Guía Esencial
Seguridad Informática

Técnicas y Mejores prácticas para la Seguridad Informática y el Hacking

Capacity Academy
www.CapacityAcademy.com

CAPACITY
Information Technology Academy

Educación en Tecnología de la Información
Online, Efectiva y Garantizada

Tabla de Contenido

CAPITULO 1

Introducción y Pre-ámbulo

Introducción y Pre-ámbulo

Vamos a iniciar esta guía con un antiguo y pequeño, pero revolucionario, ensayo que anda rodando por la Internet desde hace años, titulado La Conciencia del Hacker.

Este ensayo fue escrito en 1986 por un hacker estadounidense que utilizaba el pseudónimo *The Mentor*, momentos después de su arresto por parte del FBI, acusado de supuestos crímenes informáticos.

La primera vez que este ensayo salió a la luz pública fue a través de una publicación underground en línea orientada al público hacker conocida como Phrack.

La Conciencia del Hacker es considerado por muchos como la obra que sembró la base conceptual de la cultura hacker. Su lectura brinda una visión panorámica de la psicología, composición y motivaciones existentes dentro de la comunidad hacker.

La Consciencia del Hacker

A continuación, el ensayo: "La Consciencia del Hacker":

Lo siguiente, fue escrito poco después de mi arresto….

\/\La Conciencia de un Hacker/\/

by +++The Mentor+++

Escrito en Enero 08 de 1986.

Soy un Hacker, entra a mi mundo . . .

El mío es un mundo que comienza en la escuela . . . Soy más inteligente que la mayoría de los otros muchachos, esa basura que ellos nos enseñan me aburre . . .

//-Malditos subrealizados. Son todos iguales.//

Estoy en la preparatoria. He escuchado a los profesores explicar por decimoquinta vez como reducir una fracción. Yo lo entiendo.

"-No, Srta. Smith, no le voy a mostrar mi trabajo, lo hice en mi mente . . ."

//-Maldito muchacho. Probablemente se lo copió. Todos son iguales.//

Hoy hice un descubrimiento.

Encontré una computadora.

La Consciencia del Hacker

Espera un momento, esto es lo máximo. Esto hace lo que yo le pida. Si comete un error es porque yo me equivoqué.

No porque no le gusto . . .

O se siente amenazada por mí . . .

O piensa que soy un engreído . . .

O no le gusta enseñar y no debería estar aquí . . .

//-Maldito muchacho. Todo lo que hace es jugar. Todos son iguales.//

Y entonces ocurrió . . . Una puerta abierta al mundo . . .Corriendo a través de las líneas telefónicas como la heroína a través de las venas de un adicto, un pulso electrónico es enviado, un refugio para las incompetencias del día a día es buscado . . .una tabla de salvación es encontrada. “Este es . . . Este es el lugar a donde pertenezco . . .”

Y entonces ocurrió . . . una puerta abierta al mundo . . .

Corriendo a través de las líneas telefónicas como la heroína a través de las venas de un adicto, un pulso electrónico es enviado, un refugio para las incompetencias del día a día es buscado . . . una tabla de salvación es encontrada.

“Este es . . . este es el lugar a donde pertenezco . . .”

La Consciencia del Hacker

El mundo del electrón y el switch, la belleza del baudio. Hacemos uso de un servicio que ya existe sin pagar, porque podría ser ridículamente barato, si no estuviera en manos de glotones hambrientos de ganancias, y ustedes nos llaman criminales.

Nosotros exploramos . . . y ustedes nos llaman criminales.

Nosotros buscamos detrás del conocimiento . . .

y ustedes nos llaman criminales.

Nosotros existimos sin color, sin nacionalidad, sin prejuicios religiosos . . . y ustedes nos llaman criminales.

Ustedes construyen bombas atómicas,

ustedes hacen la guerra, asesinan, engañan y nos mienten y tratan de hacernos creer que es por nuestro bien, ahora nosotros somos los criminales.
Si, soy un criminal.

Mi crimen es la curiosidad.

Mi crimen es el juzgar a las personas por lo que dicen y piensan, no por cómo se ven.

Mi crimen es ser mucho más inteligente que ustedes, algo por lo cual jamás podrán perdonarme.

Soy un Hacker, y este es mi manifiesto.

Pueden detener a este individuo, pero no podrán detenernos a todos… después de todo, todos somos iguales.

+++The Mentor+++

CAPITULO 2

6 Pasos para Convertirse en un Hacker Informático

6 Pasos para Convertirse en un Hacker Informático

El término hacker es mal utilizado todos los días en las noticias, revistas, blogs y televisión. Los medios de comunicación utilizan el término hacker para difundir noticias relacionadas con los delitos informáticos.

