Insegnamento: Cyber Security (6 CFU, SSD INF/01))

docente: prof. Aniello Castiglione

Obiettivi

Lo scopo principale del corso è quello di dare un concreto assetto teorico/metodologico nell'ambito della Cybersecurity al fine di fornire architetture, strumenti e metodologie utili a supporto dei vari aspetti della sicurezza logica dei sistemi informatici attualmente disponibili nei vari scenari operativi quali ad esempio IoT, smartphone, cloud, ecc..
CONOSCENZA E CAPACITA' DI COMPRENSIONE:
Lo studente deve dimostrare di conoscere e saper comprendere i concetti e le metodologie di base per la rilevazione dei rischi e per la protezione dei sistemi software. Egli deve inoltre dimostrare di conoscere e saper comprendere le nozioni, le tecniche e i risultati principali di Crittografia moderna. A seguito del corso, lo studente acquisirà padronanza con i principali temi di Network Security tra cui firewalling, anomaly detection, steganography, honeypot, social network reverse engineering. Ulteriore capacità che si intende trasferire allo studente è quella di fornire modelli organizzativi e aspetti legislativi basilari da utilizzare nei contesti del Cloud Computing, Edge Computing, Fog Computing, principalmente in mobile ed IoT.
CAPACITA' DI APPLICARE CONOSCENZA E COMPRENSIONE: Lo studente deve dimostrare di saper applicare metodi e strumenti per la rilevazione dei rischi e per la protezione dei sistemi software a determinati contesti d'uso o ambienti operativi, come indicato dal docente. Lo studente deve inoltre dimostrare di saper realizzare script Bash e Python che implementano alcuni dei metodi e strumenti introdotti nella teoria. Dopo aver seguito il corso, ciascun studente saprà calare i principi fondamentali della Data Security ai contesti di networking più recenti (Cloud Computing, Edge Computing, Fog Computing, IoT) riuscendo a valutare ed arginare i rischi a cui tali contesti sono attualmente soggetti facendo predisporre adeguate contromisure.
AUTONOMIA DI GIUDIZIO: Lo studente deve essere in grado di sapere valutare e interpretare in maniera autonoma i risultati di una analisi per la rilevazione dei rischi e la correttezza di enunciati e ragionamenti di tipo logico-matematico utilizzati in Crittografia. Egli inoltre deve essere in grado di valutare e interpretare la correttezza e sicurezza di script e moduli sviluppati in Bash e Python. Infine, lo studente sarà in grado di effettuare le attività di Vulnerability Assessment di una Infrastruttura Critica valutandone i risultati ottenuti al fine di suggerire agli stakeholder le giuste attività da intraprendere per ridurre i rischi che la minacciano.
ABILITA' COMUNICATIVE: Lo studente deve essere in grado di redigere una relazione di presentazione di un algoritmo, protocollo o altro sistema di Sicurezza Informatica, anche lavorando in gruppo, servendosi di strumenti avanzati di scrittura/documentazione e usando correttamente la terminologia di base dell'Informatica, anche in lingua inglese. Ulteriore capacità sarà quella di riuscire ad argomentare su problematiche di sicurezza anche tra loro disomogenee o completamente nuove da quelle presentate al corso.
CAPACITA' DI APPRENDIMENTO: Lo studente deve essere in grado di aggiornarsi e approfondire in modo autonomo argomenti e applicazioni specifiche della Cybersecurity, anche accedendo a banche dati, repository on-line di articoli scientifici e altre modalità messe a disposizione dalla rete. Inoltre, verrà considerata molto positivamente ogni attività che lo studente deciderà di approfondire in modo autonomo ed al di fuori dal materiale formativo già fornito dal docente.

Prerequisiti

Pur non essendoci dei prerequisiti formali, per poter comprendere al meglio i contenuti del corso è preferibile avere acquisito le conoscenze e le competenze trasmesse dai corsi di "Sistemi Operativi", "Laboratorio di Sistemi Operativi", "Reti di Calcolatori" e "Laboratorio di Reti di Calcolatori". Inoltre, è preferibile che lo studente abbia una discreta conoscenza delle basi di Crittografia, in modo specifico per quanto attiene alla parte relativa alla Teoria della Complessità ("Algoritmi e Strutture Dati") e della Legge dei Grandi Numeri ("Matematica I"). Infine, considerato che i libri di testo sono tutti in lingua Inglese, sarà di aiuto per la comprensione durante lo studio una discreta conoscenza della lingua Inglese (specialmente per la interpretazione e la lettura di termini tecnici).

Contenuti

Il corso fornisce sia una introduzione ai problemi realtivi alla Cybersecurity che ai principali algoritmi e tecniche di programmazione per la protezione dei dati, dei sistemi software e degli apparati di comunicazione. Una parte del corso sarà svolta in maniera frontale ed un'altra in Laboratorio dove verranno mostrati strumenti software a supporto del corso.

Modalità di Verifica dell'apprendimento

Lo scopo dell'attività di verifica consiste nel misurare il livello di raggiungimento degli obiettivi formativi elencati in precedenza. Il processo di verifica tende a valutare il raggiungimento di alcune capacità specifiche dell'insegnamento.

Nel dettaglio, ci sarà una verifica progressiva dell'apprendimento tenendo conto dei risultati delle attività assegnate da svolgere a casa, della partecipazione che lo studente avrà in classe ed infine la prova finale in classe. In questo modo si verificherà la capacità dello studente di apprendere singolarmente. Inoltre, l'attività del progetto di gruppo verificherà la capacità di lavorare in team e la preparazione di una relazione tecnica. La fase del progetto di gruppo tenderà a verificare questo ultima capacità.
La valutazione finale deriva dalle seguenti parti: (CA) partecipazione in classe (10% del voto), (HA) attività da fare a casa (20% del voto), (IP) presentazione in classe di un progetto di gruppo in cui il gruppo è formato da 2-3 persone (30% del voto), ed infine, (IE) un esame in classe (40% del voto).
In sintesi il voto finale è dato da voto_finale = 0.1*CA + 0.2*HA + 0.3*IP + 0.4*IE.

Testi di Riferimento

[SiC] C. P. Pfleeger, S. L. Pfleeger, J. Margulies: "Security in Computing, 5th Edition", Prentice Hall, 2015, ISBN: 978-0-13408-505-0
[GCAC] D. Boneh, V. Shoup: "A Graduate Course in Applied Cryptography", 2017, FREE BOOK, https://cryptobook.us/
[ANP] J Forshaw: "Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation", No Starch Press, 2018, ISBN: 978-1-59327-750-5
[SC] J.-P. Aumasson: "Serious Cryptography: A Practical Introduction to Modern Encryption", No Starch Press, 2018, ISBN: 978-1-59327-826-7
[CADS] Y. Diogenes, E. Ozkaya: "Cybersecurity – Attack and Defense Strategies", Packt Publishing, 2018, ISBN: 978-1-78847-529-7
[LBH] OccupyTheWeb: "Linux Basics For Hackers: Getting Started with Networking, Scripting, and Security in Kali", No Starch Press, 2019, ISBN: 978-1-59327-855-7

Altre Informazioni

Il materiale didattico è disponibile solo in lingua Inglese sulla piattaforma di e-learning.