Parte I - Formazione Culturale

I.1 Introduction to Cyber Security

Responsabile: Rodolfo Zunino
Ore: 8

(4 ore Prof. Rodolfo Zunino, 4 ore Ing. Ermete Meda)

Pre-requisiti:

- (nessuno, trattandosi di modulo di presentazione degli argomenti e delle terminologie fondamentali usate nel contesto del Master)

Programma:

- CyberSecurity: aspetti generali
- Panoramica dei Moduli e razionale del syllabus
- Nozioni fondamentali di tecnologia di security (algoritmi, protocolli, appliance di rete) e di governance

Principali competenze apprese:

- Terminologia e aspetti generali di CyberSecurity

I.2 Computer Security

Responsabile: Giovanni Lagorio
Ore: 24

(8 ore Prof. Giovanni Lagorio, 8 ore Prof. Giovanni Chiola, 6 Dr. Alessandro Tomasi, 2 ore Dr. Stefano Berlato)

Pre-requisiti:

- Conoscenza base di sistemi operativi
- Conoscenza base di programmazione

Programma:

- Identificazione e Autenticazione
- Password cracking
- Software security
- Autorizzazione a livello di S.O., in particolare in ambiente POSIX
- Discretionary vs Mandatory Access Control

- ACL vs capability
- Confused deputy problem
- Memoria sicura
- Modelli, Meccanismi e Linguaggi per il Controllo degli Accessi
- Modello Role Based Access Control (RBAC)
- Modello Attribute Based Access Control (ABAC)
- Il controllo degli accessi e la privacy, questioni di conformità con il GDPR

Principali competenze apprese:

- Principi e tecniche di controllo degli accessi
- Comprensione delle vulnerabilità software più diffuse
- Principi e strumenti per il secure coding

I.3 Information Security Management and Legals

Responsabile: Ermete Meda
Ore: 24
(12 ore Avv. Elena Bassoli, 12 ore Ing. Ermete Meda)

Pre-requisiti:

- Utilizzo di un Personal Computer
- Informazioni pubbliche sugli attacchi informatici

Programma:

- Scenario Globale e Necessità di un Sistema di Gestione della Sicurezza delle Informazioni (ISMS - Information Security Management System):
  - Il Cyberspace
  - L'evoluzione dell'ICT e la Cyber Security
  - L'evoluzione delle minacce: breve storia degli attacchi ed incidenti informatici
  - I difetti della tecnologia: le vulnerabilità di reti, sistemi e applicazioni – Il fattore umano
  - Il Budget ICT e Cyber Security - Relazioni e Problemi con l'Alta Direzione
- Natura di un ISMS:
  - La triade CIA (Confidentiality, Integrity and Availability)
  - I principi di base
  - Il ciclo PDCA di Deming
  - Il significato e i contenuti del "Fare Sicurezza": le tre fasi temporali (Prevention, Detection & Reaction) e le tre aree di pertinenza (Tecnologica, Organizzativa e Legale)
  - La terna GRC: Governance, Risk e Compliance
  - Il Governo della Sicurezza delle Informazioni nell'ambito dei processi aziendali, la separazione dei ruoli e delle responsabilità, il CIO e il CISO, la tabella RACI, il corpus documentale necessario

- Definizione di SOC, CERT e Computer Forensics
- Introduzione alla legislazione europea ed italiana relativa alla Sicurezza delle Informazioni e alla Cybersecurity
- Esempio di implementazione di un ISMS

- Introduzione all'Informatica giuridica
- La cybersecurity nel Reg. UE/2016/679

Principali competenze apprese:

- Debolezze, Vulnerabilità e Minacce che insistono sulle infrastrutture IT.
- Significato della frase "Fare Sicurezza" e della natura di un ISMS
- Saper progettare un ISMS, definirne Governance e Corpus Documentale
- Le basi dell'Informatica Legale e del Codice Europeo della Privacy

---

I.4 Network Security

Responsabile: Marchese Mario

- **(12 ore Prof. Mario Marchese, 10 ore Prof. Giovanni Chiola, 6 ore Prof. Enrico Russo)**

Ore: 28

Pre-requisiti:

- Basi di reti di calcolatori

Programma:

Reti TCP/IP – 12 ore (M.Marchese)

- Introduzione alle Reti di TLC
- Commutazione di pacchetto e di circuito
- Concetti di protocollo e servizio
- Architettura a livelli funzionali
- Ethernet, 802, 802.1q, Fieldbus, Industrial Ethernet
- HDLC, PPP
- IP
- TCP/UDP
- PMU e interconnessione di PMU

Introduzione alle problematiche di sicurezza di rete

…….

