# Programmi degli insegnamenti

## Programmazione Python (facoltativo)

Docenti: Alessio Bechini (DII-UNIPI), Marco Pettorali (DII-UNIPI)
Ore totali: 30
Esercitazioni: 30 ore

### Obiettivi formativi

Il corso si propone due obiettivi. Primo, presentare le caratteristiche generali di un linguaggio di scripting, focalizzandosi sull'apprendimento del linguaggio Python. Secondo, sviluppare le capacità degli studenti di organizzare algoritmicamente soluzioni software per semplici problemi presentati, mostrando diverse alternative basate sull'impiego dei paradigmi supportati da Python. Le capacità acquisite saranno sfruttate in successivi corsi all'interno del Master.

### Programma

Linguaggi di programmazione e di scripting. Struttura del linguaggio Python. Uso di ambienti di sviluppo e di Notebook. Tipi, letterali, uso di tipo "built-in". Assegnamento, comandi di controllo del flusso. Funzioni: definizione e chiamata. Passaggio di parametri, funzioni annidate e ricorsive, chiusure, iteratori. La ricorsione e la tecnica di memo-izzazione. Gestione delle eccezioni. Elementi di programmazione funzionale: funzioni anonime, map, filter, reduce, list comprehension, generator expression. Uso dei file. Codifiche di caratteri (Unicode e utf-8). Moduli e packages. Generatori di numeri (pseudo) casuali e loro impiego. Programmazione OO: classi, istanze, metodi (di istanza, di classe, statici), inizializzazione. Ereditarietà in classi Python. Numpy: creazione di array, loro caratteristiche e operazioni. Copia di array, Matrici. SciPy. Plotting con matplotlib/pyplot.
Guida alla risoluzione di esercizi proposti, anche attraverso approcci alternativi.

# FOUNDATIONS MODULES

## Networking

Docenti: Carlo Vallati (DII-UNIPI), Francesco Di Rienzo (DII-UNIPI)
Lezioni: 14 ore; Esercitazioni: 10 ore
Ore totali: 24
CFU: 3

### Obiettivi formativi

Il corso si propone di illustrare i concetti di base sulle reti informatiche. In particolare, verranno presentati le applicazioni di rete di uso più comune, i protocolli di Internet, e le principali tecnologie di rete (sia wired sia wireless). Particolare attenzione sarà dedicata allo sviluppo di applicazioni di rete secondo il modello client-server e peer-to-peer.

**Programma**

Introduzione a Internet. La periferia di Internet. Il Core di Internet. Organizzazione di Internet. Applicazioni di rete. Paradigmi client-server e peer-to-peer. Requisiti delle applicazioni. Servizi disponibili su Internet. Applicazioni di uso comune e relativi protocolli. Reti ad accesso diretto. Livello data link. Protocollo PPP. Protocolli ad accesso multiplo. Reti Locali. Reti Local Ethernet. Ethernet Switched. Reti geografiche Packet Switched. Introduzione alle inter-reti. Architettura di un router. Protocollo IP. DHCP e NAT. Cenni su ARP e IPv6. Livello di trasporto. Multiplexing/Demultiplexing. Protocollo UDP. Protocollo TCP Reti Wireless. WLAN WiFi. Cenni su Bluetooth e Internet of Things.

## Data mining

Docenti: Beatrice Lazzerini (DII-UNIPI), Francesco Marcelloni (DII-UNIPI)
Lezioni: 16 ore; Esercitazioni: 9 ore
Ore totali: 25
CFU: 3

**Obiettivi formativi**

L'insegnamento si propone di fornire i concetti fondamentali relativi al data mining a supporto della cyber-security. In particolare, utilizzando esempi relativi ad applicazioni reali, saranno presentati i principali algoritmi e tecniche per pre-processare i dati, per identificare pattern frequenti, per classificare e raggruppare dati, e per individuare outlier. Gli studenti acquisiranno la capacità di sviluppare ed applicare tecniche di data mining nel contesto della cyber-security.

