UVM | EDUCACIÓN CONTINUA

Bootcamp:

Ciberdefensa y Ciberseguridad

Programa *online* de 224 horas
(27 semanas)

¿Qué es un Bootcamp?

Una experiencia *learning by doing* significativa de aprendizaje, en la cual los participantes adquieren conocimientos y desarrollan competencias tecnológicas de aplicación inmediata, de una manera práctica y efectiva a través de sesiones sincrónicas semanales interactivas en línea y actividades de aprendizaje en la plataforma, guiados por profesores expertos y mediante modelo educativo integral.

Características del programa:

Modalidad Bootcamp interactivo de 224 horas:

- 104 horas de clases de clases sincrónicas interactivas en línea (clases en vivo).
- 120 horas actividades asincrónicas.

Las 104 horas de clases sincrónicas interactivas en línea (clases en vivo) se imparten en un período de 27 semanas:

- Fase de Preparación
  - Semana 1: 2 horas de clases
  - Semana 2: 2 horas de clases
- Fase de Bootcamp
  - Semanas de la 3 a la 27 (total 25 semanas): 4 horas de clase por semana

Las 120 horas de actividades asincrónicas consisten en:

- Clases pregrabadas (una por semana)
- Ejercicios y casos prácticos (uno por semana)
- Foros (uno por semana)
- Exámenes de certificación (al final del bootcamp)

Objetivo del programa:

El participante aprenderá cómo hacer diagnósticos de vulnerabilidad ante *hacking* y ataques; los métodos de análisis forense y respuesta a incidencias de ciberataques; aspectos fundamentales de configuración y operaciones de sistemas para prevención de ataques; las herramientas para la ciberdefensa, así como los criterios para generar estrategias y proteger los sistemas, redes, comunicaciones y cloud conforme a prácticas internacionales de ciberseguridad.

Diferenciación:

- Certificación internacional con tecnología *Blockchain,* de *Embiz Foundation* (www.embizfoundation.org).
- Certificado de competencias laborales DC-3, de la Secretaría del Trabajo y Previsión Social (STPS).
- Experiencia de Bootcamps, en donde el aspirante se enfrentará a retos prácticos con su profesor y compañeros de grupo con la finalidad de conocer distintas perspectivas y métodos utilizando herramientas valiosas.
- Valor más alto del mercado y en horarios adecuados para nuestros alumnos.

Modelo educativo:

El programa estará distribuido de la siguiente manera:

- Acceso a plataforma
- Profesores expertos
- Clases sincrónicas (en vivo)
  - Explicaciones prácticas
  - Ejercicios guiados por el profesor
  - Retos en equipos e individuales
  - Sesiones *live code*, programación (interactiva - en vivo)
- Clases pregrabadas
- Ejercicios
- Foros de interacción
- Casos prácticos
- Exámenes de certificación

Beneficios:

Al finalizar el programa, el participante obtendrá, además de su diploma de UVM, el Certificado Digital Internacional avalado por *Embiz Foundation*, así como el Certificado DC-3 de Competencias Laborales, avalado por la STPS.

¿Qué herramientas de trabajo necesito para cursar un BootCamp en UVM?

1. Contar con computadora de escritorio o laptop y acceso a internet a través de wifi.
2. La computadora debe tener microprocesador Ryzen o Intel i5 o superior, Gen 10 o superior, 8 GB de RAM y 100 GB libres de disco duro.
3. Abrir cuentas para acceso a software libre y en la nube, acceder a un repositorio de documentos, código y proyectos, que el profesor informará en la primera clase.

TEMARIO

01 Fundamentos de la Ciberdefensa y Ciberseguridad

a) Conceptos Básicos

1. Definición de Ciberseguridad
   - Origen y evolución histórica
   - Importancia en el mundo actual
2. Principios de la Ciberseguridad:
   - Confidencialidad, Integridad y Disponibilidad (Tríada CIA)
   - Autenticidad, No repudio y Responsabilidad

b) Gobernanza, Riesgo y Cumplimiento

1. Gobernanza de la Ciberseguridad:
   - Estructuras organizativas
   - Políticas, normas y procedimientos
2. Análisis y Mitigación del Riesgo:
   - Evaluación del riesgo
   - Estrategias de mitigación
   - Modelos de madurez de ciberseguridad
3. Cumplimiento Normativo:
   - Regulaciones y estándares: GDPR, ISO 27001, NIST
   - Auditorías y controles

