https://repository.uaeh.edu.mx/revistas/index.php/huejutla/issue/archive

Ciencia Huasteca Boletín Científico de la Escuela Superior de Huejutla

Publicación semestral, Vol. 12, No. 24 (2024) 31-35

ISSN: 2007-493X

Criterios de selección de herramientas para pentesting

Tool selection criteria for pentesting

Ana María Felipe Redondo [a], Felipe de Jesús Núñez Cárdenas [b]

Abstract:

This essay highlights the importance of pentesting as a legal practice of exploiting vulnerabilities in the environments of a network, web, mobile or cloud applications and the user environment through social engineering. A review is made of the different authors who make their recommendations for the tools or consider them for their certification processes, some tools were left out, the main criterion was the coincidence of these through the different authors reviewed. Selecting the right pentesting tool can make the difference between an effective security assessment and an ineffective one.

Keywords:

Pentesting, Tools, Vulnerabilities

Resumen:

Este ensayo resalta la importancia del pentesting como una práctica legal de explotación de vulnerabilidades en los entornos de una red, de aplicaciones web, móviles o en la nube y del entorno de los usuarios a través de la ingeniería social. Se hace un repaso de los diferentes autores que hacen sus recomendaciones de las herramientas o las consideran para sus procesos de certificación, algunas herramientas quedaron fuera, el criterio principal fue la coincidencia de estas a través de los diferentes autores revisados. La selección de la herramienta de pentesting adecuada puede marcar la diferencia entre una evaluación de seguridad efectiva y una ineficaz.

Palabras Clave:

Pentesting, Herramientas, Vulnerabilidades

Introducción

Durante 2020, por medio del monitoreo cibernético, la Dirección General Científica de la Guardia Nacional identificó y desactivó 5,920 sitios web utilizados para la comercialización de productos y servicios ilegales; el tipo de actividad más frecuente en estos sitios web fue fraude por compras en internet. [1]**,** tal como se muestra en la Figura 1.

Así como en México, todos los días, en todo el mundo, los sistemas, las aplicaciones, los servidores e infinidad de activos de tecnologías de la información, son perpetrados. La forma y en nivel de sofisticación de los ataques es variable, algunos ataques tienen éxito debido a contraseñas débiles, sin embargo, hay un gran número de intrusiones que usan técnicas más avanzadas para irrumpir, por lo que su misma naturaleza los hace mucho más difíciles de detectar.

Este ensayo recaba las diez herramientas más utilizadas por los profesionales de *pentesting* que ofrecen desde su versión gratuita los elementos para poder realizar las pruebas que contribuyan a minimizar las vulnerabilidades de las aplicaciones, las redes o los entornos móviles o la nube, así como la ingeniería social.

Detrás de estos ataques emergen varias figuras, que se les identifica como "*hackers*", son aquellos que conocen los entresijos de la seguridad, las herramientas más recientes de auditoría y el *hackeo*, descubren errores y vulnerabilidades, son criaturas mortales que pueden

[a] Autor de Correspondencia, Universidad Tecnológica de la Huasteca Hidalguense, https://orcid.org/0000-0002-8579-6532, Email: ana.felipe@uthh.edu.mx

[b] Universidad Autónoma del Estado de Hidalgo, https://orcid.org/0000-0002-2462-3654, Email: felipe_nunez@uaeh.edu.mx

Fecha de recepción: 15/04/2024, Fecha de aceptación: 29/04/2024, Fecha de publicación: 05/07/2024

DOI: https://doi.org/10.29057/esh.v12i24.12763

atacar maliciosamente y ocultar sus huellas sin dejar pista de su rastro**.**

Se hace énfasis en que un ataque malicioso puede ocurrir, pero también las prácticas de ciertos *hackers* se enfocan en explorar y entender los sistemas de forma creativa y constructiva, dando pie al ***hacking*** ético.

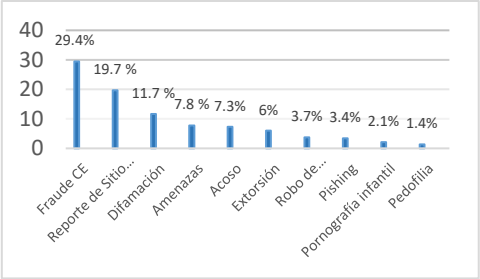

Figura 1. Reportes por incidentes electrónicos atendidos por la Dirección General Científica de la Guardia Nacional, según tipo de incidente 2020. Fuente INEGI, 2021.

