Presentación profesional de cierre de Bootcamp

Introducción

Llegamos a la fase final de este Bootcamp. Te felicitamos por el gran esfuerzo y dedicación que has demostrado. Esperamos que haya sido de utilidad y que te sirva como base para el camino que quieres desarrollar como especialista en ciberseguridad.

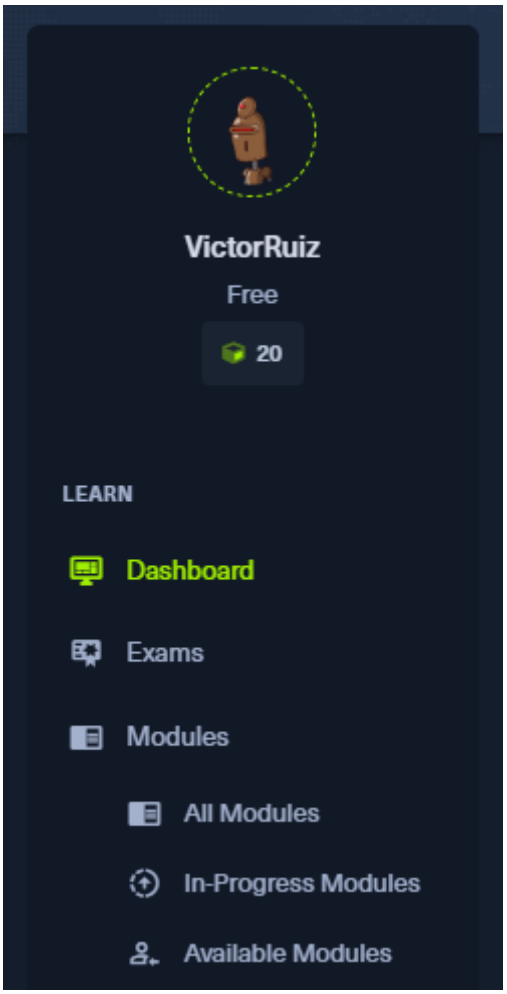
Para cerrar este Bootcamp te presentaremos el proyecto final, que servirá para evaluar tus conocimientos y destrezas. Consiste en resolver el módulo **Using the Metasploit framework** de HTB Academy.

Para esto, como primer paso, debes:

1. Abrir una cuenta gratuita en HackTheBox, en la sección Academy. Para ello, entra a la siguiente página: https://academy.hackthebox.com/

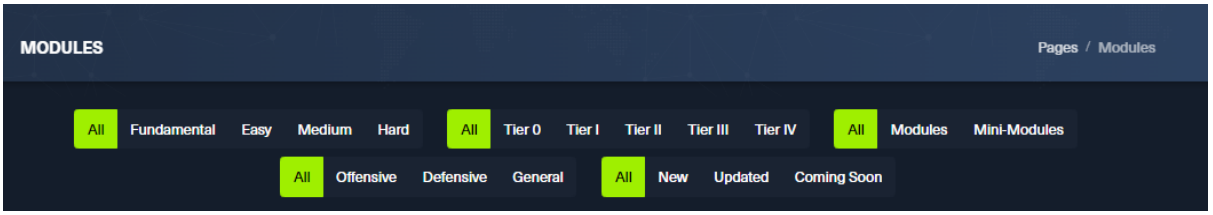
2. Una vez que tengas tu cuenta, ve al **Dashboard**:

3. En la columna izquierda, dirígete hacia **Modules** y luego a **All Modules**:

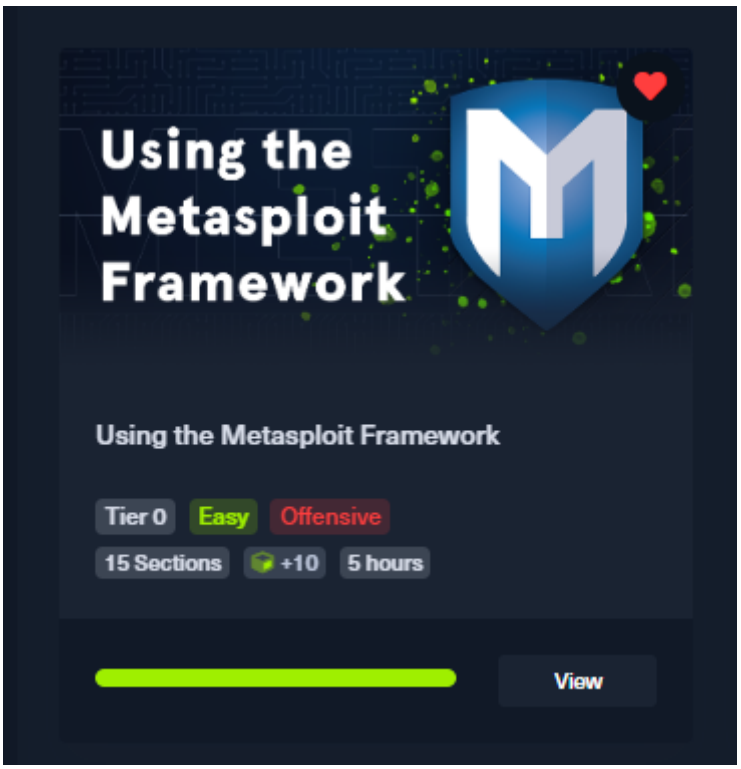


4. Ahí selecciona el botón **Tier 0**:

Nota: Con el acceso gratuito tienes 30 cubos, los cuales te sirven para ingresar a los módulos. El módulo que utilizaremos solo pide 10 cubos, por lo cual alcanza perfectamente (no necesitas comprar cubos para esta actividad).



5. Busca y da **Unlock** al módulo **Using the Metasploit Framework**:



6. Inicia la lectura de los contenidos.

Objetivos

- Resolver un reto que te implique el uso de distintas metodologías y herramientas que has usado a lo largo del bootcamp, principalmente, Metasploit.
- Elaborar un reporte (perfeccionando las secciones de metodología y teoría que has implementado en módulos anteriores) en el que colocarás

todo lo que se te solicitó en el reto de HTB, con sus respectivas respuestas.

- Elaborar una presentación ejecutiva que muestre de manera clara y sintetizada los hallazgos obtenidos en el reto realizado y tu perfil de carrera. El propósito de esta actividad es que puedas recibir una retroalimentación experta que te ayude a perfeccionar tus habilidades y a familiarizarte con el tipo de entregables que se realizan en el mundo laboral.

Contexto

Como pudiste ver en módulos recientes, el análisis de vulnerabilidades es un proceso de identificación y evaluación de debilidades en un sistema informático o en una red, con el objetivo de mejorar la seguridad y prevenir posibles ataques. ¿Qué relación tiene con Metasploit?

La relación entre el análisis de vulnerabilidades y Metasploit es que esta puede ser utilizada como una herramienta en el proceso de análisis de vulnerabilidades para identificar y explotar debilidades en un sistema.

Es importante destacar que Metasploit y otras herramientas similares deben usarse con responsabilidad y siempre con el consentimiento del propietario del sistema o red que se está evaluando. Además, es esencial que los profesionales de seguridad tengan los conocimientos y habilidades adecuados para utilizar estas herramientas de manera responsable y ética.

Por otra parte, la inteligencia de amenazas es una disciplina crucial en la defensa contra los ataques cibernéticos, ya que ayuda a los profesionales de seguridad a estar mejor preparados y a tomar medidas proactivas para prevenir y proteger contra posibles ataques.

