PENTESTING

Y

SEGURIDAD

AUTOR: Darwin Silva TWITTER: @SECURITY_ZERO

Team: ROMEO Q

ZERO

Nota del Autor:

Mi nombre es Darwin Alexander Silva Pérez (zero) soy el autor de esta revista.

Mi facebook asi como twitter, correo y canal de youtube.

https://www.facebook.com/dawin.silva.3

@security_zero

http://www.youtube.com/user/zerndate

Portada: Darwin Alexander Silva Pérez

correo: zerndate@gmail.com

Tomo numero : 1°

Hecho con Software Libre:

• Kali linux
• LibreOffice 4.0.2.2

INDICE

Pentesting

Bienvenidos a esta revista este es el primer tomo de muchos; en fin mucho se habla de seguridad y pestesting pero que son en realidad abundan muchos terminos en la red pero algunos muy extensos otros muy incoherentes etc... para fines didacticos y de aprendisaje yo explicare todo con mis palabras y razonamiento.

Un pentesting no es mas que el procedimiento que utilizamos muchos para verificar la seguridad de un sitio en concreto ya sea website o servidores; son tecnicas por las cuales nos regimos para encontrar una vulnerabilidad en el sitio analizado.

El pentest puede ser tanto legal como ilegal ya sea que te contraten para analizar una red es legal si analizamos un lugar sin los permisos ni consentimientos de los dueños es ilegal así de sencillo; pero para fines mas practicos este metodo es usado para encontrar vulnerabilidades en algun sitio y así poder parcharlo o cerrar el bug(hueco de seguridad) o aprovecharnos de el, en caso de pentest ilegal.

Para ello nos podemos valer de herramientas tanto libres como de paga dependiendo de el tipo de pentest que queramos realizar aunque la gran mayoria de pentest usan software libre que veremos en otros tomos, esto se debe a que algunas herramientas traen mas funciones si consigues las de pagas.

Otra cosa o punto es que para realizar pentesting legales en muchos paises es necesario poseer o obtener una licencia o diploma sobre ello; algunos dicen o comentan que dichas cosas solo las pueden hacer los “hackers” pero si somos realistas el terminos generales el termino hacker ya a sido modificado,alterado con lo que significaba al comienzo por eso; no es necesario ser hacker para realizar un pentest basta con estudiar,aprender,practicar y obtener un diploma o certificado que habale que estas capacitado para dicha función.

Ojo con esto no quiero decir que cualquier niño va a venir a realizar un pentesting o pentest con cumplir o llenar esos requisitos el punto esta en que debe ser una persona mayor y no me estoy refiriendo a la edad sino a su capacidad para razonar ,tomar decisiones coherentes con logica y sobre todo con responsabilidad.

Bueno en resumen es un metodo en el cual analizamos y verificamos si hay fallos de seguridad en x lugar para saber como corregirlos o explotarlos desde el punto de vista informatico cabe destacar.

PenTest

Seguridad

Bueno para explicar que es la seguridad informatica debemos algunos piensan que hay que saber primero que es seguridad en general pero yo no lo pienso así ya que si estan leyendo esto ya saben que todo va relazionado con la informatica o bien que ya saben o tienen un concepto ya sea correcto o ambiguo sobre el tema así que nos ahorraremos los conceptos.

Todos deben saber en primer lugar que la seguridad no existe en un 100 % ya que por mas que tratemos de protegernos al instalar "x" programa o antivirus ó firewall se abre alguna brecha o un atacante tratara de encontrar la brecha para sustraer y robar información confidencial de algun lugar en expecifico.

Pero cabe decir o destacar que podemos tomar ciertas medidas que minimizaran el riesgo que el atacante pueda sustraer o robar información tales como la configuracion correcta de ciertas herramientas,tener actualizado siempre nuestro sistema,analizar y cerrar puertos y protocolos que no estemos ocupando y son una brecha de seguridad a nuestro sistema.

