SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

SERICS
CYBERSECURITY
ACADEMY

FORMAZIONE PER DIPENDENTI E PROFESSIONISTI

Finanziato dall'Unione europea NextGenerationEU
Ministero dell'Università e della Ricerca
Italiadomani PIANO NAZIONALE DI RIPRESA E RESILIENZA
SERICS SECURITY AND RIGHTS IN THE CYBERSPACE

FORMAZIONE SPECIALISTICA PER DIPENDENTI E PROFESSIONISTI

CYBERSECURITY E TUTELA DEI DIRITTI NEL CYBER SPACE

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

INDICE

CYBER THREATS & DEFENSE

01 Difesa dagli attacchi avanzati, offuscati e evasivi 8
02 Metodologie e sistemi di Penetration Test e Intrusion Detection 12
03 Hardening di sistemi e servizi Linux 16
04 Log - Collezionamento, analisi e correlazione degli eventi 20
05 Contrastare la disinformazione: Strumenti e Tecniche per la gestione delle Minacce e dei Rischi 24

SOFTWARE & SYSTEM SECURITY

06 Sicurezza del software: prevenzione delle vulnerabilità tramite programmazione sicura 30
07 Intelligenza Artificiale: progettazione sicura e robusta 34
08 Sicurezza e privacy nei dispositivi mobili 38
09 Aspetti di sicurezza nei dispositivi embedded 42
10 Aspetti di sicurezza e relative normative nel mondo automotive 46

DATA PROTECTION & PRIVACY

11 La sicurezza dei dati e dei servizi nella trasformazione digitale 52
12 Privacy e sicurezza nella condivisione e gestione dei dati in scenari emergenti 56
13 Digital Sovereignty: Beyond tensions of data protection and cybersecurity 60

CRYPTOGRAPHY & AUTHENTICATION

14 Crittografia e applicazioni 66
15 Protocolli e tecnologie per l'autenticazione, l'identità e la firma digitale 70

RISK MANAGEMENT & EVALUATION FRAMEWORKS

16 Common Criteria for Information Technology Security Evaluation 76
17 Framework e Standard open per Cyber Risk Assessment 80
18 Framework e Standard commerciali per Cyber Risk Assessment 84

SECURITY OF CLOUD & EMERGING TECHNOLOGIES

19 Orchestratori distribuiti e applicazioni "Cloud Native" 90

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

CYBER THREATS & DEFENSE

01 Difesa dagli attacchi avanzati, offuscati e evasivi 6
02 Metodologie e sistemi di Penetration Test e Intrusion Detection 10
03 Hardening di sistemi e servizi Linux 14
04 Log - Collezionamento, analisi e correlazione degli eventi 18
05 Contrastare la disinformazione: Strumenti e Tecniche per la gestione delle Minacce e dei Rischi 22

CORSO 01

DIFESA DAGLI ATTACCHI AVANZATI, OFFUSCATI E EVASIVI

Questo modulo affronta nel dettaglio le tecniche utilizzate per la realizzazione di attacchi evasivi, cioè attacchi che eludono i sistemi di difesa. Verranno illustrate le tecniche di offuscamento del codice che rendono difficile l'analisi statica e dinamica, e le tecniche di evasione per confondere o eludere i sistemi di analisi dinamica.

argomenti

Panoramica sulle principali tecniche di rilevazione di attacchi, basati su firme e sull'analisi statistica. Analisi delle debolezze degli approcci di difesa. Tecniche di offuscamento del software e del traffico di rete. Effetti dell'offuscamento nella rilevazione di attacchi informatici. Attacchi sofisticati per eludere i sistemi di rilevazione delle minacce basati sulla analisi del traffico di rete o della esecuzione die processi. Tecniche di difesa avanzate per la rilevazione di attacchi offuscati e evasivi. Tecniche di difesa avanzate per la rilevazione di attacchi sofisticati. Machine e deep learning per la rilevazione di attacchi informatici.

target

- **AZIENDE CHE OFFRONO SERVIZI DI GESTIONE E SICUREZZA SISTEMI IT, SECURITY OPERATION CENTER**
- **ANALISTI DI SICUREZZA**
- **THREAT ANALYST**

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

PANORAMICA SULLE TECNICHE DI RILEVAZIONE DEGLI ATTACCHI

10 ORE

- Approcci basati su firme:
  - Definizione di firme (signature-based detection)
  - Esempi pratici: antivirus e intrusion detection systems (IDS)
- Approcci basati su analisi statistica:
  - Rilevazione di anomalie attraverso analisi statistica dei dati
  - Limiti e vulnerabilità di questo approccio
- Analisi delle debolezze dei sistemi di difesa:
  - Attacchi noti che sfruttano limiti di modelli signature-based e anomaly-based

modulo 02

TECNICHE DI OFFUSCAMENTO DEL CODICE E DEL TRAFFICO DI RETE

10 ORE

- Offuscamento del codice:
  - Tecniche statiche: trasformazioni del codice per renderlo meno comprensibile (e.g., r enaming, control flow obfuscation)
  - Tecniche dinamiche: codice auto-modificante, packed executables
- Offuscamento del traffico di rete:
  - Crittografia e tunnel crittografici (VPN, SSH, HTTPS)
  - Tecniche di payload obfuscation e pattern evasion
- Effetti dell'offuscamento sulla rilevazione di attacchi:
  - Impatti sull'analisi statica e dinamica
  - Rischi per i sistemi di rilevazione tradizionali

modulo 03

ATTACCHI SOFISTICATI ED EVASIVI

10 ORE

- Attacchi per eludere sistemi di analisi dinamica:
  - Tecniche anti-debugging e anti-virtualizzazione
  - Malware polimorfico e metamorfico
- Attacchi sul traffico di rete:
  - Esempi di attacchi avanzati come il masquerading
  - Tecniche per eludere IDS basati su traffico (e.g., fragmented packets, timing attacks)
- Social Engineering:
  - Principi psicologici alla base degli attacchi di social engineering
  - Tecniche comuni: phishing, spear-phishing, baiting, pretexting