c) Planificación de la Continuidad del Negocio

1. Business Continuity Planning (BCP):
   - Elementos clave del BCP
   - Desarrollo y pruebas del BCP
2. Disaster Recovery (DR):
   - Diferencias entre BCP y DR
   - Estrategias de DR: *backups*, sitios de recuperación y redundancia

d) Infraestructura y Seguridad en Sistemas Operativos

1. Configuración Segura:
   - Linux: *hardening*, permisos, SELinux/AppArmor
   - Windows: políticas de grupo, configuración del Active Directory, Kerberos
2. Tareas y Automatización:
   - Uso de tar, cron y cronjobs en Linux
   - Programación y scripting en Bash para tareas de seguridad
3. Monitorización y Logging:
   - Syslog en Linux, Event Viewer en Windows
   - Importancia del logging para la detección de amenazas de seguridad

e) Desafíos Actuales y Tendencias en Ciberseguridad

1. Amenazas emergentes:
   - *Malware* avanzado, *ransomware*, APTs
   - Desafíos de IoT y dispositivos conectados
2. Soluciones y tendencias:
   - Inteligencia contra amenazas
   - *Machine learning* y AI en ciberseguridad

Práctica:

1. Analiza y evalúa las políticas de ciberseguridad de una organización ficticia
2. Desarrolla un plan básico de continuidad del negocio para un caso de estudio
3. Realiza tareas de *hardening* en una máquina virtual Linux y Windows
4. Automatiza tareas de seguridad usando *scripts* en Bash
5. Configura el *logging* en Linux y Windows y simula eventos para monitorización

02 Configuración y Operaciones de Sistemas

a) Configuración y Hardening de Sistemas Operativos

1. Configuración de Linux:
   - Instalación y configuración inicial
   - Servicios esenciales y demonios
   - Gestión de usuarios y grupos
   - Uso y configuración de sudo
2. Configuración de Windows:
   - Instalación y roles de Windows Server
   - Gestión de usuarios y grupos
   - Políticas de grupo (GPOs)
   - Servicios y características de Windows
3. *Hardening* de sistemas:
   - Principios del *hardening*
   - Herramientas para auditoría y *hardening* (ej. Lynis para Linux, Security Compliance Toolkit para Windows)
   - Limitación de servicios y puertos abiertos
   - Actualizaciones y parches

b) Automatización y Tareas Programadas

Tar, Cron, Cronjobs:
- Uso de Tar para la gestión de archivos
- Programación de tareas con Cron

2. - Creación y gestión de Cronjobs

Automatización en Windows:
- Programador de tareas
- Uso de PowerShell para la automatización

c) Logging y Monitorización

Gestión de registros en Linux:
- Herramientas de registro (ej. *syslog, rsyslog*)

2. - Rotación y retención de *logs*

Gestión de registros en Windows:
- Visor de Eventos

3. - Políticas de auditoría

Centralización de logs:
- Introducción a soluciones como ELK Stack (Elasticsearch, Logstash, Kibana)
- Configuración y envío de logs a sistemas centralizados

d) Scripting y Automatización Avanzada

1. Bash Scripting:
   - Conceptos básicos y estructuras de control
   - Uso de scripts para tareas de administración
2. PowerShell en Windows:
   - Conceptos básicos
   - Automatización y administración con PowerShell

e) Administración de Directorio Activo y Autenticación

1. Introducción al Active Directory:
   - Estructura y componentes (Dominio, OUs, DC)
   - Gestión de usuarios y políticas
2. Kerberos:
   - Fundamentos y arquitectura
   - Autenticación y *tickets*
   - Problemas comunes y soluciones

Práctica:

1. Configura y protege un servidor Linux y Windows de acuerdo a las Mejores Prácticas.
2. Automatiza tareas comunes utilizando cron y PowerShell.
3. Establece políticas de registro adecuadas y centraliza los *logs* usando ELK Stack.
4. Implementa *scripts* en Bash y PowerShell para tareas administrativas.
5. Configura un dominio en Active Directory y realiza autenticación con Kerberos.
6. Configura un servidor Linux y Windows, implementa una tarea programada y escribe un *script* simple en Bash.