Tan pronto como alguien es arrestado por la policía cometiendo un delito haciendo uso de computadoras, inmediatamente esa persona es etiquetada como hacker. El verdadero significado del término hacker ha sido mal utilizado durante un largo periodo de tiempo. Ahora, es tiempo de saber cual es su verdadero significado.

¿Qué es un hacker?

Un hacker es alguien que tiene grandes habilidades técnicas en computación. El ser hacker es también una actitud ante la vida. Los hackers resuelven problemas y construyen cosas. Ellos creen en la libertad y la ayuda voluntaria mutua. Los hackers construyeron Internet, World Wide Web (WWW), Linux, Google, Facebook, Twitter y todo lo que hoy existe haciendo la vida más fácil a todas las personas alrededor del mundo. Los hacker son simplemente genios.

Lo contrario de un hacker se llama cracker. Los cracker son individuos dedicados a penetrar en los sistemas informáticos con el propósito de romperlos. Un cracker es una persona que intencionalmente viola la seguridad informática de un sistema con el fin de cometer algún delito.

A menudo tratan de comprometer los sistemas informáticos con el fin de obtener información valiosa para luego venderla al mejor postor y así obtener alguna ganancia económica. En pocas palabras, **los crackers son delincuentes cibernéticos.**

Para ser un hacker se requiere más que buena comprensión de cómo funcionan los ordenadores y las redes. También es necesario tener la actitud correcta.

6 Pasos para Convertirse en un Hacker Informático

A continuación le mostramos los pasos recomendados extraídos de la guía escrita por el famoso hacker de Eric Steven Raymond para todas aquellas personas que quieren convertirse en un futuro hacker.

1) Adoptar la mentalidad hacker: Los hackers tienen su propio credo. Si quiere convertirse en hacker, debe repetir las siguientes afirmaciones hasta el punto que la interiorice en su mente :

- El mundo está lleno de problemas fascinantes que hay que resolver.
- Nadie debería tener que resolver un problema dos veces.
- El aburrimiento y la monotonía son el mal.
- La libertad es buena.
- La actitud no es sustituida de la competencia.

2) Aprenda programación: Aprenda a programar algunos de los lenguajes de programación más populares tales como Java, PHP, C, C + +, Python, Perl y otros. Usted puede aprender a programar tomando cursos o leyendo libros, pero la lectura y la escritura de código de otros programadores es el método más efectivo para convertirse en un programador avanzado.

3) Aprenda a usar Linux: Linux es el sistema operativo por defecto en el reino de los hackers. Linux es software libre y fue hecho por hackers para hackers. Se trata de un proyecto de código abierto, lo que significa que usted puede leer, escribir y modificar su código fuente.

Usted puede adaptar Linux de acuerdo a sus necesidades individuales. También tiene todas las herramientas necesarias para convertirse en un hacker como son: compiladores, lenguajes de programación, herramientas de seguridad, herramientas de penetración, la documentación, la comunidad y mucho más. Puede descargarlo e instalarlo en computados en cualquier momento.

6 Pasos para Convertirse en un Hacker Informático

4) Aprenda inglés: El inglés es el idioma estándar dentro de la cultura hackers y el Internet. Aprender a hablar y a escribir correctamente el idioma inglés ya que es requisito casi obligatorio para ser aceptado dentro de la comunidad hacker. Los hackers tienden a ser fuertes y groseros con aquellas personas que son saben escribir correctamente en inglés.

5) Afíliese a una comunidad de hackers en línea: La mayoría de las comunidades de hackers son dirigidas y administrada por voluntarios. Únase a una comunidad. Ayude a otros miembros, haga preguntas, escriba guías y comparta sus conocimientos. Al mostrar su dedicación a la comunidad esto le traerá el respeto y la admiración de los demás miembros.

6) Comuníquese con otros hackers: para los hacker el dinero no es su principal motivación, por lo tanto, en un mundo donde el dinero no es un signo de status lo es la reputación. Dentro de una comunidad hacker usted gana reputación a través de las siguientes acciones: brindando su tiempo, sus energías, su creatividad y su cooperación a la comunidad y sus miembros.

El intercambio de información técnica y de ideas es la mejor manera de mantenerse en contacto y conocer a otros hackers.

CAPITULO 3

8 Aplicaciones para Convertirse en Hacker

8 Aplicaciones para Convertirse en Hacker

Para ser un hacker no sólo se debe contar con vastos conocimientos sobre los sistemas informáticos, también que hay que tener a disposición las herramientas correctas. Un buen hacker sabe sacarle el máximo provecho estas herramientas.

