S.E.I.M.

CIBER SEGURIDAD

MASTER PRIVADO DE EXPERTO EN CIBERSEGURIDAD

PRESENCIAL

CENTRO FP SEIM Y TSSCIBERSEGURIDAD

Presentación

En un mundo hiperconectado, donde el acceso a cualquier información está solo a un clic, proteger la seguridad de personas, empresas y organizaciones en la red se ha convertido en algo fundamental. Así, a la misma vez que avanza la tecnología, también lo hacen las amenazas y las técnicas de ataque. Cuantas más nuevas funcionalidades existen y más comunicados estamos, más aumenta nuestra superficie de ataque. Es decir, crecen las posibilidades y vías que tienen los ciberdelincuentes para conseguir sus objetivos.

Es en este contexto donde CENTRO SEIM y TSSCIBERSEGURIDAD presentan este programa con el que los profesionales aprenderán de manera completa a proteger y asegurar diversos entornos digitales. Todo ello, desde una perspectiva eminentemente práctica y adaptada a los tiempos actuales.

El programa incluye, en su cuadro docente, a profesionales del sector que vierten en esta capacitación la experiencia de su trabajo.

OBJETIVOS

Siendo plenamente conscientes de la relevancia que tiene la Ciberseguridad para las empresas, CENTRO SEIM y TSSCIBERSEGURIDAD han desarrollado este Máster Título Propio que tiene como objetivo nutrir y actualizar los conocimientos de los profesionales en materia de detección, protección y prevención de delitos informáticos.

De esta manera, el futuro egresado se convertirá en una pieza clave en el cuidado de los datos y la información, minimizando la posibilidad de que los delincuentes se beneficien de posibles brechas de seguridad existentes. Una competencia profesional que en CENTRO SEIM, en tan solo 9 meses, el profesional podrá adquirir.

ESTRUCTURA Y CONTENIDO

Introducción a la Ciberseguridad

- LAN-WAN
- Internet
- Privacidad – Anonimato
- Seguridad Wifi
- Amenazas
- Contraseña segura
- Correo seguro
- Backup / Recuperación / Borrado
- Antivirus

Arquitectura de Redes

- Introducción
- Modelo OSI
- Creación laboratorios
- NAT vs Bridge en virtual
- GNS3
- Creación de redes locales

ESTRUCTURA Y CONTENIDO

Hacking Ético

- Introducción
- Uso de distribuciones específicas
- Recolección de información
    - Uso de herramientas de red (Whois, Traceroute, ping…)
    - Google Dorks
    - OWASP – Mantra (http-headers, Passive Recon…)
    - Extracción de metadatos (FOCA)
    - Plugins de Firefox útiles
    - Técnicas OSINT
    - Ingeniería social
    - Uso de herramientas de Kali
    - Recolección de información de una red LAN
    - Anonimato (Tor, uso de vpn)

ESTRUCTURA Y CONTENIDO

- Escaneos de puertos y vulnerabilidades
  - Análisis de servicios y puertos
    - Nmap (uso de la herramienta en sus distintos tipos de escaneo)
    - Evasión de Firewalls
  - Análisis de vulnerabilidades
    - Clasificación de las mismas
    - Acunetix
    - Nessus
    - Nikto
    - Cmsmap
    - Wpscan
    - Joomscan
    - Zap
    - Burp Suite Pro

ESTRUCTURA Y CONTENIDO

- Ataque
  - Análisis de situación
  - Búsqueda de exploits
  - Ataque manual y automatizado
  - Metasploit
  - Ataque directo e inverso
  - Pivoting
- Post-Explotación
  - Escalada de privilegios
  - Backdoors
  - Extracción de información sensible y útil
  - Tipos de ataque – escalada posterior
    - Directos – Inversos – Ingeniería Social
- Password Cracking
  - Ataques online y offline
  - Hashcat
  - Hydra
  - Ophcrack
  - Metasploit (auxiliares)
  - John
  - Cracking online

ESTRUCTURA Y CONTENIDO

- Hacking Wifi
  - Material necesario
  - Uso de Airgeddon
- Malware
  - Configuración de troyano
  - Crypter
  - Evasión de antivirus
  - Creación de troyano
  - Metodos de infección
- Auditorías Web
  - Taxonomía de un ataque
  - Ejemplos de vulnerabilidades y ataques:
    - Inyección SQL
    - Xss
    - LFI
    - Inyección de código
    - RFI

ESTRUCTURA Y CONTENIDO

- Hacking Infraestructuras
  - Redes
    - Linux
    - Windows
    - OS
- Escalada de privilegios
  - Shell Scripting
    - Linux
    - Windows
- Forense
  - Introducción a la informática forense
  - Evidencia digital
  - Análisis de datos
  - Mail
  - Forense en redes y geo
  - Forense móviles
  - Elaboración de informe

ESTRUCTURA Y CONTENIDO

- Programación en Python
  - Introducción sobre Python
  - Instalación de Python en Windows y Linux y librerías externas
  - Python Shell y entorno IDE
  - Introducción a la programación
    - Tipo de datos
    - Estructuras de control y flujo
    - Funciones
    - Módulos
    - Objetos
    - Recolección de información
    - Escaneo de la red
    - Análisis de vulnerabilidades

ESTRUCTURA Y CONTENIDO

- Seguridad
  - Instalación de Firewall
    - Configuración básica
    - Creación de reglas
  - Instalación de UTM
    - Configuración
    - Análisis del mismo
  - Monitorización
    - Tipos de monitorización
    - Instalación de monitorización IDS
    - Instalación de master y sensores en la red
    - Creación de reglas
    - Análisis de eventos

Proyecto fin de curso

- Creación de proyecto fin de curso

PERFILES DE ENTRADA Y SALIDA

PERFILES DE ENTRADA

A continuación se describen los perfiles de entrada ideales que han de tener los alumnos:

	Master
Experiencia profesional (Emprendedor, Directivo, Vicepresidente, Director, Manager, Con experiencia, Sin experiencia)	Profesionales del mundo tecnológico. Administradores de sistemas y/o profesionales de dptos. de informática. Toda persona dispuesta a dar un cambio de rumbo a su formacion profesional.
Conocimiento del área (Alta/Media/Baja)	Media-baja
	100% técnica y practica.

PERFILES DE SALIDA

A continuación se describen los perfiles de salida:

Master
Consultor de ciberseguridad. Experto en Hacking ético. Pentester Junior-Senior. Team leader Red team. Auditor de seguridad informatica.

CARACTERÍSTICAS DEL MASTER

- Máster Presencial.
- Inicio: 7 de Noviembre
- Clases presenciales: Lunes y miércoles de 18:00h a 20:30h
- Precio: 1900€ (pago de 211€/mes durante 9 meses).
- Duración para la realización del máster: 9 meses.
- Examen, certificado y tutorización incluida en el precio.
- Cartas de recomendación.
- Bonificable por la Fundae