SCUOLA	Scuola di Scienze di Base e Applicate
ANNO ACCADEMICO	2014/2015
CORSO DI LAUREA MAGISTRALE	Informatica
INSEGNAMENTO	Reti e sicurezza informatica
TIPO DI ATTIVITÀ	Attività caratterizzanti
AMBITO DISCIPLINARE	Discipline Informatiche
CODICE INSEGNAMENTO	
ARTICOLAZIONE IN MODULI	NO
NUMERO MODULI	1
SETTORI SCIENTIFICO DISCIPLINARI	INF/01
DOCENTE RESPONSABILE	Alfonso Maurizio Urso Ricercatore CNR Docente a contratto
CFU	6
NUMERO DI ORE RISERVATE ALLO STUDIO PERSONALE	102
NUMERO DI ORE RISERVATE ALLE ATTIVITÀ DIDATTICHE ASSISTITE	48
PROPEDEUTICITÀ	Nessuna
ANNO DI CORSO	Primo
SEDE DI SVOLGIMENTO DELLE LEZIONI	Dipartimento di Matematica e Informatica di Palermo
ORGANIZZAZIONE DELLA DIDATTICA	Lezioni frontali, Attività in laboratorio
MODALITÀ DI FREQUENZA	Facoltativa
METODI DI VALUTAZIONE	Prova scritta, prova orale. La prova scritta può essere sostituita da un elaborato progettuale realizzato in gruppo.
TIPO DI VALUTAZIONE	Voto in trentesimi
PERIODO DELLE LEZIONI	Primo semestre
CALENDARIO DELLE ATTIVITÀ DIDATTICHE	Consultare il sito www.cs.unipa.it
ORARIO DI RICEVIMENTO DEGLI STUDENTI	Consultare la home page del corso

RISULTATI DI APPRENDIMENTO ATTESI

Conoscenza e capacità di comprensione

Il corso intende fornire agli studenti le nozioni necessarie per comprendere ed affrontare le diverse problematiche relative alla sicurezza informatica anche nell'ambito di realtà produttive, alla progettazione di sistemi informatici e reti con un certo livello di sicurezza, alla gestione delle attività legate alla sicurezza informatica.

Capacità di applicare conoscenza e comprensione

Il corso si pone come obiettivo principale la comprensione, da parte dello studente, delle tecniche e dei modelli computazionali che sono alla base degli aspetti riguardanti la sicurezza dei sistemi informatici e delle reti. Tali conoscenze saranno applicate per la progettazione e gestione di sistemi informatici sicuri, anche attraverso la realizzazione di un elaborato progettuale.

Autonomia di giudizio

Agli studenti verrà proposto un metodo di lavoro che li guiderà verso un apprendimento critico e responsabile degli argomenti che verranno loro proposti in aula e in laboratorio. Ciascuno studente avrà inoltre occasione di arricchire la propria autonomia di giudizio attraverso la realizzazione di un progetto o di un elaborato che sarà parte integrante della prova di valutazione.

Abilità comunicative

Attraverso le attività di laboratorio previste, il corso tenderà a sviluppare negli studenti l'interazione e la capacità di saper lavorare in gruppo, di confrontarsi sulle problematiche al fine di individuare le soluzioni in base alle conoscenze acquisite durante il corso. L'acquisizione delle abilità comunicative sarà realizzata tramite la partecipazione attiva dello studente alle attività di laboratorio nonché l'esposizione dei risultati del lavoro individuale o di gruppo su argomenti o problematiche proposti dal docente.

Capacità d'apprendimento

Gli argomenti affrontati nel corso delle lezioni frontali e delle esercitazioni in laboratorio dovranno consentire lo sviluppo delle capacità di apprendimento degli studenti in modo da consentire loro di "interrogare" in modo integrato le proprie conoscenze-competenze a fronte delle problematiche affrontate. Gli studenti saranno stimolati inoltre ad una conoscenza più approfondita e critica dei sistemi informatici e delle reti in un'ottica volta alla loro messa in sicurezza.

OBIETTIVI FORMATIVI DEL CORSO

Il corso si pone un obiettivo culturale volto all'introduzione dei principali aspetti teorici che sono alla base della sicurezza informatica. In aggiunta esso ha l'obiettivo di sviluppare le capacità progettuali e realizzative degli allievi attraverso l'applicazione delle nozioni teoriche sulla sicurezza informatica, in contesti ben delineati anche nell'ambito di specifiche realtà produttive

CORSO	**RETI E SICUREZZA INFORMATICA**
ORE FRONTALI	**LEZIONI FRONTALI**
2	Introduzione: Architettura di sicurezza del modello OSI. Servizi di sicurezza. Meccanismi di sicurezza. Modelli per la sicurezza di rete.
10	Crittografia simmetrica: Crittografia Classica. Tecniche di crittografia classiche e crittoanalisi. Cifrari di Cesare, Playfair e Hill. Cifrari a sostituzione polialfabetica. Macchine cifranti. One-time pad. Steganografia. Crittografia Simmetrica. Principi della cifratura a blocchi. Strutture di Feistel. DES e modalità operative. Crittoanalisi lineare e differenziale. Standard AES. Cifratura AES. Trasformazioni: substitute bytes, shift rows, mix columns, add round key. Cifratura inversa equivalente. Cifratura a flussi e RC4
8	Crittografia chiave pubblica e funzioni hash: Crittografia Asimmetrica. Principi dei crittosistemi a chiave pubblica. RSA. Sicurezza e aspetti computazionali. Test di primalità. Gestione delle chiavi. Crittografia a curva ellittica. Funzioni Hash e MAC. Funzioni hash: attacco a compleanno, funzioni hash iterate, MD4, MD5, SHA-1, funzioni hash basate su cifrari a blocchi. Message Authentication Code: CBC-MAC, MAC basati su funzioni hash, HMAC

	Firme Digitali, Digital Signature Standard, DSA
6	Sicurezza di rete e Web Sicurezza a livello di rete - protocollo IPsec. Protocollo DNSSec. Proxy servers, NAT. Sicurezza a livello di trasporto - protocollo SSL, Virtual Private Networks. Sicurezza a livello applicazione - HTTPS, POP3/IMAP/SMTP over SSL.
6	Sicurezza di sistema: Intrusioni. Rilevamento delle intrusioni. software doloso, I virus e altre minacce correlate. Contromisure contro i virus. Gli attacchi DoS distribuiti. Firewall: progettazione e configurazione. Sistemi trusted.
	ATTIVITA' in LABORATORIO
6	Esercitazioni pratiche su analisi e filtraggio del traffico di rete attraverso l'utilizzzo di specifici tool (ad es. wireshark)
10	Esercitazioni pratiche di installazione e sviluppo di server web sicuri, certificati digitali, CA, servizi web sicuri.
TESTI CONSIGLIATI	William Stallings, Crittografia e sicurezza delle reti, 2/E italiana, McGrawHill, 2007. William Stallings, Cryptography and Network Security, 4/E, Prentice Hall, 2006. James F. Kurose, Keith W. Ross, Computer Networking: A Top-Down Approach, 6/E, 2013 Addison-Wesley Materiale didattico distribuito a lezione dal docente.