Introduction to Ethical Hacking using Hack the Box

Instituto Tecnológico de Pachuca

Imagen de portada del libro: Linux Basics for Hackers

DISCLAIMER / DESLINDE DE RESPONSABILIDAD

El presente taller tiene como objetivo proporcionar información y conocimientos relacionados con la ciberseguridad y el hacking ético. Los materiales, ejemplos y ejercicios ofrecidos en este taller están destinados exclusivamente a fines educativos y formativos.

El uso indebido de la información o las técnicas presentadas en este taller para actividades ilegales o maliciosas es estrictamente prohibido y desalentado.

La institución, organizadores, e instructores de este taller no se hacen responsables de cualquier uso inapropiado o ilegal que los participantes puedan hacer de la información o las habilidades adquiridas durante el taller. Es responsabilidad de cada participante utilizar estos conocimientos de manera ética, legal y conforme a las leyes y regulaciones locales y nacionales aplicables.

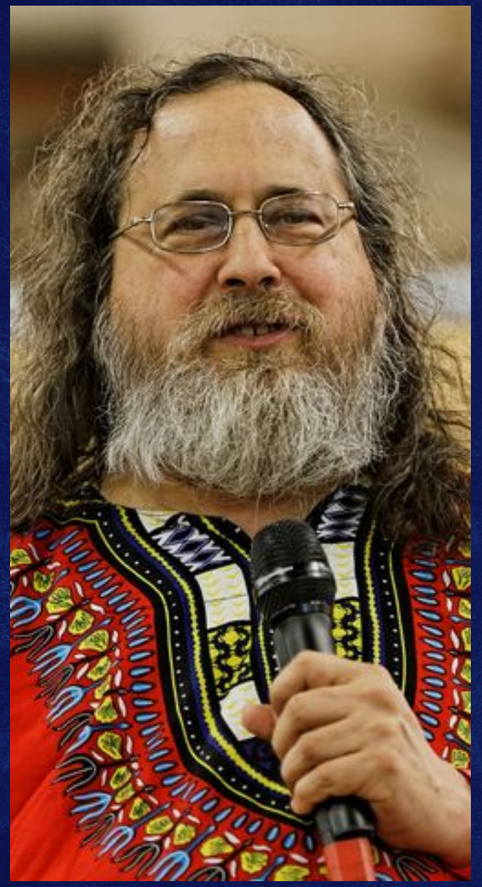
Además, este taller no respalda ni promueve la participación en actividades ilegales, como el acceso no autorizado a sistemas informáticos, el robo de datos o cualquier otra forma de actividad delictiva relacionada con la ciberseguridad.

El hacking ético debe llevarse a cabo en un entorno legal y con el consentimiento explícito del propietario del sistema o datos.

Los participantes deben recordar que el uso indebido de las habilidades adquiridas en este taller puede tener graves consecuencias legales y éticas. Se insta a los participantes a actuar con responsabilidad y a buscar siempre el consentimiento adecuado antes de realizar cualquier prueba o evaluación de seguridad en sistemas o redes.

Al asistir y participar en este taller, los participantes aceptan plenamente este descargo de responsabilidad y se comprometen a utilizar sus conocimientos de manera ética y legal.

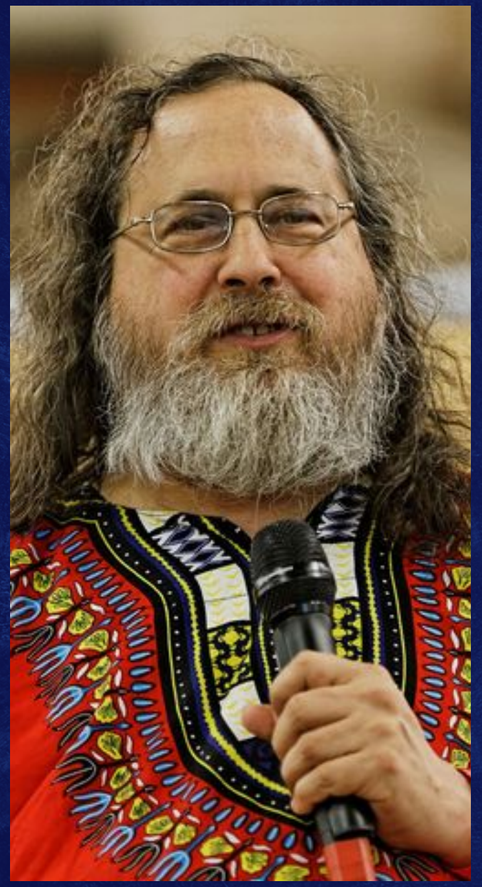
¿Qué si es y que no es un Hacker?



¿Qué si es y que no es un Hacker?

