Capstone Project Report: Full Alert-to-Response Cycle

Executive Summary

A simulated cyberattack was conducted against a vulnerable Metasploitable2 host using the VSFTPD 2.3.4 backdoor exploit. The attack successfully gave root-level shell access to the target. Wazuh agent detected suspicious activity and generated alerts mapped to MITRE technique T1190 (Exploit Public-Facing Application). After detection, a response was executed from the defending Kali system using CrowdSec to isolate the attacker by banning its IP address for one hour. This action prevented further communication attempts, completing the full detect-to-response cycle.

Technical Timeline

Timestamp	Action
06:15	Metasploit exploit executed against 192.168.56.102 (vsftpd_234_backdoor)
06:16	Root shell established
06:25	Wazuh alert generated and logged
06:35	CrowdSec installed and configured
06:40	Manual ban applied on attacker IP 192.168.56.102
06:41	Isolation confirmed via failed ping

Detection Evidence (Wazuh Alert)

Timestamp	Source IP	Description	MITRE
2025-11-21 05:25:50	192.168.56.102	VSFTPD Exploit Detected	T1190

Response Evidence (CrowdSec)

```
sudo cscli decisions add --ip 192.168.56.102 --duration 1h
```

ID	Source	Scope:Value	Reason	Action	Events	Exp	Alert ID
1	cscli	Ip:192.168.56.102	manual 'ban' applied	ban	1	59m	1

Recommendations

- Disable outdated services such as VSFTPD.
- Enforce continuous log monitoring through Wazuh dashboard.
- Automate CrowdSec bouncers for real-time blocking.
- Segment vulnerable test machines from internal networks.

100-Word Non-Technical Manager Briefing

A security test was performed on a deliberately vulnerable server to evaluate our monitoring and response capability. The attacker successfully accessed the server using an outdated FTP service. Our monitoring tool, Wazuh, detected the attack immediately and logged the event. To protect the environment, we used CrowdSec to block the attacker’s IP address, preventing further communication with our systems. This shows that our detection and response pipeline works effectively, but also highlights the importance of removing outdated services and improving network isolation. Strengthening these areas will reduce risk and improve our overall cybersecurity posture.