Artículo de revisión

Herramientas fundamentales para el hacking ético

Fundamental Tools for Ethical Hacking

Alain Eduardo Rodríguez Llerena[1*] 0000-0002-4254-727X

[1]ETECSA, Dirección Territorial Oeste. La Habana, Cuba.

* Autor para correspondencia: alain.rodriguez@uic.cu

RESUMEN

En Cuba la mayoría de los especialistas de seguridad informática tienen un escaso conocimiento sobre las herramientas indispensables del *hacking* ético. Para realizar la presente investigación se hicieron búsquedas bibliográficas nacionales e internacionales. De la gran cantidad de herramientas disponibles en distribuciones especializadas para la seguridad informática (Parrot Security, Black Arch y Kali Linux), se seleccionaron aquellas que se ajustaban más a las características de las redes cubanas. Este trabajo tuvo como objetivo describir algunas de las herramientas seleccionadas para el escaneo y explotación de vulnerabilidades, y conceptos fundamentales sobre el tema. Consideramos que este estudio puede ser provechoso para los especialistas cubanos en seguridad informática pues les servirá no solo para conocer sobre el *hacking* ético, sino también cuáles son las herramientas que se pueden emplear, teniendo en cuenta las características de nuestras redes nacionales.

Palabras clave: hacking ético; vulnerabilidades; escaneo; seguridad informática.

ABSTRACT

In Cuba, most computer security specialists have little knowledge about the essential tools of ethical hacking. To carry out the present investigation, national and international bibliographic searches were made. From the large number of tools available in specialized distributions for computer security (Parrot Security, Black Arch

and Kali Linux), those that best fit the characteristics of Cuban networks were selected. Our research aimed to describe some of the selected tools for scanning and exploiting vulnerabilities, and fundamental concepts on the subject. We believe that this study will be very useful for Cuban specialists in computer security because it will serve them not only to learn about ethical hacking; but also, what are the tools that can be used taking into account the characteristics of our national networks.

Keywords: ethical hacking; vulnerabilities; scanning; computer security.

Introducción

Debido a los grandes casos de intrusión de *hackers* en el mundo (por ejemplo, en 1994 Vladimir Levin robó, desde San Petersburgo, a través de los sistemas de Citibank, más de 10 millones de dólares por medio de transferencias a sus cuentas. En los dos años siguientes, desde otros bancos de los EE. UU., 300 millones de dólares se movilizaban electrónicamente de modo fraudulento), fue necesario un servicio profesional que imitara esos ataques o que diera capacitación con las mismas metodologías que empleaba el intruso.[(1)] De esta manera, se podía evaluar, con certeza, las condiciones de seguridad de la organización, y de haber agujeros en el sistema, se podrían descubrir y solucionar de forma preventiva. Desde los años noventa del pasado siglo, varios especialistas en seguridad informática fueron estudiando y practicando metodologías de intrusión en sus trabajos, laboratorios o casas. Así, empezaron a ofrecer a las instituciones un servicio a modo de proveedores externos o contratados, y "para darle un nombre medianamente formal, lo llamaron ethical hacking".[(1)]

El *hacking* ético es una rama de la seguridad tecnológica dirigida a prevenir, erradicar, estabilizar y contraatacar vulnerabilidades de *software* o de *hardware*. Para ello se debe contar con los conocimientos necesarios en redes, administración de servidores y sus respectivos servicios, que más adelante se presentarán. *Hacking* ético es cuando una persona utiliza sus conocimientos de informática para encontrar fallos, huecos o vulnerabilidades.

Hace algunos años, el mundo se mueve digitalmente, ejemplo de ello es Internet de las cosas, la Nube, casas inteligentes, edificios inteligentes y hasta ciudades inteligentes. Todo está conectado a una red específica y se nutren de Internet.

En nuestra isla no se está exento de esto, ya que Internet está cada vez más en los hogares y por medio de los datos móviles. Además, todas las entidades cuentan con los servicios de Internet y en ellas se está abogando por la masificación de las TIC. Ahora, mientras más se expanda la informatización en Cuba, se necesitará de más seguridad tecnológica y de más especialistas en la rama del *hacking* ético.