**Programma**

Preprocessazione dei dati: pulizia (cleaning), integrazione, trasformazione e riduzione dei dati ed estrazione, selezione e analisi di rilevanza delle caratteristiche. Estrazione di pattern frequenti: concetti base, algoritmi A-Priori e FP-Growth, regole associative, misure di correlazione. Clustering: concetti base, algoritmi di clustering, metodi di valutazione dei risultati. Classificazione: concetti base, alberi di decisione, classificatori bayesiani, metodi di valutazione dei risultati. Individuazione degli outlier: metodi statistici e basati sulla prossimità.
Reti neurali artificiali. Principali modelli di rete neurale. Addestramento delle reti neurali. Deep learning. Convolutional neural networks. Recurrent neural networks. Esempi di applicazioni.

## Web Technology

Docenti: Mario Cimino (DII-UNIPI)
Lezioni: 14 ore
Ore totali: 14
CFU: 2

**Obiettivi formativi**
Il corso si propone di fornire le conoscenze di base sull'architettura e sulle tecnologie del Web e delle sue applicazioni. Gli studenti potranno inoltre acquisire competenze sulle architetture orientate ai servizi e sulla interoperabilità machine-to-machine.

**Programma**

Il corso tratterà le applicazioni Web cliente-servitore, il protocollo HTTP, i cookie, il caching del Web ed il protocollo Secure Socket Layer (SSL). Il corso fornirà anche un'introduzione ad XML ed agli Web Services. Saranno anche presentate tecniche di privacy preserving data integration in ambienti dinamici.

## CORE MODULES

### Applied Cryptography and Access Control

Docenti: Gianluca Dini (DII-UNIPI), Pericle Perazzo (DII-UNIPI)
Lezioni: 13 ore; Esercitazioni: 17 ore
Ore totali: 30
CFU: 3

**Obiettivi formativi**

Il corso si propone un duplice obiettivo. Primo, illustrare le principali operazioni crittografiche ed i principali modelli di controllo degli accessi, le loro proprietà di sicurezza ed il loro impatto sulle prestazioni. Secondo, permettere agli studenti di esercitarsi nella realizzazione di semplici protocolli di sicurezza utilizzando librerie crittografiche open-source.

**Programma**

I requisiti CIA: confidenzialità, integrità, autenticazione. La cifratura simmetrica. I cifrari perfetti: one-time pad. I cifrari a blocchi, cenni su DES e AES. Modalità di cifratura: Electronic Codebook (ECB) e Cipher Block Chaining. Cifratura multipla: 3DES. Le funzioni hash e message authentication code (MAC). La crittografia a chiave pubblica. Il cifrario RSA. La firma digitale, i certificati e le infrastrutture a chiave pubblica (PKI). Lo scambio di chiavi Diffie-Hellmann. Autenticazione ed identificazione.

### Network Security & Ethical hacking

Docenti: Michele Pagano (DII-UNIPI), Christian Callegari (DII-UNIPI)
Lezioni: 14 ore; Esercitazioni: 10 ore
Ore totali: 24
CFU: 3

**Obiettivi formativi**

Il corso si propone di introdurre i concetti di base relativi alla sicurezza di rete e le soluzioni protocollari in ambito IPv4/IPv6. Quindi verranno considerati gli aspetti più significativi dell'ethical hacking e infine saranno considerate le principali tipologie di attacco a diversi livelli protocollari e alcuni dei principali metodi di difesa.

**Programma**

Firewall: principali funzionalità e limiti dei firewall; confronto tra le diverse architetture; IPTables. Intrusion Detection Systems (IDS): tassonomia e parametri prestazionali; cenni su SNORT. IPSec: principali standard e servizi offerti; modalità trasporto e tunnel; Authentication Header e Encapsulating Security Payload; cenni sui database di IPSec e sui protocolli per lo scambio di chiavi. Ethical Hacking: definizioni, tassonomia degli attacchi, Security Assessment e Penetration Testing. Scanning e Information Gathering. Esempi di attacchi di rete a diversi livelli protocollari: ARP spoofing e ARP poisoning, attacchi a ICMP, SYN flooding; attacchi al DNS.

