Logo Image not found or type unknown

PROGRAMMA DEL CORSO DI CYBERSECURITY

SETTORE SCIENTIFICO

ING-INF/05

CFU

9

OBIETTIVI FORMATIVI PER IL RAGGIUNGIMENTO DEI RISULTATI DI APPRENDIMENTO PREVISTI

/**/
Il corso ha l'obiettivo di presentare i fondamenti della cybersecurity e delle su declinazioni sia da un punto di vista preventivo, andando a presentare le policy e gli applicativi utili per la protezione delle infrastrutture informatiche, sia da un punto di vista più attivo andando a analizzare e a comprendere il funzionamento di tutte le componenti digitali che vengono attivamente utilizzate per l'ingresso abusivo o il danneggiamento dei sistemi informatici. Si presenterà inoltre come gli attuali sviluppi dell'intelligenza artificiale possano potenziare questo genere di attacchi e come invece possano essere utilizzati per proteggere le reti e i terminali informatici con modalità più efficienti.

RISULTATI DI APPRENDIMENTO ATTESI

/**/
Conoscenza e capacità di comprensione

Lo studente al termine del corso avrà conoscenza delle problematiche inerenti alla sicurezza informatica. In particolare lo studente sarà in grado di analizzare i più comuni attacchi informatici moderni e di identificare e comprendere le implicazioni della cyber security e delle violazioni dei dati su sistemi informatici.

Capacità di applicare conoscenza e comprensione

Lo studente, partendo dalla conoscenza di che cos'è il cyber security e ciò che esso comporta a livello di violazione dei dati, sarà in grado di identificare la migliore soluzione per il sistema informatico oggetto di studio. Dimostreranno competenza nell'identificare le soluzioni più adatte per affrontare le minacce attuali alla sicurezza informatica, incluse le minacce basate sull'intelligenza artificiale (AI), quali adversarial attacks e malware generato da AI.

Autonomia di giudizio

Lo studente dimostrerà la capacità di analizzare criticamente situazioni complesse relative alla sicurezza informatica. Utilizzando una comprensione approfondita del contesto, sarà in grado di valutare le opzioni disponibili e prendere decisioni informate per migliorare efficacemente il livello di sicurezza dei sistemi informatici. Questo include l'autonomia nella gestione, definizione e nell'attuazione di strategie di difesa avanzate, consentendo agli studenti di adottare un approccio proattivo e informato nella protezione delle risorse digitali.

Abilità comunicative

Lo studente svilupperà la capacità di comunicare in modo chiaro ed efficace, esprimendo concetti e problematiche legate alla sicurezza informatica. Sarà in grado di condurre conversazioni su argomenti quali la sicurezza informatica, il terrorismo informatico, gli attacchi ai modelli di machine learning e le soluzioni più efficaci e comuni. Questa competenza consentirà di comunicare in modo informato, sia tra i colleghi che con le parti interessate esterne, contribuendo così a una migliore comprensione e gestione dei rischi informatici.

Capacità di apprendimento

Lo studente sarà in grado di comprendere e affrontare le sfide della sicurezza informatica, acquisendo una solida base di conoscenze su attacchi e difese informatiche e la capacità di continuare ad apprendere e adattarsi alle nuove minacce emergenti.

Programma didattico

Programma didattico (per macro aree + numero lezioni previste)

1. Protocolli di Autenticazione Remota (lezioni previste n. 9)
2. Sicurezza del Livello di Trasporto (lezioni previste n. 9)
3. Sicurezza delle Reti Wireless (lezioni previste n. 9)
4. Modelli di Intelligenza Artificiale per la Cybersecurity (lezioni previste n. 9)
5. Adversarial Attacks nel Machine Learning (lezioni previste n. 9)
6. Malware: Virus informatici, Worm, Trojan, Ransomware, Spyware, Adware, Scareware. (lezioni previste n. 9)

Modalità di raccordo con altri insegnamenti (indicare le modalità e gli insegnamenti con i quali sarà necessario raccordarsi)

Nessun raccordo

MODALITÀ DI ESAME ED EVENTUALI VERIFICHE DI PROFITTO IN ITINERE

L’esame può essere sostenuto sia in forma scritta che in forma orale.