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

modulo 04

TECNICHE DI DIFESA AVANZATE

10 ORE

- Approcci per contrastare attacchi offuscati:
  - Utilizzo di tecniche di de-offuscamento per analisi statica e dinamica
  - Sistemi di rilevazione basati su behavior profiling
- Approcci per attacchi sofisticati:
  - Sistemi di rilevazione adattivi: aggiornamento dinamico delle regole
  - Analisi del contesto per mitigare attacchi evasivi
- Machine e Deep Learning per la Cybersecurity:
  - Modelli per la rilevazione di anomalie nel traffico di rete (e.g., autoencoder, RNN)
  - Applicazioni di classificatori supervisionati e non supervisionati
  - Tecniche di addestramento e prevenzione di bias nei modelli AI per la sicurezza

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

- Esempi di offuscamento del traffico di rete e di applicazioni software
  Attacchi di social engeneering
  Esempi di approcci basati sul machine learning per la rilevazione di attacchi informatici

- Approcci per attacchi sofisticati:
  - Sistemi di rilevazione adattivi: aggiornamento dinamico delle regole
  - Analisi del contesto per mitigare attacchi evasivi

- Machine e Deep Learning per la Cybersecurity:
  - Modelli per la rilevazione di anomalie nel traffico di rete (ades., autoencoder, RNN)
  - Applicazioni di classificatori supervisionati e non supervisionati
  - Tecniche di addestramento e prevenzione di bias nei modelli AI per la sicurezza
  - Applicazione della teoria su casi studio

CORSO 02

METODOLOGIE E SISTEMI DI PENETRATION TEST E INTRUSION DETECTION

I partecipanti avranno le basi per condurre penetration test, dalla ricognizione all'analisi del traffico di rete, identificando e classificando vulnerabilità e mappando le minacce tramite il framework MITRE ATT&CK. Inoltre, saranno in grado di applicare tecniche di exploitation e post-exploitation e comprendere l'uso e le funzionalità di soluzioni IDS/IPS per migliorare la sicurezza dei sistemi.

argomenti

Introduzione al penetration testing (tipologie, attori, modelli di attacco); Presentazione framework MITRE ATT&CK; Tecniche di ricognizione (attiva e passiva); Scansioni di rete e identificazione vulnerabilità; Analisi di vulnerabilità, metodologie e classificazioni; Cenni a tecniche di exploitation; Tecniche di post-exploitation, movimenti laterali, persistenza; Introduzione e nozioni su IDS e IPS, caratteristiche e panoramica soluzioni; Analisi del traffico di rete.

target

COMPETENZE IN INGRESSO

Per lo svolgimento del corso è consigliata una conoscenza di base delle reti, dei sistemi operativi (con particolare riferimento ai sistemi Linux), dei principi fondamentali di sicurezza informatica.

COMPETENZE IN USCITA

Al termine del corso, i partecipanti avranno le basi per condurre penetration test, dalla ricognizione all'analisi del traffico di rete, identificando e classificando vulnerabilità e mappando le minacce tramite il framework MITRE ATT&CK.
Inoltre, saranno in grado di applicare tecniche di exploitation e post-exploitation e comprendere l'uso e le funzionalità di soluzioni IDS/IPS per migliorare la sicurezza dei sistemi.

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

5 ORE

- Introduzione al penetration testing (tipologie, attori, modelli di attacco)
- Presentazione framework MITRE ATT&CK
- Tecniche di ricognizione (attiva e passiva)

modulo 02

5 ORE

- Scansioni di rete e identificazione vulnerabilità
- Analisi di vulnerabilità, metodologie e classificazioni
- Cenni a tecniche di exploitation

modulo 03

5 ORE

- Tecniche di post-exploitation, movimenti laterali, persistenza
- Introduzione e nozioni su IDS e IPS, caratteristiche e panoramica soluzioni
- Analisi del traffico di rete

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

CORSO 03

HARDENING DI SISTEMI E SERVIZI LINUX

Il corso fornisce competenze avanzate di hardening per la protezione di sistemi Linux, con un focus sulla sicurezza dei servizi, della rete e dei dati. Verranno affrontate strategie di protezione per l'accesso ai sistemi, la gestione dei permessi, il firewalling e l'uso di container per l'isolamento delle applicazioni. Saranno illustrati strumenti per il monitoraggio e l'auditing della sicurezza, oltre a tecniche di crittografia per la protezione dei dati sensibili.

argomenti

Gestione degli accessi e autenticazione; Sicurezza dei file e gestione dei permessi; Protezione della rete, firewalling e VPN; Hardening dei servizi critici; Hardening dei servizi tramite containerizzazione; Monitoraggio e logging per la sicurezza; Auditing e security compliance (es. Lynis, CIS Benchmark e OpenSCAP); Crittografia e protezione dei dati a riposo (es. LUKS) e in transito.

target

COMPETENZE IN INGRESSO

Conoscenza di base dell'amministrazione di sistemi Linux, della gestione degli utenti, dei permessi e dei principali comandi di configurazione di rete e servizi. È utile una familiarità con concetti di sicurezza informatica e virtualizzazione.

COMPETENZE IN USCITA

Al termine del corso, i partecipanti saranno in grado di implementare tecniche avanzate di hardening su sistemi Linux, rafforzare la sicurezza di servizi e reti, proteggere dati sensibili con crittografia, monitorare le attività sospette, verificare la compliance con strumenti di auditing e applicare strategie di sicurezza tramite container e ambienti virtualizzati.

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

HARDENING DI BASE

4 ORE

- Gestione degli accessi e autenticazione avanzata
- Sicurezza dei file e gestione dei permessi

modulo 02

HARDENING DEI SERVIZI E PROTEZIONE DELLA RETE

4 ORE

- Configurazione avanzata di firewall (iptables, nftables) e VPN
- Sicurezza dei servizi critici: SSH, web server, database

modulo 03

MONITORAGGIO, AUDITING E COMPLIANCE

4 ORE

- Analisi e gestione dei log per la sicurezza (syslog, journald)
- Strumenti di auditing e compliance (Lynis, CIS Benchmark, OpenSCAP)

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

modulo 01

HARDENING DI SISTEMI LINUX

3 ORE

- Configurazione sicura degli accessi
- Principi di sicurezza per i permessi sui file

modulo 02

PROTEZIONE DEI SERVIZI E DELLA RETE

3 ORE

- Firewalling, VPN e segmentazione della rete
- Sicurezza dei servizi critici e protezione degli ambienti containerizzati

modulo 03

MONITORAGGIO, AUDITING E COMPLIANCE

3 ORE

- Tecniche di logging e monitoraggio degli eventi di sicurezza
- Strumenti per la verifica della compliance ai principali standard

