# Brute Force Incident Response Playbook

Prepared by: Jamie Christian — Cybersecurity Analyst

## Detection

|  |  |  |
| --- | --- | --- |
| Task | Owner | Tools |
| Monitor SIEM for high-volume failed logins | SOC Analyst | Splunk/Wireshark/Nmap |
| Look for unusual geo IP login attempts | SOC Analyst | Splunk/Wireshark/Nmap |
| Identify spikes in AuthFailure events within 10 minutes | SOC Analyst | Splunk/Wireshark/Nmap |

## Immediate Actions

|  |  |  |
| --- | --- | --- |
| Task | Owner | Tools |
| Isolate affected host from network | SOC Analyst | Splunk/Wireshark/Nmap |
| Disable compromised account | SOC Analyst | Splunk/Wireshark/Nmap |
| Block malicious IPs at firewall | SOC Analyst | Splunk/Wireshark/Nmap |
| Collect forensic evidence for investigation | SOC Analyst | Splunk/Wireshark/Nmap |

## Containment & Recovery

|  |  |  |
| --- | --- | --- |
| Task | Owner | Tools |
| Reset credentials and enforce MFA | SOC Analyst | Splunk/Wireshark/Nmap |
| Patch RDP configuration | SOC Analyst | Splunk/Wireshark/Nmap |
| Scan for lateral movement | SOC Analyst | Splunk/Wireshark/Nmap |
| Restore systems from clean backup if necessary | SOC Analyst | Splunk/Wireshark/Nmap |

## Escalation & Communication

|  |  |  |
| --- | --- | --- |
| Task | Owner | Tools |
| Notify SOC lead | SOC Analyst | Splunk/Wireshark/Nmap |
| Inform CISO and Compliance officer | SOC Analyst | Splunk/Wireshark/Nmap |
| Prepare HIPAA incident documentation | SOC Analyst | Splunk/Wireshark/Nmap |