

## ACTIVIDAD DE APRENDIZAJE 2 UNIDAD 3:

### Explotando Vulnerabilidades I

#### ***Fase Transversal - Interpretación, aprehensión y transferencia conceptual / temática.***

En esta actividad se va a ahondar en el concepto de los ataques que puede sufrir un sistema, enfocándose en el impacto que tienen sobre la información que reside o es manipulada, especialmente en la confidencialidad y autenticidad, dos de los pilares de los sistemas de información. Se expondrán los tipos de ataques asociados a estos pilares y ejemplos por medio de los cuales se pueda ver como se ejecutan en el mundo real estas actividades que buscan aprovechar alguna vulnerabilidad existente en el sistema objetivo y valerse de algún objetivo por parte del atacante, este punto seguirá la línea de las defunciones de conceptos relacionados con la ciberseguridad.

Luego, se expondrán las vulnerabilidades existentes en los sistemas operativos más usados en la actualidad, como lo son Windows, macOS, Linux y Android, exponiendo información relacionada con los componentes y servicios en los cuales se encuentra presente en fallo y los exploits existentes, de modo tal nos podremos contextualizar con relación al estado de seguridad de los sistemas operativos que están en nuestros dispositivos y ver como las empresas responsables o propietarias de estos componentes de software actúan con relación a las vulnerabilidades, esto siguiendo la línea de las vulnerabilidades existentes en software como se trabajo en la actividad anterior.

Finalmente, se expondrá información sobre repositorios y plataformas en las cuales se pueden poner en practica las habilidades de Pentesting, análisis de vulnerabilidades e intrusión a sistemas, todo esto en un entorno simulado enfocándose en las vulnerabilidades existentes en los sistemas que se emplean en la actualidad, teniendo como primera referencia a Hack The Box y exponiendo otras plataformas similares las cuales nos brinden maquinas en las cuales debemos obtener los privilegios del usuario Root u obtener algún dato almacenado en un archivo dentro de la maquina

### ***Fase Uno – Planteamiento de estudio de casos o actividad***

- 1. En clase se mencionó los ataques contra el secreto y la autenticidad como mecanismos para la explotación de vulnerabilidades. Indaga cuales son los 3 tipos de ataques contra el secreto y los 4 tipos de ataques contra la autenticidad.*
- 2. En la última parte de la clase se mencionó además que los sistemas operativos son objetivo de explotación de vulnerabilidades indaga cuales son las principales vulnerabilidades de Windows, Linux, MacOS y Android, y como se explotan algunas de las mismas*
- 3. Hack The Box es una excelente herramienta para ejercicios de Pentesting, has una búsqueda en la red de otros repositorios similares a Hack The Box en que se puedan descargar maquinas deliberadamente débiles para pruebas de seguridad, elabora un listado con el nombre del sitio, el tipo de máquinas virtuales y el enlace de acceso.*

### ***Fase Dos – Planteamiento de la respuesta y solución de la actividad***

#### **1. Ataques contra el secreto y la autenticidad**

Un ataque es una actividad intencional la cual busca aprovechar las vulnerabilidades existentes en un sistema y de esta forma poder comprometer el funcionamiento del sistema o en alguno de sus componentes, lo cual a su vez genera un impacto en la integridad, autenticidad, confidencialidad y disponibilidad de la información (CSIRT, 2018). Dicha actividad se hace de forma premeditada por el atacante definiendo el objetivo del ataque, el cual puede ser un usuario directo del sistema o algún actor externo a este. Cabe destacar que muchos ataques a su vez pueden tener un impacto es más de uno de los pilares definidos por lo que, una actividad que, aunque haya sido premeditada y con un objetivo fijo, no logre vulnerar los pilares, simplemente quedara como un intento de ataque (Gútiérrez, 2020). Con esta definición del concepto de ataque, se debe contemplar precisamente los ataques que tienen un impacto en dos de los pilares de los sistemas de información: la confidencialidad y la autenticidad de la información. A continuación, se definirán estos grupos de ataques y los tipos de ataques dentro de estos.

## Ataques contra el secreto o la confidencialidad

Cuando hablamos de la información que se manipula dentro de un sistema, una de las cualidades que principalmente queremos darle a dicha información es la confidencialidad de la información, es decir, que alguien sin autorización tenga acceso a información delicada. Un ejemplo directamente citable es la información que maneja una entidad tales como números de cuenta, documentos de sus clientes, contraseñas y claves de acceso, aquí se debe contemplar no solo los datos de los clientes, sino de los empleados o miembros de la entidad. Con este ejemplo se deja en claro la importancia de la confidencialidad dentro de un sistema, la cual se puede garantizar por medio de políticas de seguridad para la manipulación de los datos, el acceso a estos e implementación de medidas de seguridad en el software y hardware con el que se manipula la información (Gutiérrez et al., 2005). Pero, no olvidemos que un sistema nunca podrá ser 100% seguro, y, en el caso de la confidencialidad de la información, podemos encontrar los siguientes tipos de ataques que atenten ten contra esta cualidad de la información y de los sistemas que la manipulan:

1. **Acceso no autorizado a recursos:** este tipo de ataques se caracteriza por como un actor, sea interno o externo al sistema, logra hacerse con los medios que le permitan acceder a alguno de los recursos dentro de un sistema sin tener el permiso de los propietarios, administradores o responsables de este. Al tener acceso a dicho recurso o activo de información, dicho actor genera un impacto en la confidencialidad que tenía la información que residía o a la cual permitía tener acceso dicho recurso. Se puede definir que este tipo de ataques, inicialmente vulneran la confidencialidad de la información, pero, al tener dicho acceso y lograr ciertos privilegios sobre los recursos y la información, se puede vulnerar la integridad, disponibilidad y autenticidad de la información (Gómez Vieites, 2019). Como ejemplos de este tipo de ataques tenemos los siguientes:

- Un ciberdelincuente logra tener acceso al servidor de base de datos de una empresa de contabilidad, esto por medio de una vulnerabilidad que le permitió ejecutar código de forma remota y obtener los privilegios de usuario que le permitieron acceder al servidor y a la base de datos que residía en este. En este ejemplo se puede definir

que el actor es externo al sistema y el recurso al que accedió sin autorización fue la base de datos.

- Un empleado logro tener acceso a un archivo delicado el cual se encontraba almacenado en el equipo de su jefe, esto con el fin de vender la información dentro del archivo a un tercero. En este ejemplo se puede definir que el actor es interno al sistema y el recurso al que accedió sin autorización el equipo de su jefe.



*Ilustración 1 Un atacante accediendo a un sistema por un archivo*

2. **Ingeniería social:** este tipo de ataques contra la confidencialidad de la información se basan en aprovechar la vulnerabilidad que representan los usuarios o actores humanos dentro de un sistema, los cuales pueden acceder a la información o son poseedores de esta, todo por medio de herramientas de manipulación de psicológica, o, en otras palabras, engañando a las personas. Los ataques de ingeniería se pueden realizar por medios tecnológicos, como llamadas telefónicas, mensajes de texto o instantáneos, redes sociales, correo electrónico y hasta de forma presencial. El objetivo de estos ataques es aprovechar a las personas sin requerir en la intrusión al sistema aprovechando vulnerabilidades asociadas a este o a alguno de sus componentes de software o hardware (Gomez & BBVA, 2018). Como ejemplo de estos ataques se pueden exponer los siguientes:

- Una persona recibe una llamada de su “entidad bancaria”, en la cual se le pedían sus datos personales y credenciales bancarias esto con la premisa de que se estaba

actualizando el sistema y se habían perdido sus datos. A los pocos días, esta persona se dio cuenta que su cuenta se encontraba vacía, por lo que acudió a una sucursal de dicha entidad, en donde le notificaron que, la persona que la llamo no era empleada del banco y que, por ende, esta había sido quien se robó su dinero. Este tipo de ataque se llama *vishing*, en el cual se usan las llamadas telefónicas como medio para valerse de la información.

- Un señor estaba revisando su bandeja de correo electrónico en su trabajo, y en esta se encontró un mensaje de uno de sus “superiores” el cual le pedía una documentación importante y de carácter privado de la empresa. El mensaje dejo inquietado al señor, y por miedo a ser despedido, envió el documento sin consultar a sus compañeros. A los pocos días, el señor se encontraba hablando con sus compañeros y menciona lo anteriormente ocurrido, y estos le notificaron que, dentro de la empresa no había ningún superior con el nombre que se identificaba el supuesto superior, por lo que el señor tuvo que avisarles a sus jefes el inconveniente. Este ejemplo es un ejemplo claro de *phishing*, los cuales se basan en ataques por correo electrónico.



