openwebinars.net/cert/r574G

Gracias a

OpenWebinars

OpenWebinars certifica que

Juan Carlos Villegas Mendoza

Ha superado con éxito

Ciberseguridad

CEO de OpenWebinars

Manuel Agudo

Duración de la ruta

78 horas

Fecha de expedición

14 mayo 2020

Contenido

Ciberseguridad

1. Curso de introducción a Ethical Hacking

1. Introducción

Presentación del profesor y del curso

Introducción a Ciberseguridad

2. Cifrado y PKI

Identificación digital

PKI (Public Key InfrastructurePKI)

3. Netfilter e Iptables

Netfilter - Iptables

Reglas de Iptables

4. Descubrimiento de puertos y servicios

NMAP

Escaneo con Shodan

5. Ataques sobre servicios

Fuerza bruta

Inyecciones SQL

XSS

6. Ataques a nivel de red

Introducción

Mac Flooding

Mac Spoofing

Man in the middle

DNS Spoofing

7. Vulnerabilidades y Metasploit

Introduccio■n Metasploit

Primeros pasos MSF

Meterpreter

8. Anonimato

Introducción al anonimato

2. Curso de Triage informático

1. Introducción

Presentación

Tipos de malware y características

Procesos, conexiones, puertos y protocolos

Diferencias entre un Hacker y un Cracker

C&C (Comand & Control) y direccionamiento

Test repaso Introducción

2. Búsqueda de malware

Mito y realidad sobre el malware

Metadatos, firma y descripción

Análisis heurístico y Herramientas

Test repaso Búsqueda de malware

3. Análisis de archivos ejecutables

Paquetes, ruta de instalación y ruta de ejecución

Uso de recursos

Establecimiento de conexiones

Test repaso Análisis de archivos ejecutables

4. Emails y phishing

Emails sospechosos y archivos infectados

Laboratorio: Creación de máquinas virtuales con VMware

Test repaso Emails y phishing

3. Curso de análisis de malware

1. Introducción

Presentación

¿Qué es el malware?

Procedimiento para el análisis de malware

Análisis dinámico, estático y online

Consideraciones de hardware para análisis

Test repaso Introducción

2. Laboratorio de análisis

Software de virtualización

Diseño y despliegue de máquinas virtuales

Herramientas de análisis

Test repaso Laboratorio de análisis

3. Análisis de malware

Obtención de malware y análisis estático

Sandbox y análisis dinámico

Interpretación de informes

Test repaso Análisis de malware

4. Creación de Malware

Herramientas para la creación de malware

Laboratorio: Creación de un malware básico (Parte I)

Laboratorio: Creación de un malware básico (Parte II)

Test repaso creación de Malware

4. Curso de Hacking web

1. Introducción

Presentación

¿Qué es el hacking?

2. Inyecciones de código

SQL Injection

SQL Injection: Ataque en Login

SQL Injection: Obtención de datos

Cross-Site Scripting (XSS)

Tipos de Cross-Site Scripting

Ataque: Cross-Site Scripting (XXS)

3. Ficheros

Unrestricted File Upload

Ataque: Unrestricted File Upload

Local File Inclusion

Ataque: Local File Inclusion

4. Robo de sesiones

Session Prediction

Ataque: Session Prediction

Fuerza bruta

Ataque: Fuerza bruta

5. Accesos ilegales

Parameter Tampering

Ataque: Parameter Tampering

Control inseguro de roles

Ataque: Control inseguro de roles

5. Curso de Hacking con buscadores: Google, Bing y Shodan

1. Tipos de buscadores, ¿cual elijo?

Presentación

Motores de búsqueda

2. Google robots

Qué son los archivos robots.txt

Obtención de información con Google robots.txt

Hacking con Google robots.txt

3. Hacking con Google

Operadores lógicos con Google

Google dorks

4. Hacking con Bing

Operadores lógicos de Bing

Bing dorks

5. Hacking con Shodan

¿Qué es Shodan? Operadores lógicos y ejemplos.

6. Herramientas automatizadas

¿Para que sirven?

