Uso de las Técnicas Del Hacking Ético para la Reducción de Amenazas de Ciberseguridad

José M. González González
Maestría en Ingeniería de Computadoras
Mentor: Dr. Nelliud D. Torres Batista
Departamento de Ingeniería Eléctrica y Computadoras y Ciencia de Computadoras
Universidad Politécnica de Puerto Rico

Resumen *— A medida que las empresas tanto públicas como privadas comienzan a acomodar gran parte de sus capacidades de sistemas de información en la Internet, se hacen más propensas a que hackers de índole criminal puedan utilizar sus técnicas para acceder información sensitiva a través de una aplicación web. Ante la apremiante necesidad de asegurar los sistemas, surge la necesidad de que las empresas cuenten con hackers éticos para que estos se encarguen de identificar vulnerabilidades e implementar métricas correctivas para salvaguardar el activo más importante de una empresa, la información.*

Términos Claves *— Hacking, Hackers, Hackers Éticos, HTTP.*

INTRODUCCIÓN

A medida que las tecnologías relacionadas con la computación aumentan, también así ocurre con el lado oscuro, es decir, los hackers [1]. Ciertamente, si se ve desde un punto de vista estadístico, se puede inferir que existe una correlación positiva y fuerte entre el crecimiento de las tecnologías relacionadas a la computación y el crecimiento del lado oscuro, es decir, los hackers. De igual forma, se puede inferir que a medida que el uso de la Internet aumenta, incluyendo la vasta cantidad de datos que se mueven en línea, la seguridad de los datos se vuelve un problema mayor, basado en lo propuesto por los autores citados en este párrafo.

Kumar y Agarwal [2] expusieron en su artículo que a medida que el número de computadoras asociadas a la Internet aumenta, empresas privadas y el usuario tradicional de los sistemas de información sienten un temor mayor a que sus datos privados o información sean comprometidos por un hacker criminal. De hecho, estos mismos autores expusieron en su artículo que uno de los activos más importantes de las empresas lo es la información, es por esto por lo que cada vez son más las empresas que velan por implementar mecanismos de seguridad cada vez más estrictos para salvaguardar su activo más importante, la información. Ejemplos de tales mecanismos pueden ser la autenticación de dos pasos y el uso de características biométricas para probar la identidad de la persona que desea acceder a los sistemas de información.

Cabe mencionar que, gracias a las tecnologías relacionadas con la Internet, hubo un aumento en la digitalización de procesos como la banca, transacciones en línea, transferencia de dinero en línea, envío y recibo de varios formatos de datos en línea, causando un gran aumento en riesgos asociados a la seguridad de los datos [1]. Estos mismos autores mencionaron en su artículo que un gran número de empresas, organizaciones, banca y páginas web han sido afectadas por varios tipos de ataques realizados por hackers. Por ende, resulta imperativo que se aborden técnicas de seguridad que permitan que estas empresas puedan salvaguardar su activo más importante, la información.

Cuando se habla de hacker, se tiende a pensar mayormente que son personas con malas intenciones, expertos en computación con intenciones dañinas que tratan de robar, divulgar o destruir información de índole confidencial o de valor sin el conocimiento de la víctima. No obstante, un hacker es una persona que tiene un vasto conocimiento en computadoras y que con sus destrezas y habilidades en estas trata de corromper la seguridad de una persona o empresa con el fin de obtener acceso a información personal o confidencial. Por lo cual, un hacker no necesariamente es una persona dañina, sino más bien, una persona con vasta habilidad en computadoras.

Por ende, para reducir los ataques realizados por los hackers, se necesitan personas que sean expertas en sistemas de computadoras y que utilicen su conocimiento por el bien común de la empresa. Bajo este contexto, entra lo que son los hackers éticos. Estos son personas que tienen la habilidad para utilizar herramientas de seguridad y realizan análisis de vulnerabilidades, es decir, son hackers que son contratados por compañías que desean hacer un avalúo de su sistema de seguridad [2].

El propósito de este artículo es auscultar las técnicas que utilizan los hackers éticos para salvaguardar los sistemas de información de la empresa y como tales técnicas pueden disminuir en gran medida los ataques que estas pueden recibir. Se comenzará abordando conceptos tales como hacker y hacker ético. Además, se cubrirán tópicos relacionados a los orígenes del hacking, tipos de hackers, metodología utilizada por los hackers para realizar un ataque, el proceso del hacker ético, código de ética de los hackers éticos, tipos de ataques, herramientas utilizadas por los hackers, tipos de hackeo y aplicaciones del hacking. Finalmente, se cubrirán técnicas de protección ante ataques, parchos de seguridad y reducción de amenazas de ciberseguridad.

¿QUÉ ES EL HACKING?