En nuestro país, cuando se habla de *hacking* ético a nivel empresarial, muchos de los directivos lo consideran como algo "lejano en el tiempo". Hasta el momento, cuando sucede algo en las redes corporativas (un fallo debido a una vulnerabilidad latente o no descubierta a tiempo por un ataque, un fallo interno por uno o varios usuarios de la empresa, o un ataque externo), y no tienen o no encuentran una explicación, entonces, es cuando algunos de ellos se preocupan y empiezan a indagar sobre el tema, para ver si en realidad, sus especialistas en seguridad informática y redes cuentan con los conocimientos idóneos sobre el tema. Y ciertamente, hay un pobre conocimiento sobre el *hacking* ético y sus herramientas indispensables en la mayoría de los especialistas de seguridad informática. De hecho, por primera vez en nuestro país, se está llevando a cabo un postgrado de especialización en seguridad informática en la Universidad de Ciencias Informáticas y se abrirá una ingeniería en Ciberseguridad en dicha institución a partir de septiembre de 2020. Sobre el *hacking* ético, lamentablemente se ha trabajado muy poco y hay escasos conocimientos en nuestro país. Por ello, el objetivo de esta investigación fue describir algunas de las herramientas seleccionadas para el escaneo y explotación de vulnerabilidades, y conceptos fundamentales sobre el *hacking* ético. Se tuvo en cuenta las herramientas que se adecúan a las características de nuestras redes nacionales.

Hacking ético y pentesting

Ciertamente, a lo largo de los años el llamado "hacking ético" ha tenido adeptos y contrincantes. Ello ha estado relacionado fundamentalmente por la combinación de estos dos vocablos: ético (se refiere a algo correcto, bueno), *hacking* (indica lo contrario).[2] El desconocimiento del rol que juega el *hacking* ético es la principal causa de esta problemática.

El *hacking* ético no entra en los sistemas informáticos para robar o alterar información, sino para encontrar vulnerabilidades y fallos.[3] También es conocido como prueba de

intrusión o *pentest*, o sea, es "el *arte* de comprobar la existencia de vulnerabilidades de seguridad en una organización, para posteriormente, a través de un informe, revelar aquellos fallos de seguridad encontrados, mitigarlos a la brevedad posible y evitar fugas de información y ataques informáticos".[2] A aquellos que realizan las pruebas de intrusión o *pentest* se les denomina pentester.

La labor de los pentester siempre está ligada a las necesidades y preocupaciones que pueda tener una entidad. Por ello, cada prueba de intrusión será diferente y su éxito dependerá de las habilidades y experiencias que tenga el profesional. Existen tres tipos de *pentesting*, los cuales están relacionados con la cantidad de información que se posea sobre la entidad a auditar y la manera en que se vayan a realizar las pruebas de intrusión (Fig. 1):[4]

Caja blanca (*White box*): Es el más completo, debido a que parte de un análisis integral. Con este se evalúa toda la infraestructura de la red. El pentester tiene conocimiento sobre todos los aspectos de seguridad de la entidad (medidas, estructura de la red, contraseñas, etcétera).

Caja gris (*Grey box*): Es el más recomendado por los especialistas. A diferencia del anterior, el pentester no posee la información específica para realizar el test de penetración, por eso, requiere de tiempo y recursos para identificar la información necesaria acerca de las posibles vulnerabilidades existentes.

Caja negra (*Black box*): En este caso no hay información sobre la entidad y se actúa de forma similar a un ciberdelincuente para tratar de reconocer fallos en la estructura de la red.

Fig. 1 - Tipos de pentesting.

Como se señaló al principio, los *hackers* han tenido una mala fama a lo largo de la historia, pero todos no son delincuentes cibernéticos. Para evitar confusiones, se han creado denominaciones que marcan bien la diferencia entre ellos. Se han propuesto

los términos *crackers* y *hackers* éticos. Los primeros son aquellos que realizan técnicas de intrusión con fines maliciosos y lucrativos; los segundos son los que lo hacen con fines éticos, por el bien de la entidad que lo solicita.[2] A su vez, existe otra clasificación: sombrero blanco (*White hat*) y sombrero negro (*Black hat*). Los hackers de sombrero blanco son los hackers éticos; mientras los de sombrero negro son aquellos que explotan las vulnerabilidades en los sistemas con el propósito de demostrar que han burlado la seguridad de la entidad (Fig. 2). [2]

Fig. 2 - Clasificación de sujetos que realizan las pruebas de penetración.

