HACKING ETICO: IMPACTO EN LA SOCIEDAD

Miguel Angel Sánchez Avila.
Especializacion Seguridad Informática.
Universidad Piloto de Colombia.
Bogotá, Colombia.
Ing_miguelsanchez@hotmail.com.

***Abstract*: Today, security is the main problem. Almost all the work is done over the internet crucial data are sent over the web and other information is placed over internet. While all the data is available online, there are many type of users who interact with data some of them for their need and others for gaining knowledge that how to destroy the data without the knowledge of the owner. There are various techniques used for protection of data but the hacker (or cracker) is more intelligent to hack the security, basically there are two categories of hackers that are different from each other on the basis of their intensions. The one who has good intensions are known as ethical hackers because they ethics to use their skill and techniques of hacking to provide security to the sensitive data of the organization. The cracker break the safety of someone with malicious intentions or bad intentions to steal or damage important information.**

I. INTRODUCCIÓN.

Dado que la información hoy en día es uno de los activos más importantes de las organizaciones, crece la necesidad fundamental de buscar los diferentes métodos, estrategias y tecnologías para proteger dicha información, con el objetivo de garantizar y preservar la confidencialidad, integridad y disponibilidad como eje fundamental.

Durante el paso de los años se ha evidenciado el crecimiento que han tenido las diferentes herramientas tecnológicas que se han desarrollado, con el objetivo de brindar mayores facilidades y comodidades en las labores que desarrolla el hombre en su día a día, con el desarrollo de estas herramientas se generó un gran conocimiento tanto es su uso como aplicabilidad (una orientada a aprovechar y sacar utilidad de las herramientas creadas y otras personas poco éticas orientadas a aprovecharse de las vulnerabilidades de esas herramientas con fines poco éticos y fraudulentos) de aquí donde nacen dos conceptos fundamentales Hacker, Cracker, a continuación se describen algunas de las características y habilidades de estos conceptos, ver Figura1.

Cracker	*Hacker*
Robo de identidad	Accesos por conocimiento
Acciones fraudulentas	Fines pedagógicos
Cyber-Crimen	Hacking Ético
Cyber-Guerra	

Figura 1: Hacker – Cracker características, 07 de Diciembre de 2015, Imagen del autor.

II. ETHICAL HACKING.

Antes de definir hacking ético vamos a definir hacking.

El hacking consiste en acceder desde algún lugar del ciberespacio a un ordenador privado valiéndose de deficiencias en los sistemas de seguridad, aprovechando su vulnerabilidad u obteniendo contraseñas de acceso haciéndose pasar por usuarios legítimos. Según Peter G. Neuman (1984), científico en computación, el hacking es una intromisión maliciosa que trata de hurgar entre datos buscando información valiosa, en conclusión, se trata de una intromisión ilegal a sistemas de computación ajenos.

[1]. Hacking ético es el término inicialmente usado por los profesionales para hacer el sistema más seguro y confiable. Una persona es llamada como un hacker ético cuando no destruye la seguridad en los sistemas, tiene cuidado con la seguridad y salvaguardara el sistema desde el punto de vista del Hacker. Evalúa la seguridad e identifica vulnerabilidades en sistemas, redes o infraestructura de sistemas, esto incluye encontrar y explotar algunas vulnerabilidades para determinar cuándo hay acceso sin autorización u otras actividades maliciosas. Las personas que realizan este esfuerzo y tienen este conocimiento son conocidas como hackers éticos o hackers blancos.

El hacking ético tiene dos significados o definiciones:

Uno es el hobby o profesión de una persona en particular que está interesada en hacer una carrera en este campo. La otra es que con los conocimientos obtenidos en el área de tecnología o área afines y con herramientas explotan o rompen los sistemas para un propósito específico, los cuales pueden ser beneficios económicos, reconocimiento u alguna otra ganancia que se obtenga por extraer, modificar o eliminar información.

Algunos de los motivos por los que se realiza hacking, según Kenneth Himma (2007), profesor de Filosofía en la Universidad de Seattle, son:

Por cuestiones de seguridad: para demostrar la vulnerabilidad de un sistema o sus debilidades.

Por inactividad del sistema: porque no se explota totalmente su capacidad.

Con fines de aprendizaje: entrar a un sistema con el fin de instruirse.

En pro de la sociedad: irrumpen para descubrir casos de abusos o delitos en contra de la sociedad, manteniendo una especie de vigilancia, en este caso el hacker es considerado un protector; esta tendencia es más fuerte en Europa que en Estados Unidos, sin embargo, no es muy claro qué tan efectiva es para solucionar dichas infracciones.

III. TIPOS DE HACKING ÉTICO.

Existen principalmente cuatro tipos diferentes de hacking ético según el conocimiento del Hacker.

