Instituto Tecnológico y de Estudios Superiores de Monterrey

Actividad 3.1.2.1 Conocimiento de herramientas usadas en pentesting.

Nombre	Matrícula
Juan Pablo Echeagaray González	A00830646
Verónica Victoria García De la Fuente	A00830383
Emmanuel Isaí Godínez Flores	A01612966
Carlos David Lozano Sanguino	A01275316
Emily Rebeca Méndez Cruz	A00830768
Eugenio Santisteban Zolezzi	A01720932

Aplicación de criptografía y seguridad

MA2005B.201

Dr. Alberto Francisco Martínez Herrera

Dr. Oscar Eduardo Labrado Gómez

03 de octubre del 20222

1. Hack The Box

Hack The Box fue fundado por Haris Pylarinos en 2017, ya que Pylarinos se dio cuenta que la forma más productiva de desarrollar habilidades de ciberseguridad era a través de la práctica, en lugar de aprender la teoría leyendo libros [1]. Esta plataforma se especializa en el uso de "piratería ética"para entrenar técnicas de ciberseguridad. Los usuarios enfrentan desafíos para atacar laboratorios virtuales vulnerables en un entorno simulado, gamificado y de prueba [2].

Al aplicar la mecánica del juego en la plataforma, Pylarinos desarrolló un entorno de entrenamiento donde las personas entusiastas de la ciberseguridad practiquen sus habilidades. Cada semana, *Hack The Box* crea una nueva máquina virtual para que los jugadores entren; en esta dinámica se le otorgan puntos a los jugadores que tengan intentos exitosos de piratería y un lugar en la tabla de clasificación mundial. La plataforma tiene oportunidades para aspirantes a hackers de todos los niveles de dificultad, algunos de los desafíos más difíciles pueden llegar a tardar días en completarse [1].

"Hack The Box es un campo de juegos de piratería masivo y una comunidad de seguridad de la información de más de 1,2 millones de miembros de la plataforma que aprenden, piratean, juegan, intercambian ideas y metodologías", es la definición que se puede encontrar en la página web de Hack The Box, puede ver más información acerca de esto en este enlace [3].

Este enfoque ha atraído a más de 1.2 millones de miembros a la plataforma, desde principiantes hasta expertos, cuenta con más de 450 laboratorios de hackeo, también con más de 1.4 miles de organizaciones, que buscan mejorar su conocimiento acerca de los ciberadversarios, y más de 150 de CTFs (Capture The Flag) junto con otros eventos [3].

Un atractivo nuevo a este sitio es la posibilidad de obtener una certificación de *pentesting*. La plataforma ahora ofrece la certificación *HTB Certified Penetration Testing Specialist*, la cual tiene como objetivo desarrollar competencias técnicas de hackeo ético y *pentesting* a un nivel intermedio, se espera que al obtener la certificación el alumno pueda detectar problemas de seguridad así como sus medios de explotación respectivos, que no serían sencillos de aplicar buscando directamente CVEs [4]. La empresa destaca también que el poseer las habilidades técnicas no será suficiente para obtener la certificación, sino que se tienen que desarrollar las habilidades de comunicación necesarias para transmitir los descubrimientos hechos, en particular, uno de los medios de evaluación es que el alumno pueda escribir un reporte técnico de alta calidad que documente el procedimiento realizado así como las vulnerabilidades identificadas.

Algunas de las áreas en las que se enfoca la certificación son [4]:

- Técnicas de pentesting
- Técnicas de recopilación de información
- Ataques a sistemas Windows y Linux
- Ataques al Active Directory
- Pentesting para aplicaciones web
- Escalamiento de privilegios para Windows y Linux
- Comunicación de riesgos y vulnerabilidades

Hack in the box ha generado un impacto importante en la forma en la cual se preparan las personas interesadas en implementar métodos de ciberseguridad para las empresas. A través de sistemas como este se abre la posibilidad de mantenerse a la vanguardia en cuanto a los conceptos nuevos que surgen cada día y el impacto que estos pueden tener en la seguridad de las empresas [5]. Actualmente *Hack in the box* busca que los métodos gamificados se vuelvan el estándar de las empresas para desarrollar este tipo de habilidades. [6].

