FACOLTÀ: Giurisprudenza

CORSO DI LAUREA: Servizi Giuridici

INSEGNAMENTO: Cybercrime

CFU: 6

EVENTUALE ARTICOLAZIONE IN MODULI: No

ANNO DI CORSO: III

NOME DOCENTE: Alessandro Comi

Indirizzo e-mail: alessandro.comi@uniecampus.it

I docenti possono essere contattati attraverso la sezione *Ricevimento docenti*, presente nell'area riservata del sito di Ateneo, che comprende *Ufficio virtuale*, *Sistema di messaggistica* e *Ricevimento Telefonico.*
Per le comunicazioni scritte bisogna utilizzare il *Sistema di Messaggistica*.

Orario ricevimento on line:
Sabato dalle 14:30 alle 15:30 tramite ufficio virtuale e ricevimento telefonico.
Il docente è a disposizione per il ricevimento frontale degli studenti in occasione delle sessioni di esami previste a Roma e Novedrate.

RISULTATI DI APPRENDIMENTO DELL'INSEGNAMENTO

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

1. Con riferimento alla conoscenza e capacità di comprensione
    a. Conoscenza dei concetti fondamentali alla base della scienza informatica, intesa, nel suo significato più profondo, come gestione delle informazioni mediante procedure automatizzabili. Lo studente dovrà saper descrivere le modalità con cui vengono trattati i dati digitali ed i principali componenti che ne permettono la gestione automatizzata.
    b. Comprensione del concetto di reato informatico e delle sue peculiari caratteristiche, legate principalmente alla violazione di disponibilità, integrità, riservatezza, autenticità e non ripudiabilità dei sistemi informatici e telematici o delle informazioni in essi contenute. Conoscenza delle principali e più diffuse tipologie di reato informatico, delle modalità con le quali vengono lesi i beni giuridici informatici e di come la criminalità informatica è stata inquadrata nella Normativa italiana.
    c. Conoscenza delle problematiche legate alla trasmissione sicura di informazioni, e delle tecniche sempre più sofisticate che nel corso dei secoli sono state ideate per nascondere l'esistenza di dati trasmessi in segreto

(steganografia) o per rendere tali dati incomprensibili a chi li dovesse intercettare (crittografia).

d. Conoscenza delle corrette procedure da adottare per recupero e analisi del materiale contenuto nei dispositivi digitali, sia nell'ambito della criminalità informatica che di quella tradizionale, al fine di evidenziare l'esistenza di prove utili allo svolgimento delle attività investigative.
e. Comprensione dei principali meccanismi di funzionamento delle reti di telecomunicazione radiomobile, di quali informazioni è possibile ricavare da tali reti e della corretta metodologia per utilizzare tali informazioni in ambito forense, con particolare riferimento alla localizzazione delle utenze cellulari.

2. Con riferimento alla conoscenza e capacità di comprensione applicate
   a. Padronanza delle nozioni base della scienza informatica, e capacità di impostare e sostenere una discussione sui sistemi informatici e telematici, adducendo razionali che siano tecnicamente validi.
   b. Capacità di analisi critica delle principali tecniche utilizzate per rendere sicure le comunicazioni digitali, dei pro e contro di ognuna delle tecniche.
   c. Applicazione di quanto appreso sul cybercrime per individuare le vulnerabilità degli attuali sistemi informatici e tecniche e procedure per limitare i rischi di attacco.
   d. Capacità di applicare in modo corretto in ambito forense le potenzialità fornite dalle reti di telecomunicazione radiomobile.

3. Con riferimento all'autonomia di giudizio
   a. Capacità di individuare in autonomia la tecnica più idonea a garantire integrità e segretezza di una comunicazione digitale, a seconda dell'obiettivo che hanno le informazioni trasmesse, della mole di dati da inviare e della loro natura.
   b. Capacità di individuare le fattispecie di reato in cui sono inquadrabili specifiche condotte illecite nell'ambito della criminalità informatica.
   c. Capacità di individuare in autonomia le tecniche di digital forensics più appropriate per un determinato scenario investigativo.
   d. Capacità di sviluppare in autonomia una corretta strategia forense che utilizzi le informazioni estraibili dalle reti di telecomunicazione radiomobile in modo scientificamente rigoroso.

