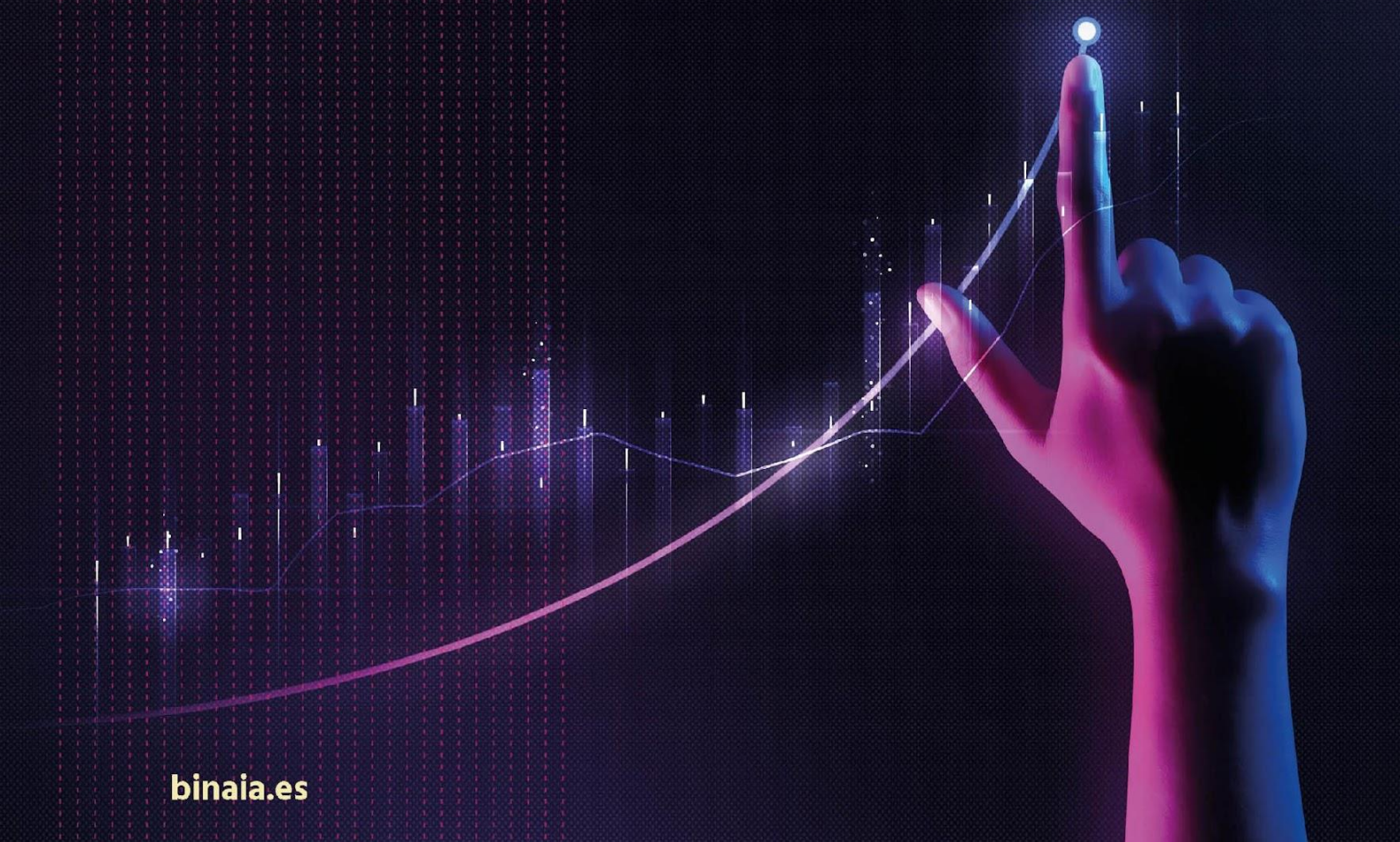
BINAIA

BCIT in **Cybersecurity**



binaia.es

Objetivos

El objetivo general de la formación consiste en preparar a los alumnos de forma intensiva en el área de la Ciberseguridad, conociendo los diferentes conceptos y herramientas más usadas en esta área.