A continuación un listado de 8 de las herramientas más utilizadas por los hackers, y lo mejor de todo, son gratuitas.

1. Nmap: Esta herramienta permite scannear direcciones IPs y puertos en una red. Con ella podemos descubrir cuántos dispositivos están conectados en la red y cuáles servicios están corriendo. También con el "Footprint" podemos descubrir qué sistema operativo y cuál versión específica tiene instalado el dispositivo. En el curso de Seguridad Informática aprendes a utilizar esta herramienta.

2. Wireshark: Esta herramienta es un Sniffer, lo que significa que podemos capturar el tráfico que atraviesa por la red. Por ejemplo, podemos conectar una PC corriendo Wireshark a un puerto configurado como "mirror" en un switch Ethernet, de esta forma podemos recibir y analizar todas las tramas que se envían por la red. Si el tráfico no está cifrado, podemos ver en "clear text" todos los usuarios y contraseñas de todos los usuarios. Si la red transporta tráfico VoIP, podemos grabar en el disco duro y escuchar todas las conversaciones telefónicas. En el curso de Seguridad Informática aprendes a utilizar esta herramienta. Si quieres aprender VoIP tienes a tu disposición el curso de Cisco CCNA Voice y Asterisk / VoIP.

8 Aplicaciones para Convertirse en Hacker

3. Cain and Abel: Esta herramienta ha evolucionado bastante. Cuando comencé en la informática, esta herramienta se utilizaba principalmente para hacer "crack" de contraseñas a través de ataques de fuerza bruta y "Dictionary Based". Hoy en día esta herramienta es utilizada para diferentes fines: capturar y grabar paquetes VoIP para escuchar conversaciones telefónicas, "hacking" de redes Wireless y también como analizador de protocolos de enrutamiento. Toda una gama de servicios de seguridad informática en una sola herramienta.

4. Metasploit: Para mi es la herramienta cumbre del hacking. Es sencillamente lo mejor que he visto. Metasploit es todo un "Framework" de hacking y seguridad informática. Con esta herramienta podemos lanzar ataques de manera automática a gran escala utilizando cientos de "exploits" y "payload" disponibles. También nos permite desarrollar y diseñar nuestras propias herramientas hacking. Esta herramienta la podemos instalar en cualquier distribución de Linux pero, la forma más común de utilizar es a través de una distribución conocida como "Backtrack Linux" que, recientemente cambió de nombre a Kali Linux. En el curso de Seguridad Informática aprendes a utilizar Metasploit y BackTrack Linux. Si además quieres aprender Linux, en nuestro curso Linux Servidores te convertirás en experto en administración de este sistema operativo.

5. Burp Suite: Esta herramienta permite probar qué tan segura es una aplicación Web. A través de Burp Suite podemos lanzar ataques automatizados para descubrir y explotar las vulnerabilidades existentes en aplicaciones Web.

6. Aircrack-ng: Esta herramienta es utilizada para hacker "crack" de contraseñas en una red inalámbrica 802.11. Aircrack es más que una simple aplicación, es en realidad toda una suite de herramientas que, combinadas todas, pueden descifrar contraseñas WEP y WAP.

8 Aplicaciones para Convertirse en Hacker

7. Nessus: Esta es una de mis preferidas. Esta herramienta es muy fácil de utilizar, ya que toda la administración y configuración la realizamos a través de una interfaz web muy intuitiva. Con Nessus podemos scannear la red completa, ver cuáles nodos están arriba, saber cuáles servicios están corriendo en cada nodo y cómo explotarlos si son vulnerables algún exploit conocido, todo esto de manera automática. Nessus junto a Metasploit es lo que llamaríamos la "combinación del dinero". En el curso de Seguridad Informática aprendes a utilizar esta herramienta.

8. Putty: este el cliente SSH y Telnet por default. Putty es un cliente "lightweight" que ocupa poco espacio en disco. Putty está en versiones para Windows y Linux.

CAPITULO 4

7 Tipos de Hackers y sus Motivaciones

7 Tipos de Hackers y sus Motivaciones

Un hacker es básicamente alguien que penetra en las redes informáticas y los sistemas de información con el objetivo de probarse a sí mismo (y a veces a los demás) sus habilidades intelectuales en el uso de la tecnología o porque persigue sacar algún tipo de provecho de sus capacidades innatas de hacking.

La subcultura hacker que se ha desarrollado a través de los años es definida a menudo como una comunidad informática clandestina, aunque en los últimos tiempos se ha convertido en una sociedad más abierta de clases. En cualquier caso, aquí están los diferentes tipos de piratas informáticos que conviven actualmente en el Internet.