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

CORSO 04

LOG - COLLEZIONAMENTO, ANALISI E CORRELAZIONE DEGLI EVENTI

I partecipanti acquisiranno la capacità di progettare e implementare una pipeline completa di logging, raccogliere, elaborare e arricchire i log, utilizzare sistemi di archiviazione con funzionalità di ricerca, applicare tecniche avanzate di analisi e correlazione eventi, e creare dashboard efficaci per la visualizzazione dei dati di logging.

argomenti

Logging e formati di logging; Architettura della logging pipeline; Log collection; Tecniche di elaborazione, filtraggio, trasformazione dei log; Processo di arricchimento dei log; Sistemi di archiviazione dei log e full text search; Tecniche di analisi log; Correlazione degli eventi; Dashboarding e visualizzazione.

target

COMPETENZE IN INGRESSO

Conoscenze base di sistemi informatici, fondamenti di networking, comprensione elementare di sistemi distribuiti, familiarità con la configurazione di sistemi e servizi.

COMPETENZE IN USCITA

Capacità di progettare e implementare una pipeline completa di logging, raccogliere, elaborare e arricchire i log, utilizzare sistemi di archiviazione con funzionalità di ricerca, applicare tecniche avanzate di analisi e correlazione eventi, e creare dashboard efficaci per la visualizzazione dei dati di logging.

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

4 ORE

- Logging e formati di logging
- Architettura della logging pipeline
- Log collection

modulo 02

4 ORE

- Tecniche di elaborazione, filtraggio, trasformazione dei log
- Processo di arricchimento dei log
- Sistemi di archiviazione dei log e full text search

modulo 03

4 ORE

- Tecniche di analisi log
- Correlazione degli eventi
- Dashboarding e visualizzazione

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

CORSO 05

CONTRASTARE LA DISINFORMAZIONE: STRUMENTI E TECNICHE PER LA GESTIONE DELLE MINACCE E DEI RISCHI

Il modulo approfondisce le principali minacce della disinformazione e le tecniche di verifica delle informazioni, con un focus su strumenti OSINT (Open Source INTelligence), valutazione delle fonti, propaganda e tecnologie emergenti come l'IA generativa e i deepfake, per formare professionisti capaci di gestire i rischi informativi.

argomenti

Principali Minacce; Valutazione delle Fonti; Open Source Intelligence; Verifica delle Informazioni; Propaganda e Fallacie Argomentative; Echo Chamber e Filter Bubbles; Generative AI e DeepFake; Framework per la Valutazione del Rischio.

target

SETTORE GIORNALISTICO
Redazioni, agenzie di stampa e professionisti dell'informazione che necessitano di competenze avanzate per contrastare la disinformazione (Giornalisti, fact-checker, editori e responsabili di comunicazione).

AMBITO AZIENDALE
Ufficio comunicazione, brand reputation, marketing e PR, per la protezione dell'immagine aziendale e la gestione di crisi mediatiche (Responsabili PR, brand managers, e social media strategists).

PUBBLICA AMMINISTRAZIONE
Enti locali e nazionali interessati a contrastare la disinformazione nel contesto di politiche pubbliche e comunicazione istituzionale (Decision makers, Policy makers e funzionari pubblici responsabili di strategie di comunicazione e gestione delle crisi).

SETTORE DELLA SICUREZZA E DELLA DIFESA
Intelligence e forze dell'ordine impegnate nella protezione da campagne di disinformazione e propaganda (Analisti OSINT, operatori di intelligence e responsabili di cyber security).

ORGANIZZAZIONI NO-PROFIT E ONG
Entità che combattono la disinformazione su temi globali, sociali o umanitariIstruzione e ricerca: Università, centri di ricerca e istituti di formazione (Studiosi di media, disinformazione e comunicazione, studenti di corsi di laurea o master in giornalismo, scienze della comunicazione, data science e sicurezza informatica).

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

PRINCIPALI MINACCE DELLA DISINFORMAZIONE

6 ORE

- Tipologie di disinformazione
- Esempi pratici: Analisi di casi studio come Cambridge Analytica, campagne elettorali e crisi sanitarie
- Impatto della disinformazione

modulo 02

OSINT

10 ORE

- Ciclo di Intelligence
- Introduzione agli strumenti OSINT: (i) Acquisizione, (ii) Analisi, (iii) Visualizzazione
- Limiti e Sfide
- Casi di Esempio

modulo 03

FACT-CHECKING E ANALISI DEI CONTENUTI

8 ORE

- Criteri per la valutazione delle fonti
- Analisi delle fonti online
- Strumenti per l'analisi e la verifica di contenuti

modulo 04

ANALISI DELLE RETI SOCIALI

8 ORE

- Algoritmi e strumenti
- Polarizzazione, echo chamber e filter bubbles
- Casi di esempio

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

modulo 05

GENERATIVE AI, DEEPFAKE

6 ORE

- Creazione e rilevamento di deepfake: immagini, video e audio
- Generative AI per la creazione di testi persuasivi (e.g., LLM come ChatGPT)
- Strumenti di rilevamento
- Esempi di campagne mediatiche costruite con Generative AI

modulo 06

FRAMEWORK DI VALUTAZIONE DEL RISCHIO

6 ORE

- DISARM (Disinformation Analysis and Risk Management)
- ABCDE (Actor, Behaviour, Content, Degree, Effect)
- Altri
- Esempi di utilizzo: FIMI Report I e II

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

Esercitazioni pratiche su verifica delle informazioni, fact-checking e analisi di contenuti manipolati con strumenti digitali e software per l'analisi di rete.

Approfondimento di un caso di giornalismo investigativo svolto con strumenti OSINT da esperti, ad esempio: Bellingcat, RAND, etc.

Analisi uno o più casi di disinformazione a scelta identificando: la tipologia di minaccia, gli attori, il messaggio, il target.

Fact-checking su notizie reali utilizzando tool introdotti al corso.

Analisi dei contenuti che per l'individuazione di narrative emergenti su dataset noti o acquisiti utilizzando tool di propaganda detection, clickbait, stance, etc.

Utilizzo di tool (e.g., Gephi) per analisi delle reti sociali (misure di centralità, identificazione di community, etc.) su dataset noti o acquisiti.

