UNIVERSITÀ DEGLI STUDI LINK

CORSO DI LAUREA

A.A. 2023/2024

Insegnamento	Programming (Mutuato da Sicurezza Informatica)
CFU	6
Anno di corso	
Semestre	primo
Docente/i	Prof. Marco Angelini
e-mail	m.angelini@unilink.it
ricevimento	al termine delle lezioni o per appuntamento da concordare tramite e-mail

RISULTATI DI APPRENDIMENTO

L'insegnamento ha l'obiettivo di far conseguire i seguenti risultati di apprendimento:

1. **CONOSCENZA E CAPACITÀ DI COMPRENSIONE**: la/o studente dovrà essere in grado di apprendere e riconoscere i principi fondamentali della sicurezza informatica, le grandezze che la caratterizzano, le principali caratteristiche degli attaccanti informatici, degli attacchi, delle vulnerabilità informatiche, dei malware. Dovrà ulteriormente apprendere i principi di una corretta difesa cibernetica e le principali tecniche ed attori necessari ad implementare una postura di sicurezza informatica adeguata.
2. **CONOSCENZA E CAPACITÀ DI COMPRENSIONE APPLICATE**: alla fine del corso, la/o studente dovrà essere in grado di valutare la pericolosità di una minaccia informatica, estrarre informazioni dai database di vulnerabilità pubblici e saperle interpretare, riconoscere e ragionare su azioni di riduzione della superficie di esposizione alle minacce al fine di implementare una corretta postura cyber
3. **AUTONOMIA DI GIUDIZIO**: la/o studente dovrà acquisire una visione critica e analitica sugli aspetti fondamentali ed i principi di sicurezza informatica, ed essere in grado di saper valutare correttamente la superficie di minaccia e l'esposizione alla stessa, individuando azioni correttive di alto livello necessarie ad informare implementazioni tecniche.
4. **ABILITÀ COMUNICATIVE**: la/o studente dovrà altresì acquisire la padronanza del linguaggio specialistico della materia e maturare la capacità di argomentare sia con personale tecnico che con personale adibito alle scelte decisionali in materia di postura cyber.
5. **ABILITÀ AD APPRENDERE**: la/o studente dovrà dimostrare valutare correttamente la superficie di minaccia e l'esposizione alla stessa, individuando azioni correttive di alto livello necessarie ad informare implementazioni tecniche

PROGRAMMA DETTAGLIATO

Il corso affronta, nel dettaglio, i seguenti temi:

1. Introduzione alla sicurezza informatica
2. Concetti fondamentali di sicurezza informatica
3. La triade CIA
4. La triade CIA: aspetti avanzati
5. Autenticazione
6. Autenticazione multi-fattore
7. Vulnerabilità informatiche
8. Repository di vulnerabilità pubblici e sistemi di scoring

9. Esempi di attacchi informatici
10. Attori e attaccanti coinvolti in attacchi informatici
11. I malware
12. Malware avanzati e APT
13. Autorizzazione e controllo accessi
14. Hardening: principi fondamentali
15. Hardening: misure
16. Tipologie di attacchi informatici
17. Modellazione di attacchi informatici
18. Reazione ad attacchi informatici, SOC e CERT

EVENTUALI PROPEDEUTICITÀ CONSIGLIATE

nessuna

MODALITÀ DI SVOLGIMENTO DELL'ESAME

L'esame finale consiste nella produzione di un elaborato scritto su un tema scelto tra gli argomenti del corso ed in un colloquio orale che presenti lo stesso e permetta di rispondere ad una serie di quesiti sull'elaborato e gli argomenti del corso

CRITERI DI VALUTAZIONE

Nel colloquio orale la/o studente dovrà dimostrare:

1. **CONOSCENZA E CAPACITÀ DI COMPRENSIONE**: di aver acquisito le nozioni fondamentali della sicurezza informatica su tutti i temi trattati nel corso.
2. **CONOSCENZA E CAPACITÀ DI COMPRENSIONE APPLICATE**: la propria capacità di applicare le nozioni fondamentali della sicurezza informatica su tutti i temi trattati nel corso.
3. **AUTONOMIA DI GIUDIZIO**: di aver maturato una capacità di valutazione ed applicazione dele nozioni fondamentali della sicurezza informatica su tutti i temi trattati nel corso.
4. **ABILITÀ COMUNICATIVE**: di avere padronanza nella comunicazione degli aspetti di sicurezza informatica trattati nel corso e del loro gergo tecnico.
5. **ABILITÀ AD APPRENDERE**: la propria capacità di utilizzare gli strumenti concettuali e metodologici acquisiti inerenti le nozioni fondamentali della sicurezza informatica sui tutti i temi trattati nel corso.

CRITERI DI ATTRIBUZIONE DEL VOTO FINALE

Il voto si attribuisce in trentesimi. Nell'attribuzione del voto finale si terrà conto:

1. per il 50%, dell'elaborato scritto prodotto per l'esame
2. per il 25%, nell'esposizione dell'elaborato scritto e la capacità di rispondere alle domande
3. per il 25%, nella capacità di rispondere a domande orali inerenti gli argomenti del corso.

MATERIALE DIDATTICO

Per la preparazione dell'esame, è fondamentale integrare i contenuti forniti durante le lezioni con i seguenti **testi obbligatori**:

non sono previsti testi obbligatori. E' consigliato il testo:
Sicurezza in informatica di Charles P. Pfleeger, Shari L. Pfleeger, Pearson
•Collana: Prentice Hall
•Edizione: 2
•Data di Pubblicazione: 1 gennaio 2008 •EAN: 9788871923635
•ISBN: 8871923634
•Pagine: XXVII-767
•Formato: brossura
•Ean altre edizioni: 9788871921976

La/o studente **non frequentante** dovrà altresì studiare il seguente testo obbligatorio: ...

CONSIGLI DEL DOCENTE

Seguire le lezioni, studiare il materiale didattico fornito ed integrare con fonti esterne o il libro consigliato.