L’esame orale consiste in un colloquio nel corso del quale il docente formula di solito tre domande. L’esame scritto consiste nello svolgimento di un test con 31 domande. Per ogni domanda lo studente deve scegliere una di 4 possibili risposte. Solo una risposta è corretta.

Sia le domande orali che le domande scritte sono formulate per valutare sia il grado di comprensione delle nozioni teoriche sia la capacità di ragionare utilizzando tali nozioni. Le domande sulle nozioni teoriche consentiranno di valutare il livello di comprensione. Le domande che richiedono l’elaborazione di un ragionamento consentiranno di valutare il livello di competenza e l’autonomia di giudizio maturati dallo studente.

Le abilità di comunicazione e la capacità di apprendimento saranno valutate attraverso le interazioni dirette tra docente e studente che avranno luogo durante la fruizione del corso (videoconferenze, e-tivity report, studio di casi elaborati) proposti dal docente o dal tutor.

DESCRIMODALITÀ DI ISCRIZIONE E DI GESTIONE DEI RAPPORTI CON GLI STUDENTI ZIONE

/**/
L'iscrizione ed i rapporti con gli studenti sono gestiti mediante la piattaforma informatica che permette l'iscrizione ai corsi, la fruizione delle lezioni, la partecipazione a forum e tutoraggi, il download del materiale didattico e la comunicazione con il docente.

Un tutor assisterà gli studenti nello svolgimento di queste attività.

Attività di didattica erogativa (DE) 54 Videolezioni + 54 test di autovalutazione

Impegno totale stimato: 54 ore.

Attività di didattica interattiva (DI) ed e-tivity con relativo feed-back al singolo studente da parte del docente o del tutor Redazione di un elaborato

Partecipazione a una web conference

Svolgimento delle prove in itinere con feedback

Svolgimento della simulazione del test finale, Totale 9 ore.

Attività di autoapprendimento 162 ore per lo studio individuale.

Libro di riferimento Dispense del docente.

LEZIONI

1 - Panorama delle minacce cibernetiche

2 - Impatto delle minacce cibernetiche sulla società

3 - Panorama delle minacce cibernetiche Le infrastrutture critiche

4 - Attacchi alle supply chain

5 - Il crimine informatico

6 - Principali modelli alla base del cybercrime

7 - Information Warfare concetti chiave

8 - Information Warfare Casi reali di cyber war

9 - Cybercrime

10 - Cyberpedofilia

11 - I Criminali Informatici

12 - Malware-as-a-Service

13 - Approccio degli stati alle minacce cibernetiche

14 - La diplomazia nel cyberspazio

15 - Tipologie di Web

16 - Approfondimento sulla Sicurezza nelle reti P2P

17 - Deep e Dark Web

18 - Modelli di servizi basati sul cybercrime

19 - Cyber Threat Intelligence

20 - Intelligence

21 - Cyber threat intelligence e threat detection

22 - CTI Maturity Model

23 - Standard STIX/TAXII

24 - MISP e TIP

25 - OSINT

26 - CTI report e Bad Rabbit

27 - IPS

28 - Cyber threat intelligence e threat detection

29 - SOC

30 - CSIRT

31 - XDR - Extended detection and response (AGGER)

32 - Introduzione alla Incident Response

33 - Il processo di Incident Response del NIST

34 - Forensic Tools

35 - Playbooks

36 - I Framework del MITRE

37 - La difesa Attiva

38 - Threat Actors

39 - Basi di Offensive Security e Ethical Hacking

40 - Tecniche di Hacking Information Gathering

41 - Tecniche di Hacking - Scanning / Enumeration

42 - Tecniche di Hacking System Hacking

43 - Tecniche di Hacking Maintaining Access

44 - Tecniche di Hacking House Keeping

45 - Tecniche di Hacking Tecniche e Strumenti di Enumerazione

46 - Tecniche di Hacking Vulnerability Management

47 - Tecniche di Hacking Web application hacking

48 - Tecniche di Hacking - Network Attack

49 - Tecniche di Hacking Post-Exploitation e Maintaining Access

50 - Tecniche di Hacking Maintaining Access

51 - Reconnaissance e Footprinting

52 - Scanning

53 - Enumeration

54 - Strategie di Difesa nel Cyber-Reconnaissance e Footprinting Il/La docente si riserva il diritto di modificare l'elenco delle lezioni