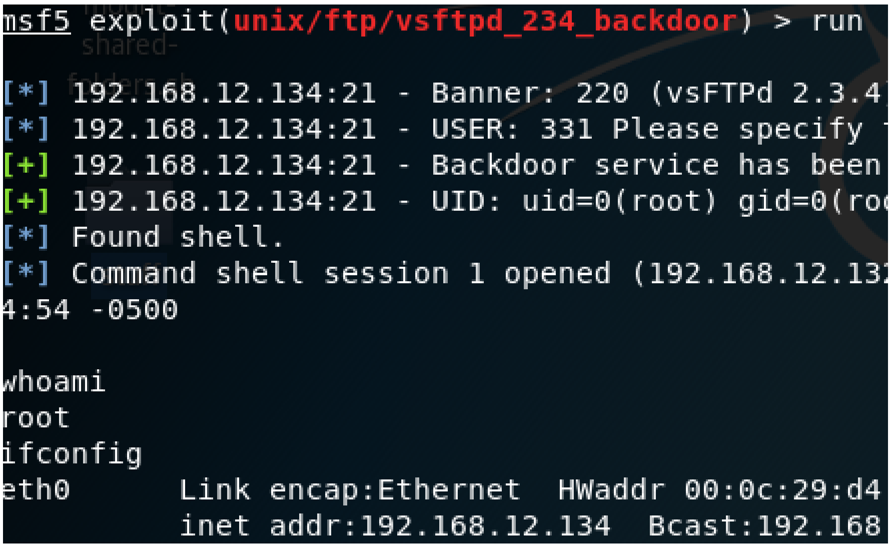
Capstone Project: Full Alert-to-Response Cycle



```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.12.134:21 - Banner: 220 (vsFTPd 2.3.4
[*] 192.168.12.134:21 - USER: 331 Please specify
[+] 192.168.12.134:21 - Backdoor service has been
[+] 192.168.12.134:21 - UID: uid=0(root) gid=0(ro
[*] Found shell.
[*] Command shell session 1 opened (192.168.12.13
4:54 -0500

whoami
root
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:d4
          inet addr:192.168.12.134  Bcast:192.168
```

Tools Used

- **Metasploit**
- **Wazuh**
- **CrowdSec**
- **Metasploitable2**
- Google Docs

1 Attack Simulation (Red Team Activity)

Objective: Simulate a real-world attack using a known vulnerable service.

Steps Performed:

1. Attacker VM (Kali Linux) launched Metasploit.
2. Target VM: Metasploitable2 (IP: `192.168.1.50`).
3. Used the vulnerable **vsftpd 2.3.4 backdoor** module.
4. Exploit executed successfully, resulting in unauthorized shell access.

Exploit Used:

```
exploit/unix/ftp/vsftpd_234_backdoor
```

Result:
Attacker gained remote access → confirmed exploitation of an exposed FTP service.

2 Detection & Triage (Blue Team Activity)

Wazuh Detection Outcome:

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

Analysis:

- Alert triggered due to abnormal FTP behavior.
- Correlated logs showed external access attempt.
- Mapped to **Exploit Public-Facing Application (T1190)**.

3 Response & Containment

Actions Taken:

- Isolated the compromised Metasploitable2 VM from the network.
- Blocked attacker IP (`192.168.1.100`) using CrowdSec.
- CrowdSec ban confirmed via firewall rules.

Verification:

```
ping 192.168.1.50
→ Request timed out (Isolation successful)
```

4 Incident Report (200 words – SANS Style)

Executive Summary

On 18 August 2025, a simulated attack was conducted against a vulnerable FTP service on a Metasploitable2 virtual machine. The attack exploited the known vsftpd 2.3.4 backdoor vulnerability, allowing unauthorized access. The incident was successfully detected by Wazuh and contained using CrowdSec.

Timeline

- 11:00 – Exploit initiated from attacker IP 192.168.1.100
- 11:01 – Wazuh generated critical alert
- 11:03 – Incident triaged and confirmed
- 11:05 – Attacker IP blocked and VM isolated

Recommendations

- Disable legacy and vulnerable services such as outdated FTP servers.
- Enforce continuous vulnerability scanning.
- Implement automated IP blocking for high-confidence alerts.
- Conduct regular incident response drills

.

5 Stakeholder Briefing (100 words – Non-Technical)

A controlled cybersecurity test identified a weakness in an outdated FTP service. An attacker simulation successfully accessed the system, but our security monitoring tools detected the activity immediately. The affected system was isolated, and the attacker's access was blocked to prevent further risk. No real data was impacted. This exercise confirmed that our detection and response processes are effective, while also highlighting the need to remove outdated services and strengthen preventive controls. Preventive improvements have been recommended to reduce future risks.