

## **Práctica 45. Borrado de huellas (Por HxC Mods-Adm)**

El borrado de huellas es algo que se produce después de ocurrir una intrusión y responde a la necesidad de ocultar los rastros que el intruso haya podido dejar en el sistema atacado.

Como todo, dependerá de lo que se haya tocado... básicamente podemos agrupar estos pasos como siguen:

- Eliminar o esconder los archivos copiados en el destino
- Parar la auditoría
- Eliminar los logs de sucesos, de seguridad
- Parar el antivirus, firewall, etc.
- Eliminar los logs de sucesos de las aplicaciones “tocadas”, por ejemplo, si accediésemos a la víctima mediante un bug de un webserver habrá que eliminar los logs de ese servidor web
- Dejar una puerta trasera
- Volver a dejar todo como estaba antes de la intrusión

Es IMPOSIBLE describir todos y cada uno de los pasos a seguir para cada tipo de intrusión, los anteriormente mencionados son muy genéricos pero como muestra de lo que se debe hacer son un ejemplo válido.

### **Eliminar o esconder los archivos copiados en el destino**

Lo más simple será borrar los archivos subidos mediante el comando del mismo sistema operativo

Para ocultarlos ya hemos descrito alguna técnica, los stream de ficheros, los atributos de oculto, sistema, etc...

Otras técnicas usadas son los rootkits, esas pequeñas utilidades son muy peligrosas porque pueden ocultar hasta los mismísimos procesos en ejecución, casi todas ellas afortunadamente las detectan los antivirus pero hay que tener cuidado con las que vayan apareciendo.

La mejor técnica para defenderse de ellas es mantener un inventario y auditar los servicios, los procesos en ejecución, la capacidad de disco, los permisos de acceso a archivos....

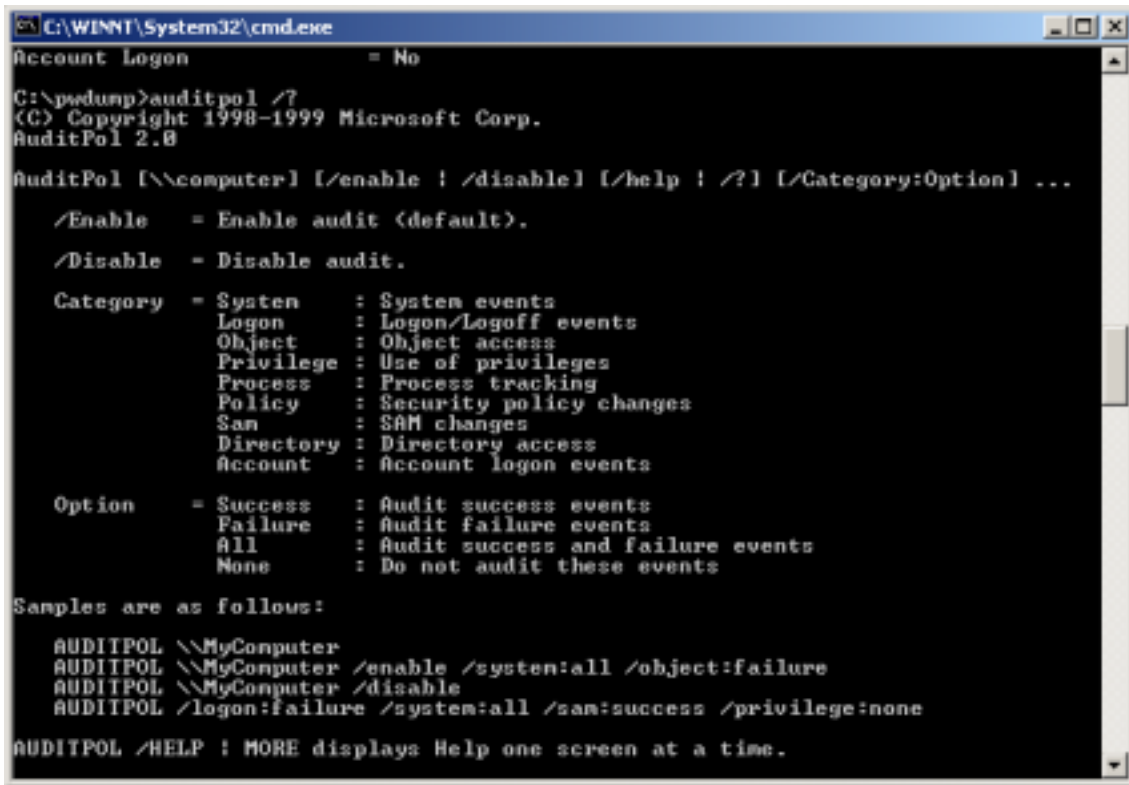
Una de las rootkis más conocidas es ntroot, pero te advierto, a parte de que tu antivirus la detectará como un programa sospechoso, tu Windows puede dejar de funcionar correctamente.

