Pentesting 101® Level 1

Student Handbook

Certified by csASC CYBERSECURITY ASSOCIATION COUNCIL

Pentesting 101™ Level 1 PT101–L1

csASC CYBERSECURITY ASSOCIATION COUNCIL

Copyright and Disclaimer

Pentesting 101 Level 1| r1.2.1

Copyright

Disclaimer

Information provided about the course, modules, topics and any services for courses including simulations or handouts, are an expression of intent only and are not to be taken as a firm offer or undertaking. The Publisher reserves the right to discontinue or vary or maintain such course, modules, topics, or services at any time without notice and to impose limitations on enrolment in any course.

The course materials provided may have hypertext links to a number of other web sites as a reference to users. This service does not mean that the publisher endorses those sites or material on them in any way. The publisher is not responsible for the use of a hypertext link for which a commercial charge applies. Individual users are responsible for any charges that their use may incur.

The information in this course is written using a blend of British and American English. Although every effort has been made regarding the usage of correct spelling, punctuation, vocabulary, and grammar with regard to the Standard English, the publisher accepts no responsibility for any loss or inconvenience caused due to the regional differences in the usage of the spanish language.

Contenido

Prólogo

El **Pentesting** no solo es **fascinante** sino también **desafiante** para aquellos a los que nos apasiona. Comparable con tan pocas cosas y con exigencias personales sumamente grandes, pero increíblemente satisfactorio cuando se obtienen los resultados buscado.

El Pentesting te abrirá nuevos panoramas si eres de los que les gusta romper platos en vez de lavarlos, este es tu camino.

Lo más interesante de este manual busca no solo compartir relevantes conceptos de este mundo y la seguridad de la información sino también transmitir y contagiar esa pasión que mueve el engranaje intelectual que dará fruto a la innovación. Contagiar nuestra pasión es nuestro objetivo principal.

VISION GENERAL

Este curso de 2 días introduce a los participantes en Pentesting.

Dando seguimiento al nivel 0 donde se ven los conceptos fundamentales, en este nivel no profundizaremos en los conocimientos básicos de redes y sistemas operativos.

En el curso abordaremos todo lo relacionado a un **Penetration Testing o Pentesting** al igual se demostrará lo fácil que podemos llegar a ser vulnerables y lo importante que un **Pentester** realice dichas pruebas en los sistemas. La distribución que se utilizará en el curso será **Kali Linux** (la cual fue seleccionada por la calidad y apoyo de la comunidad la cual, lo tiene en constantes actualizaciones), otra opción podría ser **Parrot**, conoceremos el funcionamiento correcto de las herramientas, bajo entornos controlados al igual que entornos reales como estemos avanzando de nivel.

Está orientado a profesionales de informática que desean llevar a cabo pruebas de ciberseguridad en distintos entornos informáticos de forma profesional, dando un paso delante de lo que una herramienta automatizada puede generar y diferenciando falsos positivos para entregar los resultados en auditorías informáticas.

Introducción

VAMOS A CONOCERNOS

Preséntese siguiendo el siguiente formato:

- Nombre
- Compañía
- Rol y antecedentes
- Familiaridad con los conceptos Ciberseguridad y sus prácticas
- Expectativas de este curso

¿Qué es Penetration Testing?

- Un **Penetration Testing o Pentesting** es un conjunto de técnicas que permiten evaluar el nivel de seguridad de una organización o servicio brindado.
- "*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)*

www.csascouncil.org

¿Qué es Penetration Testing?

Antes de definir lo que es Penetration Testing, primero corresponde pensar como lo entendemos o interpretamos, ya que muchas personas tienen la idea, pero incompleta. En el mundo existen jefes de seguridad (socios de firmas) e individuos de altos cargos que piensan que **Penetration Testing** es **Red Team** y no pueden estar más equivocados.

¿Qué es para usted?

Antes de continuar, preguntase a usted mismo ¿Qué es Penetration Testing?

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 curso 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**)*

Definición

Penetration Testing o Pentesting 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 (Ciberdelincuentes). Realizar dicha prueba **no** certifica que un sistema es "**seguro**", hoy puede ser seguro, es decir a las 12:00 horas, pero a las 12:01 puede que ya no sea seguro, esto es debido a que todo está en constante actualización. Por otro lado, entra por medio del **factor Humano** (que por pereza o simpleza no modifica o deja las configuraciones por defecto) 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 respuestas se resumen en que: "*Solo damos una falsa sensación de estar seguros, de que nadie podrá observar ni robar nuestras pertenencias, ya que si un ladrón desea ingresar a tu casa lo hará*". Con la seguridad informática ocurre exactamente lo mismo, por más que estemos totalmente seguros de que nada malo va a ocurrir la Ley de Murphy se hace presente.

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

Actualmente, **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. Una de las ventajas del *Penetration Testing* es que llega a tener diferentes alcances tomando en cuenta lo que desea y la definición de lo que se hará y lo que no se hará.

¿Por qué es importante el Pentesting?

https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

https://cybermap.kaspersky.com/es

https://torflow.uncharted.software/

https://apt.securelist.com/

¿Por qué es tan importante el Pentesting?