En fin varias de las cosas que podemos implementar para mantener un nivel de seguridad respetable van desde configuraciones faciles a mas complejas que iremos viendo poco a poco en estas revistas; ya me sali un poco de tema pero en resumen es tratar de mantener y salvaguardar datos,información clasificada o confidencial tomando medidas de proteccion para que no llegen a manos equivocadas.

TCP/IP

Describe un conjunto de guías generales de diseño e implementación de protocolos de red específicos para permitir que un equipo pueda comunicarse en una red. TCP/IP provee conectividad de extremo a extremo especificando cómo los datos deberían ser formateados, direccionados, transmitidos, enrutados y recibidos por el destinatario. Existen protocolos para los diferentes tipos de servicios de comunicación entre equipos.

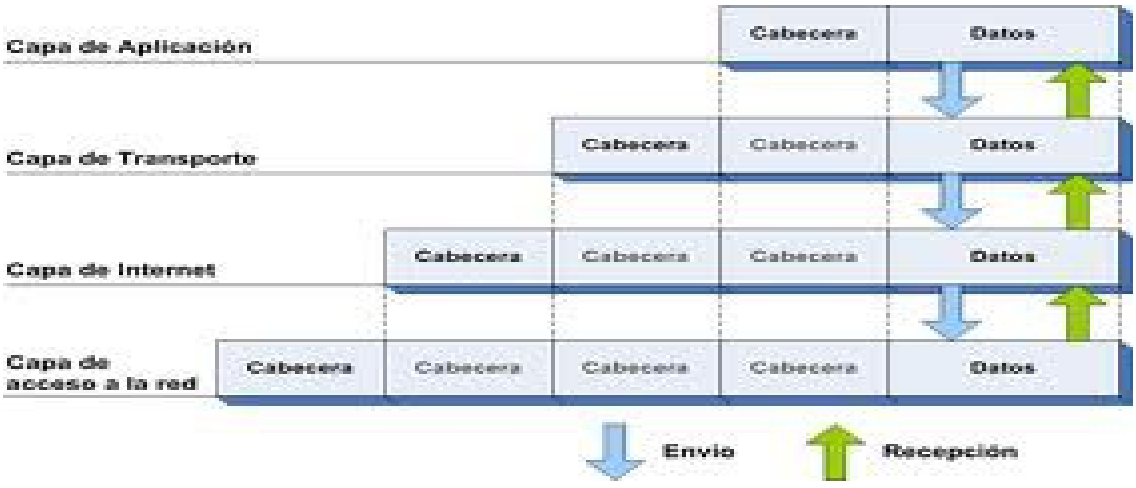
El TCP/IP es la base de internet, y sirve para enlazar computadoras que utilizan diferentes sistemas operativos, incluyendo pc y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

El conjunto TCP/IP está diseñado para enrutar y tiene un grado muy elevado de fiabilidad, es adecuado para redes grandes y medianas, así como en redes empresariales. Se utiliza a nivel mundial para conectarse a internet y a los servidores web. Es compatible con las herramientas estándar para analizar el funcionamiento de la red.

Los protocolos TCP/IP puede ser vulnerada en base a dos conceptos inherentes a su diseño:

1.- El formato de los paquetes de los diferentes protocolos: Aparte de la propia información trasportada, la información contenida en cada uno de los campos de las cabeceras de los protocolos proporciona una fuente muy valiosa de conocimiento.

2.- El modo de funcionamiento de los protocolos: Las etapas asociadas a cada proceso en los protocolos, así como el método de actuación en las diferentes situaciones posibles, ofrecen la información necesaria para analizar la existencia de vulnerabilidades.



Amenazas

Bueno ahora hablaremos un poco sobre las amenazas mas comunes en los sistemas operativos que usan los “hackers” por no decir personas sin nada que hacer que andar infectando a los demas solo para espiarte por tu web cam; entre otras cosas comunes como los grandes “juakers de facebooks” pero eso es irrelevante empezemos ya antes que me salga mas del tema.