El concepto de *hacking* ético se refiere a la realización de actividades de *hacking* de manera legal y ética, con el objetivo de identificar y solucionar vulnerabilidades en sistemas de información, sin embargo, a medida que la seguridad se vuelve más compleja se hace palpable la necesidad de realizar pruebas de penetración, denominándolas "*pentesting*".

Estos escenarios de vulnerabilidad de los sistemas de información hacen fundamental orientar las actividades de las organizaciones hacia sistemas de información seguros, con la finalidad de proteger la información, cumplir con el marco legal, promover una cultura de prevención, minimizar los costos asociados con los ataques y las brechas de seguridad, proteger contra las amenazas internas y externas, para garantizar la integridad, confidencialidad y disponibilidad de la información, así como a mantener la confianza de los usuarios y la continuidad del negocio.

¿Qué es *pentesting* ?

El *pentesting*, puede ser definido como una opción legal y reconocida de localizar y explotar vulnerabilidades en diferentes entornos computacionales, con el propósito de hacerlos más seguros. Es un vocablo inglés formado de las palabras "*penetration testi*ng", que se traduce como "pruebas de penetración". Estas pruebas de penetración son una técnica orientada a simular ataques sobre un sistema, red o aplicación con la finalidad de evaluar la seguridad informática e identificar vulnerabilidades y brechas de seguridad.

El *pentesting* también se conoce como: pen testing, PT,*Hacking*, Etical *Hacking* (*Hacking* ético), White hat *Hacking* (*Hacking* de sombrero blanco), Offensive *Hacking* (*Hacking* ofensivo), Red teaming (Equipo rojo). El *hacking* ético fue usado por primera vez en 1995 por John Patrick, Vice Presidente, de IBM [2].

Las pruebas de penetración adecuadas siempre terminan con recomendaciones específicas para abordar y solucionar los problemas que se descubrieron durante la prueba a fin fortalecer la seguridad contra futuros ataques. Por lo tanto, la idea general es encontrar los fallos de seguridad utilizando herramientas y técnicas similares a un atacante, estos hallazgos pueden minimizar los riesgos antes de un ataque real [3].

Independientemente del propósito final de un atacante, todos los ataques buscarán afectar alguna de estas dimensiones básicas:

Confidencialidad, que consiste en proteger la información del acceso por parte de personas o sistemas no autorizados.
Integridad, que consiste en evitar que se produzcan cambios no autorizados en la información o en los sistemas [4].
Disponibilidad, esto hace que la información y los sistemas sean accesibles a los usuarios autorizados.
Autenticidad, esto se refiere a que una entidad es quien dice ser, de modo que se garantice la fuente de donde procede la información.
Control de acceso, define las acciones que se pueden llevar a cabo los usuarios del sistema.
Trazabilidad, esto con la finalidad de identificar las acciones realizadas sobre la información y los sistemas [5].

Clasificación del *Pentesting*

Cuando se trata de evaluar la capacidad de resistencia de un ataque para mejorar la seguridad los diferentes aspectos que se pueden comprobar durante la realización del *pentesting*, es necesario identificar los tipos de *pentesting* que se pueden realizar, en la Figura 2. Clasificación de *pentesting* de acuerdo a Keshav Malik [6], se puede observar una de las muchas clasificaciones que diversos autores proponen, elegí esta clasificación porque agrupa los aspectos de red, de aplicaciones (incluidas las bases de datos) y de ingeniería social.

Prueba de penetración de red, se orienta a verificar la seguridad de una red, evaluando la vulnerabilidad de una red a la intrusión. Una prueba de penetración simula un ataque para determinar las vulnerabilidades de la red y

determinar si un ataque real tendría éxito. Los *pentests* de red son ideales para empresas que transmiten grandes cantidades de datos y empresas con uso de la nube que dependen de redes.

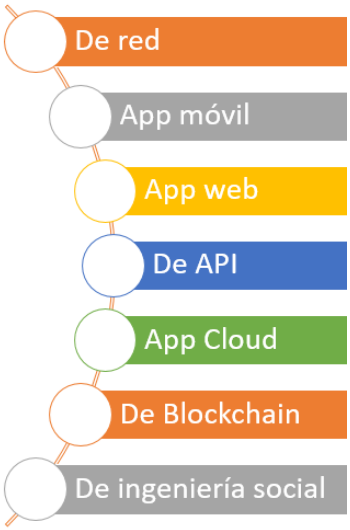

Figura. 2 Clasificación del Pentesting [6].