Principali competenze apprese:

- Basi di network security

I.5 Cryptography

Responsabile: Giovanni Lagorio

- **Ore: 24**
- **(10 ore Prof. Giovanni Lagorio, 10 ore Prof. Giovanni Chiola, 4 ore Prof. Rodolfo Zunino)**

Pre-requisiti:

- **…**
- **….**

Programma:

- Segretezza perfetta
- Cifratura a chiave segreta; cifrari a blocchi e a flusso
- Message authentication code
- Funzioni Hash e applicazioni
- Crittosistemi a chiave pubblica, firma digitale e certificati digitali

Principali competenze apprese:

- Capacità di analisi di sistemi crittografici e uso corretto delle primitive

Parte II - Formazione Professionale

II.1 Security and Threats to Critical Infrastructures

Responsabile: Paola Girdinio
Ore: 12

- **(4 ore Prof.ssa Paola Girdiniio, 4 ore Ing. Francesco Perna, 4 ore Prof. Mario Marchese)**

Pre-requisiti:

- Reti di telecomunicazioni

Programma:

Introduction to security and threats over critical infrastructures - (M.Marchese) – 4 ore

- The Need of Security and Resilience
- Physical security and Cybersecurity
- Definition of critical infrastructure
- Sectors linked to critical infrastructures
- Cybersecurity of critical infrastructures
- ICS and SCADA systems
- Security of ICS
- Impact of networking and IoT
- Smart City and Smart Industry
- SCADA network communication architecture
- SCADA systems security and evolution
- Real world attacks
- ICS security properties
- Security threats faced by SCADA networks
- Standard attacks on SCADA networks
- Taxonomy of cyber attacks to SCADA systems
- Standards and guidelines
- Detection of SCADA attacks
- Intrusion Detection Systems: definition and classification
- Misuse and Anomaly detection, examples of features sets

Security and threats over critical infrastructures: Cyber Security as the key enabler, framework, organization and CERT - (Perna/Girdinio) – 8 ore

- ENEL Digital Journey
- The transition in the Energy Industry
- The paradigm change in the utilities
- The digital transformation
- The growth of generated data and expenses: M2M, IoT and Big Data
- IT/OT/IoT convergence
- Cybersecurity regulations
- NIS Directive
- A new approach to security
- Cyber Security as the key enabler in Enel digital plan
- Cloud transformation journey of Enel
- Framework, organization and CERT
- Computer Emergency Response Team (CERT)
- CERT services
- Information sharing
- Service activation for incidents management
- Incident identification, analysis and response

Principali competenze apprese:

- What is a critical infrastructure and how it is managed through ICS and SCADA systems
- Impact of networking and IoT over SCADA systems security
- ICS security properties
- Security threats and attacks
- Detection of SCADA attacks
- Cyber Security as the key enabler
- Framework, organization and CERT
- The concept of CERT

II.2 Cryptographic Protocols

Responsabile: Alessandro Armando

Ore: 16 ore

- **(8 ore Prof. Alessandro Armando, 4 ore Dr. Roberto Carbone, 4 ore Prof. Rodolfo Zunino)**

Pre-requisiti:

- Protocolli di rete (TCP/IP)
- Modello ISO/OSI

Programma:

- Basic notions (protocol execution, assumptions and goals, attacker model)
- Cryptography (black box view)
- Reply protection (timestamps, nonces)
- Examples of protocols and attacks (NSPK, Otway-Rees, Andrew Secure RPC, Denning & Sacco)
- Prudent engineering of security protocols
- Kerberos (architecture, protocol, inter-realm communication, limitations)
- SSL/TLS, SSH
- GPG
- Elliptic Curve Cryptography (ECC): nozioni teoriche, ECDH, ECDSA
- Introduzione alla tecnologia blockchain e del consenso distribuito alla base delle applicazioni decentralizzate

Principali competenze apprese:

- Principi di funzionamento dei protocolli crittografici
- Obiettivi di sicurezza
- Principali vulnerabilità, attacchi e meccanismi di protezione
- Conoscenza del formalismo e delle tecnologie relative alle applicazioni dell'Algebra basata su Curve ellittiche

