Pentesting 101
Ethical Hacker lvl 1

CSASC

CYBERSECURITY ASSOCIATION COUNCIL

Copyright and Disclaimer

Pentesting 101 Ethical Hacker Level 1| r1.0.0

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

En la actualidad todo nuestro mundo, rutinas y trabajo giran alrededor del Internet, la tecnología cada vez se torna más fascinante, útil y poderosa, aunque muchas veces la seguridad no es una de las virtudes fuertes. Es aquí donde se presenta el reto para los futuros profesionistas en el área de la ciberseguridad, un mundo tan amplio y con distintos retos que cada día es igual o más desafiante que el anterior.

La ciberseguridad es comparable con tan pocas cosas que incluso puede ser considera como un arte; introduce a las personas a la carrera del aprendizaje continuo y constantemente presenta nuevos retos que es increíblemente satisfactorio cuando se obtienen los resultados deseados.

Este manual busca compartir relevantes conceptos de la ciberseguridad y la seguridad de la información mediante esa pasión con la cual fue diseñado, para así lograr transmitir el conocimiento y dar pie a un mundo más seguro.

Contagiar nuestra pasión es nuestro objetivo principal.

Visión General

Este curso de 2 días introduce a los participantes en las **Pruebas de Intrusión** (también conocidas como ***Penetration Testing*** o ***Pentesting*** en inglés) y abordará todos los conceptos necesarios para comprender esta rama de la ciberseguridad y la importancia de que un ***Pentester*** realice dichas pruebas en los sistemas.

La distribución que se utilizará en el curso será Kali Linux con la cual se va a mostrar el funcionamiento correcto de sus herramientas bajo entornos controlados al igual que entornos reales conforme se avance de nivel.

Este contenido está destinado a profesionales que desean realizar pruebas de seguridad de manera profesional en una variedad de entornos informáticos, dando un paso delante de lo que una herramienta automatizada puede generar y distinguir entre falsos positivos para garantizar resultados confiables y correctos en las auditorías informáticas.

Introducción

Vamos a conocernos

Para CSASC es un honor contar con su presencia en este curso enfocado a la ciberseguridad. A lo largo del trayecto de tu aprendizaje con nosotros es fundamental conocer un poco de ti para hacer las cosas más amenas y entendibles, para lograr eso por favor preséntese siguiendo el siguiente formato:

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

Pentesting 101 Ethical Hacker lvl 1

¿Qué son las Pruebas de Intrusión?

- Las pruebas de Intrusión son una práctica de seguridad que consta de un conjunto de técnicas que permiten evaluar el nivel de seguridad tecnológico 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)*

CYBERSECURITY ASSOCIATION COUNCIL
Pentesting 101Ethical Hacker Level 1® is a registered trademark of CSASC Limited.

¿Qué son las Pruebas de Intrusión?

Antes de definir lo que son las Pruebas de Intrusión (**Pentesting** o **Pentest** también puede ser utilizado de aquí en adelante), primero debe pensar en su propia interpretación, ya que muchas personas tienen la idea, pero incompleta.

¿Qué son para usted las Pruebas de Intrusión?

Antes de continuar, responda con honestidad lo que para usted significa el Pentesting.

Para tener una idea más precisa del concepto basta tomar como referencia a las principales fuentes de ciberseguridad como **Wikipedia**, **OSSTMM, ENISA** y **NIST** con la finalidad de obtener una concepción más acertada. En seguida se muestran sus definiciones.

*"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**).*

*"Es la evaluación de la seguridad de un sistema frente a diferentes tipos de ataques realizados por un experto en seguridad autorizado. El experto intentará identificar y explotar las vulnerabilidades del sistema." (**ENISA – The European Union Agency for Cybersecurity**)*

*"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

Para CSASC las Pruebas de Intrusión son definidas de la siguiente manera:

"Las pruebas de Intrusión son una práctica de seguridad que consta de un conjunto de técnicas que permiten evaluar el nivel de seguridad de una organización o servicio brindado."

