Logo Image not found or type unknown

PROGRAMMA DEL CORSO DI SICUREZZA DELLE RETI E CYBER SECURITY

SETTORE SCIENTIFICO

ING-INF/03 (IINF-03/A)

CFU

6

SETTORE SCIENTIFICO DISCIPLINARE

/**/
ING-INF/03

ANNO DI CORSO

/**/
III Anno

TIPOLOGIA DI ATTIVITÀ FORMATIVA

/**/
Base q

Caratterizzante X

Affine q

Altre attività q

NUMERO DI CREDITI

/**/
6 CFU

DOCENTE

Roberto Caldelli

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.

OBIETTIVI FORMATIVI SPECIFICI

/**/
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.

RISULTATI DI APPRENDIMENTO SPECIFICI

/**/
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.

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 - modalità 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

TIPOLOGIE DI ATTIVITÀ DIDATTICHE PREVISTE E RELATIVE MODALITÀ DI SVOLGIMENTO

/**/
Ogni Macro-argomento è articolato in 15-17 videolezioni da 30 min. corredate da dispense, slide e test di apprendimento.

Per ogni insegnamento sono previste sino a 6 videolezioni (n.1 CFU) di didattica innovativa secondo modalità definite dal docente di riferimento.

Le videolezioni sono progettate in modo da fornire allo studente una solida base di competenze culturali, logiche e metodologiche atte a far acquisire capacità critiche necessarie ad esercitare il ragionamento matematico, anche in una prospettiva interdisciplinare, a vantaggio di una visione del diritto non meramente statica e razionale, bensì quale espressione della società e della sua incessante evoluzione.

Il modello didattico adottato prevede sia didattica erogativa (DE) sia didattica interattiva (DI):

La didattica erogativa (DE) prevede l'erogazione in modalità asincrona delle videolezioni, delle dispense, dei test di autovalutazioni predisposti dai docenti titolari dell'insegnamento; la metodologia di insegnamento avviene in teledidattica. La didattica interattiva (DI) comprende il complesso degli interventi didattici interattivi, predisposti dal docente o dal tutor in piattaforma, utili a sviluppare l'apprendimento online con modalità attive e partecipative ed è basata sull'interazione dei discenti con i docenti, attraverso la partecipazione ad attività didattiche online.
Sono previsti interventi brevi effettuati dai corsisti (ad esempio in ambienti di discussione o di collaborazione, in forum, blog, wiki), e-tivity strutturate (individuali o collaborative), sotto forma tipicamente di produzioni di elaborati o esercitazioni online e la partecipazione a web conference interattive.

Nelle suddette attività convergono molteplici strumenti didattici, che agiscono in modo sinergico sul percorso di formazione ed apprendimento dello studente. La partecipazione attiva alle suddette attività ha come obiettivo quello di stimolare gli studenti lungo tutto il percorso didattico e garantisce loro la possibilità di ottenere una valutazione aggiuntiva che si sommerà alla valutazione dell'esame finale.

Per le attività di autoapprendimento sono previste 108 ore di studio individuale.

L'Ateneo prevede 7 h per ogni CFU articolate in 6 h di didattica erogativa (DE) e 1 h di didattica interattiva (DI).

Nel computo delle ore della DI sono escluse le interazioni a carattere orientativo sui programmi, sul cds, sull'uso della piattaforma e simili, che rientrano un semplice tutoraggio di orientamento. Sono altresì escluse le ore di tutorato didattico disciplinare, cioè la mera ripetizione di contenuti già proposti nella forma erogativa attraverso colloqui di recupero o approfondimento one-to-one.

MODALITÀ E CRITERI DI VALUTAZIONE DELL'APPRENDIMENTO

/**/
La partecipazione alla didattica interattiva (DI) ha la finalità, tra le altre, di valutare lo studente durante l'apprendimento in itinere.

L'esame finale può essere sostenuto in forma scritta o in forma orale; lo studente può individuare, in autonomia, la modalità di svolgimento della prova, sempre rispettando la calendarizzazione predisposta dall'Ateneo.

L'esame orale consiste in un colloquio nel corso del quale il docente formula almeno tre domande.

L'esame scritto consiste nello svolgimento di un test a risposta multipla con 31 domande. Per ogni domanda lo studente deve scegliere una delle 4 possibili risposte. Solo una risposta è corretta.

Sia i quesiti in forma orale che i quesiti in forma scritta sono formulati per valutare il grado di comprensione delle nozioni teoriche e la capacità di sviluppare il ragionamento utilizzando le nozioni acquisite. I quesiti 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.

CRITERI DI MISURAZIONE DELL'APPRENDIMENTO E ATTRIBUZIONE DEL VOTO FINALE

/**/
Sia lo svolgimento dell'elaborato, sia la presenza attiva durante le web conference prevedono un giudizio, da parte del docente, fino a un massimo di 2 punti. Lo studente può prendere parte ad entrambe le attività ma la votazione massima raggiungibile è sempre di 2 punti.

La valutazione proveniente dallo sviluppo dell'elaborato può essere pari a 0, 1 o 2 punti.

La valutazione derivante dalle web conference è strutturata tramite lo svolgimento, al termine della stessa, di un test finale a risposta multipla che può garantire da 0 a 1 punto.

È data facoltà allo studente di partecipare o meno alla didattica interattiva.

La valutazione finale ha lo scopo di misurare il raggiungimento degli obiettivi di apprendimento definiti alla base dell'insegnamento. Il giudizio riguarda l'intero percorso formativo del singolo insegnamento ed è di tipo sommativo. Il voto finale dell'esame di profitto tiene conto del punteggio che lo studente può aver ottenuto partecipando correttamente alla didattica interattiva e deriva, quindi, dalla somma delle due valutazioni. Il voto derivante dalla didattica interattiva verrà sommato al voto dell'esame se quest'ultimo sarà pari o superiore a diciotto trentesimi.
Il voto finale è espresso in trentesimi. Il voto minimo utile al superamento della prova è di diciotto trentesimi.

Ciascun test dovrà essere composto da 31 domande, così da garantire la possibilità di conseguire la lode, in ottemperanza alle norme Europee sul Diploma Supplement. L'attribuzione della lode è concessa esclusivamente allo studente che ha risposto positivamente alle prime 30 domande.

ATTIVITÀ DI DIDATTICA EROGATIVA (DE)

/**/
è 36 Videolezioni + 36 test di autovalutazione Impegno totale stimato: 36 ore

ATTIVITÀ DI DIDATTICA INTERATTIVA (DI) ED E-TIVITY CON RELATIVO FEED-BACK AL SINGOLO STUDENTE DA PARTE DEL DOCENTE O DEL TUTOR

/**/
è Redazione di un elaborato

è Partecipazione a web conference
è Svolgimento delle prove in itinere con feedback
è Svolgimento della simulazione del test finale
Totale 6 ore

MATERIALE DIDATTICO UTILIZZATO

è Videolezioni

è Dispense predisposte dal docente e/o slide del docente

è Testo di riferimento suggerito dal docente (facoltativo):

"Crittografia e Sicurezza delle Reti" 2/ed., William Stallings, Ed. McGraw-Hill. "Cryptography and Network Security", 7/ed., William Stallings, Pearson.
Il materiale didattico è sempre disponibile in piattaforma e consultabile dallo studente nei tempi e nelle modalità ad egli più affini.