#2

UNDERCODE

TALLER DE PENTESTING CON KALI LINUX
PARTE I

TEMAS

PENETRATION TESTING
TIPOS DE PRUEBAS
CATEGORÍAS
METODOLOGÍAS
Y MAS...!

TUTOR

SNIFER

Contenido

0.- *Pre - Boarding*

1.- Que es un *Penetration Testing*

2.- Tipos de Pruebas en un *Penetration Testing*

- Pruebas de Caja Gris- "*Gray Box" / "Partial Disclosure*"
- Pruebas de Caja Blanca - "*White Box" / "Full Disclosure*"
- Pruebas de Caja Negra - "*Black Box" / "Blind*"

3.- Categorización de un *Penetration Testing*

- Intrusión Externa
- Intrusión Interna

4.- Metodologías

- OSSTMM (*Open Source Security Testing Methodology*)
- ISSAF (*Information Systems Security Assessment Framework*)
- Penetration Testing Framework (*Vulnerability Assessment Penetration Testing Execution Standard*)
- OWASP

Pre – Boarding

Antes de iniciar con este taller, déjenme presentarme, soy Jose Moruno Cadima A.K.A Snifer, el cual andaré como “tutor” entre comillas; mas todo lo contrario, procederé a compartir el poco conocimiento que he ido adquiriendo en la vida profesional. Tengo el gusto de estar trabajando en el área de seguridad informática, por lo que continuamente voy mejorando e incorporando nuevos conocimientos.

En el Taller abordaremos todo lo relacionado a un *Pentesting*: La distribución Kali Linux (la cual fue seleccionada por la calidad y apoyo de la comunidad que lo tiene en constantes actualizaciones), conoceremos el funcionamiento de las herramientas, bajo entornos reales daremos objetivos a ser escaneados y obtención de información. Otro aspecto importante a destacar, es que habrá algunos papers con *Hacks, Tips* relacionados a *Pentesting* en los cuales se abordará alguna herramienta de Seguridad, la que no estará directamente relacionada con el contenido del Paper en curso.

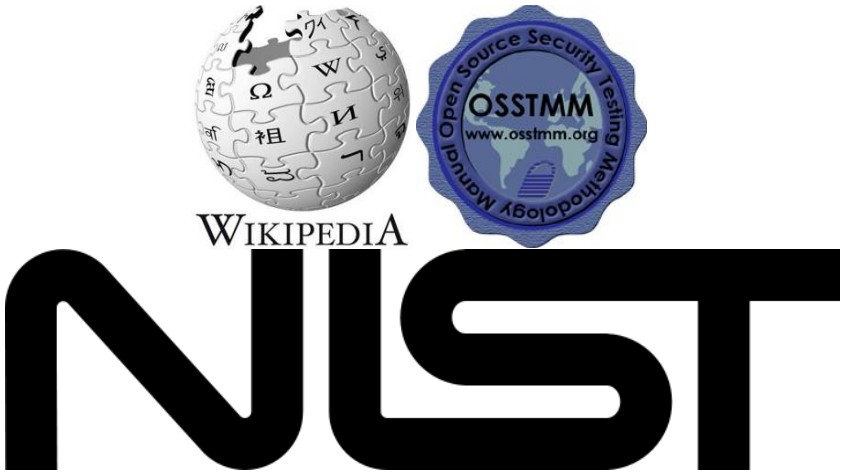
Qué es un Penetration Testing

Antes de definir lo que es un *Penetration Testing*, primero corresponde pensar como lo entendemos o lo interpretamos.

¿Qué es para ti?

"Por favor, antes de seguir, pregúntate a ti mismo ¿qué es un *Penetration Test*?"

Ahora veamos qué es lo que dicen las principales fuentes de información tomando a *Wikipedia, OSSTMM*, y *NIST* a efectos de obtener una concepción más acertada, permitiéndonos continuar el Taller con los conocimientos necesarios.



“Método para evaluar la seguridad de un sistema o red informática simulando un ataque de origen hostil” (***Wikipedia***)

“Una prueba de seguridad con un objetivo específico que termina cuando dicho objetivo se obtiene o se acaba el tiempo disponible” (***OSSTMM – Open Source Security Testing Methodology Manual***)

“Prueba de seguridad donde los evaluadores copian ataques reales para subvertir las funciones de seguridad de un aplicativo, sistema o red” (***NIST – National Institute of Standards and Technology***)