Ciertamente, cuando se habla del verbo hackear, mejor conocido en inglés como hacking, se tiende a pensar en solo actividades ilícitas con el fin de hacer algún daño u alteración a un sistema de información. No obstante, Gupta y Anand [1] definieron el concepto de hacking como una técnica ampliamente utilizada para encontrar vulnerabilidades o huecos en seguridad en sistemas de computadoras o redes y explotar estos con el fin de ganar acceso no autorizado a tales sistemas o alterar su configuración. Por su parte, Kumar y Agarwal [2] definieron el concepto de hacking como la utilización no aprobada de computadoras y activos del sistema de información. De hecho, estos mismos autores expusieron en su artículo que el hacking consiste en cambiar u alterar los equipos de computadoras y su programación con el fin de lograr algún objetivo externo, tales como acceder al sistema para ganar control de este. Por otra parte, Uhsmani [3] expuso en su escrito que el hacking es un proceso común que corrompe la seguridad y la confidencialidad de la información, tanto de una persona como de un sistema de información completo. En síntesis, se podría inferir que el hacking es el acto de acceder a un sistema, sin permiso previo, con el fin de alterar su configuración y programación para lograr ganar control de este y, por ende, lograr acceder al activo más importante de una persona u empresa, la información.

ORÍGENES DEL HACKING

El hacking no es un concepto nuevo o reciente. De hecho, originalmente el hacking no tenía intenciones maliciosas, sino más bien se refería a métodos o acciones que se tomaban como atajos para finalizar tareas en una forma más eficiente [4]. Originalmente los hackers disfrutaban de explorar nuevas tecnologías sin alguna intención maliciosa [5]. Por consiguiente, se puede inferir que el hacking no siempre tuvo que ver con hacer algún daño a un sistema de información. Aunque el hacking comenzó siendo una actividad que se realizaba de forma inocente, algunos hackers utilizaron sus destrezas y habilidades para lograr acceso no autorizado a los sistemas de información de las empresas.

En términos de tiempo, Smith et al. [4] expusieron en su artículo que el hacking tuvo sus comienzos en campos universitarios, específicamente en *Stanford University* y *Massachusetts Institute of Technology* en la década de los 1960. Ya para la década de los 1970, Steve Jobs y Steve Wozniak, futuros fundadores de *Apple Computer*, crearon y vendieron dispositivos que fueron conocido como cajas azules. Tales dispositivos utilizaban un silbato, obtenido de una caja de cereal de *Cap'n Crunch* que permitía a los usuarios realizar llamadas gratuitas a través de la red de *AT&T* [6].

Ya para la década de los 1980 fue que entonces el término hacking comenzó a tener connotaciones

negativas. De hecho, fue para esta misma década que se formó uno de los primeros grupos de hackers los cuales tenían el firme propósito de bloquear las líneas telefónicas. Debido a las acciones perpetuadas por este grupo de hackers, el gobierno tuvo que crear la Ley de Abuso y Fraude Informático, aprobada en el 1986, con el fin de imponer sanciones a aquellos que corrompieran los sistemas de información [6]. Luego de que la Ley de Abuso y Fraude Informático fuera aprobada, se creó y liberó el primer gusano informático, se publicó un grupo de hackers informáticos y tales grupos atacaron sitios web de índole gubernamental y académica [6].

TIPOS DE HACKERS

Como fue mencionado en el presente artículo, el término hacker se utiliza para describir a cualquier persona u entidad que corrompe la seguridad de una computadora o sistema de información utilizando fallas o huecos en el sistema con el fin de explotar los mismos o utilizar sus conocimientos para actuar de forma productiva o maliciosamente. Cabe mencionar que los hackers son entusiastas con las computadoras y generalmente, tienen conocimiento y experiencias con lenguajes de programación de alto nivel, cuentan con conocimiento en seguridad de sistemas y redes. Típicamente, el perfil de un hacker se estriba en ser una persona que le encanta aprender diversas tecnologías y detalles de los sistemas de computadoras. De igual forma, estos se mantienen en constante mejoría de sus capacidades y destrezas. De acuerdo con Tulasi [7], existen tres grupos comunes de hackers, siendo estos los siguientes:

Hacker de Sombrero Blanco

Bajo esta categoría, típicamente se encuentran los hackers éticos, ya que son considerados como profesionales de la seguridad de sistemas de información y utilizan sus conocimientos de una forma ética. Estos hackers deben tener vasto conocimiento en enrutadores, sistemas operativos, muros de fuego y sistemas de detección de intrusos (IDS, por sus siglas en inglés), servidores, protocolos de red y gerencia de proyectos [8]. Típicamente, este tipo de hacker es contratado en las empresas para detectar vulnerabilidades en los sistemas de información e implementar métricas o políticas que ayuden a mitigar los efectos adversos de tales vulnerabilidades. Por su parte, Gupta y Anand [1] expusieron en su artículo que este tipo de hackers utilizan sus conocimientos y destrezas para proteger la empresa u organización antes de que un hacker malicioso encuentre sus vulnerabilidades y corrompa la seguridad del sistema. Los hackers bajo esta clasificación están autorizados por la industria, aunque cabe mencionar que los métodos y técnicas utilizadas por estos son similares a la de los hackers de sombrero negro, sin embargo, estos cuentan con el permiso de la empresa que lo subcontrate para realizar sus ataques de prueba con el fin de detectar vulnerabilidades e implementar correcciones al sistema.