- Conoscenza del funzionamento di crittovalute

II.3 Blockchain Technologies

Responsabile: Marina Ribaudo
Ore 16 ore

- **(12 ore Prof.ssa Marina Ribaudo, 4 ore Dr. Paolo Dal Checco)**

Pre-requisiti:

-
-

Programma:

- Introduzione alla tecnologia blockchain e del consenso distribuito alla base delle applicazioni decentralizzate
-

Principali competenze apprese:

- Conoscenza del funzionamento di crittovalute
-

II.4 Web Security

Responsabile: Alessio Merlo
Ore: 20 ore

- **(4 ore Prof. Alessio Merlo, 4 ore Prof. Alessandro Armando, 8 ore Dr. Giuseppe Porcu)**

Pre-requisiti:

- Conoscenza base contesto e protocolli web (HTTP/S,Ftp,Smtp,...) e applicazioni ad esso correlati (browser, client generici)
- Conoscenza base linguaggi di programmazione server-side e client-side nel contesto web (HTML, Javascript, PHP, Java, Asp, etc..)

Programma:

- Fundamentals Web Application Security (APPSEC)
- Sicurezza applicativa nel ciclo di sviluppo del software (Secure - Software Development Life Cycle)
- Metodologia di testing basata su OWASP Testing Guide
- Analisi tecnica vulnerabilità e attacchi basati sulla OWASP Top 10

Principali competenze apprese:

- Conoscenza security in contesto applicativo web
- Metodologia e strumenti per analizzare applicazioni web basati su metodologia OWASP Testing Guide
- Analisi attacchi web basati su OWASP Top 10

II.5 Information Security & Risk Management

Responsabile: Ermete Meda
Ore: 28
(12 ore Ing. Ermete Meda, 12 ore Dr. Fabio Guasconi, 4 ore Dr. Enrico Ferretti)

Pre-requisiti:

- Modulo Information Security Management and Legals o conoscenza equivalente

Programma:

- La necessità di disporre di standard e best practice nella rivoluzione industriale
- La produzione degli Standard Internazionali: Organismi BSI e ISO
- La Normazione Internazionale ISO, lo standard per il Sistema di Gestione della Qualità ISO 9001 e l'estensione agli altri Sistemi di Gestione
- Gli Standard Internazionali e le Best Practice di Information & Cyber Security
- Il processo di Certificazione volontaria di terza parte
- La famiglia ISO/IEC 27000
- Introduzione alle norme ISO/IEC 27001 e 27002
- La compliance di un ISMS allo standard ISO/IEC 27001
- Procedure e modalità e gestione degli Audit interni di prima e seconda parte. Norme internazionali di riferimento

- Introduzione alla Continuità Operativa: Alta Affidabilità, Fault Tolerance, Business Continuity e Disaster Recovery
- La Gestione del Rischio:
  - Scope, Asset e Classificazione dell'Informazione
  - Risk Assessment, Gap Analysis, Risk Treatment e Reduction
  - Esempi di Calcolo del Rischio: con metodi artigianali e mediante strumenti SW commerciali
  - L'Analisi del Rischio secondo gli standard ISO 31000 e ISO/IEC 27005
- L'organizzazione delle attività di Vulnerability Assessment e Penetration Test
- La definizione di un modello di Information Security Governance:
  - Contromisure ispirate alla Defense in Depth e Maturity Model
  - Requisiti e Policy per la Sicurezza delle Informazioni
  - Strumenti SW a supporto delle conformità di legge
  - Vulnerability Management & Exposure, Virtual Patching
- Etica nell'Informatica: i pericoli della Tecnomediazione, il Codice Etico, i nuovi interrogativi posti dai sistemi autonomi e robotizzati

Principali competenze apprese:

- Conoscere approfonditamente la natura di un ISMS coerente con le norme e le best practice internazionali e saperlo implementare e gestire in un'organizzazione

---

II.6 Business Continuity and Crisis Management

Responsabile: Susanna Buson
Ore: 16
(12 ore D.ssa Susanna Buson, 4 ore Dr. Diego Marson)

Pre-requisiti:

- Nessuno

Programma:

- Concetti di Business Continuity
- Standard 22301
- Metodologia per la gestione di Programma di Business Continuity (basato sulle GPG 2018 del Business Continuity Institute)
- Policy di Business Continuity
- Ruoli e responsabilità nella Business Continuity
- Business Impact Analysis e Risk Assessment
- Progettazione di soluzioni di continuità
- Realizzazione di soluzioni di continuità
- Esercitazione e test
- Miglioramento continuo
- L'incorporazione della Business Continuity nella cultura aziendale

