IFCD072PO. Ciberseguridad, hacking ético.

Sku: 41562IN

Horas: 300

Formato: HTML

OBJETIVOS

- Conocer las funciones, herramientas, procesos y regulación para dominar las actuaciones del *hacker* ético.
- Conocer de manera introductoria el mundo *hacker,* comparando el retrato del ciberdelincuente tradicional con otras imágenes reales del *hacker* asociadas al campo de la ciberseguridad.
- Conocer la metodología del *hacking* ético, introduciendo conceptos relacionados con el sistema de seguridad de la información de una empresa.
- Conocer el funcionamiento del sistema de evaluación de vulnerabilidades CVSS *(Common Vulnerability Scoring System),* aprendiendo cómo son las mecánicas de esta metodología.
- Profundizar en el concepto ciberataque, conociendo cómo es el ciclo de vida de un ataque cibernético junto con un importante método de análisis de intrusión, que es empleado por los *hackers* éticos con idea de entender las acciones del atacante y poder combatirlo mediante una sólida defensa.
- Abordar el concepto *malware* como herramienta clave de los ciberataques, conociendo los distintos tipos de programas maliciosos y sus funciones.
- Revelar la importancia del buen diseño de una arquitectura de redes ciberseguras, escalables y sostenibles, destacando la necesidad de contar con sistemas de controles suficientes e independientes que permitan la operatividad de las organizaciones y su buen funcionamiento.
- Adquirir conocimientos sobre fallos de seguridad en los dispositivos de red para explotar las vulnerabilidades encontradas, conociendo las particularidades de los protocolos de seguridad para redes wifi.
- Crear un campo de entrenamiento o laboratorio de *Pentesting* virtual, utilizando la aplicación *VirtualBox.*
- Comprometer las redes *Wireless* rompiendo la seguridad, aprovechando las vulnerabilidades que presentan los protocolos WEP, WPA/WPA2 y WPS.
- Aplicar una metodología ágil en la organización para la identificación de intrusiones y amenazas en la red a través de herramientas específicas, conociendo las peculiaridades de los distintos tipos de ciberataques y las técnicas empleadas.

- Conocer recursos, herramientas y técnicas de ataque sobre credenciales para aprovechar las vulnerabilidades que presentan los sistemas operativos.
- Comprender los fundamentos de la criptografía y los conceptos relacionados con ella para abordar retos propuestos en las cibercompeticiones CTF.
- Asegurar el ejercicio correcto de la profesión de *hacker* ético conociendo tanto los límites marcados por el Código Penal como la manera de definir un plan de trabajo de calidad apoyándose en referencias normativas de la familia de estándares ISO 27000.

CONTENIDOS

UD1: Planeta *Hacker.*

- Introducción.
- *Hackers:*
  - Clasificaciones de *hackers*.
  - Comunidad *hacker*.
  - Gurús *hackers*.
  - Comunidad Anonymous:
    - Objetivos del movimiento asociativo.
    - Ataques famosos.
  - Mujeres *hackers*.
- El fenómeno *hacker*.
- Manifiesto *hacker* ético:
  - Actitudes del *hacker* ético.
  - Valores del *hacker* ético.
  - Emblema *hacker*.

UD2: Auditorías de *hacking* ético o *Pentesting*.

- Introducción.
- *Pentesting*:
  - Tipos de *Pentesting*.
  - Fases del *Pentesting*.
- Beneficios de las auditorías de hacking ético:
  - Ámbito de actuación de las auditorías de ciberseguridad.
- Principios de protección de la seguridad de información.
- Amenazas clave para la gestión de la seguridad de la información de una organización:
  - Clasificación de la información.
  - Fuentes de amenazas.
  - Principales amenazas para la gestión de la seguridad en la empresa.
  - El riesgo.
  - Medición del riesgo de los activos de información.
- *Pentesting* y gestión de riesgos.
- *Common Vulnerabilities and Expsures* (CVE).

UD3: Análisis de Vulnerabilidades.

