Capstone Project (Full Alert → Detection → Response → Documentation)

An attacker exploited a vulnerability on a Linux machine and gained access using the VSFTPD backdoor exploit.

Full Incident Report

Section 1 — Executive Summary

- What happened
- How it was detected
- What was impacted
- What actions were taken

Example :

On 18-08-2025, Wazuh generated an alert indicating exploitation of the VSFTPD backdoor vulnerability on Linux server Ubuntu-SRV01.
The attack originated from IP 192.168.1.100 and attempted to create a backdoor shell.
SOC analysts validated the alert and confirmed the activity as malicious using MITRE ATT&CK mapping (T1190 – Exploit Public-Facing Application).
The server was isolated, the malicious process was terminated, and the attacker IP was blocked using firewall rules.
No data exfiltration or lateral movement was detected during the investigation.

Section 2 — Timeline of Events

Date & Time	Action
2025-08-18 11:00	Alert received from Wazuh
2025-08-18 11:10	Server Ubuntu-SRV01 isolated from network
2025-08-18 11:25	Malicious process terminated
2025-08-18 11:40	Attacker IP blocked
2025-08-18 12:10	System restored and monitoring enabled

Section 3 — Technical Analysis

- Exploit used: VSFTPD 2.3.4 Backdoor
- MITRE Technique: T1190 – Exploit Public-Facing Applications
- Source IP: 192.168.1.100
- Affected Host: Ubuntu-SRV01
- Log Entry Indicators: reverse shell creation
- Severity: Critical

Section 4 — Remediation & Recovery

- Isolated affected host
- Terminated malicious process
- Blocked attacker IP in firewall
- Patched VSFTPD vulnerability
- Reset credentials for affected host
- Enabled continuous monitoring

Section 5 — Recommendations

- Apply security patches regularly
- Disable unnecessary services
- Implement intrusion detection alerts for login anomalies
- Enforce access logging and retention
- Conduct periodic vulnerability scans