*Ilustración 2 Ataques de ingeniería social = suplantación y engaños*

3. **Software malicioso:** este tipo de ataque se refiere a cualquier programa, secuencia de códigos o software desplegado por un atacante hacia o dentro de un sistema con el fin de aprovechar una vulnerabilidad existente en este y obtener acceso a la información o obtener el control de esto o de algún activo de información. El software malicioso es en realidad un

tipo de ataque que puede afectar cualquiera de los pilares de la información, pero, específicamente en el caso de la confidencialidad, si el software le permite al atacante de valerse de información a la cual no debería tener acceso, es ahí donde se ve vulnerado este pilar (Reyes, 2021). Como ejemplo de estos ataques se pueden exponer los siguientes:

- Un atacante de forma remota ejecuta código que le permite tener acceso al servidor de archivos de una empresa en el cual se almacena información delicada sobre las finanzas de la empresa.
- El caso de Pegasus por medio del cual se valieron al acceso de los dispositivos móviles de varios periodistas y personas de interés alrededor del mundo por medio de enlaces enviados por mensajes de texto, emails o mensajería instantánea. (Reyes, 2021)



*Ilustración 3 los ataques de malware son de los más conocidos*

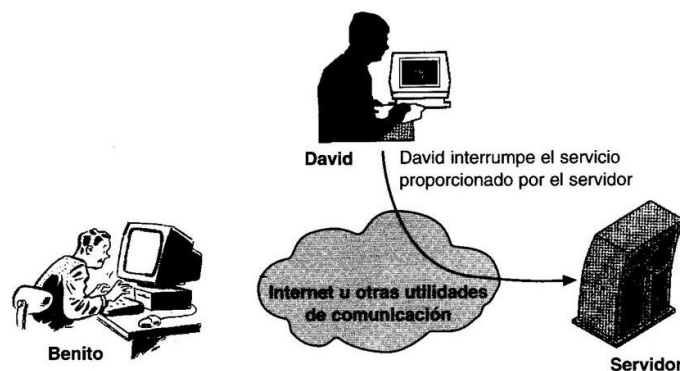
### Ataques contra la autenticidad

Continuando con los ataques que atentan contra los pilares de la seguridad de la información, se debe mencionar precisamente la autenticidad de la información, lo cual se relaciona con garantizarle a los usuarios de la información que esta proviene de fuentes confiables y que la información a su vez no haya sufrido modificaciones que le quiten este valor. Siguiendo con el ejemplo anterior de la entidad bancaria, la entidad debe tener en cuenta que los datos que sus clientes y empleados le entreguen deben ser reales, ya que esto es critico para que las actividades de la entidad también sean autenticas y le representen a los clientes y a la entidad

confianza en las actividades y servicios. Para garantizar esta cualidad de la información, la entidad se puede valer de consultas a bases de datos en los cuales validen que la información que están usando si es autentica, un ejemplo de esto puede ser como las entidades bancarias usan bases de datos que almacenan información de las personas, relacionadas con su información básica y su estado financiero con otras entidades (LOPEZ FUENTES, 2015). Con base a lo anteriormente expuesto, se exponen los siguientes tipos de ataques contra la autenticidad de la información:

1. **Interrupción:** este tipo de ataques se enfocan en como se obstaculiza el flujo de la información dentro de un sistema o se logra detener el funcionamiento de un servicio, esto con el fin de lograr valerse con la información y controlar como esta se mueve por el sistema y como esta llegara al destino al que originalmente debía llegar. No solo se define la interrupción sino el objetivo de esta, lo cual puede derivar en la modificación de la información y restablecer el flujo de la información, o simplemente limitar el acceso a esta (LOPEZ FUENTES, 2015; Vega, 2021). A continuación, se expone un ejemplo de este tipo de ataques:

- Uno de los empleados de una empresa recibió un pago para dañar la red de comunicaciones de una empresa, por lo que decidió cortar los cables de red de los computadores que permiten la comunicación entre los empleados y el jefe.

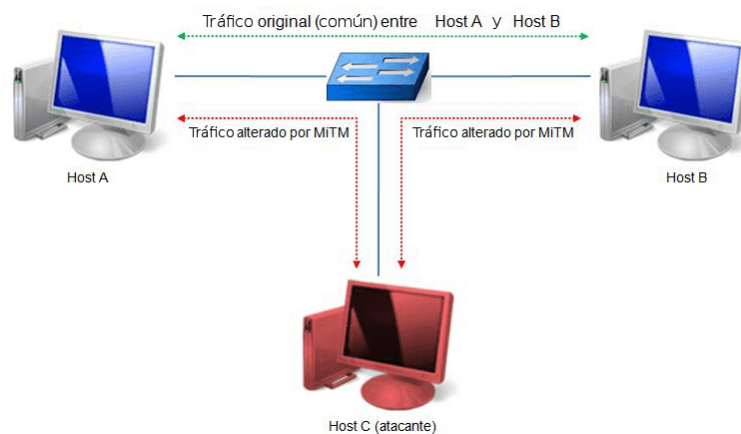


*Ilustración 4 Ejemplo de un ataque de interrupción*



2. **Intercepción:** este tipo de ataques hace relación a cualquier actividad la cual añade un nuevo destino al cual la información también ira a parar al momento de que esta sea enviada por parte de los emisores de esta. El actor que intercepta la información puede ser un programa, un equipo o una persona, el objetivo de la interceptación es valerse de la información para poder realizar cualquier acción que vulnere su autenticidad (LOPEZ FUENTES, 2015; Vega, 2021). Un ejemplo de este tipo de ataques es el siguiente:

- Un atacante ejecuto un código de forma remota el cual le permitió añadir su dirección IP para recibir toda la información que era enviada desde el servidor de una entidad bancaria.



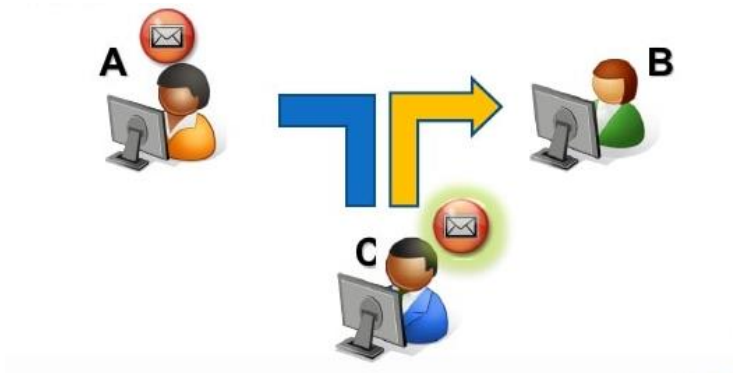
*Ilustración 5 Ejemplo de un ataque de interceptación*

3. **Modificación:** este tipo de ataques define cualquier ataque el cual, después de obtener acceso a la información, la comienza a modificar, sea por medio de un acceso directo a la información, una interceptación de esta o cualquier medio. El objetivo de este tipo de ataques es dañar la fiabilidad de la información y a su vez dañar las operaciones que se realizan con esta dentro del sistema (LOPEZ FUENTES, 2015; Vega, 2021). Un ejemplo de este tipo de ataques es el siguiente:

- Un atacante logro ingresar al servidor de una base de datos, el cual enviar información por medio del protocolo HTTP a la central de una empresa, y para dañar las operaciones de esta, instalo un programa el cual recibe la información y, aunque esta



este encriptada, modifica caracteres de los datos enviados y finalmente los envía al destinatario original, de modo tal, las actividades de la empresa se estropean.



*Ilustración 6 Ejemplo de un ataque de modificación*

4. **Suplantación:** este tipo de ataques se enfoca en las fuentes y destino de los datos, en donde el atacante suplanta la identidad de alguno de estos, con el objetivo de enviar información falsa y a su vez obtener información. La suplantación o fabricación puede ser desde la suplantación de usuarios o recursos del sistema, los cuales reciben o envían información requerida en las actividades dentro del sistema (LOPEZ FUENTES, 2015; Vega, 2021). Un ejemplo de este tipo de ataques es el siguiente:

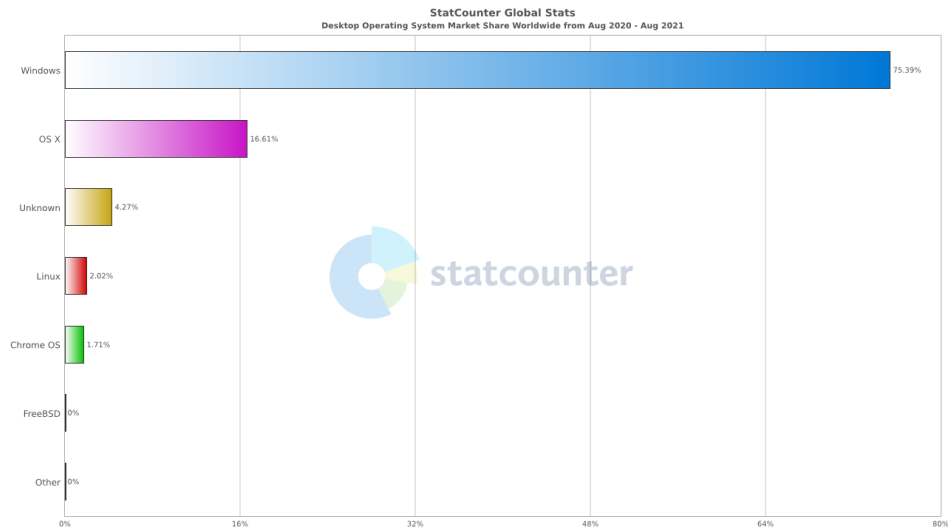
- Una persona deja abierta la cuenta de una de sus redes sociales en un computador de un café internet, y al cabo de un rato llega otra persona a usar el mismo computador, la cual, aprovecha la oportunidad para hacerse pasar por el propietario de la cuenta y comienza a pedirle dinero a los contactos de esa persona para que se lo consignen en una cuenta.