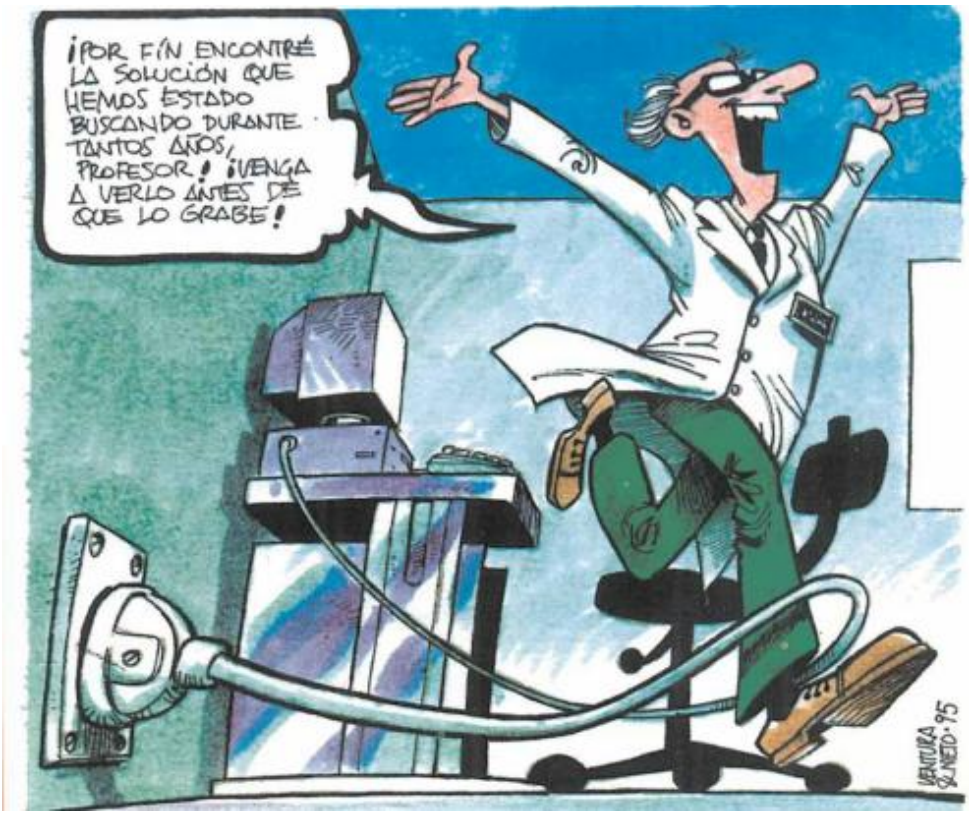
Para mí, un *Penetration Testing* , es un conjunto de técnicas que permiten evaluar el nivel de seguridad de una organización o servicio brindado.

Por lo tanto un *Penetration Testing*, permite identificar falencias tecnológicas identificando vulnerabilidades, mediante la simulación del comportamiento de intrusos. Realizar dicha prueba no certifica que un sistema es "*seguro*"; hoy puede ser seguro a las 00:00 horas pero a 00:01 ya no es seguro, porque todo está en constante actualización. Por otro lado, entra por medio el Factor Humano -que por pereza o simpleza no modifica o deja las configuraciones por defecto- aunado además, que la seguridad absoluta no existe, es solo una ilusión falsa de seguridad, por lo que es ilustrativa la siguiente analogía.

- *¿Por qué tenemos paredes en nuestras casas?*

- *¿Por qué tenemos una puerta en nuestro hogar?*

Las repuestas se resumen en que: *"Solo damos una falsa sensación de estar seguros, de que nadie podrá observarnos ni robar nuestras pertinencias; ya que si un ladrón desea ingresar a tu casa lo hará".* Con la seguridad informática ocurre lo mismo, por más que estemos totalmente seguros que nada malo va a ocurrir la Ley de Murphy se hace presente.



"Notan que en el momento menos esperado sucede una desgracia."

Actualmente, un *Penetration Testing* es considerado un recurso más inmerso en las tareas de seguridad de las empresas, ya que algunas cuentan con un área específica que se dedica totalmente a esta actividad. Un *Penetration Testing* llega a tener diferentes alcances tomando en cuenta lo que desea y la definición de lo que se hará y lo que no.

Tipos de Pruebas en un *Penetration Testing*

Al realizar una *Penetration Testing* se tiene 3 tipos de prueba las cuales son: Caja ***Negra, Blanca y Gris.*** A continuación, se especifica a mayor detalle cada una de ellas.

- ✓ **Pruebas de Caja Negra - "*Black Box*" / "*Blind*"**

  Consiste en obtener la mayor información posible debido a que no se tiene ningún conocimiento ni información previa sobre el sistema o red a ser analizado.

- ✓ **Pruebas de Caja Blanca - "*White Box*" / "*Full Disclosure*"**

Consiste en que el consultor tiene acceso a **toda** la información, es decir, infraestructura, topología de Red, Direcciones IP, código fuente de los aplicativos, etc.

- ✓ **Pruebas de Caja Gris- "*Gray Box" / "Partial Disclosure*"**

Es un término medio entre *Black* y *White (*cuya unión nos da el color gris), es una mezcla entre ambos; lo que implica que se obtiene un conocimiento parcial y, siendo este limitado no se tiene en detalle todo; definición que proviene de la contraparte, esto es, el contratante que solicita el test.