Tipos de hacking ético en Cuba

En nuestro país, las pruebas de penetración son facultadas solo para los especialistas de seguridad informática (ESI), por tanto, el *hacking* ético es desempeñado por dichos especialistas. Se emplean de manera diferente, según el nivel de acceso a los datos de la entidad a auditar:

Caja blanca: Aquellos especialistas que tienen un conocimiento completo sobre los datos de la red. (Ejemplo: un especialista que lleva la seguridad tecnológica de su entidad).

Caja gris: Aquellos especialistas que no tienen un conocimiento completo sobre los datos que se van a auditar. (Ejemplo: un especialista que audita una parte de su

entidad que no está bajo su responsabilidad, por tanto, no cuenta con toda la información necesaria para realizar las pruebas de penetración).

Caja negra: Aquellos especialistas que salen de su entidad a auditar otras entidades, por tanto, no tienen ningún conocimiento sobre la red a la que le realizarán las pruebas de *hacking* ético.

Conocimientos indispensables para un especialista en seguridad informática para el pentesting

Un especialista en seguridad informática debe estar preparado como *hacker* ético para poder tener una mayor visibilidad y un total control sobre el sistema de la entidad. Es necesario que dicho especialista cuente con un título en Informática o afín, y tenga un conocimiento avanzado en redes (LAN, WAN), en los protocolos (TCP/IP-IPv4-IPv6), en sistemas operativos y servicios estándares empleados en casi todas las empresas (DNS, Ldap, Squid ,mySql, FTP); todo ello para poder interpretar los datos que dan las herramientas empleadas en el escaneo de las vulnerabilidades y su explotación.

Herramientas básicas para el especialista de seguridad informática

El especialista en seguridad informática es quien realiza el proceso de *hacking* ético. Con ello puede identificar qué incidentes podrían ocurrir antes de que sucedan y, posteriormente, reparar o mejorar el sistema, de forma tal que se eviten estos ataques.

Para realizar una prueba de penetración de forma profesional, se requieren también conocimientos de programación, metodologías y documentación. No obstante, esos aprendizajes se adquieren una vez que se conocen y se saben utilizar muchas herramientas que son parte del proceso de *penetration testing*. A continuación, se describirán las herramientas básicas y factibles para las empresas cubanas, en tanto se ajustan a las características de nuestras redes nacionales.

Network Mapper (NMAP)

Se trata de una herramienta de código abierto que sirve para el escaneo de redes. Emplea paquetes IP sin procesar para identificar qué servicios se están ejecutando en un dispositivo remoto, así como la identificación de equipos activos, sistemas operativos en el equipo remoto, existencia de filtros o *firewalls*, entre otros.[5] Fue diseñado para escaneo rápido de redes grandes, aunque también se emplea en *hosts*

únicos. Se puede ejecutar en todos los principales sistemas operativos y los paquetes binarios oficiales están disponibles para Linux, Windows y MacOS X. Se describe en la literatura a Network Mapper como una herramienta flexible, portable, fácil, poderosa, libre, de soporte, popular.[6]

Open Vulnerability Assessment Scanner (OpenVAS)

Es un *framework* que cuenta con servicios y herramientas para la evaluación de vulnerabilidades y puede usarse de forma individual o como parte del conjunto de herramientas de seguridad incluidas en OSSIM (Open Source Security Information Management). Distribuciones como Parrot Security, Black Arch y Kali Linux ya cuentan con esta herramienta instalada de forma predefinida, o se encuentran dentro de sus repositorios.[7]

Este escáner es desarrollado y mantenido por Greenbone desde 2009. Es una herramienta de código abierto y está bajo la Licencia Pública General de GNU.[8]

OpenVAS puede también ser utilizado a través de dos clientes, desde línea de comandos (OpenVAS CLI) o una interfaz web (Greenbone Security Assistant). Una vez que se instala en el sistema, también puede emplearse desde Metasploit *framework* para la explotación de vulnerabilidades.[7]

Interactúa con dos servicios mediante las interfaces: OpenVAS Manager y OpenVAS Scanner. El primero realiza el filtrado o clasificación de los resultados del análisis, control de las bases de datos que contienen la configuración o los resultados de la exploración y la administración de los usuarios, incluyendo grupos y roles.[7] En el caso del OpenVAS Scanner, este ejecuta las denominadas NVT (Network Vulnerability Tests), es decir, las pruebas de vulnerabilidades de red**,** conformadas por rutinas que comprueban la presencia de un problema de seguridad específico conocido o potencial en los sistemas. Las NVT se agrupan en familias de pruebas similares, por lo que la selección de las familias y/o NVT individuales forma parte de la configuración de escaneo.[7]

