SCORPION
CYBERTECH

Módulos de Ciberseguridad

Scorpion Cybertechnologies® S.L.
CIF: B75987222

Entidad inscrita en el Registro
Estatal de Entidades de Formación

Fundación Estatal
PARA LA FORMACIÓN EN EL EMPLEO

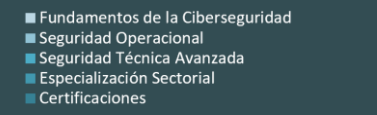
Versión 1.2

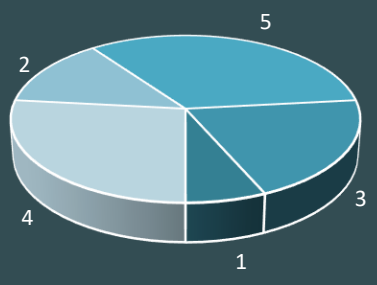
SCORPION
CYBERTECH

Resumen

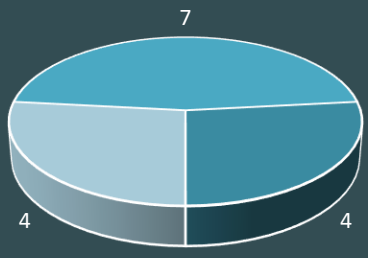
15 Módulos

5 Categorías

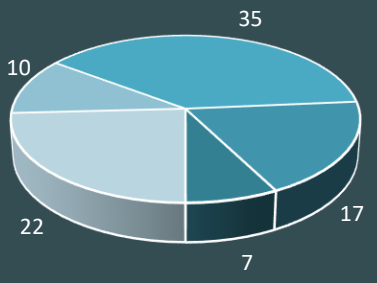


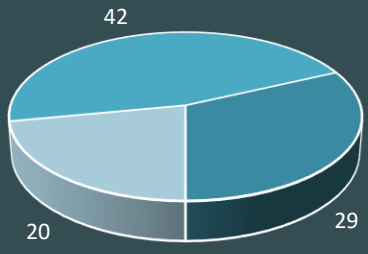


3 Niveles

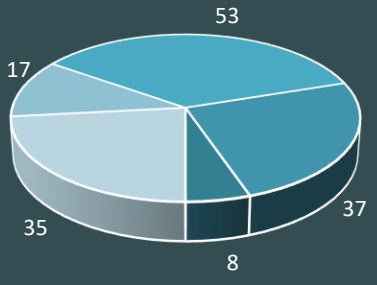


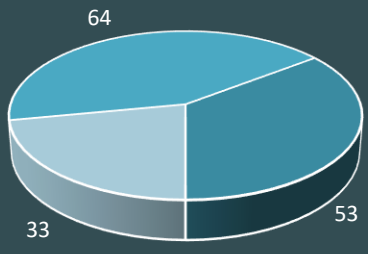
+90h Teoría





+150h Práctica





SCORPION
CYBERTECH

Índice

SCORPION
CYBERTECH

IV. Especialización Sectorial

V. Certificaciones

SCORPION CYBERTECH

Fundamentos de la Ciberseguridad

Módulo 1.01 Introducción a la Ciberseguridad y Ciberamenazas

Nivel
Básico

Duración
4h Teoría + 8h Práctica

Público Objetivo
- Empresas
- Administraciones Públicas
- Instituciones Académicas

Objetivos Formativos

✓ Comprender los fundamentos y principios esenciales de la ciberseguridad, incluyendo el modelo CID
✓ Identificar los principales tipos de ciberamenazas y analizar casos reales de ciberincidentes
✓ Reconocer el marco legal y normativo básico que regula la ciberseguridad

Temario Teórico

1. Conceptos básicos de ciberseguridad
2. Tipos de ciberamenazas
3. Principios de CID
4. Marco legal y normativo básico
5. Casos prácticos de ciberincidentes

SCORPION
CYBERTECH

Ciberejercicios Prácticos

1. CID: El triángulo de la seguridad revelado
    - ❑ Identificar qué principios del modelo CID se han vulnerado en distintos mensajes de una comunicación de mensajería entre dos personas
2. Ficheros al descubierto: detective de permisos
    - ❑ En equipos Windows/Linux se presentan estructuras de ficheros con permisos mal configurados. Identificar qué principio(s) se está(n) vulnerando respecto al modelo CID, e indicar cómo resolver la situación
3. Seguridad por oscuridad: la ilusión desenmascarada
    - ❑ En entornos Windows/Linux se han "ocultado" archivos en el escritorio. Encontrar los archivos y obtener su contenido
4. Huella digital: trazabilidad forense
    - ❑ Analizar registros básicos para identificar incidentes de seguridad en base a criterios lógicos
5. Amenazas al descubierto: ¿qué nos ataca?
    - ❑ Analizar distintos escenarios tras la acción de una ciberamenaza e identificar el tipo de amenaza y su medio de propagación
6. Datos bajo lupa: cumplimiento y riesgos
    - ❑ Revisar escenarios relacionados con el tratamiento de datos para determinar cuáles vulneran el marco legal aplicable (RGPD, ENS...)