1-Virus

Esto no es mas que un codigo que se inyecta o se ejecuta dentro de otro programa el cual necesita un programa huesped para poder sobrevir y asi mismo autoreplicarse dentro de otros y que inicia al mismo tiempo que se ejecuta el programa infectado produce que las pcs se pongan lentas por que ocupan espacio de memoria.

2-Conejos

Los conejos o bacterias son programas que de forma directa no dañan al sistema, sino que se limitan a reproducirse, generalmente de forma exponencial, hasta que la cantidad de recursos consumidos (procesador, memoria, disco. . .) se convierte en una negación de servicio para el sistema afectado.

3-Troyanos

Es un programa que aparentemente realiza una funcion util para quien lo ejecuta, pero que en realidad,realiza o ejecuta una funcion que el user desconose o no se da cuenta que esta alli; con ellos pueden encender tu webcam,captar pulsaciones de teclado etc.

4-Puertas traseras

Son trozos de codigo en un programa que permiten saltarse los metodos usuales de autenticacion para realizar cierta tarea. Habitualmente son insertados por los programadores para agilizar la tarea de probar su codigo durante la fase de desarrollo del mismo y se eliminan en el producto final, pero en ciertas situaciones el programador puede mantener estas puertas traseras en el programa funcional, ya sea deliberada o involuntariamente.

Bueno omito algunas amenazas como las bombas logicas y las denegaciones de servicios por que son amenazas algo viejitas que en la gran mayoria de pcs actuales y herramientas de proteccion ya no sirven del todo por eso no presento información sobre ellas si gustan pueden investigar sobre ellas en internet.

Ingenieria Social

Es el arte o tecnica de poder manipular a las personas de tal forma que podamos tener acceso a algun lugar concreto o acceso a cierta información confidencial ya sea de una empresa o una persona en concreto.

Desde el punto de vista psicologico:

Existen determinados procesos que son automáticos tanto en el ser humano como en los animales en virtud de las relaciones con los demás. Así que depende de quién lo analice y los convierta en una ventaja o una desventaja para obtener información. Estos procesos son comúnmente utilizados en campañas de mercadeo y negocios para influenciar sobre la gente.

Otras estrategias o principios de la ingeniería social se basan en rutas periféricas de persuasión en donde se utiliza la emoción como una forma de distracción.

Técnicas de Ingeniería Social

a)Técnicas Pasivas:
Observación

b)Técnicas no presenciales:
Recuperar la contraseña
Ingeniería Social y Mail
IRC u otros chats
Teléfono
Carta y fax

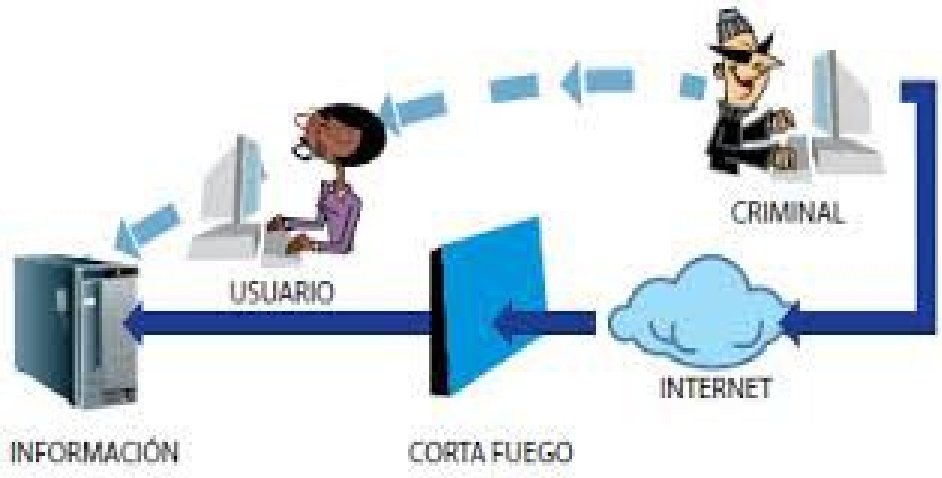
c)Técnicas presenciales no agresivas:
Buscando en La basura
Mirando por encima del hombro
Seguimiento de personas y vehículos
Vigilancia de Edificios
Entrada en Hospitales
Acreditaciones
Ingeniería social en situaciones de crisis
Ingeniería social en aviones y trenes de alta velocidad
Agendas y teléfonos móviles
Desinformación

