# Programmi degli insegnamenti

## Corso di Python (facoltativo)

Docente: Alessio Bechini, DII-UNIPI
Ore totali: 27

### 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. 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. Utilizzo di ricorsione e memorizzazione. Gestione delle eccezioni. Elementi di programmazione funzionale: lambda, map, filter, reduce, list comprehensions, generator expressions. Uso dei file. Codifiche di caratteri (Unicode e utf-8). Moduli e packages. Utilizzo di generatori di numeri (pseudo) casuali. Programmazione OO: classi, istanze, metodi (di istanza, di classe, statici), inizializzazione. Ereditarietà in classi Python. Uso di Notebook. Numpy: creazione di array, loro caratteristiche e operazioni. Copia di array, Matrici. SciPy. Plotting con matplotlib/pyplot.

# FOUNDATIONS MODULES

## Networking

Docenti: Carlo Vallati (DII-UNIPI), Francesca Righetti (DII-UNIPI)
Lezioni: 16 ore; Esercitazioni: 8 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: 14 ore; Esercitazioni: 9 ore
Ore totali: 23
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. Apprendimento supervisionato. Apprendimento non supervisionato. Applicazioni delle reti neurali a problemi di classificazione, clustering e predizione.

## Web Technology

Docenti: Alessio Vecchio (DII-UNIPI), 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: 14 ore; Esercitazioni: 10 ore
Ore totali: 24
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. Controllo degli accessi. La matrice di controllo degli accessi: capability e ACL. I modelli discretionary, mandatory e role-based.

### 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: Maurizio Martinelli (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, classificazione della DF, fasi di identificazione, acquisizione e analisi delle digital evidence e relativi cenni giuridici. Analisi forense di sistemi di file sharing, con particolare riferimento alla disciplina della Digital Forensics applicata ai sistemi P2P. Analisi forense di sistemi di cloud computing con particolare riferimento ai modelli di servizio SaaS, PaaS e IaaS.

## Cyber Intelligence

Docenti: Maurizio Tesconi (IIT-CNR), Tiziano Fagni (IIT-CNR)
Lezioni: 14 ore; Esercitazioni: 10 ore
Ore totali: 24
CFU: 3

**Obiettivi formativi**

Lo scopo del corso è fornire agli studenti le principali tecniche di Cyber Intelligence, in particolare si mostrerà come utilizzare i Social Media ed i dati provenienti dal Web (visible web & dark web) per un'azione di Intelligence volta alla prevenzione e a tutela della società.
Verranno presentate le principali tecniche di acquisizione dati da fonti Web allo scopo di raccogliere e preparare i dati per ulteriori analisi, condotte ad esempio mediante tecniche di data mining e social network analysis. Verranno inoltre presentati dei casi di studio specifici nell'ambito della Cyber Intelligence: cyberbullismo, flame detection, costruzione della rete delle interazioni su social media.

**Programma**

Introduzione e definizione di Intelligence. Varie branche dell'Intelligence: Human Intelligence (HUMINT), Open Source Intelligence (OSINT), Social Media Intelligence (SOCMINT), etc. Il ciclo dell'Intelligence: pianificazione, raccolta, analisi, produzione, disseminazione. Sorgenti dati per l'Intelligence. Honeypots. Logs. Tecniche di raccolta dati da Web. Web crawling e Web scraping. Social media crawling. Deep Web e Dark Web. Strumenti in Python e Javascript per la raccolta dati da Web. La rete TOR. Scenari applicativi ed esempi di analisi: contrasto al cyberbullismo, flame detection, rete delle interazioni su social media, analisi su dati multimediali.