Mr. Robot

E-CORP



R. Stallman

GNU / FSF

J.M. Alonso

TELEFÓNICA

A. E. Torres

FORTINET / UANL

R. Marin

IBM

Conceptos

Ethical Hacking (hackeo ético) es explotar las vulnerabilidades existentes en el sistema de "interés" valiéndose de test de intrusión, que verifican y evalúan la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, etc. Con la intención de ganar acceso y "demostrar" que un sistema es vulnerable, esta información es de gran ayuda a las organizaciones al momento de tomar las medidas preventivas en contra de posibles ataques malintencionados.

Los hackers éticos también conocidos como Pen-Tester, como su nombre lo dice, realizan "Pruebas de Penetración". Un hacker ético es un experto en computadoras y redes de datos, su función es atacar los sistemas de seguridad en nombre de sus dueños, con la intención de buscar y encontrar vulnerabilidades que un hacker malicioso podría explotar. Para probar los sistemas de seguridad, los Ethical Hackers (hackers éticos) utilizan los mismos métodos que sus homólogos, pero se limitan únicamente a reportarlos en lugar de sacar ventaja de ellos.

Fuente: UNAM-CERT
https://www.seguridad.unam.mx/historico/documento/index.html-id=7

Legislación y regulaciones en México y el Estado de Hidalgo

CAPITULO II
ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

Adicionado. P.O. Alcance cinco del 15 de julio de 2022.

Artículo 178 Bis. - Se impondrá de tres meses a dos años de prisión y de 5 a 40 días multa, al que dolosamente y sin consentimiento de quien tenga derecho a otorgarlo, copie, modifique, destruya, conozca o provoque la pérdida de la información contenida en sistemas o equipos de informática.

Artículo Adicionado. P.O. Alcance cinco del 15 de julio de 2022.

Artículo 178 Ter. - Las penas previstas en el artículo 178 bis se incrementarán hasta en una mitad más, cuando los sistemas o equipos de informática pertenezcan a una institución pública estatal o municipal.

Artículo Adicionado. P.O. Alcance cinco del 15 de julio de 2022.

EXTRACTO DEL CÓDIGO PENAL DEL ESTADO DE HIDALGO. LIBRO SEGUNDO. TITULO PRIMERO. DELITOS CONTRA LA VIDA Y LA SALUD PERSONAL. CAPITULO II ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA.

CAPÍTULO II
Acceso ilícito a sistemas y equipos de informática

Capítulo adicionado DOF 17-05-1999

Artículo 211 bis 1.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y de cien a trescientos días multa.

Al que sin autorización conozca o copie información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de tres meses a un año de prisión y de cincuenta a ciento cincuenta días multa.