d)Métodos agresivos
Suplantación de personalidad
Chantaje o extorsión
Despersonalización
Presión psicológica

Kevin Mitnick fundamenta las estrategias de Ingeniería Social en los siguientes postulados:

>Todos los seres humanos quieren ayudar
>El primer movimiento es siempre de confianza hacia el otro
>No nos gusta decir NO
>A todos nos gusta que nos alaben
>Todos tenemos algo de ingenuos

Bueno termino este capitulo diciendo que podemos mejorar la seguridad de nuestros servidores,pcs y todo lo que podamos modernizar conforme avanza la tecnologia pero el unico punto debil de toda compañía que no podemos reforzar es la humana; si podemos dar charlas sobre distintos puntos de seguridad pero recuerda toda empresa subsiste por sus clientes por ende cualquier persona tratara de brindar la información mas fiable y exacta sobre algun producto o algun servicio que preste en dicha empresa si reciben una llamada de alguien que dice ser cliente de la empresa o posible cliente en el futuro.



Inyección SQL

Bueno compañeros despues de unas reseñas y todo las palabrerias que escribi empezamos con la parte que seguro les interesa a muchos las pentesting y seguridad empezare mostrandole una simple vulnerabilidad que muchas webs tienen y que por esa falla les terminan defaceando la misma.

Inyección SQL es un método de infiltración de código intruso que se vale de una vulnerabiliad presente en una aplicación en el nivel de validación de las entradas para realizar consultas a una base de datos.

El origen de la vulnerabilidad radica en el incorrecto chequeo y/o filtrado de las variables utilizadas en un programa que contiene, o bien genera, código SQL.Se conoce como Inyección SQL, indistintamente, al tipo de vulnerabilidad, al método de infiltración, al hecho de incrustar código SQL intruso y a la porción de código incrustado.

Bueno yo les mostrare una inyeccion sql con sqlmap un metodo automatizado y sencillo contando que el lector no sabe nada esta empezando desde 0 por eso no mostrare el metodo manual si quieren indagar sobre el hay muchos tutoriales en la red sobre inyeccion sql manual.

Bueno como sabemos si una web es vulnerable a sql inyeccion hay dorks para google que automattizan eso pueden buscar en google dorks de inyeccion sql hay muchos foros de ello pero nosotros veremos algo mas directo.

Simple la gran mayoria a visto que en las url de algunas webs al indexar o cargar alguna sub pagina queda al final algo asi " .php?id=" pues hay webs que podemos probar facilmente su vulnerabilidad de esta forma.

Pagina a atacar : http://www.mckl.cl/noticias.php?id=9

Simplemente pondremos al lado de el numero 9 una comilla simple por lo tanto la url nos quedara de esta forma: http://www.mckl.cl/noticias.php?id=9' solo debemos recargar la web con f5 o ponernos en la url y dar enter al instante nos mostrara un mensaje de error sql y sabremos si es vulnerable si no pasa nada la web no es vulnerable el mensaje es el siiguiente.

You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near '' at line 2

Bien ahora que sabemos que es vulnerable vamos a abrir la herramienta SQLMAP que en muchas distros de seguridad linux viene preinstalada los que usan windows igual la pueden instalar hay muchos tutos en la red de como hacerlo.

