|  |
| --- |
| Proyecto FCT  Vulnerabilidades Active Directory |
| Dacio Alberto Alcalde Leal Correo electrónico: daciogamers@gmail.com |



dg

## Vulnerabilidades Active Directory

### **¿Qué es Active Directory?**

Active Directory (AD) es una base de datos y un conjunto de servicios que conectan a los usuarios con los recursos de red que necesitan para realizar su trabajo.

### **¿Qué información se almacena?**

### La base de datos (o el directorio) contiene información crítica sobre su entorno, incluidos los usuarios y los equipos que hay y quién puede hacer qué. Por ejemplo, la base de datos puede contener una lista de 100 cuentas de usuario con detalles como el puesto de trabajo, el número de teléfono y la contraseña de cada persona. También registrará sus permisos.

### **¿Cuáles son los beneficios de usar Active Directory?**

### Active Directory simplifica la vida de los administradores y usuarios finales al tiempo que mejora la seguridad de las organizaciones a través de la función políticas de grupo de AD. Los usuarios pueden autenticarse una vez y luego acceder sin problemas a cualquier recurso en el dominio para el que están autorizados.

### **¿Cómo funciona Active Directory?**

### El servidor de directorio que ofrece dichos servicios en Active Directory es conocido como controlador de dominio (DC, Domain Controller). Es el encargado de autenticar y autorizar todos los usuarios y equipos de una red que implementa AD. También se encarga de responder a las peticiones de autenticación como es el inicio de sesión o logon, comprobación de permisos etc.… para ello es necesario que almacene y gestione la base de datos de usuarios y recursos de la red.

### Active Directory utiliza distintos protocolos como LDAP, DNS o DHCP, entre otros. Como protocolos de autentificación en Windows, soporta Kerberos y NLTM, siendo Kerberos el que predominante.

### Dentro de Windows los protocolos que más se utilizan son LDAP y Kerberos, LDAP se encarga de la estructura de nuestro directorio activo, y Kerberos se encargara de la autentificación y seguridad entre equipos dentro del directorio activo.

### Los equipos que por ejemplo lleven instalados Linux como SO utilizaran como método de autentificación RADIUS o LDAP.

### **¿Qué es un ataque informático?**

### Un ataque informático consiste en aprovechar alguna vulnerabilidad o debilidad que exista en el software o hardware el cual se utilizara principalmente para beneficio económico. En nuestro caso, en Active Directory vamos a “explotar” el servidor de resolución de nombres (servidor DNS).

### **¿Qué tipos de ataque son los más utilizados?**

### Los ataques que más se utilizan hoy en día son los malware (software malicioso), phishing (suplantación de identidad), Man-In-The-Middle, ataques de denegación de servicio e inyección SQL. En nuestro caso vamos a centrarnos en la denegación de servicio del servidor de resolución de nombre (DNS).

### Dentro de los ataques informáticos existen el concepto de movimiento lateral que no es más que el proceso de como un atacante de propaga desde el punto de entrada hasta el resto de la red, que es lo que vamos a intentar a hacer una vez consigamos acceso al Active Directory. También con ello podremos intentar escalar privilegios que es el hecho de que un usuario tengas más permisos de los que debería tener.

### Configuración de Active Directory

### Lo primero que deberemos hacer es cambiar de nombre nuestro equipo para así poder identificar los controladores de dominio

### Luego tendremos que darle una dirección IPv4 estática para evitar que el servidor DHCP nos dé una automáticamente.

### Ahora comenzaremos a crear el Active Directory, para ello cuando estemos agregando los roles al servidor deberemos instalar los Servicios de domino de Active Directory y el Servidor DNS

### Interfaz de usuario gráfica, Texto, Aplicación Descripción generada automáticamente

### Una vez instalado los roles debemos promocionar el servidor.

### Añadir activos a nuestro Active Directory

### Principalmente configuraremos el DNS con la dirección IPv4 del DC, seguido de esto configuraremos el nombre del equipo y lo añadiremos al dominio.

### Luego seguido de esto nos iremos al DC y añadiremos a los usuarios para que puedan autentificarse.

### Ahora debemos activar la detección de red en ambos activos tanto como para dominio, así como para todas las redes.

### **Técnicas de ataque**

### **Envenenamiento LLMNR (LLMNR Poisoning)**

### La base de estos ataques se basa en el protocolo LLMNR que es una alternativa para cuando se intenta resolver un nombre de dominio vía DNS y falla.

### Link-Local Multicast Name Resolution (LLMNR) y NetBIOS Name Service (NBT-NS) son servicios propios de dominios de Windows que actúan como alternativa para identificar activos. LLMNR se puede asociar como un DNS permitiendo una resolución de nombres.

