

Capstone Report – Full Alert to Response Cycle

Attack Simulation

A simulated attack was conducted against a vulnerable Metasploitable2 virtual machine using a known VSFTPD backdoor vulnerability. The exploit allowed unauthorized access to the target system, demonstrating a remote code execution scenario.

Timestamp	Source IP	Alert Description	MITRE Technique
2025-08-18 11:00	192.168.1.100	VSFTPD exploit attempt detected	T1190

The alert was categorized as a high-severity remote exploit attempt. The activity was mapped to MITRE ATT&CK Technique T1190 (Exploit Public-Facing Application).

Response Actions

1. The affected VM was immediately isolated from the network.
2. The attacker's IP address (192.168.1.100) was blocked using firewall controls.
3. Logs were preserved for forensic analysis.
4. System integrity was verified before restoration.

Executive Summary

On 18 August 2025, a simulated exploit attempt targeting a vulnerable VSFTPD service was detected during routine monitoring activities. The attack originated from IP address 192.168.1.100 and attempted remote exploitation of a publicly exposed FTP service.

Detection & Timeline

The intrusion attempt was detected at 11:00 IST via SIEM alerting. The alert was mapped to MITRE ATT&CK technique T1190, indicating an exploit of a public-facing application. Initial triage confirmed the exploit attempt without evidence of persistent compromise.

Containment & Remediation

The affected virtual machine was isolated immediately to prevent lateral movement. The malicious source IP was blocked using firewall controls. System logs and artifacts were preserved for analysis. The vulnerable service was reviewed and patched accordingly.

Recommendations

It is recommended to restrict unnecessary public services, apply regular patch management, and implement intrusion prevention systems to detect similar exploitation attempts in real time.

Stakeholder Briefing

A simulated security incident involving an attempted system exploit was successfully detected and contained. The affected test server was isolated, and the suspicious external IP address was blocked immediately. No data loss or system damage occurred. The issue was resolved quickly due to timely monitoring and response procedures. Preventive measures, including improved patch management and network monitoring, are being reinforced to minimize future risks.