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.

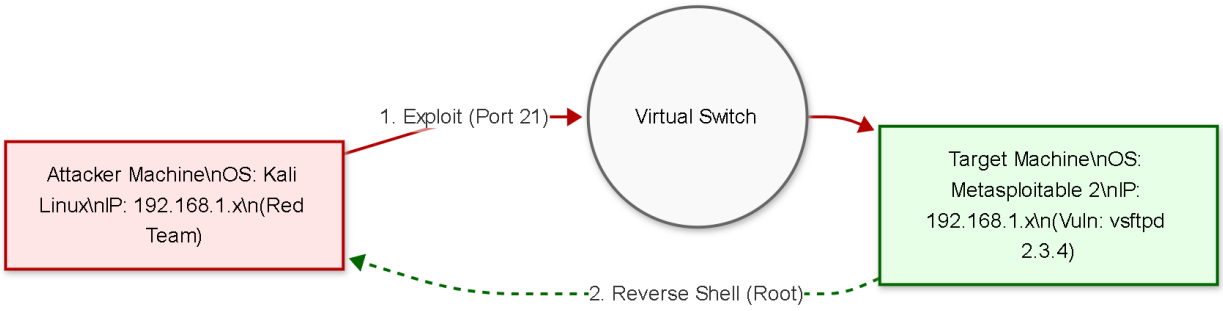
2.3 Appendix A: Technical Command Reference

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.