1. Hackers de sombrero blanco (White Hat Hackers):

Este término se refiere a los expertos en seguridad informática que se especializan en realizar pruebas de penetración con el fin de asegurar que los sistemas de información y las redes de datos de las empresas. Estos hackers cuando encuentran una vulnerabilidad inmediatamente se comunican con el administrador de la red para comunicarle la situación con el objetivo de que sea resuelta los más pronto posible.

2. Los hackers de sombrero negro (Black Hat Hackers):

Este término se utiliza a menudo específicamente para los hackers que se infiltran en redes y computadoras con fines maliciosos. Los hackers de sombrero negro continúan superando tecnológicamente sombreros blancos. A menudo se las arreglan para encontrar el camino de menor resistencia, ya sea debido a un error humano o pereza, o con un nuevo tipo de ataque.

A diferencia de un hacker de sombrero blanco, el hacker de sombrero negro se aprovecha de las vulnerabilidades con el objetivo de destruir o robar información. El término proviene de viejas películas del Oeste, donde héroes a menudo llevaban sombreros blancos y los “chicos malos” llevaban sombreros negros.

7 Tipos de Hackers y sus Motivaciones

3. Script Kiddies:

Es un término peyorativo, originado en el mundo de los hackers de sombrero negro para referirse a los "hackers" inmaduros. Los script Kiddies son aquellos piratas informáticos que no tienen conocimientos profundos de programación y seguridad informática pero siempre están intentando vulnerar la seguridad de los sistemas de información utilizando herramientas desarrolladas por los verdaderos hackers.

Podemos encontrar hoy en día innumerables herramientas "Script Kiddies" que permiten a cualquier persona sin muchos conocimientos de informática hackear un computador que tenga instalado un sistema con una vulnerabilidad conocida. Debido a la facilidad de uso de estos programas, hay cientos de miles (o millones) de los script-kiddies en Internet. Cualquier máquina que se conecta directamente a Internet con una conexión de alta velocidad es probable que vea un buen número considerables de ataques contra su sistema utilizando estos script-kiddies.

4. Hacktivistas:

Algunos activistas hackers están motivados por la política o la religión, mientras que otros pueden querer denunciar los abusos, o la venganza, o simplemente acosar a su objetivo para su propio entretenimiento.

Un hacktivista utiliza las mismas herramientas y técnicas de un hacker, pero lo hace con el fin de interrumpir los servicios y brindar atención a una causa política o social. Por ejemplo, uno puede dejar un mensaje muy visible en la página principal de un sitio web que recibe una gran cantidad de tráfico o que incorpora un punto de vista que se está en contra. O se podría lanzar un ataque de denegación de servicio para interrumpir el tráfico a un sitio determinado.

7 Tipos de Hackers y sus Motivaciones

Una demostración reciente de hacktivismo tras la muerte de un piloto chino, cuando su avión de combate chocó con un avión de vigilancia de EE.UU. en abril de 2001. Hacktivistas chinos y estadounidenses de ambos países hackearon sitios Web y los utilizaron como “pizarras” por sus declaraciones.

5. Los hackers patrocinados por el estado: los gobiernos de todo el mundo se han dado cuenta de la importancia del cyber espacio para sus objetivos militares. El refrán que solía ser: “El que controla los mares controla el mundo”, y entonces fue: “El que controla el aire controla el mundo.” Ahora se trata de controlar el ciberespacio. Los estados patrocinan hackers con el objetivo de llevar a cabo ataques informáticos a civiles, corporaciones y gobiernos opositores.

6. Los piratas informáticos espía:

Las empresas contratan hackers para infiltrarse en la competencia y robar secretos comerciales. Los piratas informáticos espía puede utilizar tácticas similares a los hacktivistas, pero su única agenda es servir a los objetivos de sus clientes y se les paga.

7. Los terroristas cibernéticos: Estos hackers, generalmente motivados por creencias religiosas o políticas, tratan de crear miedo y el caos mediante la interrupción de las infraestructuras tecnológicas críticas de los países y corporaciones. Los terroristas cibernéticos son por mucho el más peligroso de todos los tipos de hackers, ya que cuentan un amplio arsenal de habilidades y metas. Su motivación última es la difusión del miedo y el terror.

CAPITULO 5

La Diferencia Entre Hacker y Cibercriminal

La Diferencia Entre Hacker y Cibercriminal

Existe una confusión generalizada, principalmente en los medios de comunicación masivos en cuanto al uso del término hacker.

La palabra “Hacker” en la cultura popular es asociada a la figura de delincuente. Algo que no puede estar más lejos de toda realidad.

