



UNIVERSITÀ DI PISA NETWORK SECURITY

ROSARIO GIUSEPPE GARROPPO

Anno accademico	2023/24
CdS	CYBERSECURITY
Codice	933II
CFU	9

Moduli	Settore/i	Tipo	Ore	Docente/i
NETWORK SECURITY	ING-INF/03	LEZIONI	72	ROSARIO GIUSEPPE GARROPPO MICHELE PAGANO

Obiettivi di apprendimento

Conoscenze

Al completamento del corso, lo studente sarà in grado di dimostrare una conoscenza avanzata degli aspetti scientifici e tecnologici relativi alla sicurezza nelle reti e le soluzioni allo stato dell'arte per la progettazione, realizzazione, verifica e manutenzione di reti sicure e protette. Inoltre, lo studente sarà in grado di aggiornare le proprie conoscenze anche attingendo a pubblicazioni scientifiche e standard nell'ambito della sicurezza nelle reti, oltre a saper progettare e valutare soluzioni innovative.

Modalità di verifica delle conoscenze

Lo studente sarà valutato sulla sua capacità di discutere i contenuti del corso usando la terminologia appropriata e di mettere in pratica, con una consapevolezza critica, le attività illustrate durante il corso.

Capacità

Lo studente avrà le conoscenze necessarie per progettare una rete sicura.

Lo studente sarà in grado di valutare in modo critico il livello di sicurezza di un'infrastruttura di rete.

Lo studente conoscerà i servizi di sicurezza definiti negli standard delle tecnologie di rete più comuni.

Modalità di verifica delle capacità

Le capacità saranno verificate principalmente in sede di esame orale in cui lo studente dovrà dimostrare di avere acquisito la capacità di discutere i contenuti del corso usando la terminologia appropriata e di mettere in pratica le attività illustrate.

Comportamenti

Lo studente potrà acquisire e sviluppare sensibilità alle problematiche tecniche relative alla sicurezza nelle reti.

Lo studente potrà acquisire sensibilità sui diversi livelli di sicurezza offerte dalle differenti tecnologie di rete.

Lo studente potrà sviluppare la sensibilità per i diversi aspetti tecnici ed economici da considerare nella fase di progetto di una rete con un determinato livello di sicurezza.

Modalità di verifica dei comportamenti

In seguito alle diverse attività saranno richieste agli studenti delle brevi relazioni orali concernenti gli argomenti trattati.

Prerequisiti (conoscenze iniziali)

Conoscenza generale di una rete di telecomunicazioni e delle nozioni base sul funzionamento di Internet.

Principi fondamentali delle reti wireless

Indicazioni metodologiche

Le lezioni sono erogate in presenza con l'ausilio della proiezione di diapositive. Saranno inoltre svolte attività di laboratorio per approfondimento sugli argomenti trattati.

Programma (contenuti dell'insegnamento)

Principi fondamentali di progettazione della sicurezza, modello di sicurezza della rete, distribuzione delle chiavi e autenticazione dell'utente,



UNIVERSITÀ DI PISA

sistemi di Network Access Control, Extensible Authentication Protocol, lo standard IEEE 802.1X Port-Based Network Access Control
Minacce e contromisure di sicurezza a livello IP, protocollo IPSec, Internet Key Exchange (IKE), Transport-Level Security (TLS), attacchi a SSL/TLS, TLSv1.3, cenni sulla sicurezza nell'e-mail, sicurezza del DNS e DNSSEC

Sistemi di Intrusion Detection, cenni su tecniche di Statistical Anomaly Detection, Rule-Based Intrusion Detection, rilevamento delle intrusioni distribuite, caratteristiche dei firewall e criteri di accesso, tipi di firewall, posizione e configurazioni del firewall, reti DMZ, reti private virtuali, firewall distribuiti

Sicurezza della rete wireless: minacce e contromisure, le reti wireless LAN IEEE 802.11, lo standard IEEE 802.11i Wireless LAN Security, il programma di certificazione WPA2 e WPA3. Sicurezza nelle reti radiomobili: GSM/GPRS, UMTS, LTE e 5G, servizi e procedure di sicurezza, architettura di sicurezza 5G in 3GPP, minacce e contromisure nei sistemi LTE e 5G.

Sicurezza e privacy nelle reti per servizi IoT, Sicurezza tradizionale verso sicurezza Lightweight, Sicurezza nelle tecnologie di comunicazione wireless di IoT.

Bibliografia e materiale didattico

I testi suggeriti sono:

W. Stallings, Network security essentials: applications and standards, 6th ed., Ed. Pearson, 2017

Penttinen, Jyrki T. J., 5G explained: security and deployment of advanced mobile communications, ed. Wiley, 2019

Glen D. Singh, The Ultimate Kali Linux Book - Second Edition, Ed. Packt Publisher, January 2022

Inoltre, saranno forniti dal docente articoli scientifici su argomenti specifici del corso.

Indicazioni per non frequentanti

Viene rilasciato tutto il materiale (slide, appunti, riferimenti bibliografici, etc.) del corso attraverso la relativa pagina web. Inoltre, il docente rimane a disposizione per chiarimenti sui diversi argomenti trattati a lezione.

Modalità d'esame

Esame Orale con presentazione di un progetto su un argomento del corso.

Ultimo aggiornamento 03/08/2023 09:30