Imagen que contiene Texto

Descripción generada automáticamenteCOMENTARIOS LECTURA #8

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

**“¿Cuáles son las fases del proceso de prueba de penetracion?”**

La lectura “¿Cuáles son las fases del proceso de prueba de penetracion?” 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, dándonos herramientas y la manera de como encontrar estas vulnerabilidades que tenemos día a dia.

El artículo es interesante debido a que nos habla de las fases que hay a la hora de las pruebas de penetraciones, viendo desde el principio las responsabilidades de los probadores de penetración, que no son mas que los que encuentran las vulnerabilidades de la seguridad. Dándonos a entender que obviamente estos probadores de vulnerabilidades deben trabajar con una gran cantidad de formas de aprovechar estas vulnerabilidades.

Me parece muy interesante la lectura, ya que nos empieza hablando de estos testings de penetración, la parte emocionante es cuando habla de las 5 fases que hay en donde se ven especificadas una por una, en donde de estas 5 son:

**RECONOCIMIENTO:**

La primera etapa de las pruebas de penetración es el reconocimiento. En esta etapa, el individuo que ejecuta la prueba recopila toda la información viable sobre el sistema objetivo. Esto incluye información acerca de la topología de la red, los sistemas operativos y las aplicaciones, las cuentas de cliente y otra información importante. El propósito es recopilar muchos datos como sea viable para que el probador logre planear un plan de ataque eficaz.

**ESCANEO:**

Una vez reunidos todos los datos importantes en la etapa de reconocimiento, es el instante de pasar al escaneo. En esta etapa, el probador usa algunas herramientas para detectar los puertos abiertos y verificar el tráfico de red en el sistema objetivo. Ya que los puertos abiertos son aspectos de ingreso potenciales para los atacantes, la finalidad de esta etapa es hallar el más grande número viable para que el probador logre aprovecharlos en la siguiente etapa.

**EVALUACION DE VULNERABILIDAD:**

La tercera etapa del proceso de pruebas de penetración es la evaluación de la vulnerabilidad. El probador examina todos los datos recopilados en las etapas de reconocimiento y investigación para detectar las probables vulnerabilidades y decidir si tienen la posibilidad de ser explotadas.

**EXPLOTACION:**

Cuando se ha reconocido una vulnerabilidad, es el instante de explotarla. El probador aspira explotar la vulnerabilidad y entrar al sistema objetivo. Esto se suele hacer usando un instrumento como Metasploit para simular ataques de todo el mundo real.

**ELABORACION DE INFORMES:**

Una vez finalizada la etapa de explotación, el probador elabora un informe que documenta todos los hallazgos de la prueba de penetración. Este informe puede utilizarse para arreglar cualquier vulnerabilidad encontrada en el sistema y mejorar la postura de estabilidad de la organización.

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).

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.

**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/>