Por tanto, las pruebas de intrusión permiten identificar errores tecnológicos y humanos mediante la simulación del comportamiento de los intrusos (ciberdelincuentes o usuarios malintencionados) para identificar vulnerabilidades. Realizar dicha prueba **no** certifica que un sistema sea "**seguro**", hoy puede estar seguro, es decir a las 00:00 horas, pero a las 00:01 puede que ya no lo sea, porque en el mundo de la tecnología todo está en constante actualización y a una velocidad impresionante. También, entra por medio el **factor Humano** que por pereza, simpleza o mero desconocimiento no modifica o deja las configuraciones por defecto en los sistemas (entre otras malas prácticas). De esta forma, se puede deducir que **la seguridad absoluta no existe, es solo una falsa ilusión de seguridad.** Las siguientes preguntas ilustran mejor esta sección.

- ¿Por qué ponemos seguros a nuestros carros al subirnos o al bajarnos?

- ¿Por qué cerramos las puertas con llave en nuestro hogar?

-¿Por qué colocamos cámaras de seguridad en las casas, oficinas e inclusive carros?

Las respuestas se pueden resumir en: "*Solo creamos una falsa sensación de certeza de que nadie puede observar ni robar nuestros bienes, porque si un ladrón quiere robarnos, lo hará*". Lo mismo ocurre con la seguridad informática, aunque estemos absolutamente seguros de que no pasará nada malo, la Ley de Murphy sigue existiendo.

En el momento menos esperado puede suceder una desgracia.

En la actualidad, la seguridad de la información es una preocupación creciente para muchas organizaciones y empresas en todo el mundo. Por esta razón el pentesting se considera un recurso valioso integrado en las misiones de seguridad de las empresas (algunas incluso tienen espacios específicos completos dedicados por completo a esta actividad).

Pentesting 101 Ethical Hacker lvl 1

¿Por qué es importante el Pentesting?

Las Pruebas de Intrusión son una herramienta esencial para mejorar la seguridad informática y proteger la información confidencial. Algunas de las razones por la cuál es de suma importancia se enlistan a continuación:

- Identificar vulnerabilidades
- Protección de datos
- Cumplimiento normativo
- Reducción de riesgos

CYBERSECURITY ASSOCIATION COUNCIL
Pentesting 101Ethical Hacker Level 1® is a registered trademark of CSASC Limited.

¿Por qué son tan importantes las Pruebas de Intrusión?

Las Pruebas de Intrusión son una herramienta esencial para mejorar la seguridad informática y proteger la información confidencial. Algunas de las razones por la cuál es de suma importancia se enumeran a continuación:

1. **Identificar vulnerabilidades**: el pentesting es una herramienta importante para identificar las vulnerabilidades de seguridad en los sistemas informáticos. A través de la simulación de ataques reales, los pentesters pueden identificar las debilidades de los sistemas y aplicaciones, y recomendar soluciones para corregirlos.
2. **Protección de datos**: los pentesters pueden ayudar a proteger la información confidencial y los datos sensibles de las organizaciones. Al identificar y corregir las vulnerabilidades en los sistemas, los pentesters pueden evitar que los atacantes malintencionados accedan a datos importantes y causen daños.
3. **Cumplimiento normativo**: muchas organizaciones están sujetas a leyes y regulaciones que les exigen tener medidas de seguridad informática adecuadas en su lugar. El pentesting es una herramienta esencial para asegurarse de que las organizaciones estén en cumplimiento con estas normativas.
4. **Reducción de riesgos**: el pentesting ayuda a reducir los riesgos de seguridad informática al detectar y corregir las vulnerabilidades antes de que puedan ser explotadas por los atacantes malintencionados. Esto puede ayudar a prevenir los costos y las consecuencias graves de un ataque informático, como la pérdida de datos, la interrupción del negocio y pérdidas reputacionales.