Produzione di un report di sintesi.

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

SOFTWARE & SYSTEM SECURITY

06 Sicurezza del software: prevenzione delle vulnerabilità tramite programmazione sicura 30
07 Intelligenza Artificiale: progettazione sicura e robusta 34
08 Sicurezza e privacy nei dispositivi mobili 38
09 Aspetti di sicurezza nei dispositivi embedded 42
10 Aspetti di sicurezza e relative normative nel mondo automotive 46

CORSO 06

SICUREZZA DEL SOFTWARE: PREVENZIONE DELLE VULNERABILITÀ TRAMITE PROGRAMMAZIONE SICURA

Il modulo introduce le pratiche e tecniche per progettare, sviluppare e mantenere applicazioni sicure, proteggendole dalle vulnerabilità più comuni. Verranno forniti i fondamenti della sicurezza del software focalizzandosi su tecniche di programmazione sicura e difensiva, allo scopo di prevenire vulnerabilità e ridurre i rischi di attacco.

argomenti

Fondamenti di sicurezza del software; principi di programmazione sicura; programmazione difensiva; vulnerabilità comuni e prevenzione; testing di sicurezza; strumenti e framework di sicurezza; pratiche avanzate e DevSecOps; esercitazioni pratiche.

target

- **IMPRESE, ENTI E PUBBLICHE AMMINISTRAZIONI CHE SVOLGONO, A VARI LIVELLI, ATTIVITÀ DI SVILUPPO DI SOFTWARE**
- **PROGETTISTI E SVILUPPATORI DI SOFTWARE**
- **STUDENTI DI MASTER E DOTTORATO**

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

VULNERABILITÀ COMUNI E PREVENZIONE

14 ORE

- Esempi concreti di vulnerabilità tipiche in diversi ambiti e linguaggi di programmazione (es. stack overflow e format string in C, deserializzazione in Java, loose comparison in PHP, etc.)
- Tecniche di mitigazione e prevenzione.

modulo 02

PROGRAMMAZIONE SICURA E DIFENSIVA

14 ORE

- Standard esistenti
- Un esempio concreto: SEI CERT
- Esempi di codice vulnerabile e valutazione della sua compliance agli standard.

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

Attraverso esercitazioni pratiche, casi studio e esempi reali, i partecipanti acquisiranno le competenze necessarie per scrivere codice robusto, sicuro e resistente agli errori.

- Esercitazioni pratiche
- Challenge tematiche sulla ricerca di vulnerabilità
- Esercizi di programmazione sicura e difensiva su casi pratici (es. programmi vulnerabili da fixare e/o sviluppo di piccoli esempi che siano compliant agli standard discussi

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

CORSO 07

INTELLIGENZA ARTIFICIALE: PROGETTAZIONE SICURA E ROBUSTA

Il modulo intende approfondire le diverse fasi della progettazione di un approccio basato sull'intelligenza artificiale in diversi ambiti applicativi, incluso la cybersecurity, evidenziando quali sono le minacce alla sicurezza. Verranno fornite le linee guida per la progettazione sicura e strumenti per la valutazione della sicurezza.

argomenti

Panoramica sui diversi approcci basati su Intelligenza Artificiale. Machine Learning, Deep Learning, generative Models. Apprendimento supervisionato e non supervisionato. Aspetti critici nella definizione del modello dei dati, nella gestione del training set, nella selezione dell'algoritmo di apprendimento e della stima dei parametri, criticità in fase operativa. Definizione dei threat models. tecniche di progettazione robusta. Strumenti per la valutazione della sicurezza e robustezza del sistema sviluppato.

target

- **AZIENDE DI SVILUPPO SOFTWARE O INTEGRATORI DI SOLUZIONI DI TERZE PARTI**
- **PROGETTISTI E SVILUPPATORI SOFTWARE**

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

ELEMENTI DI BASE DI AI, MACHINE LEARNING, DEEP LEARNING

8 ORE

- Introduzione ai concetti fondamentali
- Modelli generativi e applicazioni
- Potenziali rischi in ambito cybersecurity

modulo 02

DATA SET, MODELLI DI DATI

8 ORE

- Pre-elaborazione dei dati: pulizia, normalizzazione e gestione dei valori mancanti;
- Caratteristiche dei dataset;
- Modelli di dati e training set

modulo 03

METODOLOGIE DI UTILIZZO DEI PARAMETRI

8 ORE

- Tecniche per la selezione dei parametri
- Validazione incrociata e grid search
- Metodologie di verifica delle prestazioni del modello
- Valutazione del modello
- Metriche di prestazione (precision, recall, F1-score, ROC curve)
- Analisi degli errori e miglioramento iterativo

modulo 04

TIPOLOGIE DI ERRORE E THREAT MODELLING

8 ORE

- Modelli di minaccia per i sistemi AI:
- Analisi delle vulnerabilità basate su compromissioni di confidentiality, integrity e availability (CIA).
- Impatti sulla purezza del dato:
- Manipolazioni dei dati di input (e.g., adversarial attacks.
- Robustezza ai dati rumorosi o manipolati.

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

modulo **05**

TECNICHE DI MITIGAZIONE DEI PROBLEMI

8 ORE

- Strategie per mitigare le minacce (Regularization e dropout per modelli robusti)
- Best practices per la progettazione sicura
- Principi di sicurezza by design
- Creazione di un Modello AI Sicuro
- Applicazione di tecniche di hardening del modello per aumentare la robustezza
- Validazione e test del modello progettato
- Monitoraggio continuo e auditing dei modelli

laboratorio

16 ORE

- Esercitazioni pratiche di progettazione di un sistema di machine learning, vulnerabilità e progettazione robusta e sicura in alcuni ambiti applicativi diversi
- Applicazione della teoria su casi studio Data set, progettazione, rischi e risoluzione

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

CORSO 08

SICUREZZA E PRIVACY NEI DISPOSITIVI MOBILI

Il modulo ha lo scopo di fornire le conoscenze di base per la comprensione, l'analisi e la gestione della sicurezza e della privacy sui dispositivi mobili. Per raggiungere questo obiettivo, il modulo introduce dapprima le caratteristiche principali dei sistemi operativi mobili, con un particolare focus su Android, e i processi di sviluppo delle app, per poi indagare i principali problemi di sicureza e privacy del mondo mobile nonché le tecniche allo stato dell'arte per la loro analisi e risoluzione.