4. Con riferimento alle abilità comunicative
   a. Capacità di costruire discorsi articolati e scientificamente rigorosi, utilizzando i concetti appresi nel corso in modo trasversale su tutte le tematiche affrontate (le logiche crittografiche devono essere ad esempio applicate trasversalmente su digital forensics, telecommunication forensics, prevenzione dei reati informatici).
   b. Padronanza della terminologia scientifica propria delle tematiche affrontate nel corso.

5. Con riferimento all'abilità ad apprendere
    a. Capacità di comprendere e metabolizzare a fondo le nozioni contenute nel corso, e di utilizzarle in modo critico per sfruttare al massimo le potenzialità di apprendimento rese disponibili dal web.

PROGRAMMA DETTAGLIATO

Il programma, costituito da 48 lezioni, si compone dei "nuclei tematici" di seguito riportati.

SICUREZZA INFORMATICA
Concetto di sistema informatico e telematico e loro caratteristiche principali, aspetti da proteggere per garantire la sicurezza, attacchi informatici attivi e passivi, vulnerabilità dei sistemi, cyberminacce e gestione del rischio, tecniche di protezione difensiva e proattiva, sicurezza della rete in termini di disponibilità, integrità, riservatezza, autenticità e non ripudiabilità, integrità dei file ed algoritmi di Hash, metodologie di accesso abusivo ai sistemi informatici, tecniche di autenticazione.

CYBERCRIME
Caratteristiche e peculiarità dei reati informatici, reati propri e impropri, tipologie di reati in termini di beni giuridici lesi e inquadramento nella Normativa italiana, il profilo del criminale informatico, origini e caratteristiche dei vari tipi di malware, il mondo dell'hacking, tecniche di attacco e difesa dai malware, il fenomeno del Social Engineering, attacchi alla rete internet e cloud computing, cybercrime contro dispositivi mobili.

RISERVATEZZA DEI DATI
Steganografia storica e contemporanea, crittografia storica e le macchine cifranti, crittografia simmetrica ed asimmetrica, crittografia OTP, crittografia combinata e Firma Digitale, tecniche di crittoanalisi, fondamenti di fisica quantistica, computer quantistici e crittografia quantistica, protocolli crittografici, firewall.

DIGITAL FORENSICS
Origini ed obiettivi della Digital Forensics, come va acquisita la digital evidence, tecniche di memorizzazione digitale, le memorie di massa, tecniche forensi di duplicazione e validazione dei dati, post-mortem e live forensics, analisi dei dati e documentazione delle attività al fine di preservare il valore probatorio delle prove informatiche, catena di custodia, Network Forensics, Mobile Forensics.

TELECOMMUNICATION FORENSICS
Storia delle telecomunicazioni, meccanismi di funzionamento delle reti di Telecomunicazione Radiomobile, le Reti Cellulari, applicazioni in ambito forense, analisi dei tabulati telefonici e telematici, tecniche di localizzazione utilizzabili prima e dopo il fatto criminoso.

FONDAMENTI DI INFORMATICA
Introduzione all'era digitale, concetti base di informatica e di gestione delle informazioni, composizione ed architettura di alto livello dei computer, meccanismi di funzionamento di rete, porte e protocolli, cos'è internet e come funziona.

EVENTUALI PROPEDEUTICITÀ CONSIGLIATE

Non sono previste propedeuticità, il corso include un ripasso dei concetti fondamentali di informatica e architettura delle reti.

MODALITÀ DI SVOLGIMENTO ESAME

L'esame si svolge a scelta dello studente in modalità scritta, attraverso una prova costituita da domande a risposta chiusa e aperta con eventuale orale integrativo, o in modalità orale, in base a quanto previsto dal *Regolamento per lo svolgimento degli esami di profitto* consultabile sul sito dell'Ateneo, al seguente link.

