CYBERSECURITY INCIDENT REPORT

Team Name: CyberGuard
Competition: SkillsUSA Cybersecurity Demonstration
Incident ID: CG-2026-0618-01
Date/Time Detected: June 18, 2026 09:18 PM
Date/Time Reported: June 18, 2026 10:30 PM

1. Executive Summary

Security monitoring systems detected suspicious authentication activity originating from an external source. Analysis identified multiple failed login attempts followed by a successful authentication event and attempted lateral movement.

2. Incident Details

Incident Type: Unauthorized Access Attempt / Brute Force Activity
Affected Systems: WIN10-CLIENT5, SRV-APP01
Source IP: 203.0.113.77

3. Timeline of Events

09:18 PM - Port scan detected
09:21 PM - SSH brute force activity observed
09:23 PM - Successful login detected
09:25 PM - Lateral movement attempt observed
09:27 PM - Firewall containment rule applied

4. Evidence Collected

• pfSense Firewall Logs
• Windows Security Event Logs
• Wireshark Packet Capture
• Nmap Scan Results
• Network Topology Diagram
• SIEM Dashboard Screenshots

5. Analysis

Evidence suggests credential compromise through repeated authentication attempts. Network monitoring identified reconnaissance activity followed by targeted access attempts.

6. Containment Actions

• Blocked source IP at perimeter firewall
• Disabled affected credentials
• Increased monitoring thresholds
• Verified system integrity

7. Remediation Plan

• Enforce MFA
• Review privileged accounts
• Patch affected systems
• Conduct user awareness training

8. Conclusion

The incident was contained successfully. No evidence of data exfiltration was identified during the investigation period.