Actualmente *Hack in the box* está predominando como la principal plataforma gamificada para entrenarse en métodos de *Pentesting* de forma activa y dinámica sin enfocarse únicamente en la teoría [5]. Esto se puede observar en que cada día más empresas optan por el uso de este método para el entrenamiento de sus empleados, entre ellas se encuentran Siemens *S.A., Electronic Arts, NTT Ltd., NortonLifeLock* entre otras. En 2021 el valor de la empresa cerró en $10.6 millones de dólares. Sus principales patrocinadores han sido US Paladin Capital y Marathon Venture Capital, quienes han apostado por este nuevo e innovador método de aprendizaje y práctica[6].

1.1. Registro en el sitio web

En la figura 1 podemos observar la interfaz de registro y lo sencillo que es crear una nueva cuenta para comenzar con esta plataforma. Como parte del registro deberemos llenar un formulario sencillo que se puede observar en la figura 2.

Al finalizar este proceso podremos ver la interfaz principal donde podemos acceder a las diferentes secciones de esta herramienta y lo amigable que es al usuario como se puede observar en la figura 3.

1.2. Realización de una actividad en *Hack The Box*

Para esta entrega también hemos probado una de las actividades introductorias que *Hack The Box* le ofrece a sus usuarios, en particular nos hemos enfocado en la serie de actividades *Learn the basics of Penetration Testing* 4.

El primer paso de estas actividades siempre será la configuración de una máquina virtual; los usuarios pueden disponer de un equipo virtualizado por sus propias cuentas, o hacer uso de *pwnbox*, esta opción tiene un límite de 2 horas de cómputo, pero para fines prácticos es la más amigable de las 2, un ejemplo de su configuración puede ser visualizado en la figura 5, cuando se realice el proceso con éxito, se podrá abrir una nueva pestaña en el navegador, en la que una máquina virtual como la mostrada en la figura 6 podrá ser usada para completar los pasos de la actividad en cuestión.

Las preguntas a resolver irán escalando en complejidad, en la figura 7 se muestra un ejemplo de las preguntas iniciales de esta actividad. Una vez que el usuario haya completado la actividad, verá un *pop-up* como el de la figura 8.