SCORPION CYBERTECH

Fundamentos de la Ciberseguridad

Módulo 1.02 Principios de Seguridad Digital para Ciudadanos

Nivel
Básico

Duración
5h Teoría + 9h Práctica

Público Objetivo
- Empresas
- Administraciones Públicas
- Instituciones Académicas

Objetivos Formativos

✓ Adoptar hábitos de higiene digital y navegación segura, aplicando buenas prácticas al usar dispositivos, redes y sitios web
✓ Implementar medidas de protección personal y familiar, incluyendo la configuración de contraseñas, autenticación segura y control parental
✓ Prevenir amenazas humanas y sociales en línea, identificando y evitando ataques de ingeniería social y riesgos en redes sociales

Temario Teórico

1. Principios de higiene digital
2. Gestión segura de contraseñas y MFA
3. Identificación de phishing y fraude online
4. Seguridad en redes sociales y vida digital
5. Navegación segura y control parental básico

SCORPION
CYBERTECH

Ciberejercicios Prácticos

1. Puertas abiertas: el poder de las credenciales por defecto
   - ❑ Obtener acceso a servicios web mediante el uso de credenciales por defecto o contraseñas fácilmente derivables de los nombres de los servicios
2. Contraseñas frágiles: patrón y explotación
   - ❑ Identificar patrones en credenciales generadas de forma insegura, y obtener acceso a servicios web aprovechando la información recabada
3. Historias de horror: brechas por credenciales inseguras
   - ❑ Analizar situaciones reales donde se han comprometido servicios informáticos aprovechando el uso de credenciales inseguras
4. Fortaleza de contraseñas: construye murallas
   - ❑ Generar credenciales seguras mediante la aplicación de buenas prácticas, identificando y descartando credenciales inseguras
5. Cebo digital: detectando phishing
   - ❑ Revisar mensajes de correo electrónico identificando cuáles son mensajes legítimos y cuáles son ataques de tipo "phishing"
6. Higiene digital: rastros y MFA al rescate
   - ❑ Aplicar técnicas básicas de ingeniería social para acceder a otras cuentas de usuario con mala higiene digital. Verificar como las soluciones MFA protegen accesos sensibles
7. Surf seguro: control parental y señales
   - ❑ Implementar configuraciones de control parental y navegación segura en equipos Windows

SCORPION CYBERTECH

Fundamentos de la Ciberseguridad

Módulo 1.03

Fundamentos de Redes y Seguridad de la Información

Nivel
Medio

Duración
5h Teoría + 9h Práctica

Público Objetivo
- Empresas
- Administraciones Públicas
- Instituciones Académicas

Objetivos Formativos

✓ Comprender la arquitectura y funcionamiento de las redes de comunicación, reconociendo los principales componentes, topologías y protocolos que permiten el intercambio seguro de información
✓ Identificar vulnerabilidades, amenazas y riesgos en entornos de red, evaluando su impacto y aplicando medidas de mitigación
✓ Conocer herramientas de protección en redes y datos, aplicando principios de seguridad perimetral, segmentación y análisis de tráfico

Temario Teórico

1. Arquitectura de redes
2. Protocolos básicos
3. Principales vulnerabilidades y riesgos
4. Seguridad perimetral y segmentación
5. Herramientas de análisis de tráfico

SCORPION
CYBERTECH

Ciberejercicios Prácticos

1. Rutas y atajos: misterios del enrutamiento
    - ❑ Analizar tablas de enrutamiento ARP y de red para identificar gateways y posibles rutas alternativas
2. Escucha activa: captura y análisis de tráfico
    - ❑ Interceptar y analizar comunicaciones abiertas en la red local mediante el uso de herramientas básicas
3. Safari de red: descubre hosts y servicios
    - ❑ Explorar las redes accesibles, descubriendo hosts activos y servicios expuestos mediante el uso de herramientas básicas
4. Puertos con sorpresas: identifica servicios ocultos
    - ❑ Descubrimiento e identificación de servicios expuestos en puertos no habituales mediante análisis manual
5. Nmap en acción: análisis avanzado
    - ❑ Utilizar nmap para descubrimiento y análisis de servicios expuestos, identificando versiones y encontrando posibles vulnerabilidades
6. Fortaleza de red: diseño y hardening
    - ❑ Diseñar e implementar configuraciones de redes seguras en entornos de producción simulada, aplicando criterios de hardening y buenas prácticas
7. Escudo en tiempo real: protección de servicios
    - ❑ Identificar servicios y configuraciones inseguras en sistemas de producción simulados, diseñando e implementando medidas de protección frente a ciberataques automatizados

SCORPION CYBERTECH

Fundamentos de la Ciberseguridad

Módulo 1.04 — Criptografía y su Aplicación Práctica en Entornos Reales

Nivel
Medio

Duración
8h Teoría + 9h Práctica

Público Objetivo
- Empresas
- Administraciones Públicas
- Instituciones Académicas

Objetivos Formativos

✓ Comprender los principios y funciones de la criptografía moderna, distinguiendo los métodos simétricos y asimétricos y su papel en la protección de la información
✓ Analizar y aplicar los principales algoritmos y estándares criptográficos, valorando su idoneidad según el tipo de datos y nivel de seguridad requerido
✓ Implementar soluciones de cifrado, autenticación y gestión de claves, integrando infraestructuras de clave pública y certificados digitales

Temario Teórico

1. Fundamentos de criptografía
2. Criptografía simétrica
3. Criptografía asimétrica
4. Protocolos y estándares criptográficos
5. Criptografía aplicada y PKI

SCORPION
CYBERTECH

Ciberejercicios Prácticos

1. Códigos antiguos: rompiendo cifrados clásicos
   - ❑ Analizar varios textos cifrados con métodos clásicos para determinar el algoritmo utilizado, romper el cifrado y reconstruir el mensaje original
2. Sello de verdad: verificación de integridad
   - ❑ Comparar firmas digitales de ficheros para identificar manipulaciones, recalcular valores correctos y localizar ficheros íntegros
3. Criptografía en práctica: cifrar, firmar, proteger
   - ❑ Aplicar algoritmos de cifrado, tanto simétricos como asimétricos; analizando modos de operación y tamaños de clave, para cifrar y descifrar información sensible
4. Vector de inicialización y modos: pequeños errores, grandes filtraciones
   - ❑ Estudiar el efecto de diferentes modos de operación y la reutilización de un mismo vector de inicialización en varios ficheros cifrados, identificando configuraciones vulnerables que permiten recuperar la información original
5. Beso criptográfico: intercambio híbrido de claves
   - ❑ Simular intercambios de información mediante cifrado híbrido, gestionando claves simétricas y asimétricas, para establecer canales seguros
6. Radiografía TLS: análisis de sesiones cifradas
   - ❑ Examinar capturas de tráfico de un protocolo cifrado para identificar versiones, suites criptográficas y certificados utilizados, localizando datos en las sesiones correctas
7. Blindaje criptográfico: protección de servicios
   - ❑ Evaluar la configuración criptográfica de servicios en sistemas de producción simulados, detectar parámetros débiles y ajustar configuraciones para resistir ciberataques automatizados
8. Maestro de certificados: PKI interna en juego
   - ❑ Trabajar con una PKI interna para emitir, firmar y validar certificados de distintos roles
9. Acceso por certificado: autenticación basada en certificados
   - ❑ Configurar y utilizar autenticación basada en certificados en un servicio simulado, diferenciando accesos válidos e inválidos

SCORPION CYBERTECH

Seguridad Operacional

Módulo II.01 — Seguridad en el Puesto de Trabajo y Buenas Prácticas

Nivel
Básico

Duración
4h Teoría + 8h Práctica

Público Objetivo
- Empresas
- Administraciones Públicas
- Instituciones Académicas

Objetivos Formativos

✓ Adoptar hábitos de higiene digital y protección personal, aplicando buenas prácticas para mantener la seguridad en el uso cotidiano de dispositivos y redes
✓ Configurar contraseñas seguras y sistemas de autenticación multifactor, fortaleciendo el acceso a cuentas y recursos frente a amenazas comunes
✓ Reconocer y prevenir intentos de phishing y fraude en línea, aplicando criterios seguros en el teletrabajo y el uso de dispositivos móviles

Temario Teórico

1. Principios de higiene digital
2. Gestión segura de contraseñas y MFA
3. Identificación de phishing y fraude online
4. Uso seguro de dispositivos móviles
5. Buenas prácticas en teletrabajo

SCORPION
CYBERTECH

Ciberejercicios Prácticos

1. Puertas abiertas: el poder de las credenciales por defecto
   - ❑ Obtener acceso a servicios web mediante el uso de credenciales por defecto o contraseñas fácilmente derivables de los nombres de los servicios
2. Contraseñas frágiles: patrón y explotación
   - ❑ Identificar patrones en credenciales generadas de forma insegura, y obtener acceso a servicios web aprovechando la información recabada
3. Historias de horror: brechas por credenciales inseguras
   - ❑ Analizar situaciones reales donde se han comprometido servicios informáticos aprovechando el uso de credenciales inseguras
4. Fortaleza de contraseñas: construye murallas
   - ❑ Generar credenciales seguras mediante la aplicación de buenas prácticas, identificando y descartando credenciales inseguras
5. Cebo digital: detectando phishing
   - ❑ Revisar mensajes de correo electrónico identificando cuáles son mensajes legítimos y cuáles son ataques de tipo "phishing"
6. Higiene digital: rastros y MFA al rescate
   - ❑ Aplicar técnicas básicas de ingeniería social para acceder a otras cuentas de usuario con mala higiene digital. Verificar como las soluciones MFA protegen accesos sensibles

SCORPION CYBERTECH

Seguridad Operacional

Módulo II.02 — Gestión de Incidentes y Respuesta ante Ciberataques

Nivel
Medio

Duración
6h Teoría + 9h Práctica

Público Objetivo
- Empresas
- Administraciones Públicas
- Fuerzas y Cuerpos de Seguridad del Estado

Objetivos Formativos

✓ Comprender el ciclo de vida y clasificación de los ciberincidentes, identificando las fases y actores implicados en su gestión
✓ Aplicar procedimientos de respuesta y recuperación ante ciberataques, siguiendo protocolos establecidos de detección, contención y comunicación
✓ Utilizar herramientas básicas de monitorización y análisis forense, apoyando la investigación y documentación de incidentes de seguridad

Temario Teórico

1. Definición y clasificación de ciberincidentes
2. Ciclo de vida de gestión de ciberincidentes
3. Herramientas de monitorización y detección
4. Procedimientos de comunicación y reporte
5. Introducción al análisis forense

SCORPION
CYBERTECH

Ciberejercicios Prácticos

1. Triage relámpago: clasificando incidentes
   - ❑ Analizar eventos de seguridad y registros de actividad procedentes de varios sistemas, diferenciando entre incidencias operativas, falsos positivos y ciberincidentes reales. Clasificar estos eventos según tipología y criticidad
2. Hilo del ataque: reconstrucción temporal
   - ❑ A partir de múltiples hallazgos técnicos, reconstruir la cronología completa de un ciberincidente, identificando las fases de detección, contención, erradicación y recuperación
3. Matriz de alarmas: correlación sin SIEM
   - ❑ Examinar un panel simulado de alertas de seguridad con eventos procedentes de distintos sistemas y aplicaciones, correlacionando alertas relevantes e identificando incidentes reales
4. Logs al microscopio: detectando anomalías
   - ❑ Revisar registros de sistema y de aplicación en un equipo comprometido, buscando patrones de comportamiento sospechoso. Localizar el conjunto coherente de entradas que describen una intrusión
5. Evidencia en caja fuerte: identificación y preservación
   - ❑ Explorar un entorno afectado por un incidente de seguridad, localizando y extrayendo los elementos que deben considerarse evidencias
6. Artefactos desenmascarados: análisis inicial
   - ❑ Trabajar sobre un sistema simulado tras un incidente, examinando procesos, eventos y otros elementos relevantes. Detectar y extraer los artefactos asociados a la intrusión
7. Crono-Forense: construyendo la línea de tiempo
   - ❑ A partir de distintas trazas en un gran sistema de ficheros, construir una línea de tiempo forense básica que refleje las acciones del atacante

SCORPION CYBERTECH

Seguridad Técnica Avanzada

Módulo III.01

Seguridad en Aplicaciones Web: Amenazas y Contramedidas

Nivel
Medio

Duración
6h Teoría + 8h Práctica

Público Objetivo
- Empresas
- Administraciones Públicas
- Fuerzas y Cuerpos de Seguridad del Estado

Objetivos Formativos

✓ Analizar las vulnerabilidades más comunes en aplicaciones web, comprendiendo su origen y el impacto que generan en la seguridad de los sistemas
✓ Aplicar técnicas y buenas prácticas para prevenir ataques como inyección SQL, XSS o CSRF, siguiendo los lineamientos de OWASP y otros estándares de desarrollo seguro
✓ Implementar medidas de protección y hardening en entornos web, fortaleciendo la configuración y la respuesta ante incidentes de seguridad

Temario Teórico

1. Introducción a la seguridad web
2. Ataques de inyección SQL, LDAP y comandos
3. Cross-Site Scripting (XSS)
4. Cross-Site Request Forgery (CSRF)
5. Buenas prácticas y hardening de aplicaciones web

SCORPION
CYBERTECH

Ciberejercicios Prácticos

1. Mapa de superficie: recon de app web
   - ❑ Navegar por una aplicación web simulada, identificando páginas, formularios y puntos de entrada de datos. Elaborar un inventario básico de superficies de ataque típicas según OWASP
2. Inyección SQL: rompe y repara
   - ❑ Interactuar con un formulario vulnerable hasta acceder a información no autorizada. Identificar la causa de la vulnerabilidad y proponer medidas como consultas parametrizadas y validación de entrada
3. Tipos de inyección: detecta y clasifica
   - ❑ Examinar varios puntos de entrada de una aplicación y determinar qué tipo de inyección (SQL, LDAP o comandos) sería explotable en cada uno
4. XSS en vivo: explota y parcha
   - ❑ Localizar puntos vulnerables a XSS en formularios y áreas de comentarios. Construir cargas que ejecuten código en el navegador e identificar las causas, proponiendo medidas como codificación de salida y sanitización
5. CSRF: prueba de integridad anti-cebo
   - ❑ Analizar operaciones sensibles para comprobar si están protegidas frente a CSRF. Intentar construir peticiones maliciosas e indicar qué controles deberían implementarse
6. Código bajo fuego: OWASP style guide
   - ❑ Revisar fragmentos de código que manejan entradas, sesiones y acceso a datos, identificando patrones inseguros. Reescribir las secciones críticas aplicando buenas prácticas de desarrollo seguro OWASP
7. Endurece tu web: hardening de servidor y app
   - ❑ Partir de un entorno web mal configurado e identificar debilidades (cabeceras de seguridad, directorios listables, versiones expuestas). Proponer ajustes de configuración para reducir la superficie de ataque
8. Incidente web: detective y remedio
   - ❑ A partir de registros y trazas de aplicación, reconstruir un incidente en una aplicación web. Identificar el vector de ataque y aplicar contramedidas técnicas y de proceso