## Operating Systems Security

Docente: Giuseppe Lettieri (DII-UNIPI)
Lezioni: 14 ore; Esercitazioni: 10 ore
Ore totali: 24
CFU: 3

**Obiettivi formativi**

Il corso ha lo scopo di presentare i meccanismi che Sistemi Operativi tradizionali e moderni impiegano per applicare vincoli di sicurezza. Il percorso formativo presenterà sia le tecniche per eludere questi meccanismi sia le possibili contromisure.

**Programma**

The Orange Book e Common Criteria. Autenticazione basata su password; PAM. Introduzione a Mandatory e Discretionary Access Control con esempi concreti tratti da Unix tradizionale, le Access Control Lists e SELinux/AppArmor. Principali errori di programmazione che portano ad attacchi alla sicurezza e possibili contromisure: buffer e heap overflow; return-to-libc; Return Oriented Programming; canaries, Address Space Randomization; symlink attacks. Isolamento delle applicazioni tramite chroot/contenitori/jail o macchine virtuali.

## Digital Forensics

Docenti: Luca Vasarelli (IIT-CNR), Arianna Del Soldato (IIT-CNR), Rita Rossi (IIT-CNR)
Lezione: 14 ore
Ore totali: 14
CFU: 2

**Obiettivi formativi**

Il corso è incentrato sui concetti principali della Computer Forensics e delle investigazioni digitali. Saranno trattate le tecniche e le strategie informatico-giuridiche di gestione degli incidenti informatici. Il percorso formativo farà acquisire agli studenti le competenze nella valutazione, acquisizione e gestione del rischio e della prova digitale, con riferimento ad alcuni casi specifici.

**Programma**

Introduzione e definizione di Digital Forensics (DF), nozioni ed elementi tecnici di principio, la figura dell'investigatore digitale. Fasi principali della DF (identificazione, acquisizione, conservazione, analisi e presentazione della digital evidence) e relativi cenni giuridici. Analisi forense di sistemi di file sharing, con particolare riferimento alla disciplina della DF applicata ai sistemi P2P. Analisi forense di sistemi di cloud computing con riferimento ai modelli di servizio SaaS, PaaS e IaaS. Vehicle forensics nei casi di crimini perpetrati tramite veicoli e incidenti automobilistici. Specifica attenzione sarà infine dedicata alla legge 18 marzo 2008 che ha apportato modiche al codice penale e di procedura penale e con cui sono stati introdotti nel nostro ordinamento nuovi mezzi di ricerca della prova informatica forense.

## Cyber risk management

Docente: Artsiom Yautsiukhin (IIT-CNR)
Lezioni: 12 ore; Esercitazioni: 3 ore
Ore totali: 15
CFU: 2

**Obiettivi formativi**

L'obiettivo principale del corso è introdurre i concetti di base della gestione del rischio cyber. Il corso definisce cosa sia un rischio, stabilisce il processo di gestione del rischio cyber e ne descrive le principali fasi. Particolare attenzione è dedicata all'identificazione degli asset cyber, delle minacce, delle vulnerabilità, dei controlli di sicurezza e delle relative conseguenze. Il corso introdurrà diversi approcci all'analisi del rischio e le possibili opzioni per il trattamento del rischio.

