UVM GO! FORWARD

BOOTCAMP EN CIBERDEFENSA Y CIBERSEGURIDAD

Híbrido

(224 horas)

Objetivo:

Adquirir conocimientos y competencias ejecutar diagnósticos de protección en sistemas de seguridad informática para las empresas.

Dirigido a:

Profesionales en tecnología o abierto a público en general que esté interesado en cambiar de carrera hacia un enfoque de la protección de sistemas de seguridad informática para las empresas.

Reconocimiento:

Al finalizar tu programa recibirás:

- **Diploma Digital UVM con validez curricular y tecnología Blockchain con código QR y de verificación.**
- **Certificado Internacional de Embiz Foundation.**
- **Certificado de competencias laborales DC-3 de la STPS.**

UVM GO! FORWARD

¿Por qué UVM?

60 años de experiencia académica, más de 150 programas educativos y más de 180 programas de excelencia a nivel nacional.

Adquieres conocimientos y habilidades esenciales aplicables de manera inmediata a tu actividad profesional.

Los profesores que imparten las Certificaciones y Diplomados siguen un modelo de enseñanza con ejemplos reales, pues cada uno de ellos es experto y reconocido en su campo.

Flexibilidad educativa que te permite estudiara tu ritmo, a cualquier hora y en cualquier lugar.

Los Diplomados y Certificaciones de UVM enriquecen tu CV y te posiciónan como el mejor candidato.

MÓDULOS

01 Fundamentos de la Ciberdefensa y Ciberseguridad

1. Conceptos Básicos
   a. Definición de Ciberseguridad:
      i. Origen y evolución histórica.
      ii. Importancia en el mundo actual.
   b. Principios de la Ciberseguridad:
      i. Confidencialidad, Integridad y Disponibilidad (Triada CIA).
      ii. Autenticidad, No repudio y Responsabilidad.
2. Gobernanza, Riesgo y Cumplimiento
   a. Gobernanza de la Ciberseguridad:
      i. Estructuras organizativas.
      ii. Políticas, normas y procedimientos.
   b. Análisis y Mitigación del Riesgo:
      i. Evaluación del riesgo.
      ii. Estrategias de mitigación.
      iii. Modelos de madurez de ciberseguridad.
   c. Cumplimiento Normativo:
      i. Regulaciones y estándares: GDPR, ISO 27001, NIST.
      ii. Auditorías y controles.
3. Planificación de la Continuidad del Negocio
   a. Business Continuity Planning (BCP):
      i. Elementos clave del BCP.
      ii. Desarrollo y pruebas del BCP.
   b. Disaster Recovery (DR):
      i. Diferencias entre BCP y DR.
      ii. Estrategias de DR: backups, sitios de recuperación, redundancia.
4. Infraestructura y Seguridad en Sistemas Operativos
   a. Configuración Segura:
      i. Linux: hardening, permisos, SELinux/AppArmor.
      ii. Windows: políticas de grupo, configuración del Active Directory, Kerberos.
   b. Tareas y Automatización:
      i. Uso de tar, cron y cronjobs en Linux.
      ii. Programación y scripting con Bash para tareas de seguridad.
   c. Monitorización y Logging:
      i. Syslog en Linux, Event Viewer en Windows.
      ii. Importancia del logging para la detección de amenazas.
5. Desafíos Actuales y Tendencias en Ciberseguridad
   a. Amenazas emergentes:
      i. Malware avanzado, ransomware, APTs.
      ii. Desafíos de IoT y dispositivos conectados.
   b. Soluciones y tendencias:
      i. Inteligencia contra amenazas.
      ii. 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.