BetterCap

Se trata de una herramienta potente, flexible y portátil, que fue creada para realizar varios tipos de ataques MITM (man-in-the-middle) contra una red, manipular HTTP, HTTPS y tráfico TCP en tiempo real, buscar credenciales (texto plano), etcétera.[9] Estos

ataques se realizan interponiéndose entre dos equipos para ver qué datos se intercambian, de ahí la terminología "hombre en el medio" (Man in the middle). Pero ello no es suficiente, se requiere también de un SSLstrip para poder leer los datos que se envían entre ambos dispositivos.[10]

BetterCap, en una sola herramienta, proporciona al investigador de seguridad todo lo que se necesita para medir vulnerabilidades, fundamentalmente de texto plano. Además, funciona en sistemas GNU/Linux, MacOS X y OpenBSD.[9]

Metasploit framework

Se trata de otro *framework*, software libre, para las pruebas de penetración y explotación de sistemas operativos, aplicaciones, testeo de hardware, etcétera. Esta herramienta posibilita a los equipos de seguridad no solo detectar vulnerabilidades, sino también administrar evaluaciones de seguridad y mejorar su conocimiento sobre la seguridad de la entidad. A su vez, permite a los especialistas estar alerta ante cualquier ataque. Contiene un conjunto de herramientas que proporcionan un entorno completo para las pruebas de penetración y desarrollo de *exploits*.[11]

Una vez identificados los servicios y sus vulnerabilidades (con OpenVas), corresponde la explotación de las vulnerabilidades. Es decir, primero se tiene que probar si realmente las vulnerabilidades identificadas posibilitan que un atacante cause algún daño. Luego hay que conocer cuál sería ese daño. Aunque se haya identificado una vulnerabilidad en la instancia anterior, podría ser que, al momento de intentar explotarla, existan otras medidas de control que no hayan sido consideradas, puedan existir otras capas de seguridad o distintas variables que podrían hacer más complicada su explotación. Igualmente, si se logra explotar la vulnerabilidad, se puede comprobar y dimensionar cuál sería el daño hacia la entidad, en función de la información o sistemas que estuvieran "detrás" de dicha vulnerabilidad.[12]

Metasploit es una herramienta ideal pues permite realizar dichas pruebas. Mientras OpenVas posee una base de datos de vulnerabilidades, Metasploit posee una base de *exploits* que se pueden aprovechar. En lugar de revisar si existe alguna vulnerabilidad en un equipo remoto, se intenta directamente la ejecución de un *exploit* y se simulan las consecuencias posteriores.[12]

Armitage

Es una herramienta que funciona con una estructura de cliente/servidor y permite la colaboración en equipo, pues posibilita el uso de Scripts para Metasploit, posibilita visualizar objetivos, recomienda *exploits* y expone las características avanzadas de postexplotación que tiene el *framework*.

A través de una instancia de Metasploit, su equipo o (grupo de trabajo) podrá realizar lo siguiente[13]

- Usar las mismas sesiones.
- Compartir *host*, datos capturados y archivos descargados.
- Comunicarse a través de un registro compartido de eventos.
- Ejecutar *bots* para automatizar las tareas del equipo (grupo de trabajo).

Armitage organiza las capacidades de Metasploit y de todo el proceso de *hacking*. Permite descubrir, acceder, postexplotar y manejar los sistemas o aplicaciones vulnerables.

Esta herramienta recomienda *exploits* y ejecuta opcionalmente controles activos para identificar qué *exploits* trabajan. Si estas opciones fallan, es posible utilizar el ataque de Hail Mary para la explotación automática e inteligente de Armitage en contra de sus objetivos.[13]

Una vez dentro de los dispositivos y PC vulnerables, Armitage expone las herramientas integradas de postexplotación en el agente *meterpreter*, con un clic en el menú se puede escalar privilegios, capturar pulsaciones de teclado, volcar los *Hash* de las contraseñas, navegar por los archivos del sistema, y utilizar comandos en la Shell.[13]

El paquete de cliente de Armitage está disponible para Windows, MacOS X y Linux. Armitage no requiere una copia local del Metasploit Framework para conectarse a un servidor de nuestro equipo de trabajo.