**Programma**

Misurazioni tecniche specifiche e punteggi di conformità non sono sufficienti per prendere decisioni efficienti a livello elevato su come costruire o modificare la cybersecurity di un sistema. Il corso definisce la valutazione del rischio come un modo per misurare e analizzare la qualità della cybersecurity e introduce i termini e i concetti di base. Viene descritto il processo di gestione del rischio e i suoi passaggi sono presentati in dettaglio. Particolare attenzione è dedicata alla valutazione e trattamento del rischio. Vengono identificati i tipici asset informatici e si stabiliscono le interdipendenze tra di essi. Vengono anche discusse in dettaglio le minacce esistenti e i controlli di sicurezza che le prevengono (secondo ISO27002). Vengono presentati vari approcci per condurre l'analisi del rischio (ad es., quantitativa vs qualitativa) e la sua documentazione (ad es., tabelle di rischio). Vengono introdotte le quattro opzioni di trattamento del rischio (riduzione del rischio, trasferimento del rischio, prevenzione del rischio e accettazione del rischio). Il corso tocca solo brevemente altri passaggi della gestione del rischio (come la comunicazione del rischio, il monitoraggio, la segnalazione, ecc.).

## Complex network analysis

Docente: Chiara Boldrini (IIT-CNR)
Lezioni: 14 ore; Esercitazioni: 10 ore
Ore totali: 24
CFU: 3

**Obiettivi formativi**

Il corso ha lo scopo di fornire agli studenti gli strumenti e le conoscenze necessarie ad analizzare reti complesse a larga scala e le possibili minacce in termini di attacco alla struttura di rete, e - quindi - possibili contromisure. Il corso ha un approccio "hands-on", nel senso che gli strumenti presentati vengono immediatamente applicati su dataset relativi a vari tipi di rete a larga scala in ambiente Internet, tra cui la rete degli Autonomous Systems di Internet, il WWW e le Online Social Networks, come casi di studio e di esercizio.

**Programma**

Reti complesse. Strumenti e metriche di analisi di reti complesse. Degree distribution, clustering coefficient, path length, assortativity, community detection. Small-world properties. Modelli generativi di reti complesse. Reti complesse di riferimento: WWW, Internet Autonomous Systems, Online Social Networks, Road Networks, Collaboration Networks. Attacchi alla struttura di rete e loro possibili effetti.
Strumenti di analisi di reti complesse utilizzati: tool di analisi iGraph in ambiente Python.

## Mobile and cloud security

Docenti: Fabio Martinelli (IIT-CNR), Paolo Mori (IIT-CNR), Andrea Saracino(IIT-CNR)
Lezioni: 14 ore; Esercitazioni: 7 ore
Ore totali: 21
CFU: 3

**Obiettivi formativi**

Il corso tratterà i principali aspetti di sicurezza dei sistemi Cloud, quali autenticazione, autorizzazione, protezione dei dati e delle risorse, multi-tenancy, etc.. Il corso tratterà anche aspetti di sicurezza per devices mobili, in particolare per quelli con sistema operativo Android, inclusi meccanismi di rilevamento e prevenzione delle intrusioni e controllo delle applicazioni.

**Programma**

Breve introduzione ai sistemi Cloud: modelli di servizio e di deployment, alcuni esempi di sistemi Cloud esistenti (e.g., Amazon AWS). Principali problemi di sicurezza dei sistemi Cloud. Gestione dell'identità, autenticazione, autorizzazione e controllo dell'utilizzo delle risorse in sistemi Cloud: alcuni esempi di soluzioni di sicurezza adottate in sistemi Cloud esistenti (e.g., Amazon AWS). Introduzione ai sistemi Android, modelli di minaccia specifici per sistemi mobili, sistemi di protezione e sicurezza per devices mobili android (sistemi di permessi e controllo accessi, verificatore di app (bouncer), antivirus, sistemi per garantire politiche di sicurezza definite dall'utente e

dell'organizzazione (p.es. Bring Your Own Device (BYOD). Sistemi di rilevamento e prevenzione delle intrusioni su devices mobili basati su tecniche di classificazione e machine learning.

## Regulations on general data protection (GDPR) and cybersecurity

Docenti: Rita Rossi (IIT-CNR)
Lezioni: 14 ore
Ore totali: 14
CFU: 2

**Obiettivi formativi**

Il corso si propone di offrire agli studenti conoscenze e approfondimenti riguardo alla normativa in materia di tutela dei dati personali attraverso l'esame del Regolamento Generale per la protezione dei dati (UE) 679/2016 (in acronimo inglese GDPR), del codice privacy (decreto legislativo 2003/196), delle linee guida e raccomandazioni emesse dal Comitato europeo per la protezione dei dati e dal Garante per la protezione dei dati personali.
Il corso si propone, inoltre, di far acquisire agli studenti conoscenze e informazioni in materia di cybersecurity attraverso l'esame del decreto legislativo 138/2024 che recepisce la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (NIS2).

