openwebinars.net/cert/g3jv

Gracias a

OpenWebinars

OpenWebinars certifica que

Carlos Juan Viñas

Ha superado con éxito

Especialista en Hacking Ético

CEO de OpenWebinars

Manuel Agudo

Duración de la ruta

35 horas

Fecha de expedición

11 mayo 2023

Contenido

Especialista en Hacking Ético

1. Análisis forense básico en sistemas Windows

1. Taller

Análisis forense básico en sistemas Windows

2. Análisis forense avanzado en sistemas Windows

1. Taller

Análisis forense avanzado en sistemas Windows

3. Análisis forense básico en sistemas Linux

1. Taller

Análisis forense básico en sistemas Linux

4. Análisis forense avanzado en sistemas Linux

1. Taller

Análisis forense avanzado en sistemas Linux

5. 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

6. Herramientas avanzadas para búsquedas OSINT

1. Taller

Herramientas avanzadas para búsquedas OSINT

7. 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

8. Curso de Hacking Tools: Blue Team

1. Introducción

Presentación

2. Linux 100%

Usuarios, grupos y permisos

Práctica: Usuarios, grupos y permisos

Accesos remotos

Práctica: Accesos remotos

Squid

Práctica: Squid

Uso de Iptables

Práctica: Uso de Iptables

3. Metasploit 100%

Funcionalidad de la herramienta

Práctica: Funcionalidad de Metasploit

Uso en diferentes fases del hacking

Atacando Linux y Windows

Práctica: Atacando Windows

Práctica: Atacando Linux

4. Phyton para pentesting

Uso de librerías específicas para hacking y scripts

Práctica: Librerías específicas para hacking y scripts

Scapy

Beautifulsoup

Creación de un script automatizado para extracción de links

9. Curso de Hacking Tools & Forensic: Red Team

1. Introducción

Presentación

2. Taxonomía de un ataque

Inyección SQL y fuerza bruta

Práctica: Inyección SQL y fuerza bruta

Cross-site Scripting (XXS) y Server Side Includes (SSI)

Práctica: XXS y SSI

Inyección de código

Phishing

3. Hacking infraestructuras

Buscando objetivos con Shodan y ZoomEye

Google Dorks

Ataques Man in the Middle

Cracking wifi

4. Forensic■

Introducción a la informática forense

Normativa RFC3227

Volcados de memoria en Linux y Windows

Herramientas útiles: Nmap

Herramientas útiles: Wireshark

Herramientas útiles: Volatility

Herramientas útiles: Dumpit

Herramientas útiles: Autopsy

10. Metasploit para pentesting

1. Taller

Metasploit para pentesting

11. Autopsy: Recuperación de datos

1. Taller

Autopsy