

PROGRAMMA DEL CORSO DI SICUREZZA INFORMATICA

SETTORE SCIENTIFICO

ING-INF/05

CFU

6

OBIETTIVI FORMATIVI PER IL RAGGIUNGIMENTO DEI RISULTATI DI APPRENDIMENTO PREVISTI

Il corso intende fornire gli strumenti per dare informazioni adeguate in merito ai rischi che ogni utente corre relativamente alla sicurezza delle informazioni su supporti informatici e spiegare con esempi pratici le modalità da adottare per garantire la sicurezza informatica dei propri dati.

RISULTATI DI APPRENDIMENTO ATTESI

Conoscenza e capacità di comprensione.

Lo studente dovrà acquisire conoscenza e comprensione degli aspetti teorici e pratici della sicurezza di sistemi informativi e della loro difesa da attacchi informatici via rete; conoscenza e comprensione delle tecniche di intrusione e di rilevamento delle intrusioni; conoscenza e classificazione di virus e malware, di tecniche e strumenti per la loro analisi ed individuazione; conoscenza e comprensione di firewall e loro configurazione.

Capacità di applicare conoscenza e comprensione.

Il corso consentirà allo studente di comprendere come installare e gestire soluzioni per la difesa di sistemi informativi in rete; capacità di affrontare attacchi informatici, di applicare le conoscenze acquisite per la prevenzione e la eliminazione di intrusioni, virus e malware con riferimento a software, dati e postazioni di lavoro.

Autonomia di giudizio.

Capacità di valutare punti di forza e punti di debolezza di soluzioni, tecniche, strumenti e servizi di sicurezza di sistemi informatici.

Abilità comunicative.

La presentazione dei vari argomenti consentirà allo studente di interagire e comunicare con operatori e fornitori di tecnologie e servizi di sicurezza; capacità di comunicare con l'utente per l'attuazione di comportamenti e politiche per la sicurezza.

Capacità di apprendimento.

La capacità di apprendimento sarà incentivata attraverso la somministrazione di esercitazioni operative, caricate in piattaforma nella sezione elaborati, finalizzata a verificare l'effettiva comprensione degli argomenti trattati. Lo studente acquisirà la di seguire l'evoluzione di virus e malware, di accedere a letteratura e documentazione tecnica di settore, di autoaggiornarsi su nuovi strumenti e tecniche di rilevamento e difesa.

PROGRAMMA DIDATTICO

Ogni Macro-argomento è articolato in 35 video-lezioni da 30 min. corredate da dispense, slide e test di apprendimento.

1. Politiche di sicurezza
2. Tipologie di attacchi informatici
3. Crittografia(a)simmetrica, firme digitali, hash sicuri;
- 4/5. Vulnerabilità e contromisure: Malware, buffer overflow, hostbased Intrusion Detection System
6. Sicurezza dei Sistemi
7. Sicurezza delle reti
8. Servizi di rete; protezione dei servizi di rete
9. Vulnerabilità e contromisure: Intercettazione (sniffing), impersonificazione (spoofing), Denial of Service (DoS), firewall, Virtual Private Network Network-based Intrusion, Detection System.

MODALITÀ DI ESAME ED EVENTUALI VERIFICHE DI PROFITTO IN ITINERE

L'esame può essere sostenuto sia in forma scritta che in forma orale. Gli appelli orali sono previsti nella sola sede centrale di Roma. Gli esami scritti, invece, possono essere sostenuti sia nelle sede centrale che nelle sedi periferiche.

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 ed elaborati proposti dal docente).

ATTIVITÀ DI DIDATTICA EROGATIVA (DE)

- 36 Videolezioni + 36 test di autovalutazione (DE)

Impegno totale stimato: 36 ore

ATTIVITÀ DI DIDATTICA INTERATTIVA (DI)

- Redazione di un elaborato (DI)
- Partecipazione a una web conference
- Svolgimento delle prove in itinere con feedback
- Svolgimento della simulazione del test finale

Totale 6 ore

ATTIVITÀ DI AUTOAPPRENDIMENTO

- 108 ore per lo studio individuale

LIBRO DI RIFERIMENTO

Dispense, testi ed ulteriori materiali didattici saranno indicati e/o caricati sulla piattaforma