- Concetti di Crisis Management
- Esercitazione Table Top di Crisis Management
- Definizione di SOC e CERT e interazione con la Business Continuity attraverso il processo di gestione degli incidenti e di escalation

Principali competenze apprese:

- Competenza base per il professionista della Business Continuity

---

II.7 Legal Informatics, Privacy and Cyber Crime

Responsabile: Elena Bassoli

Ore: 36

- **(8 ore Avv. Elena Bassoli, 4 ore Ing. Ermete Meda, 4 ore Ing. Roberto Surlinelli, 8 ore Prof. Rodolfo Zunino, 8 ore Studio Legale Losengo Soliani, Avv. Elisa Marini, Avv. Vincenzo Morgione, 4 ore Dr. Giorgio Volta)**

Pre-requisiti:

- Nessuno

Programma:

- (Losengo) Le basi del diritto penale: reati, delitti e contravvenzioni, depenalizzazione 2016, elementi soggettivi ed oggetti di reato. Concetto di imputabilità. Tipologia di sanzioni.
- (Losengo) Reati ordinari in Rete: diffamazione, ingiuria, sostituzione di persona, atti persecutori.
- (Losengo) I crimini informatici: L. 547/1993.
- (Surlinelli) La Convenzione di Budapest e la L. 48/2008: metodologie di acquisizione delle prove digitali
- (Surlinelli) La pedopornografia: L. 38/2006.
- (Zunino) Caratteristiche del Cybercrime, e genesi del Cybercrime e Identità Digitale,
- (Bassoli) La tutela del software e delle opere dell'ingegno ex L. 633/1941.
- (Bassoli) La tutela dei dati personali nel nuovo Regolamento europeo 2016/679 (GDPR) e decreto legislativo di adeguamento n. 101/2018.
- (Bassoli) Convenzione internazionale di Budapest del 2001 contro il Cybercrime. L. 48/2008 di sottoscrizione, Dir. UE 2016/680 sui dati personali e le forze di polizia
- (Meda) La norma internazionale IEC 62443 sulla Cybersecurity Industrial e panoramica sulla legislazione internazionale ed europea in materia di Cybersecurity: direttive NIS e NIST, GDPR, Cybersecurity Act e Cybersecurity IoT
-

Principali competenze apprese:

Conoscenza dei fondamenti di diritto dell'informatica con particolare attenzione ai risvolti penalistici connessi alla cybersecurity, mediante analisi di singole fattispecie di reato e di illecito, in relazione sia ai reati ordinari che assumono rilievo nelle condotte criminose commesse a mezzo di uno strumento informatico o telematico, sia ai più specifici computer crime introdotti dalla L. 547/1993. Caratteristiche del Cybercrime, e genesi del Cybercrime e Identità Digitale, cenni su transnazionalità del Cybercrime. Analisi degli illeciti contenuti all'interno della L. 633/1941 sul diritto d'autore, L. 48/2008 in esecuzione della Convenzione di Budapest, con relative modifiche al cpp in ordine alla valenza probatoria della prova digitale acquisita secondo le Best practices internazionali della digital forensics, L. 38/2006 sulla pedopornografia, fondamenti di tutela dei dati personali ai sensi del Regolamento europeo 2016/679 e d. lgs. 101/2018.

II.8 Fundamentals of Computer Forensics

Responsabile: Mattia Epifani
Ore: 8
(4 ore Dr. Mattia Epifani, 4 ore Dr. Danilo Massa)

Pre-requisiti:

- Conoscenza di base dei principali file system e sistemi operativi

Programma:

- Digital forensics e digital evidence: definizioni e aspetti tecnici di base
- Le linee guida e le best practices in materia
- Digital Forensics Process Model
- Ordine di volatilità
- Forensic imaging
- Chain of custody
- Digital Forensics & Incident Handling
- NIST sp 800-86 Recommendations
- Enterprise Forensics elements

Principali competenze apprese:

- **Comprendere gli aspetti di base della Digital Forensic**

II.9 Cyber Security in Financial and Credit Systems

Responsabile: Rodolfo Zunino
Ore: 4
(4 ore Dr. Luca Gaudio)

Pre-requisiti:

- Nessuno

Programma:

- Aspetti specific della Cyber security nel settore bancario
- Policy e normativa

Principali competenze apprese:

- Consapevolezza delle specifiche tematiche relative al settore Bancario/Finanziario e loro peculiarità

II.10 Cybersecurity in SCADA Systems, Industry, Power, and Energy

Responsabile: Mario Marchese

Ore: 32

(6 ore Prof. Mario Marchese, 6 ore Dr. Alessio Aceti, 6 ore Ing. Gaetano Sanacore, 6 ore Ing. Micaela Caserza Magro, 6 ore Ing. Gabriele Nani, 2 ore Ing. Lorenzo Ivaldi)

Pre-requisiti:

- Conoscenze di base sulle infrastrutture critiche e sui Protocolli Industriali (TCP/IP based)
- Conoscenza base delle reti industriali (IT/IIoT/OT)
- Basi di ICS and SCADA systems

Programma:

Industrial Networks: Reti di Comunicazione in tempo reale (M. Caserza Magro) – 6 ore)

- I sistemi di automazione
- I protocolli di comunicazione
- Gli standard di riferimento
- Profinet, Profibus

Cybersecurity for Power and Energy (M. Marchese) – 8 ore

- Link to Critical Infrastructures and ICS
- Transmission and Distribution Grid
- ICT model in a transmission system and in a distribution system
- Elements: SCADA and PMU
- Vulnerabilities in power systems
- PMU and Networking, PMU Network as a SCADA Network
- PMU Network as a part of a Smart GRID
- PMU architecture and standards
- Practical example of PMU communications interfaces: Ethernet

Communication, Serial Communication, RS232, RS485, K-BUS

- Available Data Protocols over Ethernet and Serial solutions
- IEEE C37.118-2005
- IEEE C37.118 - Data type format
- Cyber attacks to PMU networks
- Microgrids: control loop and requirements
- Microgrids: vulnerabilities and vectors, Cyber-incidents and Violations
- Impacts of cyberattacks on microgrid operations
- Defense-in-Depth framework enabled by SDN technologies
- Vulnerability assessment in a smart grid
- Major standards for operating a smart grid
- MODBUS: protocol, PDU, function codes
- Operative Examples

Cyber Security of SCADA Systems: Drive effective operations with complete plant information (Nani) – 8 ore

- Overview
- SCADA concept and high level structure
- S+ Operations Overview
- Architecture
- High performance workplace
- Integrated alarm management
- Integrated information management
- Secure operations
- IT vs OT best practices
- Cybersecurity for ABB, position and approach
- ABB cybersecurity in a power plant
- Cybersecurity workplace
- Network Monitoring
- Security patch and anti-virus updates
- Backup and recovery solutions
- Physical hardening
- COC evolution to support SOC features

Cyber defense approach in SCADA/ICS/OT systems for manage the generation/ transmission/ distribution systems (G. Sanacore) – 8 ore

- Cyber Defense approach in Generation/Transmission/Distribution Systems;
- A2A Power Energy Systems Resilience approach;
- Overview to National security Framework – NIS Directive approach;
- Computer Security Incident Response Team(CSIRT) overview - A2A case study;
- Overview to Cybernetic National Security Perimeter (L. n.133);

- Cyber Security compliance for systems/devices procurement;
- ISO/IEC Protocols security suite(CT 57) for Electrical SCADA Systems;
- New IIoT Protocol security suite for Industrial-OT networks;
- Policy for Managing the Electrical Grid Security in SCADA/ICS systems;
- Smart Grid, Power Plants, Transmission & Distribution Grids Cyber Security procedures;
- System security solution & Case study

Cybersecurity and ICS: how can we handle critical infrastructures hacking? (Aceti) – 8 ore

- How did we get involved
- Critical Infrastructures being hacked everyday
- How does it happen?
- What do we learned?
- How can we handle?
- IT and ICS cyber kill chain
- What do you need: patrolling or investigating?
- ICC IoT Security Maturity Model
- Industroyer attack scheme
- Recap
- Assess your SOC
- Alignment to the NIST Cybersecurity framework
- You cannot do it alone
- Virtual CISO
- Ho to disclose cyber incidents?
- Global ICS situation: ransomware, common malware, vulnerabilities
- What to do
- Browser isolation
- Cyber-physical security
- Phased-approach
- Threat Assessment
- Situational Awareness
- Countermeasures
- Operative examples

