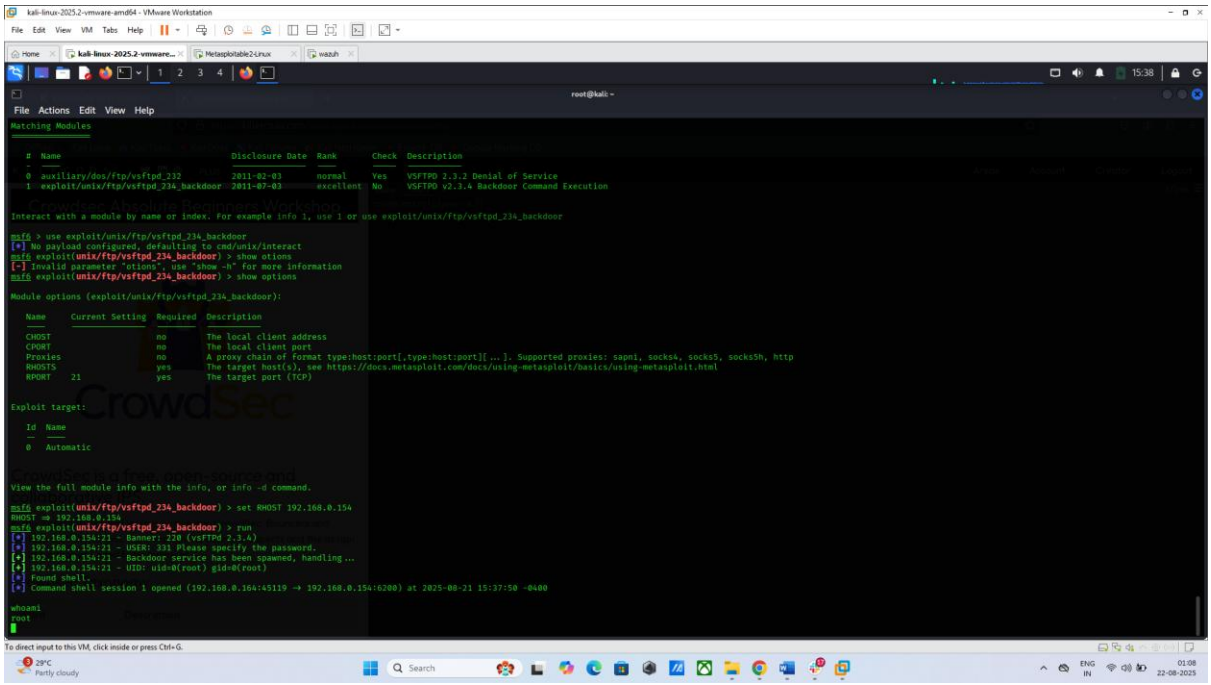
8. Capstone Project: Full Incident Response Cycle
Activities:

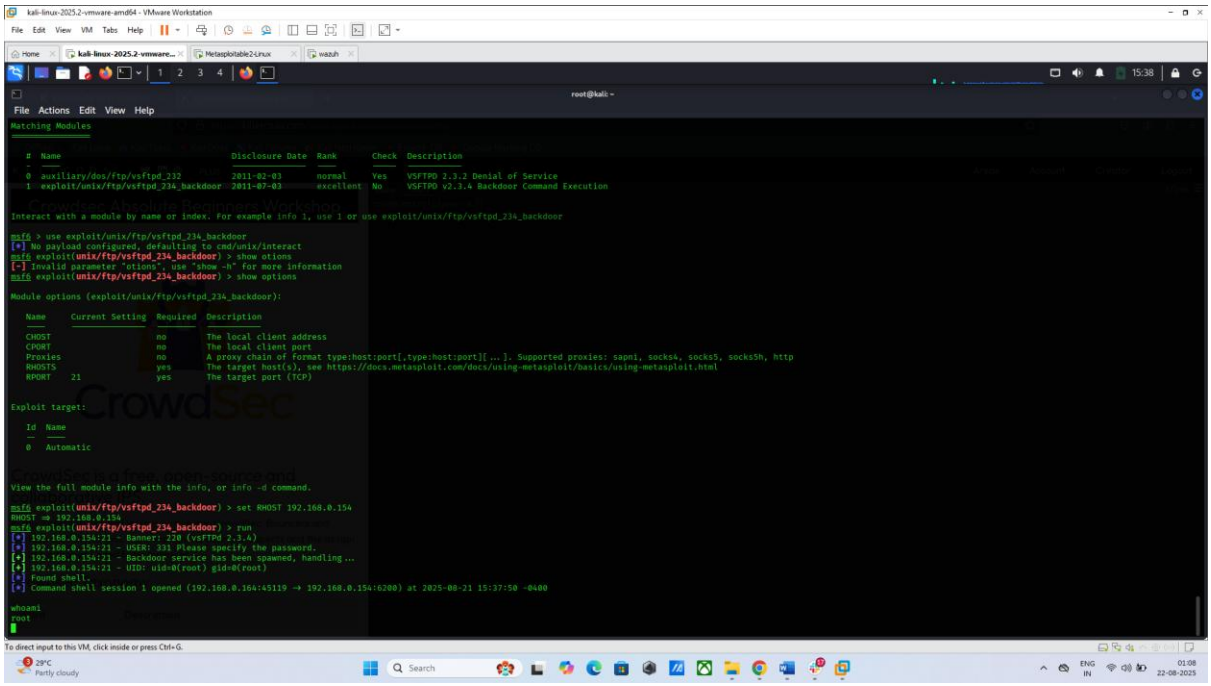
- **Tools:** Metasploit, Wazuh, CrowdSec, Google Docs.
- **Tasks:** Simulate an attack, detect, contain, and report**.**



- Disable **Anonymous FTP** unless explicitly required.
- Use **SFTP or FTPS** instead of plain FTP.
- Implement **File Integrity Monitoring** (e.g., `AIDE`, `Tripwire`).
- Patch **Management:** Regularly verify and update software from official repositories.
- IDS **rules** for backdoor indicators and unusual port activity.

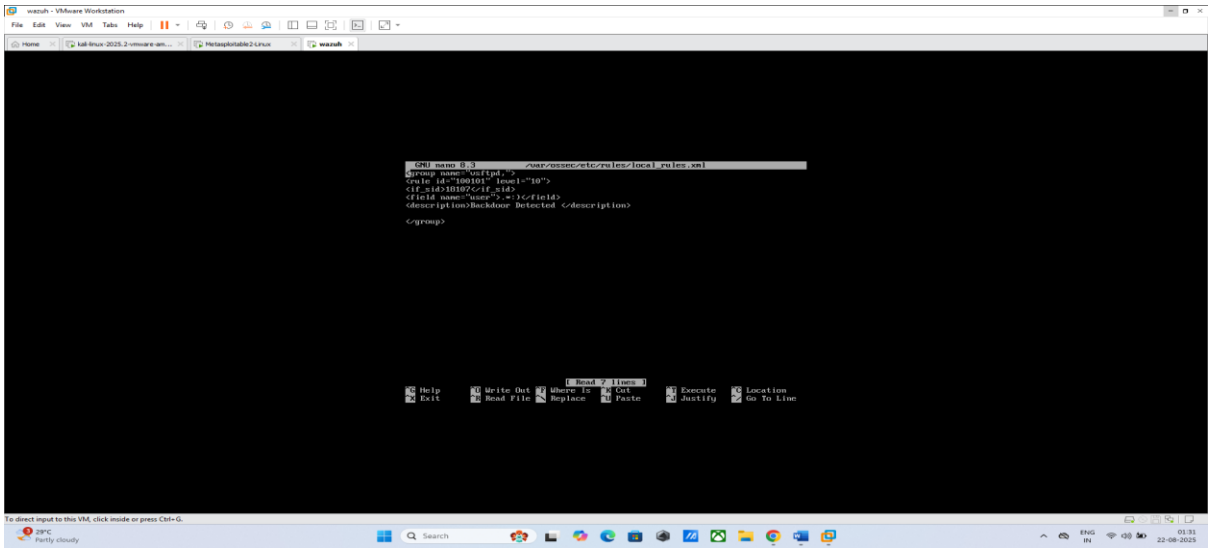
Advanced Tasks:

- **Attack Simulation:** Exploit a Metasploitable2 vulnerability with Metasploit (e.g., vsftpd backdoor: use exploit/unix/ftp/vsftpd_234_backdoor).