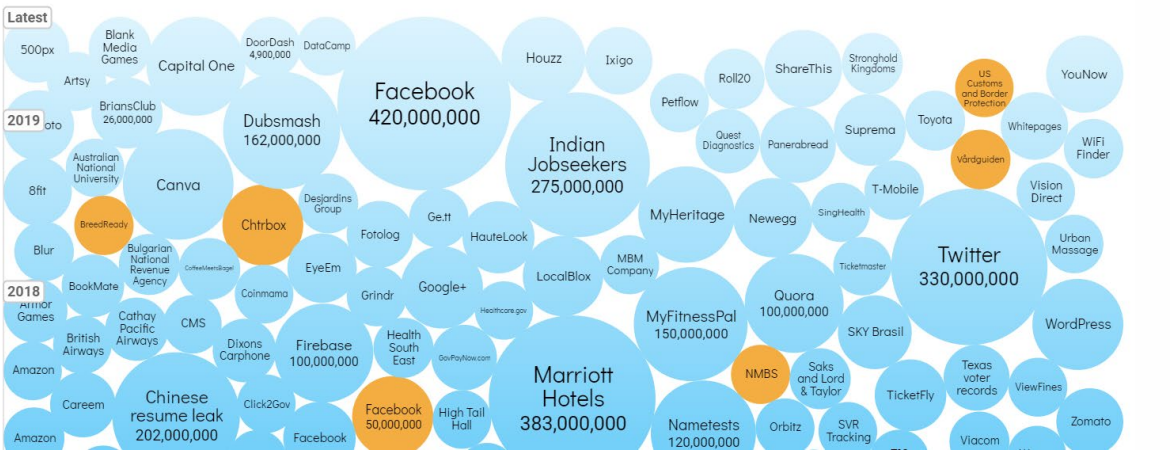
¿Qué tan seguro está usted?

Probablemente usted se encuentre a salvo y no sea el objetivo de un ciberdelincuente, aunque eso no excluye que su información este intacta. Los servicios que utiliza día a día como el correo, servicios de entretenimiento, plataformas *e*-commerce, entre otros han sido y seguirán siendo objetivos de los ciberdelincuentes. Es difícil estar seguro si su información ha sido comprometida, ya que a menudo no se sabe hasta que se produce algún tipo de daño o fraude.

¿Cuántos servicios de estos utilizas en tu día?

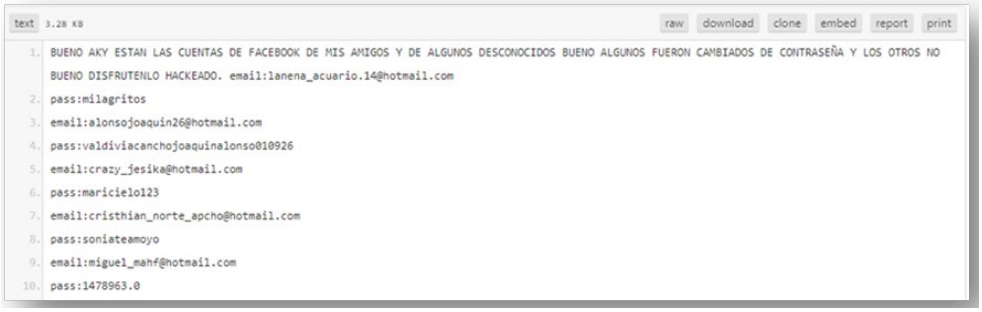
Es normal que todas las personas ocupen servicios de mensajería, transporte, redes sociales, *streaming*, etc. Probablemente piense que nunca lo han hackeado, pero que pasaría si ya lo han hackeado indirectamente con alguno de los servicios ya mencionados. En el siguiente enlace verá algunos ejemplos de algunas empresas nacionales y multinacionales conocidas que se han visto comprometidas en el transcurso del tiempo.