Un hacker es simplemente una persona con altos conocimientos computacionales que utiliza sus capacidades y habilidades para descubrir vulnerabilidades en las redes y sistemas informáticos. La motivación primordial de un hacker es la búsqueda del conocimiento per se y el respeto de la comunidad hacker.

La actividad de penetrar en los sistemas y redes de información en la búsqueda de vulnerabilidades es toda una profesión en sí. En la industria de la seguridad informática a esta actividad se le denomina hacking ético.

Todas las grandes empresas del mundo, sin importar su naturaleza, necesitan los servicios de expertos informáticos para que validen la seguridad de sus sistemas y redes computacionales.

Estos trabajos obviamente son ejecutados por hackers bajo previa autorización soportados por un acuerdo contractual de los servicios, ya que estos son los que conocen las “intríngulis” de las últimas técnicas de penetración y asalto de información.

La Diferencia Entre Hacker y Cibercriminal

Ahora bien, un cibercriminal es un individuo que se aprovecha de las vulnerabilidades de las redes y sistemas de información para llevar a cabo actos tipificados por ley como criminales: robo de información, destrucción información, extorsión, divulgación de información confidencial, distribución de pornografía infantil, envío de correo basura, terrorismo, fraudes, robo de identidad, falsificación de información, piratería, etc.

En los círculos y en las comunidades de seguridad informática a los primeros se les denominan White Hat Hackers (Hackers de sombrero blanco), a los segundos Black Hat Hackers (Hacker de sombrero negro), aunque antiguamente se les decía Crackers también.

Conclusión, aprenda mucho de seguridad informática y hacking. Esta es una profesión bien desafiante y emocionante. En la actualidad, dentro de la industria de las TIC la seguridad informática es una de las profesiones mejor pagada y más demandada.

Saber Más Sobre Seguridad Informática

CAPITULO 6

Las 12 Amenazas Más Peligrosas en Internet

Las 12 Amenazas Más Peligrosas en Internet

En todo momento es vital para las empresas evaluar sus prácticas de seguridad hacia los sistemas de información que estas dependen, con el fin de estar preparados y pensar en planes de acción para mitigar las amenazas que puedan surgir en cualquier momento.

Cada día las amenazas de seguridad son cada vez más graves, sofisticadas y difíciles de detectar, he aquí la importancia para las empresas de comprender y entender cuales son las posibles amenazas que toda organización está hoy en día expuesta.

A continuación vamos a describir las 12 amenazas más peligrosas en Internet:

1. Cross-site scripting:

Es un ataque que utiliza secuencias de comandos en el navegador web de la víctima. Esto ocurre cuando un navegador visita un sitio web malicioso o hace clic en un enlace malicioso. Las consecuencias más peligrosas ocurren cuando se utiliza este método para explotar las vulnerabilidades que pueden permitir a un atacante robar los cookies (datos intercambiados entre el servidor web y un navegador), realizar capturas de pantalla, descubrir y recoger información de la red y/o controlar la máquina de la víctima.

2. Denegación de servicio (Denial-of-service):

Este tipo de ataque también conocido como DoS, impide o dificulta el uso autorizado de las redes, sistemas, aplicaciones debido al agotamiento de los recursos. Por lo general, este tipo de ataques está dirigido a los servidores de una compañía con el fin de imposibilitar el acceso de los usuarios.

Las 12 Amenazas Más Peligrosas en Internet

3. Denegación de servicio distribuido (Distributed denial-of-service):

Una variante del ataque de denegación de servicio con la diferencia de que se utilizan numerosas computadoras (computadoras zombies) para llevar a cabo el ataque.

4. Bomba lógica (Logic bomb):

Este tipo de ataque se lleva a cabo colocando intencionalmente un pedazo de código de programación dañino dentro del código fuente de un software. El objetivo es ejecutar una función maliciosa al momento que se produzcan ciertas condiciones determinadas.

5. Phishing:

Es un tipo de ataque informático que se lleva a cabo a base de ingeniería social con el objetivo de intentar conseguir información confidencial de forma fraudulenta. El estafador, conocido como phisher, se hace pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo común un correo electrónico, o algún sistema de mensajería instantánea o incluso a través de llamadas telefónicas.

6. Intercepción (Passive wiretapping):

Es un tipo de ataque mediante el cual un tercero capta la información (esta puede estar en texto claro o cifrada) que estaba siendo transmitida entre dos nodos en la red. La captación de la información puede realizarse por múltiples medios (redes alambricas, redes wireless, etc). Este tipo de ataque tiene la particularidad de que es muy difícil de detectar mientras es llevado a cabo, por lo que un atacante puede capturar cierta información privilegiada (usuarios y contraseñas) para acceder luego al sistema o a la red para buscar más información o causar algún daño.