Hacker de Sombrero Negro

Este tipo de hacker se le conoce como cracker. Al igual que el hacker de sombrero blanco, son expertos en software y hardware de computadoras y poseen vasto conocimiento en redes y seguridad de sistemas de información. No obstante, estos utilizan sus destrezas y habilidades con fines maliciosos con el fin de robar o corromper información secreta, comprometiendo a su vez la seguridad y la integridad de los sistemas de información. También, estos con capaces de apagar o sacar de servicio redes y páginas web. Estos violan la seguridad de los sistemas de información para su ganancia personal. Típicamente, son personas quienes desean probar su conocimiento extensivo en computadoras y cometen varios crímenes cibernéticos como robo de identidad, fraude a tarjetas de crédito, entre otros [1].

Hacker de Sombrero Gris

Los hackers bajo esta clasificación pueden trabajar de forma ofensiva o defensiva, dependiendo mayormente de la situación [7]. Gupta y Anand [1], expusieron que un hacker bajo esta clasificación es un hacker informático o experto en seguridad que a veces viola las leyes, pero no tiene intenciones maliciosas como los hackers de sombrero negro.

Esta clasificación de hackers se deriva de la combinación del hacker de sombrero blanco con el de sombrero negro, ya que el hacker de sombrero blanco se encarga de encontrar las vulnerabilidades en el sistema de información o las redes, pero no la informa hasta tanto se está reparando. Mientras que, los hackers de sombrero negro son los que ilegalmente acceden a sistemas informáticos con el fin de corromper su seguridad e integridad y encontrar vulnerabilidades, con el propósito de informar a otros como hacerlo, mientras que el hacker de sombrero gris, aunque accede al sistema, este no lo hace con la finalidad de explotar el mismo o indicarles a otros como hacerlo. Por lo cual, se puede inferir que el hacker de sombrero gris representa al hacker de sombrero blanco ya que se encarga de mantener la seguridad de los sistemas de información y representa a su vez al hacker de sombrero negro el cual opera maliciosamente para explotar los sistemas de información.

Hacker de Sombrero Azul

Bajo este grupo de hackers, son las organizaciones u empresas quienes solicitan que intenten atacar un sistema, pero tal organización u empresa no los emplea. Tienen conocimientos y destrezas al igual que un hacker de sombrero negro [9].

Hackers Tipo Elite

Estos hackers son los que usualmente primero logran identificar las vulnerabilidades en comparación con los otros grupos de hackers. Se estima que existe un (1) hacker elite por cada 10,000 hackers a nivel mundial [9].

Script Kiddies

Son personas que usualmente no cuentan con peritaje técnico o su nivel de conocimiento es bajo en esta área. Típicamente, utilizan códigos que han sido escrito por otras personas y que están libremente accesibles por la Internet [9].

Hacktivistas

Son hackers que cometen sus actos como forma de protesta ante el gobierno, cambios sociales, promover agendas políticas o promover el ciberterrorismo [9].

Grupos de Crímenes Organizados

Se compone de hackers que pertenecen a un gripo de crímenes organizados. Estos cuentan con un alto nivel de sofisticación con relación a las destrezas y habilidades que tienen de sistemas [9].

Amenazas Persistentes Avanzadas (APTs)

A menudo, una entidad APT tiene el nivel más alto de recursos, incluida la inteligencia de código abierto (OSINT) y las fuentes de inteligencia encubiertas [9].

METODOLOGÍA DE LOS HACKERS

Típicamente, los hackers siguen una metodología que se divide en seis (6) pasos. Estos pasos tienen la finalidad de no tan solo lograr con éxito el ataque, sino más bien mantener el acceso y no dejar huella alguna [8]. En la Figura 1, se pueden apreciar los pasos que siguen los hackers para realizar sus ataques:

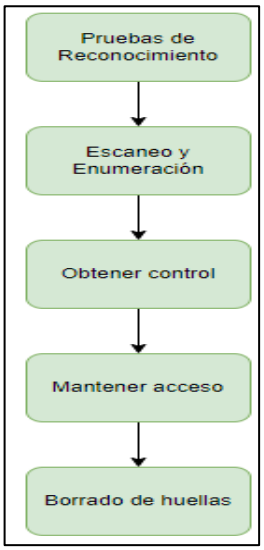

Figura 1
Metodología de los Hackers

A continuación, se describen más en detalle cada una de las fases:

- **Pruebas de reconocimiento:** Durante esta fase se trata de obtener la mayor cantidad de información del equipo o sistema que se desea atacar. Este proceso incluye identificar vulnerabilidades en el sistema [1]. Esta fase también es conocida como el proceso de obtención de información de forma pasiva. Algunas técnicas que entran en esta fase son la ingeniería social, investigación mediante la Internet y la búsqueda en vertederos (dumpster diving) [8].
- **Escaneo y enumeración**: Fase utilizada para que el hacker pueda determinar en efecto las características del sistema en términos de hardware y software. Durante esta fase, el hacker podría obtener información sobre la versión del sistema operativo y que aplicaciones se están utilizando, incluyendo sus versiones. Durante esta fase, se pueden utilizar aplicaciones como NMAP para identificar el estatus de los puertos de TCP/IP y aplicaciones asociadas a tales puertos. De igual forma, incluye el obtener la dirección IP del objetivo, cuentas de usuario, entre otros [1]. La fase de escaneo se encarga de tratar de conectarse activamente al equipo que se desea atacar y obtener una respuesta donde se pueden identificar el estatus de los puertos. Esta fase es una que involucra el proceso de obtención de información de forma activa [8].
- **Obtener acceso:** Es aquí donde realmente comienza la fase de ataque. Se utiliza la información obtenida de las dos fases anteriores con el fin de ingresar y tomar el control del sistema que se desea atacar a través de la red o de forma física. A esta fase se le conoce como "adueñarse del sistema" [1]. Es en esta fase donde el hacker se mueve de hacer pruebas a la red a atacarla (ceh). El acceso al sistema se puede lograr mediante una variedad de técnicas tales como una conexión inalámbrica abierta, sistema con poca seguridad, vulnerabilidades del sistema, ingeniería social, vulnerabilidades de aplicaciones web, entre otros [8].
- **Escalación de privilegios:** Aunque esta fase no está descrita en el diagrama, ya que básicamente es parte de lograr obtener el acceso. Es aquí donde el hacker intenta obtener privilegios administrativos mediante la técnica de escalación de privilegios. Esto se puede lograr explotando alguna vulnerabilidad o falla en el sistema o aplicación. Luego de que se logra la escalación de privilegios, el hacker podrá tener control completo del sistema e inclusive, de la red [8].
- **Mantener acceso:** Luego de ingresado al sistema en el paso anterior, el próximo paso consiste en lograr mantener acceso al sistema para que, en efecto, el hacker pueda volver a atacar el mismo. Esto se puede dar mediante cambios en el sistema, identificando huecos de seguridad, obteniendo contraseñas adicionales, colocando rootkits y mediante el uso de rastreadores (sniffers) [8].
- **Borrado de huellas**: Esta es la técnica donde el hacker intenta remover los archivos de registro u cualquier tipo de evidencia en el sistema atacado la cual pueda ser utilizada para identificarlo. De hecho, existen varias técnicas utilizadas por los hackers éticos que pueden ser utilizadas para identificar al hacker tales como las pruebas de penetración (Gupta). Por otra parte, el borrado de huellas puede darse mediante la modificación de archivos de registro, escondiendo archivos y carpetas y colocando rootkits [8].

HACKING ÉTICO

El hacking ético es una rama del área de seguridad de sistemas de información. También es conocido como prueba de penetración o más bien, hacking de sombrero blanco. Es un tipo de hackeo realizado por una persona u empresa que tiene el firme propósito de identificar vulnerabilidades, huecos de seguridad y fallas en los sistemas de computadoras o la seguridad de red de la

organización. Cabe mencionar que las técnicas o métodos utilizados en el hacking ético son bastante similares a las utilizadas en el hacking tradicional pero la diferencia estriba en que el primero es legal y se utiliza en una forma productiva. La información obtenida del hacking ético es utilizada para mantener la seguridad de los sistemas de información y mitigar los riesgos asociados a futuros ataques potenciales [1].

TIPOS DE ATAQUES

Existen varios tipos de ataques que los hackers realizan a los sistemas, entre los cuales destacan los siguientes:

- **Ataques no técnicos**: Se refiere a un tipo de ataque el cual incluye controlar a personas, clientes, empleados o inclusive a usted mismo. De hecho, una de las vulnerabilidades más grandes dentro de las empresas generalmente son sus propios empleados. Algunas formas en las que se comete este ataque incluyen el obtener información sensitiva mediante el engaño a las personas y también incluye el adentrarse en estructuras o cuarto de servidores para obtener datos. De igual forma, puede incluir técnicas de búsqueda en la basura para hallar información protegida, contraseñas, datos de la red, entre otros [2].
- **Ataques a nivel de red**: Este tipo de ataque suele ser simple, en vista de que una gran cantidad de redes pueden venir desde cualquier lugar en el planeta a través de la Internet. Algunos ejemplos de ataques a nivel de red son los siguientes [2]:
  - Inundación de la red con una gran cantidad de solicitudes, provocando una denegación de servicio (DoS, por sus siglas en inglés).
  - Instalación de un analizador de red para la captura de paquetes, como, por ejemplo, la herramienta Wireshark.
- **Ataques a nivel de sistema operativo**: Los ataques a los sistemas operativos siempre han sido de las técnicas más favorecidas por los hackers. Estos se aprovechan de las vulnerabilidades existentes en los sistemas operativos y explotan las mismas. Mayormente, se enfocan en sistemas operativos más utilizados comercialmente como Microsoft y Linux [2].
- **Ataques a nivel de aplicación**: Ejemplos de este tipo de ataque son los realizados por los hackers a programas de manejo de servicios de correos electrónicos como Microsoft Outlook y aplicaciones web. Ejemplos de este tipo de ataque incluyen, pero no se limitan a [2]:
  - Ataques a aplicaciones de HTTP (Hyper Text Transfer Protocol) y SMTP (Simple Mail Transfer Protocol).
  - Software de código malicioso que incluye infecciones, gusanos, trojanos y spyware. El código malicioso obstruye el funcionamiento de las redes y puede provocar que los sistemas colapsen.
  - Email basura (spam) que afecta la accesibilidad a la red y almacenamiento ya que inunda a los servidores de correos no deseados o innecesarios.

