Pentesting de infraestructuras

Bienvenidos al curso **Pentesting de infraestructuras.** Encontrarás esta guía en el temario del curso para que puedas consultarla en cualquier momento.

N.º Horas: 40 Fecha Inicio: X Fecha Fin: X

Objetivos del curso

Cada día es más habitual escuchar noticias sobre fallos de seguridad en grandes empresas o no tan grandes que exponen datos de clientes, o han tenido interrupciones en sus servicios.

En este curso veremos cómo podemos detectar fallos de seguridad en infraestructuras, qué riesgos implican y qué podemos hacer para solucionarlos.

¿Qué voy a aprender?

- Conceptos básicos necesarios para entender el proceso que se lleva a cabo en las auditorías a infraestructuras
- Comenzaremos con una introducción al mundo de este tipo de auditorías, qué son, cuál es el objetivo de las mismas, los diferentes alcances y escenarios que se pueden dar.
- Aprenderemos a diferenciar y a tomar importancia sobre el impacto que supone tener expuesto a Internet determinados servicios que se consideran críticos y que se puedan

- A su vez, evaluaremos la importancia que supone mantener nuestros sistemas parcheados y con las actualizaciones más recientes liberadas por los fabricantes.
- Además, aprenderemos a utilizar y sacar el mayor rendimiento de las diferentes técnicas y herramientas que se convertirán en nuestros mejores aliados para detectar vulnerabilidades o fallos de seguridad.
- Cada apartado irá acompañado de prácticas para aprender las diferentes técnicas y casuísticas que nos podemos encontrar en un entorno real.
- El objetivo final, es ser capaces de realizar evaluaciones de seguridad de infraestructuras en entornos reales detectando el mayor número de vulnerabilidades y malas configuraciones posibles, consiguiendo así entornos empresariales más seguros.

Conocimientos necesarios

Este curso está pensado para todos aquellos profesionales, desde estudiantes, gente que ya trabajé en ciberseguridad, desarrolladores, etc. que quieran empezar a formarse en el campo de la ciberseguridad o quieran profundizar sus conocimientos sobre vulnerabilidades en aplicaciones web.

Materiales y programas necesarios

- Ordenador con al menos 8GB de RAM
- Vmware/VirtualBox
- KALI Linux

Plataforma de formación

Cada alumno ha recibido un email con los datos de acceso a la plataforma. Además de a este curso todos los alumnos matriculados con TrainingIT tienen acceso al curso **"Conociendo la plataforma TrainingIT"**. Este curso está conformado por una serie de videos cortos donde se explican las principales funcionalidades de la plataforma.

Resumen de contenidos

El curso está dividido en **3 módulos** temáticos. Puedes consultar el temario al final de esta guía.

En cada módulo puede encontrar diferentes elementos:

-***Apuntes de la lección***

-Videos teórico-prácticos

-Código de la lección

- Test

- Otros recursos

Además, cuenta con un ejercicio práctico voluntario que se debe desarrollar durante el curso y que el profesor corregirá y evaluará al finalizar.

Profesor

Rubén Ortega está ligado al mundo de la ciberseguridad desde que comenzó su carrera profesional. Su desempeño viene ligado a las auditorías de Hacking Ético en diferentes plataformas y tecnologías. A día de hoy, trabaja como Consultor en el departamento de Risk Advisory en Deloitte España.

Marta Barrio tiene más de ocho años de experiencia en el campo de la ciberseguridad. Está especializada en hacking ético y pentest en diferentes plataformas y tecnologías. Actualmente trabaja como arquitecto de seguridad de aplicaciones en Beam Suntory.

Jaime Salas está ligado al mundo de la ciberseguridad desde hace 6 años. Especializado y dedicado profesionalmente al Hacking Ético y pentest en varias tecnologías y arquitecturas de seguridad. Actualmente trabaja como pentester en el departamento de Risk Advisory en Deloitte España.

Enrique Pascual y **Beatriz Pino**, actuarán como gestores del curso en todo lo relacionado con la plataforma de formación. Te puedes poner en contacto vía mensaje a través de la plataforma, o directamente en **epascual@trainingit.es** o **bpino@trainingit.es**.

A todos ellos los puedes encontrar en la sección **"Participantes"** del curso con sus respectivos roles.

Calendario del curso

El curso comienza el **X** y la fecha de finalización será el **X**, último día en que se podrán entregar la práctica final.

A partir de esa fecha los profesores dejarán de participar en los foros del curso.

Si no lo terminas a tiempo, seguirás teniendo acceso a la plataforma con todo el material disponible. Pero no tendrás a los profesores a tu disposición, aunque sí a otros alumnos que puedan estar en tu misma situación.

Para facilitar el seguimiento del mismo se establece un calendario de temas. No obstante, a ser un curso online cada alumno puede seguir el ritmo que mejor se adapte a sus necesidades.