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



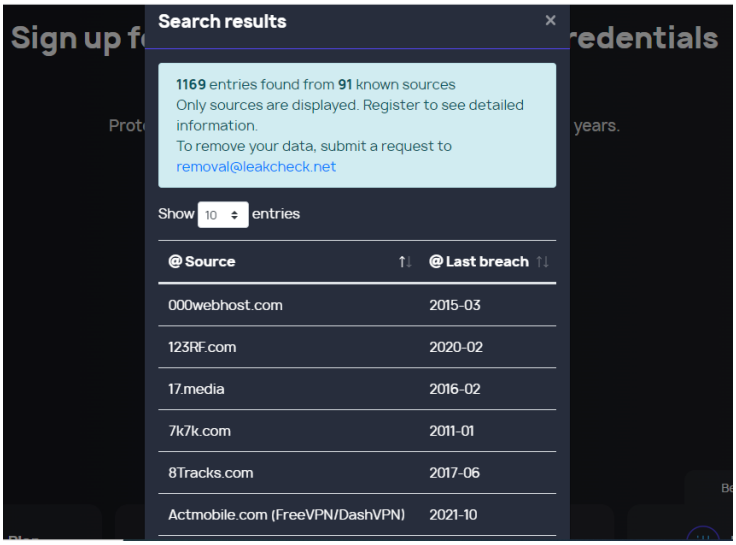
Después de observar las empresas que han sido comprometidas es cuestión de buscar esta información. Algunos de los sitios donde puede encontrar este tipo de datos o ver si su información se ha visto comprometida son:

- https://pastebin.com/



- https://breachdirectory.org/index.html

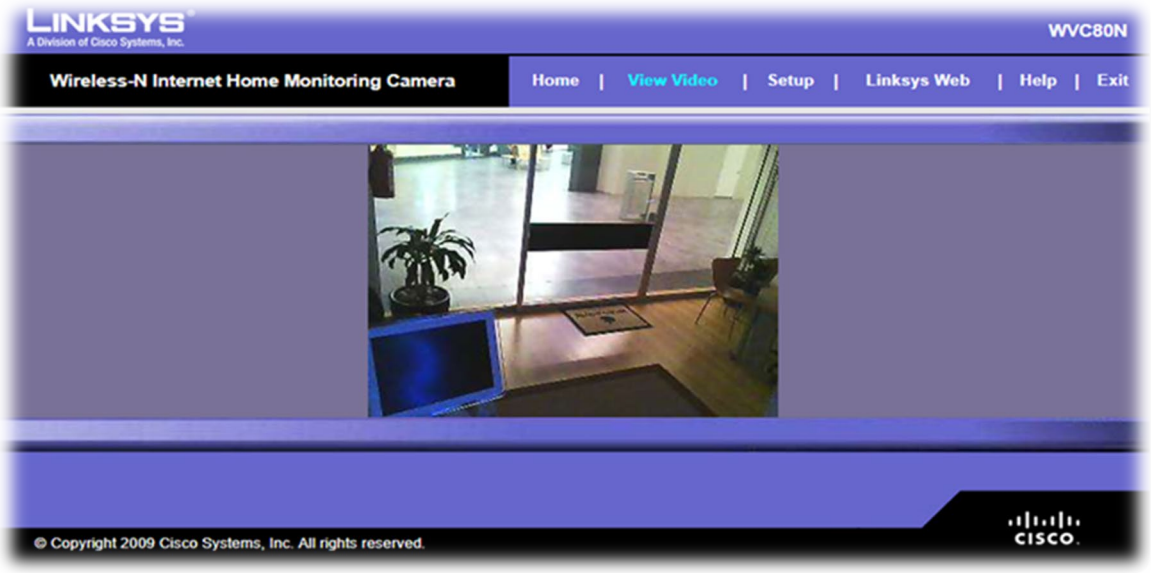
- https://leakcheck.net/



En la actualidad es mejor estar prevenidos y no confiar en todo, incluyendo las cámaras de videovigilancia. Una cosa es esencial de entender: Todo lo que está en Internet puede ser accedido desde cualquier parte del mundo.

