SCHEDA DELL'INSEGNAMENTO (SI)

"CYBERSECURITY DATA ANALYSIS"

SSD ING INF 05*

DENOMINAZIONE DEL CORSO DI STUDIO: INGEGNERIA INFORMATICA

ANNO ACCADEMICO 2023-2024

INFORMAZIONI GENERALI - DOCENTE

DOCENTE: ANTONIO PESCAPE'
TELEFONO: 0817683856
EMAIL: ANTONIO.PESCAPE@UNINA.IT

INFORMAZIONI GENERALI - ATTIVITÀ

INSEGNAMENTO INTEGRATO (EVENTUALE):
MODULO (EVENTUALE):
CANALE (EVENTUALE):
ANNO DI CORSO (I, II, III): II
SEMESTRE (I, II): II
CFU: 6

INSEGNAMENTI PROPEDEUTICI (se previsti dall'Ordinamento del CdS)

Nessuno

EVENTUALI PREREQUISITI

Nozioni di protocolli di rete Internet.

OBIETTIVI FORMATIVI

L'obiettivo dell'insegnamento è quello di fornire agli studenti le nozioni specialistiche utili all'analisi di una moderna rete internet con particolare riferimento agli aspetti legati alla sicurezza di rete. Il corso presenta i contenuti adottando un approccio ingegneristico ed empirico e fonde lezioni teoriche, lezioni pratiche, seminari ed esercitazioni. Esso presenta in modo approfondito gli aspetti principali e le motivazioni alla base dell'analisi di una rete di calcolatori, per poi approfondire gli aspetti metodologici e pratici legati all'analisi di rete con un focus specifico sulla analisi, identificazione e classificazione di eventi anomali quali, ad esempio, attacchi informatici. L'obiettivo è studiare le principali tecniche, tecnologie e strumenti per il monitoraggio e l'analisi del traffico di rete e le loro applicazioni alla cybersecurity. Il corso esamina i principali approcci per effettuare misurazioni della rete Internet (monitoraggio passivo e attivo), le tecniche utilizzate per identificare il traffico di applicazioni e servizi (classificazione del traffico) e i metodi utilizzati per la sicurezza di rete, come il rilevamento e la mitigazione degli attacchi, utilizzando approcci ad apprendimento automatico (Machine Learning). Il corso prevede inoltre attività sperimentali finalizzate alla redazione di una relazione tecnico-scientifica.

RISULTATI DI APPRENDIMENTO ATTESI (DESCRITTORI DI DUBLINO)

Conoscenza e capacità di comprensione

Lo studente deve dimostrare di conoscere e saper comprendere le problematiche relative all'analisi e al monitoraggio delle reti Internet e del traffico di rete, sia benigno sia malevolo. Deve dimostrare di sapere elaborare argomentazioni concernenti le relazioni tra il traffico di rete e fenomeni quali attacchi, malfunzionamenti di rete, problematiche prestazionali. Tali strumenti consentiranno agli studenti di comprendere le connessioni causali tra l'uso di applicazioni di rete, il traffico generato da tali applicazioni e le condizioni di esercizio della rete in presenza sia di traffico benigno sia malevolo. Inoltre, ci si aspetta che lo studente sia in grado di riconoscere le relazioni tra le operazioni eseguite attraverso la rete (esecuzione di applicazioni, configurazione di dispositivi di rete, attacchi a dispositivi di rete) e gli eventi osservabili (mutamenti nelle caratteristiche del traffico e nelle funzionalità dei dispositivi di rete).

Capacità di applicare conoscenza e comprensione

Lo studente deve dimostrare di essere in grado di trarre le conseguenze da un insieme di informazioni per identificare e risolvere problemi concernenti le infrastrutture e le applicazioni di rete, pianificare infrastrutture e servizi sulla base dei requisiti di sicurezza richiesti alle comunicazioni effettuate tramite la rete Internet. Analizzando i dati di rete, lo studente deve essere in grado di inferire la natura (benigna/malevola) e caratteristiche volumetriche della comunicazione (numero di dispositivi coinvolti, quantità e tempistica dei messaggi scambiati). Lo studente deve essere in grado di applicare gli strumenti metodologici appresi ai seguenti ambiti: raccolta dei dati di traffico Internet, analisi delle applicazioni di rete e sicurezza di rete. Più precisamente, le analisi di sicurezza eseguite osservando e analizzando scenari operativi di rete, costituiscono un approccio proattivo alla sicurezza informatica, che utilizza capacità di raccolta, aggregazione ed analisi dei dati al fine di portare a termine funzioni di sicurezza essenziali che rilevano, analizzano e mitigano le minacce informatiche alle reti.

