Hacking Etico

Introducción

La inseguridad informática esta en constante crecimiento, cada día surgen nuevas amenazas que pueden dañar nuestros sistemas e inclusive robar información sensible de la organización, para estos acontecimientos debemos estar preparados día con día para poder proteger nuestros datos de una posible amenaza, para mitigar este posible riesgo existe el estudio de la seguridad e inseguridad informática en el cual se basa en aplicar las técnicas en que un posible atacante pueda obtener acceso a nuestros sistemas o inclusive la manera en que esa persona malintencionada pueda robar datos sensibles de la organización, de igual forma se aprende como proteger estos sistemas blindando nuestros datos para tener una mayor seguridad de estos.

objetivo

Se aprenderá actuar como un posible atacante, o bien pentester para de esta manera obtener las posibles vulnerables y/o amenazas de la organización. Con esta información sensible podremos observar los puntos críticos para posteriormente blindar y proteger los sistemas informáticos de usuarios malintencionados que deseen filtrar,robar,dañar y atacar su datos.

En este curso se tocan todos los aspectos que un pentester debe tomar en cuenta para una prueba de penetración tales como:

Obtención de información

Numeración

Análisis de vulnerabilidades

Explotación

Post-explotación

Generación de reportes.

A quien va dirigido

Personas que deseen aprender mas sobre la (in)seguridad informática, apasionados de los sistemas computacionales informáticos, empresas, organizaciones, estudiantes entusiastas y autodidactas.

Requisitos.

1- Conocimientos de redes y telecomunicaciones

2- Conocimientos de sistema operativo Windows

3- Conocimientos de sistema operativo Gnu/Linux

4- Conocimientos de programación (no importa el lenguaje)

5- Computadora personal (Con requisitos suficientes para virtualizar) (no netbook o procesadores atom) procesador i5 equivalente o superior, memoria ram 4 gb o superior y 20gb de discoduro libres

TEMARIO

1- Introducción
2- Instalación del escenario
3- Fases del pentesting
4- Obtención de información
5- Numeración
6- Sniffers
7- Envenenamientos ARP
8- Análisis de vulnerabilidades
9- Explotación
10- Pos-explotación
11- Ingeniería social
12- Botnets

Ing. Juan Diego Hinojosa Sandoval
Dirección General

Av. Pavorreal No. 49
Col. Provitec, Torreón,
Coahuila
arkebit.com

Exploiting Ideas