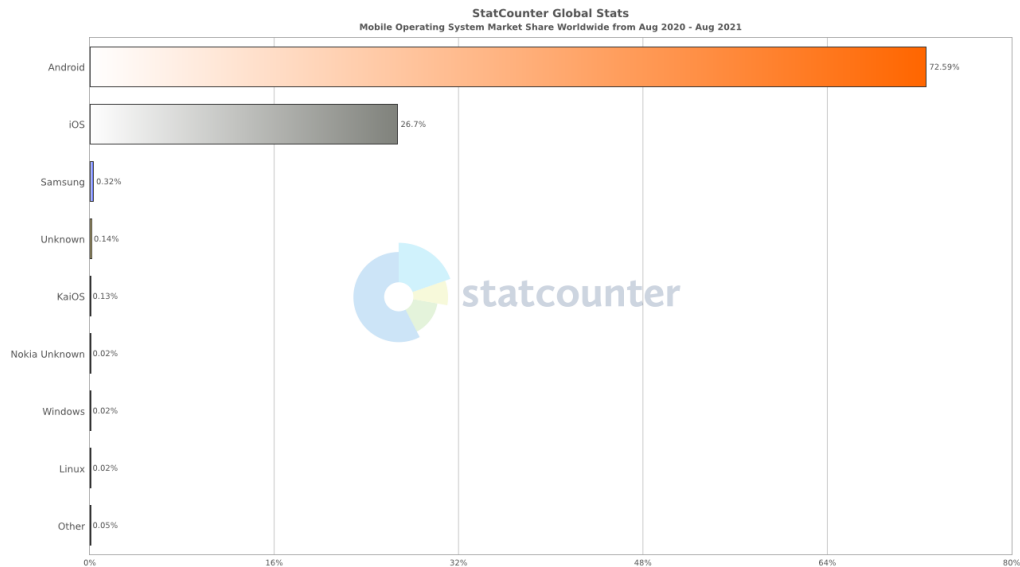
*Ilustración 7 suplantación de identidad digital*

## 2. Vulnerabilidades de sistemas operativos

Continuando con el tema de las vulnerabilidades, recordemos que previamente se habló de la definición de este concepto, su relación otros como el de amenaza y riesgo, y se enfocó en la exposición del top 10 de vulnerabilidades en aplicaciones web presentado por la OWASP (OWASP, 2017) el cual, como adicional no relacionado con este punto, estos días tuvo su actualización del 2021 (OWASP, 2021). Con esta introducción enlazando trabajos previos, ahora nos enfocaremos en exponer las vulnerabilidades a las que se encuentran expuestos los principales sistemas operativos en la actualidad, viendo como cada una de las empresas propietarias de estos manejan las vulnerabilidades en las versiones más recientes de uno de los componentes de software más importantes en los dispositivos y máquinas que usamos diariamente. Antes de ahondar en las vulnerabilidades, me gustaría destacar la información expuesta por (Statcounter, 2021a, 2021b) en donde se nos expone datos estadísticos con relación a los sistemas operativos más usados en la actualidad, tanto en computadores de escritorio como en dispositivos móviles, siendo esto un factor determinante con relación a las vulnerabilidades, ya que, un sistema con muchos usuarios y con vulnerabilidades es una gran oportunidad para los ciberdelincuentes en sus actividades, y estos personajes precisamente se encuentran día a día informándose de las vulnerabilidades existentes en dichos sistemas operativos, siendo las siguientes imágenes gráficas de interés.



*Ilustración 8 Sistemas operativos para computadores de escritorio más usados en el último año*



*Ilustración 9 Sistemas operativos para dispositivos móviles más usados en el último año*

La imagen anterior nos expone como, para los ciberdelincuentes, Windows y su familia de sistemas operativos, son una gran oportunidad para desplegar sus ataques, siendo este sistema uno de los más usados en organizaciones y empresas alrededor del mundo, además de ser el más empleado en computadores de consumo comercial, por lo que Microsoft como compañía



propietaria de Windows tienen una gran responsabilidad con la seguridad de sus usuarios. Por otro lado, en la siguiente imagen, se expone otro dato de vital importancia con relación a los sistemas operativos más usados en dispositivos móviles, siendo el líder en esta lista Android, por lo que otra vez se debe recalcar la responsabilidad de Google como compañía propietaria y a las empresas desarrolladoras de dispositivos móviles que emplean este sistema operativo sobre la seguridad de sus usuarios. En base a lo anterior, de cada uno de los sistemas operativos se expondrán tres de las vulnerabilidades existentes en estos, brindando información extraída del NVD y demás fuentes que soporten por qué cada vulnerabilidad requiere demuestratención, no solo como usuarios de estos sistemas operativos, sino como futuros responsables de la seguridad de los sistemas a los que tendremos acceso.

**NOTA:** la mayoría de las vulnerabilidades a exponer actualmente cuentan con parches de seguridad parciales o completos entregados por medio de las actualizaciones de cada sistema operativo.

## Windows

Esta familia de distribuciones de sistemas operativos, principalmente para computadores de escritorio, desarrollado por la compañía de tecnología Microsoft y lanzado al mercado en 1985, es por lejos el sistema operativo más usado en la actualidad, según (Ramirez, 2020; Statcounter, 2021a), cubriendo un 75.39% del mercado actual. Y precisamente por ser uno de los sistemas operativos más usados, que se ha enfocado principalmente en su apartado de interfaz gráfica, es a su vez el grupo de sistemas operativos con más vulnerabilidades, y aunque en la actualidad Microsoft buscan parchear regularmente las vulnerabilidades detectadas en los sistemas operativos que aún tienen soporte técnico por parte de la compañía, las actualizaciones por medio de las que se busca este objetivo pueden llegar a ser problemáticas, siendo esto una experiencia propia con el uso de Windows 10 y sus actualizaciones. A continuación, se expondrán tres de las vulnerabilidades existentes en las últimas versiones del sistema operativo Windows 10.

CVE	CVE-2021-40444
-----	----------------



Servicio afectado	MSHTML
Puntaje	7.8 (Alto)
Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Descripción	
Vulnerabilidad que permite la ejecución remota de código por medio de MSHTML(Trident), el cual es el motor del navegador Internet Explorer integrado de varias distribuciones de Windows y que empleado para los componentes de conectividad externa de las aplicaciones de Office, aprovechando precisamente a Office por medio de documentos los cuales creen un control Active X y permitan tomar el control de la maquina infectada. (Háran & ESET, 2021)	
Exploit	<a href="https://github.com/lockedbyte/CVE-2021-40444">https://github.com/lockedbyte/CVE-2021-40444</a>
URL	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-40444">https://nvd.nist.gov/vuln/detail/CVE-2021-40444</a>

Ilustración 10 Descripción de vulnerabilidad CVE-2021-40444

CVE	CVE-2021-34494
Servicio afectado	Servidor DNS
Puntaje	8.8 (Alto)
Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Descripción	
Vulnerabilidad que permite la ejecución remota de código por medio del servidor DNS integrado en varias distribuciones del sistema operativo Windows, la gravedad que representa esta vulnerabilidad reside en como un atacante podrá aprovechar un puerto que se mantiene en escucha y que, bajo ciertas condiciones del usuario del equipo y de la red, se le permitirá la ejecución de código sin que se requiera la interacción del usuario.	
URL	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-34494">https://nvd.nist.gov/vuln/detail/CVE-2021-34494</a>

Ilustración 11 Descripción de vulnerabilidad CVE-2021-34494

CVE	CVE-2021-34458
Servicio afectado	Kernel de Windows
Puntaje	9.9 (Critico)
Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Descripción	
Esta vulnerabilidad de ejecución remota de código del kernel de Windows se enfoca en los equipos que alojen máquinas virtuales los cuales se apoyen en dispositivos de virtualización de entrada y salida, por medio de los cuales, un software de virtualización, dividen en varios puertos uno o varios de los puertos de la maquina host para que sean empleados por la maquina huésped. Lo recomendado para la prevención de un ataque por medio de esta vulnerabilidad es actualizar el software de virtualización y comprobar las actualizaciones de Windows en las cuales se pueden encontrar parches para esta vulnerabilidad.	
URL	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-34458">https://nvd.nist.gov/vuln/detail/CVE-2021-34458</a>