Las **pruebas de penetración de aplicaciones móviles**, consiste en probar una aplicación móvil en busca de vulnerabilidades de seguridad. El alcance de las pruebas varía desde pruebas funcionales hasta pruebas de seguridad. Las pruebas de penetración han evolucionado significativamente a medida que ha crecido la cantidad de dispositivos móviles y usuarios, por ejemplo, las pruebas de penetración de Android e iOS. Las pruebas de penetración de aplicaciones móviles se realizan para obtener acceso a datos confidenciales o interrumpir la funcionalidad de la aplicación, estas pruebas ayudan a los desarrolladores a minimizar los riesgos de la app.

Las **pruebas de penetración de aplicaciones web** se realizan para exponer las vulnerabilidades de una aplicación web y evitar filtraciones de datos, robo de identidad, fraude y otras consecuencias negativas. Algunas pruebas tales como inyección SQL, XXS, secuencias de comandos entre sitios y falsificación de solicitudes, permiten identificar oportunamente cualquier vulnerabilidad y mitigarlas antes de que sean explotadas.

Pruebas de penetración de API, una interfaz de programación de aplicaciones (API) puede ser un recurso de un tercero, por lo que aquellas empresas que utilizan y desarrollan productos como aplicaciones web o aplicaciones móviles que tienen un backend API deben realizar periódicamente pruebas de penetración de API para protegerlas de la exposición o de códigos inadecuados, con la finalidad de detectar cualquier falla de seguridad dentro del código que pueda hacer que la aplicación web o móvil sea propensa a un ciberataque.

Pruebas de penetración en la nube, está orientada a analizar el entorno de computación en la nube en busca de vulnerabilidades, pudiendo ser manuales o automatizadas a través de un proceso de CI/CD, evaluando la infraestructura para determinar la efectividad de los controles implementados para protegerla.

Pruebas de penetración de *blockchain*, evalúan la seguridad de una red, aplicación o contrato inteligente de *blockchain*. Buscan determinar si la solución implementada puede resistir los ataques que se realizan para comprometer la seguridad de la red.

Pruebas de penetración de ingeniería social, implican probar la seguridad de los empleados de una empresa para identificar vulnerabilidades que podrían ser aprovechadas por un atacante. Estas pruebas buscan asegurarse de que sus empleados conocen los riesgos de los ataques de ingeniería social y puedan identificarlos y prevenirlos.

Criterio de selección de herramientas

Se llevó a cabo una investigación documental que reunió la visión de empresas de seguridad, consultoras y organizaciones de investigación, mismas que publican regularmente informes sobre tendencias y prácticas en seguridad informática. Estos informes a menudo incluyen análisis de herramientas de *pentesting* más populares basados en datos recopilados de clientes, encuestas, análisis de mercado y observaciones de la industria.

Este ensayo consideró empresas, consultoras y organizaciones de investigación para la selección de las herramientas y se tomaron las diez coincidencias para delimitar el alcance de la documentación.

- EC-Council [7]
- TechUnity, Inc [8]
- OSCP Certification Preparation Guide [9]
- Hacking México [10]

Herramientas de software libre para *pentesting*

Existen diferentes propuestas de herramientas para realizar *pentesting*, a continuación, se describe un marco de referencia de los tipos de propuestas que se pueden encontrar.

Escáner: Estas herramientas están diseñadas para detectar y escanear sistemas en busca de vulnerabilidades y debilidades de seguridad. Pueden ser específicas para aplicaciones web, redes, sistemas operativos, etc.

Suite: Se trata de conjuntos de herramientas que ofrecen una variedad de funciones de seguridad, como escaneo de vulnerabilidades, pruebas de penetración, análisis de tráfico, etc., en una sola interfaz integrada.

Framework: Son plataformas que proporcionan una estructura básica y herramientas para desarrollar y ejecutar pruebas de seguridad, incluyendo la automatización de pruebas y la creación de exploits.

Analizador: Estas herramientas se centran en el análisis profundo de datos, como el tráfico de red o los paquetes de datos, para detectar problemas de seguridad, identificar comportamientos anómalos o analizar la actividad del sistema.

Proxy: Son herramientas que actúan como intermediarios entre el usuario y el servidor, lo que les permite interceptar, modificar y analizar el tráfico web para identificar vulnerabilidades o realizar pruebas de seguridad.

Sniffer: Estas herramientas se utilizan para capturar y analizar el tráfico de red en busca de información útil, como contraseñas, datos confidenciales o vulnerabilidades de seguridad.

Cada tipo de software tiene sus propias características, fortalezas y áreas de enfoque específicas, lo que los hace adecuados para diferentes situaciones y necesidades de seguridad.