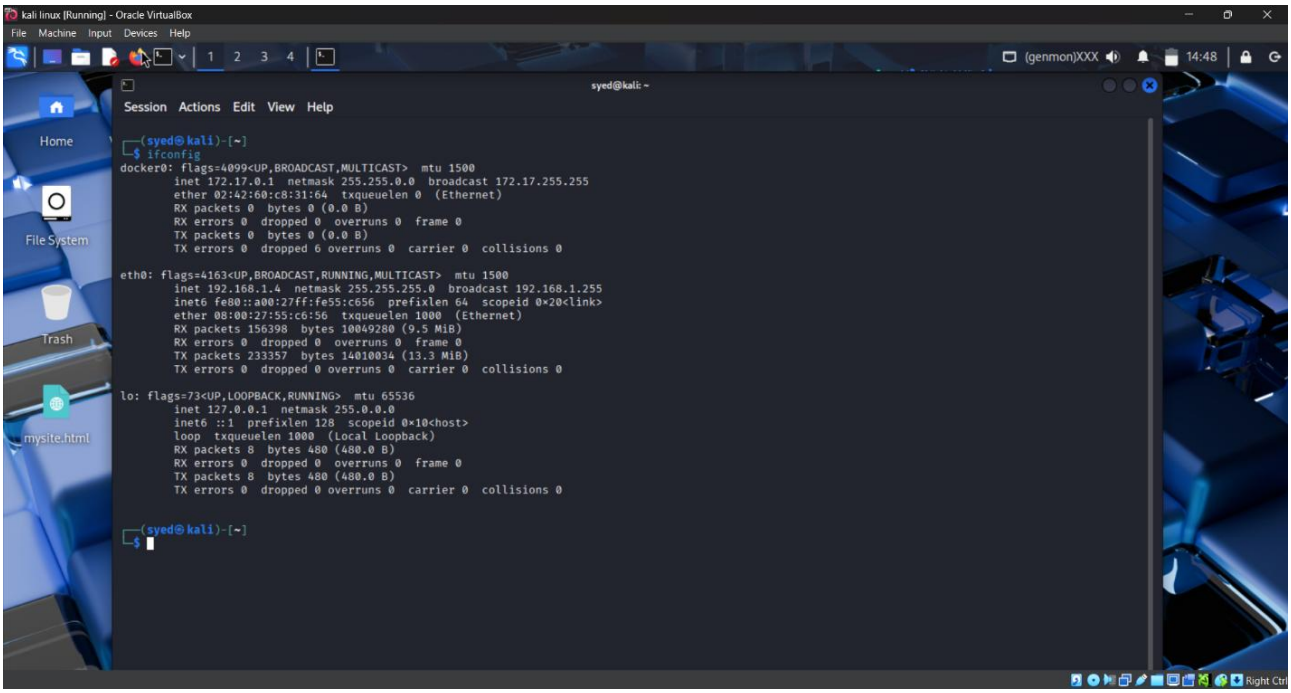


3. Phase 1: Reconnaissance & Scanning

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

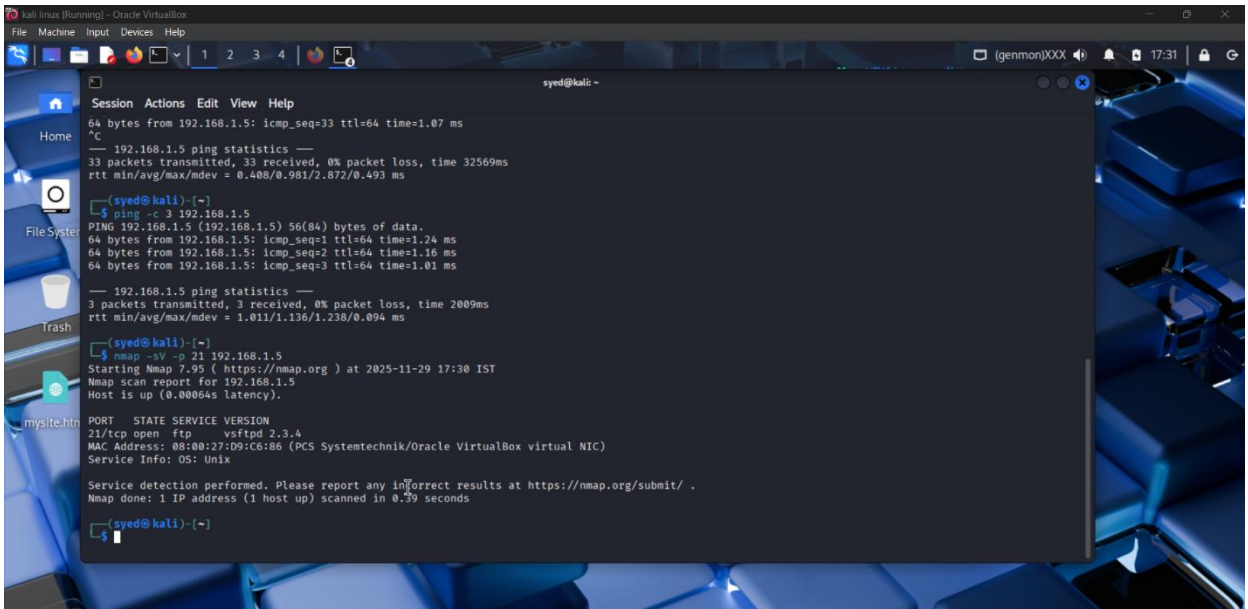


3.2 Service Enumeration

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



4. Phase 2: Vulnerability Assessment & Exploitation

4.1 Vulnerability Analysis

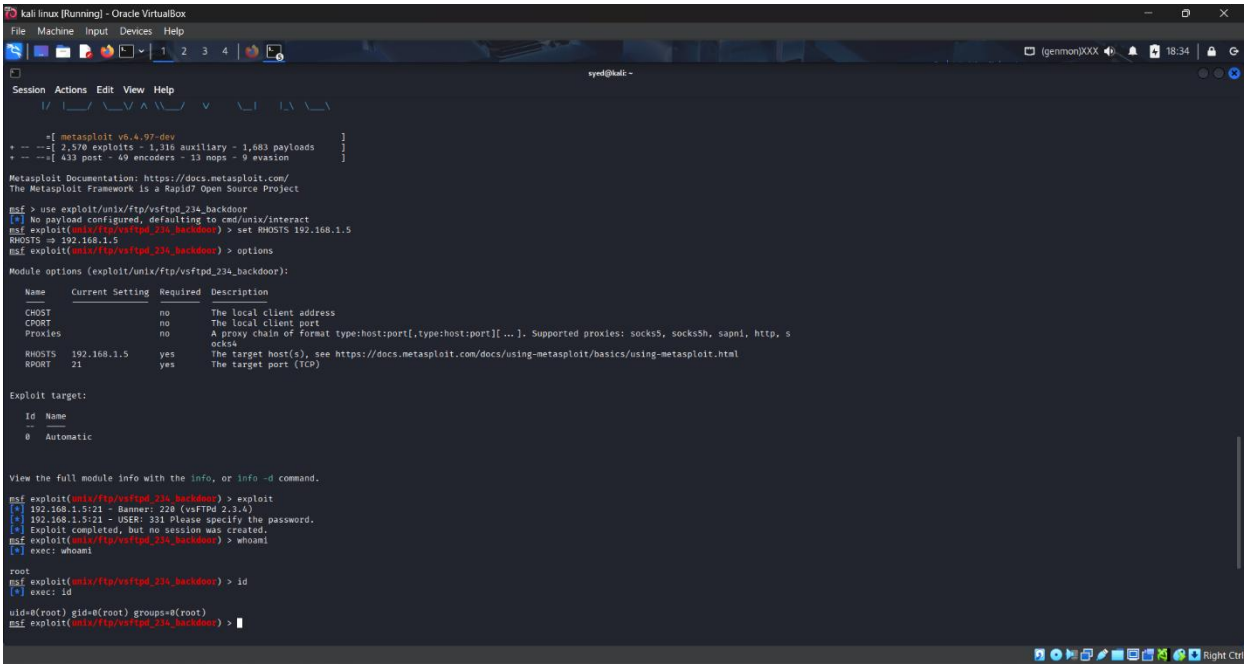
- **Vulnerability:** vsftpd 2.3.4 Backdoor Command Execution
- **CVE ID:** CVE-2011-2523
- **Severity:** Critical
- **Description:** The malicious code in this version opens a shell on port 6200 if a specific string (a smiley face `:)`) is sent during the FTP handshake.