- Introducción.
- Registro y clasificación de las vulnerabilidades:
    - Registro de nuevas vulnerabilidades en Common Vulnerabilities and Expsure (CVE).
    - Common Vulnerabilities Socring System (CVSS).
        - Base Metric Group.
        - Temporal Metric Group.
        - Environmental Metric Group.
    - Versiones CVSS:
        - Ejemplos de cambios de versiones CVSS.
    - Proceso de evaluación de vulnerabilidades con CVSS.
- Herramientas para calcular el valor CVSS:
    - Puntuaje de los grupos de métricas CVSS:
        - Puntuaje base.
        - Puntuaje temporal.
        - Puntuaje ambiental.
    - Vulnerabilidad con valores de métricas base distinta.

UD4: Ciberataques.

- Introducción.
- ¿Qué es un ataque cibernético?
    - Clasificación de ataques cibernéticos.
    - Ciclo de vida de un ciberataque.
- La cadena asesina Cyber Kill Chain.
    - Fundamentos del modelo de intrusión Cyber Kill Chain:
        - Niveles de ataque de la cadena Cyber Kill.
        - Fases de ataque de la cadena Cyber Kill.
    - Aplicación de la cadena de exterminio en entornos móviles:
        - Fase 1: reconocimiento.
        - Fase 2: militarización.
        - Fase 3: entrega.
        - Fase 4: explotación.
        - Fase 5: instalación.
        - Fase 6: comando y control.
        - Fase 7: acciones sobre objetos.
        - Estrategias de defensa para entornos móviles.
    - Análisis de intrusión de ataques cibernéticos en la industria 4.0.

UD5: Malware.

- Introducción.
- Definición de *malware*.
- Tipos de *malware*.
    - Virus.
    - Troyanos.
    - Gusanos.

    - *Spyware*.
    - *Adware*.
    - *Trojan-clickers*.
    - *Ransomware*.
    - RAT.
    - *Exploits*.
    - *Cryptojacking*.
    - *Botnets*:
        - Consulta de códigos AntiBotnet.
        - Chequeo online AntiBotnet de la conexión.
    - App maliciosas.
- Características del *malware*.
- Procedimiento de inyección de un *malware*.

UD6: Arquitectura de redes.

- Introducción.
- *Network*.
- Arquitectura de redes:
    - Características de la arquitectura de redes.
    - Arquitectura de red por capas o niveles.
    - Componentes de una arquitectura de red.
- Protocolos de comunicación.
- Protocolos SNA (*System Network Architecture*):
    - Protocolos *NetWare*.
    - Protocolos *Apple Talk*.
    - NetBEUI (*NetBIOS Extended User Interface*).
- Protocolos TCP/IP (*Transmission Control Protocol / Internet Protocol*) estándares.
- Estándares de internet.
- Vulnerabilidades en las redes de nueva generación:
- Arquitectura de redes inalámbricas 5G.

UD7: *Routers* y puertas.

- Introducción.
- ¿Son seguras las redes inalámbricas?:
    - *Routers* y puertas:
        - Módem.
        - *Router*.
        - Puntos de acceso.
        - Puertos del router.
    - Auditorías wifi:
        - *Software* de *hacking* ético para auditar redes *Wireless*.
    - Protocolos de seguridad wifi:
        - Seguridad WEP.
        - Seguridad WPA/WPA2.
        - Seguridad WPS.

        - Seguridad WPA3.
        - Seguridad WPA6.

UD8: Técnicas y tecnologías de escaneo: laboratorio de entrenamiento del *hacker* ético.

- Introducción.
- Plataformas para entrenar:
    - Tipos de máquinas virtuales:
        - Máquinas virtuales de sistemas.
        - Máquinas virtuales de procesos.
    - Funcionamiento y uso de las máquinas virtuales.
- Instalación de *VirtualBox*.
- Creación de máquinas virtuales.

UD9: *Password cracking*.