Nos quedara así la parte de /usr/bin/sqlmap es la direccion donde esta el sqlmap en la computadora esto puede variar según la instalacion que realizaron, la parte de -u esto es para denotar o señar la url que vamos atacar luego la url y al final vemos – – dbs esta parte lo que hace es encontrar las bases de datos de la web damos enter y empezara el proceso, esto puede dilatar dependiendo de cuantas bases de datos hay en la web y de la version de la misma.

La parte que nos interesa es las que estan al lado de [*] por que ellas son las bases de datos que encontro sqlmap,ahora ya no esta la parte de – – dbs si no –D esto es para señalar la base de datos que quiero escanear en este caso la moeckelyweil_bd recuerden esta base de datos es de esta web en otras les saldra otros nombres de base de datos algunos se preguntaran por que no escojio la base information_chema por que en la mayoria de casos esa data base no tiene los users y password que queremos obtener de la web ya lo he comprobado en la mayoria de webs que he escaneado pero igual si no sale nada en la que estamos escaneando probamos con la otra hasta dar con los datos que queremos ahora la parte de – – tables es para sacar las tablas de la base de datos ya señalada y damos enter.

Como pueden notar nos devuelve las tablas user,categoria,foto etc... a nosotros nos interesa la tabla user para obtener ahora las columnas de dicha tabla escribimos lo siguiente como ven en la imagen arriba – – D ya les explique que hace ahora ponemos – – T para señalar la tabla a atacar en este caso la tabla user y – – columns es para sacar las columnas a dicha tabla damos enter y esperamos.

Bien como vemos en la imagen arriba ahora solo resta sacar la información de esas columnas para ello escribimos – – C para señalar las columnas a analizar y escribimos las columnas podemos poner una por una pero si quieren ahorrar tiempo ponen una luego coma y escriben la otra como en mi caso User,pwd y despues colocamos – – Dump que nos sacara la informacion de dichas columnas damos enter y esperamos.

Bien ya listo todo nos muestra el user para loguiarnos en el panel de la web y el password recuerden el password esta encriptado en este caso en MD5, como pueden saber esto por la longitud del encriptado de 32 datos ya basta con buscar en red algun desencriptador de MD5 los cuales hay muchos en la red; bueno en resumen esto es algo sencillo que como pueden ver es una falla tan simple y tan comun en las webs solo por no poder corregir a tiempo unas variables o mejor dicho por no querer reparalas pueden dañar todo su website.

Al final la ur con la que atacamos nos quedo asi en sqlmap /usr/bin/sqlmap -u http://www.mckl.cl/noticias.php?id=9 -D moeckelyweil_bd -T user -C user,pwd –dump.

En algunas webs el panel se puede encontrar de forma sencilla por ejemplo se le puede añadir facilmente a la url algo como esto:

http://www.mckl.cl/cpanel
http://www.mckl.cl/login
http://www.mckl.cl/admin.php

entre otras cosas pero no siempre resulta asi que hay que esforzarse mas para encontrar el panel de administracion de la web; si tienen alguna duda aun sobre inyeccion sql desde sqlmap pueden ver mi video sobre la inyeccion paso a paso.

https://www.youtube.com/watch?v=TJl5MUAIADU ←Aca el video.

Recuerden como un ultimo dato de este tema hacer este tipo de ataques a webs no los hace hackers esto es un simple y sencillo defacer aprovechandote de una vulnerabilidad simple.

Terminos que talves no conoces

Hacker

Un hacker (del inglés hack, recortar), también conocidos como sombreros blancos es el neologismo utilizado para referirse a un experto en varias o algunas ramas relacionadas con la computación y telecomunicaciones: programación, redes de comunicaciones, sistemas operativos, hardware de red/voz.

Cracker

Navegante de Internet que intenta piratear programas o introducir virus en otros ordenadores o en la Red. Otra definición: Individuo con amplios conocimientos informáticos que desprotege, piratea programas o produce daños en sistemas o redes.