Mediante el foro de avisos se os informará todas las semanas de la programación del curso. En el calendario de la plataforma tendréis marcadas todas las fechas importantes del curso.

Consejos para aprovechar tu curso

1. **Lee toda la documentación relacionada con el curso**
   Antes de comenzar, dedica tiempo a revisar toda la información proporcionada: guías, temarios, requisitos técnicos, y objetivos del curso. Esto te dará una visión clara de lo que se espera de ti y cómo organizarte.

2. **Utiliza un segundo monitor**
   Si es posible, configura un segundo monitor. Esto te permitirá seguir las clases en uno mientras practicas o tomas apuntes en el otro, optimizando tu experiencia de aprendizaje.

3. **Revisa los temas y sus elementos antes de empezar**
   Antes de ver las clases, explora los materiales asociados a cada tema: videos, lecturas, ejercicios, o recursos adicionales. Esto te ayudará a identificar conceptos clave y planificar tu aprendizaje.

4. **Haz un primer visionado de los videos**
   Visualiza los videos del curso de manera inicial, prestando atención al contenido global. No te preocupes por detenerte en cada detalle; el objetivo es obtener una comprensión general del tema.

5. **Realiza un segundo visionado siguiendo los pasos del profesor**
   En el segundo visionado, pausa el video según sea necesario y sigue los pasos del instructor. Reproduce las explicaciones en tu entorno, asegurándote de comprender y aplicar los conceptos explicados.

6. **Practica lo aprendido con otros casos y busca información adicional**
   No te límites a los ejercicios del curso. Aplica los conocimientos adquiridos en casos prácticos nuevos. Además, complementa tu aprendizaje investigando en internet, explorando foros, blogs, y tutoriales relacionados con los temas del curso.

7. **Participa activamente en el foro del curso**

   El foro del curso es una herramienta fundamental para resolver dudas, compartir experiencias y aprender en comunidad. Úsalo para plantear preguntas claras y específicas sobre los temas del curso, mencionando el módulo o ejercicio en cuestión para facilitar la respuesta del profesor. Antes de preguntar, revisa si alguien ya ha planteado una duda similar, y si tienes conocimientos o experiencias útiles, comparte tus propias respuestas para contribuir al aprendizaje de tus compañeros. Además, aprovecha el feedback del profesor, que estará disponible para aclarar conceptos y guiarte en tu progreso, enriqueciendo aún más la experiencia formativa.

Tutorías

El **"Foro de Dudas y Consultas"** es el centro de las tutorías del curso. Todas tus dudas relacionadas con el temario debes plantearlas en el foro ya que también ayudarán a otros compañeros, y otros compañeros podrán ayudarte a ti.

Al tratarse de un foro no existe un horario de tutorías. Se responderá en un plazo de 24 horas laborables. ***Utilizad siempre el foro***.

Enrique Pascual y **Beatriz Pino**, actuarán como gestores del curso en todo lo relacionado con la plataforma de formación. Te puedes poner en contacto vía mensaje a través de la plataforma, o directamente en **epascual@trainingit.es** o **bpino@trainingit.es**.

Práctica final voluntaria y examen teórico

El curso cuenta con un **ejercicio práctico final voluntario** que será corregido por el profesor.

Durante el curso se realizarán varias **pruebas de conocimientos obligatorias** mediante un examen de autoevaluación con preguntas tipo test.

Evaluaciones

En el curso habrá dos áreas de evaluación cada una con una influencia en la nota final del curso:

- ***Práctica final: 40%***
- ***Examen teórico: 60%***

Las calificaciones se podrán visualizar en el apartado **"Calificaciones"** del curso.

Certificado

El curso ofrece dos tipos de certificados:

- **Certificado de asistencia**: para aquellos alumnos que realicen el curso, pero no entreguen el ejercicio práctico voluntario.
- **Diploma acreditativo:** con evaluación positiva en las actividades realizadas en el curso para aquellos alumnos que realicen el ejercicio práctico y cuya calificación final de curso (Test+ Práctica) sea superior a 6.

Los certificados se entregarán una vez finalice el plazo del curso y se revisen que se cumplen todas las condiciones.

