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

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/