uc3m | Universidad Carlos III de Madrid

Máster Universitario en Ciberseguridad

2018-2019

Trabajo Fin de Máster

“Ciberejercicios para evaluar Active Directory en sus distinas versiones. ”

Borja Lorenzo Fernádez

Tutor

Andrés Marín López

Agradecimientos

Abstract

Microsoft Active Directory se ha convertido en una de las partes fundamentales de las empresas en la actualidad y se le considera como el *core* de la organización. Active Directory permite a los administradores gestionar de manera eficiente la información de la empresa y los límites de la misma. Esta información puede englobar usuarios, clientes, proveedores, dispositivos como ordenadores, servidores o impresoras, servicios y aplicaciones y la forma de interacción entre ellos así como los diferentes permisos que tiene cada usuario o grupo de usuarios. Esta información, como se puede deducir, supone un importante objetivo para atacantes y ciberdelincuentes y un gran problema de seguridad para las empresas si estos sistemas de gestión se ven comprometidos. Esto a llevado a cabo un gran aumento de ciberataques contra Active Directory con el objetivo principal de recolectar dicha información y comprometer la seguridad total de una empresa. Además, en los últimos años se han perfeccionado las técnica principales de ataque así como la implementación de novedosas herramientas que facilitan todo tipo de ataques.

Con el fin de contribuir al desarrollo y mejora de la seguridad de Active Directory y por ende, de las empresas y particulares que hacen uso de ello, el trabajo realizado se centra en el estudio de los principales componentes que engloban la seguridad y gestión del sistema de directorio Active Directory a través de la creación de un laboratorio, de manera local, y el análisis y revisión de los principales ataques y amenazas usadas en la actualidad para vulnerar dicho sistema de gestión. Además, se ha implementado una topología que simula una empresa ficticia e implementa las últimas versiones proporcionadas por Microsoft que gestionan cada dominio.

Palabras Clave:

Microsoft Active Directory, Domain Controller, Kerberos, Ciberseguridad, Windows Server, Pentesting, Red Team

Índice general

Índice de figuras

Índice de tablas

1. Introducción

En los últimos años, empresas y organizaciones se han visto en la necesidad de gestionar de una manera eficiente y centralizada la información y recursos en red que disponen, activo fundamental para el correcto funcionamiento del negocio. El aumento masivo de dicha información además de la necesidad de crear, distribuir y manipular tal cantidad de datos, ya sea a través de servicios de bases de datos como puede ser servicios MySQL, la obtención de servidores y dispositivos para su almacenamiento, la creación de aplicaciones web y servicios que permitan su distribución o la gestión de los usuarios que puedan manipularla o consultarla supone una gran cantidad de agentes que intervienen en el funcionamiento que es necesario controlar y regular. Microsoft Active Directory supone una solución a esa problemática a través de un servicio de directorio como base de datos distribuida que permite la gestión, administración y localización de todos los recursos en red [1].

Dentro del panorama actual, los servicios de Microsoft Active Directory se ha convertido en uno de los pilares que sostienen la organización de los recursos en red de la mayoría de las empresas vigentes así como uno de los principales objetivos para atacantes debido a dicha importancia. Esto se puede comprobar en el principal interés que tienen los principales grupos de ciberdelincuentes como APT28, Cobalt Strike... por esta infraestructura o los ataques de ransomware WannaCry, NotPetya, MBR-ONI, etc, que ponen a Active Directory en el punto de mira y centro de sus ataques [2]. En los últimos años, se ha visto un aumento considerable de vulnerabilidades críticas que afectan a la seguridad y que detectan y hacen considerablemente más sencillo su explotación.

