

TÉCNICAS Y HERRAMIENTAS DE ATAQUES A REDES TCP/IP

TÉCNICAS Y HERRAMIENTAS DE ATAQUES A REDES TCP/IP

Duración: 60 horas

Precio: consultar euros.

Modalidad: e-learning

Objetivos:

Descripción: Adoptar, pulir y reutilizar este modelo de experimentación para ponerlo en funcionamiento sobre redes que están protegidas y son inmunes a los ataques. Conocer las vulnerabilidades y los posibles ataques a las redes TCP/IP y a los sistemas libres. Conocer las diferentes técnicas de exploración de puertos. Fundamentación: La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta (incluyendo la información contenida). Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas y leyes concebidas para minimizar los posibles riesgos a la infraestructura o a la información. La seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a manos de otras personas. Este tipo de información se conoce como información privilegiada o confidencial.

Metodología:

El Curso será desarrollado con una metodología a Distancia/on line. El sistema de enseñanza a distancia está organizado de tal forma que el alumno pueda compatibilizar el estudio con sus ocupaciones laborales o profesionales, también se realiza en esta modalidad para permitir el acceso al curso a aquellos alumnos que viven en zonas rurales lejos de los lugares habituales donde suelen realizarse los cursos y que tienen interés en continuar formándose. En este sistema de enseñanza el alumno tiene que seguir un aprendizaje sistemático y un ritmo de estudio, adaptado a sus circunstancias personales de tiempo

El alumno dispondrá de un extenso material sobre los aspectos teóricos del Curso que deberá estudiar para la realización de pruebas objetivas tipo test. Para el aprobado se exigirá un mínimo de 75% del total de las respuestas acertadas.

El Alumno tendrá siempre que quiera a su disposición la atención de los profesionales tutores del curso. Así como consultas telefónicas y a través de la plataforma de teleformación si el curso es on line. Entre el material entregado en este curso se adjunta un documento llamado Guía del Alumno dónde aparece un horario de tutorías telefónicas y una dirección de e-mail dónde podrá enviar sus consultas, dudas y ejercicios El alumno cuenta con un período máximo de tiempo para la finalización del curso, que dependerá del tipo de curso elegido y de las horas del mismo.

© icaformación2026

Profesorado:

Nuestro Centro fundado en 1996 dispone de 1000 m2 dedicados a formación y de 7 campus virtuales.

Tenemos una extensa plantilla de profesores especializados en las diferentes áreas formativas con amplia experiencia docentes: Médicos, Diplomados/as en enfermería, Licenciados/as en psicología, Licencidos/as en odontología, Licenciados/as en Veterinaria, Especialistas en Administración de empresas, Economistas, Ingenieros en informática, Educadodores/as sociales etc…

El alumno podrá contactar con los profesores y formular todo tipo de dudas y consultas de las siguientes formas:

-Por el aula virtual, si su curso es on line
-Por e-mail
-Por teléfono

Medios y materiales docentes

-Temario desarrollado.

-Pruebas objetivas de autoevaluación y evaluación.

-Consultas y Tutorías personalizadas a través de teléfono, correo, fax, Internet y de la Plataforma propia de Teleformación de la que dispone el Centro.



© icaformación2026

Titulación:

Una vez finalizado el curso, el alumno recibirá por correo o mensajería la titulación que acredita el haber superado con éxito todas las pruebas de conocimientos propuestas en el mismo.

Programa del curso:

TEMA 1.TEORÍA DE REDES. PROTOCOLO TCP/IP

1. INTRODUCCIÓN
2. MODELO OSI Y TCP/IP
3. DIRECCIONES IP, MÁSCARA DE SUBRED
4. INTRANET, EXTRANET, INTERNET, ETC.
5. ENCAMINAMIENTO
6. PUERTOS, NOMBRE DOMINIO
7. PROTOCOLOS ARP, IP, TCP, UDP, ICMP

TEMA 2. TÉCNICAS DE SEGUIMIENTO, EXPLORACIÓN Y ENUMERACIÓN

1. INTRODUCCIÓN 2. ¿QUÉ ES SEGUIR EL RASTRO A UN OBJETIVO? 3. SEGUIR EL RASTRO EN INTERNET 4. ENUMERACIÓN DE LA RED 5. RECONOCIMIENTO DE LA RED Y SU TOPOLOGÍA PREVIO A UN ATAQUE

TEMA 3. EXPLORACIÓN DEL OBJETIVO

1. INTRODUCCIÓN 2.COMANDO PING, CONSULTAS ICMP, EXPLORACIÓN DE PUERTOS 3. TIPOS DE ESCANEOS A REALIZAR SOBRE EL OBJETIVO 4. DETECCIÓN DEL SISTEMA OPERATIVO, VERSIONES Y SERVICIOS EN EJECUCIÓN 5. UTILIZACIÓN DE HERRAMIENTAS (VULTERABILITY SCANNER) PARA LA AUDITORÍA DE SISTEMAS Y DETECCIÓN DE VULNERABILIDADES 6. MEDIDAS A ADOPTAR ANTE LAS FISURAS

TEMA 4. TIPOS DE ATAQUES TCP/IP

1. INTRODUCCIÓN 2. CLASIFICACIÓN DE LOS ATAQUES 3. ATAQUES TCP/IP 4. TÉCNICAS PARA LA BÚSQUEDA DE OBJETIVOS DE UN ATAQUE 5. AVERIGUACIÓN DE NOMBRES DE USUARIOS, GRUPOS Y CONTRASEÑAS 6. SAMBA: NOMBRES NETBIOS Y DOMINIOS 7. INGENIERÍA SOCIAL 8. INTENTOS DE PENETRACIÓN

TEMA 5. DEBILIDAD DE LOS PROTOCOLOS TCP/IP

1. INTRODUCCIÓN
2. ELEMENTOS DE INTERNET Y EL CONTROL DE ACCESO
3. TRANSMISIÓN DE PAQUETES Y PROMISCUIDAD

© icaformación2026

4. REDES LOCALES
5. VIGILANCIA DE PAQUETES
6. CORTAFUEGOS PERSONALES

© icaformación2026