1. Configuración y Hardening de Sistemas Operativos
   a. Configuración de Linux:
      i. Instalación y configuración inicial.
      ii. Servicios esenciales y demonios.
      iii. Gestión de usuarios y grupos.
      iv. Uso y configuración de sudo.
   b. Configuración de Windows:
      i. Instalación y roles de Windows Server.
      ii. Gestión de usuarios y grupos.
      iii. Políticas de grupo (GPOs).
      iv. Servicios y características de Windows.
   c. Hardening de sistemas:
      i. Principios del hardening.
      ii. Herramientas para auditoría y hardening (ej. Lynis para Linux, Security Compliance Toolkit para Windows).
      iii. Limitación de servicios y puertos abiertos.
      iv. Actualizaciones y parches.
2. Automatización y Tareas Programadas
   a. Tar, Cron, Cronjobs:
      i. Uso de tar para la gestión de archivos.
      ii. Programación de tareas con cron.
      iii. Creación y gestión de cronjobs.
   b. Automatización en Windows:
      i. Programador de tareas.
      ii. Uso de PowerShell para la automatización.
3. Logging y Monitorización
   a. Gestión de registros en Linux:
      i. Herramientas de registro (ej. syslog, rsyslog).
      ii. Rotación y retención de logs.
   b. Gestión de registros en Windows:
      i. Visor de Eventos.
      ii. Políticas de auditoría.
   c. Centralización de logs:
      i. Introducción a soluciones como ELK Stack (Elasticsearch, Logstash, Kibana).
      ii. Configuración y envío de logs a sistemas centralizados.
4. Scripting y Automatización Avanzada
   a. Bash Scripting:
      i. Conceptos básicos y estructuras de control.
      ii. Uso de scripts para tareas de administración.
   b. PowerShell en Windows:
      i. Conceptos básicos.
      ii. Automatización y administración con PowerShell.
5. Administración de Directorio Activo y Autenticación
   a. Introducción al Active Directory:
      i. Estructura y componentes (Dominio, OUs, DC).
      ii. Gestión de usuarios y políticas.
   b. Kerberos:
      i. Fundamentos y arquitectura.
      ii. Autenticación y tickets.
      iii. Problemas comunes y soluciones.

Práctica:

1. Configura y protege un servidor Linux y Windows de acuerdo a 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 PowerShe 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

1. Arquitectura y Diseño de Redes
   a. Fundamentos de Redes:
      i. Modelos OSI y TCP/IP.
      ii. Dispositivos de red: routers, switches, firewalls.
      iii. Subnetting y VLSM.
   b. Diseño de Red Seguro:
      i. Zonas desmilitarizadas (DMZ).
      ii. Segmentación de redes.
      iii. Diseños de alta disponibilidad.
2. Operaciones de Red y Seguridad
   a. Operación de Redes y Monitoreo:
      i. Protocolos comunes: DHCP, DNS, HTTP/HTTPS.
      ii. Herramientas de monitoreo: SNMP, NetFlow.
   b. Port Scanning y Reconocimiento:
      i. Herramientas como Nmap y Zenmap.
      ii. Técnicas de evasión y reconocimiento.
   c. Defensa y Mitigación:
      i. IDS/IPS.
      ii. Firewalls: de red, de aplicación.
      iii. Prevención de ARP spoofing y otros ataques de red.
3. Análisis de Tráfico y Herramientas
   a. Introducción a Wireshark:
      i. Funciones básicas y avanzadas.
      ii. Filtrado y análisis de paquetes.
   b. Detección de Anomalías:
      i. Patrones de tráfico sospechoso.
      ii. Signaturas de malware y exfiltración de datos.
4. Comunicación Segura y Protección de Datos
   a. Email Security:
      i. SPF, DKIM, DMARC.
      ii. Prevención de phishing y amenazas avanzadas.
   b. Wireless Security:
      i. Configuración y protección de redes Wi-Fi.
      ii. WPA3 y técnicas de hardening.
   c. Cryptography y Encryption:
      i. Conceptos de cifrado simétrico y asimétrico.
      ii. Certificados y PKI.
      iii. Protocolos seguros: SSL/TLS, SSH.
5. Seguridad en Cloud y Virtualización
   a. Fundamentos del Cloud Computing:
      i. Modelos de servicio: IaaS, PaaS, SaaS.
      ii. Proveedores principales: AWS, Azure, Google Cloud.
   b. Configuración y Hardening en la Nube:
      i. Controles de acceso.
      ii. Gestión de identidades (IAM).
      iii. Protección de datos: almacenamiento cifrado, backups.
   c. Virtualización y Contenedores:
      i. Conceptos básicos de virtualización.
      ii. Seguridad en entornos VMware, Hyper-V.
      iii. 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 (cualquier otro proveedor de cloud) y aplica medidas de seguridad, incluyendo la protección de instancias y almacenamiento.

MÓDULOS

04 Respuesta a Incidentes, Forense y Monitoreo

1. Conceptos Básicos de Respuesta a Incidentes
   a. Introducción a la Respuesta a Incidentes:
      i. Definición de incidente.
      ii. Ciclo de vida del manejo de incidentes.
   b. Equipos de Respuesta a Incidentes (CERT/CSIRT):
      i. Roles y responsabilidades.
      ii. Creación y operación de un CSIRT.
2. Preparación y Detección de Incidentes
   a. Planificación de Respuesta a Incidentes:
      i. Creación de un plan de respuesta.
      ii. Herramientas y recursos esenciales.
   b. Detección de Incidentes:
      i. Señales y alertas.
      ii. Herramientas de detección: IDS, IPS, SIEM.
3. Gestión y Mitigación de Incidentes
   a. Análisis y Valoración:
      i. Triage de incidentes.
      ii. Herramientas de análisis y correlación.
   b. Contención y Erradicación:
      i. Estrategias de contención a corto y largo plazo.
      ii. Eliminación de amenazas y restauración.
4. Forense Digital y Análisis Post-Incidente
   a. Introducción a la Forense Digital:
      i. Principios y metodologías.
      ii. Cadena de custodia.
   b. Extracción y Análisis de Evidencia:
      i. Imagenes de discos y memoria.
      ii. Herramientas de análisis: Autopsy, FTK, Volatility.
   c. Data Recovery:
      i. Principios de recuperación de datos.
      ii. Herramientas y técnicas.
5. Monitoreo Proactivo y Herramientas
   a. Introducción a Splunk:
      i. Funcionalidades principales.
      ii. Creación de dashboards y alertas.
   b. Otras soluciones de Monitoreo y Logging:
      i. ELK Stack.
      ii. Graylog.
   c. Integración y Correlación de Eventos:
      i. Técnicas para identificar patrones.
      ii. 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.

MÓDULOS

05 Hacking Ético, Pruebas de Penetración y Vulnerabilidades

1. Introducción al Hacking Ético y Pruebas de Penetración
   a. Conceptos Básicos:
      i. Diferencia entre hacker ético y cibercriminal.
      ii. Tipos de hackers: sombrero blanco, sombrero negro, sombrero gris.
   b. Metodologías de Prueba:
      i. OWASP.
      ii. Penetration Testing Execution Standard (PTES).
2. Reconocimiento y Escaneo
   a. Técnicas de Reconocimiento:
      i. Pasivo vs Activo.
      ii. Herramientas: Shodan, Censys, theHarvester.
   b. Escaneo y Enumeración:
      i. Nmap y Zenmap: detección de servicios y vulnerabilidades.
      ii. DirBuster y DirSearch: búsqueda de directorios y archivos.
3. Explotación y Post-Explotación
   a. Vulnerabilidades Web y Explotación:
      i. XSS (Cross-Site Scripting): tipos y payloads.
      ii. SQL Injection: técnicas y herramientas (sqlmap).
      iii. Webshell, File inclusion, Command injection.
   b. Frameworks de Explotación:
      i. Metasploit y Searchsploit: búsqueda, explotación y post-explotación.
      ii. BeEF (Browser Exploitation Framework): explotación de navegadores.
   c. Pivoting y Movimiento Lateral:
      i. Técnicas y herramientas: Proxychains, SSH tunneling.
      ii. Reconocimiento y explotación de redes internas.
4. Herramientas Avanzadas y Técnicas
   a. Burp Suite:
      i. Funcionalidades principales.
      ii. Intercepting, modifying requests, repeater, sequencer.
   b. Otras Herramientas:
      i. Nikto: escáner de vulnerabilidades web.
      ii. Hydra: ataque de fuerza bruta.
5. Reporte y Remediación
   a. Generación de Informes:
      i. Elementos clave de un informe.
      ii. Presentación a stakeholders.
   b. Estrategias de Remediación:
      i. Parcheo y actualización.
      ii. 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.