En concreto, los objetivos específicos de la formación son:

- Conocer conceptos básicos y avanzados del área de Ciberseguridad
- Conocer conceptos y herramientas relacionadas con redes
- Conocer conceptos y herramientas de Hacking y Hacking Ético
- Aprender sobre Análisis de Vulnerabilidades
- Aprender sobre diferentes tipos de Hacking
- Aprender sobre Criptografía

Requisitos

Es necesario tener conocimientos en ciertos lenguajes de programación y scripting, servicios y sistemas, infraestructura web y seguridad informática.

Metodología

En esta formación, el aprendizaje se llevará a cabo de una forma dinámica con una enseñanza teórica y práctica compaginando ambas mediante la realización de ejercicios que permitan hacer uso de todo lo aprendido buscando asentar el conocimiento.

Programa

El programa se estructura en los bloques que se describen a continuación:

Bloque 1: Introducción al Hacking Ético

- Seguridad de la Información
- Seguridad de la Información, Seguridad Informática y Ciberseguridad
- Ataques a la Seguridad de la Información
- Cyber Kill Chain, MITRE ATT&CK, Unified CKC
- Indicadores de Compromiso (IoCs)
- Hacking
- Hacking Ético
- Controles de Seguridad de la Información
- Leyes y normas de Seguridad de la Información
- Ciberderecho en diferentes países

Bloque 2: Footprinting y Reconocimiento

- Footprinting
- Metodología Footprinting
- Footprinting a través de los motores de búsqueda
- Footprinting a través de los servicios web
- Footprinting a través de las redes sociales
- Footprinting de sitios web
- Footprinting por correo electrónico
- Footprinting Whois
- Footprinting de DNS
- Footprinting de redes
- Footprinting a través de la ingeniería social
- Herramientas de footprinting
- Contramedidas del footprinting

Bloque 3: Redes de Exploración

- Flags TCP
- Comunicación TCP/IP

- Herramientas de escaneo
- Descubrimiento de host
- Descubrimiento de puertos y servicios
- Técnicas de escaneo de puertos
- Descubrimiento de la versión del servicio
- Contramedidas de escaneo de puertos
- Detección de Sistema Operativo (*Banner Grabbing/OS Fingerprinting*)
- Contramedidas contra la captura de Banners
- Técnicas de evasión de IDS/Firewalls
- Suplantación de direcciones IP
- Contramedidas de falsificación de IP
- Anonimizadores
- Dibujar diagramas de red

Bloque 4: Enumeración

- ¿Qué es la enumeración?
- Técnicas de enumeración
- Servicios y puertos
- Enumeración de NetBIOS
- Enumeración SNMP
- Enumeración LDAP
- Enumeración NTP
- NFS Enumeratio
- Enumeración SMTP
- Enumeración DNS usando transferencia de zona
- DNSSEC Zone Walking
- Enumeración Ipsec (Internet Protocol Security)
- Enumeración VoIP
- Enumeración RPC
- Enumeración de usuarios de Unix/Linux
- Enumeración Telnet
- Enumeración SMB
- Enumeración FTP
- Enumeración TFTP
- Enumeración IPv6
- BGP Enumeration
- Contramedidas para la enumeración

Bloque 5: Análisis de Vulnerabilidad

- Búsqueda de Vulnerabilidades (Vulnerability research)
- Análisis de Vulnerabilidades (Vulnerability Assesment)
- Sistemas de Clasificación y Bases de Datos de Vulnerabilidades
- Common Vulnerability Scoring System (CVSS)
- Common Vulnerabilies and Exposures (CVE)
- National Vulnerability Database (NVD)
- Common Weakness Enumeration (CWE)
- Ciclo de Vida en la Gestión de Vulnerabilidades
- Fase de Pre-Análisis
- Fase de Análisis de Vulnerabilidades
- Fase de Post-Análisis de Vulnerabilidades
- Clasificación de Vulnerabilidades
- Tipos de Análisis de Vulnerabilidades
- Enfoques del Análisis de Vulnerabilidades
- Características de una buena Solución de Análisis de Vulnerabilidades
- Tipos de Herramientas de Análisis de Vulnerabilidades
- Informes de Análisis de Vulnerabilidades

Bloque 6: Hackeo de Sistemas

- Conceptos
- Hacking Methodology CEH (CHM)
- Objetivos del System Hacking
- Descifrado de contraseñas
- LLMNR/NBT-NS Poisoning
- Explotación de Vulnerabilidades
- Páginas web de exploits
- Buffer Overflow
- Escalada de privilegios
- Mantenimiento del acceso
- Esconder ficheros
- Flujo de datos NTFS
- Esteganografía
- Limpiar logs/registros