Categorización de un *Penetration Testing*

Principalmente existen dos tipos que son:

- **Intrusión Externa**
- **Intrusión Interna**

A continuación, explicaremos de forma breve en que consiste cada una:

- **Intrusión Externa**

El objetivo o finalidad de una intrusión externa es la de acceder a equipos internos de la organización, escalar privilegios y obtener acceso *root* (Administrador). Cabe resaltar que este proceso es realizado con el objetivo de acceder al DMZ (Zona Desmilitarizada) desde afuera, mediante una serie de técnicas que van desde Ingenieria Social, *Sniffing, Password Cracking;* en resumen las mejores cartas del *pentester* son sacadas a la luz.

- **Intrusión Interna**

Como su nombre lo indica, una intrusión interna es dentro la organización conectándose a un punto físico o red Wifi -si se da el caso- con el fin de demostrar que tan insegura es la infraestructura tecnológica emulando ser un atacante interno; desde luego, con los privilegios inferiores. En esta prueba, el objetivo es escalar, ver la información que está expuesta ya sea en compartidos, equipos servidores, contraseñas por defecto, mala configuración de servicios.

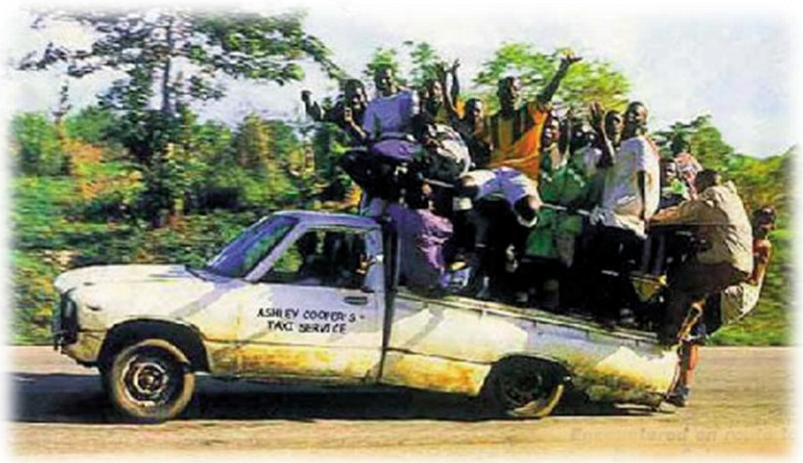
¡Hey! Alto y por qué no hablas de DoS!

Dado que lo preguntan, conviene recordar que los ataques de denegación de servicio son coordinados en la etapa interna, ya que al estar dentro de la empresa podemos ocasionar la caída de un equipo fundamental para ésta. En la etapa externa, en cambio no es necesaria la coordinación previa con nadie, debido a que cualquier persona puede ejecutar uno.

¿Pero que es un DoS o Denegación de Servicio?

Cierto, nos olvidamos de explicar qué es una denegación de servicio! Aún no es tarde para hacerlo; así, una denegación de servicio consiste en saturar un servicio con varias peticiones a la vez, siendo estas concurrentes de tal manera de sobrepasar su capacidad de concurrencia. Por ejemplo, si todos salimos de clase a la vez no podremos pasar por la puerta principal, ocasionando de esta manera una denegación de servicio, ¿cuál es el servicio? La puerta que nos brinda la opción de salir.

Una descripción gráfica de una Denegación de Servicio.



Un *Penetration Test* tiene 4 etapas principales generalmente que son:

- Reconocimiento
- Escaneo
- Enumeración
- Obtener acceso (Backdorización)

Cada una de estas etapas las iremos desglosando en las próximas entregas. En esta primera, basta con conocer y saber su existencia; rescatando que si algo se menciona y no se profundiza, es recomendable iniciar la búsqueda de información por cuenta propia. Estos talleres tienen como objetivo dar un pantallazo general y -al mismo tiempo- sean un pequeño empujón para que ustedes se animen a indagar más.

Metodologías

Al realizar un Penetration Testing -gran parte de las veces- se toma en cuenta como base Metodologías ya definidas que cumplen ciertos estándares. Asimismo, como también permiten identificar las principales falencias de la institución; a continuación, se nombran algunas y -las que según mi experiencia- considero principales o que brindan un mayor valor al momento de utilizarse.

- OSSTMM (Open Source Security Testing Methodology)
- ISSAF (Information Systems Security Assassment Framework)
- Penetration Testing Framework (Vulnerability Assessment Penetration Testing Execution Standard)
- OWASP

Desglosar cada una de ellas no tiene sentido, debido a que están debidamente documentadas en sus sitios respectivos; quizás en las próximas entregas, les dediquemos un análisis más profundo o específico.

Para terminar la primera entrega, les dejo un par de preguntas -que prefiero- sean respondidas en el foro:

1.- Prefieren realizar las pruebas en entornos reales o entornos controlables, es decir, poder usar de ejemplo algún sitio real online, o realizar la instalación de un laboratorio de pruebas y sobre él, trabajar de forma local.

2.- Sugerencias, comentarios algún punto que deseen que salga en el próximo taller como el primer bonus.