Herramientas de Penetration Testing en KALI LINUX

* Metasploit: Sirve para buscar y explotar vulnerabilidades en equipos.
* Burp Suite: Se buscan debilidades en webApps
* John the Ripper: Utilizado para adivinar contraseñas.

Digital Forensics

* TCPDUMP: Analiza paquetes de línea de comandos, captura tráfico de red.
* Wireshark: Tiene GUI para analizar y capturar los paquetes de red.
* Autopsy: Analiza los discos duros y smartphones.

**Más distribuciones de Linux**

Anteriormente, aprendiste sobre las diferentes distribuciones de Linux. Esto incluyó Kali Linux ™. (Kali Linux ™ es una marca comercial de OffSec.). Además de esta, hay otras distribuciones de Linux con las que los/las analistas de seguridad deberían estar familiarizados/as. En esta lectura, conocerás otras distribuciones de Linux.

**Kali Linux ™**

**Kali Linux ™** es una distribución de Linux de código abierto que se utiliza ampliamente en la industria de la seguridad. Se basa en Debian y se caracteriza por incluir de forma preinstalada muchas herramientas útiles para pruebas de penetración y análisis forense digital. Las **pruebas de penetración** consisten en ataques simulados que ayudan a identificar vulnerabilidades en sistemas, redes, sitios web, aplicaciones y procesos. Por otro lado, el **análisis forense digital** es una práctica que implica recopilar y analizar datos para determinar qué sucedió después de un ataque. Estas actividades son claves en el ámbito de la seguridad.

Sin embargo, Kali Linux ™ no es la única distribución de Linux utilizada  en ciberseguridad.

**Ubuntu**

**Ubuntu** es una distribución de código abierto y fácil de usar que goza de amplia popularidad en el ámbito de la seguridad y en otros sectores. Ofrece tanto una interfaz de línea de comandos (CLI) como una interfaz gráfica de usuario (GUI). Al ser un derivado de Debian, Ubuntu incluye de forma predeterminada aplicaciones comunes. Además, los/las usuarios/as pueden descargar un gran cantidad de aplicaciones adicionales a través de un gestor de paquetes, incluyendo herramientas especializadas en seguridad. Debido a su extenso uso, Ubuntu cuenta con una gran cantidad de recursos comunitarios para brindar apoyo a los/las usuarios/as.

Ubuntu también se utiliza ampliamente en el ámbito de la computación en la nube. Por lo tanto, a medida que las organizaciones migran hacia servidores en la nube, el trabajo en ciberseguridad puede involucrar con mayor frecuencia derivados de Ubuntu.

**Parrot**

**Parrot** es una distribución de código abierto ampliamente utilizada en el ámbito de la seguridad. Al igual que Kali Linux ™, Parrot viene con herramientas preinstaladas relacionadas con pruebas de penetración y análisis forense digital. Asimismo, como Kali Linux ™ y Ubuntu, está basada en Debian.

Una característica destacada de Parrot es su enfoque en brindar una experiencia de uso amigable. Esto se logra mediante una interfaz gráfica de usuario (GUI) intuitiva que facilita la navegación. Además, también ofrece una interfaz de línea de comandos (CLI).

**Red Hat®**

**Red Hat®** es una distribución de Linux basada en suscripción y diseñada para su uso en empresas. A diferencia de las distribuciones mencionadas anteriormente, Red Hat no es gratuita. Debido a que está diseñada y respalda para uso corporativo, también cuenta con un equipo de soporte dedicado, al que las empresas clientes pueden consultar ante incidentes.

**CentOS**

**CentOS** es una distribución de código abierto que está estrechamente relacionada con Red Hat. Utiliza el código fuente publicado por Red Hat para proporcionar una plataforma similar. Sin embargo, no ofrece el mismo soporte corporativo y se basa en el respaldo y la colaboración de la comunidad de usuarios/as para obtener apoyo.

**Conclusiones clave**

Kali Linux ™, Ubuntu, Parrot, Red Hat y CentOS son distribuciones de Linux ampliamente utilizadas en el ámbito de la seguridad. Es importante que las/los analistas de seguridad estén al tanto de estas distribuciones con las que podrían encontrarse en su carrera profesional.

Marcar como completo

Me gusta

No me gusta

Informar de un problema