Bloque 7: Amenazas Malware

- Diferentes formas de entrar al sistema
- Técnicas comunes para la distribución de Malware en la Web
- Componentes del Malware
- ¿Qúe es el APT (Advanced Persistent Threaths)?
- ¿Qué es un Troyano?
- Introducción a los Virus
- Gusanos Informáticos
- Fileless Malware
- Análisis de Malware
- Métodos de Detección de Virus

Bloque 8: Sniffing

En este bloque se llevará a cabo una especialización en una de las siguientes herramientas:

- AWS
- Databricks
- ELK
- Snowflake
- Terraform

Bloque 9: Ingeniería Social

- ¿Qué es la Ingeniería Social?
- Fases de un ataque de Ingeniería Social
- Técnicas de Ingeniería Social
- Ingeniería Social basada en humanos
- Ingeniería Social basada en ordenadores
- Ingeniería Social basada en móviles
- Robo de Identidad
- Contramedidas
- Objetivos comunes de la Ingeniería Social y estrategias de defensa

Bloque 10: Denegación de Servicios

- Qué es un Ataque DoS

- Qué es un ataque DDoS
- Categorías básicas de Vectores de Ataque DoS/DDoS
- Sindicatos de Crimen Organizado
- Botnets
- Métodos de escaneo
- Herramientas de Ataques DoS/DDoS
- Técnicas de Detección
- Estrategias de Contramedida
- Protección a nivel de ISP

Bloque 11: Secuestro de Sesión

- ¿Qué es Secuestro de Sesión?
- Proceso de Secuestro de Sesión
- Tipos de Secuestro de sesión
- Herramientas para el Secuestro de Sesión
- Contramedidas

Bloque 12: Evadir IDS, Firewalls y Honeypots

- Conceptos de IDS, IPS, Firewall y Honeypots
- Soluciones IDS, IPS, Firewall y Honeypots
- Diferentes técnicas de Bypass IDS
- Diferentes técnicas de Bypass Firewalls
- Herramientas de evasión IDS/Firewall
- Diferentes técnicas para detectar Honeypots
- Contramedidas

Bloque 13: Hacking de Servidores Web

- Conceptos de Servidor Web
- Ataques de Servidor Web
- Metodología de Ataque de Servidor web
- Herramientas de Ataque de servidor Web
- Contramedidas de Ataque de Servidor web
- Conceptos de Gestión de Parches
- Herramientas de Seguridad de Servidor Web

Bloque 14: Hacking de Aplicaciones Web

- Conceptos de Aplicación Web
- Amenazas de Aplicación Web
- Metodología de Hacking de Aplicaciones Web
- Herramientas de Hacking de Aplicaciones Web
- Conceptos de Web APIs, Webhooks y Web Shells
- Contramedidas
- Herramientas de Seguridad de Aplicaciones Web

Bloque 15: Inyección SQL

- Conceptos de Inyección SQL
- Ataques de Inyección SQL
- Metodología de Inyección SQL
- Herramientas de Inyección SQL
- Contramedidas

Bloque 16: Hacking de Redes Inalámbricas

- Conceptos de Redes Inalámbricas
- Algoritmos de Redes Inalámbricas cifradas
- Amenazas de Redes Inalámbricas
- Metodología de Hacking de Redes Inalámbricas
- Herramientas de Hacking de Redes Inalámbricas
- Contramedidas

Bloque 17: Hacking de Plataformas Móviles

- Vectores de Ataque de Plataformas Móviles
- Hacking Android
- Hacking iOS
- Herramientas de Seguridad Móvil

Bloque 18: Hacking IoT

- Conceptos IoT
- Herramientas de Hacking IoT
- Contramedidas de Hacking IoT
- Conceptos OT
- Herramientas de Hacking OT
- Contramedidas de Hacking OT

Bloque 19: Cloud Computing

- Conceptos de Cloud Computing
- Amenazas de Cloud Computing
- Hacking Cloud
- Seguridad Cloud Computing

Bloque 20: Criptografía

- Conceptos de Criptografía
- Acceso gubernamental a claves (GAK)
- Algoritmos de Cifrado
- Funciones de resumen de mensajes
- Otras técnicas de Cifrado
- Herramientas de Criptografía
- Infraestructura de clave pública (PKI)
- Conjuntos de herramientas criptográficas
- Criptoanálisis
- Ataques criptográficos
- Herramientas de criptoanálisis