argomenti

Ecosistema Mobile; Sicurezza & Privacy applicazioni mobile; Metodologie statiche e dinamiche per il VA/PT; Resilienza & Offuscamento; Malware.

target

- **FORMAZIONE PER DIPENDENTI E PROFESSIONISTI**

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

ECOSISTEMA MOBILE

6 ORE

- Panoramica sull'ecosistema mobile
- Analisi delle architetture di Android e iOS
- Approfondimento sul sistema operativo Android
- Modello di sviluppo delle app Android e iOS

modulo 02

SICUREZZA & PRIVACY APPLICAZIONI MOBILE

6 ORE

- Concetti di rischio, vulnerabilità, superfici di attacco
- Vulnerabilità e attacchi al sistema operativo e alle app
- Tecniche di profilazione dell'utente e del dispositivo mobile
- Attacchi alla privacy dell'utente

modulo 03

METODOLOGIE STATICHE E DINAMICHE PER IL VA/PT

18 ORE

- Analisi statica di applicazioni Android e iOS
- Analisi dinamica di applicazioni Android e iOS

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

modulo **04**

RESILIENZA & OFFUSCAMENTO

5 ORE

- Attacchi di repackaging e tecniche di anti-repackaging
- Tecniche di offuscamento del bytecode e del codice nativo

modulo **05**

MALWARE

5 ORE

- Panoramica mobile malware
- Realizzazione e analisi di malware mobile (basi)

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

- Analisi statica e dinamica di app Android reali con metodologie e tool allo stato dell'arte
- Protezione di una app vera dal repackaging tramite l'utilizzo di tecniche di anti-repackaging e offuscamento
- Implementazione di tecniche di anonimizzazione su un'app

CORSO 09

ASPETTI DI SICUREZZA NEI DISPOSITIVI EMBEDDED

Il modulo affronta i principali aspetti di sicurezza legati ai dispositivi embedded, con un focus su hardware e software utilizzati in applicazioni critiche. Verranno esplorati attacchi e contromisure specifici per l'ambiente embedded, con laboratori pratici per consolidare le conoscenze teoriche. Il modulo ha come obiettivi: (i) comprendere i principi di sicurezza nei sistemi embedded, (ii) Identificare vulnerabilità hardware e software specifiche dei dispositivi embedded (iii) applicare tecniche di protezione contro attacchi mirati a piattaforme embedded (iii) sviluppare competenze pratiche in analisi e mitigazione delle minacce.

argomenti

Introduzione alla Sicurezza nei Sistemi Embedded; Architetture e Modelli di attacco; Sicurezza Hardware; Sicurezza del Software Embedded; Comunicazioni Sicure; Tendenze e Case Study

target

- **FORMAZIONE PER DIPENDENTI E PROFESSIONISTI**

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

INTRODUZIONE ALLA SICUREZZA NEI SISTEMI EMBEDDED

10 ORE

- Differenze tra sicurezza nei sistemi embedded e nei sistemi generici
- Principi di sicurezza: confidenzialità, integrità, disponibilità
- Minacce specifiche: attacchi fisici, attacchi software e vulnerabilità del firmware

modulo 02

ARCHITETTURE E MODELLI DI ATTACCO

10 ORE

- Architetture hardware di dispositivi embedded (SoC, MCU, FPGA)
- Modelli di attacco (Threat Models) e analisi di rischio
- Introduzione a TrustZone, SGX e altre tecnologie per sicurezza

modulo 03

SICUREZZA HARDWARE

10 ORE

- Attacchi a livello hardware:
- Side-channel attacks (DPA, SPA)
- Fault injection (laser, glitching).
- Contromisure hardware:
- Randomizzazione
- Tecniche di masking e DPA countermeasures

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

modulo 04

SICUREZZA DEL SOFTWARE EMBEDDED

5 ORE

- Buffer overflow e mitigazioni
- Sicurezza del firmware
- Tecniche di cifratura e autenticazione
- Secure Boot e aggiornamenti sicuri
- Utilizzo di strumenti come Binwalk per analisi firmware

modulo 05

COMUNICAZIONI SICURE

5 ORE

- Protocolli crittografici per IoT ed embedded (TLS/DTLS, MQTT)
- Implementazione di chiavi crittografiche sicure
- Vulnerabilità nei protocolli wireless (ZigBee, Bluetooth)

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

- Analisi di firmware: Decodifica e reverse engineering con Binwalk e Ghidra
- Side-channel attack: Simulazione e rilevazione di attacchi DPA su hardware demo.
- Secure Boot: Implementazione di un sistema di avvio sicuro con microcontrollori.
- Simulazione di attacchi wireless: Analisi della sicurezza di ZigBee o Bluetooth.
- Testing hardware: Identificazione di vulnerabilità con fault injection su FPGA

CORSO 10

ASPETTI DI SICUREZZA E RELATIVE NORMATIVE NEL MONDO AUTOMOTIVE

Il modulo fornisce una panoramica completa sulle normative di sicurezza nell'industria automobilistica, con particolare attenzione agli standard funzionali e di cybersecurity. L'obiettivo è di preparare i partecipanti ad affrontare le sfide tecniche e normative necessarie per progettare e certificare veicoli sicuri secondo le regolamentazioni globali.

argomenti

Introduzione alle Normative Automotive; Sicurezza Funzionale - ISO 26262; Cybersecurity nei Veicoli - ISO/SAE 21434; Certificazioni e Conformità

target

- **FORMAZIONE PER DIPENDENTI E PROFESSIONISTI**

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

INTRODUZIONE ALLE NORMATIVE AUTOMOTIVE

8 ORE

- Concetti base di sicurezza in ambito automotive
- Panoramica delle normative principali:
  - ISO 26262 (Functional Safety)
  - ISO/SAE 21434 (Cybersecurity)
  - UNECE WP.29 (Regolamento per la cybersecurity e l'aggiornamento software)

modulo 02

SICUREZZA FUNZIONALE - ISO 26262

16 ORE

- Principi di sicurezza funzionale:
  - ASIL (Automotive Safety Integrity Level)
  - Hazard and Risk Analysis (HARA)
- Ciclo di vita della sicurezza (Safety Lifecycle):
  - Concetti di progettazione sicura
  - Validazione e verifica
  - Processi di testing e rilascio