PROGRAMMA-SYLLABUS

Introduzione, Concetti di Base e Fondamenti: Contestualizzazione didattico/scientifica del Corso, Terminologia di Base, Inquadramento degli aspetti principali dell'analisi di Internet e motivazioni (precedenti e successivi al proliferare di attacchi informatici), Risoluzione dei Problemi di Rete, Requisiti delle Reti, Sicurezza di Rete, Analisi di Sicurezza; Background Analitico (probabilità, statistica, rappresentazione dei dati, forecasting, grafi, etc.), Metodologie e Tecniche di Machine/Deep Learning e Data Mining; Task di Apprendimento: Classificazione, Predizione e Anomaly Detection; Tecniche di eXplainable AI (XAI) per approcci Machine/Deep Learning; Reinforcement Learning; Adversarial Learning; Continuous e Few Shot Learning; Framework di Valutazione e Metriche di Prestazione; Data Visualization. [1,5 CFU]

Dati e Monitoraggio di Rete: Modelli e Metriche per l'Analisi ed il Monitoraggio di Internet; Approcci al Monitoraggio di Internet (attivo, passivo, ibrido, etc.); Dalla Rete al Traffico: Metodologie e strumenti per l'acquisizione e la caratterizzazione di dataset di traffico di rete (generati da utenti e generati da bot); Tipi di dato per la sicurezza della rete (pacchetti di rete, feature e statistiche estratte, log file di rete e di sistema); Dataset pubblici per l'analisi del traffico di

rete e la sicurezza di rete: caratterizzazione e principali utilizzi; Gestione e configurazione degli strumenti per il monitoraggio di rete; Metodologie e Tecniche per l'analisi del Traffico di Internet: workload di rete, caratterizzazione e modelling statistico, Traffico Self-Similare, Modelli di generazione del Traffico Internet; "Practical Issues" nell'Analisi e nel Monitoraggio di Internet: middleboxes (PEP, PDP, Firewall, etc). [1,5 CFU]
Analisi dei Dati e Sicurezza Informatica: Dal traffico ai dati, dai dati alle feature: analisi ed interpretazione dei dati di rete, analisi e selezione delle feature di rete; Identificazione e Classificazione del traffico di rete con approcci basati sull'intelligenza artificiale; Identificazione e Classificazione del traffico di rete anomalo e malevolo (malware, attacchi DoS/DDoS, BotNet, ecc.) con particolare riferimento agli scenari 5G, IoT (Industriale), Cloud, Web e Mobile; Identificazione delle Anomalie Automatica, Zero-day Detection, Machine Learning Network Intrusion Detection Systems (ML-NIDS), nuovi attacchi a sistemi ML e "adversarial input perturbations", Piattaforme sperimentali su larga scala per l'analisi e il monitoraggio del traffico Internet e generato da attacchi; Neutralità di Rete ed applicazione, rilevamento ed elusione di meccanismi di censura; Robustezza agli attacchi ai percorsi di rete ed alle topologie (ad esempio, attacchi al protocollo di instradamento); Sfide legali ed etiche che emergono dalla raccolta di dati sulle attività di utenti umani e dal loro utilizzo al fine di costruire modelli di apprendimento automatico. [3 CFU]

MATERIALE DIDATTICO

Il materiale didattico è costituito dalle Slide, dalle Dispense e dagli articoli forniti dal docente.
Libro di testo di approfondimento: *Internet Measurement: Infrastructure, traffic & applications, Mark Crovella, Balachander Krishnamurthy, Wiley.*

MODALITÀ DI SVOLGIMENTO DELL'INSEGNAMENTO

Il docente utilizzerà:
a) lezioni frontali per circa il 40% delle ore totali,
b) esercitazioni per approfondire praticamente aspetti teorici per circa il 40% delle ore totali,
c) seminari per approfondire tematiche specifiche per circa il 20% delle ore totali.

VERIFICA DI APPRENDIMENTO E CRITERI DI VALUTAZIONE

a) Modalità d'esame:

L'esame si articola in prova	
scritta e orale	
solo scritta	
solo orale	X
discussione di elaborato progettuale	X
altro	

In caso di prova scritta i quesiti sono (*)	**A risposta multipla**	
	A risposta libera	
	Esercizi numerici	

b) Modalità di valutazione: