Ethical Hacking en Sistemas

Código: HACK-105

Propuesta de Valor: SEGURIDAD INFORMÁTICA

Duración: 24 Horas

ste es un curso totalmente práctico que le ayudará a identificar vulnerabilidades técnicas en su infraestructura. Además de este conocimiento práctico también se realizará la preparación para la certificación internacional: "KALI LINUX CERTIFIED PROFESSIONAL" (KLPC). Incluye simulación del examen de certificación. Nota: Buen nivel de ingles técnico es requerido para el examen de certificación. El curso es desarrollado de manera teórica/práctica, cada módulo cuenta con una sección de laboratorios para que el participante aprenda el uso de herramientas según el contenido del módulo en estudio.

E

AUDIENCIA

Este curso está dirigido a profesionales de las carreras relacionadas a TI (Ing. Sistemas, Ing. Informática, Ing. Telecomunicaciones, Ing. Electrica/Electricidad) que deseen actualizar sus conocimientos e incursionar en el área de seguridad de la información y hacking ético.

PRE REQUISITOS

Para un mejor aprovechamiento del curso los participantes deberán tener conocimientos básicos de:

- Redes (Protocolos, Modelo OSI)
- Configuración y administración de sistemas operativos Windows, Linux

OBJETIVOS

Conoce gracias a este curso la valoración del riesgo al que están sometidos los activos de información de una organización. Aprenderás a actuar frente a los vectores de ataque más habituales en la informática moderna, utilizando las contramedidas y mecanismos defensivos recomendados. Así mismo, en el caso de penetración, se analizarán las medidas y acciones que una organización debe tomar, desde la valoración inicial de la amenaza hasta las acciones legales que pudieran aplicarse

CERTIFICACIÓN DISPONIBLE

Este curso lo prepara para la certificación "KALI LINUX CERTIFIED PROFESSIONAL" (KLPC).

CONTENIDO

1. CONOCIMIENTOS BASICOS

1.1. TERMINOLOGIA
1.2. TIPOS DE PRUEBAS DE PENETRACION
1.3. SHELL DIRECTA (BIND SHELL)
1.4. SHELL REVERSA (REVERSE SHELL)
1.5. PASOS DE UN ETHICAL HACKING
1.6. RECURSOS ADICIONALES

2. ESCANEOS

2.1. ESCANEANDO REDES LOCALES
2.2. DESCUBRIR HOST VIVOS
2.3. ESCANEO ARP
2.4. ESCANEO ICMP (PING)
2.5. ESCANEO SMB
2.6. ESCANEO TCP A PUERTOS 22,23,80,443 (PUERTOS ADMINISTRATIVOS)
2.7. ESCANEANDO PUERTOS
2.8. NMAP
2.9. ESCANEADORES DE VULNERABILIDADES

3. ENUMERACIÓN Y RECOLECCIÓN DE DATOS

3.1. PUERTOS RELEVANTES
3.2. TIPOS DE RECOLECCION DE DATOS
3.3. RECOLECCION DE DATOS PASIVA
3.4. RECOLECCION DE DATOS ACTIVA
3.5. DNS (PUERTO 53/UDP)
3.6. SNMP (PUERTO 161/UDP)
3.7. SMB (PUERTO 445/TCP)
3.8. WEB (PUERTO 80, 8080, ETC. /TCP)
3.9. PROXY (PUERTO 3128-8080/TCP)
3.10. LDAP (PUERTO 389/TCP)
3.11. SMTP (PUERTO 25/TCP)
3.12. RTSP (PUERTO 554 /TCP)
3.13. FTP (PUERTO 21/TCP)
3.14. MS-SQL (PUERTO 1434 /UDP)

4. METASPLOIT

4.1. BUSCANDO VULNERABILIDADES EN LA RED
4.2. TIPOS DE MODULOS DE METASPLOIT
4.3. USO BASICO
4.4. BUSCANDO EL MODULO ADECUADO
4.5. METERPRETER (META-INTERPRETER)
4.6. COMANDOS BASICOS DE METERPRETER
4.7. COMANDOS BASICOS DE METASPLOIT
4.8. EXPLOITS COMUNES POR DEFECTO (WINDOWS)
4.9. RECOLECTAR CREDENCIALES ALMACENADAS
4.10. EXTRAER PASSWORD Y HASHES DE MEMORIA/SAM

5. ATAQUES EN REDES LAN

5.1. SNIFFING PASIVO
5.2. SNIFFING ACTIVO
5.3. ENVENAMIENTO ARP
5.4. CAPTURAR CREDENCIALES
5.5. ENVENENAMIENTO LLMNR Y NBT-NS

6. PASSWORD ATTACKS

6.1. CREACION DE DICCIONARIOS PERSONALIZADOS
6.2. APLICANDO PATRONES COMUNES
6.3. ATAQUES ONLINE
6.4. ATAQUES OFFLINE
6.5. PASSWORDS POR DEFECTO
6.6. PASS THE HASH

7. PREPARACION PARA EL EXAMEN DE CERTIFICACION

7.1. ABOUT KALI LINUX
7.2. GETTING STARTED WITH KALI LINUX
7.3. LINUX FUNDAMENTALS
7.4. INSTALLING KALI LINUX
7.5. CONFIGURING KALI LINUX
7.6. SECURING AND MONITORING KALI LINUX
7.7. DEBIAN PACKAGE MANAGEMENT
7.8. ADVANCED USAGE
7.9. KALI LINUX IN THE ENTERPRISE
7.10. INTRODUCTION TO SECURITY ASSESSMENTS

BENEFICIOS

Al finalizar el curso, los estudiantes podran actuar frente a los vectores de ataque más habituales en la informática moderna, utilizando las contramedidas y mecanismos defensivos recomendados.