A. Hacktivistas.

Esta es la técnica mediante la cual un hacker informático está ingresando ilegalmente a cualquier sistema informático por cualquier motivo, ya sea social o político. En esta actividad, un hacker informático puede dejar un mensaje muy grande en la página principal de cualquier sitio web conocido o cualquier otro mensaje importante para que el visitante vea ese mensaje y reaccione en consecuencia. Puede mostrar cualquier tipo de discurso o cualquier mensaje social que pueda atraer a los usuarios. Esto puede llevar a ingresar al sistema sin el consentimiento del objetivo. Puede tener cualquier mensaje social, como el hacker ético es ético o no, lo que puede atraer a muchos usuarios.

[2]. Quizás lo que mejor que define a uno de estos grupos hacktivista más conocidos sea su lema:

Figura 2: Grupo hacktivista , Imagen del autor.

“El conocimiento es libre. Somos anónimos. Somos legión. No perdonamos. No olvidamos. ¡Esperadnos! “

A este grupo se les han atribuido ataques a webs oficiales del gobierno Chino, a la web de Justicia Británica y al Instituto Tecnológico de Massachusetts, o el robo de un gran número de perfiles de usuario del portal SonyPictures.com en 2011. Pero quizás por el hecho que más se les conoce a nivel mundial es por declarar de forma abierta su “guerra” al Estado Islámico tras los atentados de Charlie Hebdo y Paris en noviembre de 2015. Por ejemplo, publicaron en una web el listado de unos 9.200 tuiteros, supuestamente afines y vinculados a ISIS, así como una guía para ‘hackear’ el Estado Islámico, además de difundir un vídeo en el que advierten que dirigirán “numerosos ciberataques” a los yihadistas.

A parte de Anonymous no se puede dejar a Wikileaks con su fundador Julian Assange que han hecho públicos informes y documentos con contenido sensible en materia de interés público, o a Snowden que filtró documentos de la CIA.

B. Cyber-Warrior

[3]. Un cyber-warrior es una persona que participa en la guerra cibernética, ya sea por razones personales o por creencias patrióticas o religiosas. La guerra cibernética puede perseguirse para defender los sistemas informáticos y de información, o para atacarlos. Los guerreros cibernéticos vienen en diferentes formas, dependiendo de sus roles, pero todos se relacionan con la seguridad de la información de una forma u otra.

Los países que no pueden igualar a los EE. UU. En términos de tecnología militar han recurrido a la guerra cibernética, un método que todavía puede hacer mucho daño en términos de costo económico. Varias agencias en los Estados Unidos están bajo ataque constante de numerosos países. En respuesta, el ejército de Estados Unidos está entrenando a veteranos de guerra y soldados heridos que ya no pueden luchar en el campo en el arte de la guerra cibernética para convertirse en guerreros cibernéticos y continuar defendiendo a su país en esta nueva forma de batalla. Dado esto, el término ciber-guerrero tiene diferentes significados según el contexto en el que se usa; el término puede referirse a alguien con intenciones maliciosas (el atacante) o a un profesional que esté trabajando para defenderse contra tales atacantes. El último contexto es un campo profesional emergente, similar al hackeo ético.

Uno de los grupos conocidos es:

Figura 3: Grupo Cyber-warrior, Imagen del autor.

La misión de este grupo es:
- Evitar ataques a nuestras creencias y valores morales.
- Nuestras acciones contra el estado y nuestro país.
- Eventos que afectan adversamente a la conciencia pública y pública, es un grupo hacktivista que lucha contra el mundo virtual.

¿Que han realizado?

Para Turquia, el 4 de Julio de 2003 Piratearon 1500 sitios estadounidenses Se hizo mucho eco sobre estos ataques en todo el mundo.

Contra los ataques de hackers brasileños, conocidos como los mejores hackers del mundo, que han librado una guerra

contra los sitios turcos, especialmente los sitios oficiales; hackearon más de 10,000 sitios de Brasil. Como resultado de estos ataques, Brasil llegó al número 1 en la lista de los países más hackeados.

Han entregado muchos documentos de confidencialidad que no han sido revelados aún.

Para Seguridad Corporativa, Brindan soporte de seguridad gratuito para muchas organizaciones oficiales como gov.tr y pol.tr dentro de Cyber Security.

C. Pruebas de penetración de caja blanca.

Las pruebas de penetración de caja blanca también se denominan hackers de caja blanca. Son los empleados contratados por la organización para ingresar a su sistema o red de computadoras actual. Son los probadores legales de penetración. Están irrumpiendo legalmente el sistema o en la red de computadoras de la organización o de un individuo para ayudarlos, explicando las vulnerabilidades y las debilidades del sistema actual.