Ilustración 12 Descripción de vulnerabilidad CVE-2021-34458

## MacOS - OSX

Siendo este el segundo sistema operativo más usado en computadores de escritorio con, según (Statcounter, 2021b), un 16.61% de dispositivos, distribuido y creado por Apple, este sistema operativo lanzado en el 2001, se ha caracterizado por reunir la implementación de una interfaz grafica muy amigable con el usuario y un sistema de seguridad robusto, pudiendo resaltar como una de sus características las limitaciones en la instalación de software el cual no se encuentre avalado y firmado digitalmente, lo cual a su vez lo vuelve un sistema muy hermético el cual le sus usuarios seguridad y rendimiento. Las vulnerabilidades que regularmente se reportan en este sistema se asocian a elementos nuevos integrados en sus actualizaciones, comúnmente clasificadas como vulnerabilidades de día cero (Fernández, 2015), es decir, estas vulnerabilidades son detectadas por terceros, más no por los usuarios y/o la empresa propietaria del sistema, y aunque este tipo de vulnerabilidades son un problema evidente, Apple

trabaja regularmente en la identificación de las vulnerabilidades, parchándolas lo más pronto posible. Con base al documento de soporte de seguridad de Apple para la última versión de macOS (Apple Inc., 2021), se pueden exponer las siguientes vulnerabilidades recientemente descubiertas y parcheadas:

CVE	CVE-2021-30860
Servicio afectado	CoreGraphics
Puntaje	7.8
Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Descripción	
<p>Esta vulnerabilidad de ejecución de código remoto se encuentra en el navegador Safari, los dispositivos móviles con iOS y el sistema operativo macOS en los cuales se encuentra implementado el componente CoreGraphics el cual se encuentra encargado de la parte grafica del despliegue de archivos y paginas web, siendo explotada principalmente por archivos PDF en los cuales se encuentra el Payload que permite la ejecución del código diseñado para el ataque que busca el desbordamiento del buffer. Esta vulnerabilidad cuenta con un parche brindado en las actualizaciones de los siguientes dispositivos: iPhone 5s, iPhone 6, iPhone 6 Plus, iPad Air, iPad mini 2, iPad mini 3, iPod touch de sexta generación y computadores de escritorio con macOS Big Sur y macOS Catalina. (Apple, 2021; Ministerio del Interior y Seguridad &amp; CSIRT, 2021)</p>	
URL	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-30860">https://nvd.nist.gov/vuln/detail/CVE-2021-30860</a>

*Ilustración 13 Descripción de vulnerabilidad CVE-2021-30860*

CVE	CVE -2021-30657
Servicio afectado	Gatekeeper
Puntaje	5.5



Vector	CVSS:3.1/AV:L/AC:L/PR:N/UI:R/S:U/C:N/I:H/A:N
Descripción	
<p>Dentro del sistema operativo macOS en su versión Big Sur 11.3 y demás distribuciones anteriores se encuentra implementado una Gatekeeper el cual se encarga de la comprobación de la fiabilidad y seguridad de los programas que se instalan, por lo que, esta vulnerabilidad se halla en este componente permitiéndole a un atacante saltar la revisión que realiza Gatekeeper y de esta forma instalar programas potencialmente peligrosos creados con código el cual permite omitir la validación (ZK Hacking, 2021).</p>	
URL	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-30657">https://nvd.nist.gov/vuln/detail/CVE-2021-30657</a>

Ilustración 14 Descripción de vulnerabilidad CVE -2021-30657

CVE	CVE-2021-30858
Servicio afectado	WebKit
Puntaje	8.8
Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H
Descripción	
<p>Vulnerabilidad del día cero de desbordamiento de buffer en una función del componente Webkit incluida en el sistema operativo masOS en su versión 11.5.2 y iOS en su versión 14.7.1, la cual, por medio de la ejecución de código incrustado en un sitio web enfocado en la modificación del input generando un daño en el dispositivo con el desbordamiento del buffer. Esta vulnerabilidad ya cuenta con un parche incluido en las ultimas actualizaciones para los sistemas operativos mencionados. (Apple Inc., 2021; Aranda, 2021)</p>	
URL	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-30858">https://nvd.nist.gov/vuln/detail/CVE-2021-30858</a>

Ilustración 15 Descripción de vulnerabilidad CVE-2021-30858

## Linux – GNU/Linux

Linux como conjunto de distribuciones de sistema operativo, desarrollado por Linus Torvalds en 1991, es uno caso especial dentro de los sistemas operativos que se exponen en este punto. Con base a (Statcounter, 2021a) se debe recalcar que es usado solo 2.02% de los computadores de escritorio, pero esta cifra puede estar muy lejos de la realidad ya que Linux al ser un sistema operativo Open-source ha desglosado en una infinidad de variaciones realizadas por la comunidad, y, aunque no es muy usado en el entorno comercial, es empleado en la mayoría de los proyectos relacionados con la seguridad. Es un sistema operativo muy liviano, contando con distribuciones que trabajan con pocos requerimientos de hardware y siendo ideal para procesos de virtualización, instancias de CM en la nube y uso de contenedores. Este sistema operativo y sus distribuciones han sido analizados por Trend Micro, empresa de ciberseguridad multinacional estadounidense- japonesa, entregando un listado en el cual se exponen las siguientes vulnerabilidades en Linux (Logan et al., 2021):

CVE	CVE-2017-5638
Servicio afectado	Apache Struts
Puntaje	10.0 (Critico)
Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Descripción	
Vulnerabilidad de ejecución de código de forma remota por medio de los servidores con Apache Struts, todo por medio del protocolo HTTP, lo cual deja en total desprotección a los datos almacenados en el servidor o a los cuales este tienen acceso, siendo esta una vulnerabilidad que desde el 2017, y aun contando con un parche, ha generado grandes problemas en la seguridad, tal cual como en el caso Equifax, en donde los atacantes explotaron esta vulnerabilidad y lograron comprometer los datos de 143 millones de usuarios (Varmazis, 2017).	

Exploit	<a href="https://www.hackplayers.com/2017/03/exploit-rce-para-apache-struts-cve-2017-5638.html">https://www.hackplayers.com/2017/03/exploit-rce-para-apache-struts-cve-2017-5638.html</a>
URL	<a href="https://nvd.nist.gov/vuln/detail/CVE-2017-5638">https://nvd.nist.gov/vuln/detail/CVE-2017-5638</a>

Ilustración 16 Descripción de vulnerabilidad CVE-2017-5638

CVE	CVE-2018-7600
Servicio afectado	Drupal
Puntaje	9.8
Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Descripción	
Vulnerabilidad de escalada de privilegios la cual emplea una función implementada en Drupal (sistema para la gestión de contenido que permite la creación de páginas web similar a WordPress) la cual permite la alteración del input sobre la maquina y de esta forma permitir obtener permisos de acceso al servidor.	
Exploit	<a href="https://www.exploit-db.com/exploits/44482">https://www.exploit-db.com/exploits/44482</a> <a href="https://github.com/pimps/CVE-2018-7600">https://github.com/pimps/CVE-2018-7600</a>
URL	<a href="https://nvd.nist.gov/vuln/detail/CVE-2018-7600">https://nvd.nist.gov/vuln/detail/CVE-2018-7600</a>

Ilustración 17 Descripción de vulnerabilidad CVE-2018-7600

CVE	CVE-2020-25213
Servicio afectado	File manager de WordPress
Puntaje	9.8 (Critico)
Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Descripción	

Vulnerabilidad de ejecución remota de código PHP aprovechando el componente de administrador de archivos de WordPress, en el cual se encuentra el archivo conector elFinder, el cual, por medio del código ejecutado por el atacante se puede cambiar el nombre de este y crear un archivo que suplante el archivo anterior y cargar en estas instrucciones que permitan al atacante obtener privilegios dentro del servidor.