Foca forensic

Snitch

SQLI Hunter

Bingoo

7. Metadatos que son y como obtenerlos

Herramienta Exiftool

Herramienta PyExifToolGui

6. Curso de desarrollo seguro

1. Ciclo de desarrollo seguro de software

Introducción al curso y presentación del profesor

Ciclo de desarrollo de software

Requisitos

Arquitectura y diseño

Implementación

Testeo

Despliegue

Mantenimiento

2. Seguridad en el desarrollo

Validación de entradas

Práctica de validación de entradas

Codificación de salidas

Práctica de codificación de salidas

Criptografía

Práctica de criptografía

Buffer overflow

Práctica de buffer overflow

3. Seguridad en los procesos y procedimientos

Autenticación y manejo de contraseñas

Práctica de Autenticación y manejo de contraseñas

Manejo de sesiones

Práctica de manejo de sesiones

Manejo de errores y log

Práctica de manejo de errores y log

4. Seguridad en la configuración del entorno

Control de acceso

Práctica de control de acceso

Protección de datos

Prácticas de protección de datos

Seguridad de comunicaciones

Práctica de seguridad de comunicaciones

Configuración del sistema

Práctica de configuración del sistema

Seguridad en Bases de datos

Práctica de seguridad en Bases de datos

Manejo de ficheros

Práctica de manejo de ficheros

Manejo de memoria

7. Curso OSINT: Técnicas de investigación e inteligencia en fuentes abiertas

1. Introducción

Presentación del curso y profesor

2. OSINT

Inteligencia y ciberinteligencia

OSINT, HUMINT, SOCMINT, CYBINT

Ciclo de inteligencia

Credibilidad vs. fiabilidad

Factor humano

3. Hacking con buscadores

Google Hacking

Dorks en buscadores generalistas

Búsqueda inversa de imágenes

Buscadores tecnológicos

Buscadores en Deep&Dark Web

Reto: Hacking con buscadores

4. Metadatos

¿Qué son los metadatos?

Herramientas para la extracción de metadatos: ExifTool

Herramientas para la extracción de metadatos: Foca

Reto: Metadatos

5. Herramientas

Entorno

OSRFramework (Parte I)

OSRFramework (Parte II)

OSRFramework (Parte III)

Maltego

Repositorios OSINT

WHOIS y direcciones IP

Reto: Herramientas

6. Monitorización en OSINT

Herramientas de monitorización OSINT

Servicios de alerta

7. Privacidad y anonimato

Creación de identidad anónima digital

Enmascarando nuestra identidad

8. Curso de Metasploit Framework

1. Introducción a Metasploit

Presentación

¿Qué es Metasploit?

2. Instalación de Metasploit Framework

Instalación de Metasploit en Linux

Instalación de Metasploit en Microsoft Windows

3. Configuración y fundamentos de Metasploit Framework

Ejecutar servicios de Metasploit

Comandos msfconsole

Exploits y tipos de Payloads

Generando Payloads

Bases de datos

Shell Meterpreter

4. Information Gathering (Recopilación de información)

Escaneo de puertos

Usando Metasploit para descubrir vulnerabilidades MSSQL

Identificación de servicios

5. Escáner de vulnerabilidades

Nmap Scripts

Nessus: escáner de vulnerabilidades

6. Ataques del lado del cliente

Troyano para Linux

Phishing

PDF Malicioso

7. Post explotación

Escalada de privilegios

Persistencia con NetCat

Capturando tráfico

Captura de pantalla

Buscando contenido en máquinas comprometidas

John the Ripper: rompiendo Hashes

8. Meterpreter scripting

Personalización del Payload Meterpreter

9. Mantenimiento de acceso

Keyloggin

Shell Meterpreter persistente

10. Uso avanzado de Metasploit

Backdorizando archivos .EXE

11. Entorno gráfico de Metasploit Framework

Armitage GUI

Módulos auxiliares

9. Curso de Seguridad en Redes con Snort

1. Snort

Presentación del profesor e introducción a Snort

Instalación de Snort

Reglas I

Reglas II

Unified I

Unified II

Adquisición de datos (DAQ)

Configuración

2. Preprocesadores

Session I

Session II

Reputation

HTTP I

HTTP II

PortScan