Las pruebas de caja blanca funcionan de la misma manera que los Cyber-Warrior. La única diferencia es que los Cyber-Warrior no tienen conocimiento del sistema o la red de computadoras de la organización o del individuo, mientras que los hackers informáticos de caja blanca tienen pleno conocimiento del sistema, red o la computadora. También se puede considerar que el ataque está siendo simulado por un interno de la organización.

Una prueba de penetración (prueba de pluma) a menudo se confunde con un análisis de vulnerabilidad, una auditoría de cumplimiento o una evaluación de seguridad. La penetración va más allá de las comprobaciones del sistema y hace lo siguiente:

- Lleva la información de exploración de vulnerabilidad a un nivel más alto.
- Si descubre vulnerabilidades durante un pen-test, puede explotar esas vulnerabilidades para probar o refutar el potencial ataque del mundo real.
- Se enfoca en el individuo o equipo de evaluadores.
- Es importante tratar de entender los posibles motivos sobre las modalidades sofisticadas en este tipo de pruebas.
- Busca información sobre la efectividad real de su sistema de seguridad.
- Una vez más, el motivo es clave con las pruebas de penetración. Se trata de determinar si el sistema, sin importar qué tan avanzada sea su seguridad, puede hacer frente a un hacker sigiloso e implacable.
- Considera múltiples vectores de ataque contra el mismo objetivo.
- Limita el alcance de las amenazas, como centrarse únicamente en el vector de su navegador de Internet, limita su comprensión de su sistema y su disposición para protegerlo.

D. Hacker ético certificado.

Como su nombre lo indica es un hacker ético certificado o un realizador de pruebas de penetración con licencia, son aquellos profesionales certificados o con licencia en el campo de seguridad que desempeñan las funciones de hacker ético de caja negra y de caja blanca. Son responsables de investigar el sistema y las redes para descubrir las vulnerabilidades y debilidades.

Estas certificaciones o licencias son otorgadas por el Consejo Internacional de Consultores de Comercio Electrónico. Los hackers éticos deben recertificarse cada tres años.

[4]. Algunas certificaciones reconocidas:

1). Certified Ethical Hacker por EC-Council.

Figura 3: Certificación CEH, Imagen del autor.

Es un amplio programa de hacking ético y de formación de seguridad en redes para cumplir con los más altos estándares para profesionales. Cientos de pymes y autores han contribuido al contenido que se presenta en el material pedagógico del CEH. En cada pack se ofrecen las últimas herramientas y exploits descubiertos en la comunidad.

2). Gerente Certificado de Seguridad de la Información (CISM) por ISACA.

Figura 4: Certificación CISM, Imagen del autor

El CISM es el estándar aceptado globalmente para las personas que diseñan, construyen y gestionan los programas de seguridad de la información empresarial. CISM es la principal certificación para administradores de seguridad de la información. El último índice trimestral de valoración de Habilidades y Certificaciones IT (ITSCPI) de Foote Partners

clasificó a CISM como la más codiciada y la que más se paga de las certificaciones de seguridad.

3). Profesional Certificado de Sistemas de Información de Seguridad (CISSP) por ISC2.

Figura 5: Certificación CISSP, Imagen del autor.

La certificación CISSP es un estándar reconocido a nivel mundial que confirma el conocimiento de un individuo en el campo de la seguridad de la información. Los certificados en CISSP son profesionales de la seguridad de la información que definen la arquitectura, el diseño, la gestión y/o los controles que garantizan la seguridad de los entornos empresariales. Fue la primera certificación en el ámbito de la seguridad de la información para cumplir con los estrictos requisitos de la norma ISO/IEC 17024.

IV. TIPOS DE HACKERS

De acuerdo a la manera de trabajo o basado a sus intenciones un Hackers puede ser clasificado dentro de tres grupos.

1). Hacker blancos.

Es un especialista de seguridad computacional que rompe y encuentra vulnerabilidades en redes protegidas o sistemas computacionales de algunas organizaciones o compañías, corrigen y mejora aquellas vulnerabilidades mejorando la seguridad de los sistemas. Usan sus habilidades y conocimiento para proteger la organización antes de que un hacker malintencionado encuentre y hago daño a la organización.

2). Hacker Negros.

También conocidos como "Cracker" es un experto en software y hardware de computadores quienes rompen la seguridad de alguien con intenciones maliciosas o intenciones malas para robar o dañar la información importante, comprometiendo la seguridad de grandes organizaciones, apagando o alterando funciones de sitios web o redes. Violan la seguridad para su beneficio, realizan cibercrimen como robo de identidad y fraude en tarjetas de crédito.

3). Hacker Grises.

Es un experto que algunas veces viola las leyes, aunque no tiene intenciones maliciosas como los hackers negros, representan a los hackers blancos porque operan y mantienen la seguridad del sistema y los hackers negros cuando mal intencionalmente explotan los sistemas computacionales.