Las 12 Amenazas Más Peligrosas en Internet

7. SQL injection:

Este tipo de ataque consiste en la inserción del código malicioso en un aplicación web con el propósito de obtener acceso no autorizado a información confidencial grabadas en una base de datos.

8. Caballo de Troya (Trojan horse):

Es un programa de computadora que a simple vista parece tener una función útil, pero al mismo tiempo también tiene una función oculta y potencialmente peligrosa, evadiendo de esta forma los mecanismos de seguridad.

9. Virus:

Son programas capaces de copiarse a sí mismos e infectar un ordenador sin el permiso o conocimiento del usuario. Un virus puede dañar o eliminar datos guardados. Regularmente utilizan los programas de correo electrónico para propagarse a través de la red hacia otros ordenadores, o incluso borrar todo el contenido del disco duro. A diferencia de un gusano informático, un virus requiere la intervención humana (por lo general sin saberlo) para propagarse.

10. War driving:

Es la actividad que se realiza con el objetivo de buscar en las avenidas de las ciudades redes inalámbricas no seguras. El wardriving regularmente se realiza desde un automóvil utilizando una computadora portátil junto con una antena WiFi de largo alcance.

Las 12 Amenazas Más Peligrosas en Internet

11. Worm (gusano):

Es una programa malicioso que utiliza mecanismos de red para propagarse. A diferencia de los virus informáticos, el gusano no requieren intervención humana para propagarse.

12. Ataque del día cero (Zero-day exploit):

En este tipo de ataque el atacante se aprovecha de una vulnerabilidad de seguridad desconocida para el público en general. En muchos casos, el código de explotación ha sido escrito por la misma persona que descubrió la vulnerabilidad. Al escribir un exploit para la vulnerabilidad previamente desconocida, el atacante crea una gran amenaza, ya que el marco de tiempo comprendido entre los descubrimiento de la vulnerabilidad y el lanzamiento del parche de seguridad a dicha vulnerabilidad por parte del fabricante de la aplicación toma un tiempo determinado. En ese espacio de tiempo, todos los sistemas afectados por dicha vulnerabilidad se encuentran en una posición difícil de defender.

CAPITULO 7

5 Errores Comunes de Seguridad

5 Errores Comunes de Seguridad

No importa cuánto lo intentemos, los usuarios – y, a veces incluso los departamentos de TI – pasan por alto algunos errores de seguridad que son relativamente fáciles de corregir. En este capítulo vamos a aprender los 5 errores de seguridad que podrían evitarse, y al mismo tiempo vamos a describir lo que usted puede hacer para corregir el descuido.

1- Usar contraseñas débiles

Tiempos atrás, la gente pensaba que utilizar como contraseña la palabra “password” era una manera segura de engañar a los hackers y otros malhechores. Después de todo, ¿quién podría utilizar una contraseña tan obvia? La mayoría de la gente hoy en día se ha dado cuenta de la gravedad que es usar contraseñas de éste tipo, aún así muchos todavía las utilizan sabiendo el riesgo en que incurren especialmente en esta época donde las redes sociales son tan populares. Le voy a dar un ejemplo : Usted inteligentemente utiliza su fecha de aniversario en su contraseña, junto con el segundo nombre de su hijo mayor. Ambos datos son fáciles de averiguar en Facebook y por otros medios.

Solución

No utilice en sus contraseñas datos relacionados con usted. Tampoco utilice palabras del diccionario. Al momento de elegir una contraseña utilice caracteres aleatorios. Le recomiendo utilizar el sistema de generación de contraseñas aleatorias random.org

5 Errores Comunes de Seguridad

2- Nunca cambia la contraseña

Esto es un patrón que se repite todo el tiempo. Las personas que mantienen la misma contraseña, y al mismo tiempo la utilizan en varios sitios son más propensos a sufrir una violación de seguridad. Incluso dentro en las organizaciones que tienen implementadas políticas de seguridad que requieren cambios de contraseña, algunas personas tratan de encontrar formas de evitar tener que cambiar las contraseñas de forma periódica. Algunas personas solo cambian un carácter de la contraseña cada vez llegar la fecha de cambio de contraseña.

Solución

Edúquese usted mismo y a sus usuarios sobre la importancia de mantener una buena contraseña, y por qué cambiarla cada cierto tiempo es crítico. Como parte de su política de seguridad, considere usar una herramientas de terceros para no permitir contraseñas similares en determinado periodo de tiempo.