Por todo ello y con el fin de abordar esta problemática, el trabajo realizado se ha centrado en la revisión, análisis y prueba en profundidad de las principales amenazas que suponen un problema de seguridad para Active Directory en sus diferentes versiones, técnicas como Pass-The-Hass, NTLM Relay, Kerberoast, etc que serán detalladas en los capítulos posteriores. Además, también se proporciona las directrices para la creación de un laboratorio local que permite la prueba de los ataques detallados así como la posibilidad de probar nuevas técnicas y ataques sin poner en riesgo la seguriidad de ningún entorno real u organización.

1.1. Estado del Arte

Para el desarrollo del trabajo, se ha considerado las siguientes versiones proporcionadas por Microsoft para la instalación de los dominios que van a formar partes del Active

Directory y van a ejecutar los Domain Controllers:

- **Windows Server 2019**
- **Windows Server 2016**
- **Windows Server 2012 R2**

Por lo tanto, se ha dejado la versión más antigua Windows Server 2008 como objeto de estudio o posible implantación en trabajo futuro al ser la versión más obsoleta. Aunque esto no implica que no haya empresas que aún siguen usando dicha versión.

En cuanto a los ataques a analizar de manera detallada se han considerado los siguientes:

- **Pass-The-Hash**
- **NTLM Relay**
- **Overpass-The-Hash**
- **Pass-The-Ticket**
- **Golden/Silver Ticket**
- **Kerberoast**

Como se puede observar, la mayoría de los ataques no son específicos de Active Directory si no que atacan a los protocolos NTLM y Kerberos, por lo que, también se van a detallar en profundidad estos protocolos en los capitulos siguientes.

1.2. Objetivos

El objetivo principal de este trabajo es la creación de un laboratorio que provea la infraestructura necesaria para la replicación de las principales técnicas de ataque a Active Directory así como la revisión de las mismas sobre las diferentes versiones proporcionadas por Microsoft. La creación del laboratorio posibilita tanto a *Pentesters* o expertos en seguridad ofensiva realizar ejercicios de *Read Team* en entornos controlados o réplicas de un entorno real como a administradores de sistemas para probar nuevas configuraciones y reglas para equipos de *Blue Team*.

Además, este trabajo tiene como objetivo la adquisición de conocimiento sobre Active Directory como punto de partida para futuras investigaciones. Como se ha visto en la

introducción Active Directory es una parte fundamental de una empresa y es uno de los principales objetivos de atacantes, conocer los principales ataques y cómo está organizado es de gran importancia hoy en día, permitiendo aasí una correcta implementación que minimice los riesgos a los que está sometido.

1.3. Organización del Proyecto

El presente documento se divide en 7 capítulos, en los cuales en primera instancia se detallan los aspectos a tener en cuenta relacionados con Active Directoy, se detalla el laboratorio implementado, las pruebas que se van a realizar, la experimentación realizada así como los resultados obtenidos durante el trascurso:

En el Capítulo 2 se detalla los aspectos relacionados con Active Directory, en primer lugar se define la autenticación y autorización en sistemas Windows tanto localmente como en dominio, se analizan los protocolos NT Lan Manager y Kerberos y la terminología relacionada con Active Directory.

En el Capitulo 3 se desarrolla la topología que se ha elegido para la creación del laboratorio de pruebas con las diferentes versiones de Windows y su implementación.

En el Capítulo 4 se detallan los ataques elegidos para realizar la experimentación.

En el Capítulo 5, una vez detalladas tanto el laboratorio como las ataaques principales objeto de estudio, se muestran las diferentes pruebas realizas en las versiones de Windows especificadas en el estado del arte.

En el Capítulo 6 se presentan y se discuten los resultados obtenidos.

En el Capítulo 7, para finalizar el proyecto, se lleva a cabo una reflexión sobre el esfuerzo realizado y sus diferentes líneas de trabajo futuro.

2. Aspectos Clave

Este capítulo aborda los términos y definiciones a tener en cuenta y sirve como introducción a Active Directory. En primer lugar, se define la forma en la que los Sistemas Windows gestioana la autenticación y la auterización. Posteriormente, se definen los protocolos de seguridad para la verificación de la autenticación NT Lan Manager y Kerberos. Finalmente, se presenta Active Directory y la terminología necesaria relativa a este.

