
Especialista en gestión
de la ciberseguridad
Bootcamp 22
by
avante
¿hasta dónde quieres llegar?

Un bootcamp en el que conocerás las claves del marco de trabajo CISSP, uno de los más reconocidos del mercado, y podrás disfrutar trabajando con las herramientas técnicas que proporciona Ethical Hacking

Intensivo 6 semanas – De lunes a jueves de 17:00 a 19:30 (ESP)
12:00 a 15:00 pm (ARG) /10:00 am - 13:00 pm (CHILE) /
10:00 am - 13:00 pm (MEX)

Del 6 de febrero al 21 de marzo
80 horas

avante
¿hasta dónde quieres llegar?

CISSP Certified Information Systems Security Professional

/PROGRAMA/

1. Gestión de seguridad y riesgos

- Conceptos de confidencialidad, integridad y disponibilidadPrincipios de gobernanza de la seguridad
- Cumplimiento
- Cuestiones legales y regulatoriasÉtica profesional
- Políticas, estándares, procedimientos y directrices de seguridad
- Requerimientos para la continuidad del negocioPolíticas de seguridad del personal
- Conceptos de gestión de riesgo
- Modelado de amenazas Consideracio nes de riesgo
- Educación, captación y concienciación en seguridad

1. Seguridad de activos

- Clasificación de la información y de activos Propiedad
- Protección de la privacidad
- Retención apropiada
- Controles de seguridad de los datosRequisitos de manejo

2. Ingeniería de seguridad

- Procesos de ingeniería utilizando principios de diseño seguroConceptos básicos de modelos de seguridad
- Modelos de evaluación de seguridad
- Capacidades de seguridad de los sistemas de información Vulnerabilidades de las arquitecturas de seguridad, del diseño y de loselementos de las soluciones de seguridad
- Vulnerabilidades de los sistemas basados en la Web Vulnerabilidades de los sistemas móviles
- Vulnerabilidades de los dispositivos integrados y de sistemas ciber-físicos
- Criptografía
- Principios de seguridad en el diseño de sitios e instalaciones Seguridad física

4. Seguridad de comunicaciones y redes

- Diseño de la arquitectura de red segura
- Componentes de red segura
- Canales de comunicación segura
- Ataques de red

5. Gestión de identidad y acceso

- Control de activos físicos y lógicos
- Identificación y autentificación de personas y dispositivos
- La identidad como servicio
- Servicios de identidad de terceros
- Ataques de control de acceso
- Ciclo de vida del aprovisionamiento de identidad y acceso

6. Evaluación y pruebas de seguridad

- Estrategias de evaluación y pruebas
- Datos de proceso de seguridad
- Pruebas de control de seguridad
- Resultados de pruebas
- Vulnerabilidades en la arquitectura de seguridad

7. Operaciones de seguridad

- Apoyo a las investigaciones y requisitos
- Registro y seguimiento de las actividades
- Aprovisionamiento de recursos
- Conceptos básicos de operaciones de seguridad
- Técnicas para la protección de recursos
- Gestión de incidentes
- Medidas de prevención
- Gestión de correcciones y vulnerabilidades
- Procesos de gestión del cambio
- Estrategias de recuperación
- Planes y procesos para la recuperación de desastres
- Planificación y ejercicios de Continuidad del Negocio Seguridad física
- Preocupaciones de seguridad del personal

8. Seguridad en el desarrollo de software

- Seguridad en el ciclo de vida de desarrollo de software
- Controles de seguridad del ambiente de desarrollo
- Efectividad de la seguridad del software
- Impacto en la seguridad del software adquirido

/PROGRAMA/

1. Principios de la seguridad de la información
   - ¿Qué entendemos por seguridad de la información?
   - Definición de un Servicio de Seguridad.
   - El principio de defensa en profundidad (Defense in Depth)
   - Análisis y gestión de riesgos.
   - Definición de las directrices de seguridad empresarial: Respuestas frentea los incidentes de seguridad.

2. El hacking ético y las políticas de seguridad en la organización
   - Seguridad versus empleados: La Ingeniería Social.
   - Buenas prácticas a la hora de adquirir productos de software.
   - Seguridad física de las instalaciones.
   - Sistemas de vigilancia de tráfico de red: NIDS (Network Intrusion Detection System)
   - ¿Qué es el hacking ético?
   - Pruebas de penetración (Pen-Tests)