Criterios de selección de herramientas para *pentesting*

Los usuarios consideran “n” criterios para seleccionar una herramienta para realizar *pentesting*, algunos de estos criterios pueden ser:

Si el escaneo es automático o manual, si permite la post-explotación, la gestión de vulnerabilidades, la comunicación encubierta, las auditorías de seguridad, la auditoría de redes, el análisis de tráfico, las pruebas de penetración propiamente dichas, la protección web, la distribución, la facilidad de uso, el tipo de soporte, entre otros.
A continuación, se presenta una lista de las herramientas más utilizadas por profesionales de acuerdo a las mencionadas por EC-Council, TechUnity, Inc, OSCP Certification Preparation Guide y Maril Vernon [11], quien realizó un estudio similar.

Nmap combina de una herramienta de explotación de redes y un auditor de seguridad, fácil de configurar en los diversos criterios de tipos de vulnerabilidades y alcance.

Metasploit
Aunque hay opciones emergentes como Atomic Red Team, Metasploit sigue siendo un conjunto de herramientas completo para desarrollar, probar y ejecutar código de explotación contra objetivos remotos. Metasploit no se trata sólo de encontrar vulnerabilidades; se trata de probarlos, ejecutarlos y comprender cómo pueden explotarse en escenarios del mundo real. Incluso si eres un converso de Cobalt Strike, lo más probable es que hayas comenzado con esto primero, porque es gratuito y fácil de usar [12].

BURP Suite es un paquete completo, una plataforma integrada que tiene que ver con la versatilidad y la profundidad. Desde escanear y rastrear hasta atacar y explotar, BURP puede interceptar, manipular, codificar cargas útiles en URL, cambiar métodos de entrega y enviar solicitudes directamente a un sitio web [13].

Sistemas operativos especializados para pentesting. Funcionan como una ventanilla única que incluye tantas herramientas como sea posible en una sola descarga para cada fase del *pentesting*.. Incluso incluye funciones complementarias como análisis forense, ingeniería inversa y herramientas sencillas de auditoría de seguridad, Kali Linux y Parrot OS son dos ejemplos de esto [14].

Nessus, se utiliza para buscar vulnerabilidades de red, problemas de configuración, puntos de referencia insuficientes y parches faltantes, entre otros problemas. Es el tipo de herramienta que no sólo funciona en la superficie; profundiza y ofrece conocimientos y hallazgos que son tan valiosos como completos [14] [16].

John the Ripper es particularmente eficaz para probar la resistencia de las contraseñas en un entorno de red [15].

Wireshark, es un analizador de protocolos de red utilizado para capturar y mostrar los datos que viajan hacia adelante y hacia atrás en una red en tiempo real, lo que permite examinar información detallada sobre protocolos de red, paquetes de datos y tráfico de red [16].

ZAP (Zed Attack Proxy), es un escáner de seguridad de aplicaciones web diseñado para encontrar automáticamente vulnerabilidades de seguridad en aplicaciones web mientras se encuentran en fase de desarrollo y pruebas [17].

SQLmap, automatiza el proceso de detección y explotación de vulnerabilidades de inyección SQL (SQLi) en aplicaciones web [18].

El uso principal de **Aircrack-ng** es identificar y explotar vulnerabilidades en redes Wi-Fi, particularmente dirigidas a los protocolos de seguridad WEP y WPA/WPA2-PSK.

Funciona capturando paquetes de red y luego aplicando varios algoritmos para descifrar [19] las claves utilizadas para proteger las redes inalámbricas.

La Tabla 1, concentra las diez opciones presentadas, considerando criterios comunes tales como: la posibilidad de escaneo automático o manual, la post-explotación, la gestión de vulnerabilidades, la auditoria de redes, el análisis de tráfico, las pruebas de penetración, la facilidad de uso y los costos.

Tabla 1. Tabla comparativa de herramientas de pentesting

Software	Tipo	Escaneo Automático	Escaneo Manual	Post - Explotación	Gestión de Vulnerabilidades	Auditoría de Redes	Análisis de Tráfico	Pruebas de Penetración	Facilidad de Uso
Burp Suite Pro	Suite	No	Sí	Sí	Sí	No	No	Sí	Alto
Nessus Pro	Escáner	Sí	No	No	Sí	Sí	No	Sí	Alto
Kali Linux	Distribución	No	Sí	No	No	No	No	Sí	Alto
NMap	Escáner	No	Sí	No	No	Sí	No	Sí	Medio
Wireshark	Analizador	No	No	No	No	No	Sí	No	Alto
Aircrack-ng	Suite	No	Sí	No	No	No	No	Sí	Bajo
ZAP	Proxy	Sí	No	No	No	No	No	Sí	Medio
Metasploit	Framework	Sí	Sí	Sí	No	No	No	Sí	Medio
Parrot OS	Distribución	No	Sí	Sí	No	No	No	Sí	Medio
John the Ripper	Suite	No	Sí	No	No	No	No	Sí	Medio

Elaboración propia

Conclusiones

Determinar las herramientas de *pentesting* más utilizadas en los últimos años puede variar según la fuente y la metodología utilizada para recopilar los datos.

