PUNTO Com
Informática y Capacitación Técnica

CIBERSEGUIRIDAD

TEMARIO DETALLADO

Módulo 1: Fundamentos de la Ciberseguridad

Introducción a la ciberseguridad y su importancia. Amenazas cibernéticas y actores involucrados. Conceptos básicos de seguridad de la información. Políticas de seguridad y buenas prácticas. Ética y responsabilidad en ciberseguridad. Aspectos legales y regulaciones relevantes. Criptografía vs Cifrado. Autenticación, autorización y gestión de contraseñas seguras. Seguridad en redes y sistemas operativos. Seguridad en aplicaciones web.

Módulo 2: Google y Bing Dorks

Introducción a Google y Bing Dorks. Explicación de qué son los Google Dorks y Bing Dorks. Objetivos y aplicaciones de estas técnicas en ciberseguridad.
Ejemplos de búsquedas avanzadas con operadores específicos. Búsqueda de Información Sensible y Vulnerabilidades. Uso de operadores avanzados en Google y Bing para buscar información sensible. Identificación de vulnerabilidades en sitios web utilizando Dorks. Prácticas seguras y éticas al utilizar Dorks. Ejercicios prácticos de búsqueda de información y vulnerabilidades.

Módulo 3: Preparación de Escenarios Controlados

Creación de entornos controlados para pruebas. Configuración de laboratorios virtuales. Instalación de herramientas de seguridad. Escaneo de puertos y servicios en un entorno controlado. Identificación de sistemas y servicios vulnerables. Prácticas seguras en la preparación de entornos.
Desarrollo de escenarios de ataque. Configuración de sistemas víctimas.
Pruebas de intrusión en entornos controlados. Tipos de pruebas de penetración.

Módulo 4: Búsqueda de Información.

Recopilación y análisis de información. Footprinting y enumeración de objetivos. Uso de fuentes de información públicas y técnicas de búsqueda. Enumeración de recursos y servicios. Búsqueda y recopilación de datos de dominio público. Uso de herramientas y técnicas de OSINT (Open Source Intelligence). Enumeración de redes y sistemas. Escaneo de puertos y servicios en la web. Identificación de vulnerabilidades. Pruebas de enumeración y obtención de información. Respeto de límites éticos en la recopilación de datos. Reportes de hallazgos. ón de la comunidad. Estrategias de crecimiento. Que son los catálogos.

Módulo 5: Identificación de Vulnerabilidades.

Conceptos clave sobre vulnerabilidades. Clasificación de vulnerabilidades y sus riesgos. Herramientas de escaneo y detección de vulnerabilidades. Escaneo y evaluación de vulnerabilidades en aplicaciones web. Identificación de vulnerabilidades comunes. Pruebas en laboratorios virtuales. Identificación de vulnerabilidades en sistemas y redes. Evaluación de configuraciones inseguras. Análisis de logs y registros de eventos. Pruebas de identificación de vulnerabilidades. Documentación y clasificación de hallazgos. Mitigación de vulnerabilidades y parcheo.

Módulo 6: Explotación de Vulnerabilidades

Introducción a la explotación de vulnerabilidades. Uso de exploits y herramientas de penetración. Desarrollo de scripts de explotación. Explotación de vulnerabilidades en servicios web. Ataques a aplicaciones web y servidores. Uso de técnicas avanzadas de explotación. Explotación de vulnerabilidades en sistemas y redes. Pruebas de intrusión y explotación en entornos controlados. Medidas de mitigación y protección. Ética y responsabilidad en la explotación de vulnerabilidades. Análisis ético de los resultados. Presentación de proyectos prácticos de explotación.

Módulo 7: Reportes

Importancia de los reportes en ciberseguridad. Estructura de un informe de seguridad. Documentación de hallazgos y evidencia.
Test de Evaluación Final

Querés inscribirte o buscás más información?

Paysandú: José P. Varela 806 - Tel: 472 31837
Sucursal Zona Norte: Zorrilla esq. Éxodo - Tel:472 47345
Salto: Sarandí 56 - Tel: 473 30650 - Cel. 092 002 003
Tacuarembó: Rivera 268 - Tel: 463 42376

Seguínos en:
092 002 003
puntocomuy
Instituto PuntoCom

PUNTO Com
Informática y Capacitación Técnica
www.puntocom.edu.uy