**Programma**

L'insegnamento sarà incentrato sui principi fondamentali in materia di protezione dei dati personali, sui ruoli, compiti e responsabilità dei soggetti coinvolti nel trattamento: titolare del trattamento, responsabile del trattamento, autorizzati e incaricati. In questo contesto particolare attenzione sarà dedicata al Responsabile della Protezione dei Dati (DPO o RDP), la cui designazione è obbligatoria per tutte gli organismi pubblici e autorità pubbliche e per tutti i titolari e responsabili del trattamento che si trovano nelle condizioni stabilite dal Regolamento. Particolare riguardo sarà riservato al principio di accountability, che costituisce la chiave di interpretazione dei compiti e degli obblighi del titolare e del responsabile del trattamento, finalizzato a mettere in atto e dimostrare l'efficacia e l'adeguatezza delle misure di tutela dei dati personali, sia sotto il profilo organizzativo, che tecnico di sicurezza del trattamento, alla luce della natura dei dati personali trattati.
Nell'ambito del decreto legislativo 138/2024, che recepisce la direttiva (UE) 2022/2555, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione (NIS2), un preciso esame sarà rivolto agli operatori che rientrano nel campo di applicazione della normativa e ai consistenti aggiornamenti che in tale contesto vi sono stati rispetto alla prima direttiva NIS. Specifica attenzione sarà inoltre rivolta al quadro nazionale di sicurezza informatica, agli obblighi in materia di gestione del rischio per la sicurezza informatica e di notifica di incidente. Saranno, infine, prese in considerazione le misure per la vigilanza ed esecuzione in ordine alla corretta osservanza delle normative stabilite nel decreto di attuazione. L'insegnamento comprenderà, altresì, riferimenti al perimetro di sicurezza nazionale cibernetica.

## Java Fundamentals (facoltativo)

Docente: Andrea Saracino (DII-UNIPI)
Esercitazioni: 5 ore
Ore totali: 5

**Obiettivi formativi**
Il principale obiettivo del corso è di insegnare agli studenti i concetti base dello sviluppo di software in Java. Ulteriori obiettivi del corso sono l'insegnamento del pensiero computazionale, per permettere agli studenti di analizzare e decomporre problemi in passi algoritmi e di implementare tali passi in Java. Gli studenti apprenderanno a usare strutture dati di base, come array, stringhe, tabelle hash. Gli studenti impareranno a scrivere, compilare e correggere programmi in Java, sia da riga di comando che nell'ambiente di sviluppo integrato Eclipse.

**Programma**
Introduzione a Java. Introduzione e uso di Eclipse. Operatori aritmetici, logici e relazionali. Variabili e tipi di dato. Conversioni di tipo. Visibilità delle variabili. Comandi di I/O. Comandi condizionali. Comandi iterativi. Array e stringhe. Dichiarazione e definizione di funzioni. Passaggio di parametri. Introduzione a classi, oggetti e metodi. Introduzione alle classi di librerie standard. Introduzione alle interfacce e classi generiche.

# LAB MODULES

## LAB on Secure system configuration, device hardening and firewall management

Docenti: Alessandro Mancini (IIT-CNR), Filippo Lauria (IIT-CNR)
Lezioni: 7 ore; Esercitazioni: 18 ore
Ore totali: 25
CFU: 3

**Obiettivi formativi**

Il corso, basato principalmente su attività pratica, ha diversi obiettivi:

i. progettare e realizzare un'infrastruttura di rete sicura utilizzando gli apparati (switch, router, firewall) di laboratorio;
ii. mantenere il corretto funzionamento della rete realizzata, implementando delle politiche di sicurezza mediante l'uso di next-generation firewall;
iii. effettuare security test su servizi di rete alla ricerca di vulnerabilità, concentrandosi sulle applicazioni web.