Exploit	<a href="https://github.com/mansoorr123/wp-file-manager-CVE-2020-25213">https://github.com/mansoorr123/wp-file-manager-CVE-2020-25213</a>
URL	<a href="https://nvd.nist.gov/vuln/detail/CVE-2020-25213">https://nvd.nist.gov/vuln/detail/CVE-2020-25213</a>

*Ilustración 18 Descripción de vulnerabilidad CVE-2020-25213*

## Android

Con el nacimiento de los dispositivos móviles, a lo largo de los años hemos visto ir y venir sistemas operativos cada uno acorde a las especificaciones del dispositivo, desde los primeros teléfonos móviles con teclas y un sistema operativo simple, hasta la aparición de Android en el 2008 de forma masiva, desarrollado inicialmente por Andy Rubin, Rich Miner, Nick Sears, y Christopher White, y finalmente comprado por Google, el cual es un sistema operativo basado en el núcleo de Linux y que cuenta con una configuración base para dispositivos con pantallas táctiles se ha masificado de tal manera que, en la actualidad, supera a sistemas operativos como Windows, OS X o iOS, posicionándose en el primer lugar de los sistemas operativos empleados en dispositivos con el 32.76% (Statcounter, 2021c), esto debido principalmente a cómo, en los últimos 10 años, se ha presentado una masificación en las comunicaciones móviles alrededor del mundo. Cabe resaltar que, con diferencia a iOS el cual es un sistema operativo dedicado únicamente a los dispositivos móviles de Apple, Android se encuentra desplegado en la mayoría de los dispositivos móviles desarrollados por otras compañías, como Samsung, Motorola o Xiaomi, de modo tal, no solo se contempla en este caso a Android como sistema operativo sino a todas las capas de personalización que cada compañía implementa sobre Android para sus dispositivos. A continuación, se expondrán algunas de las principales vulnerabilidades actuales presentes en los dispositivos en donde se encuentra Android como sistema operativo:

CVE	CVE-2021-1905
Servicio afectado	GPU de dispositivos con procesador Qualcomm Snapdragon y ARM
Puntaje	7.8 (Alto)
Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Descripción	
Vulnerabilidad de escalada de privilegios que le permite a los atacantes aprovechar la GPU de los dispositivos con los procesadores mencionados, de modo tal, el atacante puede aprovechar esta vulnerabilidad por medio de aplicaciones con código malicioso que les permitan tomar el control del dispositivo de forma remota.	
URL	<a href="https://nvd.nist.gov/vuln/detail/cve-2021-1905">https://nvd.nist.gov/vuln/detail/cve-2021-1905</a>

Ilustración 19 Descripción de vulnerabilidad CVE-2021-1905

CVE	CVE-2021-24026
Servicio afectado	WhatsApp para Android V2.21.3
Puntaje	9.8 (critico)
Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Descripción	
Esta vulnerabilidad se enfoca en el apartado de llamadas de voz, en las cuales un atacante puede ejecutar de forma remota un audio especialmente diseñado que permita desencadenar el desbordamiento del buffer del dispositivo y/o ejecutar código malicioso que permita al atacante tomar el control del dispositivo de forma remota. Se puede considerar a esta vulnerabilidad como la ejecución de código de forma remota (CSIRT, 2021)	
URL	<a href="https://nvd.nist.gov/vuln/detail/CVE-2021-24026">https://nvd.nist.gov/vuln/detail/CVE-2021-24026</a>

Ilustración 20 Descripción de vulnerabilidad CVE-2021-24026

CVE	CVE-2020-11261
Servicio afectado	Dispositivos con procesadores Qualcomm Snapdragon
Puntaje	7.8 (Alto)
Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H
Descripción	
Esta vulnerabilidad le permite al atacante el daño del sistema generando un problema de validación de entrada, esto por medio de una aplicación con código malicioso que le exija al dispositivo que le reserve un gran espacio en la memoria. Los ataques que se realizan explotando esta vulnerabilidad son de tipo local y dirigidos, requiriendo tener acceso físico al dispositivo objetivo o infectando una pagina web a la que se sepa que el usuario del dispositivo tiene acceso comúnmente.	
URL	<a href="https://nvd.nist.gov/vuln/detail/CVE-2020-11261">https://nvd.nist.gov/vuln/detail/CVE-2020-11261</a>

Ilustración 21 Descripción de vulnerabilidad CVE-2020-11261

### 3. Repositorios de máquinas para Pentesting

Dentro del contexto de la tecnología, sea en el ámbito del desarrollo de software o la ciberseguridad, es importante tener presente que podemos recoger mucha información, pero el valor de esta se obtendrá al momento de ponerlo en práctica, y al momento de centrarnos en la seguridad de los sistemas de información es de vital importancia el saber y hacer. Ejemplo de la importancia de estos conceptos son los repositorios de información relacionada con vulnerabilidades, amenazas y exploits, los cuales recopilan datos de vital importancia para saber cómo actuar frente a estos conceptos materializados en el mundo real. Pero estos repositorios siguen siendo fuente de información, por lo que aquí es donde entra en juego los repositorios de máquinas o software con vulnerabilidades, por medio de los cuales se puede poner en práctica las habilidades relacionadas con el Pentesting y la información sobre vulnerabilidades presentes en los sistemas (Frias, 2020; Paus, 2016). A continuación, se va a exponer información sobre **Hack The box**, uno de los repositorios más conocidos, y otras



opciones similares que nos ayuden a poner en practica todo lo que aprendimos sobre vulnerabilidades:

## Hack The Box

Fundada por el ingeniero y desarrollador web Haris Pylarinos en 2017, Hack The box o HTB es una de las plataformas más completas en las cuales se reúne una comunidad de hackers e interesados en la ciberseguridad para poner a prueba sus habilidades mediante el repositorio de máquinas con vulnerabilidades y distintos sistemas operativos (Windows, Linux, Android, etc.) creadas por los mismos miembros de la comunidad. El llamativo de esta plataforma radica en la implementación de gamificación (uso de métodos y elementos propios de los juegos) por medio del uso de puntajes, clasificaciones y listados que obtienen cada uno de los usuarios al cumplir con el objetivo de tomar el control de cada maquina que se encuentre activa, también se debe mencionar la existencia de retos y eventos especiales que intensifican su curiosidad y ayuden a enriquecer sus habilidades y por último la forma en que se accede a las maquinas, las cuales solo requieren el uso de OpenVPN que permite la conexión a la máquina, por lo que no se requiere de la instalación completa de la instancia. Hack The Box es una gran opción si se quiere poner a prueba sus habilidades de Pentesting e instrucción a sistemas, ya que cuenta con una comunidad y material de ayuda que le permitirá familiarizarse con la plataforma, sus funcionalidades y recursos. (Frias, 2020; Hack The Box, 2021)

Para acceder a Hack The Box, dar clic [aquí](#), cree su cuenta y comience a descubrir la plataforma que le permitirá poner en práctica sus habilidades en un entorno seguro y simulado, además de presentar funcionalidades por medio de pago las cuales permiten acceder a un repertorio de máquinas y tener ciertas ventajas al momento de irrumpir en estas, como el control de acceso a la instancia en la que hayamos accedido. HackTheBox es la plataforma más recomendada, la cual hasta incluye apartados para estudiantes universitarios y empleados de compañías, en los cuales se brindan cursos acorde a las necesidades de este tipo de usuarios, siendo esto de gran ayuda para los interesados en prepararse para el mundo laboral.



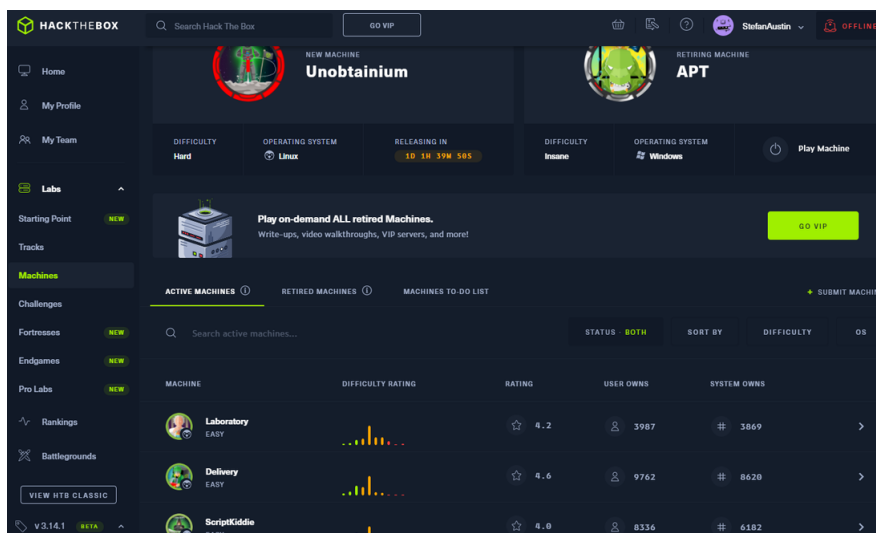


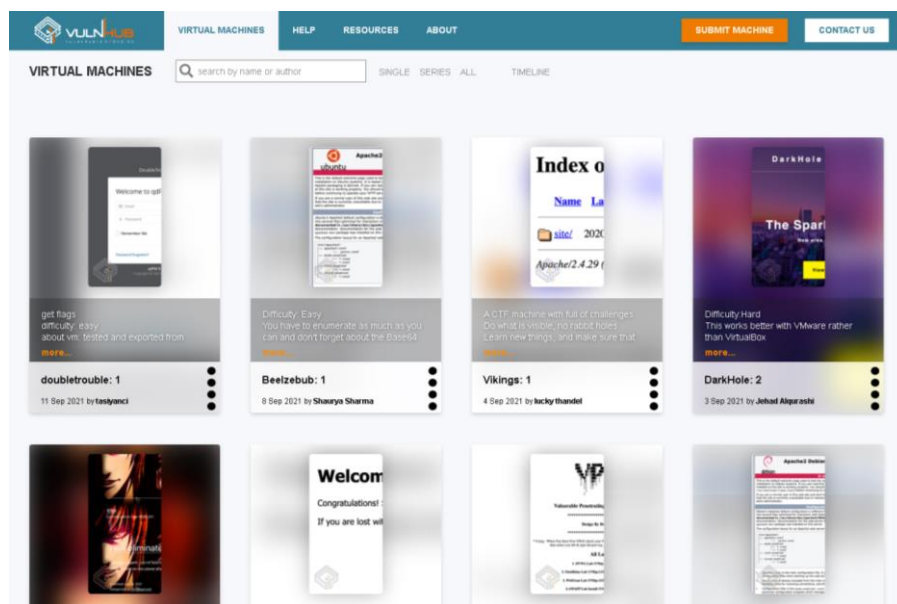
Ilustración 22 ejemplo del funcionamiento de HackTheBox