El Pentesting nos ayuda a detectar las vulnerabilidades y mitigarlas antes que otras personas las detecten, exploten y abusen de ellas. Imagine que no se realizaran nunca las pruebas de penetración, sería vivir sin seguridad y todos los datos confidenciales estarían expuestos en Internet.

¿Qué tan seguro está usted?

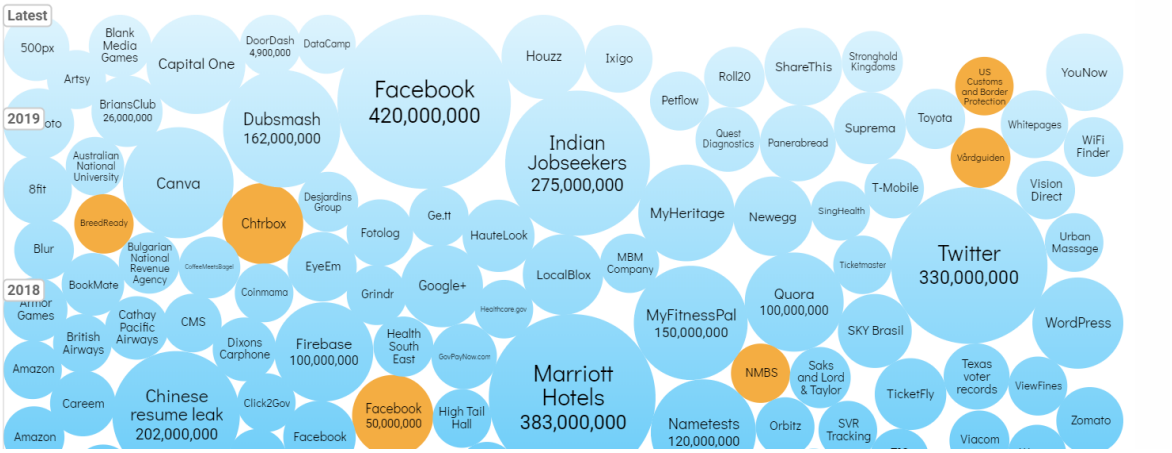
Probablemente usted esté seguro y no haya sido objetivo de un atacante, eso no excluye que lo hayan hackeado alguna vez. Los servicios que se utilizan día a día como el mail, servicios de comida, servicios de entretenimiento, entre otros, han sido y seguirán siendo objetivos de los ciberdelincuentes.

¿Cuántos servicios de estos utilizas?

Es normal que todas las personas ocupen servicios de mensajería, transporte, redes sociales, streaming, etc.

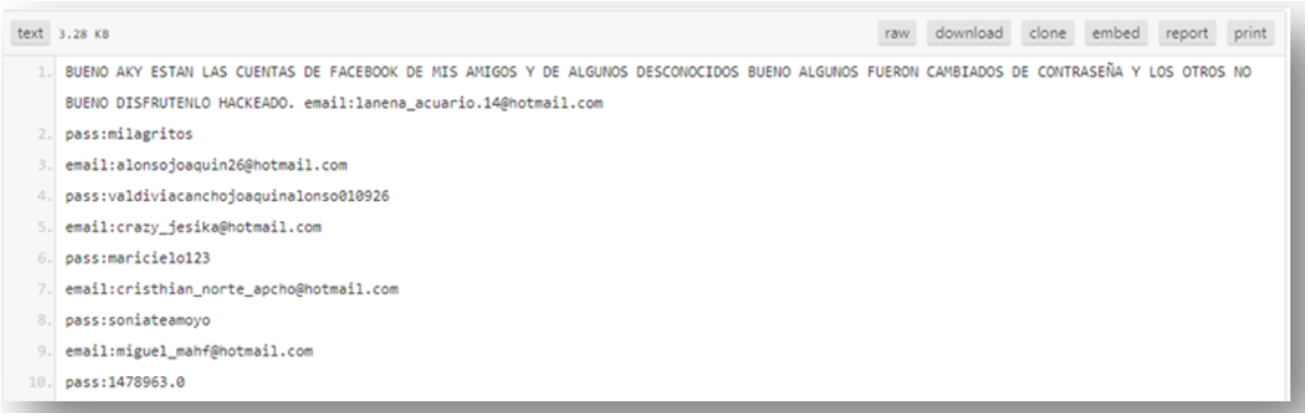
Probablemente piensas que nunca lo han hackeado directamente, pero que pasaría si lo han hackeado indirectamente con alguno de los servicios ya mencionados. En el siguiente enlace vera algunos ejemplos de algunas empresas famosas que fueron hackeadas con el paso del tiempo, esperamos que usted no esté en esos datos filtrados que robaron los ciberdelincuentes.

