CBRT

Cybersecurity Blue & Red Team

USO CONTROLADO

DE PRIVILEGIOS ADMINISTRATIVOS

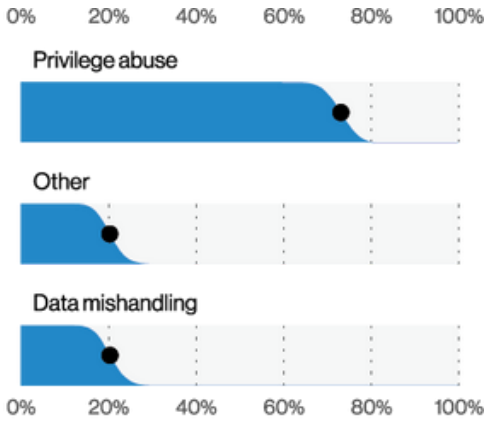
Secure today, prevent and defend everyday

(829) 878-7214

Info@cbrt.com.do

INTRODUCCIÓN

En 2021, la compañía de telecomunicaciones, Verizon, presentó un reporte de investigación sobre la filtración de datos, en el cual se observa el uso destacable del abuso de privilegios. Se registraron 256 incidentes, donde un 64% de los datos comprometidos eran de carácter personal.



Data Breach Investigations Report (2021) / Privilege Misuse. Verizon

La escalación de los privilegios administrativos es una de las principales formas en que los atacantes se propaguen dentro de las organizaciones. Estos invasores toman ventaja, conociendo diversas vulnerabilidades existentes, para luego elevar sus privilegios, alcanzando las credenciales administrativas. Esto se refiere a que la infraestructura tecnológica ha sido comprometida previamente al acceder a ella de alguna forma. El intruso que posea un control completo de un activo puede ejercer un daño serio a la compañía.

Una gestión efectiva de privilegios administrativos mejora la seguridad interna, ya que nadie está libre de ser víctima de un incidente informático.

PRINCIPALES TÉCNICAS

DE ESCALACIÓN DE PRIVILEGIOS

Tener un uso controlado de dichos privilegios nos ayudan a prevenir, observar y corregir las configuraciones en nuestra infraestructura. Existen varias técnicas o métodos para que un atacante pueda emplear privilegios no autorizados o controlados, tales como:

01. Escalación horizontal y vertical

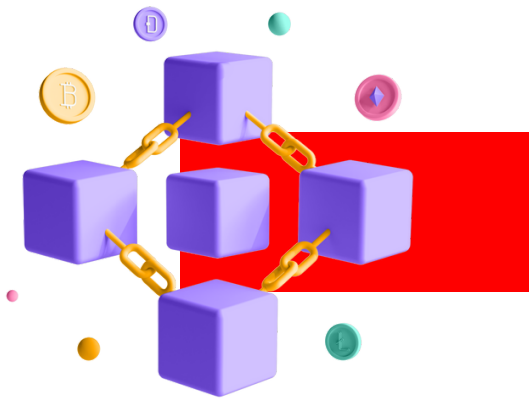
En la horizontal, el usuario no autorizado intenta acceder a los recursos, funciones y otros privilegios que pertenecen al usuario autorizado que tiene permisos de acceso similares. Mientras que en la vertical, el usuario no autorizado intenta obtener acceso a los recursos y funciones del usuario con mayores privilegios, como administradores de aplicaciones o sitios.

Privilege escalation (s.f) EC-COUNCIL CSA v1

02. Manipulación de sesión por tokens

Los adversarios pueden modificar los tokens de acceso para operar bajo un usuario diferente y eludir los controles de acceso.

Del mismo modo, estos pueden configurar los ajustes del sistema para ejecutar automáticamente un programa durante el arranque o inicio de sesión del sistema para mantener la persistencia u obtener privilegios de nivel superior en sistemas comprometidos.



MITREATT&CK CAPEC-633 (03 mayo del 2022) Manipulación de tokens de acceso.
MITREATT&CK CAPEC-633 (18 de abril de 2022) Ejecución de inicio automático de inicio de sesión o arranque.

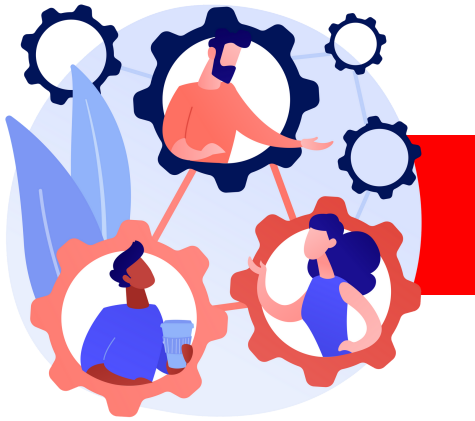
03. Secuencia de comandos de inicialización

Los scripts (secuencia de comandos) de inicialización se pueden utilizar para realizar funciones administrativas, que a menudo pueden ejecutar otros programas o enviar información a un servidor de registro interno.

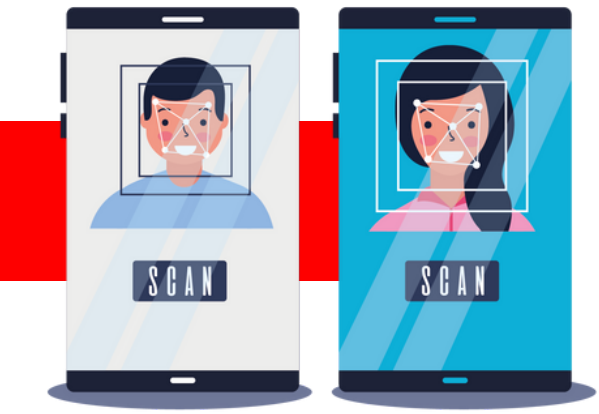
MITREATT&CK CAPEC-564 (01 de abril del 2022) script de inicialización.