Persona que se dedica a entrar en redes de forma no autorizada e ilegal, para conseguir información o reventar redes, con fines destructivos. No hay que confundir este término con el de hackers.

Phreaking

Hacking relativo al sistema telefónico. Conjunto de técnicas para engañar al sistema de telefonía. Con esto pueden hacer que las llamadas que realicen sean gratuitas, que la cuenta de teléfono disminuya, llamar gratis de teléfonos públicos, escuchar celulares ajenos, y un sin fin de utilidades más sobre telefonía.

Carder

Persona que usa las tarjetas de crédito de otras personas, generación de nuevas tarjetas de crédito para realizar pagos a sistemas de compra a distancia (principalmente). En general, cualquier actividad fraudulenta que tenga que ver con las tarjetas de crédito.

Defacer

Este se dedica a explotar fallos en sitios web. Generalmente con ayuda de programas (tendencia de convertirse en lamer) o bien, con sus conocimientos propios (puede llegar a cracker o hacker).

Los defacer generalmente lo hacen por diversión o manifestar su inconformidad antes ciertas páginas, generalmente de gobierno. Aunque también solo intentar retar o intimidar a administradores.

Anarquistas

Un Anarquista es un individuo al que le gusta jugar con fuego, explosivos, químicos, etc. Ya es de por sí malo elaborar una bomba que se hará explotar en el desierto para ver qué ocurrirá. Estos sujetos tienen su biblia en el libro The Anarchist Cookbook.

Warez

Son los sujetos que distribuyen software de manera ilegal. Son piratas. La mayoría de los warez son distribuidos por grupos warez que existen con el objeto de sacar software de los BBSs antes de que otro grupo publique ese mismo programa primero.

Los gurus

Son los maestros y enseñan a los futuros Hackers. Normalmente se trata se personas adultas, me refiero adultas , porque la mayoría de Hackers son personas jóvenes, que tienen amplia experiencia sobre los sistemas informáticos o electrónicos y están de alguna forma hay, para enseñar a o sacar de cualquier duda al joven iniciatico al tema.

Los bucaneros

En realidad se trata de comerciantes. Los bucaneros venden los productos crackeados como tarjetas de control de acceso de canales de pago. Por ello, los bucaneros no existen en la Red. Solo se dedican a explotar este tipo de tarjetas para canales de pago que los Hardware Crackers, crean.

El Newbie

Traducción literal de novato. Es alguien que empieza a partir de una WEB basada en Hacking. Inicialmente es un novato, no hace nada y aprende lentamente. A veces se introduce en un sistema fácil y a veces fracasa en el intento, porque ya no se acuerda de ciertos parámetros y entonces tiene que volver a visitar la pagina WEB para seguir las instrucciones de nuevo.

SCRIPT KIDDIE

Similar al lamer, inexperto que usa programas, scripts, exploits, troyanos, nukes, etc. creados por terceros para romper la seguridad de un sistema. Suele presumir de ser un hacker o cracker cuando en realidad no posee un grado relevante de conocimientos.

LAMER

Persona falta de habilidades técnicas, sociabilidad o madurez considerada un incompetente en una materia, actividad específica o dentro de una comunidad, a pesar de llevar suficiente tiempo para aprender sobre la materia, actividad o adaptarse a la comunidad que le considera un lamer.

Se trata de una persona que presume de tener unos conocimientos o habilidades que realmente no posee y que no tiene intención de aprender. Un hacker sería el opuesto de un lamer al tener gran cantidad de conocimientos y no presumir de ello.

Generalmente hace uso de programas creados por crackers y presume de sus “logros”, con ayuda de estos programas pretende robar contraseñas de correos electrónicos o acceder a computadoras de forma no autorizada. Grave error: un lamer es el primer incauto porque los programas que usa suelen estar infectados para atraparlos.