1. Red Team vs Blue Team
   a. Dinámica de Equipos y Objetivos:
      i. Definición y diferencias fundamentales.
      ii. Cómo se complementan en ejercicios prácticos.
   b. Herramientas y Metodologías:
      i. Herramientas específicas del Red Team: C2 (Command & Control), payloads, post-explotación.
      ii. Herramientas específicas del Blue Team: IDS/IPS, SIEM, Hunting.
2. Programas de Concienciación
   a. Importancia de la Educación en Ciberseguridad:
      i. Repercusiones de la falta de conciencia.
      ii. Beneficios a corto y largo plazo.
   b. Diseño de Campañas:
      i. Contenidos y formatos efectivos: videos, infografías, talleres.
      ii. Medición y seguimiento: cómo evaluar la eficacia de un programa.
3. Simulación de Ataques
   a. Escenarios de Ataque:
      i. Phishing, spear phishing, ransomware.
      ii. Ataques DDoS, inyecciones.
   b. Entornos Controlados:
      i. Sandboxes y laboratorios virtuales.
      ii. Importancia del aislamiento.
4. Psicología en Ciberseguridad
   a. Comportamiento Humano y Seguridad:
      i. Errores comunes y sesgos cognitivos.
      ii. Ingeniería social y manipulación.
   b. Cultura de Seguridad:
      i. Construir una mentalidad de seguridad.
      ii. Factores motivacionales y disuasorios.
5. Técnicas OSINT (Open Source Intelligence)
   a. Herramientas y Plataformas:
      i. Búsquedas avanzadas en Google, Shodan.
      ii. Recon-ng, Maltego.
   b. Aplicaciones y Limitaciones:
      i. Beneficios en investigaciones de seguridad.
      ii. Ética y privacidad.
6. Ciberespionaje
   a. Tácticas y Herramientas:
      i. Keyloggers, micrófonos ocultos, spyware.
      ii. Operaciones encubiertas y fuentes humanas.
   b. Defensas y Contramedidas:
      i. Técnicas anti-espionaje.
      ii. Herramientas de detección y eliminación.
7. Estudio de APTs (Amenazas Persistentes Avanzadas)
   a. Características y Metodologías:
      i. Ciclo de vida y técnicas de evasión.
      ii. Objetivos y motivaciones.
   b. Caso Práctico:
      i. Análisis de una APT conocida.
      ii. Medidas defensivas implementadas.

Prácticas:

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.

07 Proyecto Final.

Beneficios de la modalidad

Clases en vivo, actividades interactivas y casos prácticos. Puedes interactuar con profesores y otros alumnos para tener una experiencia más enriquecedora.

Networking. Tienes la oportunidad de construir una red de contactos profesionales con otras personas que tienen intereses similares o se desempeñan en el mismo ámbito.

Estudia a tu ritmo. Consulta todas las sesiones grabadas en el horario que más te convenga.

*Aplica lo que aprendas de forma inmediata.

Nota: Si no asistes a las sesiones en vivo con el profesor en las fechas y horarios establecidos, tendrás 30 días naturales para ver completa la grabación de la clase en Teams® y realizar la actividad asignada para que acredites el módulo.

UVM GO! FORWARD

SÉ PARTE DE LA UVM

@uvmmx uvm @uvmmx uvm.mx