03 Redes, Seguridad en Comunicaciones y Cloud

a) Arquitectura y Diseño de Redes

1. Fundamentos de Redes:
   - Modelos OSI y TCP/IP
   - Dispositivos de red: Routers, Switches, Firewalls
   - Subnetting y VLSM
2. Diseño de Red Seguro:
   - Zonas desmilitarizadas (DMZ)
   - Segmentación de redes
   - Diseños de alta disponibilidad

b) Operaciones de Red y Seguridad

1. Operación de Redes y Monitoreo:
   - Protocolos comunes: DHCP, DNS, HTTP/HTTPS
   - Herramientas de monitoreo: SNMP, NetFlow
2. Port Scanning y Reconocimiento:
   - Herramientas como Nmap y Zenmap
   - Técnicas de evasión y reconocimiento
3. Defensa y Mitigación:
   - IDS/IPS
   - Firewalls: de red, de aplicación
   - Prevención de ARP spoofing y otros ataques de red

c) Análisis de Tráfico y Herramientas

1. Introducción a Wireshark:
   - Funciones básicas y avanzadas
   - Filtrado y análisis de paquetes
2. Detección de Anomalías:
   - Patrones de tráfico sospechoso
   - Signaturas de *malware* y exfiltración de datos

d) Comunicación Segura y Protección de Datos

1. Email Security:
   - SPF, DKIM, DMARC
   - Prevención de phishing y amenazas avanzadas
2. Wireless Security:
   - Configuración y protección de redes Wi-Fi
   - WPA3 y técnicas de hardening
3. Cryptography y Encryption:
   - Conceptos de cifrado simétrico y asimétrico
   - Certificados y PKI
   - Protocolos seguros: SSL/TLS, SSH

e) Seguridad en Cloud y Virtualización

1. Fundamentos del Cloud Computing:
   - Modelos de servicio: IaaS, PaaS, SaaS
   - Proveedores principales: AWS, Azure, Google Cloud
2. Configuración y Hardening en la Nube:
   - Controles de acceso
   - Gestión de identidades (IAM)
   - Protección de datos: almacenamiento cifrado, *backups*
3. Virtualización y Contenedores:
   - Conceptos básicos de virtualización
   - Seguridad en entornos VMware, Hyper-V
   - Introducción a Docker y Kubernetes y su seguridad

Práctica:

1. Diseña una arquitectura de red segura utilizando segmentación y DMZ.
2. Realiza un escaneo de puertos sobre una red ficticia, analiza el tráfico con Wireshark.
3. Configura una red inalámbrica segura y establece medidas de seguridad para un servidor de correo.
4. Aplica técnicas de cifrado para proteger datos en tránsito y en reposo.
5. Configura un entorno básico en AWS (o cualquier otro proveedor de cloud) y aplica medidas de seguridad, incluyendo la protección de instancias y almacenamiento.

04 Respuesta a Incidentes, Forense y Monitoreo

a) Conceptos Básicos de Respuesta a Incidentes

1. Introducción a la Respuesta a Incidentes:
   - Definición de incidente
   - Ciclo de vida del manejo de incidentes
2. Equipos de Respuesta a Incidentes (CERT/CSIRT):
   - Roles y responsabilidades
   - Creación y operación de un CSIRT

b) Preparación y Detección de Incidentes

1. Planificación de Respuesta a Incidentes:
   - Creación de un plan de respuesta
   - Herramientas y recursos esenciales
2. Detección de Incidentes:
   - Señales y alertas
   - Herramientas de detección: IDS, IPS, SIEM

c) Gestión y Mitigación de Incidentes

1. Análisis y Valoración:
   - Triage de incidentes
   - Herramientas de análisis y correlación
2. Contención y Erradicación:
   - Estrategias de contención a corto y largo plazo
   - Eliminación de amenazas y restauración

d) Forense Digital y Análisis Post-Incidente

1. Introducción a la Forense Digital:
   - Principios y metodologías
   - Cadena de custodia
2. Extracción y Análisis de Evidencia:
   - Imágenes de discos y memoria
   - Herramientas de análisis: *Autopsy, FTK, Volatility*
3. Data Recovery:
   - Principios de recuperación de datos
   - Herramientas y técnicas

e) Monitoreo Proactivo y Herramientas

1. Introducción a Splunk:
   - Funcionalidades principales
   - Creación de *dashboards* y alertas
2. Otras soluciones de Monitoreo y Logging:
   - ELK Stack
   - Graylog
3. Integración y Correlación de Eventos:
   - Técnicas para identificar patrones
   - Configuración de correlación en SIEMs.

