Imagen que contiene Texto

Descripción generada automáticamenteCOMENTARIOS LECTURA #7

Fundamentos Avanzados Ciber Seguridad

Daniel Alejandro Olarte Ávila

Universidad Sergio Arboleda

Universidad Sergio Arboleda Cl. 74 #14-14

Bogotá, Colombia

Correo: [daniel.olarte01@correo.usa.edu.co](mailto:daniel.olarte01@correo.usa.edu.co)

Escuela de Ciencias Exactas e Ingeniería

Profesor: Juan Carlos Galindo Piraquive

29/03/2022

**“¿Qué es Kali Linux y por qué lo usan los hackers?”**

La lectura “¿Qué es Kali Linux y por qué lo usan los hackers?” me pareció muy interesante, este tema que ya llevamos viendo desde el principio del semestre me llama mucho la atención y cualquier cosa relacionada a esta me hace leer más artículos como este y seguir investigando por mi parte, lo que me parece interesante de esta lectura es el cómo resalta un montón de aspectos nuevos que normalmente la gente no conoce sobre esto, dándonos a entender lo vulnerables que somos y en la cantidad de riesgos que podemos estar sin darnos cuenta.

El artículo es interesante debido a que nos habla del Sistema Operativo de Kali Linux, en donde es esta que brinda gran cantidad de herramientas, y facilidades a la hora de ataques cibernéticos, en donde abarca todos los aspectos posibles en el mundo del Hackeo, siendo así una de las mas escogidas por los atacantes cibernéticos hoy en día para su día a día.

Me parece muy interesante como comienza esta lectura, ya que nos empieza hablando de los aspectos positivos y beneficios que tiene el uso de Kali Linux a la hora de trabajar en estos ataques, como son: La cantidad de recursos que ocupa el sistema, siendo esta una cantidad pequeña de recursos que consume, es fácil de usar para los principiantes en el tema, brindando gran habilidad en la arquitectura del software para que no hayan errores, la legalidad es otro aspecto importante para la preferencia de estos piratas cibernéticos, y la gran cantidad de herramientas que brinda para la realización de cualquier aspecto del ataque que se desea llevar acabo.

La lectura resalta siempre el aspecto más importante que tiene Kali que son la gran cantidad de herramientas que abarca para toda la funcionalidad deseada en este mundo de ataques cibernéticos, la parte entretenida es cuando mencionan pocas de las principales herramientas que contiene este super Sistema Operativo.

De las herramientas importantes que menciona este articulo están unas que ya hemos visto en clase como son:

Nmap: Es un escáner de red usado para escanear redes para sustraer información. Es un instrumento de código abierto que envía paquetes a un host para examinar su contestación y produce los detalles requeridos. Además, puede usarlo para la detección del sistema operativo, el hallazgo de hosts y el escaneo de puertos abiertos.

Burp Suite: Esta herramienta funciona como un proxy, lo cual supone que cada una de las demandas de un navegador web pasan por medio de él. Esta transmisión de demandas posibilita a los usuarios hacer cualquier cambio según con sus necesidades. Burp Suite es correcto para probar vulnerabilidades en relación con el sistema o la web. Este instrumento tiene ediciones gratuitas y de pago, y puede obtener más funcionalidades en la versión de pago que en la versión comunitaria (gratuita).

Aircrack-ng: Esta herramienta es un instrumento de craqueo, estudio y captura de hash WPA/WPA2. Es un instrumento espectacular que puedes utilizar para hackear Wi-Fi. Aircrack-ng puede capturar paquetes y leer hashes además. Además, puede descifrar hashes por medio de diversos sistemas de ataque. Este instrumento puede enfocarse de forma fácil en detectar superficies fundamentales de estabilidad Wi-Fi.

Marco Metasploit: Este Framework pertenece a los marcos de prueba de penetración más usados. Principalmente, funciona en una red local, empero además puede usarlo en el servidor host por medio del reenvío de puertos. Metasploit es un instrumento basado en escrito, empero puede bajar su paquete GUI, o sea, Armitage. Armitage convierte Metasploit en un instrumento más simple de utilizar y correcto.

Netcat: Esta herramienta se usa para la depuración de redes y pruebas de demonios. Es la mejor herramienta de red gracias a sus posibilidades y su gran lista de funcionalidades. Puede utilizar este instrumento para diferentes labores, incluida la redirección de puertos, el listado y el escaneo. Netcat además se utiliza para operar conexiones remotas, sockets de dominio UNIX, etcétera.

**Referencias:**

* <https://somoslibres.org/index.php/16-nieuws/seguridad/10977-cual-seria-la-finalidad-de-los-hackers-en-usar-kali-linux>
* <https://prezi.com/p/hd4ubywx1mp-/kali-linux/>
* <https://underc0de.org/foro/dudas-generales-121/t37078/>
* <https://www.softzone.es/noticias/open-source/kali-linux-ser-distros-queridas/>