### NBT-NS se usa para identificar los sistemas de una red por su nombre de NetBIOS

### En nuestro caso vamos a utilizar la herramienta Responder (Python 2) para falsificar el origen en la resolución de nombres, permitiéndonos responder a las peticiones LLMNR y NBT-NS como si conociéramos donde se encuentra el recurso que nos pide, envenenando así el servicio para que los activos del domino se comuniquen con nuestro equipo, recibiendo el hash NTLMv2 de autenticación el cual contiene el usuario y contraseña encriptada. Este hash lo podemos crakear de manera offline y obtener la contraseña en texto plano.

### **¿Cómo nos protegemos?**

### Como primer paso los administradores del dominio deben utilizar siempre cuentas sin privilegios para cuando no estén realizando labores administrativas, aunque la solución mas eficaz es deshabilitar los dos protocolos que hacen posible este ataque, los cuales serian los protocolos LLMNR y NBT-NS

### **Ataque SMB Relay**

### La base de este ataque se basa en el mismo concepto que el anterior (Envenenamiento LLMNR), el objetivo es conseguir las credenciales de un usuario, esto lo podemos conseguir haciendo una denegación de servicio al servidor DNS o bien porque el usuario se equivoque al introducir sus credenciales o busque un recurso que no existe.

### Por ejemplo, en nuestro caso vamos a hacerle una denegación de servicio al servidor DNS obligando a que se tenga que utilizar el protocolo LLMNR, el cual esta basado en el broadcast.

### Para explotar esta vulnerabilidad vamos a utilizar la herramienta de responder que viene por defecto en Kali.

### Lo primero que deberemos de hacer es editar el archivo **/usr/share/responder/Responder.conf** y asegurarnos que se muestre como en la imagen siguiente

### Texto Descripción generada automáticamente

### Seguido le diremos a Responder que se ponga a escuchar por nuestra interfaz de red

### **Responder -I ens33 -rv exec bash**

### Imagen que contiene Texto Descripción generada automáticamente

### Estas peticiones de broadcast son las que el script Responder se encarga de interceptar y responder.

### En nuestro caso lo que hacemos en pedirle al usuario su contraseña para que la victima nos filtre sus credenciales NTLMv2

### Pero claro una vez tenemos montado todo, ahora necesitamos algo que nos reinserta esas credenciales en la maquina víctima.

### Para ello haremos uso de Multirelay, su ruta es la siguiente **/usr/share/responder/tools/**

### Para lanzar el script usaremos la siguiente orden

### **python MultiRelay.py -t DIRECCION\_IP\_VICTIMA -u ALL**

### Pero claro primero debemos saber que maquina es la adecuada para atacar, por tanto, para ello utilizaremos la herramienta RunFinger(**/usr/share/responder/tools**), la cual consiste en buscar dentro de un segmento de red las maquinas que tengan SMB Signing desactivado, que serán las maquinas que no dispongan de medios adicionales de autenticación.

### **python RunFinger.py -I SEGMENTO\_A\_BUSCAR**

### **¿Cómo nos protegemos?**

### Una de las primeras opciones que podemos aplicar seria bloquear el acceso SMB saliente, bloqueando el puerto TCP 455 de salida a internet, y si no utilizamos el servicio SMB lo más eficaz será deshabilitarlo, también podemos deshabilitar IPv6 ya que este a la hora de resolución de nombres (DNS) tiene prioridad sobre IPv4 o también podríamos aplicar las soluciones para el caso anterior de deshabilitar los protocolos LLMNR y NBT-NS.

### Ninguna de estas medidas por si sola va a detener un ataque, pero añadir contramedidas ayudaran a evitar las amenazas.

### **GOLDEN TICKET**

### Este ataque consiste en construir nuestro propio TGT cifrados con una clave que derive de la contraseña de la cuenta KRBTGT, de modo que si se obtiene ese hash, se podrán generar tickets TGT validos en todo momento.

### Para obtener ese ticket necesitamos 4 piezas claves:

### El FQDN (Fully Qualified Domain Name) del dominio

### El SID (Security Identifier) del dominio

### El nombre de usuario de la cuenta que intentamos impersonar

### El hash de la contraseña de la cuenta KRBTGT

### Las tres primeras son relativamente sencillas de conseguir ya que con cualquier cuenta del dominio las podríamos obtener, pero el hash de la contraseña de la cuenta KRBTGT es algo mas complicado, aunque no imposible, por ello voy a citar varias formas de hacerse con ese hash:

### Robar el archivo NTDS.DIT, ya que aquí están almacenados todos los hashes de las contraseñas de los usuarios del dominio. Este archivo se puede encontrar en la siguiente ruta por defecto **C:\Windows\NTDS**

### Por tanto, cualquier persona que tuviera los hashes de las contraseñas podría dedicar el tiempo que hiciera falta para descifrarlos de manera offline sin ser detectado

### A través de un ataque DCSync, usualmente los Active Directory poseen mas de un controlador de dominio, el cual debe estar sincronizado el uno con el otro