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

modulo 03

CYBERSECURITY NEI VEICOLI - ISO/SAE 21434

12 ORE

- Minacce alla cybersecurity dei veicoli connessi
- Cybersecurity lifecycle:
  - TARA (Threat Analysis and Risk Assessment)
  - Progettazione sicura di sistemi elettronici
  - Impatti del regolamento UNECE WP.29 e CSMS (Cybersecurity Management System)

modulo 04

CERTIFICAZIONI E CONFORMITÀ

4 ORE

- Preparazione e gestione degli audit.
- Redazione della documentazione tecnica:
  - Safety Case
  - Cybersecurity Case

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

- Laboratorio di Hazard and Risk Analysis (HARA): Identificazione dei rischi per un sistema ADAS
- Laboratorio di TARA: Valutazione delle minacce cybersecurity in un'architettura CAN bus
- Validazione e Verifica: Analisi di test funzionali basati su ISO 26262
- Redazione della Documentazione: Creazione di un Safety Case per un componente automobilistico

SERICS

SECURITY AND RIGHTS IN THE CYBERSPACE

DATA PROTECTION & PRIVACY

11 La sicurezza dei dati e dei servizi nella trasformazione digitale 52

12 Privacy e sicurezza nella condivisione e gestione dei dati in scenari emergenti 56

13 Digital Sovereignty: Beyond tensions of data protection and cybersecurity 60

CORSO 11

LA SICUREZZA DEI DATI E DEI SERVIZI NELLA TRASFORMAZIONE DIGITALE

Questo modulo affronta i temi relativi ai rischi introdotti dalla digitalizzazione dei processi, con particolare riferimento alla sicurezza dei dati e dei servizi. Dopo aver discusso le principali novità apportate dalla trasformazione digitali verranno introdotti i rischi di cybersicurezza connessi. Per ciascuno di questi saranno illustrate le principali best practice, e relative tecnologie, oggi disponibile per mitigarne l'impatto.

argomenti

- Panoramica sulla trasformazione digitale, impatti sui processi e sui servizi aziendali
- Concetti chiave di cybersicurezza: minacce, vulnerabilità e obiettivi di protezione
- Ruolo della cybersicurezza nei processi di digitalizzazione
- Tipologie principali di attacchi: phishing, ransomware, etc.
- Tecnologie per la protezione dei dati sensibili: cifratura, gestione degli accessi e controllo
- Compliance normativa: GDPR e altre normative rilevanti
- Best practice per la protezione della privacy in contesti digitalizzati
- Tecnologie per la protezione dei sistemi: firewall, VPN, segmentazione delle reti, etc.
- Modelli di sicurezza per il cloud computing e l'IoT
- Pianificazione della risposta agli incidenti
- Business Continuity e Disaster Recovery
- Gestione delle crisi e comunicazione interna ed esterna durante un incidente

target

- **IMPRESE E PUBBLICHE AMMINISTRAZIONI.**
- In generale tutto il **PERSONALE IMPATTATO DAI PROCESSI DI TRASFORMAZIONE DIGITALE**
- Particolarmente di interesse per il **PERSONALE CON FUNZIONI MANAGERIALI**
- Di interesse per **NEOLAUREATI DI DISCIPLINE NON TECNICHE CHE INTENDONO FORMARSI SUI TEMI GENERALI DELLA CYBERSECURITY PRIMA DELL'INGRESSO NEL MONDO DEL LAVORO**

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

TRASFORMAZIONE DIGITALE

10 ORE

- Panoramica sulla trasformazione digitale, impatti sui processi e sui servizi aziendali

modulo 02

INTRODUZIONE AL RISK MANAGEMENT NELLA CYBERSECURITY

8 ORE

- Definizioni e concetti chiave
- Analisi degli impatti sui processi e sui servizi aziendali
- Strategie di mitigazione: prevenzione, protezione, rilevamento e risposta

modulo 03

COMPLIANCE NORMATIVA

10 ORE

- GDPR e altre normative rilevanti
- Best practice per la protezione della privacy in contesti digitalizzati
- Tecnologie per la protezione dei dati sensibili: cifratura, gestione degli accessi e controllo

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

modulo 04 — TIPOLOGIE DI ATTACCHI E PRINCIPALI RISPOSTE

4 ORE

- Tipologie principali di attacchi: phishing, ransomware, etc.
- Tecnologie per la protezione dei sistemi: firewall, VPN, segmentazione delle reti, etc.
- Pianificazione della risposta agli incidenti
- Business Continuity e Disaster Recovery
- Gestione delle crisi e comunicazione interna ed esterna durante un incidente

modulo 05 — CLOUD E IOT

5 ORE

- Modelli di sicurezza per il cloud computing e l'IoT

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

Simulazione di un attacco (e.g. phishing) e pianificazione della risposta per consentire ai partecipanti di riconoscere segnali di compromissione, rispondere all'incidente e attuare misure di contenimento e recupero.

CORSO 12

PRIVACY E SICUREZZA NELLA CONDIVISIONE E GESTIONE DEI DATI IN SCENARI EMERGENTI

Il modulo fornisce una panoramica di problematiche, rischi e soluzioni di particolare rilievo per la protezione dei dati in scenari emergenti nei quali coloro che operano in realtà pubbliche e private o come professionisti si confrontano con crescente frequenza. Tali contesti includono la condivisione, la pubblicazione, l'analisi, la gestione e l'archiviazione di dati nel rispetto della loro privacy e sicurezza. Legislazioni e regolamentazione per la protezione di dati impongono restrizioni che limitano l'uso dei dati, e gli individui, così come le aziende, chiedono il rispetto dei loro requisiti di protezione e la garanzia di un controllo effettivo dei loro dati.

argomenti

Concetti di privacy e anonymity. Problematiche inerenti la protezione dei dati; Aspetti normativi; Requisiti e Politiche; Approcci alle protezione dei dati (ad es. anonimizzazione, pseudonimizzazione); Apprendimento delle tecniche e metriche di protezione (ad es. k-anonymity, l-diversity, differential privacy); Protezione dei dati in scenari emergenti (ad es. AI, Smart Cities, Cloud); Privacy in contesti AI (ad es. Machine Learning); Sicurezza e privacy dei dati in contesti di outsourcing e distribuiti (ad es. Cloud, IoT, Fog/edge computing).

