La escalada de privilegios es una técnica utilizada en ciberseguridad para obtener un mayor nivel de acceso en un sistema después de haber obtenido acceso inicial con privilegios limitados. Este proceso es crucial en las pruebas de penetración y en las actividades maliciosas, ya que permite al atacante realizar acciones con mayores permisos, que de otro modo estarían restringidas.

**Tipos de Escalada de Privilegios**

**1. Escalada de Privilegios Horizontal**

* **Descripción:** Ocurre cuando un usuario con un conjunto de permisos accede a los recursos de otro usuario con un conjunto similar de permisos.
* **Ejemplo:** Un atacante con acceso a la cuenta de un empleado común logra acceder a la cuenta de otro empleado sin aumentar sus permisos.

**2. Escalada de Privilegios Vertical**

* **Descripción:** Ocurre cuando un usuario con pocos privilegios consigue aumentar sus permisos para acceder a recursos que normalmente serían inaccesibles.
* **Ejemplo:** Un atacante con acceso a una cuenta de usuario estándar logra elevar sus privilegios para obtener acceso administrativo o de root en el sistema.

**Técnicas Comunes de Escalada de Privilegios**

**1. Explotación de Vulnerabilidades del Sistema**

* **Descripción:** Utilizar vulnerabilidades conocidas en el sistema operativo o en aplicaciones para ejecutar código con privilegios más altos.
* **Ejemplo:** Explotar una vulnerabilidad en el kernel de Linux para obtener acceso root.

**2. Errores de Configuración**

* **Descripción:** Aprovechar configuraciones incorrectas que permiten a los usuarios ejecutar acciones con privilegios elevados.
* **Ejemplo:** Un servicio configurado para ejecutarse con privilegios elevados y que permite la inyección de comandos.

**3. Ingeniería Social**

* **Descripción:** Engañar a los usuarios legítimos para que revelen información sensible o realicen acciones que permitan la escalada de privilegios.
* **Ejemplo:** Phishing para obtener las credenciales de un administrador.

**4. Archivos y Directorios Inseguros**

* **Descripción:** Acceder a archivos o directorios mal configurados que contienen información sensible o permiten la ejecución de comandos con privilegios elevados.
* **Ejemplo:** Encontrar un archivo de configuración con permisos de escritura para todos los usuarios.

**5. Escalada de Privilegios en Aplicaciones Web**

* **Descripción:** Explotar vulnerabilidades en aplicaciones web para obtener un mayor nivel de acceso.
* **Ejemplo:** Inyección SQL para ejecutar comandos con privilegios administrativos en la base de datos.

**Herramientas Comunes para Escalada de Privilegios**

1. **LinPEAS:** Una herramienta de post-explotación para la escalada de privilegios en sistemas Linux.

sh

Copy code

./linpeas.sh

1. **Windows Exploit Suggester:** Identifica posibles vulnerabilidades explotables en sistemas Windows.

sh

Copy code

python windows-exploit-suggester.py --update

python windows-exploit-suggester.py --database <path-to-db> --systeminfo <path-to-systeminfo>

1. **Metasploit:** Framework que incluye múltiples exploits y módulos para la escalada de privilegios.

sh

Copy code

use post/multi/recon/local\_exploit\_suggester

set SESSION <session-id>

run

1. **BeRoot:** Herramienta de escalada de privilegios para Windows, Linux y macOS.

sh

Copy code

./beRoot.exe

**Ejemplo Práctico de Escalada de Privilegios**

**Linux**

* **Explotación de Sudo Mal Configurado:** Si sudo está configurado incorrectamente y permite que ciertos comandos se ejecuten sin contraseña, podrías usarlo para escalar privilegios.

sh

Copy code

sudo bash

**Windows**

* **Explotación de Vulnerabilidades de Servicios:** Si un servicio vulnerable está corriendo con privilegios elevados, puedes explotarlo para ejecutar comandos con esos privilegios.

sh

Copy code

net start vulnerable\_service

**Conclusión**

La escalada de privilegios es una técnica crítica en el pentesting y en los ataques reales, ya que permite al atacante expandir su control y acceso dentro del sistema objetivo. Utilizando técnicas variadas y herramientas específicas, los profesionales de la ciberseguridad pueden identificar y mitigar estos riesgos para proteger mejor sus sistemas. Si tienes más preguntas o necesitas detalles adicionales sobre alguna técnica específica, no dudes en preguntar.