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



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

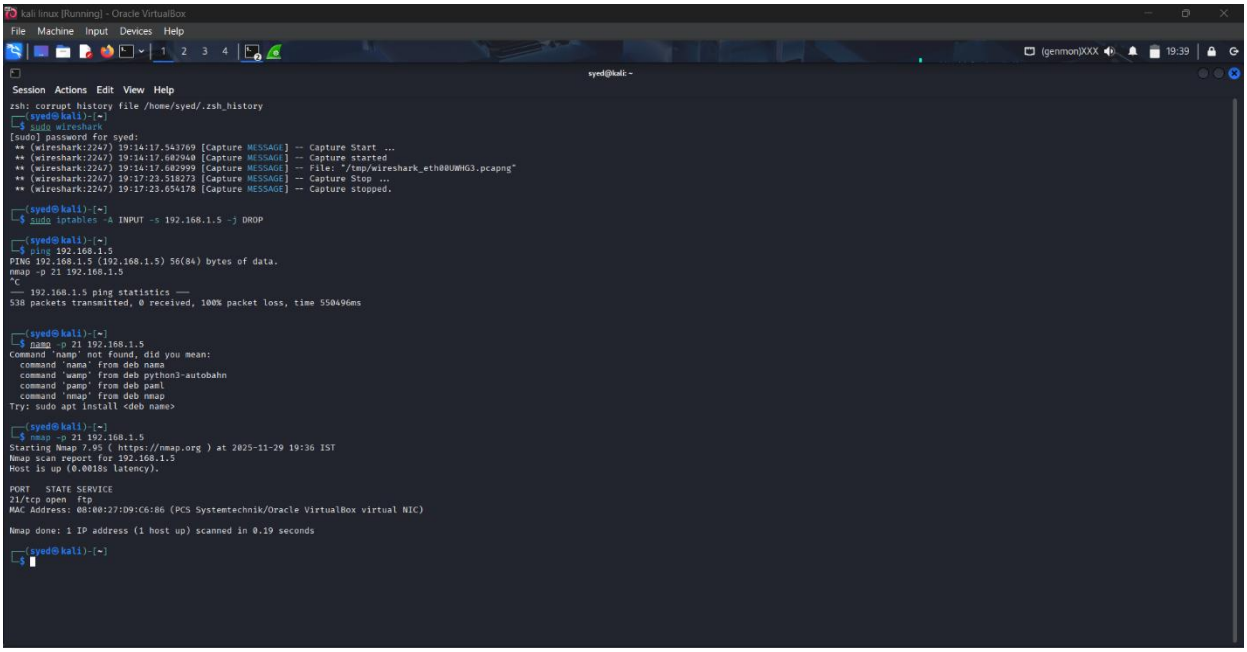
To prevent data exfiltration and stop the attacker from maintaining access, immediate containment measures were deployed using iptables . We implemented a rule to drop all incoming traffic from the attacker's IP address.

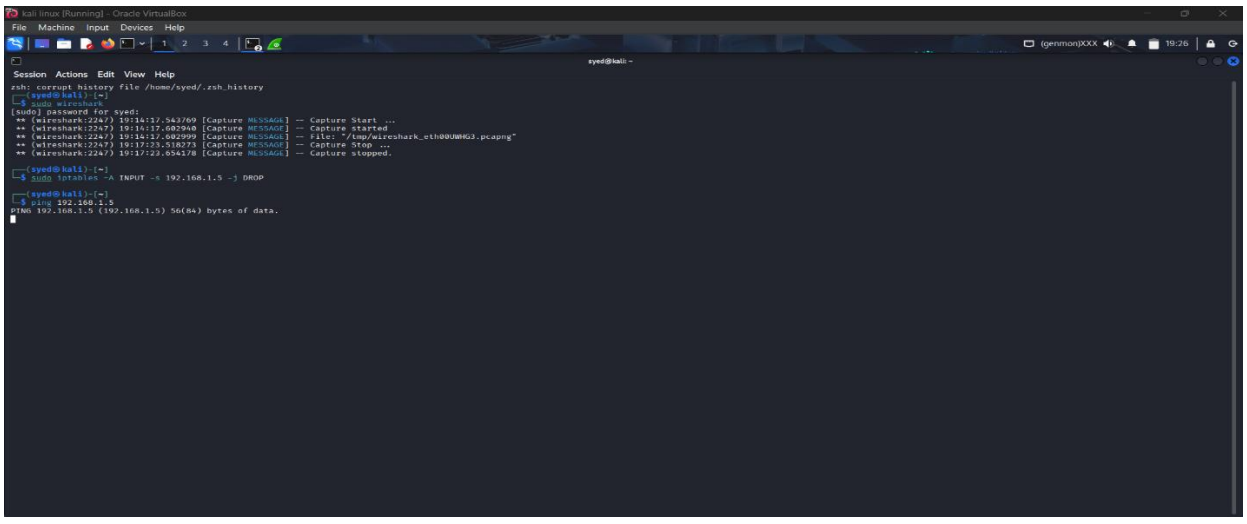
Command Executed:

```
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





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.