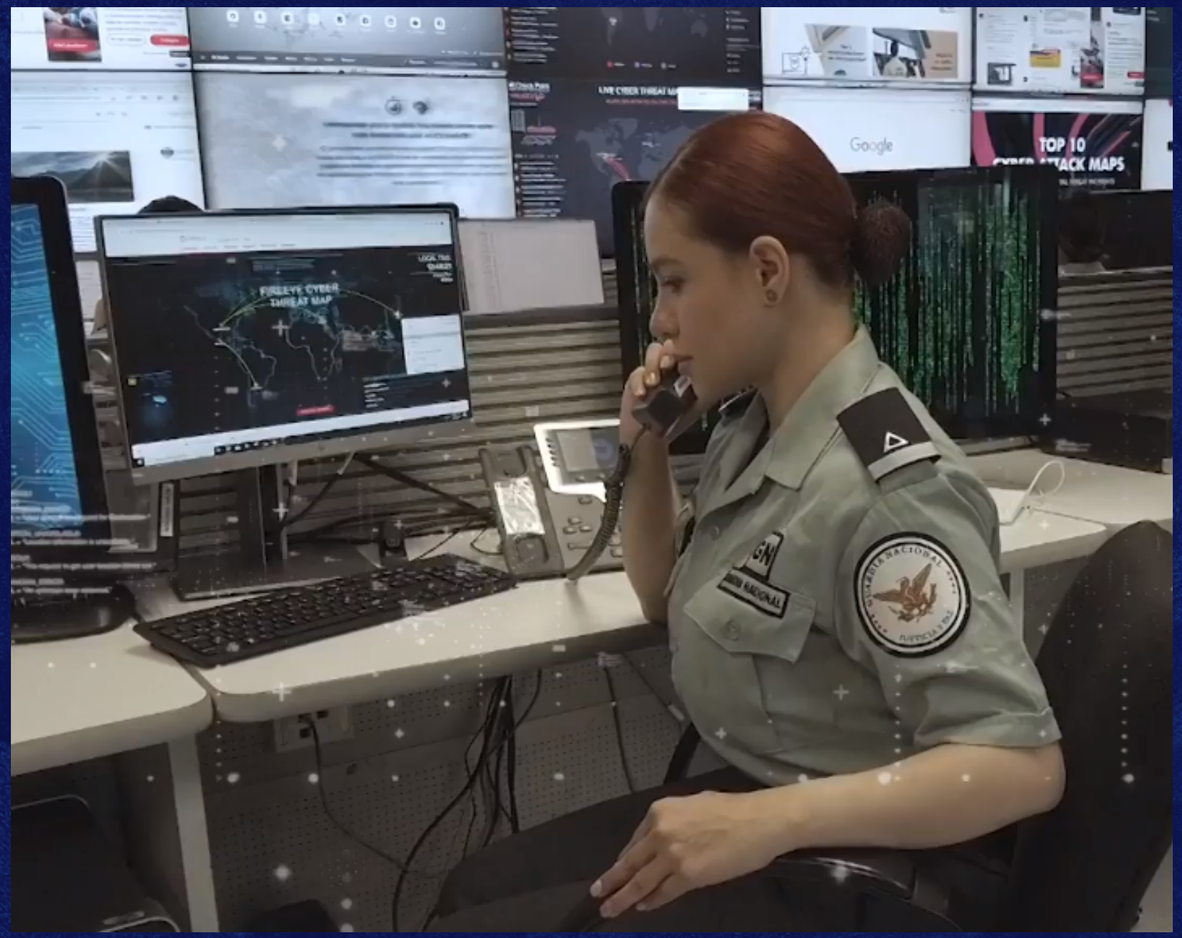
Artículo adicionado DOF 17-05-1999

Artículo 211 bis 2.- Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática del Estado, protegidos por algún mecanismo de seguridad, se le impondrán de uno a cuatro años de prisión y de doscientos a seiscientos días multa.

EXTRACTO DEL CÓDIGO PENAL FEDERAL. LIBRO SEGUNDO. TÍTULO NOVENO - REVELACIÓN DE SECRETOS Y ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA. CAPÍTULO II - ACCESO ILÍCITO A SISTEMAS Y EQUIPOS DE INFORMÁTICA

- Ley Federal de Protección de Datos Personales en Posesión de Particulares
- Ley de Ciberseguridad Nacional
- Norma Oficial Mexicana NOM-024
- Código Penal Federal
- Código Penal del Estado de Hidalgo
- Regulaciones de la Autoridad Nacional de Protección de Datos Personales (INAI)
- Unidad de Policía Cibernética del Estado de Hidalgo

México y la Ciberseguridad



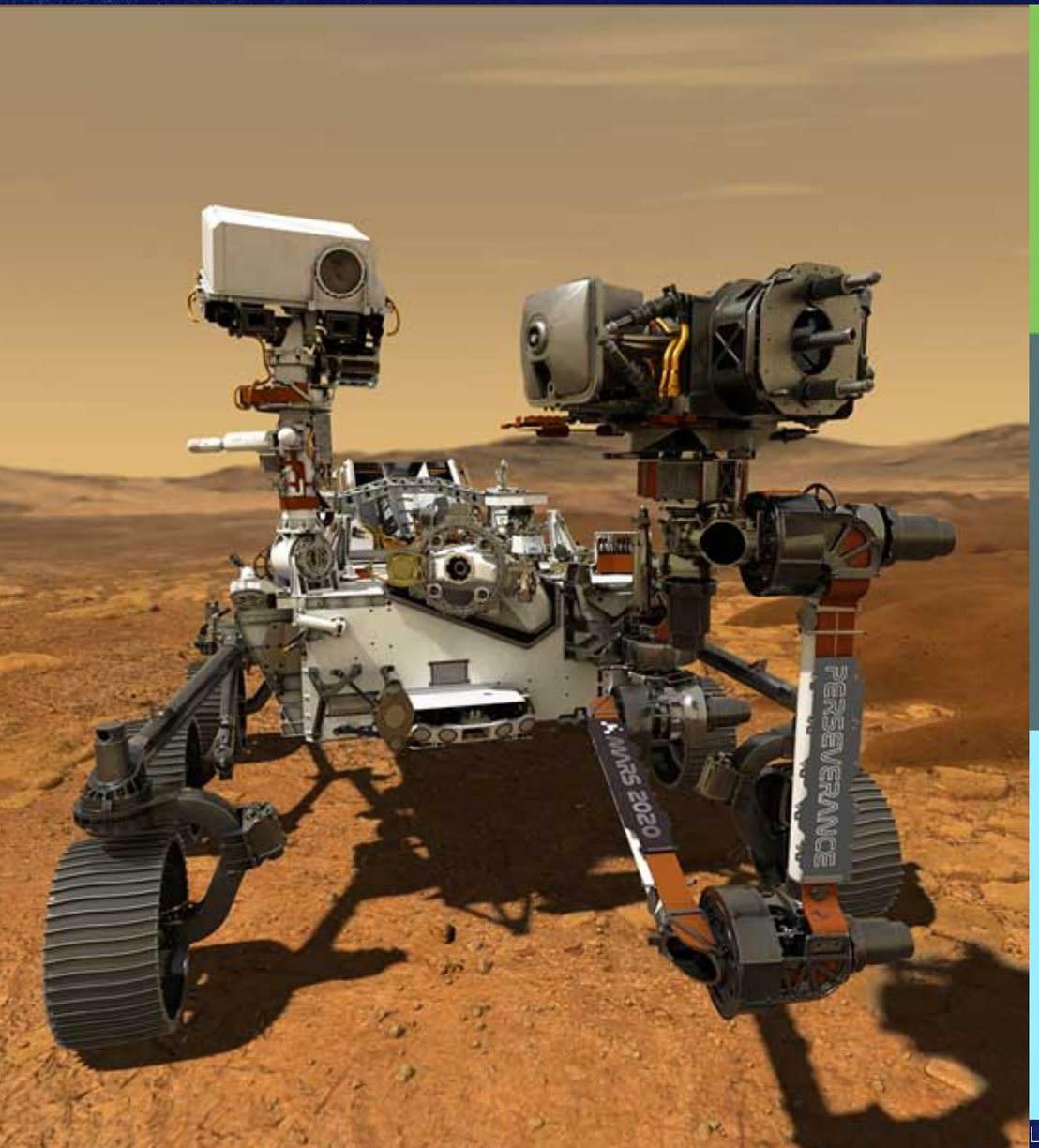
- POLICÍA CIBERNETICA
- GUARDIA NACIONAL
- ARMADA DE MÉXICO
- UNICIBER - ESTADO MAYOR GENERAL
- C5, C5I, C4
- FORENSES INFORMÁTICOS
- FGR