04. Ingeniería social

Los adversarios pueden obtener y abusar de las credenciales de las cuentas existentes como un medio para obtener acceso inicial, persistencia, escalada de privilegios o evasión de defensa. Las credenciales comprometidas se pueden usar para omitir los controles de acceso colocados en varios recursos en sistemas dentro de la red e incluso se pueden usar para el acceso persistente a sistemas remotos y servicios disponibles externamente, como VPN, Outlook Web Access, dispositivos de red y escritorio remoto.



MITREATT&CK T1078 (19 de octubre del 2022) cuentas válidas.



05. Credential dumping

Es una técnica para obtener información de inicio de sesión y contraseña de la cuenta para el sistema operativo de la víctima. Una vez que los adversarios establecen el acceso inicial a un sistema, uno de sus principales objetivos es encontrar credenciales para acceder a otros sistemas y recursos en el entorno. Se apunta especialmente a las credenciales del sistema operativo porque estas credenciales tienen un gran valor para otras técnicas como el movimiento lateral, el descubrimiento y la recopilación.

MITREATT&CK T1003 (8 de marzo del 2022) OS Credential Dumping

RECOMENDACIONES

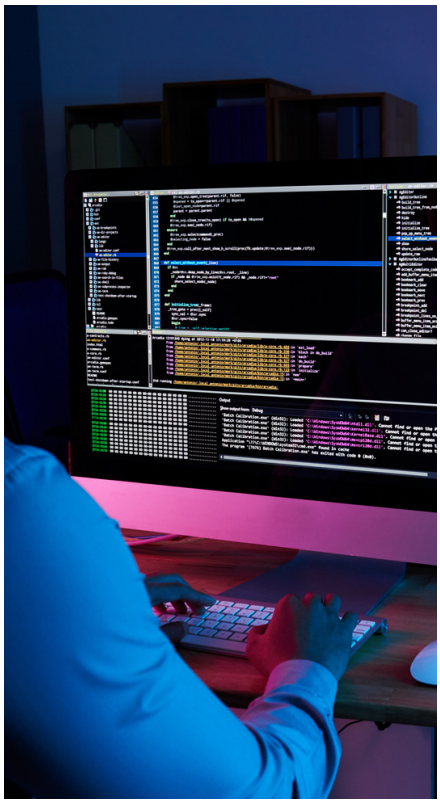
01. Escalación horizontal y vertical

- **Escanear** todos los componentes de la infraestructura de TI con el fin de encontrar vulnerabilidades que pueden ser explotadas.
- **Bloquear** los puertos de red que no se estén utilizando.
- **Mantener** las aplicaciones, los sistemas actualizados y parchados, ya que muchos ataques de escalación de privilegios se aprovechan de las vulnerabilidades del software para obtener el acceso.

02. Manipulación por tokens

- Utilizar un administrador de sesión incorporado y seguro de parte del servidor, que genere un nuevo token de sesión aleatorio después de iniciar sesión.
- El token de sesión no debe estar en la URL, se debe almacenar de forma segura e invalidarse después de los tiempos de espera de cierre de sesión o inactividad.

03. Secuencia de comandos



- **Limitar el acceso** de escritura a los scripts de inicio de sesión a administradores particular.
- **Examinar** los archivos recién creados que pueden usar scripts ejecutados automáticamente en el arranque o el inicio de sesión para establecer la persistencia.
- **Vigilar** los cambios realizados en Active Directory que logren utilizar scripts ejecutados automáticamente en la oficialización de inicio de sesión para establecer la persistencia.
- **Asegúrese** de que se establecen los permisos adecuados para las ramificaciones del registro a fin de evitar que los usuarios modifiquen las claves de los scripts de inicio de sesión que pueden provocar persistencia

04. Ingeniería social

- **Autenticación de dos factores.** La autenticación de doble factor aumenta la seguridad de la cuenta. Esto engloba la doble autenticación o la autenticación de factores, que a su vez ayuda a restringir la entrada de los atacantes que quieren saquear información confidencial.
- **Sistema tecnológico adecuado.** La activación de sistemas de obstrucción, nos ayudarán a poder percibir y bloquear los elementos maliciosos que provienen de los correos o de mensajería.

05. Credential dumping

- **Implementar** la tecnología "Credential Guard" para proteger el almacenamiento de credenciales en la memoria del proceso LSASS (Servicio del Subsistema de la Autoridad de Seguridad Local)

- **Habilitar** las reglas de reducción de superficie de ataque (ASR), esto nos ayuda a mantener a los actores maliciosos alejados y tener una postura de seguridad más madura para proteger las credenciales en memoria.

- **Capacitar y sensibilizar** a los usuarios y administradores de no utilizar las mismas contraseñas para varias cuentas.

- **Deshabilitar** la autenticación por NTLM, ya que esto facilitara a los atacantes el acceso a varias aplicaciones o dispositivos al momento de irrumpir en la infraestructura. Por consecuente, este método no permite la autenticación de factor múltiple (MFA).