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/



Después de observar las bases de datos que han sido hackeadas, es cuestión de buscar en **Google** esta información, es decir los datos filtrados. Uno de los sitios donde se sube mucho de este tipo de información es:

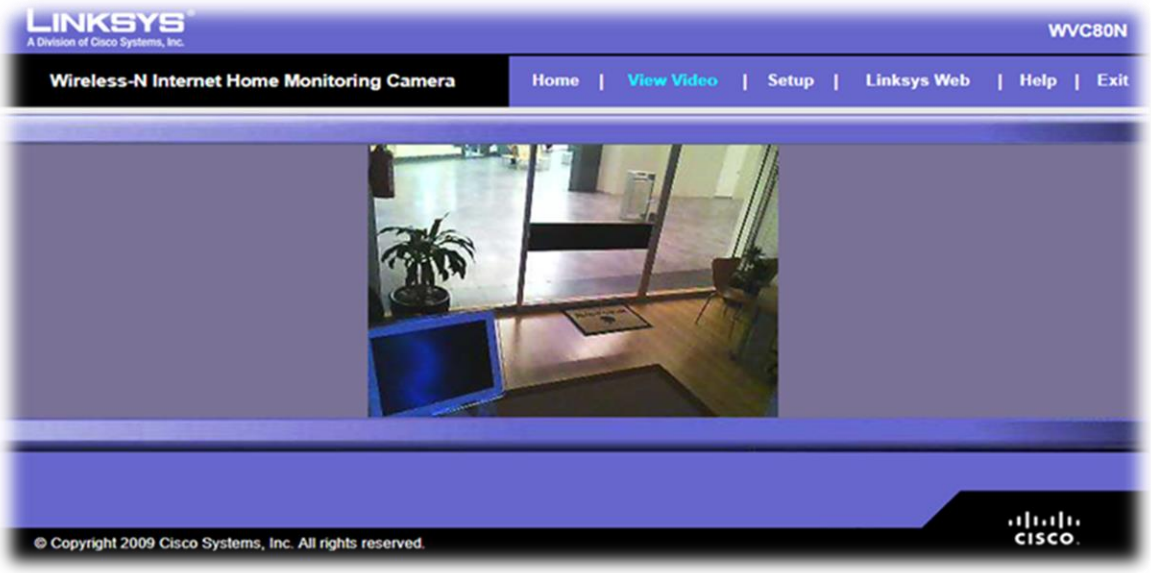
https://pastebin.com/



En la actualidad debemos de desconfiar de todo incluyendo las cámaras de video vigilancia. Algo que debemos de entender es: Si está en internet, cualquier persona en cualquier lado del mundo lo puede ver.

El siguiente ejemplo es el claro ejemplo que, sin necesidad de hacer hacking, pentesting o de romper un login podemos estar observando a casi a quien sea.

https://www.insecam.org/



Filosofía HACKER

Hacker: es la persona que posee grandes habilidades en el manejo de un tema específico; éste, usa todo este conocimiento para lograr que las cosas puedan realizar funciones para las cuales no fueron creadas.

■ **Black Hat**

■ **Grey Hat**

■ **White Hat**

Tipos de hackers / Filosofía Hacker

Hacker: Esta es una definición por parte de **CSASC**, ya que actualmente se cuentan con muchas definiciones por Internet.

Hacker: es la persona con grandes habilidades en el manejo de algún tema específico, en este caso sistemas informáticos, que usa sus conocimientos para descubrir fallos de seguridad y protegerlos de posibles ciberataques.

Una definición más global, Hacker: es la persona que posee grandes habilidades en el manejo de un tema específico; éste, usa todo este conocimiento para lograr que las cosas puedan realizar funciones para las cuales no fueron creadas.

Si bien hemos definido la palabra hacker, existen una subdivisión entre ellos que se distinguen dependiendo de sus acciones y su moral, esto son

- ***Sombrero Blanco / White Hat***
- ***Sombrero Gris / Grey Hat***
- ***Sombrero Negro / Black Hat***

A continuación, se especifica a mayor detalle cada uno de ellos.

Sombrero Blanco / White Hat

Los **White Hat Hackers** son personas con grandes conocimientos de hacking que utilizan con fines defensivos. Aprovechan dicho conocimiento para localizar vulnerabilidades e implementar contramedidas, estos hackers no hacen nada que no esté definido en un contrato y no usan su conocimiento para quebrantar la ley, se pueden denominar como **"Ethical Hackers"**

Sombrero Gris / Grey Hat

Los **Grey Hat Hackers** son personas con grandes conocimientos que trabajan por momentos de manera ofensiva y/o defensiva dependiendo de la circunstancia. Esta categoría plantea una línea divisora entre **"Ethical Hacker"** y un **"Ciberdelincuente"**

Sombrero Negro / Black Hat

Los **Black Hat Hackers** son personas con grandes conocimientos que están del lado opuesto de la ley y la moral. Realizan actividades maliciosas y/o destructivas, utilizan todo su conocimiento para su propio beneficio sin importar los daños colaterales y son denominados "**Ciberdelincuentes**".

Tipos de Pruebas en un Penetration Testing

Al realizar un **Penetration Testing** existen 3 tipos de pruebas:

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

A continuación, se especifica a mayor detalle cada una de ellas.