## VulnHub

La alternativa open-source se debe mencionar obligatoriamente a VulnHub, un repositorio de máquinas virtuales creado por g0tm1k y patrocinado por Offensive Security, misma organización que tienen en su repertorio de herramientas a Kali Linux, Exploit Database, Google hacking Database y entre otras herramientas enfocadas en la seguridad, Pentesting y hacking ético. Se puede decir que esta herramienta, a comparación de Hack the Box, es mucho más simple ya que almacena instancias de maquinas virtuales que pueden ser desplegadas por medio de software de virtualización como Oracle VirtualBox y de esta forma comenzar a realizar exploración y explotación de vulnerabilidades. Como tal, esta plataforma presenta como única funcionalidad el permitir descargar imágenes de VM, por otro lado, se debe destacar que cuenta con material de ayuda que ayudara en el proceso de instancia de las máquinas virtuales, pero, al ser una plataforma open-source y a la cual la comunidad es la que contribuye subiendo las máquinas virtuales, VulnHub como organización se exime de su responsabilidad sobre la calidad y seguridad de las maquinas virtuales a las que accedemos. (Frias, 2020; VulnHub, 2021)

Para acceder a VulnHub, dar clic [aquí](#), Cabe destacar que esta herramienta también se encuentra incluida en el catalogo de Kali Linux. VulnHub puede ser usado para poner a prueba

sus habilidades de ciberseguridad en sistemas y redes, pero cuenta con muchas desventajas como la poca fiabilidad de las maquinas con las que cuenta, la forma en que se accede a las máquinas y un sistema sin incentivos, esto hace poco atractivo el uso de VulnHub, pero lo importante es que permita el desarrollo de ejercicios de exploración, explotación y análisis de vulnerabilidades.



*Ilustración 23 Ejemplo del repositorio de VulnHub*

## TryHackMe

Volviendo con las plataformas que usan la gamificación como recurso que genere un mayor interés en los conceptos presentados, en el 2018 nació TryHackMe, la cual fue desarrollada por Ashu Savani y Ben Spring, quienes siendo estudiantes se preguntaron cómo podrían poner a prueba sus habilidades por medio de maquinas virtuales que se enviaban entre si o que alojaban en servidores, desde aquí, se comenzó a generar una plataforma la cual le permite a sus usuarios aprender por medio de ejercicios de intrusión a instancias de VM en la nube, de modo tal, se presentan maquinas con vulnerabilidades a las cuales se puede tener acceso por medio de VPN o AttackBox (herramienta en el navegador que permite realizar instrucción a la maquina desde el navegador). A parte de contar con un repositorio de maquinas en donde podemos

poner a prueba nuestras habilidades, también cuenta con cursos relacionados con distintos ámbitos de ciberseguridad, como redes, sistemas operativos y Pentesting, los cual son una gran ayuda para cualquier persona interesada en el tema en el camino para obtener mayor conocimiento. (Frias, 2020; TryHackMe, 2021)

Para acceder a TryHackMe, dar clic [aquí](#). Esta plataforma es una de las más contempla debido a como integra los ejercicios de instrucción a máquinas virtuales siendo un ambiente propicio para el aprendizaje tanto de principiantes como de personas con mucha más experiencia en los temas relacionados con el hacking ético y la ciberseguridad.

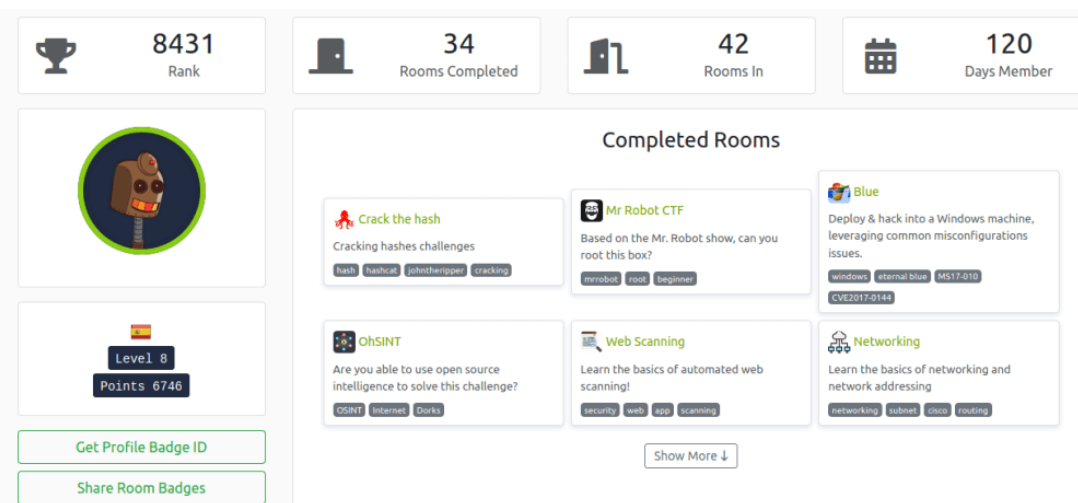


Ilustración 24 Ejemplo de funcionamiento de TryHackMe

## PentestIT

Esta plataforma en realidad es una simulación en tiempo real de los servidores de una compañía alrededor del mundo, la cual se encuentra lo más actualizada con las vulnerabilidades a las que se pueden enfrentar los sistemas en el mundo real, todo esto de forma legal y segura. Pestestit presenta laboratorios en los cuales se propone un escenario al cual se puede tener acceso por medio de la conexión a la VPN de la plataforma haciendo uso de OpenVPN ingresando el username con el cual nos encontramos identificados en la plataforma y una clave secreta dada por la misma, y, al estar dentro de dicha red virtual, se podrá acceder a cada uno de los laboratorios los cuales se identificados por medio de IPs. El propósito general de esta plataforma

es entregar un entorno lo más real y actualizado posible, el cual le permita a sus usuarios poner a prueba sus habilidades en distintos apartados del Pentesting como lo son el escaneo de vulnerabilidades, el análisis de redes, revisión de servicios alojados, implementación de herramientas, entre otros que se apeguen a las exigencias en ciberseguridad actuales (Paus, 2016; Pentestit, 2021).

Para acceder a Pentestit, dar clic [aquí](#). El progreso de cada uno de los usuarios en los laboratorios vigentes se basan en la recolección de tokens relacionados con distintos apartados y servicios que se encuentren alojados en las maquinas especificadas para cada laboratorio, por ejemplo, en el laboratorio de este año hay 23 tokens listos para la recolección de los usuarios, cada uno representando el uso de distintas habilidades y técnicas, y se puede deducir que la complejidad de los laboratorios es alta ya que se encuentra vigente un laboratorio por año, de modo tal, los usuarios que suman el reto de la recolección de tokens tendrán este tiempo para obtener la mayor cantidad de tokens posibles (Pentestit, 2021).