En prácticas anteriores ya te comenté el uso de ellas, revisa la práctica 19 para obtener más información

### **Parar la auditoría**

Detener el proceso de auditoría es otro de los pasos a seguir... las auditorías del sistema permiten seguir los pasos que un usuario realizó, sus cambios de pass, sus accesos a los archivos y carpetas del equipo, etc.

Para detener-iniciar la auditoría de Windows puedes usar auditpol



```
C:\WINNT\System32\cmd.exe
Account Logon = No
C:\psdump>auditpol /?
(C) Copyright 1998-1999 Microsoft Corp.
AuditPol 2.0

AuditPol [\\computer] [/enable | /disable] [/help | /?] [/Category:Option] ...

/Enable = Enable audit (default).
/Disable = Disable audit.

Category = System : System events
           Logon   : Logon/Logoff events
           Object  : Object access
           Privilege : Use of privileges
           Process : Process tracking
           Policy  : Security policy changes
           Sam     : SAM changes
           Directory : Directory access
           Account : Account logon events

Option = Success : Audit success events
        Failure  : Audit failure events
        All      : Audit success and failure events
        None     : Do not audit these events

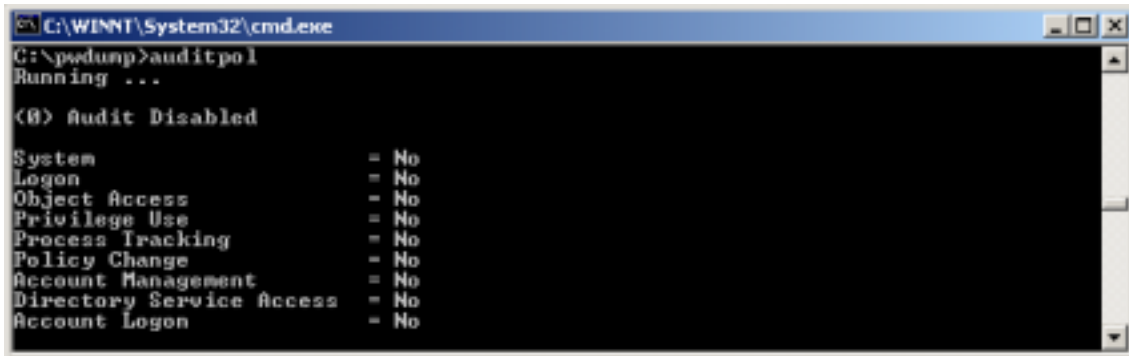
Samples are as follows:

AUDITPOL \\MyComputer
AUDITPOL \\MyComputer /enable /system:all /object:failure
AUDITPOL \\MyComputer /disable
AUDITPOL /logon:failure /system:all /sam:success /privilege:none

AUDITPOL /HELP ! MORE displays Help one screen at a time.
```

Como ves su uso es sencillo

C:\>auditpol, mostrará el estado de la auditoria



```
C:\WINNT\System32\cmd.exe
C:\psdump>auditpol
Running ...

(0) Audit Disabled

System = No
Logon = No
Object Access = No
Privilege Use = No
Process Tracking = No
Policy Change = No
Account Management = No
Directory Service Access = No
Account Logon = No
```

Auditpol /enable activa la auditoria

Auditpol /disable desactiva la auditoria

Si tenemos permisos suficientes podemos iniciarla-pararla si indicamos la ip del equipo remoto

Auditpol [\\ip.del.equipo](#) /disable

Cuando la auditoría está activa en el visor de sucesos se mostrarán los registros de los eventos auditados, auditpol es una utilidad del Kit de Recursos de Windows

## Eliminar los logs de sucesos, de seguridad

Para esto tendremos que recurrir a herramientas de terceros

Se conocen como zappers y hay muchos: Clearlogs, Winzapper, elsave, rmlogs, etc...

Su uso es muy simple, basta con indicar el equipo en cuestión y se eliminarán los logs del visor de sucesos.

También hay otros como Dumpreg, Dumpwin, etc.. que vuelcan (copia) los registros de sucesos, luego solo hay que manipularlos con algun editor, volver a subirlos y ya está.

Esta técnica es más util porque el administrador de la red se mosqueará si de la noche a la mañana desaparecen todos los registros de sucesos, si los manipulamos en lugar de borrarlos conseguiremos ocultar sólo lo que nos interesa y no eliminar todo.

Para estos menesteres también son útiles herramientas del tipo psservices o sc, etc... con ellas podemos ver los procesos en ejecución.. incluso pararlos o reiniciarlos, de ese modo también podremos parar el antivirus o el firewall o cualquier otro tipo de aplicación “que moleste”