

Práctica 16. Habilitar y deshabilitar las auditorías (Por HxC Mods-Adm)

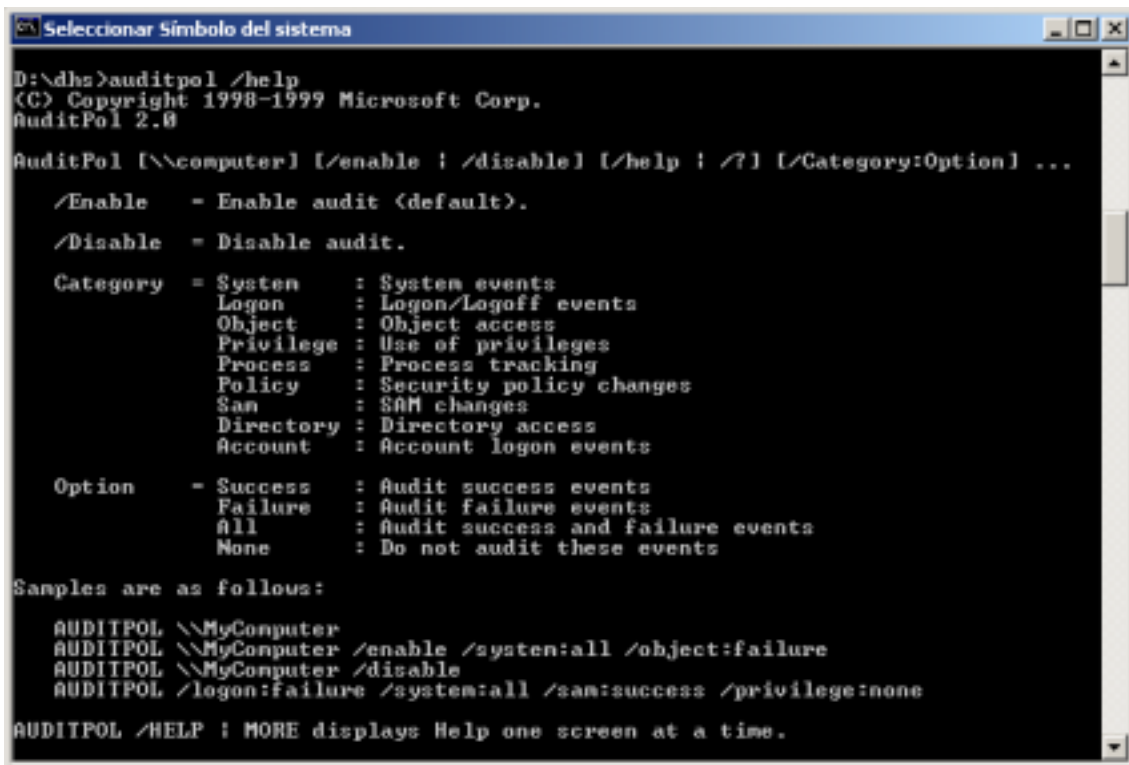
Una de las principales maniobras que debemos realizar una vez alcanzado el objetivo es detener las auditorías y/o eliminar los rastros dejados en el momento de la intrusión. Existen aplicaciones y software (antivirus, firewalls, IDS, etc.) que reactivan las auditorías si se desactivan por cualquier motivo, de forma que ya tenemos otro frente abierto, así que recuerda: conoce y estudia bien el sistema al que accedes o te comerán vivo.

Además deberemos “ganar acceso” como administrador, con lo cual la cosa puede empeorar mucho sin no lo conseguimos, por tanto PIENSA: Si no estás seguro de lo que haces puedes tener problemas, prueba siempre en “redes propias”, búscate un PC de apoyo para simular las técnicas y si puedes, intenta adoptar el mismo escenario de tu objetivo. No necesitas un super-equipo para eso, cualquier viejo PC te puede servir, en el mercado de 2ª mano puedes encontrar Pentium II/III completitos y con prestaciones aceptables por menos de 200 euros, así que quedas advertido.

Detener la auditoría de un Servidor Web es un delito, aunque “no toques” ni un solo byte, no digamos nada si además le borras o modificas el registro de sucesos, advertido de nuevo, las pruebas en casa.

Para inspeccionar, iniciar o detener la auditoría puedes usar la herramienta auditpol del Kit de Recursos de Windows 2000.