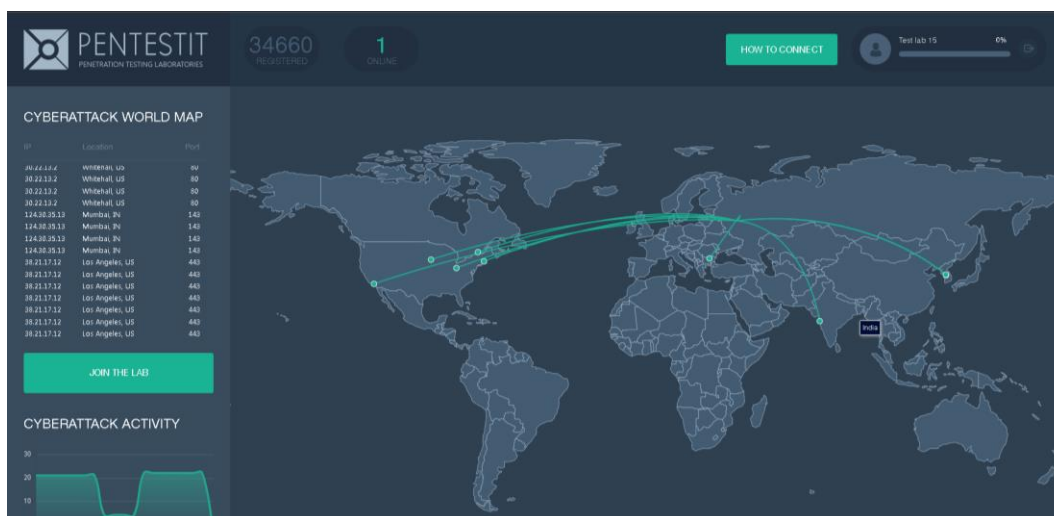


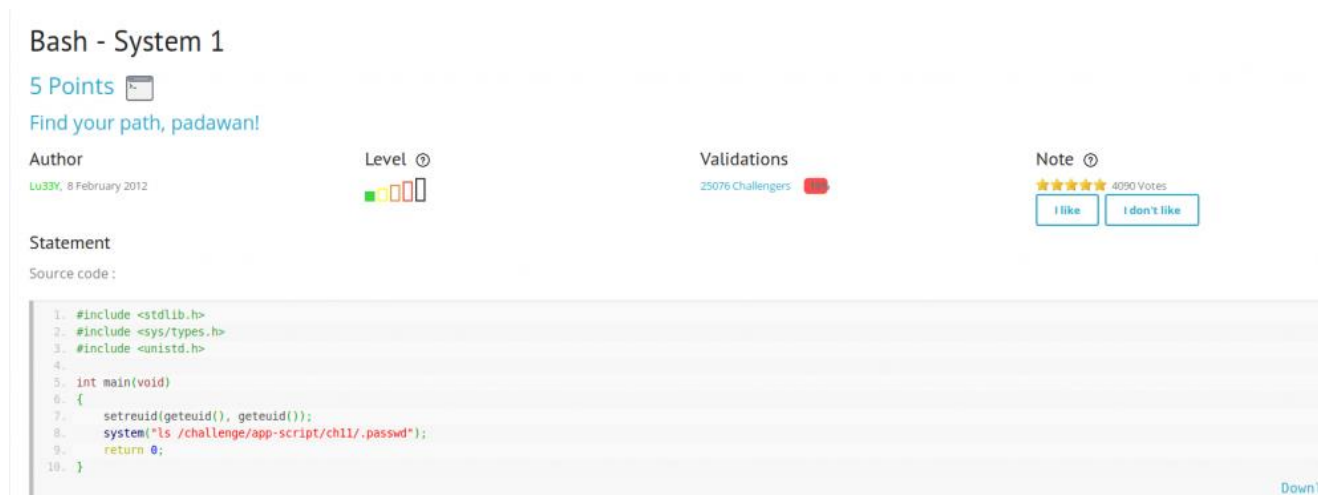
Ilustración 25 ejemplo de funcionamiento de PentestIT

## Root Me


Esta plataforma como tal no cuenta con maquinas virtuales o instancias de estas a las que tengamos que acceder, en cambio, se puede finir a Root Me como una plataforma que cuenta con distintos ejercicios relacionados con la instrucción a sistemas como servidores, redes o

sistemas criptográficos, en los cuales se nos define un objetivo, sea el obtener un dato en específico, como una contraseña alojada en un servidor, lo cual nos permitirá poner a prueba nuestras habilidades. Esta plataforma se soporta en el alojamiento de servidores y scripts en distintas plataformas o entornos virtuales como BlueBox, Vulnix, VulnVPN, entre otros, los cuales son invocados por medio de la IP o Hostname generado por el entorno, de modo tal solo se requiera este dato para poder comenzar a realizar la instrucción o la tarea especificada en cada ejercicio. Los ejercicios que presenta esta herramienta son variados, por lo que permite a personas con distintos niveles de conocimiento en muchos de los campos y aspectos de la ciberseguridad y el hacking ético el poder afianzar y ganar nuevas habilidades, además de tener como incentivo el recibir una puntuación por cada uno de los ejercicios resueltos y de esta forma poder aumentar su posición en la clasificación interna de la plataforma (Guillem, 2018).

Para acceder a RootMe, dar clic [aquí](#). Esta plataforma es una buena opción si se quiere acceder a ejercicios y actividades, como en la imagen anterior, en donde se nos exija pensar no solo enfocado en como acceder a un sistema, sino como podemos explotar las vulnerabilidades en distintos componentes de software, como programas, redes o servidores, y lo mejor aún, en un entorno seguro y gratuito, con una comunidad grande y en constante crecimiento y mejora de cada uno de sus apartados.





**Bash - System 1**


5 Points 

Find your path, padawan!

Author: Lu33ry, 8 February 2012

Level: 

Validations: 25076 Challengers 

Note:  4090 Votes

I like I don't like

Statement

Source code:




```
1. #include <stdlib.h>
2. #include <sys/types.h>
3. #include <unistd.h>
4.
5. int main(void)
6. {
7.     setreuid(geteuid(), geteuid());
8.     system("ls /challenge/app-script/ch1/.passwd");
9.     return 0;
10. }
```

Download

Ilustración 26 ejemplo de ejercicio de Root me

## Resumen de los repositorios

A continuación, se presentará una tabla con el resumen de la información de cada una de las plataformas expuestas, principalmente enfocándose en las maquinas, servidores e instancias a VM a los que permiten el acceso y los métodos de acceso definidos a las maquinas.

Nombre	Icono	Tipo de maquinas	Metodos de acceso	URL
<b>Hack The Box</b>		Instancias de VM en la nube	Por medio de OpenVPN y un archivo de configuración de acceso a la instancia	<a href="https://app.hackthebox.eu/">https://app.hackthebox.eu/</a>
<b>VulnHub</b>		Imágenes de máquinas virtuales	Descarga de los archivos de las maquinas virtuales para ser desplegadas en Oracle VM VirtualBox	<a href="https://www.vulnhub.com/">https://www.vulnhub.com/</a>
<b>Try Hack Me</b>		Instancias de VM en la nube	Por medio de VPN o una cliente Web con interfaz gráfica de la maquina	<a href="https://tryhackme.com/">https://tryhackme.com/</a>



<b>PentestIT</b>		Servidores o maquinas encapsuladas dentro de una red privada virtual	Acceso por medio de OpenVPN y las IPs definidas para cada laboratorio	<a href="https://lab.pentestit.ru/">https://lab.pentestit.ru/</a>
<b>Root Me</b>		Servidores alojados en distintos entornos y ubicaciones	Servicios de acceso por medio de VPN y uso de IPs o Hostnames, Ninguno de los servicios requiere de alguna instalación	<a href="https://www.root-me.org/?var_hasard=20712908396154edd1bfd1">https://www.root-me.org/?var_hasard=20712908396154edd1bfd1</a>

Ilustración 27 Tabla comparativa entre las plataformas expuestas

## Bibliografía

- Apple. (2021, September 23). *Acerca del contenido de seguridad de iOS 12.5.5*. Soporte Técnico de Apple (CO). <https://support.apple.com/es-co/HT212824>
- Apple Inc. (2021, September 13). *Acerca del contenido de seguridad de macOS Big Sur 11.6 - Soporte técnico de Apple (CO)*. Soporte de Apple. <https://support.apple.com/es-co/HT212804>
- Aranda, J. (2021, September 24). *Apple parchea varios zero-day que afectan a iPhone y Mac*. Una Al Día. <https://unaaldia.hispasec.com/2021/09/apple-parchea-varios-zero-day-que-afectan-a-iphone-y-mac.html>
- CSIRT. (2018). *CIBERATAQUES: LAS ESTRATEGIAS DELICTIVAS DEL MUNDO DIGITAL*.





[https://bacsirt.buenosaires.gob.ar/files/boletines/B46\\_AtquesCiberneticos.pdf](https://bacsirt.buenosaires.gob.ar/files/boletines/B46_AtquesCiberneticos.pdf)

CSIRT. (2021). *Alerta de Seguridad Cibernética.*

<https://www.csirt.gob.cl/media/2021/04/9VSA21-00420-01.pdf>

Fernández, C. (2015). *Definición de metodología para el descubrimiento del Zero Days*  
[UNIVERSIDAD DE ALCALÁ].

<https://ebuah.uah.es/dspace/bitstream/handle/10017/22752/> TFG Fernández Rivas  
2015.pdf?sequence=1&isAllowed=y#:~:text=Exploit es un fragmento de,comportamiento  
no deseado del mismo.