1. Definición de los diferentes tipos de ataques a la infraestructurainformática
   - Reconocimiento de sistemas.
   - Detección de vulnerabilidades.
   - Robo de información por interceptación de mensajes (Sniffing)
   - Suplantación de IP (IP Spoofing)
   - Suplantación de DNS (DNS Spoofing)
   - Inyección de código SQL javascript
   - Ataques a sistemas criptográficos.
   - Ataques de Man in the Middle (MitM)
   - Ataques al protocolo HTTP (Cross-Site Scripting)Virus, Gusanos, Espías y Troyanos
   - Ataques de denegación de servicio (DoS) y denegación de serviciodistribuido (DDoS)
   - Redes Zombies (botnets y spamnets)
   - Elevación de privilegios en los sistemas (RootKits)
   - Capturadores de teclado (Keylogger)

4. Diseño del laboratorio para las prácticas
   - Cuestiones legales a considerar antes de realizar los labs.
   - Determinar el entorno de virtualización idóneo.
   - Creación de redes virtuales y segmentación.
   - Creación de la máquina virtual de Kali Linux.
   - Creación de máquina virtual de Windows 10 con licencia.
   - Creación de la máquina virtual “metasploitable”
   - Conectar una tarjeta WiFi a la máquina virtual de Kali.

5. Reconocimiento (Information Gathering)
   - Consideraciones legales sobre las búsquedas OSINT.
   - Google search y la recolección de información de e-mail (e-mailharvesting) theHarverster
   - Maltego
   - Escaneo de puertos y fingerprinting con nmap.Zenmap, GUI para nmap.
   - Determinación del sistema operativo objetivo con NetCraft.
   - Búsqueda de vulnerabilidades con cvedetails y Nessus.

6. Ganar acceso a la víctima
   - Introducción a Metasploit. Qué es una Shell.

- Diferencia entre Shell directa e inversa.
- Qué es el payload.
- Ataque directo basado en vulnerabilidad presente en el sistemaoperativo de la víctima
- Crear un payload usando msfvenom.
- Crear un payload encriptado para evadir al antivirus.
- Determinar el grado de detección del malware en las solucionesantivirus comerciales.

7. Encriptación avanzada del payload

- Introducción a Veil.
- Instalación de Veil.
- Creación de un payload indetectable con Veil.
- Incrustación del payload en un ejecutable.
- Incrustar el payload en archivos jpg, pdf, mp3…
- Incrustar el payload en una macro de documentos de Office.
- Falsear la extensión de los archivos.

8. Captura de tráfico y MitM con Kali

- Uso de Wireshark para la disección de paquetes.
- Capturas de contraseñas con Cain
- Envenenamiento de la tabla ARP (ARP Spoofing) con arpspoof.
- Ataque Man in the Middle contra la puerta de enlace
- Envenenamiento de la caché de DNS (DNS Spoofing)
- Uso de ettercap para realizar ataque MitM.
- Ataque MitM en conexiones protegidas por SSL

9. Post exploitation

- Conseguir persistencia para las puertas traseras.
- Escalado de privilegios: getsystem.
- Migración del proceso del payload.
- Determinar si la victima es un sistema operativo virtualizado ofísico.
- Desinstalación de software en la víctima.
- Creación de usuarios, cambio de password y pertenencia a grupolocal administradores.
- Qué es el pivoting (pivotaje)
- Robar los password de WiFi de la víctima con Metasploit.Instalar un keylogger en la víctima.
- Ataque offline a las credenciales de Windows: los hashes, john the Ripper y Rainbow Tables.
- Compendio de técnicas de ataques de Ingeniería social con SET.
- Eliminar la protección del antivirus
- Recuperación de archivos que no están en la papelera de reciclaje.
- Enumeración de unidades USB

10. El framework BeEF

- Introducción a BeEF.
- Secuestrar navegadores con BeEF.
- Realizar capturas de pantalla en los dispositivos secuestrados por BeEF.
- Redirigir la navegación de un equipo comprometido.
- Robar las credenciales online a través de BeEF.
- Integrar BeEF con Metasploit.

11. Vulnerabilidades en aplicaciones web

- Vulnerabilidad en sistemas vs desarrollo de aplicaciones web.
- El proxy Burp.
- Determinar las vulnerabilidades de la aplicación por medio deBurp.
- Pentesting de aplicaciones web con Nessus.

12. Ataque a redes inalámbricas y dispositivos móviles

- Búsqueda de puntos de acceso.
- Los protocolos WEP, WPA y WPA2 y sus ataques.Framework para atacar la WiFi.
- Smartphone pentest framework (SPF)
- Configuración de SPF y de emuladores de Android.

13. Hacking con acceso físico

- Robo de información por medio de USB de inicio con Kali.
- Microcontroladores y su aplicación para el hackeo de sistemas.
- Qué es el framework Arduino.
- Qué es Rubber Ducky.
- Instalación del software necesario.
- Comandos de Rubber Ducky.
- Conversión de comandos a un script de Arduino
- Cambiar el password del administrador en cuestión de segundos.
- Denegación de servicios WiFi con Arduino