SCORPION CYBERTECH

Seguridad Técnica Avanzada

Módulo III.02

OSINT: Técnicas y Herramientas para la Inteligencia en Fuentes Abiertas

Nivel
Medio

Duración
6h Teoría + 7h Práctica

Público Objetivo
- Empresas
- Administraciones Públicas
- Fuerzas y Cuerpos de Seguridad del Estado

Objetivos Formativos

✓ Comprender los principios y alcance de la inteligencia en fuentes abiertas (OSINT), reconociendo su utilidad en la investigación y la ciberseguridad
✓ Aplicar técnicas de búsqueda avanzada y uso de herramientas OSINT, recopilando y correlacionando información proveniente de diversas fuentes públicas
✓ Analizar, interpretar y presentar los resultados obtenidos, aplicando metodologías OSINT a casos prácticos y escenarios reales de investigación

Temario Teórico

1. Fundamentos de OSINT
2. Fuentes de información
3. Técnicas de búsqueda avanzada
4. Herramientas OSINT
5. Análisis y presentación de resultados

SCORPION
CYBERTECH

Ciberejercicios Prácticos

1. Cacería OSINT: fuentes que importan
    - ❑ A partir de un caso de investigación, identificar y clasificar fuentes OSINT útiles (web pública, redes sociales, registros públicos, repositorios, etc.), señalando cuáles son prioritarias para el caso
2. Operadores al rescate: búsqueda avanzada
    - ❑ Utilizar operadores de búsqueda avanzada y filtros en motores y directorios públicos para localizar información específica sobre una entidad a partir de datos limitados iniciales
3. Dossier digital: perfilado básico
    - ❑ Recopilar información pública dispersa sobre un objetivo (usuario, organización o servicio online) y construir un perfil básico, agrupando datos de contacto, presencia online y posibles relaciones
4. Huella técnica: dominios e IPs
    - ❑ Analizar dominios, direcciones IP y servicios expuestos asociados a un objetivo, empleando fuentes públicas para mapear su huella en Internet
5. Conexiones ocultas: correlación multi-fuente
    - ❑ Partiendo de varias entradas de información parcial, correlacionarlas entre distintas plataformas y registros para descubrir conexiones y relaciones ocultas
6. Veracidad OSINT: chequeo de evidencias
    - ❑ Evaluar la fiabilidad de capturas, publicaciones y documentos obtenidos y descartar información dudosa o poco verosímil

SCORPION CYBERTECH

Seguridad Técnica Avanzada

Módulo III.03 — Hardening de Sistemas y Redes

Nivel
Avanzado

Duración
6h Teoría + 11h Práctica

Público Objetivo
- Empresas
- Administraciones Públicas
- Fuerzas y Cuerpos de Seguridad del Estado

Objetivos Formativos

✓ Comprender los principios del hardening en sistemas y redes, identificando configuraciones y prácticas que fortalezcan la seguridad de los entornos tecnológicos
✓ Aplicar técnicas para reducir la superficie de ataque, configurando de forma segura servicios, sistemas operativos y componentes de red
✓ Realizar auditorías y automatizar procesos de hardening, verificando el cumplimiento de las políticas y estándares de seguridad establecidos

Temario Teórico

1. Concepto de hardening
2. Hardening en sistemas operativos
3. Configuración segura de redes
4. Auditoría de servicios
5. Automatización del hardening

SCORPION
CYBERTECH

Ciberejercicios Prácticos

1. **Debilidades a la vista: auditoría inicial**
   - ❑ Revisar la configuración inicial de un sistema (usuarios, servicios, permisos, políticas) e identificar elementos que incrementan la superficie de ataque, priorizando qué corregir primero
2. **Hardening 101: el Sistema Operativo**
   - ❑ Aplicar medidas de hardening en un sistema simulado: deshabilitar servicios innecesarios, configurar políticas de contraseñas, ajustar permisos y revisar configuraciones por defecto inseguras
3. **Servicios blindados: configuración segura**
   - ❑ Analizar la configuración de uno o varios servicios de red y aplicar ajustes de seguridad recomendados
4. **Cortafuegos inteligente: segmentación y filtrado**
   - ❑ Sobre un entorno de red con pocos controles: ajustar reglas de cortafuegos, segmentación y ACLs para limitar movimientos laterales y accesos no autorizados
5. **Exposición cero: auditoría de puertos y servicios**
   - ❑ A partir de un listado de puertos y servicios detectados, identificar exposiciones innecesarias o configuraciones débiles y aplicar acciones de mitigación para cada uno
6. **Tesoro oculto: encontrando backdoors**
   - ❑ Analizar un sistema aparentemente hardenizado para localizar una puerta trasera oculta; determinar cuál fue el vector que la permitió y aplicar medidas correctivas
7. **Escalando por error: privilegios por mala configuración**
   - ❑ Revisar permisos, grupos y configuraciones en un sistema para localizar una vía de escalada de privilegios derivada de un hardening incompleto o erróneo, aplicando la corrección adecuada
8. **Saltando barreras: bypass de firewall**
   - ❑ Examinar la configuración de filtrado de red de un entorno y encontrar una combinación de rutas o puertos que permita eludir las restricciones previstas. Proponer una versión corregida de las reglas para evitar el bypass
9. **Checklist en mano: verificación de baseline**
   - ❑ Comparar la configuración de un sistema con una checklist o baseline de seguridad proporcionada, identificando desviaciones y clasificándolas según su criticidad
10. **Hardening automático: plantillas en acción**
    - ❑ Diseñar y ejecutar plantillas de configuración sobre entornos simulados de producción. Verificar los cambios producidos en el entorno
11. **Post-Hardening: ¿de verdad seguro?**
    - ❑ Evaluar un entorno tras la aplicación de medidas de hardening, comprobando qué vectores de ataque se han reducido y qué debilidades persisten, implementando medidas adicionales