INSTRUMENTOS UTILIZADOS POR LOS HACKERS

Existe un sinnúmero de instrumentos que utilizan los hackers para cometer sus ataques e infiltrarse en los sistemas de información. Ciertamente, un hacker ético debe tener conocimiento pleno de estos instrumentos para poder diseñar técnicas que mitiguen los riesgos asociados a ataques realizados por estas. Entre los instrumentos más utilizados por los hackers, están los siguientes:

- **Caballos de troya**: Son proyectos maliciosos o software que se hace pasar por benigno utilizado con el fin de que el hacker logre acceso a la computadora objetivo. Un ejemplo de esto podría ser un programa que descargue de la web con la intención de mejorar el rendimiento de la computadora y resulte ser uno que solo se encarga de capturar las teclas que el usuario utiliza en la computadora. Estos también pueden

ser transferidos fácilmente por medios removibles, como las memorias flash USB [9].

- **Virus**: Un virus es un código que se ejecuta en la computadora objetivo sin el conocimiento del usuario de esta. Infecta la computadora con el código que se accede y ejecuta. Puede tener capacidad reproductiva y puede generar copias a través de la computadora si este es ejecutado por el usuario [9].
- **Gusanos**: Similar al virus, con la gran diferencia de que tiene la peculiaridad de que se replica de forma automática, mientras que un virus no. Se puede regar en otras computadoras. De igual forma, toman ventaja de los huecos en seguridad en el sistema operativo y aplicaciones, incluyendo puertas traseras (backdoors). Puede o no incluir otro código malicioso. No obstante, lo incluya o no, puede interrumpir el tráfico en la red y afectar las operaciones de la computadora debido a su naturaleza de replicación automática [9].
- **Ransomware:** Es un tipo de código malicioso que restringe el acceso a la computadora y demanda un ramson a ser pagado para devolver el acceso. Los archivos personales se encriptan y se bloquea la cuenta de usuario. El código malicioso incluido en el ramsonware informa al usuario que para poder desencriptar los archivos o desbloquear la computadora, se debe realizar un pago. Un ejemplo de este tipo de código malicioso es el CryptoLocker, el cual encriptaba cierto tipo de archivos en las unidades de disco de la computadora utilizando una llave pública [9].
- **Escáner de vulnerabilidad:** Instrumento utilizado por hackers para verificar de forma rápida las computadoras en una red para vulnerabilidades previamente conocidas. Hackers en su lugar, utilizan herramientas para escaneo de puertos como NMAP (Linux) y ZenMap (Windows). Ambas herramientas verifican que puertos en una computadora predeterminada están abiertos o accesibles para acceder a la misma [2].
- **Rastreador de red (sniffer):** Son herramientas utilizadas para monitorear el tráfico de la red con el fin de obtener información que viaja a través de la computadora o a través de la red. Ejemplo de un sniffer es la herramienta Wireshark [2].
- **Explotación (exploit):** Aplicaciones utilizadas para explotar vulnerabilidades [2].
- **Ingeniería Social:** Es una técnica, que, mediante el engaño, se trata de obtener información. Ejemplo de una herramienta para cometer ataques de Ingeniería Social lo es el Social Engineering Toolkit (SET) incluido en la distribución de Kali Linux [2].
- **Root kit**: Tipo de programa malicioso que le brinda al hacker la capacidad de introducirse a un dispositivo y tomar el control de este [10].

TIPOS DE HACKEO

Entre los distintos tipos de hackeo que existen, cabe mencionar los siguientes:

- **Trabajos internos**: La mayoría de las brechas de seguridad ocurren dentro de la misma red que está siendo atacada. Este tipo de ataque puede provenir de personas dentro de la organización, tales como empleados, exempleados, contratistas o asociados, los cuales tienen información acerca de las prácticas de seguridad de la organización, sus datos y sistemas de información [2].
- **Puntos de acceso no autorizado (Rouge Access Point):** Se refiere a un punto de acceso instalado en una red sin el permiso del administrador de red. Si el hacker es dueño del punto de acceso instalado de forma ilegal, este puede interceptar los datos que viajan a través de la red. Ciertamente, esto es un gran riesgo para cualquier empresa que haga uso de tecnología inalámbrica para permitir

dispositivos inalámbricos conectarse a la misma [2].

- **Puerta trasera (backdoor):** Permite al autor o creador del troyano administrar de forma remota la computadora víctima. Se emplea como control remoto para fines maliciosos [2].
- **Denegación de Servicio (DoS, por sus siglas en inglés):** Ataque que tiene la finalidad de paralizar una computadora, servidor o red, haciéndolos inaccesibles. Un ejemplo de este tipo de ataque es el enviar una cantidad de paquetes indeterminado a un equipo en particular, inundándolo de solicitudes con el fin de que su acceso a la red quede paralizado [2].
- **Denegación de Servicio Distribuido (DDoS, por sus siglas en inglés):** Similar al ataque DoS con la diferencia de que, en vez de venir de un solo equipo, puede provenir de varios equipos a su vez. Por ejemplo, se podría utilizar varias estaciones de trabajo o servidores para atacar una computadora objetivo o una red completa. Este tipo de ataque puede evitarse si se instala una herramienta para monitorear el tráfico de red [2].