target

- **IMPRESE E PUBBLICHE AMMINISTRAZIONI**
- **DIPENDENTI E PROFESSIONISTI COINVOLTI NEL TRATTAMENTO DEI DATI, SIA IN AMBITO INFORMATICO CHE IN AMBITO AMMINISTRATIVO, GESTIONALE COME ANCHE IN ALTRE FUNZIONI**

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

SICUREZZA E PRIVACY DEI DATI

12 ORE

- Concetti di privacy e anonymity
- Problematiche inerenti la protezione dei dati
- Aspetti normativi e standard di riferimento
- Requisiti
- Politiche
- Introduzione a misure tecniche quali ad es. anonimizzazione e pseudonimizzazione

modulo 02

APPROFONDIMENTO DELLE TECNICHE E METRICHE DI PROTEZIONE

16 ORE

- k-anonymity
- l-diversity
- Differential privacy

modulo 03

PROTEZIONE DEI DATI IN SCENARI EMERGENTI

12 ORE

- Analisi rischi in scenari quali ad es. AI, Smart Cities, Cloud
- Approfondimento riguardante la Privacy in contesti AI (ad es. Machine Learning)
- Sicurezza e privacy dei dati in contesti di outsourcing e distribuiti (ad es. Cloud, IoT, Fog/edge computing)

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

- Esercitazioni pratiche volte ad analizzare esempi e casi di studio relativamente all'applicazione dei concetti sviluppati per valutare i rischi di compromissione della privacy e l'applicazione di misure e tecniche di protezione dei dati.
- AI e sicurezza dei dati
- Cloud/Fog/Edge Computing

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

CORSO 13

DIGITAL SOVEREIGNTY: BEYOND TENSIONS OF DATA PROTECTION AND CYBERSECURITY

Il modulo intende approfondire i punti di maggiore tensione tra la governance e disciplina dei dati, sia personali che non personali, e la cybersicurezza. Il modulo si divide in tre parti. Nella prima sono individuati i profili tecnici della digital sovereignty.
Nella seconda parte si analizzeranno i profili di connessione tra la disciplina dei dati personali e la cybersicurezza, soprattutto relativamente agli aspetti problematici della gestione e notifica dei data breach e delle notifiche cybersicurezza. La terza parte affronta i problemi collegati alla gestione della compliance alle norme NIS2 (DLGS 138/2024) e Legge 90/2024.

argomenti

Digital sovereignty (data sovereignty and trust models; confidentiality and compliance of computations); Analisi di casi studio in materia di databreach; Disciplina delle notifiche in materia di data breach e notifiche cybersecurity; La gestione della compliance NIS 2; Cenni alla compliance DORA.

target

- **PA TENUTE ALLA COMPLIANCE NIS 2 O DORA.**
- **AZIENDE NAZIONALI NON TENUTE ALLE NORME PERIMETRO MA A NIS 2 O DORA**
- **STUDENTI MASTER E DOTTORATO**
- **PERSONALE DELLA PA, PERSONALE DI AZIENE E PROFESSIONISTI CHE HANNO GIÀ INTERESSE AL TEMA CYBER E LAVORANO GIÀ NEL MONDO DELLA PROTEZIONE DEI DATI**

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

DIGITAL SOVEREIGNTY

8 ORE

- Data sovereignty and trust models
- Confidentiality and compliance of computations

modulo 02

DATA BREACH

20 ORE

- Analisi di casi studio in materia di databreach
- Disciplina delle notifiche in materia di data breach e notifiche cybersecurity

modulo 03

ELEMENTI DI COMPLIANCE

12 ORE

- La gestione della compliance NIS 2
- Cenni alla compliance DORA

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

Descrizione e analisi di casi studio specifici
con esercitazione mirate.

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

CRYPTOGRAPHY & AUTHENTICATION

14 Crittografia e applicazioni 66

15 Protocolli e tecnologie per l'autenticazione, l'identità e la firma digitale 70

CORSO 14

CRITTOGRAFIA E APPLICAZIONI

L'obiettivo del modulo è fornire le conoscenze di base relative alla crittografia e alla sua applicazione ai servizi di sicurezza.

argomenti

Funzioni one-way e trap-door; Ciphers; Cifrari simmetrici e a chiave pubblica; Principi di confusione e diffusione; Crittografia classica; Attacchi e criptoanalisi; Modelli di attacco; Known Ciphertext Attack; Known Plaintext Attack; Chosen Plaintext Attack; Chosen Ciphertext Attack; Cifrari a blocchi e cifrari a flusso; Rete di Feistel; Data Encryption Standard (DES); Vulnerabilità di DES; composizione di funzioni di cifratura e meet in the middle attack; Triple DES; Blowfish; AES; Modalità di funzionamento della cifratura a blocchi; ECB; CBC; Cipher feedback; OFB; Counter; Pseudo and True Random Number Generators (PRNG and TRNG); Stream Ciphers; Hash crittografici; SHA1 - SHA-256; Attacco del compleanno; Schemi crittografici a chiave pubblica; RSA; Malleability di RSA; Vulnerabilità di RSA; Crittografia probabilistica; OAEP RSA; Curve ellittiche; Autenticazione dei messaggi basata su crittografia simmetrica e a chiave pubblica; Autenticazione dei messaggi basata su hash crittografici (MAC); Prefisso segreto; Postfisso segreto; HMAC; Schemi crittografici a chiave pubblica e firma digitale; Blind signature; Algoritmo Diffie-Hellman e scambio di chiavi; Approcci basati su KDC (Key Distribution Center); Approcci basati su PKI X.509. Applicazioni della crittografia per il web sicuro: TLS. Sicurezza al livello rete: IP sec e VPN.

target

- **IMPRESE E PUBBLICHE AMMINISTRAZIONI** in particolare se appartenenti al perimetro. Studenti di Master e Dottorato
- **PERSONALE IT PER IMPRESE E PA**
- **STUDENTI DI MASTER E DOTTORATI NEL SETTORE IT** con interesse verso cybersecurity

