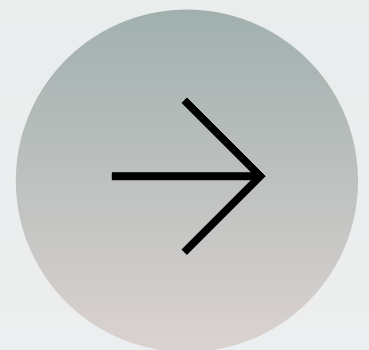
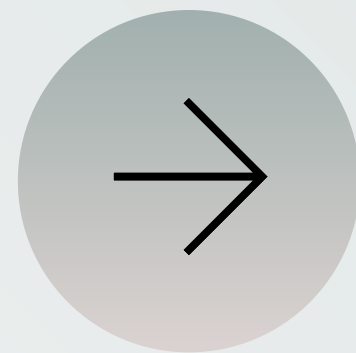


@SAULRUIZPLAZA

ROOTKIT VS BACKDOOR

DIFERENCIAS





INTRODUCCIÓN

En ciberseguridad, las amenazas evolucionan constantemente, y términos como **rootkit** y **backdoor** son claves para entender las tácticas de los atacantes. Aunque suelen confundirse, cada uno tiene un propósito distinto que impacta directamente en la seguridad de los sistemas.

¿QUÉ ES UN ROOTKIT?

Un **rootkit** es una colección de herramientas diseñadas específicamente para **proporcionar acceso privilegiado** a un sistema, permitiendo a un atacante **controlar procesos, modificar configuraciones** y, lo más importante, ocultar su presencia. Estas herramientas pueden operar a nivel del kernel, haciendo extremadamente difícil su detección.

Se usan comúnmente para **esconder malware**, como keyloggers o troyanos, y mantener la persistencia en el sistema durante largos periodos.



¿QUÉ ES UN BACKDOOR?

Es una "puerta trasera" instalada en un sistema para proporcionar **acceso remoto no autorizado**. Esta herramienta permite a los atacantes **evitar las medidas de autenticación tradicionales**, abriendo una vía directa al control del dispositivo.

A menudo, los backdoors son introducidos por desarrolladores maliciosos o mediante la explotación de vulnerabilidades. Herramientas como **NetBus**, populares a finales de los 90, permitían tomar control de sistemas remotamente, desde manejar archivos hasta activar micrófonos o cámaras.





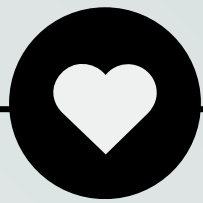
DIFFERENCIAS

	Rootkit	Backdoor
Propósito	Ocultar la presencia del atacante en el sistema, manteniendo el acceso a largo plazo.	Permitir acceso remoto al sistema, evitando los mecanismos de autenticación.
Funcionamiento	Actúa profundamente en el sistema operativo, a menudo a nivel del kernel.	Funciona como un canal de comunicación entre el atacante y el sistema comprometido.
Ejemplo	Un rootkit que oculta un keylogger para registrar contraseñas sin que el usuario lo note.	NetBus , usado para controlar computadoras remotamente , permitiendo a los atacantes acceder a archivos y recursos del sistema.

EJEMPLO PRÁCTICO

Imagina que un atacante instala **NetBus** en un ordenador de forma oculta. Gracias a este **backdoor**, puede **acceder remotamente** al sistema y, con un **rootkit** adicional, **esconder el backdoor** del usuario y de los antivirus. Esta combinación resulta en una amenaza extremadamente difícil de detectar y eliminar.





**MUCHAS
GRACIAS**

@SAULRUIZPLAZA