:18:00	Alert acknowledged and verified by **Chieb Mohamed Anouar**	*SOC Analyst*
14:20:00	Block rule implemented on firewall for IP 203.0.113.45	*Network Team (Simulated)*
14:22:00	Web server logs isolated for forensic analysis	*SOC Analyst*
14:30:00	Incident documentation completed for portfolio	***Chieb Mohamed Anouar***

4. AFFECTED ASSETS (LAB ENVIRONMENT)

Asset	Role	IP Address	Environment
WEB-SRV-LAB-01	Simulated Enterprise Web Server	192.168.1.100	Isolated Lab Network

⚠️ *All assets are part of a controlled cybersecurity lab environment. No production systems were involved.*

5. INDICATORS OF COMPROMISE (IOCs)

Malicious IP Address

`203.0.113.45`

Source Network

`External Untrusted Network`

Attack Time Window

`14:10 - 14:15 UTC`

Targeted Usernames

`Common default administrative usernames targeted`

MITRE ATT&CK MAPPING

Tactic	Technique	Sub-technique

`Credential Access`
`TA0006`
	`Brute Force T1110`	`Password Guessing`
		`T1110.001`

8. RISK ASSESSMENT

Severity	Impact	Likelihood
HIGH	Medium	High

OVERALL RISK LEVEL: HIGH

6. ACTIONS TAKEN

1. **Immediate Containment:** IP address **203.0.113.45** was added to the firewall blocklist within 5 minutes of alert verification.
2. **Forensic Analysis:** Web server logs were secured and analyzed to confirm no successful authentication before blocking.
3. **Enhanced Monitoring:** Implemented additional logging and alerting rules for similar brute-force patterns.
4. **Incident Documentation:** Complete timeline and technical details documented for portfolio and learning purposes.

7. RECOMMENDATIONS

1. **Implement account lockout** after 5 failed attempts within 10 minutes to prevent brute-force attacks.
2. **Enable Multi-Factor Authentication (MFA)** for all privileged accounts and remote access.
3. **Deploy Web Application Firewall (WAF)** to filter and block malicious traffic patterns.
4. **Enable geo-blocking** for high-risk regions to reduce attack surface.
5. **Implement centralized log retention policy** (90+ days) for compliance and forensic analysis.
6. **Conduct regular brute-force simulation exercises** to test detection and response capabilities.

Cybersecurity Portfolio - Incident Report IR-2025-09-18-001 | Document generated on 18 September 2025
This document is part of a simulated lab environment for educational and portfolio purposes only.