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 distribuirla 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-Hass**
- **NTLM Relay**
- **Overpass-The-Hass**
- **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

1.3. Organización del Proyecto

2. Aspectos Clave

2.1. Autenticación

2.2. NT Lan Managey (NTLM) y Kerberos

2.3. 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/.