2.1. Autenticación y Autorización

Uno de los principales requisitos a la hora de entender como funcionan la mayoría de los ataques contra Sistemas Windows pasa por la gstión de la autenticación y autorización de los usuarios que inician sesión en el ordenador ya sea a nivel local o en red.

Por un lado, la **autenticación** consiste en la verificación de la identidad de un usuario, dicho con otras palabras, que el sistema de autenticación se asegure de que un usuario es quién dice ser. Por ejemplo, conociendo la contraseña del usuario que dice ser.

Por otro lado, la **autorización** consiste en establacer y delimitar los recursos a los que puede acceder, o no puede acceder ya que los tiene restringidos un usuario (o grupos de usuarios).

2.1.1. Inicio de sesión interactivo (Interactive Logon)

El proceso de autenticación a través de inicio de sesión interactivo del inglés *Interactive Logon*, a diferencia del inicio de sesión en red o *Network Logon*, es llevado a cabo por el proceso *WinLogon* que se encarga de recoger las credenciales introducidas por el usuario y su posterior validación. Un usuario que inicia sesión en un equipo ya sea localmente o un inicio de sesión en red introduce el usuario y la contraseña (denominado credenciales de usuario) y sirve para verificar la identidad del usuario. Por otro lado, cuando se inicia sesión a través de una Smart Card *(Smart Card Logon)* las credenciales están almacenadas en el chip de la tarjeta y estas son leídas por un dispositivo externo y el usuario introduce el *Personal Identification Number (PIN)* [3].

