Curso Hacking Puro

Introducción

Las computadoras alrededor del mundo están siendo sistemáticamente victimizadas por atacantes. Este no es sólo un hackeo generalizado, está siendo ejecutado tan fácilmente que los atacantes comprometen un sistema, roban todo lo valioso y borran completamente su información en 20 minutos.

El objetivo de Ethical Hacker es ayudar a la organización a tomar medidas preventivas en contra de ataques maliciosos atacando el sistema por si mismo, pero manteniéndose dentro de los límites legales permitidos. Esta filosofía resulta de la práctica probada: Para atrapar a un ladrón debes pensar como un ladrón. Así como la tecnología avanza y la organización depende cada vez más de esta, la protección de los activos de información se ha convertido en un componente crítico de supervivencia. Si el "hackeo" involucra creatividad y un pensamiento "out-of-the-box", entonces las pruebas de vulnerabilidad y auditorias de seguridad no aseguran un blindaje en la seguridad de la organización.
Para asegurar que las organizaciones han protegido adecuadamente sus activos de información, deben adoptar un enfoque de defensa profundo. En otras palabras, deben penetrar sus redes y evaluar su nivel de seguridad frente a las vulnerabilidades y la exposición. La definición de un Ethical Hacker es muy similar a la de una prueba de penetración.
El Ethical Hacker es un individuo que pertenece a la organización y en quien puede confiarse para hacer un intento de penetración en sus redes y/o sistemas computacionales, usando los mismos métodos que un Hacker. El Hackeo es considerado una traición en los Estados Unidos y muchos otros países. Cuando este es realizado por solicitud y bajo un contrato entre un Ethical Hacker y una organización, es legal.

Objetivos Generales del Programa:

Esta clase llevará al participante a un entorno interactivo, donde se le mostrará como explorar, probar, "hackear" y asegurar sus propios sistemas. El entorno intensivo del laboratorio da a cada estudiante un profundo conocimiento y experiencia práctica con los actuales sistemas esenciales de seguridad. Los estudiantes empezarán por entender cómo funcionan las defensas periféricas y posteriormente serán llevados a explorar y atacar sus propias redes; ninguna red real es dañada. Luego los estudiantes aprenden como los intrusos escalan privilegios y que pasos se pueden tomar para asegurar un sistema. Los estudiantes también aprenderán sobre, Ingeniería Social, Ataques DDoS, Sobrecarga de Memoria y Creación de Virus. Cuando el estudiante termina este curso intensivo, tiene entendimiento y experiencia en Ethical Hacking.

El Curso es totalmente práctico, los alumnos ejecutan varias herramientas usando Kali Linux.

Compatible con la certificacion CEH de Ec council.

Modalidad: Presencial

Instructor: Ing. Juan Baby

Duración: 20 Horas

PROGRAMA

1	**Linux tutorial** Uso básico de Linux y comandos básicos para poder usar Kali Linux.
2	**Reconocimiento** Aprendemos como buscar el rango de direccions IP de nuestro objetivo, ubicaciones geográficas y servidores activos y la dirección IP de cada uno. Vemos como ejecutar una trasferencia de zonas en servidores DNS. Aprendemos como usar las herramientas Dnsmap,Dns Recon Recon-ng y más.
3	**Escaneo** En este segmento aprendemos como detectar puertos abiertos en cada dirección, como descubrir versión de sistemas operativos y como descubrir versión de sistemas operativos adicionalmente aprendemos como ejecutar escaneo de forma que no sea detectado por los Firewalls ni lo IPS (Intrution Prevention Systems). En la segunda parte vemos como ejecutar escanciadores de vulnerabilidades y detectar vulnerabilidades en equipos. En la tercera parte vemos como ejecutar ataques de DOS (Denegación de servicios) y como prevenir los mismos. En la 4 parte de este segmento vemos en la forma como se lanzan exploits para obtener acceso a los equipos atacados.
4	**Client side Attacks** Aquí vemos como se realizan ataques para obtener el control de PC;s de usuarios. Ataques de ingeniería y el uso de la herramienta SET.
5	**Ataques a diferentes dispositivos de red** En este segmento vemos ventores de ataques a Routers . vemos también el uso de herramientas para capturar tráfico en la red . Aprendemos como realizar ataques de fuerza bruta y consideraciones que tenemos que tomar cuando realizamos estos ataques.
6	**Wireless** En este segmento aprendemos como ejecutar ataques a redes WiFI y como descubrir los Passwords para conectarnos a diferentes redes inalámbricas. Veremos como usar herramientas dentro de Kali Linux y Hardware específico para obtener información y Passwords en redes inalámbricas.

Material:
Al finalizar el entrenamiento se entregará un CD con las presentaciones, manuales, las herramientas utilizadas durante el seminario.

Preparación:
Los alumnos deberían instalar en sus Pc's Kali Linux dentro de un entorno virtual.