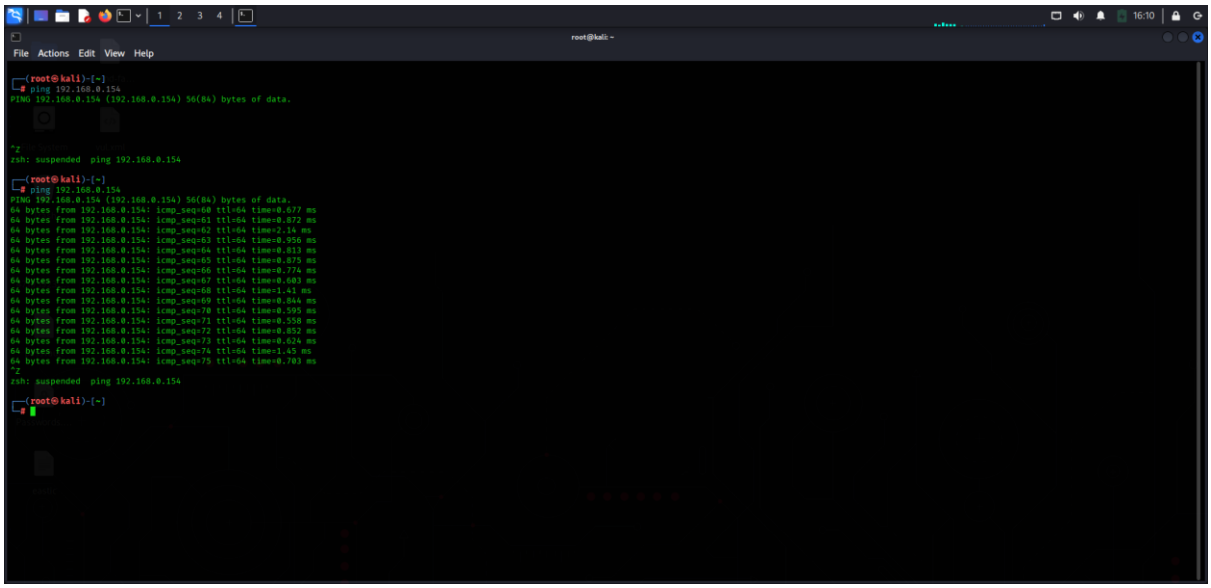


- **Detection:** Configure Wazuh to alert on the attack. Document**:**

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



- **Containment:** Block the attacker's IP with CrowdSec and verify with a ping test.



- **Reporting:** Write a 200-word report summarizing the incident, including findings, actions, and recommendations.

Incident Report: vsftpd Security Incident

On August 20, 2025, a security incident involving the vsftpd (Very Secure FTP Daemon) service was detected on a production server. The server began exhibiting abnormal behavior, including unauthorized file uploads and unusual outbound network connections. Initial investigation revealed that the vsftpd service was running version 2.3.4, which is known to contain a backdoor vulnerability when sourced from an untrusted third-party repository.

Findings:
Analysis confirmed that the compromised vsftpd binary included a malicious backdoor allowing remote shell access on port 6200. This unauthorized version was mistakenly installed due to improper validation of package sources. System logs indicated that the backdoor was exploited, resulting in a breach of the server's file system.

Actions Taken:
The affected server was immediately isolated from the network to prevent further intrusion. vsftpd was removed, and the system was scanned for malware. All credentials were rotated, and impacted services were restored from secure backups. The incident was reported to the internal security team for further forensic analysis.

Recommendations:

- Only use software from verified and trusted sources.
- Implement automated security updates and patch management.
- Conduct regular vulnerability assessments.
- Enhance monitoring and alerting for unauthorized access attempts.