El siguiente ejemplo es el claro ejemplo que, sin necesidad de hacer hacking, pentesting o de comprometer un sistema es posible observar personas en tiempo real.

- https://www.insecam.org/



Pentesting 101 Ethical Hacker lvl 1

Filosofía HACKER

Hacker: Es la persona con grandes habilidades en el manejo de algún tema específico, en este caso sistemas informáticos, que usa sus conocimientos para explorar, experimentar y mejorar la seguridad y el funcionamiento de los sistemas.

■ **Black Hat**

■ **Grey Hat**

■ **White Hat**

Filosofía Hacker

Actualmente existen muchas definiciones dependiendo del material de estudio y si bien todas se encuentran relacionadas, la siguiente es dada por parte de **csAsc y** está enfocada a la ciberseguridad.

Hacker: "Es la persona con grandes habilidades en el manejo de algún tema específico, en este caso sistemas informáticos, que usa sus conocimientos para explorar, experimentar y mejorar la seguridad y el funcionamiento de los sistemas."

Una definición más global, sería: "Es la persona que posee grandes habilidades en el manejo de un tema específico y utiliza todo ese conocimiento para hacer que las cosas realicen funciones para las que no fueron creadas."

El término "hacker" a menudo se asocia erróneamente con actividades ilegales o malintencionadas, pero es importante tener en cuenta que hay muchos hackers que trabajan de manera ética y legal para mejorar la seguridad informática. Esto permite crear una subdivisión entre ellos que se distinguen dependiendo de sus acciones y su moral, estas 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 **hackers de sombrero blanco** son hackers éticos que utilizan sus habilidades para encontrar vulnerabilidades y debilidades en los sistemas informáticos, redes y aplicaciones de una organización con el objetivo de mejorar su seguridad. Estos hackers no hacen nada que no esté definido en un contrato y siempre actúan bajo el margen de la ley.

Sombrero Gris / Grey Hat

Los **hackers de sombrero gris** 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 ***un hacker ético*** y un **ciberdelincuente** ya que no tienen intenciones maliciosas, pero tampoco trabajan siempre de manera legal o ética. Por lo general, los gray hat hackers se dedican a encontrar vulnerabilidades en los sistemas de las organizaciones, y en ocasiones comparten esa información con los propietarios de los sistemas, con el objetivo de ayudar a mejorar la seguridad.