Principali competenze apprese

- Industrial Networks: solutions and protocols
- Architectures, protocols, vulnerabilities and solutions in Power and Energy systems
- Cyber Security operations driven by complete plant
- Cyber defense approach in generation/distribution systems
- Critical infrastructures hacking Handling

II.11 IoT Applications Security

Responsabile: Alessio Merlo
Ore: 20
(8 ore Prof. Alessio Merlo, 8 ore Luca Verderame, 4 ore Konrad Wrona)

Pre-requisiti:

- Basi di sistemi operativi;
- Nozioni di linguaggi di programmazione ad oggetti (Java);
- Conoscenza di base di cybersecurity;

Programma:

- Introduzione all'IoT e ai principali sistemi operativi e scenari di applicazione;
- Principali sfide di sicurezza del mondo IoT: focus sulla sicurezza delle applicazioni;
- Introduzione ad Android Things e allo sviluppo di app;
- Focus sulla sicurezza di Android Things;
- Valutazione di sicurezza delle applicazioni per Android Things;
- Cloud Computing e IoT: basi teoriche, scenari applicativi e di sicurezza;

Principali competenze apprese:

- Conoscenza del mondo IoT e dei principali scenari applicativi;
- Conoscenza delle principali sfide di sicurezza nel mondo IoT con focus sull'aspetto applicativo;
- Conoscenza dei meccanismi di sicurezza del s.o. Android Things;
- Conoscenza delle pratiche e delle metodologie per valutare la sicurezza delle applicazioni per Android Things;
- Conoscere e scegliere gli strumenti più adeguati di Cloud Storage/Computing per specifici scenari di CyberSecurity nel mondo IoT;

II.12 Defense-in-Depth Strategies for Critical Infrastructures

Responsabile: Luca Verderame
Ore: 12

Pre-requisiti:

- Conoscenza di base delle principali problematiche legate alla cybersecurity;
- Conoscenze base di network security e application security;

Programma:

- Overview sulle infrastrutture critiche;
- Componenti principali di una infrastruttura critica;

- Sicurezza di una infrastruttura critica - problemi e sfide;
- Esempio di attacchi su una infrastruttura critica;
- Strategie di Defence-in-Depth per le infrastrutture critiche;

Principali competenze apprese:

- Conoscenza dei principali componenti che costituiscono una infrastruttura critica;
- Conoscenza dei principali rischi di sicurezza delle infrastrutture critiche;
- Conoscenza delle principali strategie di Defence-in-Depth per le infrastrutture critiche;

II.13 Standards and Best Practices for Security and Safety

Responsabile: Paola Girdinio
Ore: 16
(6 ore Dr. Gianluigi Pugni, 6 ore Dr. Yuri Rassega, 4 ore Com. Stefano Ramacciotti)

Pre-requisiti:

- Moduli dedicati alle Infrastrutture Critiche
- Modulo Information Security & Risk Management
- Modulo Legal Informatics, Privacy and Cyber Crime

Programma:

- Introduction to Cyber Security Standards for ICS Systems (Pugni)
- Cyber Security Controls for ICS Systems and Standard Mapping (Pugni)
- IEC62351 in Depth (Pugni)
- Cyber Security in Enel (Rassega)
- La norma ISO/IEC 15408 (Common Criteria) per la Certificazione di sicurezza di prodotti e sistemi IT (Ramacciotti)
- D.lgs 205/2019: Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica

Principali competenze apprese:

- Conoscenza delle norme di Security & Safety per lee Infrastrutture Critiche

---

II.13 Social Engineering and Intelligence for Cyber Security

Responsabile: Rodolfo Zunino
Ore: 16

Pre-requisiti:

- Conoscenza delle tecniche di crittografia e dei protocolli di autenticazione

Programma:

- Basi sociologiche, psicologiche e cognitive del S.E.
- Tecniche fondamentali di Social Engineering
- Tipologie di attacchi basati su S.E.

Principali competenze apprese:

- Metodologie di difesa contro attacchi di S.E.
- Procedure e requisiti di Governance per contrastare attacchi di S.E.
- Tecniche di progetto di sistemi di (cyber)security resistenti a attacchi di S.E.