El conocimiento de un hacker ético es muy similar al de un hacker real. Se ha sabido que algunos hackers negros se han convertido en hackers blancos y ahora están utilizando sus conocimientos de pentesting y hacking en sistemas de información de una manera ética. Es muy controversial contratar hackers éticos que hayan sido hackers negros, ya que el hacker ético tendrá autorización por parte del propietario de la información para ingresar y posteriormente podrá ver información sensible, entonces se necesita que sea extremadamente confiable, ya que puede posteriormente realizar un ataque como hacker para su propio beneficio.

Durante esta asignación, un hacker ético accederá a la información sensible y confidencial del cliente, podrá ver y descubrir los puntos débiles de los clientes. Por eso muchas empresas no creen en contratar a hackers previos para la realización de ataques éticos, según la comprensión es que al realizarlo, implicaría un nivel de riesgo y seguridad muy alto.

V. METOLOGIA ETHICAL HACKING

El procedimiento de hacking ético tiene básicamente cinco etapas diferentes. Cualquier hacker ético seguirá estas etapas una por una y alcanzará su objetivo. La Figura 6 muestra las cinco etapas de hacking ético que están siendo seguidas por cualquier Hacker ético en un sistema informático.

Fig.6 Completa metodología de Ethical Hacking.

A. Reconocimiento.

Objetivo: obtener la mayor información posible sobre la organización, también conocida como foot printing. El significado literal de reconocimiento significa una encuesta preliminar para obtener la información.

Personas físicas: recopilar emails, direcciones físicas, información de cuentas de redes sociales (Facebook, Twitter, etc.).

Corporaciones: obtener direcciones ip, DNS (AAA, A, PTR, MX), servidores de correo, archivos públicos.

1). Metodologías de auditoria:

Tipo Caja Blanca: la persona que realiza las pruebas tiene disposición de información sobre la infraestructura de la empresa y ya se tiene contemplado el alcance del análisis.

Tipo de Caja Negra: la persona que realiza la prueba no tiene información sobre el objetivo, en este caso la fase de reconocimiento es fundamental.

Híbridos: es la utilización de los tipos anteriormente mencionados.

2). Técnicas que realizan en esta etapa.

Footprinting (obtener rango de red, subredes, host de activos, puertos abiertos, S.O etc.).

Ingeniería Social: La Ingeniería Social es el conjunto de actividades o engaños que los atacantes usan para obtener información o bienes de las organizaciones a través de la manipulación de los usuarios legítimos. Es decir, la Ingeniería Social es la ciencia y el arte de hackear a las personas.

A pesar de que las tecnologías que mitigan las vulnerabilidades informáticas evolucionan rápidamente, es fácil olvidarse del elemento más importante presente en todas las TIC: el ser humano. Por lo tanto, es importante que las personas conozcan los procedimientos que pone en peligro la seguridad de la información.

Durante esta fase de reconocimiento, se pueden utilizar diferentes tipos de herramientas, como el mapeo de redes y el análisis de vulnerabilidades de la red, un ejemplo es Cheops-ng**;** es una herramienta de administración de redes para mapear y monitorear la red.

B. Escaneo.

La siguiente etapa de ethical hacking es el escaneo. Con esta técnica, la persona que realiza la prueba puede encontrar fácilmente las puertas abiertas para cualquier red. En esta etapa, un hacker siempre trata de hacer un esquema de la red objetivo. El esquema incluye las direcciones IP de la red final o de destino que están activas, detección de host activos, escaneo de puertos, detección del Sistema Operativo, identificación de vulnerabilidades, etc. En algunos de los casos, la mayoría de los escáneres de vulnerabilidades realizan un trabajo maravilloso de minimizar los aspectos positivos, y muchas organizaciones los utilizan para reconocer sistemas obsoletos o una posible experiencia nueva que podría ser explotada por hackers informáticos.

1). Tipos de escaneo.

-Escaneo de puertos.

Con la ayuda del moderno escaneo de puertos que utiliza el protocolo TCP, podemos incluso saber qué sistema operativo se está ejecutando en los hosts en particular. En el término tecnológico, el escaneo de puertos se utiliza principalmente para descubrir las vulnerabilidades y los puntos débiles del puerto utilizado en la red. En este proceso, tenemos que ubicar el host activo, el sistema operativo que se está utilizando, los firewalls, los sistemas de detección de intrusos, los diferentes servidores y servicios que se ejecutan en esos servidores, dispositivos de límites, topologías de enrutamiento y otras topologías utilizadas en la red de la organización objetivo. Al utilizar la técnica de foot printing, podemos rastrear la dirección IP de la organización objetivo. Una vez que se encuentra la dirección IP, la exploración de los puertos TCP y UDP del sistema de destino se vuelve bastante fácil para el hacker ético para mapear la red. La herramienta de mapeo de redes más común y popular es Nmap, que es muy potente y flexible y muy fácil de usar. El mapeador de red Nmap está disponible para varios sistemas operativos, Linux y Windows. Además de Nmap, hay muchas herramientas de mapeo de red disponibles en Internet como netscantools, Superscan, Unicornscan, Scanrand y Portscan.