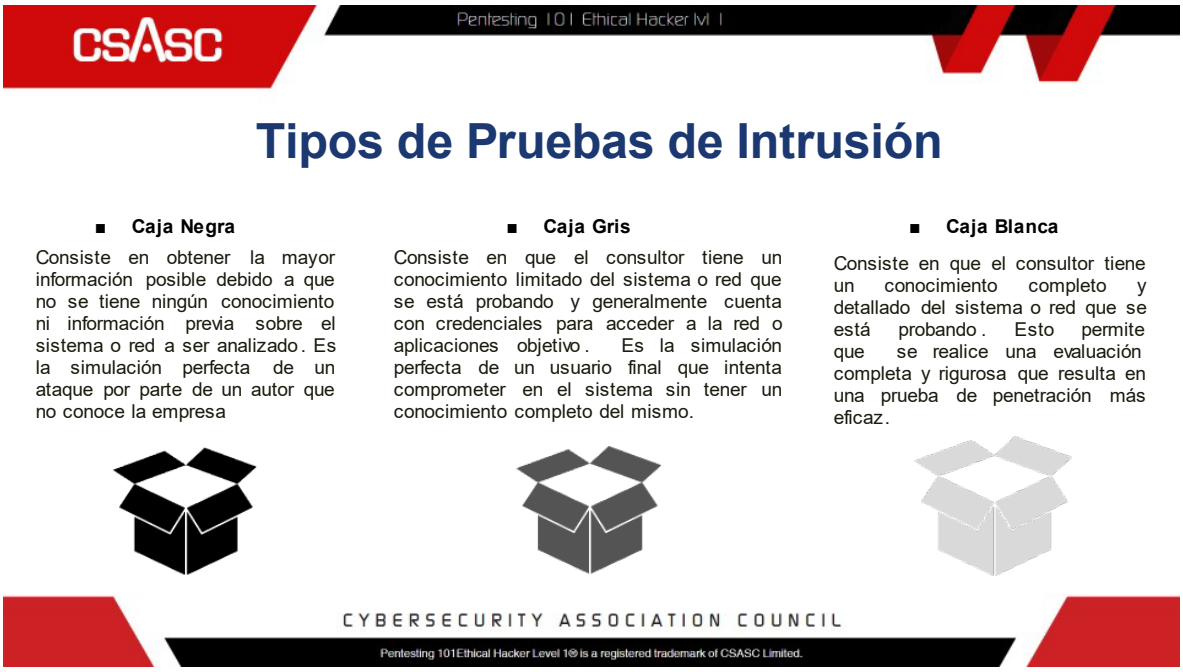
Sombrero Negro / Black Hat

Los **hackers de sombrero negro** son personas con grandes conocimientos que están del lado opuesto de la ley y la moral. Realizan una variedad de actividades maliciosas, como robo de datos, espionaje corporativo, ataques de denegación de servicio (DDoS), phishing, ransomware y otros ataques. A menudo buscan obtener acceso no autorizado a sistemas y redes, con el objetivo de obtener información confidencial o causar daños a la organización o a los usuarios también son denominados como **ciberdelincuentes**.



En la literatura también es posible encontrar otras clasificaciones de personas en ciberseguridad que se basan en función de sus motivaciones y objetivos. Algunas de estas clasificaciones son:

- Hackers éticos
- Hackers maliciosos
- Hacktivistas
- Crackers
- Lamers
- Script Kiddies



Tipos de Pruebas de Intrusión

Al realizar pruebas de penetración, se pueden **clasificar** 3 tipos diferentes de pruebas en función de**l conocimiento previo que tiene** que el pentester, qué esperar de la prueba y la legitimidad de la **misma**. Algunos de estos escenarios **primero** pondrán a prueba la habilidad del pentester más que la seguridad del objetivo. Cada uno de ellos se detalla a continuación.

Pruebas de Caja Negra - “Black Box” / “Blind Black”

En este tipo de prueba de penetración, el equipo de seguridad no tiene ningún conocimiento previo del sistema o red que se está probando. El equipo de seguridad realiza la evaluación de la misma manera que un atacante externo, sin tener acceso a detalles de la arquitectura, el código fuente o la documentación. Esto permite que el equipo de seguridad evalúe la resistencia del sistema o red a los ataques externos. Es la simulación perfecta de un ataque por parte de un autor que no conoce la empresa.

Pruebas de Caja Blanca - “White Box” / “Full Disclosure”

En este tipo de prueba de penetración, el equipo de seguridad tiene un conocimiento completo y detallado del sistema o red que se está probando. El equipo tiene acceso a los detalles de la arquitectura, el código fuente, la documentación y otra información relevante del sistema o red que se está evaluando. Esto permite que el equipo de seguridad realice una evaluación más completa y rigurosa del sistema o red, lo que resulta en una prueba de penetración más eficaz. Es la simulación perfecta de un ataque interno que cuenta con permisos de administración y conocimiento total de la aplicación o servicio.

Pruebas de Caja Gris- “Gray Box” / “Partial Disclosure”

En este tipo de prueba de penetración, el equipo de seguridad tiene un conocimiento limitado del sistema o red que se está probando. El equipo de seguridad tiene acceso a algunos detalles de la arquitectura, el código fuente y la documentación, pero no tiene un conocimiento completo del sistema o red que se está evaluando. Es la simulación perfecta de un usuario final que intenta comprometer en el sistema sin tener un conocimiento completo del mismo.