La inteligencia de amenazas y vulnerabilidades y Metasploit tienen una relación indirecta complementaria. La inteligencia de amenazas y Metasploit trabajan juntas para mejorar la seguridad de los sistemas informáticos: la inteligencia de amenazas proporciona una visión amplia y actualizada de las amenazas cibernéticas y Metasploit se utiliza para probar y explotar vulnerabilidades identificadas.

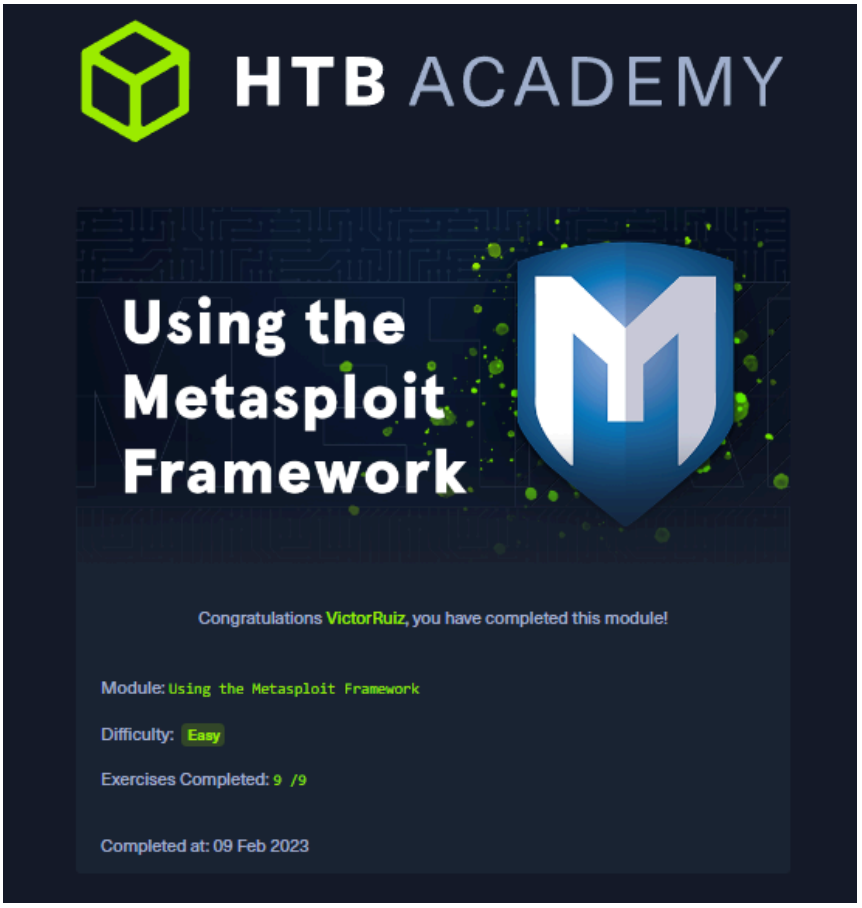
¿A qué te enfrentarás?

Como te mencionamos, deberás resolver el módulo **Using the Metasploit framework** de HTB Academy.

Procedimiento

Los pasos que deberás desarrollar son los siguientes:
1. Completar el módulo y documentar los pasos que te permitieron resolver las preguntas y laboratorios incluidos.
2. Completar las actividades de los laboratorios y detallar los pasos que seguiste para resolverlos.
4. Presentar la insignia que te otorga HTB cuando concluyes el módulo y el respectivo enlace de comprobación. Por ejemplo:

https://academy.hackthebox.com/achievement/694460/39)



Entregables

A. Harás un reporte (perfeccionando las secciones de metodología y teoría que has implementado en módulos anteriores) en el que colocarás todo lo que se te solicitó en el reto de HTB, con sus respectivas respuestas:

Preguntas:

1. Which version of Metasploit comes equipped with a GUI interface?
2. Which version of Metasploit is free and can be used only through a CLI?

