Incident Report: Unauthorized Login Attempt

Date: October 18, 2025
Prepared by: Mubaraka Mohammed
Environment: Cybersecurity Home Lab (Windows Server, Linux, SIEM: Splunk)

Incident Summary

A suspicious login attempt was detected from an unknown IP address (185.XX.XX.210) targeting the Windows Active Directory Server. SIEM logs flagged multiple failed authentication attempts within a 2-minute window.

Timeline

- **02:10 AM:** Splunk triggered "Multiple Failed Logins" alert.
- **02:12 AM:** Analyst initiated investigation and extracted event logs.
- **02:20 AM:** Confirmed repeated attempts from a foreign IP block.
- **02:25 AM:** Account temporarily locked and IP address blocked via firewall rule.
- **02:45 AM:** Review confirmed no data exfiltration or privilege escalation occurred.

Root Cause

Weak password policy allowed brute-force attempts to occur undetected initially.

Mitigation

- Implemented password complexity and lockout policy.
- Updated firewall rules to block unauthorized IP ranges.
- Configured Splunk correlation rule for faster response.

Lessons Learned

- Enhancing proactive monitoring and threshold tuning significantly reduces potential exposure to brute-force attacks.