GBM

CONFIDENTIAL

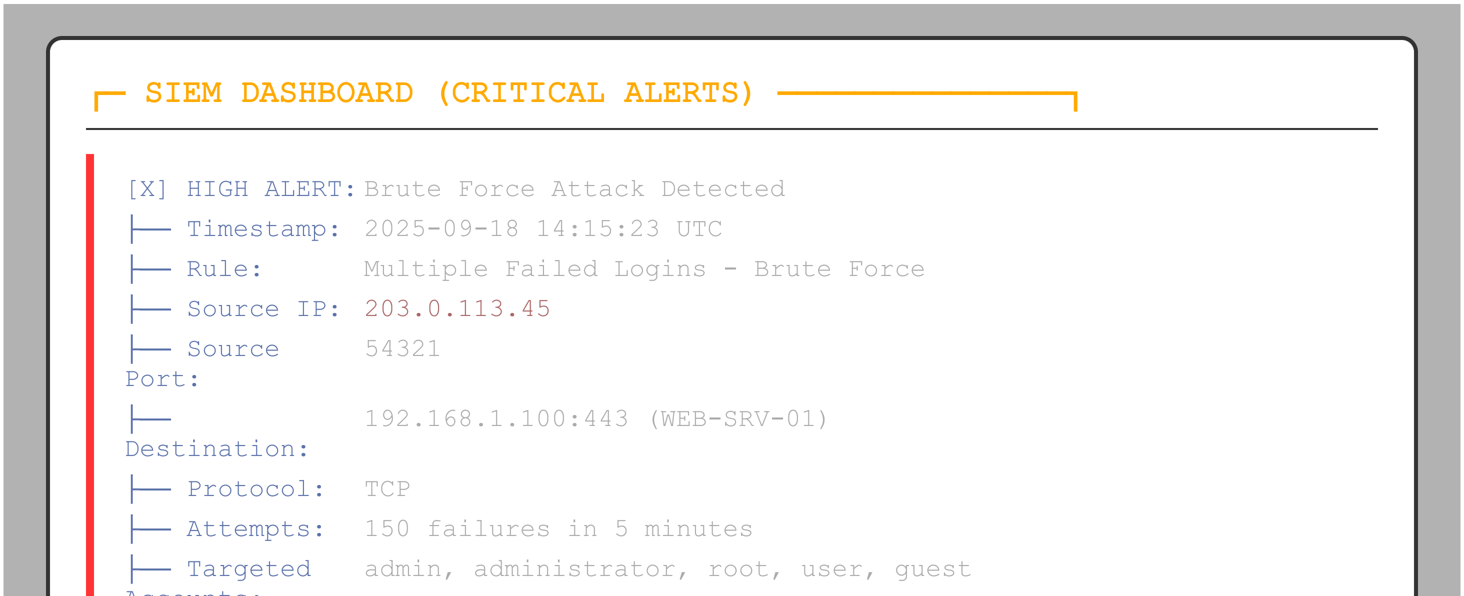
SECURITY INCIDENT REPORT

Report Reference:	IR-2025-09-18-001
Incident Date:	18 September 2025
Incident Time:	14:15 UTC
Report Date:	18 September 2025
Prepared by:	**Chieb Mohamed Anouar** (SOC Analyst)
Classification Level:	CONFIDENTIAL

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 brute-force attack attempt against the company's primary web server. The attack, originating from IP address **203.0.113.45**, was automatically blocked by the firewall. No data compromise has been detected at this stage.

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 (WEB-SRV-01)
Destination:
├── Protocol:   TCP
├── Attempts:   150 failures in 5 minutes
├── Targeted    admin, administrator, root, user, guest
Accounts:
  Accounts:
   └── Status:        Blocked (Firewall at 14:20 UTC)

[ ] INFO:       Port Scan Detected from 10.0.0.25
[ ] LOW:        Failed Login - User jdoe
```

3. EVENT TIMELINE

14:10:00	Start of failed login attempt sequence	*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*
14:22:00	Web server logs isolated for forensic analysis	*SOC Analyst*
14:30:00	Escalated to Incident Response Team (IRT)	***Chieb Mohamed Anouar***

4. AFFECTED ASSETS

Asset	Role	IP Address	Operating System
WEB-SRV-01	Primary Web Server (IIS)	192.168.1.100	Windows Server 2022

5. INDICATORS OF COMPROMISE (IOCs)

Malicious IP Address	Country of Origin	Attack Time Window
`203.0.113.45`	`Imaginary Country`	`14:10 - 14:15 UTC`

Tested Usernames

`admin, administrator, root, user, guest`

6. ACTIONS TAKEN

1. **Blocking:** IP address **203.0.113.45** was added to the firewall blocklist.
2. **Analysis:** Web server logs have been secured and are being analyzed to verify no successful logins occurred before the block.

3. **Monitoring:** Enhanced monitoring has been activated on server **192.168.1.100** to detect any subsequent anomalous activity.
4. **Notification:** Relevant teams (Network, Security, System Administration) have been notified.

7. RECOMMENDATIONS

1. **Passwords:** Enforce changing default passwords on all administrative accounts.
2. **Lockout Policy:** Implement an account lockout policy after 5 failed attempts.
3. **MFA:** Enable Multi-Factor Authentication (MFA) for all remote and administrative access.
4. **WAF:** Consider deploying a Web Application Firewall (WAF) to filter malicious traffic.
5. **Threat Intelligence:** Add IP **203.0.113.45** to the Threat Intelligence database.

APPROVALS:

SOC Analyst	Security Manager	Date
Chieb Mohamed Anouar	Chikh Hamed Allah Hamid	18/09/2025

GBM - Incident Report IR-2025-09-18-001 | Document generated on 18 September 2025