



8. Capstone Project: Full Incident Response Cycle

Activities:

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

```
Kali Linux [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help

File Actions Edit View Help

Blank@kali: ~
$ cat /dev/urandom | tr -dc 'a-z0-9' | fold -w 64 | xargs -n 1 sh
Metasploit
=====
+-- metasploit v6.4.69-dev
+-- --[ 2529 exploits - 1382 auxiliary - 432 post
+-- --[ 1672 payloads - 49 encoders - 13 nops
+-- --[ 9 evasion

Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > RHOST 192.168.29.132
[!] Unknown command: RHOST. Did you mean host? Run the help command for more details.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.29.132
RHOST => 192.168.29.132
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  ----      -
  CHOST      no               no        The local client address
  CPORT      no               no        The local client port
  Proxies    no               no        A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     192.168.29.132  yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
  RPORT      21               yes       The target port (TCP)

Exploit target:

  Id  Name
  --  --
  0    Automatic

View the full module info with the info, or info -d command.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

- 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.



- **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.