2. Imágenes

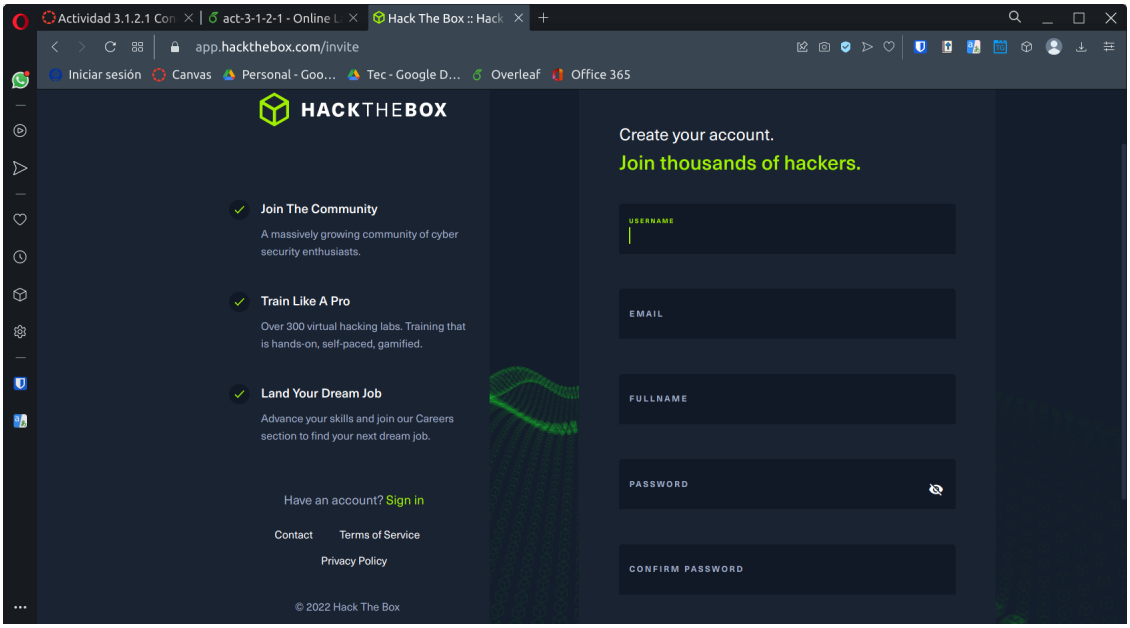

Figura 1: Ventana de registro para crear nueva cuenta en Hack the Box

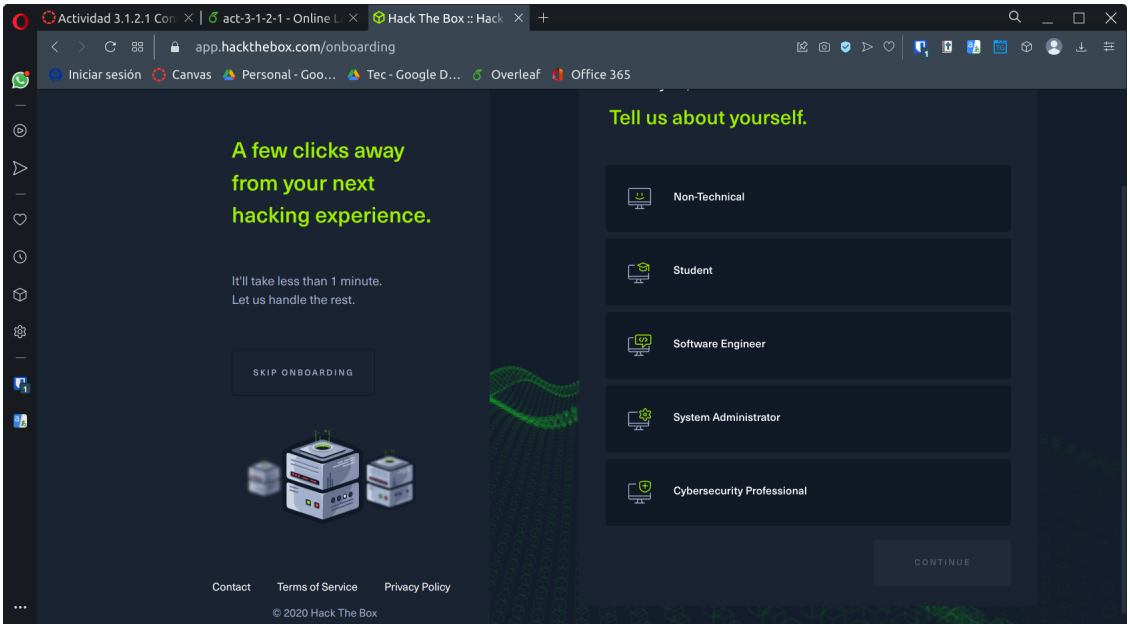

Figura 2: Proceso de registro en Hack the Box

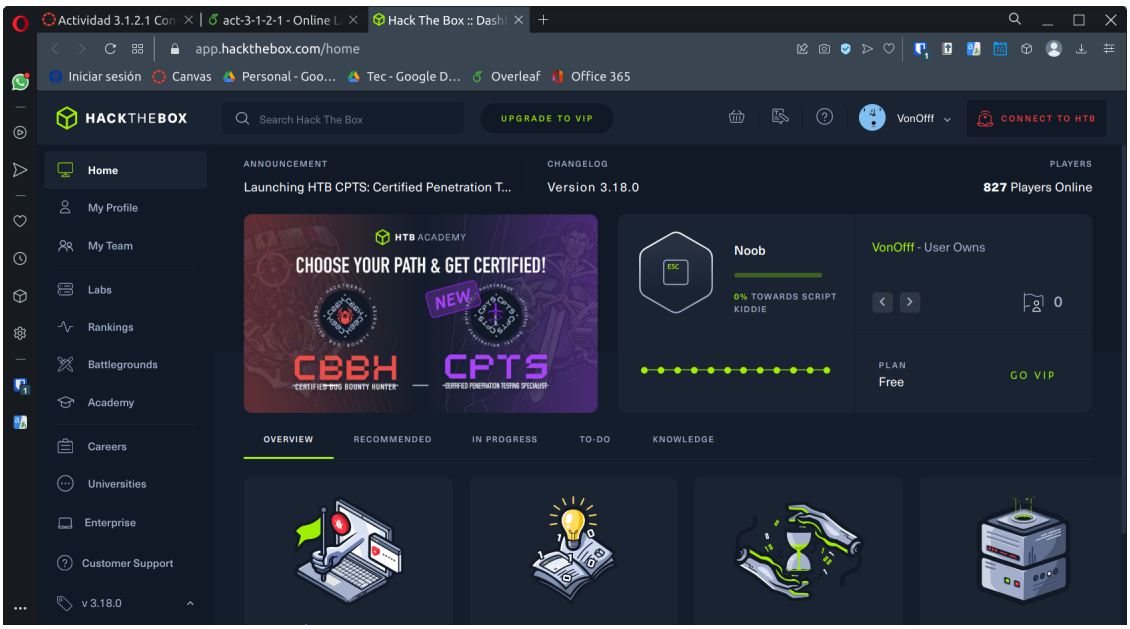

Figura 3: Ventana principal de Hack de Box

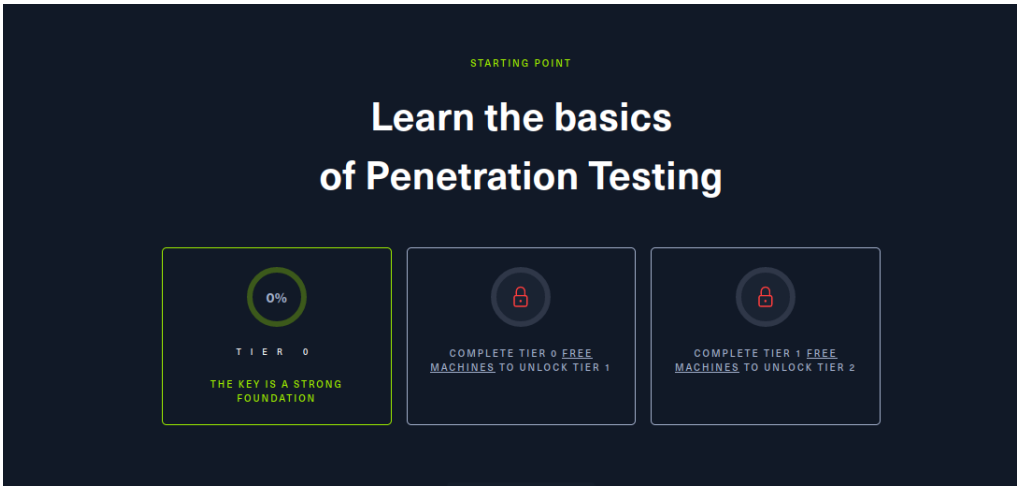

Figura 4: Primera práctica de pentest

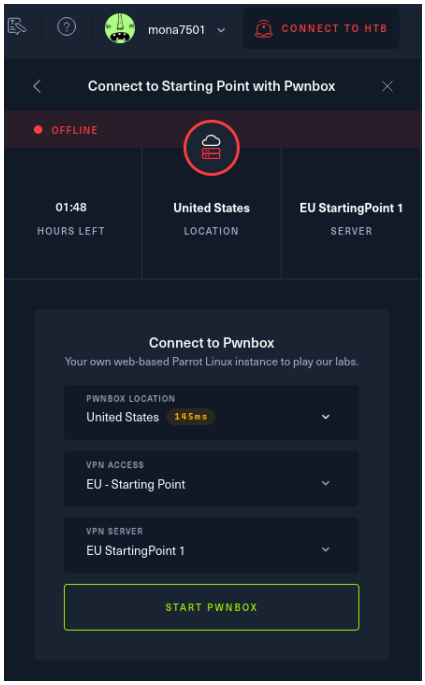

Figura 5: Configuración de máquina virtual

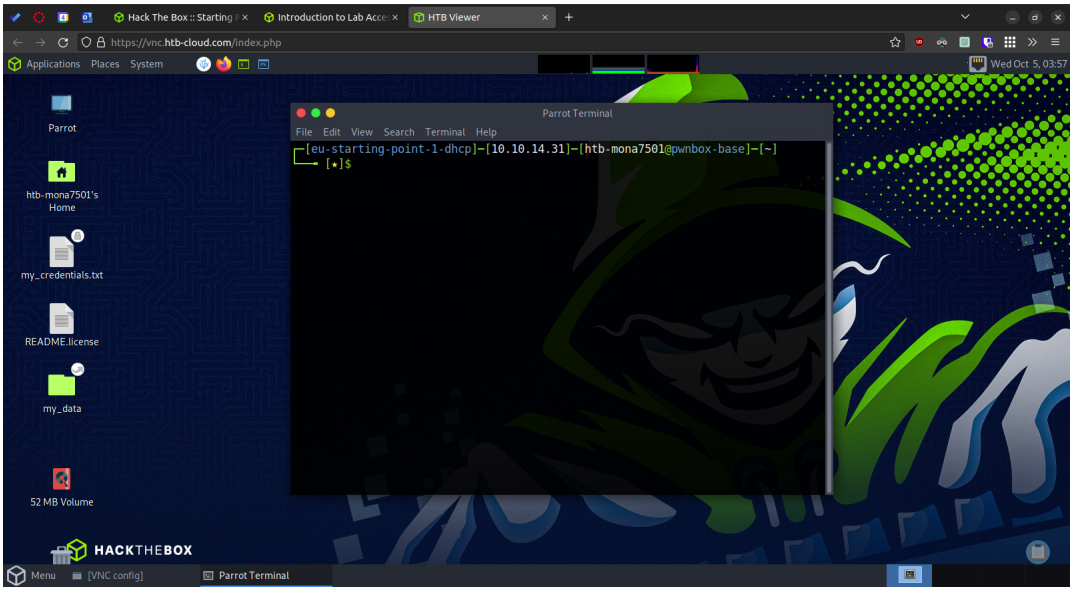

