UNIVERSITÀ DI PISA

SICUREZZA DI SISTEMI ICT

FABRIZIO BAIARDI

Anno accademico	2023/24
CdS	INFORMATICA
Codice	563AA
CFU	6

Moduli	Settore/i	Tipo	Ore	Docente/i
SICUREZZA DI SISTEMI ICT	INF/01	LEZIONI	48	FABRIZIO BAIARDI

Obiettivi di apprendimento

Conoscenze

Confidenzialità, Integrità e Disponibilità ed altre proprietà di sicurezza
Politica di sicurezza /Rischio
Vulnerabilità
Attacchi
Contromisure
tipi di vulnerabilità
ranking vulnerabilità
scoperta di vulnerabilità
tipi di attacco / esempi
attacchi automatizzabili
mitre attack framework
Autenticazione
Access control
Firewalling
Intrusion detection
Encryption & VPN
Robustezza e Resilienza

Modalità di verifica delle conoscenze

Valutazione di uno strumento di sicurezza
Presentazione di un problema di sicurezza e possibili soluzioni

Capacità

Come progettare un sistema resiliente
Design for least privilege
Design for robustness
Design for resilience
Design for recovery
Against denial of service attacks
Design for privacy

Modalità di verifica delle capacità

Valutazione di uno strumento di sicurezza
Presentazione di un problema di sicurezza e possibili soluzioni

Comportamenti

Etica della sicurezza
Etica del penetration tester
Vulnerability disclosure

UNIVERSITÀ DI PISA

Modalità di verifica dei comportamenti
Impossibile nell'accademia

Prerequisiti (conoscenze iniziali)
Sistemi operativi
Reti
Programmazione

Programma (contenuti dell'insegnamento)

1. Introduzione e terminologia 6 ore
    - Cia 1
    - Politica di sicurezza /Rischio 1
    - Vulnerabilità 1
        - Locali
        - Di sistema
    - Attacchi
        - Semplici 1
        - Complessi
        - Nozione di attack path
            - Path 1
            - Attack surface
        - Contromisure 1
            - Statiche
            - Dinamiche

1. Vulnerabilità & attacchi 17 ore
    - tipi di vulnerabilità 1
    - ranking vulnerabilità 2
    - scoperta di vulnerabilità
        - analisi statiche 1
        - fuzzing 2
        - scanning + fingerprinting 2
        - confusion matrix 1
    - esempi di attacco 2
    - attacchi automatizzabili 2
    - mitre attack framework 2
2. Contromisure 15 ore
    - Autenticazione 2
        - MFA 1
        - Zero trust 2
    - Access control 4
    - Firewalling 2
    - Intrusion detection 2
    - Encryption & VPN 2
3. Strategie di progetto 10 ore
    - Design for least privilege 2
    - Design for robustness 2
    - Design for resilience 2
    - Design for recovery 2
    - Against denial of service attacks 2
    - Design for privacy 2

Bibliografia e materiale didattico
Materiale fornito dal docente
Security Engineering Ross Anderson una qualunque edizione

Indicazioni per non frequentanti
Frequentare vengono comunque rese disponibili le registrazioni del corso

Modalità d'esame
vedi modalità di verifica

Ultimo aggiornamento 31/07/2023 14:24