Open Web Application Security Project (OwaSP)

Es un software libre destinado a mejorar la seguridad de diferentes aplicaciones y servicios web. Con esta herramienta, se hacen públicos los resultados de diferentes análisis de seguridad para que las entidades los conozcan, los puedan solucionar rápidamente y puedan proteger, al máximo, la seguridad de sus usuarios.[14]

Una de las herramientas más potentes del programa OWASP es ZAP (Zed Attack Proxy). Es una plataforma diseñada fundamentalmente para monitorear la seguridad de las aplicaciones web. Es una de las aplicaciones más activas en cuanto a las auditorías de seguridad.

Entre las principales características del OWASP ZAP se destacan:[14]

- Herramienta totalmente gratuita y de código abierto.
- Herramienta multiplataforma, compatible, incluso, con Raspberry Pi.
- Fácil de instalar, dependiendo únicamente de Java 1.7, o superior.
- Posibilidad de asignar un sistema de prioridades.
- Traducida a más de 12 idiomas, entre ellos, el español.
- Posee un excelente manual de ayuda y gran comunidad en la red.

Con esta herramienta se podrán auditar diferentes aplicaciones web con una serie de funciones y análisis específicos: [14]

- Posibilidad de comprobar todas las peticiones y respuestas entre cliente y servidor.
- Posibilidad de localizar recursos en un servidor.
- Permite análisis automáticos y pasivos.
- Posibilidad de lanzar varios ataques a la vez.
- Capacidad para utilizar certificados SSL dinámicos.
- Soporte para utilizar tarjetas inteligentes (DNI-e, por ejemplo) y certificados personales.
- Análisis de sistemas de autenticación.
- Posibilidad de actualizar la herramienta automáticamente.
- Dispone de una tienda de extensiones (*plugins*) con las que se pueden añadir más funciones a la herramienta.

DVL - DVWA

Para probar cualquiera de las herramientas anteriormente expuestas, el especialista en seguridad informática debe definir un sistema objetivo, un sistema en el que se harán las pruebas. Una práctica incorrecta de quienes se inician en este ámbito es realizar sus primeros pasos y pruebas en sistemas públicos de Internet, en un entorno real. Con

ello pueden existir problemas legales, además que no es la forma correcta (ni ética) de realizarlo. Para aprender a emplear las herramientas de *pentesting*, se debe usar un entorno de pruebas, o sea, "un escenario de investigación en donde uno pueda tener acercamientos sin riesgos de afectar algún entorno en producción".[12]

Para la realización de este escenario, se pueden emplear dos herramientas fundamentales: Damn Vulnerable Linux (DVL) y Damn Vulnerable Web Application (DVWA). Aunque el primero está desuso, aún se puede conseguir en Internet para hacer el entrenamiento. Ambas herramientas constituyen sistemas operativos y aplicaciones webs que poseen todo tipo de vulnerabilidades, de manera que, la persona que los emplea, puede intentar explotarlas y experimentar (entrenar). [12]

Igualmente, con DVL – DVWA es posible "construir" un sistema de pruebas propio (con PC virtuales). Por ejemplo, se instala cualquier sistema operativo (se desactivan las actualizaciones o se instala una versión antigua) y sobre él, se empiezan a instalar servicios en versiones anteriores a la última. De esta manera, podemos obtener un sistema vulnerable propio sobre el que se harán las pruebas. Este entorno es el propicio para comenzar la *Penetration Testing*. [12]

Nuestro cerebro

Igual que Bortnik, consideramos que el cerebro es otra herramienta fundamental para el especialista en seguridad informática. Una prueba de penetración no depende exclusivamente de la ejecución de una serie de herramientas en un orden determinado. "La elección de las herramientas, la ejecución de tareas manuales y la utilización de una metodología son tan solo algunas de las variables para convertirse en un profesional de *Penetration Testing*. Un factor común en todo el proceso es que hay que pensar." [12] Existen dos tipos de *ethical hacker*: los que solo leen y emplean lo que dicen las herramientas, y aquellos que las interpretan y emplean su cerebro para obtener y brindar un informe que esté acorde con las necesidades de la entidad que lo solicita, para poder mejorar la protección de su información e infraestructura.