SCORPION CYBERTECH

Seguridad Técnica Avanzada

Módulo III.04 — Análisis de Malware y Amenazas Avanzadas (APT)

Nivel
Avanzado

Duración
8h Teoría + 13h Práctica

Público Objetivo
- Empresas
- Administraciones Públicas
- Fuerzas y Cuerpos de Seguridad del Estado

Objetivos Formativos

✓ Comprender el ciclo de vida y comportamiento de los distintos tipos de malware, identificando sus vectores de ataque y mecanismos de propagación
✓ Detectar y analizar tácticas, técnicas y procedimientos (TTPs) asociados a APTs, utilizando marcos de referencia como MITRE ATT&CK
✓ Ejecutar análisis estático y dinámico de muestras maliciosas, empleando entornos controlados para extraer indicadores y patrones de compromiso

Temario Teórico

1. Tipos de malware y vectores de ataque
2. Ciclo de vida de APTs
3. Análisis estático de binarios
4. Análisis dinámico en entornos controlados
5. Correlación con MITRE ATT&CK

Ciberejercicios Prácticos

1. Zoológico malware: clasifica las muestras
    - ❑ Analizar descripciones, trazas y comportamientos de varias muestras de malware para clasificarlas identificando vector de entrada y objetivo principal
2. APTienda: reconstruye el ciclo de vida
    - ❑ A partir de eventos, logs y artefactos proporcionados, reconstruir las fases de un ataque APT indicando qué evidencias corresponden a cada etapa
3. Pistas del crimen: extrae IoCs
    - ❑ Examinar registros de sistema, tráfico de red y ficheros sospechosos para extraer IoCs relevantes asociados a una campaña de malware simulada
4. Binario a la vista: análisis estático
    - ❑ Trabajar en el entorno simulado, revisando cadenas, cabeceras y secciones para identificar funciones clave de una APT
5. Sandbox en acción: observa el comportamiento
    - ❑ Ejecutar una muestra en el entorno aislado y observar su comportamiento, correlacionando las acciones con sus posibles objetivos. Mapear las tácticas y técnicas empleadas a entradas concretas del marco MITRE ATT&CK
6. Ancla oculta: detectando persistencia
    - ❑ Analizar un sistema infectado para localizar mecanismos de persistencia y neutralizarlos
7. Tráfico del mal: correlando redes y ataques
    - ❑ Revisar capturas de tráfico asociadas a un ataque avanzado y relacionar patrones de comunicación con las fases del ciclo de vida del malware o la APT

SCORPION CYBERTECH

Seguridad Técnica Avanzada

Módulo III.05

Pentesting Avanzado con Kali Linux y Metasploitable

Nivel
Avanzado

Duración
9h Teoría + 14h Práctica

Público Objetivo
- Empresas
- Administraciones Públicas
- Fuerzas y Cuerpos de Seguridad del Estado

Objetivos Formativos

✓ Planificar y ejecutar pruebas de penetración completas, documentando hallazgos y proponiendo medidas correctoras
✓ Utilizar Kali Linux y su suite de herramientas para reconocimiento, escaneo y explotación controlada de vulnerabilidades
✓ Realizar post-explotación y escalado de privilegios en entornos seguros, preservando evidencia y evaluando el impacto

Temario Teórico

1. Metodología de pentesting
2. Entorno Kali Linux
3. Reconocimiento y escaneo
4. Explotación de vulnerabilidades
5. Post-explotación y escalada de privilegios