Laboratorios:

3. Use the Metasploit-Framework to exploit the target with EternalRomance. Find the flag.txt file on Administrator's desktop and submit the contents as the answer.
4. Exploit the Apache Druid service and find the flag.txt file. Submit the contents of this file as the answer.
5. The target has a specific web application running that we can find by looking into the HTML source code. What is the name of that web application?
6. Find the existing exploit in MSF and use it to get a shell on the target. What is the username of the user you obtained a shell with?
7. The target system has an old version of Sudo running. Find the relevant exploit and get root access to the target system. Find the flag.txt file and submit the contents of it as the answer.
8. Find the existing exploit in MSF and use it to get a shell on the target. What is the username of the user you obtained a shell with?
9. Retrieve the NTLM password hash for the "htb-student" user. Submit the hash as the answer.

B. Durante el **Demo day** tendrás 10 minutos para desarrollar los siguientes puntos en una presentación:

- **Diapositiva 1:** portada y presentación profesional (quién eres, qué haces y por qué te interesa estudiar y pertenecer al sector de ciberseguridad).
- **Diapositiva 2:** breve explicación del módulo que resolviste. Describe un poco el contexto de Metasploit y sus funciones, porque en el mundo laboral tendrás que compartir reportes con directivos o clientes que no conocen ninguna de las herramientas que empleas para resolver ciertos problemas.
- **Diapositiva 3:** detalles de las actividades que realizaste, así como la forma en la que encontraste las soluciones a los laboratorios. (Deberás explicar las herramientas utilizadas, si seguiste o consultaste alguna metodología para resolver el laboratorio y, sobre todo, cómo encontraste los procesos para dar con las soluciones).

- **Diapositiva 4:** resultados obtenidos de la resolución del módulo y lecciones aprendidas. (Aquí deberás mostrar las respuestas y *flags* que se piden en el módulo).
- **Diapositiva 5:** explica ¿por qué lo que resolviste es importante para tu carrera profesional?, ¿por qué es importante para el sector de ciberseguridad en general? y ¿por qué beneficia a la sociedad de acuerdo con tu propia experiencia?

  Nota: Puedes agregar más *slides* en cada apartado para que tus capturas se puedan apreciar de manera adecuada.

Requisitos

- El proyecto se realizará de forma individual.
- El participante creará un documento con los entregables solicitados y lo subirá a una unidad de Google Drive para compartirlo a través de una URL en modo lectura.

Este documento es obligatorio, igual que todos los elementos que lo conforman.

Criterios de evaluación

Actividad	Puntos	Observaciones
Solución del módulo en HTB	50	2: Resolvió el módulo solicitado, obtuvo su insignia y documentó en un reporte los pasos que lo llevaron al resultado. 1: Resolvió el módulo solicitado, obtuvo su insignia, pero no documentó con claridad los pasos que lo llevaron al resultado. 0: No obtuvo su insignia ni enlace del módulo solicitado.
Presentación del *Demo day*	40	2: Elaboró una presentación en la que mostró, de manera clara y sintética, el procedimiento que siguió para resolver el módulo solicitado; además, describió brevemente su proyección de carrera en el área de la ciberseguridad. 1: Elaboró una presentación que muestra de manera confusa o incompleta tanto el procedimiento que siguió para resolver el módulo solicitado como su proyección de carrera en el área de la ciberseguridad. 0: No elaboró su presentación o no incluyó el proceso que lo llevó a solucionar el módulo de HTB.

Entrega a tiempo	10 % 2-1-0	2: Entregó el documento en la fecha requerida. 1: Entregó la URL del documento del proyecto 10 días después de la fecha requerida. 0: Entregó la URL del documento del proyecto 11 días después o más de la fecha requerida.

Insignia

Seleccionar el grado que corresponde a la insignia, según el logro del proyecto.

Insignia	Grado	Grado	Puntos
Cyber Security Analyst (UCSA)	Beginner	Principiante	50 a 79 puntos
		Sobresaliente	80 a 100 puntos