-Escaneo de Red.

En el escaneo de la red se identifican todos los hosts activos que están presentes en una red. El propósito de este ejercicio es atacarlos o evaluar la seguridad de la red. En este procedimiento, conoceremos las direcciones IP de cada host. Todas las herramientas de escaneo de red podrán informarnos sobre los hosts activos y sus direcciones IP correspondientes en la red.

-Escaneo de vulnerabilidades.

En el escaneo de vulnerabilidades, el hacker ético conocerá el sistema operativo del sistema y otros detalles relacionados con el sistema operativo, como su versión, el paquete de actualización, si está instalado. El escáner de vulnerabilidades identificará la debilidad del sistema operativo para que luego pueda ser atacado. El escaneo de vulnerabilidades generalmente se refiere al escaneo de sistemas que están conectados a Internet.

Dentro de las principales herramientas que se utilizan se encuentra:

[5]. Nessus: es el estándar mundial para la prevención de ataques de red, identificación de vulnerabilidades y detección de problemas de configuración que utilizan los hackers para entrar en la red. Nessus se ha utilizado por más de 1 millón los usuarios en todo el mundo, por lo que es el líder mundial de evaluación de la vulnerabilidad, configuración de seguridad y cumplimiento de las normas de seguridad.
Consiste en un Daemon, nessusd, que realiza el escaneo en el sistema objetivo, y nessus, el cliente (basado en consola o gráfico) que muestra el avance e informa sobre el estado de los escaneos.

Openvas: (Open Vulnerability Assessment System,1 inicialmente denominado GNessUs), es una suite de software, que ofrece un marco de trabajo para integrar servicios y herramientas especializadas en el escaneo y gestión de vulnerabilidades de seguridad de sistemas informáticos.

C. Obtener Acceso.

Esta es la fase más importante en la que los atacantes obtendrán el acceso al sistema o la red y podrán estropearlo

por completo. Además, también es cierto que el atacante no siempre debe tener acceso al sistema para dañarlo. Se puede decir que esta es la etapa en la que realmente tiene lugar un Hackeo real. Esos puntos débiles y las vulnerabilidades que se exponen durante la fase de reconocimiento y exploración se explotan aún más para obtener acceso en el sistema objetivo. El método de conexión que utilizará un atacante o hacker ético para dañar el sistema puede ser la red de área local, el acceso local a la computadora e Internet. Hay algunos ejemplos más de lo mismo que son: desbordamientos de búferes (buffer overflows), secuestro de sesión y denegación de servicio, etc. El acceso también se conoce como propietario del sistema en el mundo de la seguridad, lo que significa que ahora el atacante o hacker ético tendrá acceso completo al objetivo. Los factores que influyen en las posibilidades de que un atacante obtenga acceso a un sistema objetivo incluyen en la arquitectura y la configuración del sistema objetivo, el nivel de habilidad del perpetrador y el nivel primario de acceso obtenido. Uno de los tipos más dañinos de los ataques de denegación de servicio que pueden distribuirse en varios ataques de denegación de servicio, donde un hacker utiliza un tipo especial de software llamado "zombie" y lo distribuye en varias máquinas en Internet de tal manera que el número máximo de máquinas pueda ser dañado.

Una de las herramientas utilizada en esta atapa es:

[6]. Metasploit Framework: es un proyecto de código abierto que ayuda a investigar las vulnerabilidades de seguridad. Vulnerabilidades conocidas, en las cuales tienen también unos módulos, llamados payloads, que son los códigos que explotan estas vulnerabilidades.

También dispone de otros tipos de módulos, por ejemplo, los encoders, que son una especie de códigos de cifrado para evasión de antivirus o sistemas de seguridad perimetral.

Otra de las ventajas de este framework es que permite interactuar también con herramientas externas, como Nmap o Nessus. Además ofrece la posibilidad de exportar malware a cualquier formato, ya sea en sistemas Unix o Windows.

Destacar también que es multiplataforma y gratuita, aunque tiene una versión de pago, en la que se ofrecen exploits ya desarrollados, pero cuyo coste es bastante elevado. La versión gratuita es muy interesante porque contiene todas las vulnerabilidades públicas.

D. Mantener el Acceso.

El objetivo es instalar y ejecutar en el host atacado un software malicioso que permita mantener un canal de conexión abierto.