Cabe destacar que dependiendo de la metodología o framework implementado estos enfoques pueden tener otros nombres o estar aún más refinados. Por ejemplo, la metodología **OSSTMM** define seis tipos distintos de pruebas:

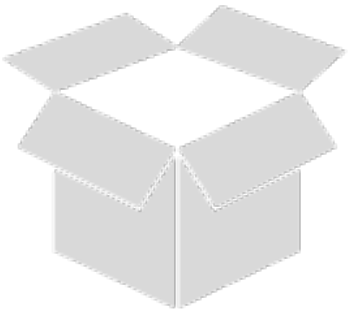
Clasificación	Descripción
Blind	En este tipo de prueba el pentester ataca al objetivo sin conocimiento previo de las defensas y activos, por lo que se prueba principalmente las habilidades del auditor. Por su parte el objetivo se prepara para la auditoría, conociendo de antemano todos los detalles. La amplitud y profundidad de este tipo de prueba solo puede ser dado conforme el conocimiento del pentester. En COMSEC y SPECSEC, esto a menudo se denomina Hacking Ético y en la clase PHYSSEC, generalmente se escribe como War Gaming.
Double Blind	En este tipo de prueba el pentester ataca al objetivo sin conocimiento previo de las defensas y activos, por lo que se prueba principalmente las habilidades del auditor. Por su parte no se notifica al objetivo el alcance de la auditoría. Este tipo de auditorías pone a prueba las habilidades del pentester y la preparación del objetivo ante posibles ataques. También se le conoce como prueba de caja negra.
Gray Box	En este escenario el pentester tiene un conocimiento previo del entorno del sistema a auditar y por su parte los sistemas de información auditados están preparados y advertidos de las actividades que se van a realizar. En la fase inicial de esta auditoría se intercambia información entre el auditado y el pentester sobre las características técnicas del sistema. El objetivo es comprobar el funcionamiento y la eficiencia de los controles implantados ante una situación lo más cercana posible a un caso de ataque externo hacia la organización.
Double Gray Box	También conocidas como caja blanca, el pentester tiene conocimiento previo del sistema de información que va a analizar mientras que el auditado conoce cuándo se va a realizar la auditoría, pero no de las técnicas que se van a utilizar. En la

	fase inicial de esta auditoría se intercambiará información entre el pentester y el auditor sobre las características técnicas, etc. El objetivo es conocer tanto las habilidades del pentester y la eficacia de los controles implantados como la de los controles de detección del sistema analizado.
Tandem	También conocida como "Crystal box", son aquellas en las que tanto el pentester como el auditado tienen toda la información acerca de la infraestuctura a analizar y parte de las pruebas se realizan conjuntamente o coordinadas entre ellos. El objetivo es hacer una evaluación intensiva de los controles de seguridad, teniendo en cuenta que los controles de detección y los procesos de gestión de evidencias no se evaluarán completamente.
Reversal	En este escenario la organización auditada no tiene conocimiento del desarrollo de las pruebas (por lo menos a nivel operativo), en cambio el pentester tiene toda la información que la organización a evaluar le haya proporcionado. El objetivo es comprobar qué tan bien está preparada la organización a la hora de gestionar las incidencias de seguridad que puedan surgir.

Caja Negra

Caja Gris

Caja Blanca



Pentesting 101 Ethical Hacker lvl 1

CYBERSECURITY ASSOCIATION COUNCIL

CYBERSECURITY ASSOCIATION COUNCIL

Pentesting 101Ethical Hacker Level 1® is a registered trademark of CSASC Limited.

Notas:

csAsc

2023

csAsc

CYBERSECURITY ASSOCIATION COUNCIL

contacto@csascouncil.com

CSASC es una organización formada por los hackers éticos más relevantes del mundo, con más de 15 años de experiencia.
Surge la necesidad de crear un órgano que certifique de manera universal los conocimientos y habilidades en ciberseguridad, ayudando a las empresas a certificar sus profesionales encargados de explotar las vulnerabilidades, en búsqueda de fortalecer sus lineas de defensa.

Torre de Cristal, Paseo de la Castellana 259C, Planta 18, 28046 Madrid, España