EVENTOS:

- HACKMEX - IPN
- UNAM
- HACKGDL - ITESO (GDL)
- BUGCON
- CONGRESOS DE EMPRESAS PRIVADAS: SICTUM, CISCO, FORTINET, PALO ALTO NETWORKS, TOTAL CYBER SEC, ETC...

FUENTE Y LOGOS DE SUS RESPECTIVAS INSTITUCIONES
WWW.GOB.MX/SEMAR | WWW.GOB.MX/SEDENA | HTTP://POLICIACIBERNETICA.HIDALGO.GOB.MX/ | HTTPS://S-SEGURIDAD.HIDALGO.GOB.MX/PAG/C5I.HTML

Linux is Everywhere



99% of the world's top supercomputers run Linux

1.4 Billion active users of Linux-based Android devices

80% of all stock exchanges rely on Linux

Linux helps IBM's Watson analyze **200 Million** pages of clinical data in 15 seconds

"The God Particle" was discovered using CERN's Linux-powered Large Hadron Collider

Google, Amazon, even Microsoft use Linux to power their cloud services

US air traffic control runs on Linux

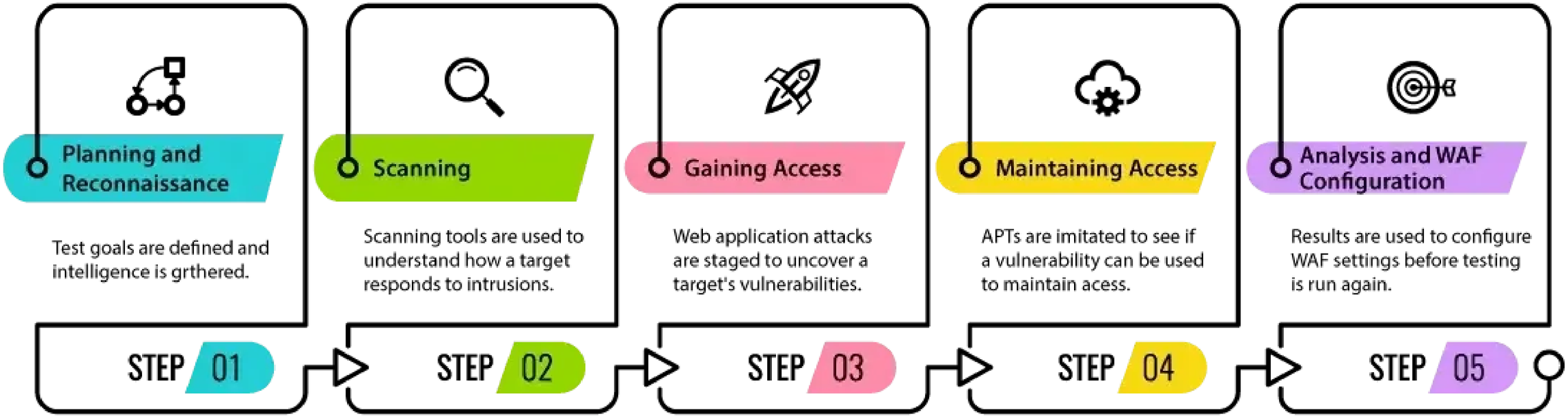
Queensland Motorways relies on Linux for smart traffic management

