Capstone Incident Report – Week 2

Capstone Incident Report – Week 2

Executive Summary
On 2025-08-18, a simulated cyber-attack was executed against a Metasploitable2 server using the vsftpd 2.3.4 backdoor expl

Timeline
- 2025-08-18 11:00 – Exploit executed via Metasploit against test VM.
- 2025-08-18 11:02 – Wazuh generated critical alert: “VSFTPD Backdoor Exploit.”
- 2025-08-18 11:05 – Analyst validated IOC (Source IP: 192.168.1.100).
- 2025-08-18 11:10 – Attacker IP blocked using CrowdSec.
- 2025-08-18 11:30 – System isolated for further analysis.

Impact Analysis
The attack targeted a vulnerable lab server. No sensitive data was compromised. The incident demonstrated potential risk if si

Remediation Steps
- Blocked malicious IP (192.168.1.100).
- Isolated the vulnerable VM.
- Patched vsftpd on lab systems.
- Reviewed firewall rules for exposed services.

Lessons Learned
1. Continuous monitoring is effective but should include automated IP blocking.
2. Patch management is critical for internet-facing services.
3. Incident workflows must emphasize quick isolation and clear communication.

Recommendations
- Implement routine vulnerability scans.
- Integrate SOAR automation with Wazuh for faster containment.
- Conduct regular red-team simulations to validate defenses.