Discusión

Es necesario que se estudien más las buenas prácticas de *hacking ético* y que cada día se profundice en los alcances que estas técnicas tienen, así como la manera de prevenir y contrarrestar sus efectos, para descubrir vulnerabilidades en la seguridad y reaccionar acorde con los inconvenientes que se presenten.

Las herramientas expuestas en este trabajo son las más usadas por los especialistas de seguridad tecnológica para detectar, prevenir y responder ante cualquier ataque que se detecte y que afecte la seguridad de las redes.

Nmap es de las herramientas más usadas mundialmente para el escaneo de puertos.[1] Sin embargo, no estamos de acuerdo con que los *testing* de páginas o sitios web sean herramientas *online*. Debido a las características de nuestras redes, es mejor tener una herramienta *offline* para comprobar las vulnerabilidades que pueda presentar un sitio o página web.[(15)] La herramienta Owasp es la más indicada para esta tarea, se ejecuta de manera local y está accesible en varias distribuciones de software libre, de seguridad tecnológica como Parrot Security y Kali Linux (sistemas dedicados al *hacking* ético que encabezan la lista en la actualidad).[(16)] Para el *testing* de páginas o sitios web se puede emplear el laboratorio o el ambiente de pruebas DVL o DVWA, según convenga.[(17)]

Muchos le temen a la herramienta Metasploit, porque es capaz de encontrar una vulnerabilidad y explotarla también. Según Katritzidakis, [(18)] y compartimos sus ideas, está equipada para ser de las mejores herramientas y es el *framework* más poderoso para un especialista en *hacking* ético. Es una herramienta que nos permite arreglar el problema desde un punto de vista real, explotándolo en un entorno seguro.

Bettercap, como dicen muchos, es la navaja de la red, pues es una herramienta versátil y se usa principalmente para ataques MITM[(19)] (Hombre en el medio). Este ninja con sable de samurái (así es el ícono de dicha aplicación) es el más indicado para encontrar texto plano, una de las vulnerabilidades más vistas en las redes, y nuestro país no está libre de esta vulnerabilidad.

Es importante no subestimar la herramienta Armitage (incluye escaneo, explotación, ayudas, vistas del *pentesting*), usada y venerada por muchos especialistas en la rama de la seguridad de las tecnologías. Según Cornejo, Armitage es un Administrador

Gráfico de Ciber Ataques para Metasploit: es una interfaz que representa gráficamente objetivos. El fin de Armitage es posibilitar que Metasploit sea de ayuda para quienes no manejen Metasploit a cabalidad pero que si saben de hacking. En este sentido, el conocer Armitage podría constituir un paso importante para aprender las características avanzadas de Metasploit. Cualquier cosa que se realice en Armitage es traducido a un comando que Metasploit entienda. Metasploit presenta sus capacidades como módulos. Cada escáner, exploit, e incluso cada payload está disponible como un módulo. Armitage existe como cliente y servidor que permite la comunicación / colaboración con el equipo comprometido.[20]

Openvas es la herramienta que escanea nuestra red y nos da posibles soluciones, algo verdaderamente muy útil para cualquier especialista de la seguridad informática. Es libre de pago, algo fundamental, y es actualizado periódicamente. Lo sigue una gran comunidad, por lo tanto, se le agregan cambios constantemente.[21]

Conclusiones

Las herramientas expuestas en este artículo se interrelacionan entre sí con un fin común: encontrar las vulnerabilidades en una red ya sea LAN o WAN; no obstante, cada una tiene un rol específico e independiente.

Los especialistas en seguridad informática deben dominar las herramientas que se describen en este artículo para poder conocer las vulnerabilidades dentro de sus redes y así implementar medidas que aseguren todos los datos sensibles o importantes que navegan por la red y servicios digitales que se brinden internos o externos en la empresa.

Independientemente de las herramientas de software que se utilicen, pensar constantemente como un atacante es la clave principal para realizar un *Penetration Testing* de forma exitosa, ética y profesional.