Linux helps run **bullet trains** in Japan

Linux Is Everywhere Infographic: https://blog.netdevgroup.com/2016/11/linux-is-everywhere-infographic/

Phases of Ethical Hacking

Ethical hacking is a process of detecting vulnerabilities in an application, system, or organization's infrastructure that an attacker can use to exploit an individual or organization. They use this process to prevent cyberattacks and security breaches by lawfully hacking into the systems and looking for weak points. An ethical hacker follows the steps and thought process of a malicious attacker to gain authorized access and test the organization's strategies and network.



Conceptos

- **VM (Máquina Virtual):** Es como una computadora dentro de tu computadora. Puedes crear varias VMs en una sola computadora y ejecutar diferentes sistemas operativos y programas en cada una de ellas.

- **VPN (Red Privada Virtual):** Es como un túnel seguro en internet. Te permite conectarte a una red privada a través de internet de forma segura, ocultando tus datos de miradas no deseadas.

- **Puerto:** Piensa en un puerto como una puerta en tu computadora por donde entran y salen datos. Cada aplicación en tu computadora usa un número de puerto específico para comunicarse con otras computadoras. Hay 65,535.

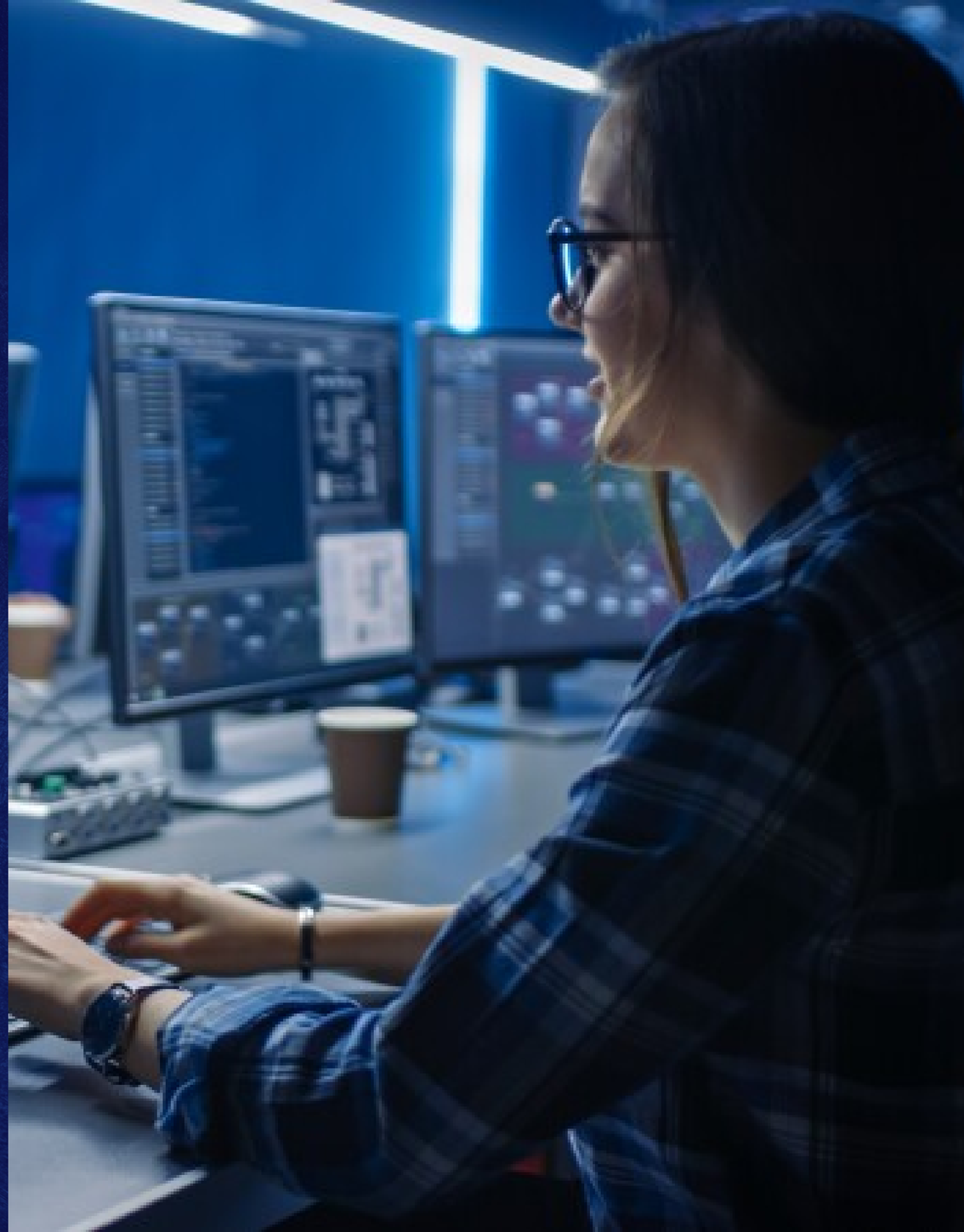
- **Servicio:** Es un programa o función que tu computadora proporciona a otras computadoras. Pueden ser cosas como un servidor web que muestra páginas web o un servicio de correo electrónico que envía y recibe correos.