- Introducción.
- Ciberataques a redes *Wireless*:
    - Técnicas para burlar la ocultación de SSID de la red.
    - Técnicas para burlar el filtro de direcciones.
    - Técnicas para burlar los DHCP inhabilitados.
- *Hackeo* WPA/WPA2.
- *Hackeo* WEP.
- *Hackeo* WPS:
    - Romper redes inalámbricas WPA y WPA2 con WPS mediante ataque de fuerza bruta.
    - Romper redes inalámbricas WPA y WPA2 con WPS mediante ataque *PixieDust*.
- Medidas de protección de la redes inalámbricas:
    - Vigilar la configuración básica de la seguridad de las redes inalámbricas.
    - Implementar servidores de identificación.
    - Proteger los puntos de acceso.
    - Actualizar *software* y *firmware*.
    - Reducir la potencia de la antena wifi.
    - Gestionar con eficacia las redes de invitados.
    - Incorporar elementos de alerta de intrusos en la infraestructura de la red.

UD10: Métodos de investigación y recolección de datos.

- Introducción.
- Tráfico en red: técnica de captura pasiva:
    - Ciberataques activos.
    - Ciberataques pasivos.
    - Herramientas de captura pasiva.
    - Medidas de protección.
- Ciberataques específicos a redes LAN:
        - IP *Spoofing*.
        - ARP *Spoofing*.

        - Web *Spoofing*.
        - DNS *Spoofing*.
        - Mail *Spoofing*.
        - DHCP *Spoofing*.
    - *Man in the Middle* (MitM):
        - Ataque MitM mediante técnicas ARP *Spoofing* con *Ettercap*.
    - Otros tipos de ciberataques a redes locales:
        - *MAC Flooding*.
        - *VLan Hooping*.
        - Ciberataque sobre STP.
        - Ciberataque sobre VoIP.
    - Métodos de investigación y recolección de datos.

UD11: Infraestructuras de la tecnología y vulnerabilidades de los sistemas.

- Introducción.
- La infraestructura de la tecnología de la información:
    - Gestión de la infraestructura de la tecnología de la información.
    - Infraestructura hiperconvergente.
- Infraestructuras *Linux* y *Windows*:
    - Infraestructura *Linux*.
    - Infraestructura *Windows*.
- Crackeando sistemas:
    - Ataques sobre credenciales.
    - Función hash y hasheo de contraseñas.
    - Herramientas para comprometer credenciales:
        - *Hydra*.
        - *John the Ripper*.
        - *Hashcat*.
        - *L0phtCrack*.
        - *Pass the hash*.
    - Fórmulas para proteger las credenciales en sistemas operativos *Linux* y *Windows* :
        - Almacenaje de contraseñas en *Linux*.
        - Almacenaje de contraseñas en *Windows*.
    - *Exploits*:
        - Herramienta de auditoría para crear y ejecutar *exploits*.
        - Ejemplo de ataque con *Metasploit*.

UD12: Disciplinas de la ciberseguridad y el aprendizaje de *hacking* ético con CTF.

- Introducción.
- Disciplinas de ciberseguridad:
    - Autenticación criptográfica.
    - Generación de claves.
    - Principios fundamentales de la criptografía.
    - Métodos criptográficos:

        - Criptografía clásica.
        - Criptografía moderna.
    - Aprendiendo *hacking* con CTF:
        - Categorías de los CTF.
        - Las reglas de las cibercompeticiones CTF.
        - Plataformas CTF.
        - ¿Dónde practicar *hacking* de forma individual?

UD13: Marco legal del *hacking*.

- Introducción.
- Marco legal del hacking:
    - Ley del Hacking:
        - Artículo 197 del Código Penal.
        - Artículo 264 del Código Penal.
    - Familia de normas ISO 27000:
        - Norma ISO 27000.
        - Norma ISO 27001.
        - Norma ISO 27002.
        - Norma ISO 27003.
        - Norma ISO 27004.
        - Norma ISO 27005.
        - Norma ISO 27007.
        - Norma ISO 27008.
        - Norma ISO 27013.
        - Norma ISO 27014.
        - Norma ISO 27021.