Después de que un hacker accede al sistema objetivo, sería muy fácil para él utilizar el sistema y todos sus recursos y explotarlos. Este también es el caso en este contexto en el que un hacker puede usar este sistema objetivo como plataforma de lanzamiento para que pueda escanear otros sistemas y dañarlos. De esta manera se puede explotar toda una organización. Hay muchos atacantes o hackers informáticos que no se han detectado y siguen eliminando todas las pruebas de su entrada en el sistema objetivo. Utilizan una puerta trasera o un troyano para obtener el acceso repetido en el sistema. Hay una opción más: pueden instalar un rootkit en el nivel del kernel del sistema operativo y pueden tener el súper acceso al sistema. Con la ayuda de troyanos, los hackers informáticos pueden obtener información de los usuarios, nombres, contraseñas y otra información confidencial, como el número de tarjeta de crédito.

E. Tarea de Limpieza.

Esta es la última etapa en la que el hacker desea eliminar o destruir toda la evidencia de su presencia y sus actividades por diversos motivos, como mantener el acceso y evadir acciones que lo involucren. Borrar evidencia es el requisito para que un hacker permanezca oscuro u oculto. Es realmente muy importante para los invasores hacer que el sistema se vea igual que antes de obtener acceso y establecer puertas traseras para su uso. Cualquier archivo, que haya sido modificado o alterado, debe volver a cambiarse a sus atributos o formato originales. La información que aparece en la lista, como el tamaño y la fecha del archivo, es solo información contenida en el archivo. A continuación se presentan algunas actividades que están presentes durante esta fase.

1). Esteganografia.

En términos informáticos, es la disciplina que estudia el conjunto de técnicas cuyo fin es la ocultación de información sensible, mensajes u objetos, dentro de otros denominados ficheros contenedores, normalmente multimedia: imágenes digitales, vídeos o archivos de audio, con el objetivo de que la información pueda pasar inadvertida a terceros y sólo pueda ser recuperada por un usuario legítimo.

2). Usando un protocolo de tunelización.

Es un protocolo que encapsula en su datagrama otro paquete de datos completo que utiliza un protocolo de comunicaciones diferente. Esencialmente, crea un túnel entre dos puntos de una red por el cual se puede transmitir de forma segura cualquier tipo de dato.

3). Alterar archivos de registro (Logs).

Los archivos de logs son eventos que ocurre en el sistema operativo (actualizaciones, modificaciones, instalaciones, apagado, errores etc.) de forma cronológica, ejemplo; visor de eventos en los sistemas operativos Windows de Microsoft.

Algunos programas utilizados:

Steghide: herramienta utilizado en Kalilinux para ocultar información en diferentes tipos de archivos.

Para alterar los log se utilizan comandos propios de cada Sistema operativo.

Se utilizan protocolos como PPTP, SSH e IPsec para realizar conexiones seguras (VPN), evitando que el canal puede ser monitoreado.

VI. IMPACTO DEL HACKEO ÉTICO EN LA SOCIEDAD

Los hackers están teniendo un impacto muy importante en la sociedad. Ellos están atrayendo a generaciones de jóvenes cada día más. Aunque el hacking ético no es malo, también es muy importante saber qué hacen exactamente para el interés de la sociedad. Si tratamos al hacker como la persona que impulsa la tecnología más allá de las normas percibidas, hay varios campos de la computación en los que el hacker etico o hacker tienen un impacto importante. Hoy en día el internet se ha convertido en la puerta de entrada para que cualquier computadora se conecte a todo el mundo, lo que también lo hace vulnerable a los ataques de hackers desde cualquier parte.

A). Impacto en la educación.

Muchas personas o jóvenes que están iniciando en el proceso de aprendizaje dentro de las diferentes áreas de tecnología, tienden a investigar y a complementarse en diferentes procesos de la sociedad que pueden influir con la tecnología (Redes sociales, páginas web, bases de datos etc), con ello adquieren muchas destrezas, permitiendo mejorar su entendimiento sobre la sociedad y cobertura de información que se puede estar generando en el mundo.

La personalidad del hacker se caracteriza por la curiosidad y la pasión por la tecnología, la persistencia, la destreza técnica y las formas novedosas de ver los problemas. Cualquier padre, maestro o escuela deberían estar orgullosos de esas destrezas en un estudiante. Desafortunadamente, los estudiantes que desean ser hackers suelen ser percibidos como algo normal o ilegal más que una posibilidad de vida.

Una de las principales causas ha sido la creación de diferentes leyes que extremadamente limitan al joven para explotar algún sistema informático. Entonces un estudiante puede ser acusado de un delito grave por cambiar un fondo de escritorio o modificar un sitio Web .Por ejemplo un joven de 16 años de edad en Staten Island, Nueva York, fue acusado de delitos graves de invasión y falsificación de computadoras por hackear el sistema para aumentar sus notas. Entonces los estudiantes ahora pueden terminar en la cárcel, simplemente porque hay una computadora comprometida.