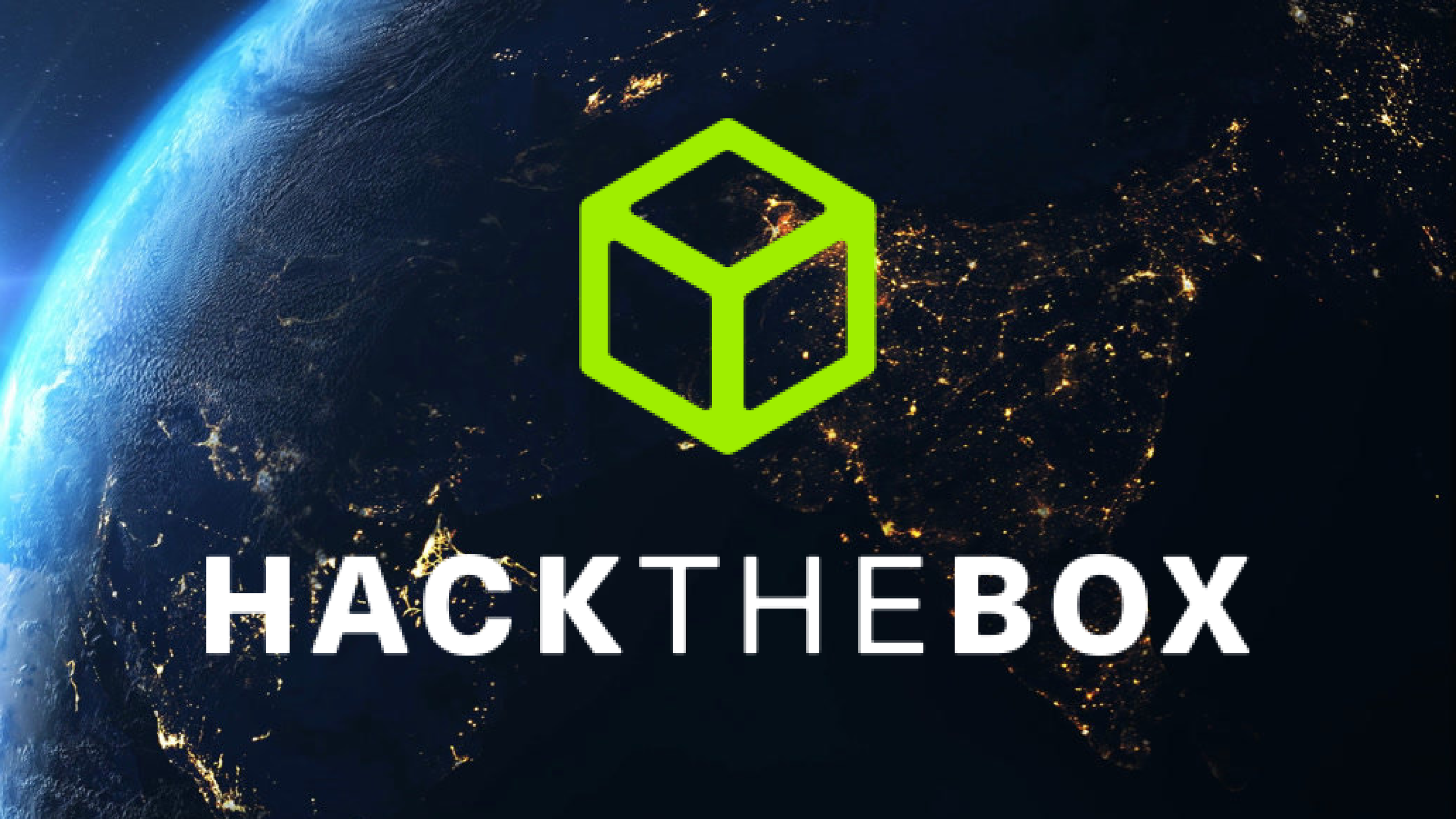
Conceptos

- **TCP/IP: Es el lenguaje de internet.** Es un conjunto de reglas que permiten que las computadoras se comuniquen entre sí en la red. TCP (Protocolo de Control de Transmisión) y IP (Protocolo de Internet) son dos partes importantes de TCP/IP.