**Programma**

Utilizzo di apparati di rete (switch, router e firewall): introduzione, installazione, configurazione e secure management. Realizzazione di una rete di laboratorio: vlan e routing. Configurazione di

firewall: IPS, IDS, stateful firewall e ACL. Next-generation firewall: APP-ID, CONTENT-ID, Threat Prevention, USER-ID, SSL Decryption, URL Filtering e DoS Protection.
Introduzione ai concetti base del web: protocollo HTTP, struttura degli indirizzi web (URL) e focus sull'URL-encoding. Utilizzo di strumenti specifici per il web application security testing, con particolare attenzione agli HTTP intercepting proxy. Dimostrazioni pratiche su applicazioni web create appositamente con vulnerabilità note, per apprendere l'identificazione e lo sfruttamento di problemi di sicurezza come: path traversal, file inclusion, remote code execution, con focus sulle tecniche di accesso non autorizzato all'host vulnerabile basate su reverse o bind shell.

## LAB on DNS/DNSSEC and network traffic analysis

Docenti: Maurizio Martinelli (IIT-CNR), Luca Deri (IIT-CNR)
Lezioni: 8 ore; Esercitazioni: 18 ore
Ore totali: 26
CFU: 3

**Obiettivi formativi**

Il Corso è incentrato su un laboratorio teorico-pratico ed e' finalizzato a: i) installazione e configurazione di applicazioni di rete centralizzate e distribuite; ii) installazione e utilizzo di applicazioni finalizzate all'analisi del traffico di rete. Particolare enfasi sarà data agli aspetti di sicurezza relativi a protocolli e applicazioni critiche. Questo percorso formativo farà acquisire agli studenti le competenze necessarie per erogare servizi sicuri nell'ambito di un'infrastruttura di rete affidabile e resiliente. Gli strumenti utilizzati nell'ambito del laboratorio saranno completamente open source e ciò consentirà agli studenti di poter implementare le nozioni apprese durante il corso, nella propria rete.

**Programma**

Protocolli e applicazioni critiche quali il DNS e il DNSSEC. In particolare sarà realizzata, in laboratorio, un'infrastruttura DNS che consentirà di installare, configurare e gestire uno o più nameserver autoritativi (sia dotati di DNSSEC che non), effettuare troubleshooting, analisi dei log, rollover delle chiavi, trasferimento di zona mediante autenticazione TSIG, ecc. Strumenti per la cattura del traffico di rete e sua analisi tramite sniffer (wireshark e ntopng), analisi del traffico di rete secondo il paradigma a flussi (netflow, ipfix, sflow), rilevazione di anomalie del traffico di rete (bro-ids) e monitoraggio del traffico di rete ad alta velocità.

## LAB on Secure Tool and Application

Docenti: Ilaria Matteucci (IIT-CNR), Andrea Saracino (IIT-CNR)
Lezioni: 14 ore; Esercitazioni: 14 ore
Ore totali: 28
CFU: 4

**Obiettivi formativi**

Il laboratorio prevede lo sviluppo di applicazioni di sicurezza per ambienti complessi in particolare con interazione cloud/mobile. Tra le piattaforme che saranno utilizzate vi sono OpenStack e

OpenNebula per il Cloud. Verranno anche illustrati sistemi per la protezione dei Dati integrati (Data Protection as a services).

**Programma**

In questo modulo verrà introdotta ai concetti base di cybersecurity con le principali definizioni delle proprietà di sicurezza. Saranno quindi spiegati e analizzati i passi di un attacco e saranno analizzati in dettaglio alcuni strumenti utilizzati da un attaccante.
Nel modulo verranno affrontate tecniche di programmazione sicura su device Android, attacchi e sviluppo di applicazioni malevole e contromisure e tecniche di analisi statica delle applicazioni Android.