HERRAMIENTAS DE HACKING

Existen un sinnúmero de herramientas que los hackers utilizan a su favor para cometer sus ataques. En el presente artículo, se mencionará las más utilizadas por estos. Cabe mencionar que gran parte de estas herramientas son creadas en ambientes de código abierto, por lo cual resulta imperativo que se familiarice con los sistemas operativos de código abierto como, por ejemplo, Linux.

- **NMAP:** Es un acrónimo de Network Mapper. Es una herramienta ampliamente utilizada para realizar pruebas de reconocimiento y auditoría en redes [11]. Además, permite identificar el estatus de los puertos, como, por ejemplo, ver que puertos están abiertos en una estación de trabajo remota. Ciertamente, es una herramienta que todo hacker o analista de red debe dominar.
- **Wireshark:** Herramienta utilizada para la captura de todo el tráfico en la red. Permite filtrar datos por protocolos e inclusive, puede llegar a capturar datos sensitivos como nombres de usuario con sus contraseñas [2].
- **Metasploit:** Herramienta ampliamente utilizada para asistir en las pruebas de penetración y provee información acerca de vulnerabilidades de seguridad. Se recomienda utilizarla dentro de la distribución Kali Linux [2].
- **Cain y Abel:** Herramienta de recuperación de contraseñas para ambientes de Windows. Utiliza varias técnicas de ataque para obtener la contraseña de un sistema. Tales técnicas pueden incluir ataques de fuerza bruta, por diccionario, entre otros [2].
- **Burp Suite:** Conjunto de aplicaciones utilizadas para realizar pruebas de penetración a aplicaciones web [2].
- **Aircrack-ng:** Herramienta incluida en algunas distribuciones de Linux que se utiliza para atacar redes inalámbricas. Para estos fines, se requiere una antena inalámbrica que pueda operar en modo monitoreo [2].
- **Nessus**: Herramienta de índole comercial que se utiliza para monitorear la red, identificando sus vulnerabilidades y clasificándolas de acuerdo con su nivel de riesgo. Se utiliza para hacer avalúos de vulnerabilidad en las redes [12].
- **Snort**: Se utiliza para análisis de tráfico en la red y registro de paquetes en redes basadas en IP (Internet Protocol). Snort puede detectar gusanos, vulnerabilidades, escanea puertos y detecta otros tipos de comportamientos sospechosos. Es una herramienta gratuita y es de código abierto. Viene para sistemas operativos Linux, Windows y Mac OS. Su último lanzamiento fue para el año 2015. No obstante, sigue siendo funcional para propósitos experimentales [13].
- **Angry IP Scanner**: Es una herramienta de código abierto multiplataforma que permite escanear direcciones IP y puertos. Permite identificar que equipos están conectados en un

segmento de red y cual o cuales de estos se encuentran activos [14].

- **Putty**: Es un excelente instrumento para el hacker ya que permite, una vez obtenida la información de la computadora objetivo, ingresar a la misma mediante los protocolos SSH (Secure Shell) o Telnet (Telecommunication Networks). Muchas veces se utiliza esta herramienta para pasar por encima de los parámetros de seguridad del firewall mediante SSH [2].

Técnicas de Protección ante Ataques

En vista de los diferentes ejercicios que los hackers éticos han hecho para identificar vulnerabilidades en la red, gran parte de estos recomiendan lo siguiente [2]:

- **Seguridad a nivel de infraestructura**: Los hackers éticos recomiendan ampliamente que el firewall esté debidamente configurado y que se establezca un monitoreo periódico de este para identificar actividad sospechosa o anómala.
- **Sistema de detección de intrusos (IDS, por sus siglas en inglés)**: Es un sistema de monitoreo que detecta actividad sospechosa y genera una alerta cuando estas son detectadas. Tales alertas son utilizadas por analistas de seguridad para investigar el problema existente y tomar acciones preventivas para remediar la amenaza.
- **Revisión de Código**: Es el proceso de revisar el código fuente de una aplicación para identificar fallas en seguridad o vulnerabilidades. Se enfoca en identificar errores de lógica para posteriormente corregir los mismos. Este es un proceso que se recomienda que se haga de forma periódica para hacer que el código sea lo más robusto posible.
- **Parchos de Seguridad**: Resulta imperativo que se instalen los parchos de seguridad, tanto a nivel de sistema operativo como de aplicaciones. Es un método de actualización de sistemas, aplicaciones o programas mediante la inserción de código para parchear o corregir la vulnerabilidad. Esto tiene como efecto el hacer el sistema más robusto ante cualquier ataque (solar winds.com).

