Logo Image not found or type unknown

PROGRAMMA DEL CORSO DI SICUREZZA INFORMATICA

SETTORE SCIENTIFICO

ING-INF/05 (IINF-05/A)

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 maleware, di tecniche e strumenti per la loro analisi ed individuazione; conoscenza e compresione 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 maleware 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 maleware, di accedere a letteratura e documentazione tecnica di settore, di autoaggiornarsi su nuovi strumenti e tecniche di rilevamento e difesa.

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

PROGRAMMA DIDATTICO

1 - INTRODUZIONE ALLA SICUREZZA 2 - MINACCE ALLA SICUREZZA 3 - CIFRATURA SIMMETRICA 4 - AUTENTICAZIONE DEI MESSAGGI E FUNZIONI HASH 5 - CRITTOGRAFIA A CHIAVE PUBBLICA 6 - FIRMA DIGITALE E GESTIONE DELLE CHIAVI 7 - PRINCIPI DI AUTENTICAZIONE 8 - AUTENTICAZIONE CON PASSWORD 9 - AUTENTICAZIONE CON TOKEN, BIOMETRICA E REMOTA 10 - PRINCIPI DI CONTROLLO DEGLI ACCESSI 11 - CONTROLLO DEGLI ACCESSI DISCREZIONALE 12 - CONTROLLO DEGLI ACCESSI BASATO SUI RUOLI 13 - CONTROLLO DEGLI ACCESSI BASATO SUGLI ATTRIBUTI 14 - ICAM E TRUST FRAMEWORKS 15 - CRIMINI INFORMATICI 16 - MALWARE 17 - VIRUS 18 - WORM 19 - TROJAN, BACKDOORS, ROOTKITS 20 - ATTACCHI DOS 21 - TIPOLOGIE DI DOS 22 - BUFFER OVERFLOW 23 - SICUREZZA DEL DATABASE 24 - SICUREZZA DEL SOFTWARE 25 - SICUREZZA DEL SISTEMA OPERATIVO 26 - SICUREZZA DEL CLOUD 27 - SICUREZZA IOT 28 - ANTI-VIRUS 29 - FIREWALL 30 - INTRUSION DETECTION SYSTEM 31 - SICUREZZA DI POSTA ELETTRONICA 32 - SSL, TLS E HTTPS 33 - IP SECURITY 34 - APPLICAZIONI PER AUTENTICAZIONE DI RETE 35 - WIRELESS SECURITY 36 - MACHINE LEARNING PER LA SICUREZZA Il/La docente si riserva la possibilità di modificare in qualsiasi momento il programma didattico