Ciberejercicios Prácticos

1. Ojo de halcón: recon pasivo y activo
    - ❑ Usar herramientas de Kali para recopilar información del entorno y elaborar un mapa básico de la superficie de ataque de Metasploitable
2. Mapa de explotación: enumeración profunda
    - ❑ Profundizar en servicios detectados en Metasploitable enumerando usuarios, versiones y directorios, identificando posibles vulnerabilidades explotables
3. Explotador artesanal: sin Metasploit
    - ❑ Ejecutar la explotación de un servicio vulnerable sin Metasploit, demostrando comprensión de la vulnerabilidad y del vector de ataque
4. Metasploit en marcha: explotación guiada
    - ❑ Utilizar Metasploit para explotar vulnerabilidades conocidas en Metasploitable, obteniendo una sesión remota controlada y documentando los pasos clave
5. De usuario a root: escalada en Metasploitable
    - ❑ Identificar y explotar una vía de escalada de privilegios para pasar de usuario básico a root en un sistema comprometido
6. Borrando huellas: arte del cover-up
    - ❑ Revisar los rastros dejados tras una intrusión previa y realizar tareas de limpieza de huellas
7. CTF: caza de banderas
    - ❑ Acceder a diversos sistemas en entornos simulados para recuperar banderas, aplicando distintas técnicas de pentesting avanzado

SCORPION CYBERTECH

Especialización Sectorial

Módulo IV.01 — Ciberseguridad para Administraciones Públicas

Nivel
Medio

Duración
5h Teoría + 11h Práctica

Público Objetivo
- Empresas del sector
- Administraciones Públicas

Objetivos Formativos

✓ Comprender y aplicar los principios del Esquema Nacional de Seguridad (ENS) en la gestión y protección de los sistemas públicos
✓ Implementar medidas de protección de datos y servicios críticos, garantizando la privacidad y continuidad operativa en las administraciones públicas
✓ Responder eficazmente ante incidentes y amenazas del sector público, aplicando planes de contingencia y protocolos establecidos

Temario Teórico

1. Introducción al ENS
2. Protección de datos y privacidad
3. Amenazas específicas en AAPP
4. Planes de contingencia
5. Ejemplos reales de incidentes

Ciberejercicios Prácticos

1. ENS Check: ¿cumple la administración?
   - ❑ Revisar la situación de seguridad de una administración ficticia simulada y detectar qué medidas y principios ENS no se cumplen
2. Riesgos críticos: servicio al ciudadano bajo la lupa
   - ❑ Evaluar una lista de activos y servicios críticos identificando amenazas relevantes y valorando el impacto de su indisponibilidad para la ciudadanía
3. Privacidad pública: protege los datos ciudadanos
   - ❑ Analizar varios formularios y procedimientos administrativos simulados para identificar tratamientos de datos personales excesivos o inseguros, señalando qué medidas deberían aplicarse
4. Amenazas gubernamentales: identifica y corrige
   - ❑ Revisar escenarios breves de post-incidente e identificar el tipo de amenaza, sus posibles causas y las debilidades organizativas asociadas
5. Post-Mortem público: lecciones aprendidas
   - ❑ Analizar un caso simplificado de incidente en un organismo público y extraer las lecciones aprendidas, relacionándolas con controles ENS que habrían mitigado o evitado el impacto

SCORPION CYBERTECH

Especialización Sectorial

Módulo IV.02

Seguridad Digital para Negocios: Comunicaciones y Transacciones Protegidas

Nivel
Medio

Duración
6h Teoría + 11h Práctica

Público Objetivo
- Empresas del sector
- Administraciones Públicas

Objetivos Formativos

✓ Comprender los principales riesgos de la comunicación digital y las transacciones online en entorno empresarial
✓ Implementar medidas de seguridad para proteger la información de clientes, proveedores y del propio negocio
✓ Adoptar buenas prácticas que reduzcan la exposición a fraudes, suplantaciones de identidad y fugas de datos

Temario Teórico

1. Panorama de amenazas para negocios
2. Comunicaciones seguras
3. Transacciones online y pasarelas de pago seguras
4. Protección de datos sensibles
5. Normativas y obligaciones

Ciberejercicios Prácticos

1. Cebo digital: detectando phishing
   - ❑ Revisar mensajes de correo electrónico identificando cuáles son mensajes legítimos y cuáles son ataques de tipo "phishing"
2. Negocio bajo riesgo: identificando activos críticos
   - ❑ Analizar la descripción de un pequeño negocio online e identificar cuáles son los activos más críticos para el negocio
3. Canales en entredicho: seguridad de comunicaciones
   - ❑ Analizar distintos canales usados por empresas ficticias y determinar cuáles de ellos son claramente inadecuados para enviar información sensible
4. Checkout en peligro: revisa la pasarela
   - ❑ Examinar una tienda online simulada para identificar elementos sospechosos en la pasarela de pago
5. Cofre de datos: protección de información sensible
   - ❑ Revisar ejemplos de almacenamiento de datos; identificar y corregir malas prácticas
6. Fraude al descubierto: investigación de casos
   - ❑ Explorar y analizar escenarios de casos de fraude en entornos simulados
7. Cumplimiento express: verifica obligaciones legales
   - ❑ Evaluar listados de prácticas de varias empresas ficticias y detectar las cláusulas o apartados concretos que vulneran obligaciones legales básicas

SCORPION CYBERTECH

Especialización Sectorial

Módulo IV.03 Ciberseguridad en Entornos Industriales (OT/SCADA)