Práctica:

1. Simula un incidente de seguridad en una red ficticia y sigue el proceso de detección, análisis y respuesta.
2. Utiliza herramientas como SIEM para correlacionar y analizar eventos.
3. Crea un plan de respuesta a incidentes para una empresa.
4. Realiza un análisis forense básico de una imagen de disco proporcionada, identificando indicadores de compromiso.
5. Configura Splunk o ELK Stack para monitorizar eventos en tiempo real, estableciendo alertas para actividades sospechosas.

05 Hacking Ético, Pruebas de Penetración y Vulnerabilidades

a) Introducción al Hacking Ético y Pruebas de Penetración

1. Conceptos Básicos:
   - Diferencia entre hacker ético y cibercriminal
   - Tipos de hackers: sombrero blanco, sombrero negro, sombrero gris
2. Metodologías de Prueba:
   - OWASP
   - Penetration Testing Execution Standard (PTES)

b) Reconocimiento y Escaneo

1. Técnicas de Reconocimiento:
   - Pasivo vs Activo
   - Herramientas: Shodan, Censys, theHarvester
2. Escaneo y Enumeración:
   - Nmap y Zenmap: detección de servicios y vulnerabilidades
   - DirBuster y DirSearch: búsqueda de directorios y archivos

c) Explotación y Post-Explotación

1. Vulnerabilidades Web y Explotación:
   - XSS (Cross-Site Scripting): tipos y payloads
   - SQL Injection: técnicas y herramientas (sqlmap)
   - Webshell, File Inclusion, Command Injection
2. Frameworks de Explotación:
   - Metasploit y Searchsploit: búsqueda, explotación y post-explotación
   - BeEF (Browser Exploitation Framework): explotación de navegadores
3. Pivoting y Movimiento Lateral:
   - Técnicas y herramientas: Proxychains, SSH Tunneling
   - Reconocimiento y explotación de redes internas

d) Herramientas Avanzadas y Técnicas

1. Burp Suite:
   - Funcionalidades principales
   - *Intercepting, Modifying Requests, Repeater, Sequencer*
2. Otras Herramientas:
   - Nikto: escáner de vulnerabilidades web
   - Hydra: ataque de fuerza bruta

e) Reporte y Remediación

1. Generación de Informes:
   - Elementos clave de un informe
   - Presentación a *stakeholders*
2. Estrategias de Remediación:
   - Parcheo y actualización.
   - Mitigación de vulnerabilidades web: WAF, configuraciones seguras

Práctica:

1. Realiza un reconocimiento pasivo y activo sobre un objetivo ficticio.
2. Identifica y explota vulnerabilidades en una aplicación web de prueba, como WebGoat o DVWA.
3. Usa Metasploit para explotar una vulnerabilidad conocida en un sistema controlado.
4. Realiza pruebas con Burp Suite sobre una aplicación, identificando y modificando peticiones.
5. Al final de las pruebas, redacta un informe con los hallazgos y recomendaciones de remediación.

06 Ejercicios Prácticos de Adversario y Concienciación

a) Red Team vs Blue Team

1. Dinámica de Equipos y Objetivos:
   - Definición y diferencias fundamentales
   - Cómo se complementan en ejercicios prácticos
2. Herramientas y Metodologías:
   - Herramientas específicas del Red Team: C2 (Command & Control), payloads, post-explotación
   - Herramientas específicas del Blue Team: IDS/IPS, SIEM, Hunting

b) Programas de Concienciación

1. Importancia de la Educación en Ciberseguridad:
   - Repercusiones de la falta de conciencia
   - Beneficios a corto y largo plazo
2. Diseño de Campañas:
   - Contenidos y formatos efectivos: videos, infografías, talleres
   - Medición y seguimiento: cómo evaluar la eficacia de un programa

c) Simulación de Ataques

1. Escenarios de Ataque:
   - *Phishing, Spear Phishing, Ransomware*
   - Ataques DDoS, inyecciones
2. Entornos Controlados:
   - Sandboxes y laboratorios virtuales
   - Importancia del aislamiento

d) Psicología en Ciberseguridad

1. Comportamiento Humano y Seguridad:
   - Errores comunes y sesgos cognitivos
   - Ingeniería social y manipulación
2. Cultura de Seguridad:
   - Construir una mentalidad de seguridad
   - Factores motivacionales y disuasorios

e) Técnicas OSINT (Open Source Intelligence)