Referencias

1. Tori C. Hacking Ético. Primera edición, Rosario Argentina 2008.

2. Guevara Soriano A. Hacking ético: mitos y realidades. Revista .Seguridad. 2012 [citado: 10/03/2020];(12). Disponible en: https://revista.seguridad.unam.mx/numero-12/hacking-%C3%A9tico-mitos-y-realidades

3. Chan R. Así trabajan los hackers éticos que se dedican a piratear legalmente empresas como Uber, Starbucks o Airbnb. Business Insider; 2020 [citado:10/03/2020]. Disponible en: https://www.businessinsider.es/son-hackers-eticos-como-trabajo-dia-dia-561195

4. Martínez Zamora L. ¿En qué consiste el trabajo de un pentester? IMF Business School. 2019 [citado: 10/03/2020]. Disponible en: https://blogs.imf-formacion.com/blog/tecnologia/en-que-consiste-el-trabajo-de-un-pentester-201908/

5. Ferranti M. What is Nmap? Why you need this network mapper. Network World. 2018 [citado: 11/03/2020]. Disponible en: https://www.networkworld.com/article/3296740/what-is-nmap-why-you-need-this-network-mapper.html

6. Nmap: The Network Mapper - Free Security Scanner. Disponible en: https://nmap.org/

7. Mendoza, MÁ. Cómo utilizar OpenVAS para la evaluación de vulnerabilidades. Welivesecurity; 2014 [citado: 22/12/2019]. Disponible en: https://www.welivesecurity.com/la-es/2014/11/18/como-utilizar-openvas-evaluacion-vulnerabilidades/

8. OpenVAS – Open Vulnerability Assessment Scanner. Disponible en: https://www.openvas.org/

9. BetterCAP stable documentation. Disponible en: https://www.bettercap.org/legacy/

10. Olmento J. Obtener credenciales HTTPS con Bettercap y SSLstrip. Hack Puntes.com. 2017 [22/02/2020]. Disponible en: https://hackpuntes.com/obtener-credenciales-https-con-bettercap-y-sslstrip/

11. Metasploit Framework. Disponible en: https://metasploit.help.rapid7.com/docs/msf-overview

12. Bortnik S. Pruebas de penetración para principiantes: 5 herramientas para empezar. Revista .Seguridad. 2013 [citado: 22/12/2019];(18). Disponible en: https://revista.seguridad.unam.mx/category/revistas/numero-18

13. Fastan and easy. Manual about Armitage. 2014 [citado: 22/12/2019]. Disponible en: http://www.fastandeasyhacking.com/manual

14. Velasco R. OWASP ZAP, herramienta para auditar la seguridad de una página web; 2015 [citado: 22/12/2019]. Disponible en: https://www.redeszone.net/2015/04/25/seguridad-web-owasp-zap/

15. Blasco Bermejo J. Ataques DoS en aplicaciones Web; 2007 [citado: 06/03/2020]. Disponible en: https://www.owasp.org/images/2/2b/Conferencia_OWASP.pdf

16. Team Ghs Software. Top sistemas operativos para Ethical Hacking; 2019 [citado: 06/03/2020]. Disponible en: https://teamghsoftware.wordpress.com/top-sistemas-operativos-para-ethical-hacking

17. Caballero Quezada AE. Instalación de Damn Vulnerable Web Application (DVWA); 2015 [citado: 06/03/2020]. Disponible en: http://www.reydes.com/d/?q=Instalacion_de_Damn_Vulnerable_Web_Application_DVWA

18. Katritzidakis P. Malware Development for Red Teaming Using Metasploit. Thessaloniki - Greece: International Hellenic University; 2018 [citado: 06/03/2020]. Disponible en: https://repository.ihu.edu.gr/xmlui/bitstream/handle/11544/29159/Dissertation_Thesis_Petros_Katritzidakis_Malware%20Development%20for%20Red%20Teaming%20Using%20Metasploit.pdf?sequence=1

19. Alonso Ch. Bettercap 2: La evolución de la navaja suiza de red y el poder de los Caplets. 09 de octubre de 2018 [citado: 06/03/2020]. En: Un informático en el lado del mal. Blog personal de Chema Alonso sobre sus cosas. Madrid: Un informático en el lado del mal. Disponible en: https://www.elladodelmal.com/2018/10/bettercap-2-la-evolucion-de-la-navaja.html

20. Cornejo G. Armitage; 2018 [citado: 06/03/2020]. Disponible en: https://www.lesand.cl/foro/armitage-0

21. Openvas. OpenVAS - Open Vulnerability Assessment Scanner; 2020 [citado: 07/03/2020]. Disponible en: https://www.openvas.org/

Conflicto de interés

El autor declara que no existe ningún conflicto de interés.

Declaración de autoría

El autor realizó todo el trabajo.