Se ha creado una atmosfera en la que los nuevos hackers prometedores se desaniman activamente por aprender, por lo tanto es probable que terminen por su cuenta sin ninguna guía que pueda mantenerlos fuera de los problemas.

En la actualidad hay muchas páginas, foros, cursos de seguridad donde los estudiantes pueden aprender fácilmente sobre ethical hacking y su importancia en la sociedad. La mayoría se sienten atraídos hacia este aprendizaje porque pueden hackear la computadora de cualquier persona o dispositivos en cuestión de minutos.

Es muy importante que con estos medios de aprendizaje, el estudiante entienda que ser hacker no es bueno si no se realiza de forma responsable, legal y ético. Un muy buen incentivo sobre la realidad es que los hackers éticos son personas altamente remuneradas. Entonces hay que asegurarnos de que al realizar tales actividades o pruebas, sea en ambientes controlados y de mutuo acuerdo con las empresas que necesiten algún servicio de seguridad de la información. Si no contamos con las medidas necesarias, se puede incurrir en un delito informático (Ley 1273 de 2009 Delitos Informáticos) que puede llevar a multas muy grandes o incluso la cárcel.

B. Impacto en la sociedad.

En el mundo actual, ninguna empresa está sin la utilización de TI para la ejecución de sus procesos. Con el apoyo de la tecnología toda la información se crea, modifica y envía de forma electrónica. Debido a esta razón, se puede decir que todas las transacciones comerciales se realizan de forma electrónica. Con el crecimiento de la Internet, existen una serie de sitios web de compras y subastas que influyen en los clientes para vender sus productos en línea. Estos sitios están dando muy buenas ganancias y agilizan en la adquisición de nuevos productos sin importar la ubicación de los clientes. Es muy fácil para un hacker ético comprar una cantidad de bienes y servicios sin pagar la cantidad porque saben que pueden hacerlo fácilmente. Incluso pueden usar los datos personales de otros o la información de cuenta para sus propios propósitos. Realmente es un hecho difícil que algunos programadores de computadoras sean muy buenos y éticos y estén haciendo su trabajo de manera efectiva y correcta, pero pueden usar su habilidad cuando lo necesiten. Es muy desafortunado que algunos profesionales capacitados utilicen sus habilidades y su capacidad para dañar a la sociedad al encontrar vulnerabilidades en el sistema de su compañía, atacarlas, crear programas de virus, crear un código para no aceptar el pago por el servicio deseado. Como la corrupción es el principal hecho en el mundo de hoy, es muy difícil encontrar el recurso perfecto y digno de confianza para realizar pruebas de ethical hacking en cualquier organización.

Por lo general, las empresas que más intentos de hackeo reciben, son las empresas del sector financiero, pues son las que manejan dinero. Los sistemas financieros son los más fortalecidos y robustos en temas de seguridad de la información, entonces los ataques tienden a irse hacia el otro lado del sistema que corresponde a los usuarios, quienes en muchas ocasiones terminan siendo el eslabón más débil de la cadena de la seguridad por su falta de conocimiento respecto al tema. Debido a las malas prácticas de seguridad por parte de la gente del común, su vulnerabilidad es tan grande que los hace presa fácil para el robo, otorgando así un buen botín para los hackers.

Igualmente, se presentan muchos casos de espionaje industrial, en el que a través de las técnicas de hackeo se busca encontrar el punto débil de la competencia para sacar provecho de esa información.

Por otro lado, son muy comunes los casos en los que organizaciones de hackers tratan de buscar que los equipos de hogares o empresas pequeñas sean manipulados como robots, creando legiones que en determinado momento son orientados hacia un mismo objetivo, por ejemplo, un sistema gubernamental, haciendo que la solicitud de recursos del sistema sea tan grande que éste termine por colapsar, saliendo

de línea. Mientras tanto, ese flujo es usado como distracción para lograr éxito con otro tipo de delitos informáticos.

C. Impacto en la Tecnología.

No hay nada malo en decir que casi nada es seguro en el mundo tecnológico. La información está disponible para todos por la misma razón. Hay ciertas herramientas disponibles a través de las cuales cualquiera puede obtener fácilmente la información relacionada con cualquier sistema local o remoto. El hacker ético puede obtener fácilmente las direcciones IP de cualquier sistema y dañarlo. Para los hackers éticos, existen muchas herramientas disponibles en el mercado global para ayudarles a realizar su trabajo de manera efectiva. NMap es la herramienta efectiva que está disponible en Internet para descargar y usar, y ayuda a un hacker ético a encontrar puertos abiertos de los diferentes sistemas. Acunetix es la herramienta que prueba las vulnerabilidades de las aplicaciones web y está disponible en Internet para un hacker ético, es muy fácil de usar y obtener la información. Estas herramientas están siendo utilizadas por un hacker ético normal o por un hacker sin ninguna discriminación. Los hackers pueden usarlas para propósitos criminales y los hackers éticos las usarían para identificar debilidades y fallas en la seguridad de la red.

