PROGRAMMA DEL CORSO DI SICUREZZA DELLE RETI E CYBER SECURITY

SETTORE SCIENTIFICO

ING-INF/03

CFU

6

MODALITÀ DI ESAME ED EVENTUALI VERIFICHE DI PROFITTO IN ITINERE

Lo studente per superare l'esame può scegliere di effettuare l'esame orale presso la sede dell'Ateneo o la prova scritta in tutte le sedi di Italia, ivi compreso Roma.

Il test finale si compone di 31 domande a risposta multipla con 4 possibili risposte.

Le domande di esame siano esse orali o scritte, coerentemente con i risultati di apprendimento attesi, sono finalizzate a misurare la preparazione acquisita in relazione a

- Conoscenza e capacità di comprensione attraverso domande sul programma del corso
- Capacità di applicare conoscenza e comprensione attraverso domande specifiche che consentano la valutazione rispetto a casi concreti
- Autonomia di giudizio attraverso domande che presuppongano la valutazione autonoma in ordine alla scelte da compiere

Gli esercizi e gli elaborati di Didattica erogativa consentono invece di verificare i risultati di apprendimento raggiunti rispetto alle abilità comunicative e alla capacità di apprendimento.

RISULTATI DI APPRENDIMENTO ATTESI

Conoscenza e capacità di comprensione.

Il corso intende fornire le conoscenze utili per comprendere gli strumenti tecnologici adoperati per garantire sicurezza nelle comunicazioni di rete in relazione alle applicazioni e alle funzionalità di sistema.

Conoscere la crittografia e le tecniche fondamentali di cifratura; conoscenza e comprensione delle più diffuse tipologie di attacchi ai sistemi di comunicazione. Conoscenza delle problematiche di sicurezza in reti interconnesse.

Capacità di applicare conoscenza e comprensione.

Il corso trasferisce la capacità di applicare le conoscenze acquisite in processi di accertamento della vulnerabilità delle reti, di verificare e testare l'applicazione di procedure, strumenti e standard di sicurezza.

Autonomia di giudizio

Attraverso le competenze acquisite, lo studente potrà valutare punti di forza e punti di debolezza di soluzioni, tecniche, strumenti e servizi di sicurezza per le comunicazioni in rete.

Abilità comunicative

Lo studente svilupperà la capacità di interagire e comunicare con operatori e fornitori di tecnologie e servizi di sicurezza; capacità di comunicare e discutere in team di progettazione ed implementazione della sicurezza in reti di TLC.

Capacità di apprendimento

La capacità di apprendimento sarà stimolata attraverso la somministrazione di esercitazioni operative, caricate in piattaforma nella sezione elaborati, finalizzata anche a verificare l'effettiva comprensione degli argomenti trattati.

Lo studente acquisirà, inoltre, la capacità di seguire l'evoluzione scientifica e tecnica in ambito cybersecurity, di autoaggiornarsi su standard e procedure, su tecnologie e strumenti, sulla comparsa di nuove tipologie di rischio e di attacco.

OBIETTIVI FORMATIVI PER IL RAGGIUNGIMENTO DEI RISULTATI DI APPRENDIMENTO PREVISTI

Il corso si propone di fornire allo studente le competenze necessarie per comprendere e valutare problematiche di sicurezza informatica nell'ambito di realtà produttive, progettare sistemi informatici e reti con un certo livello di sicurezza, gestire le attività legate alla sicurezza informatica anche in riferimento gli obblighi normativi italiani.

MODALITÀ DI RACCORDO CON ALTRI INSEGNAMENTI (INDICARE LE MODALITÀ E GLI INSEGNAMENTI CON I QUALI SARÀ NECESSARIO RACCORDARSI)

Il corso si raccorda in particolare al corso di sicurezza informatica.

Il raccordo avverrà tramite la preliminare condivisione del programma tra i docenti finalizzata ad evitare duplicazioni/sovrapposizioni del programma ed assicurare la completezza degli argomenti trattati.

MODALITÀ DI ISCRIZIONE E DI GESTIONE DEI RAPPORTI CON GLI STUDENTI

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)

- 36 Videolezioni + 36 test di autovalutazione

Impegno totale stimato: 36 ore

ATTIVITÀ DI DIDATTICA INTERATTIVA (DI)

- Redazione di un elaborato su traccia del docente
- Partecipazione a una web conference
- Svolgimento delle prove in itinere con feedback
- Svolgimento della simulazione del test finale

Impegno totale stimato: 6 ore

ATTIVITÀ DI AUTOAPPRENDIMENTO

- 108 ore per lo studio individuale

LIBRO DI RIFERIMENTO

- “Crittografia e Sicurezza delle Reti” 2/ed., William Stallings, Ed. McGraw-Hill.
- “Cryptography and Network Security”, 7/ed., William Stallings, Pearson.

ACKNOWLEDGEMENTS

Ringraziamenti al Prof. William Stallings e a Pearson per la messa a disposizione del materiale didattico utilizzato per la preparazione di parte di questo corso.

PROGRAMMA DIDATTICO

1 - CONCETTI BASE DI SICUREZZA

2 - SERVIZI E MECCANISMI DI SICUREZZA

3 - CRITTOGRAFIA SIMMETRICA

4 - CRITTOGRAFIA SIMMETRICA: TECNICHE DI SOSTITUZIONE E DI TRASPOSIZIONE

5 - CIFRATURA A BLOCCHI

6 - LA CIFRATURA DES DATA ENCRYPTION STANDARD

7 - LA CIFRATURA AES - ADVANCED ENCRYPTION STANDARD

8 - LA CRITTOGRAFIA MULTIPLA

9 - MODALIT&#65533; DI FUNZIONAMENTO DELLA CIFRATURA A BLOCCHI

10 - SEGRETEZZA E CRITTOGRAFIA SIMMETRICA

11 - CRITTOGRAFIA ASIMMETRICA

12 - L'ALGORITMO RSA

13 - GESTIONE DELLE CHIAVI E SCAMBIO DIFFIE-HELLMAN

14 - AUTENTICAZIONE DEI MESSAGGI

15 - CODICI MAC E FUNZIONI HASH

16 - L'ALGORITMO SHA-512

17 - GLI ALGORITMI HMAC E CMAC

18 - LE FIRME DIGITALI

19 - AUTENTICAZIONE IN AMBIENTI DISTRIBUITI

20 - I CERTIFICATI X.509

21 - SICUREZZA DELLA POSTA ELETTRONICA E PGP

22 - IPSEC

23 - IPSEC E IL PROTOCOLLO ESP

24 - IL PROTOCOLLO SSL

25 - I PROTOCOLLI TLS E HTTPS

26 - SET - SECURE ELECTRONIC TRANSACTION

27 - INTRUSIONI E SOFTWARE DOLOSO

28 - TIPI DI MALWARE E DDOS

29 - I FIREWALL

30 - MULTIMEDIA FORENSICS

31 - MM-FORENSICS: IDENTIFICAZIONE DELLA SORGENTE

32 - MM-FORENSICS: RILEVAZIONE DI FAKE

33 - BLOCKCHAIN E PROOF-OF-WORK

34 - BLOCKCHAIN E IL LEDGER DISTRIBUITO

35 - COMUNICAZIONI ANONIME: I PROTOCOLLI CROWDS E MIX

36 - COMUNICAZIONI ANONIME: TOR E DEEP WEB