3- No instalar Antivirus / Anti-malware

Este es un hecho, si no está ejecutando un software antivirus de algún tipo en su entorno, está condenado al fracaso. Incluso si usted tiene instalado los mejores dispositivos de seguridad (firewall, IDS, IPS, Content Filtering, etc), el concepto de seguridad por capas sigue siendo válido. Cualquier cosa que el firewall no pueda interceptar puede ser manejado por el software antivirus.

Solución

Instale un Antivirus inmediatamente. Puede descargar el software Antivirus Clamwin el cual es software libre y el totalmente gratuito.

5 Errores Comunes de Seguridad

4- No utilizar firewall

Tanto en el hogar como en las empresas un firewall siempre es necesario. Aunque Windows y Linux ambos incluyen firewall, siempre he preferido tener un instalado un firewall perimetral que sirva de punto de chequeo para todos los paquetes entran y salen de la red.

Solución

Siempre que sea posible, implementar un firewall perimetral tanto en casa como en la oficina es una opción altamente recomendable. Asegúrese de que las reglas del firewall no permite tráfico innecesario hacia la red interna. Si tiene conocimientos sobre Linux le recomiendo que instale la distribución de firewall IPCOP.

5- No actualizar el sistema operativo

Los desarrolladores de sistemas operativos y aplicaciones liberan los parches y actualizaciones por una razón. Mientras que muchas actualizaciones añaden nuevas funcionalidades, muchas fallas de seguridad también son corregidas por esta vía. He visto un montón de máquinas en las cuales los usuarios han desactivado las actualizaciones. Siempre es recomendable mantener nuestro sistema operativo y las aplicaciones con los últimos parches y actualizaciones instalados.

Solución Vigile bien los sistemas de sus máquinas! Active el sistema de actualizaciones automáticas e implemente sólidas políticas de gestión de parches.

CAPITULO 8

Certificaciones:

Cisco CCNA Security Vs CompTIA Security+

¿Cuál elegir?

Cisco CCNA Security Vs CompTIA Security+

En este capítulo vamos a explicar las diferencias a nivel de contenido entre Seguridad Informática y Cisco CCNA Security, así el candidato puede tomar una decisión informada acerca de cuál curso tomar en un momento determinado. Primeramente, el curso de Seguridad Informática comienza totalmente desde cero asumiendo que el estudiante NO tiene conocimientos previos en seguridad informática.

El curso está compuesto por 7 módulos que abarcan una diversidad de temas muy variados, desde seguridad en la red (Capa 3) hasta la seguridad en los servidores (Capa 7).

Un detalle muy importante de este curso de seguridad informática es que utilizamos una diversidad de herramientas de Hacking interesantísimas para realizar los laboratorios y así afianzar los conceptos teóricos que se imparten en cada módulo. Por ejemplo, en el módulo 2 (Seguridad en la Red) nos concentramos en cómo proteger una red de posibles amenazas de seguridad y para esto aprendemos a instalar, configurar y administrar un firewall open source llamado IPCOP. IPCOP está basado en Linux y podemos descargarlo totalmente gratis sin costos de licenciamiento. Una solución ideal para pequeña empresas.

En el módulo 3 (Protección de Red) el material se pone aún mejor. Aquí aprendemos los fundamentos de los Sistemas de Detección de Intrusos, y para llevar la teoría a la práctica instalamos y configuramos un IDS (Intrusion Detection System) open source llamado Snort.

Cisco CCNA Security Vs CompTIA Security+

En el módulo 4 (Seguridad en Servidores) aprendemos cómo implementar las medidas de seguridad necesarias para proteger servidores Windows y Linux. Luego, para asegurarnos que todo está seguro y que no seamos víctima de un hacker, aprendemos cómo "hackear" nuestros propios servidores utilizando una herramienta open source muy poderosa llamada Metasploit. Es recomendable que el estudiante que tome este curso tenga conocimientos previos en Linux. ¿Por qué? Las mejores herramientas de seguridad están hechas para corren Linux. Si no sabes utilizar el sistema operativo te recomiendo tomar nuestro curso de Linux Servidores.

El curso de Cisco CCNA Security es un curso de seguridad orientado específicamente a la Capa 2 del modelo OSI (Enlace) y Capa 3 (Red), es decir, nos concentramos en cómo implementar seguridad en los Router y Switch de nuestra red. A diferencia del curso de Seguridad Informática en el cual los laboratorios los realizamos con hardware genérico y software open source, en el curso de Cisco CCNA Security todos los laboratorios se realizan sobre hardware propietario Cisco.