- **TCP (Protocolo de Control de Transmisión):** Es como una conversación telefónica. Garantiza que los datos se transmitan de manera confiable y en el orden correcto. Es bueno para cosas como la descarga de archivos.

- **UDP (Protocolo de Datagramas de Usuario):** Es como enviar una postal. Envía datos rápidamente, pero no garantiza que lleguen en orden o incluso que lleguen en absoluto. Es útil para aplicaciones que requieren velocidad, como las llamadas de voz por internet.




HACKTHEBOX

Crear cuenta en :

www.hackthebox.com

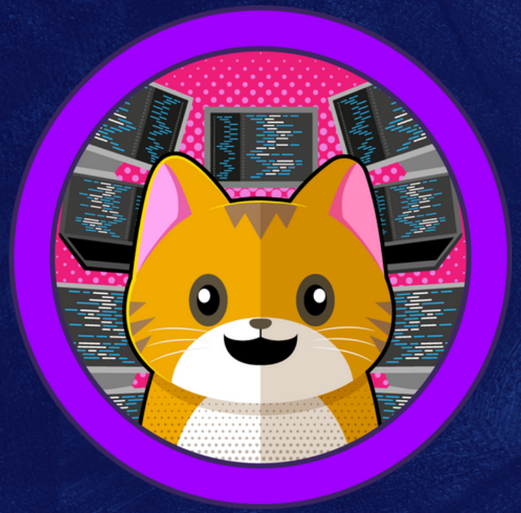
- **CORREO PERSONAL**
- **NAVEGADOR BASADO EN CHROMIUM**

TODO EL MATERIAL ESTÁ EN:

isuilugo.github.io/taller-hacking-itp

HACKTHEBOX

Meow



Linux Basics

Nmap | VPN | ICMP | SCAN | TELNET

```
~# ping -c 1 10.129.187.101
```

ICMP

10.10.14.208 **10.129.187.101**

TTL: 64 Linux & 128 Windows

```
~# sudo nmap 10.129.187.100/24
```

10.10.14.208

Parrot Security

Meow

10.129.187.101

- tcp
- port: 21

HTTP/HTTPS/DNS

10.129.187.102

- tcp
- port: 80, 443
- udp
- Port: 53

MySQL

10.129.187.103

- tcp
- port: 3306

~# sudo nmap --open -sSV -vvv 0 -n -Pn 10.129.187.101 -oG escaneo

- **sudo: S**e usa para ejecutar el comando con privilegios de superusuario o administrador.

- **nmap:** La herramienta que se está utilizando para realizar el escaneo de red.
- **--open:** Esta opción indica a Nmap que solo muestre los puertos que están abiertos

- **-sS:** Realiza un escaneo SYN, que es un escaneo sigiloso y rápido para identificar puertos abiertos**.**

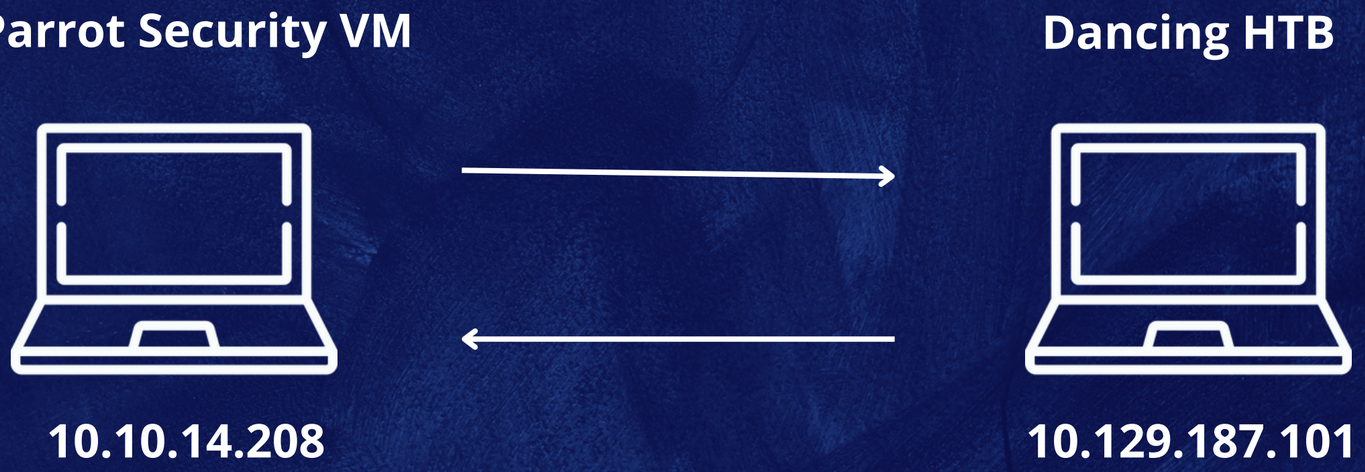
- **-V:** Habilita la detección de versiones de servicio**s**
-
- **-vvv:** Establece el nivel de verbosidad del escaneo en "muy, muy, muy" detallado, lo que proporciona una cantidad significativa de información sobre el progreso del escaneo y los resultados.
-
- **-n:** No intentará traducir las direcciones IP a nombres de host.
-
- **-Pn:** Esto significa que Nmap realizará el escaneo de puertos en la dirección IP objetivo sin importar si el host responde a los paquetes de ping**.**
-
- **10.129.198.11:** La dirección IP del objetivo que se va a escanear.
-
- **-oG escaneo:** Esta opción indica a Nmap que genere un archivo de salida en formato Greppable (Grepable). El archivo se llamará "escaneo" y contendrá los resultados del escaneo.

