DIPLOMADO EN CIBERSEGURIDAD

MÓDULO 1

“FUNDAMENTOS DE CIBERSEGURIDAD, ANÁLISIS Y GESTIÓN DE VULNERABILIDADES”

1. Definición de Ciberseguridad.
2. Historia y evolución de la ciberseguridad.
3. Componentes de la ciberseguridad: confidencialidad, integridad y disponibilidad (CIA).
4. Desafíos actuales en el panorama de ciberseguridad.
5. Malware: virus, gusanos, troyanos, ransomware.
6. Ataques de ingeniería social: phishing, vishing, spear phishing.
7. Amenazas internas y el concepto de insider threat.
8. Amenazas avanzadas persistentes (APT).
9. Identificación de vulnerabilidades: escaneo y auditoría.
10. Herramientas de análisis de vulnerabilidades (Nessus, OpenVAS, etc.).
11. Proceso de evaluación de riesgos y mitigación.
12. Gestión de parches y actualizaciones.
13. Planes de respuesta ante incidentes.
14. Detección y monitorización: SIEM y SOC.
15. Prevención frente a ataques: firewalls, IPS, y sistemas de detección.
16. Ciberseguridad en la nube.

Duración: 40 horas.

MÓDULO 2

“ÉTICA EN CIBERSEGURIDAD Y PENSAMIENTO CREATIVO”

1. Definición de ética y su relevancia en ciberseguridad.
2. Principios éticos en el ámbito de la ciberseguridad.
3. El dilema ético de la defensa frente a los atacantes.
4. Legislación internacional: GDPR, CCPA, Leyes de protección de datos.
5. Cumplimiento de normativas: ISO 27001, NIST.
6. Impacto de los incidentes de seguridad en la reputación y la ley.
7. El concepto de hacking ético y las diferencias con los ataques maliciosos.
8. Principios de trabajo en un entorno ético de pruebas de penetración.
9. El Código de Conducta Profesional en ciberseguridad.
10. La importancia del pensamiento creativo en la solución de problemas.
11. Técnicas de creatividad: mapas mentales, pensamiento lateral, brainstorming.
12. Aplicación del pensamiento creativo en la identificación de vulnerabilidades y ataques.

Duración: 24 horas.

MÓDULO 3

“VULNERABILIDADES DEL ECOSISTEMA WEB”

1. Arquitectura básica de aplicaciones web.
2. Importancia de la seguridad en el ecosistema web.
3. Principales tipos de vulnerabilidades en aplicaciones web.
4. Inyección SQL.
5. Cross-Site Scripting (XSS).
6. Cross-Site Request Forgery (CSRF).
7. Falsificación de solicitudes entre sitios (SSRF).
8. Configuración incorrecta de seguridad.
9. Explotación de XSS y ataques de scripting.
10. Inyección de comandos y SQLi.
11. Técnicas de robo de sesiones y cookies.
12. Escalado de privilegios en aplicaciones web.
13. Herramientas de seguridad en el desarrollo web (OWASP ZAP,
14. Burp Suite).
15. Buenas prácticas de codificación segura.
16. Autenticación fuerte y control de acceso.
17. Monitorización continua de aplicaciones web.

Duración: 24 horas.

MÓDULO 4

“FUNDAMENTOS Y HERRAMIENTAS DEL OPEN SOURCE INTELLIGENCE”

1. Definición de OSINT y su importancia en la ciberseguridad.
2. Fuentes de información abiertas: motores de búsqueda, redes sociales, bases de datos públicas.
3. Aspectos éticos y legales del uso de OSINT.
4. Técnicas de búsqueda avanzada en Google (Google Dorks).
5. Recolecta de datos de redes sociales y foros.
6. Herramientas básicas de OSINT: Maltego, Shodan, TheHarvester.
7. Análisis de información y validación de fuentes.
8. Investigaciones sobre actores de amenazas.
9. Mapeo de infraestructura y recopilación de datos de objetivos.
10. Monitoreo de amenazas y análisis de tendencias.
11. OSINT en la prevención de fraudes y ataques de phishing.

Duración: 32 horas.

MÓDULO 5

“PRUEBAS DE PENETRACIÓN SOBRE REDES CORPORATIVAS”

1. Definición y objetivos de las pruebas de penetración.
2. Tipos de pruebas de penetración: caja negra, caja gris y caja blanca.
3. Metodologías comunes: OWASP, PTES, NIST.
4. Escaneo de puertos y servicios.
5. Identificación de sistemas operativos y dispositivos en la red.
6. Análisis de puntos de entrada a la red corporativa.
7. Explotación de vulnerabilidades de servicios y sistemas operativos.
8. Ataques a protocolos de red (SMB, FTP, HTTP, etc.).
9. Elevación de privilegios y acceso no autorizado.
10. Técnicas de post-explotación: pivoteo, recolección de credenciales.
11. Exfiltración de datos y técnicas para evitar la detección.
12. Análisis de impacto y generación de reportes.
13. Estrategias de mitigación de vulnerabilidades encontradas.
14. Herramientas de remediación y defensa (IDS, firewalls, segmentación de red).
15. La importancia de los parches y actualizaciones.

Duración: 32 horas.

MÓDULO 6

“TALLER DE TÉCNICAS DE PENTRACIÓN OFENSIVA Y SEGURIDAD”

1. Revisión de herramientas necesarias: Kali Linux, Metasploit, Burp Suite.
2. Configuración de entornos de laboratorio: máquinas virtuales y redes simuladas.
3. Consideraciones éticas y legales en pruebas de penetración.
4. Ejercicios prácticos de escaneo de red y descubrimiento de activos.
5. Técnicas de OSINT en el ámbito ofensivo.
6. Mapeo de servicios y vulnerabilidades.
7. Explotación de vulnerabilidades comunes en redes y sistemas.
8. Técnicas de inyección y explotación remota.
9. Acceso a sistemas internos y escalada de privilegios.
10. Ejercicios prácticos de movimientos laterales dentro de la red.
11. Exfiltración de datos y evasión de detección.
12. Simulación de ataques avanzados (APT).
13. Redacción de informes técnicos y ejecutivos.
14. Presentación de hallazgos y recomendaciones de seguridad.
15. Mejores prácticas para fortalecer la infraestructura de seguridad.

Duración: 40 horas.