|  |
| --- |
| Proyecto FCT  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 mas 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 ataque que mas se utilizan a día de hoy 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 mas 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.