Frias, M. (2020, November 23). *Plataformas para practicar y aprender hacking ético.*  
OpenWebinars. <https://openwebinars.net/blog/plataformas-para-practicar-y-aprender-hacking-etico/>

Gomez, A., & BBVA. (2018, January 8). *Ataques de ingeniería social: qué son y cómo evitarlos.*  
BBVA. <https://www.bbva.com/es/ataques-ingenieria-social-evitarlos/>

Gómez Vieites, Á. (2019). *TIPOS DE ATAQUES E INTRUSOS EN LAS REDES INFORMÁTICAS*. [www.keylogger.com](http://www.keylogger.com)

Guillem, F. (2018, March 24). *Mejora tus habilidades de hacking con Root Me.* SalbarMas.  
[https://salbarmas.com/2018/03/mejora-tus-habilidades-de-hacking-con-root-me.html?\\_\\_cf\\_chl\\_managed\\_tk\\_\\_=pmd\\_GT3sWFmAyJ5cQsqKun.kianpiNTnAx2ee1V9gtmkWkk-1633044760-0-gqNtZGzNAvujcnBszQil](https://salbarmas.com/2018/03/mejora-tus-habilidades-de-hacking-con-root-me.html?__cf_chl_managed_tk__=pmd_GT3sWFmAyJ5cQsqKun.kianpiNTnAx2ee1V9gtmkWkk-1633044760-0-gqNtZGzNAvujcnBszQil)

Gutiérrez, C., Fernández-Medina, E., & Piattini, M. (2005). *Seguridad en Servicios Web.*  
[https://www.dsi.uclm.es/descargas/technicalreports/DIAB-05-01-2/Seguridad\\_en\\_Servicios\\_Web.pdf](https://www.dsi.uclm.es/descargas/technicalreports/DIAB-05-01-2/Seguridad_en_Servicios_Web.pdf)

Gutiérrez, D. (2020). *AMENAZAS CIBERNÉTICAS Y SU IMPACTO EN LAS ORGANIZACIONES DEL SECTOR INDUSTRIAL Y SERVICIOS DE COLOMBIA EN LA ÚLTIMA DÉCADA.*

Hack The Box. (2021). *All About Hack The Box.* Hack The Box.  
<https://www.hackthebox.eu/about-us>

Háran, J. M., & ESET. (2021, September 8). *Microsoft y CISA advierten sobre ataques explotando nueva zero-day en Windows utilizando documentos de Office | WeLiveSecurity.*



We Live Security. <https://www.welivesecurity.com/la-es/2021/09/08/microsoft-y-cisa-advierten-sobre-ataques-explotando-nueva-zero-day-en-windows-utilizando-documentos-de-office/>

Logan, M., Kinger, P., & Trend Micro. (2021, August 23). *Linux Threat Report 2021 1H: Linux Threats in the Cloud and Security Recommendations*. Trend Micro. <https://www.trendmicro.com/vinfo/es/security/news/cybercrime-and-digital-threats/linux-threat-report-2021-1h-linux-threats-in-the-cloud-and-security-recommendations>

LOPEZ FUENTES, F. D. A. (2015). *Sistemas distribuidos* (J. C. Rosas (ed.); Universidad Autonom...). Universidad Autónoma Metropolitana, Cuajimalpa. [www.cua.uam.mx](http://www.cua.uam.mx)

Ministerio del Interior y Seguridad, & CSIRT. (2021). *Alerta de Seguridad Cibernética 9VSA21-00492-01*. <https://csirt.gob.cl/media/2021/09/9VSA21-00492-01.pdf>

OWASP. (2017). *OWASP Top 10 - 2017 Los diez riesgos más críticos en Aplicaciones Web*. <https://github.com/OWASP/Top10/issues>

OWASP. (2021, September). *OWASP Top 10:2021*. OWASP. <https://owasp.org/Top10/>

Paus, L. (2016, December 29). *Conoce estos 10 recursos para convertirte en un gran hacker ético* |. WeLiveSecurity. <https://www.welivesecurity.com/la-es/2016/12/29/recursos-hacker-etico/>

Pentestit. (2021). *Penetration test lab "Test lab"*. Pentestit. <https://lab.pentestit.ru/>

Ramirez, P. (2020, December 22). *¿Cuáles son los sistemas operativos más usados o utilizados en 2020? - ITSoftware*. ITSoftware. <https://itsoftware.com.co/content/sistemas-operativos-mas-usados/>

Reyes, I. (2021). *Pegasus y el ciberespionaje en México. Kasblog*, 1(1). [https://www.kas.de/documents/266027/13395798/KASBlog\\_semana\\_6\\_ciberseguridad.pdf/fb010bf5-f9c3-82e1-b656-e652b6cebcdd?version=1.0&t=1627922515880](https://www.kas.de/documents/266027/13395798/KASBlog_semana_6_ciberseguridad.pdf/fb010bf5-f9c3-82e1-b656-e652b6cebcdd?version=1.0&t=1627922515880)

Statcounter. (2021a, August 31). *Desktop Operating System Market Share Worldwide | Statcounter Global Stats*. StatcounterGlobal Stats. <https://gs.statcounter.com/os-market-share/desktop/worldwide/#monthly-202008-202108-bar>

Statcounter. (2021b, August 31). *Mobile Operating System Market Share Worldwide | Statcounter Global Stats*. Statcounter Gloval Stats. <https://gs.statcounter.com/os-market-share/mobile/worldwide/#monthly-202008-202108-bar>

share/mobile/worldwide#monthly-202008-202108-bar

Statcounter. (2021c, August 31). *Operating System Market Share Worldwide | Statcounter Global Stats*. Statcounter GlobalStats. <https://gs.statcounter.com/os-market-share#monthly-202008-202108-bar>

TryHackMe. (2021). *TryHackMe | About*. TryHackMe . <https://tryhackme.com/about>

Varmazis, M. (2017, September 14). *Equifax derribado por una vulnerabilidad de Apache Struts de meses de antigüedad*. Naked Security. <https://nakedsecurity.sophos.com/es/2017/09/14/equifax-felled-by-a-months-old-apache-struts-vulnerability/>

Vega, E. (2021). *SEGURIDAD DE LA INFORMACIÓN* (1st ed., Vol. 1). 3Ciencias. <https://www.3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIÓN.pdf>

VulnHub. (2021). *About ~ VulnHub*. VulnHub. <https://www.vulnhub.com/about/>

ZK Hacking. (2021, May 11). *macOS Gatekeeper Bypass CVE-2021-30657 PoC - YouTube*. YouTube. <https://www.youtube.com/watch?v=NfbhhrKBy7M>

## Tabla de ilustraciones

Ilustración 1 Un atacante accediendo a un sistema por un archivo .....	4
- Ilustración 2 Ataques de ingeniería social = suplantación y engaños .....	5
Ilustración 3 los ataques de malware son de los más conocidos .....	6
Ilustración 4 Ejemplo de un ataque de interrupción .....	7
Ilustración 5 Ejemplo de un ataque de interceptación .....	8
Ilustración 6 Ejemplo de un ataque de modificación.....	9
Ilustración 7 suplantación de identidad digital .....	10
Ilustración 8 Sistemas operativos para computadores de escritorio más usados en el último año .....	11
Ilustración 9 Sistemas operativos para dispositivos móviles más usados en el último año .....	11
Ilustración 10 Descripción de vulnerabilidad CVE-2021-40444 .....	13



Ilustración 11 Descripción de vulnerabilidad CVE-2021-34494 .....	13
Ilustración 12 Descripción de vulnerabilidad CVE-2021-34458 .....	14
Ilustración 13 Descripción de vulnerabilidad CVE-2021-30860 .....	15
Ilustración 14 Descripción de vulnerabilidad CVE -2021-30657 .....	16
Ilustración 15 Descripción de vulnerabilidad CVE-2021-30858 .....	16
Ilustración 16 Descripción de vulnerabilidad CVE-2017-5638 .....	18
Ilustración 17 Descripción de vulnerabilidad CVE-2018-7600 .....	18
Ilustración 18 Descripción de vulnerabilidad CVE-2020-25213 .....	19
Ilustración 19 Descripción de vulnerabilidad CVE-2021-1905 .....	20
Ilustración 20 Descripción de vulnerabilidad CVE-2021-24026 .....	20
Ilustración 21 Descripción de vulnerabilidad CVE-2020-11261 .....	21
Ilustración 22 ejemplo del funcionamiento de HackTheBox .....	23
Ilustración 23 Ejemplo del repositorio de VulnHub .....	24
Ilustración 24 Ejemplo de funcionamiento de TryHackMe .....	25
Ilustración 25 ejemplo de funcionamiento de PentestIT .....	26
Ilustración 26 ejemplo de ejercicio de Root me .....	27
Ilustración 27 Tabla comparativa entre las plataformas expuestas .....	29