Nivel
Avanzado

Duración
6h Teoría + 15h Práctica

Público Objetivo
- Empresas del sector
- Administraciones Públicas

Objetivos Formativos

✓ Identificar riesgos, vulnerabilidades y vectores de ataque en sistemas OT y SCADA, comprendiendo su impacto en los procesos industriales
✓ Aplicar estrategias y medidas defensivas específicas para entornos industriales, fortaleciendo la resiliencia frente a amenazas cibernéticas
✓ Diseñar y mantener arquitecturas de red segmentadas y seguras, garantizando la protección de los sistemas de control y comunicación industrial

Temario Teórico

1. Introducción a OT y SCADA
2. Protocolos industriales
3. Amenazas y vectores de ataque OT
4. Estrategias de mitigación
5. Casos reales en industria

Ciberejercicios Prácticos

1. Choque de mundos: IT vs OT
   - ❑ A partir de la descripción de una organización, clasificar varios sistemas y redes como IT u OT e identificar el sistema que está indebidamente conectado a ambas sin controles intermedios
2. Protocolo en la mira: Modbus/DNP3 al análisis
   - ❑ Capturar y analizar tráfico de un segmento OT y localizar operaciones inseguras
3. Redes mixtas: cierra la brecha IT-OT
   - ❑ Explorar escenarios simulados de red mixta corporativa e industrial; detectar y corregir malas prácticas de acceso entre los dos tipos de red
4. Cápsulas industriales: implementa segmentación
   - ❑ A partir de un escenario de red simulado, implementar una segmentación de red básica apropiada para entornos industriales
5. PLC protegido: reglas de firewall precisas
   - ❑ Modificar la configuración de filtrado en un dispositivo perimetral para que solo se permitan las comunicaciones estrictamente necesarias con un PLC concreto. Verificar que, tras los cambios, el tráfico de prueba no autorizado es bloqueado
6. Ataque SCADA: simula y aprende
   - ❑ Revisar un escenario post-incidente de una estación de operación SCADA y determinar qué vector de ataque se ha utilizado
7. Resiliencia a prueba: defensa contra bots
   - ❑ Aplicar ajustes de configuración en un entorno OT simulado y comprobar que un ataque automatizado de prueba ya no consigue modificar parámetros de proceso críticos

SCORPION CYBERTECH

Certificaciones

Módulo V.01

Preparación para CompTIA Security+ (SY0-601 / SY0-701) – Fundamentos de Ciberseguridad

Nivel
Básico

Duración
7h Teoría + 8h Práctica

Público Objetivo
- Empresas
- Instituciones Académicas

Objetivos Formativos

✓ Comprender los principios fundamentales de la ciberseguridad, incluyendo amenazas, ataques y vulnerabilidades contempladas en el marco de CompTIA Security+
✓ Aplicar conceptos de criptografía, gestión de identidades y control de acceso, reforzando la protección de redes, sistemas y datos corporativos
✓ Desarrollar competencias prácticas para la certificación Security+, mediante la resolución de ejercicios y escenarios similares a los del examen oficial

Temario Teórico

1. Fundamentos de Seguridad y Amenazas
2. Seguridad de Redes y Dispositivos
3. Criptografía y Seguridad de Datos
4. Gestión de Identidades y Control de Acceso
5. Seguridad Operacional y Gobernanza

Ciberejercicios Prácticos

1. Jerarquía de riesgos: clasifica amenazas y fallos
   - ❑ Analizar varios escenarios breves y clasificar cada uno como amenaza, ataque o vulnerabilidad, identificando el más crítico para la organización descrita
2. Controles inteligentes: elige la defensa correcta
   - ❑ A partir de una lista de problemas de seguridad, seleccionar el control principal más adecuado en cada caso y relacionarlo con el objetivo de seguridad que protege
3. Topología bajo lupa: identifica servicios vulnerables
   - ❑ Explorar y analizar escenarios de redes internas e identificar los servicios mal protegidos según las condiciones mostradas en cada caso
4. Reglas en orden: revisión de firewalls
   - ❑ Analizar la configuración de un firewall y localizar las reglas que no siguen las directrices estudiadas. Determinar y aplicar los cambios necesarios para alinearlas con el principio de mínimo privilegio
5. Identidades en control: gestiona permisos y riesgos
   - ❑ Analizar la configuración de varias cuentas de usuario y grupos en un entorno simulado e identificar las cuentas con mayor riesgo por exceso de privilegios o mala gestión del ciclo de vida
6. Patrones de acceso: analiza logs críticos
   - ❑ Revisar logs de autenticación, accesos fallidos y cambios de permisos y detectar un patrón de actividad anómala que apunta a un posible compromiso de credenciales. Identificar el evento clave que lo evidencia
7. Políticas en práctica: revisión crítica
   - ❑ Evaluar extractos de políticas de seguridad de empresas ficticias e identificar los apartados que suponen riesgo de incumplimiento o de impacto operativo
8. Prueba final: ataque automático vs controles
   - ❑ En un entorno simulado, activar o modificar ciertos controles básicos y comprobar que un ataque automatizado ya no logra su objetivo inicial

Notas

Notas

Notas

scorpioncybertech.com

Calle Campus Universitario 7,
Edificio CEEIM, 30100, Murcia