1. Herramientas y Plataformas:
   - Búsquedas avanzadas en Google, Shodan
   - Recon-ng, Maltego
2. Aplicaciones y Limitaciones:
   - Beneficios en investigaciones de seguridad
   - Ética y privacidad

f) Ciberespionaje

1. Tácticas y Herramientas:
   - Keyloggers, micrófonos ocultos, *spyware*
   - Operaciones encubiertas y fuentes humanas
2. Defensas y Contramedidas:
   - Técnicas anti-espionaje
   - Herramientas de detección y eliminación

g) Estudio de APTs (Amenazas Persistentes Avanzadas)

1. Características y Metodologías:
   - Ciclo de vida y técnicas de evasión
   - Objetivos y motivaciones
2. Caso Práctico:
   - Análisis de una APT conocida
   - Medidas defensivas implementadas

Práctica:

1. Realiza una recopilación de datos OSINT sobre un objetivo ficticio y analiza un caso de estudio de APT.
2. Participa en un ejercicio de simulación de adversario (Red Team vs. Blue Team) y crea una pequeña campaña de concienciación.
3. Diseña y ejecuta un ataque simulado de phishing a un grupo de prueba, y luego analiza los resultados para mejorar la conciencia.
4. Lleva a cabo un ejercicio de Ingeniería Social, de forma ética y con consentimiento, y reflexiona sobre las vulnerabilidades humanas.

Beneficios de estudiar un diplomado con Modelo Educativo Ibaktor

Obtienes dos certificados:

- Certificado Internacional digital de alta seguridad y encriptación, con examen de certificación, incluido en el costo de tu diplomado.
- Certificado DC-3 de la STPS.

Temas actualizados y de vanguardia:
Con gran capacidad de actualización y reinvención al ser de una duración más corta que otros posgrados, un diplomado te ofrece una capacitación enfocada en temas relevantes y de alta demanda para el mercado laboral.

Capitaliza lo aprendido:
El alto enfoque práctico y estratégico de un Diplomado hace que cada módulo sea aplicable desde el primer día 1 en tus actividades profesionales y desarrollo personal.

Mejora tus oportunidades laborales:
Enriquece tu CV especializándote y posiciónate como el mejor candidato.

Networking:
No solo compartirás salón de clases con buenos compañeros, también con excelentes profesionistas con los que podrás intercambiar puntos de vista, *tips* y oportunidades de negocio.

Profesores con más 15 años en experiencia profesional:
Toma clases de la mano de expertos en su disciplina con amplia experiencia compartiendo su conocimiento y trabajando en las mejores empresas nacionales e internacionales.

Duración:
La duración del diplomado es de 6 meses, así podrás aplicar lo aprendido muy rápidamente y seguir creciendo profesionalmente.

Diploma:
Todos nuestros Diplomados y Certificaciones tienen validez curricular.

Beneficios del Modelo Educativo Ibaktor

Clases pregrabadas y en vivo:
Estudia a tu ritmo, con material de gran calidad, puedes consultar todas las sesiones en el horario que más te convenga. Todas las clases en vivo se graban para tu comodidad.

Experiencias de aprendizaje *online*:
Foros.
Juegos.
Ejercicio y herramientas para aplicarlas en tu trabajo o proyectos.
Casos prácticos.
Acceso a materiales complementarios.

Contenido siempre disponible:
Podrás consultar y descargar el material desde la plataforma en cualquier momento del día, durante todo el tiempo que dure tu diplomado.
Además, nuestra plataforma es multidispositivo, así podrás estudiar en cualquier computadora de escritorio, *laptop*, tableta o *smartphone*.

Soporte técnico:
El equipo de soporte técnico estará a tu disposición en todo momento para ayudarte a resolver cualquier situación.

Chatbot:
Mediante el cual te podemos apoyar en todos los temas relacionados con tu experiencia en el diplomado y generamos *tickets* de servicio para tu comodidad, tranquilidad y seguridad.

Asesoría y acompañamiento:
Cuentas con Seguimiento Académico a través de *Whatsapp* y otras herramientas a distancia en tiempo real, para resolver tus dudas y dar retroalimentación.

Evaluación y seguimiento ágil:
Tendrás retroalimentación fluida y objetiva de tu progreso en el programa para el logro de tu certificado internacional.

UVM / EDUCACIÓN CONTINUA