El curso de Cisco CCNA Security es más extenso en contenido en comparación con el curso de Seguridad Informática, ya que el primero abarca todo el contenido requerido para que el candidato pueda aprobar el examen de certificación Cisco CCNA Security 640-554 IINS. Para tomar este curso es altamente recomendable que el candidato haya tomado previamente el curso de Cisco CCNA Routing &Switching.

Cisco CCNA Security Vs CompTIA Security+

La parte diferenciadora entre ambos es que el curso de Cisco CCNA Security tenemos bastante material enfocado en la seguridad a nivel de Capa 2 de OSI (Enlace), en la cual aprendemos a implementar seguridad en Switch Ethernet. Aquí aprendemos cómo implementar Port-security, AAA, VLAN, Trunking, Inter-VLAN, Spanning Tree, etc. También el curso de Cisco CCNA Security introduce el tema de seguridad en IPv6, otro tema distintivo que no está disponible en Seguridad Informática.

En conclusión, creo que no hay un curso mejor que otro sino que ambos son complementarios. Dominar el conocimiento y las herramientas del curso de Seguridad Informática que están basadas en hardware genérico y software Open Source nos brinda mucha flexibilidad como profesionales de Seguridad de IT. Saber trabajar con un IDS como Snort y con Metasploit, así como las principalmente herramientas de Hacking del mundo Linux y Open Source es básicamente una obligación hoy en día.

Así mismo, tener el conocimiento sobre cómo implementar las medidas de seguridad en redes Cisco es vital para entrar en el mundo corporativo. Como he mencionado en artículos anteriormente, los ambientes de redes heterogéneos son los que dominan los mercados, así que mientras más herramientas y conocimientos diversos tengamos en nuestro arsenal, mayores serán nuestras oportunidades laborales y de negocios en el mundo de la seguridad informática.

Saber Más Sobre Seguridad Informática

Saber Más Sobre CCNA Security

CAPITULO 9

Conclusiones y Siguientes Pasos

Conclusiones y Siguientes Pasos

Un hacker es alguien que tiene grandes habilidades técnicas en computación. El ser hacker es también una actitud ante la vida. Los hackers resuelven problemas y construyen cosas. Ellos creen en la libertad y la ayuda voluntaria mutua.

Los hackers construyeron Internet, World Wide Web (WWW), Linux, Google, Facebook, Twitter y todo lo que hoy existe haciendo la vida más fácil a todas las personas alrededor del mundo. Los hacker son simplemente genios.

Avanzar en la Industria de TI, adquirir nuevas habilidades y conocimientos relacionados a esta rama y aumentar tu nivel de empleabilidad e ingresos, son las razones más importantes por las cuales debes capacitarte para adquirir cualquiera de las certificaciones de Seguridad Informática.

Recuerda que la metodología y el lugar que escojas para tu preparación será vital para lograr obtenerla en el primer intento. Debes elegir una academia que te garantice, no solo tu dinero, sino también un aprendizaje integral, completo y vanguardista.

En estos procesos también es muy importante la cantidad y el tipo de prácticas que se utilice durante la capacitación. Este nivel debe ser lo suficientemente alto como para que puedas obtener la seguridad necesaria para dar este importante paso en tu vida profesional.

Otra importante recomendación es que debes procurar contar con un instructor certificado y con la experiencia laboral adecuada para que todas tus dudas y preguntas sean respondidas satisfactoriamente. Esto es vital.

Conclusiones y Siguientes Pasos

Te adelanto que probablemente encontrarás varias opciones de entrenamientos disponibles, pero definitivamente uno de los mejores métodos conocidos es el Programa Bootcamp Online. Esta metodología ha sido considerada como la más efectiva cuando hablamos de ahorro de tiempo y dinero.

En Capacity Academy encontrarás 2 opciones dentro del área de la Seguridad Informática, según tu perfil profesional:

- ❑Curso-Bootcamp de CCNA Security
- ❑Curso-Bootcamp de Seguridad Informática (CompTIA Security +)

Cada uno de estos cursos está compuesto por más de 90 videos interactivos, un foro de soporte con un profesor exclusivo, una biblioteca digital actualizada y lo más importante, están 100% garantizados. Estos factores constituyen la principal diferencia y ventaja ante otros entrenamientos a distancia.

En caso de que no quieras elegir una sola, puedes optar por prepararte para estas 2 certificaciones junto a otras más, haciendo clic aquí.

La industria es muy competitiva, no hay tiempo que perder, debes tomar acción ahora para tener un futuro profesional mucho más prometedor.

¡Te aseguramos la experiencia online más enriquecedora de tu vida!

Saber Más Sobre CCNA Security