Figura 6: Ejemplo de instancia de máquina virtual

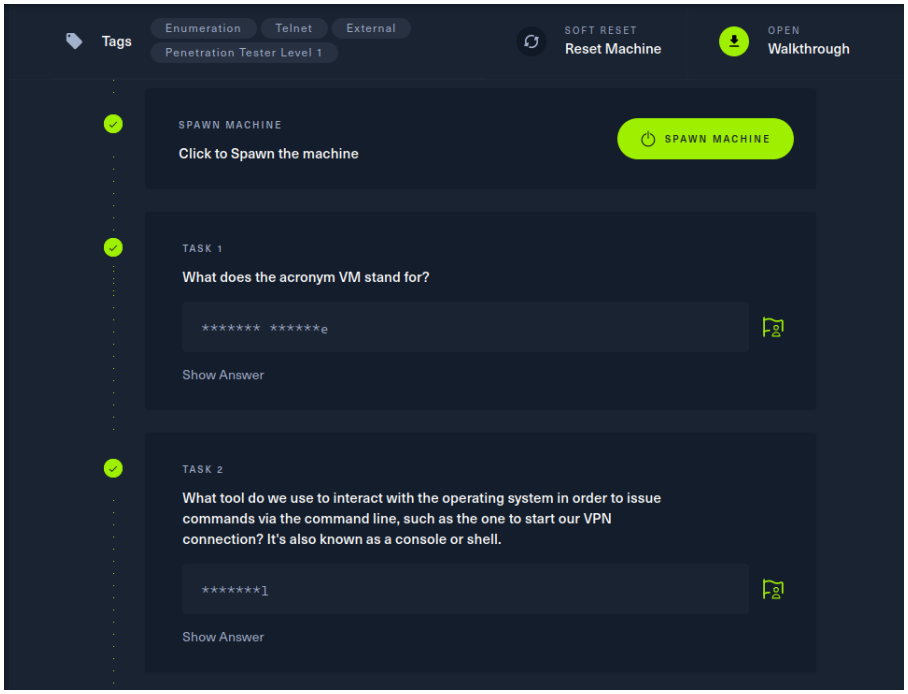

Figura 7: Ejemplo de preguntas de las actividades disponibles

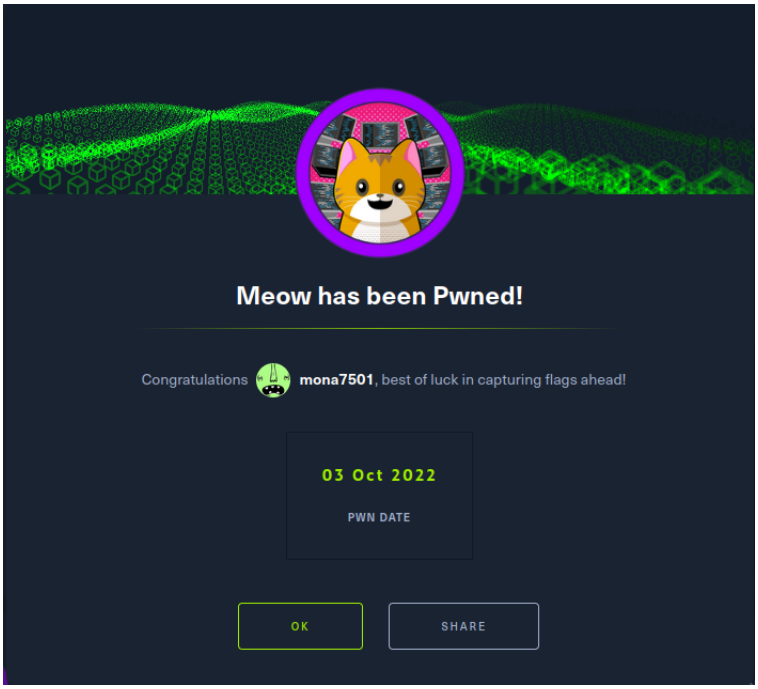

Figura 8: Ejemplo de ventana de éxito en laboratorio

Referencias

[1] N. Novick, "Uk-founded hack the box raises $1.3m to build the world's largest hacker community," Apr 2019. [Online]. Available: https://tech.eu/2019/04/01/uk-founded-hack-the-box-raises-1-3m-to-build-the-worlds-largest-hacker-community

[2] M. Butcher, "Cybersecurity training startup hack the box raises $10.6m series a led by paladin capital," Apr 2021. [Online]. Available: https://techcrunch.com/2021/04/12/cybersecurity-training-startup-hack-the-box-raises-10-6m-series-a-led-by-paladin-capital/

[3] "All about hack the box." [Online]. Available: https://www.hackthebox.com/about-us

[4] "HTB Penetration Testing Certification [CPTS] — Hack The Box." [Online]. Available: https://academy.hackthebox.com/preview/certifications/htb-certified-penetration-testing-specialist/

[5] Kim Crawleyr, "How Hack The Box is Redefining Cybersecurity Training for Business," 2021. [Online]. Available: https://www.hackthebox.com/blog/redefining-cybersecurity-training

[6] Elena Ivanova, "The Greek cybersecurity training platform Hack the Box raises $10.6M to replace certification with gamifications," 2021. [Online]. Available: https://therecursive.com/the-greek-cybersecurity-training-platform-hack-the-box-raises-10-6m-to-replace-certification-with-gamification/