## Complex network analysis

Docente: Andrea Passarella (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 in R, iGraph, 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, monitoring, audit, 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., Openstack). Principali problemi di sicurezza dei sistemi Cloud. "The Notorius Nine". 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 soluzioni innovative. 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 al Regolamento Generale per la protezione dei dati (UE) 679/2016 (in acronimo inglese GDPR), alle Guidelines interpretative emesse dal gruppo di lavoro europeo in tale ambito, alla luce del decreto legislativo di adeguamento della normativa italiana alle disposizioni del Regolamento Europeo (D. Lgs. 101/2018). Ulteriore obiettivo dell'insegnamento in questione è volto all'acquisizione delle conoscenze normative fondamentali in materia di cyber security, sancite dalla direttiva Europea (UE) 2016/1148 (Direttiva NIS), che prescrive misure per un livello comune elevato di sicurezza delle reti e dei sistemi informativi nell'Unione e dal decreto legislativo di recepimento, recentemente emanato (D. Lgs. 65/2018). Il corso si propone, altresì, di far acquisire

agli studenti conoscenze e informazioni riguardo a condotte e sanzioni proprie dei più rilevanti crimini informatici.

**Programma**

Il corso tratterà i principali argomenti correlati all'entrata in vigore del Regolamento Generale Europeo per la protezione dei dati e alla imprescindibile necessità, per tutti i titolari e responsabili del trattamento, di conoscerne principi e regole, anche alla luce delle pesanti sanzioni connesse all'inosservanza delle previsioni regolamentari. Particolare attenzione sarà rivolta al Responsabile della Protezione dei Dati, (DPO o RDP) strumento obbligatorio di ausilio del titolare e del responsabile in ordine alla corretta applicazione del Regolamento stesso 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. Il Responsabile della Protezione dei Dati (RPD o DPO) rappresenta oggi una figura determinate nell'ambito del GDPR e, conseguentemente, un'opportunità lavorativa concreta, laddove gli interessati posseggano requisiti conoscitivi, tecnici e normativi, adeguati. Con riferimento agli strumenti di sicurezza dei dati e dei sistemi informativi, propri della cyber security, nello svolgimento delle lezioni saranno esaminate le norme contenute nella direttiva Europea NIS, nel decreto legislativo di recepimento, ponendo l'accento sugli obblighi previsti per gli operatori di servizi essenziali e per i fornitori di servizi digitali. Nello svolgersi degli argomenti saranno presi in considerazione, inoltre, i documenti prodotti in ambito europeo relativamente alle strategie in materia di cybersecurity con particolare riferimento alle raccomandazioni del European Network and Information Security Agency (Agenzia Europea per la Sicurezza delle Reti e dell'Informazione, ENISA), Specifico esame sarà, infine, dedicato alle condotte di cyber criminalità comportanti violazione dei diritti essenziali delle persone, danni alle informazioni e ai sistemi, al furto d'identità, alla violazione di contenuti, all'accesso non autorizzato a un sistema informatico o telematico, alla frode ed altri comportamenti penalmente rilevanti, alla luce dei più recenti sviluppi normativi e giurisprudenziali

## Java Fundamentals (facoltativo)

Docente: Nicola Tonellotto (DII-UNIPI)
Ore totali: 18

**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. Sviluppo di script python per la verifica del corretto funzionamento della DoS Protection e per l'esecuzione dei dynamic update commands sul next-generation firewall. Web application security testing. Approfondimenti su botnet IoT mediante l'utilizzo di strumenti software per la classificazione ed il riconoscimento dei nodi infetti.

### LAB on DNS/DNSSEC and network traffic analysis

Docenti: Maurizio Martinelli (IIT-CNR), Luca Deri (IIT-CNR)
Lezioni: 6 ore; Esercitazioni: 18 ore
Ore totali: 24
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 e spiegata la popolare piattaforma per secure-testing Metasploit. Inoltre, verranno utilizzati exploit e payload che sfruttano vulnerabilità su sistemi operativi Windows e Linux. Il corso affronterà l'utilizzo di tool come: MSFvenom per la creazione di malware, e di The FarRat, per sistemi operativi sia desktop che mobile.
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.

## Seminari

Docenti: esperti del settore
Ore totali: 21
CFU: 3,5