Universidad de Navarra

Ciberseguridad (Ing.Gr.)
Guía docente 2025-26

PRESENTACIÓN

Breve descripción:

Titulación (Módulo/Materia):

- Ingeniería en Sistemas de telecomunicación (Bloque Especializado de Sistemas de Telecomunicación/Redes y Sistemas)

Detalles:

- **ECTS**: 4 ECTS
- **Curso, semestre**: 4.º curso, 1.º semestre
- **Carácter**: Obligatorio
- **Idioma**: Castellano

Profesores de la asignatura:

- Arrizabalaga Juaristi, Saioa / Profesor colaborador
- Añorga Benito, Javier / Profesor invitado
- Figueroa Lorenzo, Santiago / Invitado

RESULTADOS DE APRENDIZAJE (Competencias)

INGENIERÍA EN SISTEMAS DE TELECOMUNICACIÓN

CG3 - Conocimiento de materias básicas y tecnologías, que le capacite para el aprendizaje de nuevos métodos y tecnologías, así como que le dote de una gran versatilidad para adaptarse a nuevas situaciones.

CG9 - Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con las telecomunicaciones y la electrónica.

CE22 - Capacidad para aplicar las técnicas en que se basan las redes, servicios y aplicaciones de telecomunicación tanto en entornos fijos como móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía, radiodifusión, televisión y datos, desde el punto de vista de los sistemas de transmisión.

CE17 - Conocimiento y utilización de los conceptos de arquitectura de red, protocolos e interfaces de comunicaciones.

PROGRAMA

1. Introduction and basic concepts

2. Cryptography
    1. Symmetric and asymmetric encryption.
    2. Digital certificate and key Exchange
3. Network architecture and Linux OS
4. Threats and malware
5. Information gathering and enumeration
6. Attack automation frameworks and other tools
7. Web application security
8. Wireless security
9. Master Class David Souto Rial
10. Capture the Flag (CTF)

PROGRAM

1. Introduction and basic concepts

2. Cryptography

2.1 Symmetric encryption

2.2 Asymmetric encryption and uses of public-private key

3. Threats and malware

4. Network architecture and Linux

5. Information gathering and enumeration

6. Attack automation and other tools

7. Web application security

8. Capture the Flag exercises

ACTIVIDADES FORMATIVAS

- Clases teóricas (criptografía)
- Laboratorios de ciberseguridad "hacking"
- Master Class David Souto Rial

EVALUACIÓN

CONVOCATORIA ORDINARIA

La evaluación consistirá en:

- Examen parcial criptografía (4 puntos): tentativo 10 octubre.

- Práctica evaluada (1 punto): práctica tipo "capture the flag (CTF)" .

- Examen final (5 puntos): preguntas teóricas y prácticas sobre el contenido visto en clase.

Universidad de Navarra

Criterio de paso de la asignatura: Será necesario aprobar todas las partes para poder pasar el curso completo.

CONVOCATORIA EXTRAORDINARIA

La convocatoria Extraordinaria constará de:

- Examen parcial criptografía (4 puntos)

- Práctica evaluada (1 punto): práctica tipo "capture the flag (CTF)" : proveniente de los puntos obtenidos de la convocatoria ordinaria. En caso de estar suspendido o querer optar nuevamente a estos puntos, se incluirán de forma teórico-práctica en el el Examen final de la convocatoria extraordinaria.

- Examen final (5 puntos + otros puntos (ver apartados anteriores)): preguntas teóricas y prácticas sobre el contenido visto en clase.

Se guardarán los puntos obtenidos en trabajos o exámenes parciales anteriores si así lo desea el alumno, pudiendo optar solamente a los exámenes suspendidos en Convocatoria Ordinaria, siempre y cuando quede finalmente cumplido el "Criterio de paso de la asignatura".

- Será necesario aprobar todas las partes para poder pasar el curso completo.

HORARIOS DE ATENCIÓN

Se acordará cita mediante correo electrónico previo a los profesores (janorga@external.unav.es, sfigueroa@ceit.es)

BIBLIOGRAFÍA