10.10.14.208

10.129.187.101

Dancing

Windows Basics



Network | Protocols | SMB | Reconnaissance

¡GRACIAS!

TODO EL MATERIAL ESTÁ EN:
isuilugo.github.io/taller-hacking-itp

Bibliografía

[1] Código Penal FederalLibro SegundoTítulo Noveno - Revelación de Secretos y Acceso Ilícito a Sistemas y Equipos de InformáticaCapítulo II - Acceso Ilícito a Sistemas y Equipos de Informática", Justia, 25-may-2023. [En línea]. Disponible en: https://mexico.justia.com/federales/codigos/codigo-penal-federal/libro-segundo/titulo-noveno/capitulo-ii/. [Consultado: 20-sep-2023].
[2] Gob.mx. [En línea]. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/661790/Glosario_de_Terminos_SD-_SM_compressed.pdf. [Consultado: 20-sep-2023].
[3] "Hackers éticos, ¿qué son y cómo trabajan?", Anahuac.mx. [En línea]. Disponible en: https://www.anahuac.mx/mexico/noticias/Hackers-eticos-que-son-y-como-trabajan. [Consultado: 20-sep-2023].
[4] C. De Diputados, D. H. Congreso De, y L. A. Unión, "CÓDIGO PENAL FEDERAL", Justia.com. [En línea]. Disponible en: https://docs.mexico.justia.com/federales/testing/codigo-penal-federal.pdf. [Consultado: 20-sep-2023].
[5] "Linux Basics for Hackers", Nostarch.com, 01-dic-2017. [En línea]. Disponible en: https://nostarch.com/linuxbasicsforhackers. [Consultado: 20-sep-2023].
[6] "Linux is everywhere infographic", Netdevgroup.com. [En línea]. Disponible en: https://blog.netdevgroup.com/2016/11/linux-is-everywhere-infographic/. [Consultado: 20-sep-2023].
[7] "Secretaría de seguridad pública", Gob.mx. [En línea]. Disponible en: https://s-seguridad.hidalgo.gob.mx/pag/C5i.html. [Consultado: 20-sep-2023].
[8] "Unidad de Policía Cibernética del Estado de Hidalgo", Gob.mx. [En línea]. Disponible en: http://policiacibernetica.hidalgo.gob.mx/. [Consultado: 20-sep-2023].
[9] L. H. Raúl y P. Libien, "Los Delitos Informáticos previstos y sancionados en el Ordenamiento Jurídico Mexicano", Gob.mx. [En línea]. Disponible en: http://www.ordenjuridico.gob.mx/Congreso/2doCongresoNac/pdf/PinaLibien.pdf. [Consultado: 20-sep-2023].
[10] Gob.mx. [En línea]. Disponible en: https://www.congresocdmx.gob.mx/archivos/legislativas/Ciberseguridad.pdf. [Consultado: 20-sep-2023].
[11] S. de Marina, "Coordinadora General del Ciberespacio", gob.mx. [En línea]. Disponible en: https://www.gob.mx/semar/articulos/unidad-de-ciberseguridad-279197?idiom=es. [Consultado: 20-sep-2023].
[12] "¿Qué es una VPN y cómo funciona?", latam.kaspersky.com, 17-ago-2023. [En línea]. Disponible en: https://latam.kaspersky.com/resource-center/definitions/what-is-a-vpn. [Consultado: 28-sep-2023].
[13] Cloudflare.com. [En línea]. Disponible en: https://www.cloudflare.com/es-es/learning/network-layer/what-is-a-computer-port/. [Consultado: 28-sep-2023].