Esta propuesta está basada en una combinación de diversas fuentes de información, donde estas herramientas son constantemente citadas y utilizadas en varios informes de la industria, encuestas a profesionales de seguridad y observaciones de uso en comunidades de *pentesting* y seguridad informática.

La selección de la herramienta de *pentesting* es crucial por varias razones, depende de los objetivos del proyecto de *pentesting*, el alcance de las pruebas según las áreas que se desean evaluar; la precisión en los resultados que depende en gran medida de la herramienta utilizada. Es esencial seleccionar una herramienta confiable y precisa para evitar falsos positivos o negativos, lo que podría llevar a decisiones erróneas en cuanto a la seguridad.

La compatibilidad e Integración de la herramienta con los sistemas y herramientas utilizadas en el entorno de trabajo. Un factor determinante es la facilidad de uso y la curva de aprendizaje.

La disponibilidad de soporte técnico y actualizaciones de la herramienta, con un sólido respaldo de la comunidad puede garantizar que se aborden rápidamente cualquier problema o vulnerabilidad que surja.

En resumen, la selección de la herramienta de *pentesting* adecuada puede marcar la diferencia entre una evaluación de seguridad efectiva y una ineficaz. Es importante realizar una evaluación cuidadosa de las necesidades del proyecto y las capacidades de las herramientas disponibles antes de tomar una decisión.

Referencias

[1] INEGI, «Censo Nacional de Seguridad Pública Feederal 2022,» 2022. [En línea]. Available: https://www.inegi.org.mx/contenidos/programas/cnspf/2022/doc/cnspf_2022_resultados.pdf.

[2] National Cybersecurity Alliance, «National Cybersecurity Alliance,» 2016. [En línea]. Available: https://staysafeonline.org/cybersecurity-for-business/history-ethical-hacking/.

[3] L. Herrero Pérez, Hacking Ético, Ra-Ma, 2022, p. 29.

[4] J. M. Ortega Candel, Ciberseguridad, manual práctico, Parainfo, 2021, pp. 4-5.

[5] P. Engebretson y D. Kennedy, The basics of hacking and penetration testing, Elsevier, 2013, pp. 1-3.

[6] K. Malik, «GetAstra,» Types of Penetration Testing: A Comprehensive Guide, 2023. [En línea]. Available: https://www.getastra.com/blog/security-audit/types-of-penetration-testing/.

[7] EC-Council, «Popular Penetration Testing Tools,» 2024. [En línea]. Available: https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/what-is-penetration-testing/.

[8] Linkedin y D. Balroop, «Penetration Testing Tools: Nmap, Metasploit, Burp Suite, and Wireshark,» TechUnity, Inc, 2024. [En línea]. Available: https://www.linkedin.com/pulse/penetration-testing-tools-nmap-metasploit-burp-suite-dave-balroop/.

[9] S. Bowcut, «Cibersecurity Guide,» A deep dive on the OSCP certification aka the Offensive Security Certified Professional, 2024. [En línea]. Available: https://cybersecurityguide.org/programs/cybersecurity-certifications/oscp/.

[10] Hackingmexico, «Hackingmexico,» 2024. [En línea]. Available: https://www.hackingmexico.one/.

[11] M. Vernon, «10 herramientas de pruebas de penetración que utilizan los profesionales,» CSOOnline, 2024. [En línea]. Available: https://www.csoonline.com/.

[12] Rapid7's, «Metasploit,» 2024. [En línea]. Available: https://www.rapid7.com/products/metasploit/.

[13] PortSwigger, «Burp Suite Community Edition,» 2024. [En línea]. Available: https://portswigger.net/burp/communitydownload.

[14] Tenable Nessus, «Tenable Nessus,» 2024. [En línea]. Available: https://es-la.tenable.com/products/nessus.

[15] OpenWall, «John the Ripper password cracker,» 2024. [En línea]. Available: https://www.openwall.com/john/.

[16] Wireshark, «Wireshark,» 2024. [En línea]. Available: https://www.wireshark.org/download.html.

[17] ZAP , «ZAP Proxy,» [En línea]. Available: https://www.zaproxy.org/.

[18] SQLmap, «SQLmap,» 2024. [En línea]. Available: https://sqlmap.or.