Parte III - Specializzazioni

Indirizzo 1: Digital Forensics & Penetration Testing

IN1.1 Incident Response and Forensics Analysis

Responsabile: **Mattia Epifani**
Ore: **24**

Pre-requisiti:

- Aver frequentato e superato l'esame del corso di "Fundamentals of Computer Forensics"

Programma:

- Incident Handling procedure for IT/IoT (NIST 800-61) (8 ore) (Massa)
- File system forensic analysis (8 ore) (Picasso)
- Window forensic analysis (8 ore) (Epifani)
- Mobile forensics analysis (4 ore) (Epifani)
- Case studies (4 ore) (Picasso-Meda)

Principali competenze apprese:

- Fornire le basi per l'implementazione di una procedura per la gestione degli incidenti basata sulle raccomandazioni del NIST (sp 800-61rev.2)

- Fornire le competenze di base per la raccolta di fonti di prova informatica e la relativa analisi al fine di un eventuale utilizzo in giudizio

---

IN1.2 Malware Analysis

Responsabile: Danilo Massa
Ore: 24

Pre-requisiti:

- Aver frequentato il corso di Incident Response and Forensic Analysis
- Conoscenze di base su protocolli di rete (DNS, HTTP/S, SMB/CIFS,...)
- Conoscenze di base in linguaggi di sviluppo (C/C++, Python, …)

Programma:

- Funzionalità del malware
- Tecniche di analisi statica e dinamica (base ed avanzata)
- Sandbox commerciali ed open source
- Realizzazione di un virtual lab per l'analisi in sicurezza di campioni maligni
- Reverse engineering di eseguibili malevoli
- Malware scripts
- Individuazione ed utilizzo di IoC (indicatori di compromissione) inerenti il malware

Principali competenze apprese:

- Procedura di analisi
- Individuazione degli IoC per individuare, contenere ed eradicare malware
- Strumenti e tecniche per l'analisi di campioni (file) sospetti

---

IN1.3 Mobile Security

Responsabile: Alessio Merlo
Ore: 12

Pre-requisiti:

- Conoscenza linguaggi di programmazione ad oggetti e basi di sistemi operativi
- Contenuti dei corsi di Web, Computer e Network Security

Programma:

- Fundamentals del sistema operativo Android
- Meccanismi di sicurezza di Android
- Tecniche di analisi statica e dinamica per applicazioni mobili

- Tecniche di evasion di malware mobili
- Utilizzo di tool per analisi di app Android: ApkTools, dex2Jar, JD-GUI, MobFS, …
- Analisi di malware Android reali su dispositivi emulati

Principali competenze apprese:
- Conoscenza della struttura delle applicazioni Android
- Metodologie e strumenti per analizzare applicazioni mobili
- Conoscenza delle principali tecniche adottate da malware su Android

---

IN1.4 Cloud Security

Responsabile: **Alessio Merlo**
Ore: **12**

Pre-requisiti:
- Competenze di Web Security (OWASP testing guide - corso Web Security)
- Software di virtualizzazione VirtualBox installato e funzionante

Programma:

Il Cyber Exercise è suddiviso in due momenti formativi in cui i partecipanti dovranno prima agire come attaccanti (red team) ed in seguito come incident handlers (blue team).
Più in dettaglio la prima fase consiste in una sfida CTF (capture the flag) boot2root, in cui i partecipanti dovranno ricercare alcune vulnerabilità web 0-day su una macchina virtuale fornita e sfruttarle per ottenere un accesso non autorizzato, mentre nella seconda fase i partecipanti dovranno analizzare la macchina stessa per individuare gli artefatti che indicano le operazioni di attacco e compromissione da loro eseguite.

Principali competenze apprese:
- Eseguire una ricerca di vulnerabilità applicative ed eseguire attacchi specifici
- Individuare gli indicatori di compromissione da utilizzarsi per istruire eventuali strumenti di identificazione/protezione.

Indirizzo 2: Critical Infrastructure Protection and Security Assurance

IN2.1 Cyber Defense and Cyber Intelligence

Responsabile: Rodolfo Zunino
Ore: 24

Pre-requisiti:

- Conoscenze di problematiche legate a CyberCrime e Social Engineering

Programma:

- Advance Persistent Threat (APT) (Zunino)
- Artificial Intelligence per Cyber Security (Zunino)
- Text mining per intelligence OSINT (Zunino)
- Cyber Warfare: aspetti specifici e metodologie di difesa (Rebora)
- Intelligence per difesa preventiva e CyberWarfare (Rebora)
- Metodi di Analisi per Cyber Defence preventiva (Martinazzo)
- Tecniche di Difesa aziendale contro Cyber Attacks (Prosperi/Castagnara)