Regolamento per lo svolgimento degli esami di profitto

CRITERI DI VALUTAZIONE DELL'APPRENDIMENTO

1. Con riferimento alla conoscenza e capacità di comprensione sopra declinate:
   verrà valutata la padronanza dei contenuti teorici del corso acquisita dallo studente. La valutazione avverrà sulla base delle risposte fornite dallo studente sia alle domande a risposta chiusa sia a quelle a risposta aperta, e attraverso l'eventuale prova orale.

2. Con riferimento alla conoscenza e capacità di comprensione applicata:
   verrà valutata l'abilità dello studente nella comprensione di processi informatici di gestione dei dati digitali, tabulati, protocolli e criteri di localizzazione su mappe geografiche. La valutazione si baserà sulle risposte fornite alle domande a risposta aperta ed eventualmente in sede di prova orale.

3. Con riferimento all'autonomia di giudizio:
   verrà valutato se lo studente è in grado di impostare le strategie più idonee a garantire la sicurezza di un sistema informatico, di capire quali sono le tecniche corrette da utilizzare in digital forensics sulla base dello scenario investigativo e di applicare in modo rigorosamente scientifico i dati forniti dalle reti di telecomunicazione radiomobile. La valutazione avverrà sulla base delle argomentazioni esposte dallo studente in riferimento alle domande a risposta aperta e attraverso l'eventuale prova orale.

4. Con riferimento alle abilità comunicative sopra declinate:
   verrà valutata la capacità dello studente di utilizzare la terminologia corretta. La valutazione si baserà sulla proprietà di linguaggio tecnico utilizzato nelle risposte alle domande a risposta aperta e durante l'eventuale prova orale.

5. Con riferimento all'abilità ad apprendere:
   verrà valutata la capacità dello studente di sfruttare le nozioni apprese nel corso per approfondire ulteriori dettagli su temi specifici attraverso gli strumenti offerti dal web. La valutazione si baserà sulla eventuale prova orale.

CRITERI DI ATTRIBUZIONE DEL VOTO FINALE

Sulla base dei criteri di valutazione sopra indicati, l'attribuzione del voto finale avviene attraverso i seguenti criteri:

1) Criteri di attribuzione del voto alla prova scritta:
   a) le risposte alle domande aperte sono valutate su scala 0-3 punti, secondo i seguenti criteri:
      - 0 = risposta mancante, errata o priva di elaborazione personale;
      - 1 = prevalere complessivo di elementi non corretti con isolati spunti corretti;
      - 2 = contestualizzazione della risposta corretta, ma con presenza di elementi non corretti o esposta in modo non efficace o incompleto;
      - 3 = risposta corretta, ben esposta;
   b) le risposte alle domande chiuse sono valutate su una scala 0/1.

2) Criteri di attribuzione del voto alla prova orale:
   a) 0/30 – 17/30: prevalenza di argomentazioni non corrette e/o incomplete e scarsa capacità espositiva;
   b) 18/30 – 21/30: prevalenza di argomentazioni corrette adeguatamente esposte;
   c) 22/30 – 26/30: argomentazioni corrette e ben esposte;
   d) 27/30 – 30/30 e lode: conoscenza approfondita della materia ed elevata capacità espositiva, di approfondimento e di rielaborazione.

MATERIALE DIDATTICO

I materiali didattici disponibili sulla piattaforma sono esaustivi.
Eventuali approfondimenti **facoltativi** sono segnalati *in itinere* all'interno del corso

---

ATTIVITÀ DIDATTICHE

Attività di Didattica Erogativa (ore di impegno stimato per lo studente):
- 6 ore di Audiolezioni

Attività di Didattica Interattiva (ore di impegno stimato per lo studente):
- 30 ore di quiz

Attività di autoapprendimento (ore di impegno stimato per lo studente):
- 114 ore (slide del corso, dispense, articoli, testi d'esame)

CONSIGLI DEL DOCENTE

I dettagli vanno studiati ed approfonditi senza mai perdere di vista il contesto generale; ogni nuova invenzione, ogni innovazione tecnologica è la soluzione ad un determinato problema, e può essere compresa pienamente solo avendo ben chiaro il problema che risolve.