Ejercicio de Ejemplo: Ataque HTTP

Para este ejercicio práctico, se hará un ataque el cual consiste en capturar el tráfico de red utilizando Wireshark para capturar los paquetes que se transmiten a través de un protocolo HTTP. Se utilizará una página web la cual pide unas credenciales de acceso para ingresar a una base de datos. Cabe mencionar que al utilizar un protocolo como lo es el HTTP, este no provee ningún mecanismo de seguridad para cifrar el nombre de usuario y la contraseña. A continuación, se muestran los pasos para llevar a cabo este ejercicio. Al final, se establecen las recomendaciones para evitar este tipo de ataque.

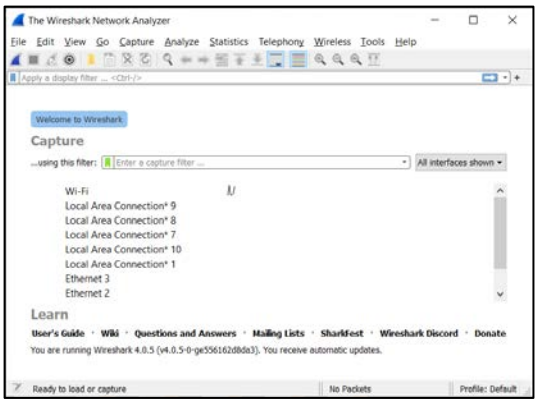

Figura 1
Pantalla Principal de Wireshark

El primer paso consiste en ejecutar la aplicación de Wireshark en su computadora. Para estos fines, se utilizará un ambiente de trabajo de Microsoft Windows 10. Es importante que se seleccione la interfaz que se utilizará para capturar el tráfico de la red. En este sentido, se utilizará el adaptador de red inalámbrica, ya que la computadora que se está utilizando para este ejercicio cuenta con conexión a la red de forma inalámbrica. Recuerde que Wireshark es una herramienta utilizada para la captura de todo el tráfico en la red. Permite filtrar datos por protocolos e inclusive, puede llegar a

capturar datos sensitivos como nombres de usuario con sus contraseñas [2]. Una vez comience la captura de paquetes, la herramienta lo realizará de forma infinita hasta que usted como usuario decida parar la misma, para esto, debe presionar el botón color rojo ubicado en la parte superior izquierda de la aplicación. Durante este ejercicio, se utilizará este botón una vez se capture lo que se desea.

Una vez le dé doble clic a la interfaz, inmediatamente saldrá la siguiente ventana de Wireshark. Es en estos momentos donde ya la aplicación se encuentra capturando paquetes, o más bien, el tráfico en la red.

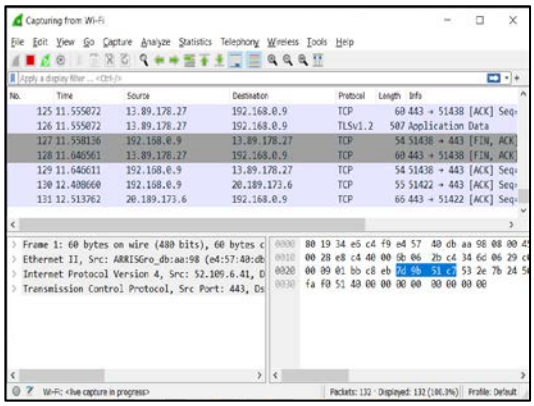

Figura 2
Captura de Paquetes en Wireshark

El próximo paso consiste en que se ingrese a la página web de prueba, la cual utiliza el protocolo HTTP. Para estos fines, se ingresará a la siguiente página web: http://www.techpanda.org/. Ingresar las credenciales de acceso, en este caso, se utilizarán los siguientes:

- Correo electrónico: admin@google.com
- Contraseña: Password2010

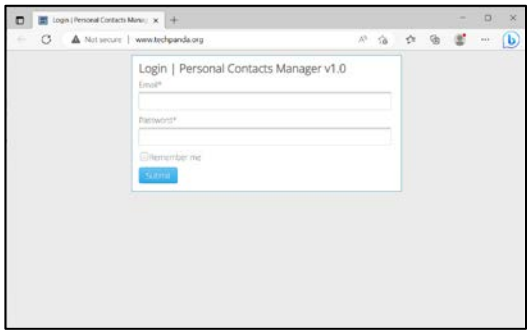

Figura 3
Página de Prueba con HTTP

Posteriormente, presionar el botón de Submit y lo redirigirá a una base de datos de prueba.

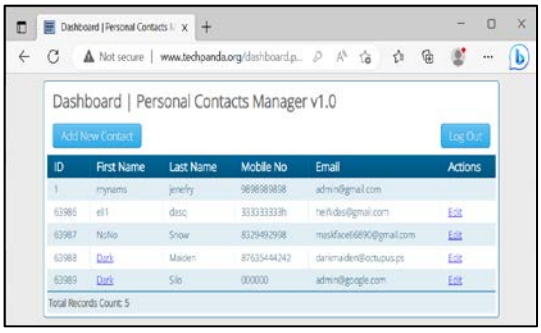

Figura 4
Bases de Datos de Prueba

Próximo paso consiste en volver a la aplicación de Wireshark y presionar el botón rojo para parar la captura de paquetes. Luego, debe aplicar el filtro escribiendo la palabra HTTP para filtrar la captura de paquetes. Posteriormente, debe buscar en la columna de información el método POST, ya que este es el que se encarga de enviar las credenciales de acceso al servidor para corroborar en efecto la identidad de la persona que desea acceder al sistema. En la siguiente imagen (ver Figura 5), se puede apreciar la captura de las credenciales de acceso.