Principali competenze apprese:

- Metodologie e procedure per la prevenzione e il contrasto ad attacchi APT
- Metodologie e procedure per OSINT

IN2.2 Standards for ISMS and BCMS Certification: ISO/IEC 27001, ISO 22301

Responsabile: Alessandro Cerasoli
Ore: 24
(20 ore Ing. Alessandro Cerasoli, 4 Dr. Fabio Andresi)

Pre-requisiti:

- Modulo Information Security & Risk Management o equivalente
- Modulo Business Continuity and Crisis Management o equivalente

Programma:

- L'impostazione delle norme per i Sistemi di Gestione: struttura HLS e requisiti
- Cenni sulle linee guida delle famiglie ISO/IEC 270xx e ISO 223xx
- I Requisiti della ISO/IEC 27001 e della ISO 22301: comprensione degli aspetti legati alla direzione dell'organizzazione
- L'approccio al rischio nelle norme ISO (cenni alla ISO 31000) e le modalità di implementazione per gli ISMS e i BCMS
- Panoramica sui controlli della ISO/IEC 27002
- Esempi di applicazione dei controlli in situazioni reali
- Estensione della ISO/IEC 27002 alla applicazione dei controlli di sicurezza in ambito cloud - ISO/IEC 27017

- Certificazione di terza parte; obiettivi e vantaggi per le organizzazioni
- Il processo di audit di terza parte: pianificazione ed esecuzione

Principali competenze apprese:

- Conoscenza degli standard relativi alla sicurezza delle informazioni
- Approccio per l'Impostazione di un Information Security Management System e di un Business Continuity Management System basato sugli standard ISO
- Conoscenza delle contromisure di sicurezza in ambito tradizionale e cloud
- Conoscenza di base per conduzione attività di audit

IN2.3 Physical Security

Responsabile: Antonio Rebora
Ore: 12
(8 ore Ing. Antonio Rebora, 2 ore D.ssa Tiziana Alliani, 2 ore Ing. Andrea Conca)

Pre-requisiti:

- Conoscenze dei concetti di base su Infrastrutture Critiche
- Conoscenza base dei principali componenti che costituiscono una infrastruttura critica;
- Conoscenza base dei principali rischi di sicurezza delle infrastrutture critiche;

Programma:

- Il dominio della sicurezza fisica e sue interdipendenze con gli altri ambiti. Concetto di interconnessione.
- Concetto di profondità della sicurezza.
- Policy
- Analisi del rischio, richiami dei concetti base
- Minacce, contromisure e capacità abilitanti
- L'architettura di un sistema di sicurezza fisica in un'infrastruttura critica
- La Centrale Operativa:
    - Struttura fisica e logica
    - Il dominio della prevenzione
    - Gestione della crisi
    - Quick Response Team
    - Comunicazione in Emergenza e relazioni con l'esterno
    - Business Continuity
- Le Infrastrutture Critiche e il Sistema Paese, compartecipazione pubblico privato: relazioni, metodologie, protocolli operativi, istituzioni preposte.
- Addestramento, esercitazioni, consapevolezza.
- Visite presso le strutture di security di Infrastrutture critiche aeroportuali e Industrie strategiche.

Principali competenze apprese:

- Concetti base per la gestione della sicurezza in un'infrastruttura critica nelle discipline complementari al dominio Cyber.

IN2.4 Risk Propagation in Interconnected Infrastructures

Responsabile: Paola Girdinio
Ore: 12
(4 ore Prof.ssa Paola Girdinio. 8 ore D.ssa Federica Livelli)

Pre-requisiti:

- Conoscenze dei concetti di base su Infrastrutture Critiche
- Normativa nazionale ed internazionale su Infrastrutture Critiche

Programma:

- Dipendenza e interdipendenza.
- Dimensioni per descrivere interdipendenze: formulazione di Rinaldi, Peerenboom, Kelly
- Modellazione olografica gerarchica
- Intra e Inter dipendenza fra i layer delle infrastrutture critiche
- Modelli e simulaziono
- Metodi olistici
- Modello di Leontief
- Approcci topologici
- Simulazioni basate su metodi ad agenti

Principali competenze apprese:

- Conoscenza delle metodiche di propagazione del danno nelle Infrastrutture Critiche
- Modelli predittivi.

.