Su uso es muy simple:



```
D:\dhs>auditpol /help
(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

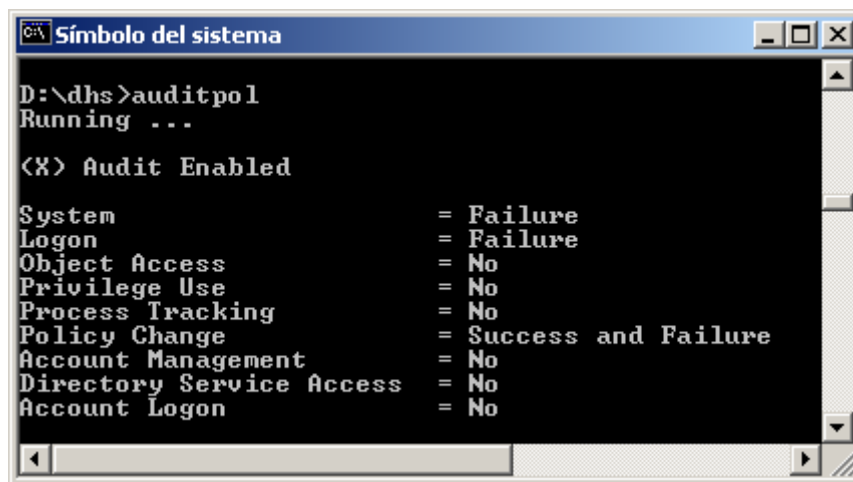
Samples are as follows:

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.
```

Para conocer el estado de la auditoría de tu propio equipo puedes usar simplemente la sintaxis auditpol y se mostrará el estado y los objetos o categorías auditadas, cuando lleguemos al escaneo de redes encontraremos herramientas que nos permitirán conocer el estado de la auditoría sin necesidad de contar con privilegios administrativos, lo de modificar la auditoría es otro asunto.

Ejemplo:



```
D:\dhs>auditpol
Running ...

<X> Audit Enabled

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

Auditoría Activa, registros de sistema y logon activados contra accesos erróneos y auditar cambios en la política de auditoría, también activados.

¿Qué significa esto? Pues que el administrador del sistema ha activado la auditoría para el equipo local de tal forma que se registrarán los accesos con nombre de usuario y/o contraseña inválidos, así como, los cambios efectuados en la política del sistema, esto es, que si desactivamos la auditoría se registrará un suceso que así lo indica, lo cual delatará lo que ocurre con un simple vistazo al registro de sucesos.

Existen aplicaciones de seguridad que además pueden enviar una alerta (vía mail o correo interno) al administrador de ello, en tiempo real.

La buena noticia es que el Registro de Sucesos de Windows advertirá de los cambios, pero en el mejor de los casos sólo mostrará el usuario y/o el nombre Netbios de la máquina del que proviene la orden, NO LA IP.

La mala noticia es que existen aplicaciones de terceros que sí registrarán la IP remota en esas situaciones.

Resumiendo, aún contando con los medios y conocimientos para acceder a un equipo remoto “atravesando” su sistema de seguridad, antes hay que conocer a fondo los servicios, aplicaciones instaladas o en ejecución, mecanismos de seguridad, etc., de todo ello se hablará en la sección correspondiente a la exploración de objetivos, aunque nuestras intenciones no sean las mismas que las de un ladrón al atracar un banco, podríamos decir que nadie “asalta un banco” sin haber estudiado previamente algunos puntos básicos: Cámaras de seguridad, Vigilantes, Número de empleados, horario de apertura/cierre, tránsito de clientes, “recompensa” a obtener, vías de escape, etc.

Aquellos que un buen día deciden escanear una red y “colarse” en un equipo remoto por el simple hecho que encuentran un puerto abierto o un servicio vulnerable consiguen el rechazo general de todos, son unos lamers, que simplemente piensan que ya son dioses por conocer cómo ocultar su IP y unas cuantas herramientas, seguro que no aprenderán nada más, hasta que un día se equivoquen en el destino y los pasarán por la piedra.

En la siguiente página se muestran unas capturas de pantalla de lo que el administrador vería cuando se deshabilita la auditoría, no creo que sea necesario explicar cómo se muestra el registro de sucesos, ¿no?

