Master I Livello in Cybersecurity - A.A. 2017-18

Programmi

Pre-corso di Programmazione

FOUNDATIONS MODULES

Networking

Docenti: Giuseppe Anastasi, Carlo Vallati, DII-UNIPI

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
Concetti Introduttivi. Applicazioni di Rete. Architettura Client-Server e Peer-to-Peer. Tipologie di servizio richieste dall'applicazione. Tipologie di servizio offerte dalla rete. Reti a connessione diretta. Reti a commutazione di pacchetto. Interconnessione di reti. Internet. Formato dei datagram. Gestione degli Indirizzi. Instradamento dei datagram. Trasferimento affidabile dei dati. Reti wireless e mobili. Reti per applicazioni multimediali.

Data mining

Lezione: 16 ore; Esercitazione: 11 ore
Docenti: Beatrice Lazzerini (DII-UNIPI), Francesco Marcelloni (DII-UNIPI)

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, per individuare outlier e per risolvere problemi di ottimizzazione. Gli studenti acquisiranno la capacità di applicare tecniche di data mining nel contesto della cyber-security.

Programma
Pre-processazione 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, algoritmo A-Priori, regole associative, misure di correlazione.
Clustering: concetti base, algoritmi, metodi di valutazione dei risultati.
Individuazione degli outlier: concetti base e algoritmi.
Classificazione: concetti base, reti neurali artificiali, metodi di valutazione dei risultati.
Algoritmi genetici a singolo obiettivo e multi-obiettivo.
Applicazioni nel contesto della cyber-security.

Web Technology

Lezione: 16 ore
Docenti: Marco Avvenuti, Mario Cimino, DII-UNIPI

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

Docente: Gianluca Dini (DII-UNIPI)
Esercitatore: Pericle Perazzo

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 cifrario 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

Docente: Michele Pagano, DII-UNIPI, Christian Callegari, CNIT; Esercitatore: Christian Callegari, CNIT

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; Esercitatore: Vincenzo Maffione

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 persenterà 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)

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

Docente: Maurizio Tesconi, IIT-CNR; Esercitatore: Stefano Cresci, IIT-CNR

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.

Large-scale network analysis

Docente ed esercitatore: Andrea Passarella, IIT-CNR

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: F. Martinelli, P. Mori Esercitatori: A. Saracino, G. Costantino

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.

Legal aspects of cybersecurity

Docenti: Rita Rossi, IIT-CNR
Lezione: 12 ore

Obiettivi formativi
Il corso si propone di offrire agli studenti: 1. le conoscenze giuridiche fondamentali, necessarie ad inquadrare la normativa che regolamenta i settori oggi più esposti ad attacchi di cyber criminalità, quali le normative a tutela dei diritti della personalità, del corretto trattamento dei dati, con specifico riferimento al settore delle comunicazioni, nonché la disciplina dei reati informatici più ricorrenti; 2. La conoscenza e l'analisi dei contesti normativi e fattuali che caratterizzano le strategie dell'Unione Europea nel settore della cybersecurity, considerato strategico per la sicurezza, oltreché della persona e delle imprese, anche dell 'assetto politico ed economico dei paesi dell'Unione europea.

Programma
Il corso tratterà gli aspetti correlati al vasto campo della cyber criminalità con riferimento, fra gli altri, alla violazione delle informazioni, dei dati personali, anche di natura sensibile, 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, ponendo in evidenza i rischi generali per la sicurezza dei singoli, delle imprese e dei Paesi stessi. 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), nonché la Direttiva dell'Unione Europea relativa all'individuazione e alla designazione delle infrastrutture critiche europee e alla valutazione della necessità di migliorarne la protezione."

LAB MODULES

LAB on Secure system configuration, device hardening and firewall management

Lezione: 8 ore; Esercitazione: 20 ore
Docente: Abraham Gebrehiwot (IIT-CNR);
Esercitatori: Abraham Gebrehiwot (IIT-CNR), Filippo Lauria (IIT-CNR)

Obiettivi formativi
Il corso ha diversi obiettivi: i) gettare basi solide su tematiche pratiche di networking; ii) fornire nozioni pratiche su come progettare e realizzare un'infrastruttura di rete sicura utilizzando apparati (switch, router) reali della CISCO Systems; iii) illustrare come mantenere il corretto funzionamento della stessa, prevenendo malfunzionamenti e/o attacchi legati a problemi di sicurezza utilizzando un firewall e diversi strumenti tipicamente usati dagli amministratori di rete e dai gestori dei servizi.

Programma
Richiami su protocolli di routing e switching. Apparati di rete (switch, router e firewall): introduzione, installazione, configurazione e secure management. Realizzazione di una rete di laboratorio: vlan, routing. Configurazione di firewall: IPS, IDS, stateful firewall e ACL. Precauzioni per la sicurezza di rete: Secure VPN, device hardening. IPv6: generalità, gli indirizzi, il datagramma; ICMPv6: NDP; Attacchi all'IPv6. Individuazione e mitigazione delle anomalie di rete: ARP Spoofing, Rogue DHCP Servers, Rogue RAs e IP-Collision Detection (utilizzo di tools come 6MoN, nmap, wireshark, ecc.). Attacchi alle password (sia on-line che off-line) e metodi di protezione. Controllo degli eventi in corso su sistemi unix-like: analisi e attacchi sui logs di sistema (utilizzo di tools come zap, cloak, ecc.). Malware: tassonomia ed analisi di sistemi compromessi.

LAB on Secure cyber security and risk monitoring for networks and applications

Docenti: Maurizio Martinelli (IIT-CNR), Luca Deri (IIT-CNR); Esercitatore: Maurizio Martinelli (IIT-CNR), Luca Deri (IIT-CNR)

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 application development (network, mobile, cloud)

Docenti: G. Costantino; Esercitatore: G. Costantino, A. Saracino

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
Mobile. Tecniche di programmazione sicura su devices android e relatiche problematiche (p.es OWASP). Techniche di testing di sicurezza ed analisi formale per modelli astratti di protocolli di comunicazione sicura. Schemi di progetto sicuri per applicazioni mobile e cloud sicure con il paradigma data protection as a service.
Installazione, configurazione, ed utilizzo di strumenti di autenticazione, autorizzazione e controllo dell'utilizzo per sistemi Cloud basati su Openstack ed OpenNebula. Definizione delle relative politiche di sicurezza per scenari realistici.