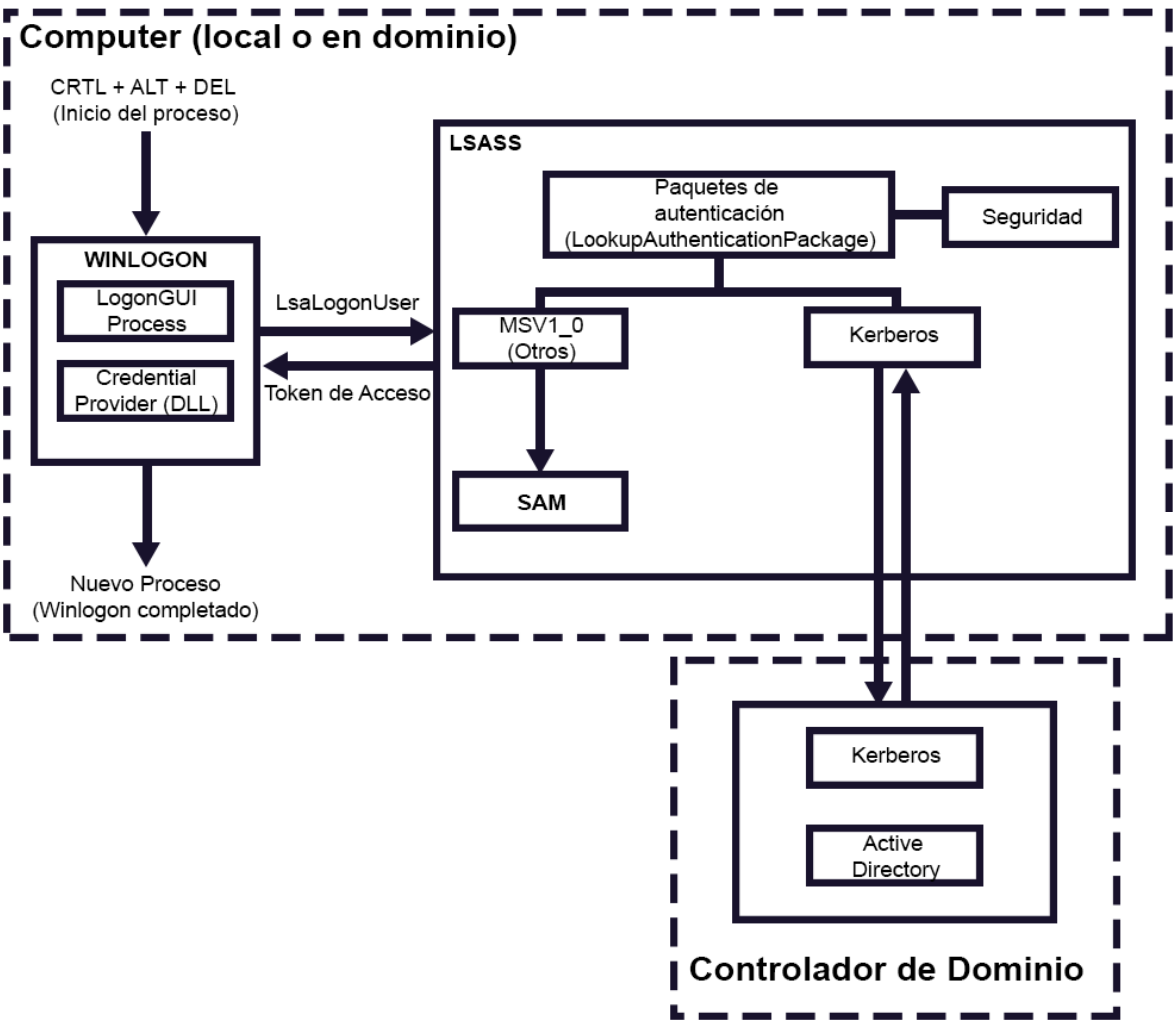

Fig. 2.1. Proceso de inicio de sesión interactivo (WinLogon).

Proceso WinLogon

WinLogon es el proceso encargado de coordinar el inicio de sesión. Además, este proceso también se encarga de gestionar el *logout*, lanzar los procesos necesarios para la autenticación de un usuario, cambiar las contraseñas, bloquear y desbloquear un equipo y proporcionar la seguridad necesaria para que ningún otro proceso pueda acceder a información sensible cuando estos procedimientos se están llevando a cabo.

Como se puede ver en la Figura 2.1 el proceso de inicio iterativo consta de varias fases [4]:

1. En primer lugar, el proceso de inicio de sesión comienza con una secuencia denominada *Secure Attention Sequence (SAS)*, esta secuencia es *CTRL + ALT + DEL* por defecto e inicia el proceso WinLogon.

2. Una vez iniciado el proceso WinLogon, este ejecuta el proceso *LogonUI* que proporciona la interfaz por defecto para introducir las credenciales y a su vez carga las bibliotecas

