ADVERTENCIA DE SEGURIDAD

Aseguramiento de Directorio Activo(DA)

[COLCERT AD-0604-015]

TLP:CLEAR

Las organizaciones públicas y privadas a menudo enfrentan desafíos únicos para proteger sus entornos de TI, incluyendo Microsoft Active Directory (AD). Este documento proporciona una guía para endurecer DA, abarcando desde las consideraciones generales de seguridad hasta estrategias de protección y mitigación más avanzadas.

Antecedentes de Ciberataques dirigidos al Directorio Activo:

Ataque PetitPotam NTLM Relay (2022)

El ataque PetitPotam aprovecha la vulnerabilidad en los servicios de Active Directory Certificate Services (AD CS) para obtener altos privilegios y comprometer la red.

La metodología incluye solicitar un certificado para la cuenta del controlador de dominio, capturar la respuesta NTLM y reenviarla a un servidor vulnerable para obtener un Ticket Granting Ticket (TGT), permitiendo al atacante realizar operaciones maliciosas con privilegios de dominio.

Ataque Golden Ticket (2024)

El objetivo del ataque Golden Ticket es obtener acceso total a la red sin necesidad de autenticación. Para lograrlo, el atacante crea un TGT falso con la identidad de una cuenta de dominio de alto privilegio, como la cuenta de administrador de dominio, y lo presenta a los servidores de Kerberos para acceder a cualquier recurso de la red.

Ataques a Kerberos (2024)

Dentro de los posibles ataques contra Kerberos se incluyen Replay Attack, Offline Password Cracking, Forged Tickets (Golden/Silver), Pass the Ticket, Over-pass the hash, entre otros. Es importante destacar que Kerberos tiene ciertas limitaciones, especialmente en relación con los protocolos de cifrado y sus debilidades, pero se puede mitigar mediante una implementación de seguridad adecuada.

Escenarios Propuestos para Ataques a la Seguridad de DA.

- Ataque de fuerza bruta: Un atacante automatizado intenta adivinar credenciales de usuario.
- Ataque de phishing: El atacante engaña a un usuario Ataque Pass-the-Ticket: El atacante roba un ticket de Kerberos.
- Vulnerabilidades sin parchar: El atacante aprovecha una vulnerabilidad conocida en el software AD que aún no se ha actualizado.

COLCERT

ADVERTENCIA DE SEGURIDAD

Aseguramiento de Directorio Activo(DA)

[COLCERT AD-0604-015]

TLP:CLEAR

Técnicas de Ataque analizado desde el Cyber Kill Chain (CKC)

Los actores maliciosos emplean diversas técnicas para poner en peligro los entornos de Active Directory (AD). Estas técnicas se pueden categorizar en diferentes fases de los modelos Cyber Kill Chain (CKC) y Kill Chain, los cuales describen las etapas de un ciberataque. Los atacantes pueden robar hashes NTLM o tickets Kerberos para autenticarse sin contraseñas (Pass the Hash, Pass the Ticket). También pueden obtener hashes NTLM mediante ataques de fuerza bruta o crear tickets Kerberos falsos con credenciales de alto privilegio (Kerberoasting, Golden Ticket Attack). Además, los atacantes pueden crear un controlador de dominio falso para capturar tráfico Kerberos y extraer credenciales (DCShadow Attack), enviar solicitudes de autenticación falsas para obtener hashes NTLM (AS-REP Roasting), inyectar código malicioso en consultas LDAP para ejecutar comandos (Ataque de Inyección LDAP) o explotar una vulnerabilidad en los Servicios de Certificados de AD para crear un ticket Kerberos falso (Ataque de Relevo NTLM PetitPotam). Al comprender estas técnicas, las organizaciones pueden tomar medidas para mitigar el riesgo de sufrir un ataque.

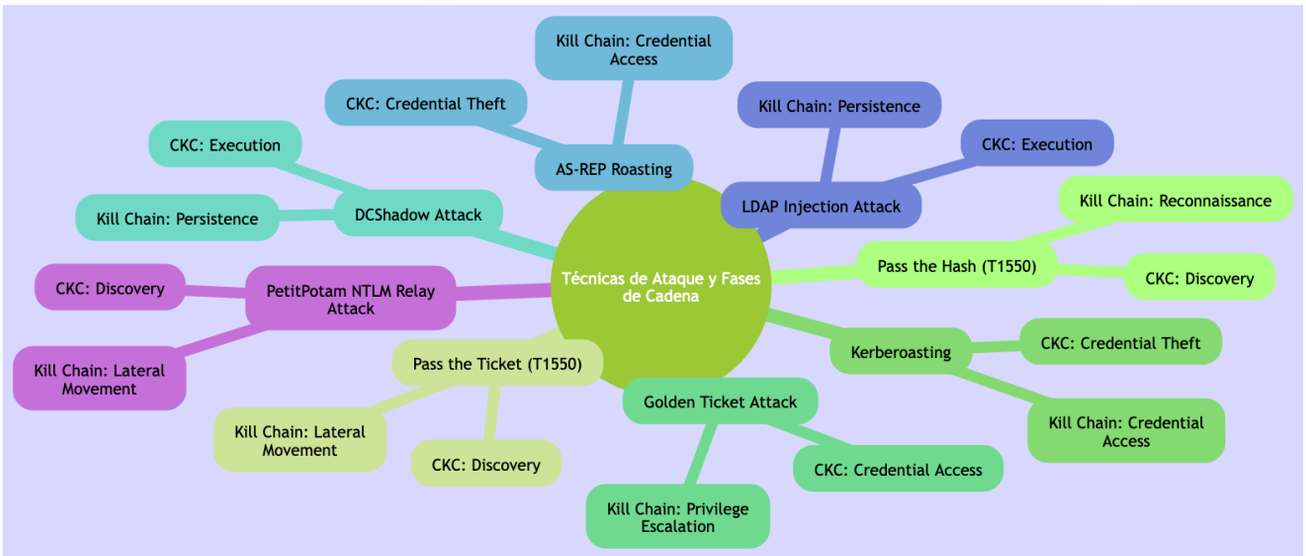

Figura 1. Elaborada por el **colCERT** para diagramar las técnicas utilizadas y la fase de Killchain explotada por el Ciberatacante.

Recomendaciones de Mitigación y Consideraciones Finales

- ❑ **Implementar la protección contra la fuerza bruta:** Bloquear automáticamente las cuentas después de un número excesivo de intentos fallidos de inicio de sesión.
- ❑ **Habilitar la protección contra la repetición de claves:** Evitar la reutilización de contraseñas comprometidas prohibiendo el uso de contraseñas anteriores.
- ❑ **Implementar la detección de anomalías:** Monitorear la actividad de la red y los sistemas AD para detectar comportamientos sospechosos que podrían indicar un ataque.
- ❑ **Segmentar su red:** Aislar los sistemas AD críticos para limitar el impacto de las intrusiones.
- ❑ **Utilizar firewalls y redes privadas virtuales (VPN):** Restringir el acceso a los sistemas AD desde redes no autorizadas.
- ❑ **Implementar soluciones de respaldo y recuperación de desastres:** Asegúrese de poder restaurar rápidamente su entorno AD en caso de un incidente de seguridad.