HACKING ÉTICO EN SISTEMAS Y REDES

TIPOS DE ROOTKITS

Servicio Nacional de Aprendizaje SENA

TIPOS DE ROOTKITS

Los virus informáticos y otros programas malignos son amenazas reales. Y los rootkits pueden ser los más peligrosos, tanto por el daño que pueden causar como por la dificultad que pueden tener para encontrarlos y eliminarlos.

Los rootkits pueden contener varias herramientas, desde programas que permiten a los hackers robar sus contraseñas hasta módulos que les facilitan el robo de su tarjeta de crédito o información bancaria en línea. Los rootkits también pueden ofrecer a los hackers la posibilidad de subvertir o desactivar el software de seguridad y rastrear las claves que usted pulsa en su palabra clave, lo que facilita a los delincuentes el robo de su información personal.

Dado que los rootkits pueden secuestrar o subvertir el software de seguridad, son especialmente difíciles de detectar, por lo que es probable que este tipo de malware pueda vivir en su equipo durante mucho tiempo causando un daño significativo. A veces, la única forma de eliminar completamente un rootkit bien escondido es borrar el sistema operativo de su ordenador y reconstruirlo desde cero.

Los escaneos de rootkit son el mejor intento de detectar una infección de rootkit, probablemente iniciada por su solución AV. El reto al que se enfrenta cuando un rootkit infecta nuestro PC es que no se puede confiar necesariamente en su sistema operativo para identificar el rootkit. Son bastante sigilosos y buenos para camuflarse. Si sospecha de un virus de rootkit, una de las mejores estrategias para detectar la infección es apagar el ordenador y ejecutar el análisis desde un sistema limpio conocido.

Los escaneos de los rootkits también buscan firmas, de forma similar a como detectan los virus. Los hackers y los desarrolladores de seguridad juegan a este juego del gato y el ratón para ver quién puede descubrir las nuevas firmas más rápidamente. Una forma segura de encontrar un rootkit es con un análisis de volcado de memoria. Siempre puedes ver las instrucciones que un rootkit está ejecutando en la memoria, y ese es un lugar que no puedes ocultar.

El análisis de comportamiento es otro de los métodos más fiables para detectar rootkits. En lugar de buscar el rootkit, se buscan comportamientos similares a los de un rootkit. O, en términos de Varonis, se aplica el Análisis de Seguridad de Datos para buscar patrones de comportamiento desviados en su red. Las exploraciones dirigidas funcionan bien si sabes que el sistema se comporta de forma extraña. El análisis de comportamiento le alertará de un rootkit antes de que un humano se dé cuenta de que uno de los servidores está siendo atacado.

TIPOS DE ROOTKITS