Ciertamente, para evitar este tipo de ataque, se recomienda utilizar el protocolo HTTPS ya que este provee un mecanismo de seguridad adicional que el protocolo HTTP no ofrece. Este protocolo provee un mecanismo de cifrado para aumentar la seguridad en la transferencia de datos. El propósito del HTTPS es que se pueda intercambiar información de forma seguridad sin que esta sea interceptada por aplicaciones como Wireshark.

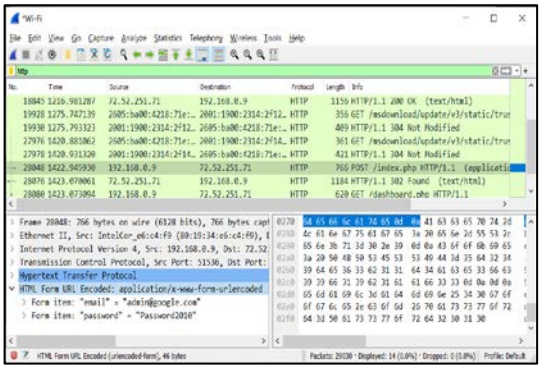

Figura 5
Captura de Credenciales de Acceso

CONCLUSIÓN

Para poder proteger a una empresa de algún ataque provocado por un hacker, resulta imperativo que se contrate a un hacker ético, ya que este ciertamente tendrá todas las destrezas y habilidades necesarias para identificar las vulnerabilidades de la empresa e implementar métricas correctivas para disminuir o eliminar los riesgos asociados a ataques. Como se pudo apreciar en el artículo, los hackers éticos deben tener las mismas destrezas y habilidades que un hacker de sombrero negro, con la diferencia principal que el primero utiliza sus conocimientos para el bien de la empresa. El hacking ético es un instrumento, que, si es utilizado legítimamente, puede demostrar ser efecto en el entendimiento de las vulnerabilidades de una red y como estas pueden ser explotadas y/o corregidas. Las empresas deben ver al hacker ético como un activo que busca salvaguardar su activo más importante, que es la información.

REFERENCIAS

[1] A. Gupta and A. Anand, "Ethical hacking and hacking attacks," in *International Journal of Engineering and Computer Science*, 2017. Doi:10.18535/ijecs/v6i4.42

[2] S. Kumar and D. Agarwal, "Hacking Attacks, Methods, Techniques and Their Protection Measures," in *IJSART*, Apr. 2018, vol. 4, no. 4, pp. 2253–2253.

[3] A. Ushmani, "Ethical Hacking," in *International Journal of Information Technology (IJIT)*, 2018, vol. 4, no. 6, pp. 1–4.

[4] L. Smith, M. M. Chowdhury, and S. Latif, "Ethical hacking: Skills to fight cybersecurity threats," in *EPiC Series in Computing*, 2022, vol. 82, pp. 102–111.

[5] R. Hartley, D. Medlin, and Z. Houlik, "Ethical Hacking: Educating Future Cybersecurity Professionals," in *Proceedings of the EDSIG Conference*, 2017, pp. 1–10.

[6] A. A. Farsole, A. G. Kashikar, and A. Zunzunwala, "Ethical hacking," in *International Journal of Computer Applications*, 2010, vol. 1, no. 10, pp. 14–20. Doi:10.5120/229-380.

[7] S. Tulasi, "Ethical Hacking and Types of Hackers," in *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)*, Oct. 2014, vol. 11, no. 2, pp. 24–27.

[8] M. Gregg, *CEH Certified Ethical Hacker Cert Guide*, 1st ed., Pearson Technology Group, 2022.

[9] D. L. Prowse, CompTIA Security+ Sy0-501 Cert Guide. Indianapolis, IN: Pearson Education, Inc., 2018.

[10] Kaspersky. (2023). *Qué es un rootkit: Definición y explicación* [En línea]. Disponible: https://latam.kaspersky.com/resource-center/definitions/what-is-rootkit. [Accedido: 16-mayo-2023].

[11] Nmap.org. (s. f.). Nmap Network [En línea]. Disponible: https://nmap.org/. [Accedido: 16-mayo-2023].

[12] Tenable. (2023). *Evaluación de Vulnerabilidades Nessus* [En línea]. Disponible: https://es-la.tenable.com/products/Nessus. [Accedido: 16-mayo-2023].

[13] Sectools.org. (s. f.). *SecTools.Org Top Network Security Tools* [En línea]. Disponible: https://sectools.org/. [Accedido: 16-mayo-2023].

[14] Angry IP Scanner. (s. f.). *Angry IP Scanner - the original IP scanner for Windows, Mac and Linux* [En línea]. Disponible: https://angryip.org/. [Accedido: 16-mayo-2023].