Un ejemplo es el motor de búsqueda de Google. Mientras se busca información en Google, no encontramos información valiosa debido a la preocupación de privacidad de Google para esas compañías. No es realmente oficial para Google mantener cualquier tipo de información para cualquier empresa; Puede ser bueno para el hacker pero no para la compañía. En este contexto, las empresas deben asegurarse de que ninguna información confidencial o segura se envíe o publique en Internet. No debe ser responsabilidad del motor de búsqueda que mostrar y qué no, sino que debe ser responsabilidad principal de la empresa y sus empleados el no proporcionar la información confidencial.

D. Impacto en la información confidencial.

La información confidencial en cualquier campo no es del todo segura en presencia de un hacker etico. Hay tantos hackers éticos trabajando en bancos donde se realizan todas las transacciones financieras. Un hacker etico puede acceder fácilmente a los datos valiosos de todos los titulares de cuentas. Él puede robar o memorizar los detalles de sus cuentas y puede realizar cualquier tipo de transacción. Él también puede chantajearlos también. Hay tantas compras en línea y otras transacciones donde se cometen fraudes. Si bien del spam se ha convertido en un problema extremadamente grande para todos los usuarios de correo electrónico, que es además la causa de ataques de virus. Un informe reciente reveló que el spam contribuyó con el 70% de todos los correos electrónicos en Internet [7]. Es realmente un gran problema para un hacker ético rastrear todos los escenarios. A veces se observa que tener acceso a la cuenta en efecto culpará a un hacker ético incluso si no han hecho nada. Es realmente muy importante saber que el hacker es diferente del hacker ético. A veces, para un hacker ético se vuelve tan difícil demostrar que él no es el responsable.

Entonces es muy importante que al realizar cualquier servicio o pruebas de etical hacking se establezca el alcance, responsabilidad y limitaciones, El hacker debe obedecer las reglas éticas de hacking. Si no siguen las reglas, sería peligroso para la organización.

Para el hacker ético, el tiempo y la paciencia son más importantes [8]. El hacker ético debe tener intenciones claras para ayudar a la organización y no a dañarlos. La privacidad es la principal preocupación desde el punto de vista de la organización, por lo que el hacker ético debe mantenerse en secreto, porque su uso indebido puede ser peligroso o ilegal.

VII. CONCLUSIONES

A medida que aumenta el uso de internet, todos se vuelven dependientes de él y guardan sus datos confidenciales e importantes en internet. Básicamente, esta es una invitación a ser hacker ético para obtener acceso a la información, ya que la seguridad es uno de los principales problemas para la organización. Esto ilustra la importancia de los hackers éticos. Para este propósito, las organizaciones contrataran hackers éticos que con su conocimiento y experiencia apoyaran en el proceso de mejora con la seguridad de la información.

Para que el Etical Hacking sea realmente efectivo y genere valor agregado a la organización, debe tener muy en cuenta otros factores tales como la valoración de riesgo de los diferentes activos, políticas de seguridad con las que cuenta la organización, aspectos ambientales , tecnológicos y formación de la organización en temas concientización de seguridad de la información.

REFERENCIAS

[1] Jon Erickson, 2008, "Hacking : The Art of Exploitation", 2nd Edition, No Starch Press Inc., ISBN-13: 978-1-59327-144-2, ISBN-10: 1- 59327-144-1

[2] Paula Rochina, Junio 16 2016, disponible https://revistadigital.inesem.es/informatica-y-tics/hacktivismo/

[3] Sitio webTechopedia, disponible https://www.techopedia.com/definition/28615/cyber-warrior

[4] Alejandro, ABRIL 18, 2018, disponible https://protegermipc.net/2018/04/18/las-5-mejores-certificaciones-de-seguridad-informatica-para-pentesters/

[5].Disponible. https://www.gb-advisors.com/es/gestion-de-vulnerabilidades/nessus-escaner-vulnerabilidad/.

[6] Héctor Rizaldo , 2018, disponible https://openwebinars.net/blog/que-es-metasploit/.

[7] Ankit Fadia, 2005, "The Ethical Hacking: Guide to Corporate Security",1st Edition, ISBN: 989-615-004-4

[8] Ethical Hacking Techniques with Penetration Testing www.ijcsit.com/docs/Volume%205/vol5issue03/ijcsit20140503161.pdf(by KB Chowdappa)