Bonificación

Para la evaluación y seguimiento del alumnado, la plataforma de Teleformación provee dos tipos de mecanismos distintos:

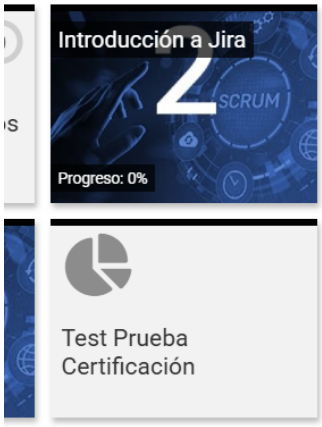
Sistemas de control internos del Aula Virtual. La plataforma registra la actividad del alumno dentro de la plataforma, obteniendo datos como:

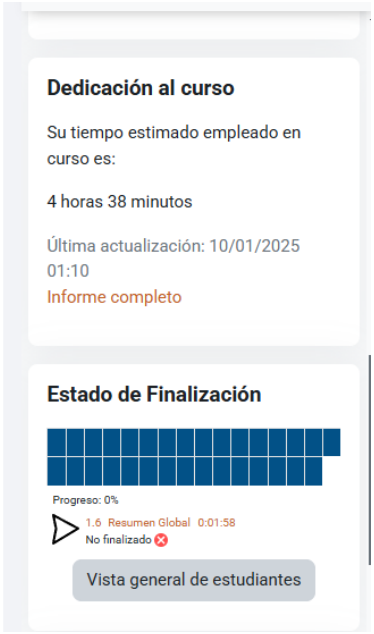
- ***Acceso del alumno a los distintos módulos del curso***
- ***Días de acceso y clics realizados dentro del curso***
- ***Tiempo total empleado en el curso***
- ***Seguimiento de las lecciones visualizadas***
- ***Seguimiento de los recursos utilizados***
- ***Evaluación obtenida en cuestionarios de autoevaluación***

Los alumnos que vayan a bonificar el curso a través de sus empresas deberán cumplir lo siguiente:

- Completar al menos el **75% de las actividades** del curso.
- Completar al menos el **75% de las pruebas** obligatorias del curso (test)
- Los **tiempos de conexión** a la plataforma deben ser iguales o superiores al **75%** del tiempo de estudio estimado del curso (el tiempo estimado de estudio se indica en la cabecera de esta guía y en la cabecera del propio curso).

Los alumnos pueden observar su progreso en el curso dentro de la plataforma en los bloques “**Dedicación al curso”** y **“Estado de Finalización”** que aparece en los menús laterales de la derecha de la pantalla.





- Desplegar menú lateral.

Acerca de TrainingIT

TrainingIT es una iniciativa para ofrecer formación especializada IT de alta calidad y bonificable por Fundae.

Descubre nuestros cursos online creados por especialistas en sus materias en www.trainingit.es.

Queremos formar a los mejores profesionales para que no se diga que en España no hay talento.

Te agradecemos que hayas confiado en TrainingIT para tu formación. Esperamos que este curso sea de tu agrado y que te ayude en tu carrera profesional.

Un saludo,

Enrique Pascual

epascual@trainingit.com

Gestor de Curso

Temario

1. Reconocimiento

1.1 Introducción

1.1.1 Índice Contenidos

1.1.2 Conceptos Básicos 1

1.1.3 Conceptos Básicos 2

1.2 Reconocimiento

1.2.1 Tipos de Reconocimiento

1.3 Reconocimiento Pasivo

1.3.1 Reconocimiento Pasivo Introducción

1.3.2 Reconocimiento Pasivo: whois

1.3.3 Reconocimiento Pasivo: whois (Ejemplo)

1.3.4 Reconocimiento Pasivo: emailharvesting

1.3.5 Reconocimiento Pasivo: emailharvesting (Ejemplo)

1.3.6 Reconocimiento Pasivo: GoogleHacking

1.3.7 Reconocimiento Pasivo: GoogleHacking (Ejemplo)

1.3.8 Reconocimiento Pasivo: Shodan

1.3.9 Reconocimiento Pasivo: Shodan (Ejemplo)

1.3.10 Reconocimiento Pasivo: Metadatos

1.3.11 Reconocimiento Pasivo: Metadatos (Practica)

1.3.12 Reconocimiento Pasivo: recon-ng

2. Escaneo y Enumeración

2.1 Introducción a escaneo y enumeración

2.2 Conceptos Básicos

2.3 Descubrimiento de red

2.4 Enumeración de servicios Parte_01

2.5 Enumeración de Servicios Parte_02

2.6 Análisis de Vulnerabilidades

2.7 Ejercicio Resuelto

3. Exploiting

3.1 Introducción

3.1.1 Introducción a la explotación

3.2 Conceptos básicos

3.2.1 Conceptos básicos: vectores de ataque, tipos de exploits

3.3 Payloads

3.3.1 Payloads

3.3.2 Payloads: Msfvenom

3.4 Metasploit

3.4.1 Metasploit

3.4.2 Metasploit: Uso básico

3.4.3 Metasploit: Meterpreter

3.5 Mimikatz

3.5.1 Mimikatz

3.6 Explotación de vulnerabilidades

3.6.1 BOF- Conceptos previos

3.6.2 Minishare: Fuzzing

3.6.3 Minishare: ControlEIP

3.6.4 Minishare: BADCHARS-BUFFERSIZE

3.6.5 Minishare: Shellcode_Explotación

3.7 BadBlue