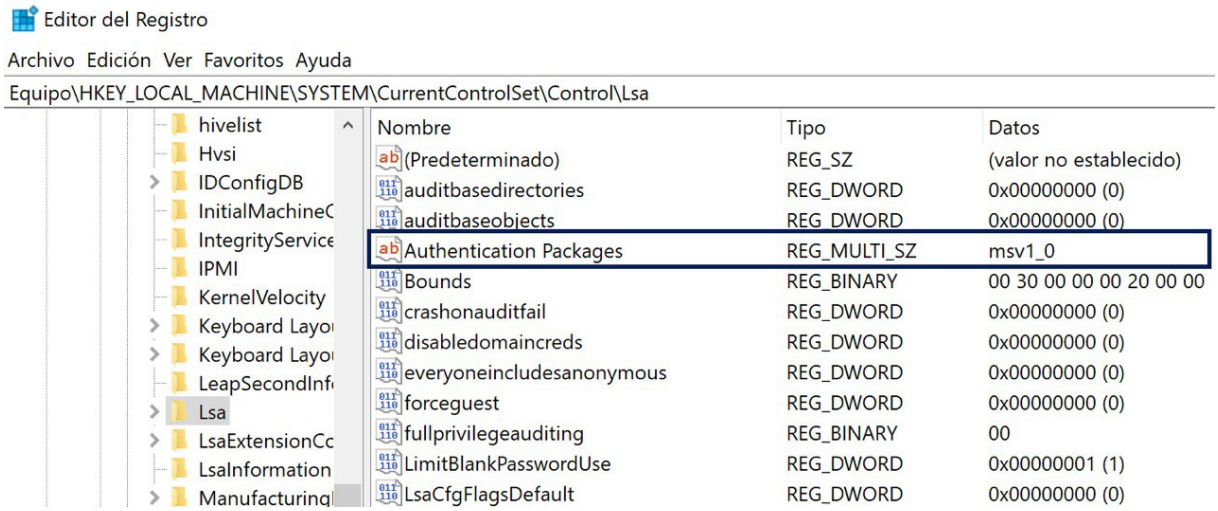

Fig. 2.2. Clave de registro sobre los paquetes de autenticación.

de enlace dinámico, del inglés *Dynamic-Link Library (DLL)* que se encargan de recoger las credenciales y pasarlas al proceso denominado Servicio Subsistema de Autoridad de Seguridad Local del inglés *Local Security Authority Subsystem Service* (LSASS). Estas DLLs denominadas *Credential Providers* se encuentran en [1] o en [2] (Si se trata de un inicio de sesión con Smart Cards).

3. Al ejecutarse Winlogon, también se crea un número identificador de seguridad del inglés *Security Identifier* (SID), este número se pasa como argumento en la llamada *LsaLogonUser* y será incluido en el Token de Acceso *(Access Token)* si la autenticación se procesa correctamente.

4. Una vez introducido usuario y contraseña, WinLogon llama al proceso LSASS a través de la función *LsaLookupAuthenticationPackage*. Esta función tiene como objetivo obtener los paquetes de autenticación disponibles en el sistema a través de la clave de registro [3] como se puede observar en la Figura 2.2.

5. Posteriormente, se envían las credendiales a través de la función *LsaLogonUser*. Si algún paquete de autenticación autentica el usuario el proceso continua, en cambio, si ningún paquete indica que se ha iniciado sesión correctamente el proceso acaba.

6. Una vez autenticado, el proceso LSASS comprobará en la base de datos de políticas locales si el usaurio autenticado tiene los permisos suficientes para realizar la acción que está solicitando. Si el inicio de sesión no coincide el proceso de autenticación acaba y LSASS elimina cualquier estructura de datos creada y lo notifica a WinLogon. Si el acceso está permitido, LSASS agrega los IDs de seguridad correspondientes, busca en la base de datos los permisos asociados a los usuarios del mismo grupo

[1] %SystemRoot%\System32\authui.dll
[2] %SystemRoot%\System32\SmartcardCredentialProvider.dll
[3] HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

del SID del usuario y los añade al token de acceso (*Access Token*) y crea el Token que será enviado a Winlogon con un mensaje de inicio de sesión correcto.

Una vez definido el proceso de inicio interactivo a grandes rasgos, se va a pasar a detallar los componentes mencionados que forman parte de dicho proceso.

Paquetes de Autenticación (Authentication Package)

2.2. NT Lan Manager

2.3. Kerberos

2.4. Active Directory

Bibliografía

[1] Microsoft, "Introducción a active directory," 2000. https://support.microsoft.com/es-es/help/196464.

[2] M. Bresman, "Wannacry, notpetya, mbr-oni and friends: Tales of wiper attacks and active directory destruction," 2018. https://www.semperis.com/blog/wannacry-notpetya-wiper-attacks-active-directory/.

[3] Microsoft, "How interactive logon works," 2017. https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2003/cc780332(v=ws.10).

[4] B. Catlin, P. Yosifovich, J. Hanrahan, M. Russinovich, A. Ionescu, and D. Solomon, *Windows Internals: User Mode*. Windows internals ; Part 1, Microsoft Press, 2017.