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01 — CIFRARI SIMMETRICI

8 ORE

- Cifrari a Blocchi e a Flusso
- Rete di Feistel
- Data Encryption Standard (DES)
- Advanced Encryption Standard (AES)
- Modalità di Funzionamento della Cifratura a Blocchi

modulo 02 — CIFRARI A CHIAVE PUBBLICA

8 ORE

- RSA (Rivest-Shamir-Adleman)
- Curve Ellittiche (ECC - Elliptic Curve Cryptography)
- Introduzione e vantaggi rispetto a RSA
- Applicazioni nei sistemi moderni (e.g., TLS)

modulo 03 — CIFRARI A FLUSSO

2 ORE

- Differenze tra cifratura a blocchi e a flusso
- Esempi di stream ciphers (RC4, Salsa20)
- Applicazioni in contesti pratici

modulo 04 — HASH CRITTOGRAFICI

6 ORE

- Proprietà degli Hash Crittografici (Unicità, irreversibilità, e dipendenza dai dati)
- SHA (Secure Hash Algorithm)/ SHA-1 e SHA-256
- Implicazioni per la sicurezza dei sistemi

modulo 05 — AUTENTICAZIONE DI MESSAGGI

4 ORE

- Autenticazione Basata su Crittografia Simmetrica e Asimmetrica
- MAC (Message Authentication Code)
- Autenticazione Basata su Hash: Generazione e verifica di codici di autenticazione

modulo 06 — PRIMITIVE DI FIRMA DIGITALE

2 ORE

- Schemi Crittografici a Chiave Pubblica e Firma Digitale
- Applicazioni legali e nei sistemi digitali

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

modulo 07

METODI PER LO SCAMBIO DELLE CHIAVI

2 ORE

- Concetto di “key exchange”
- Scambio delle chiavi asimmetriche e simmetriche
- Certificati digitali e infrastruttura a chiave pubblica (PKI)
- Autenticazione e firma digitale

modulo 08

MODALITÀ DI ESECUZIONE DEI CIFRARI A BLOCCHI

4 ORE

- Introduzione ai cifrari a blocchi
- ECB (Electronic Codebook)
- CBC (Cipher Block Chaining)
- CFB (Cipher Feedback)
- OFB (Output Feedback)
- CTR (Counter Mode)

modulo 09

CRITTOGRAFIA PER LA SICUREZZA WEB

4 ORE

- Applicazioni della crittografia per la sicurezza web e IP

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

Esercitazioni pratiche con software e tool crittografici e con i protocolli TLS e IPsec.
Utilizzo pratico di GPG.

- Cifrari e Hash: Python (PyCryptodome, cryptography), Java (BouncyCastle), OpenSSL
- CrypTool per simulazioni
- Attacchi e Criptoanalisi; John the Ripper, Hashcat per attacchi su hash;
- Burp Suite, OWASP ZAP per test di vulnerabilità
- PKI e Certificati: OpenSSL, Keytool per generare chiavi e certificati X.509
- Certbot per TLS
- Firme Digitali e Autenticazione: Python cryptography, OpenSSL per RSA, HMAC, ECDSA
- Sicurezza di Rete e Web: Wireshark per analisi TLS
- OpenVPN, StrongSwan per VPN/IPsec

CORSO 15

PROTOCOLLI E TECNOLOGIE PER L'AUTENTICAZIONE, L'IDENTITÀ E LA FIRMA DIGITALE

Il modulo descrive i principali protocolli di autenticazione e le tecnologie comunemente nel contesto dell'autenticazione su rete. Il modulo mira anche ad approfondire la nozione di firma digitale, con particolare riferimento alla nozione tecnica di firma elettronica qualificata, e agli aspetti di sicurezza ad essa collegati.

argomenti

PARTE 1

Peer-Entity Authentication e Digital Identity: Protocolli di autenticazione (password, Lamport, EKE, challenge-response, ZKP, etc.). Multi-factor authentication. Autenticazione biometrica. Gli standard FIDO e FIDO2. Protocolli e tecnologie per l'identità digitale federata e SSI-based.

PARTE 2

Electronic Signatures: Primitiva crittografica di firma digitale. Firme elettroniche e documenti informatico. Certificati, revoca, PKI X.509. Firma elettronica avanzata e qualificata. Formati di firma (CADES, PADES, XADES, ASIC-S). Vulnerabilità. Validazione temporale qualificata. Dispositivo qualificato di firma. Firma remota.

target

- **IMPRESE E PUBBLICHE AMMINISTRAZIONI** in particolare se appartenenti al perimetro. Studenti di Master e Dottorato
- **PERSONALE IT PER IMPRESE E PA**
- **STUDENTI DI MASTER E DOTTORATI NEL SETTORE IT** con interesse verso cybersecurity o profili giuridici interdisciplinari

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01 — PROTOCOLLI DI AUTENTICAZIONE

10 ORE

- Modelli base e avanzati per la gestione delle password
- Multi-Factor Authentication (MFA)
- Google Authenticator, Microsoft Authenticator
- U2F (Universal 2nd Factor) e dispositivi fisici di autenticazione.
- Autenticazione biometrica

modulo 02 — FIDO

2 ORE

- Concetti principali: autenticazione senza password, protezione delle credenziali
- Tecnologie associate: WebAuthn, UAF (Universal Authentication Framework), U2F
- FIDO2 - Evoluzioni rispetto a FIDO: supporto al protocollo WebAuthn e CTAP (Client to Authenticator Protocol)
- Esempi di implementazione nei browser moderni e nei dispositivi hardware (e.g., YubiKey).

modulo 03 — PROTOCOLLI E STANDARD PER L'IDENTITÀ DIGITALE

10 ORE

- Identità digitale e protocolli standard (e.g., SAML, OAuth 2.0, OpenID Connect)
- Principi dell'identità decentralizzata
- Uso della blockchain per la gestione sicura e autonoma dell'identità

modulo 04 — FIRME ELETTRONICHE

4 ORE

- Firme elettroniche semplici (SES), avanzate (AES), e qualificate (QES)
- Documenti informatici

modulo 05 — CERTIFICATI E PKI PER FIRME ELETTRONICHE

5 ORE

- Certificati digitali e CA
- Gestione della revoca

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

modulo 06

FORMATI FIRMA

2 ORE

- Formati standard per la firma digitale (CADES, PADES, XADES)
- Confronti tra i formati
- Scenari applicativi e vantaggi specifici di ciascun formato

modulo 07

VALIDAZIONE TEMPORALE

2 ORE

- Importanza della validazione temporale nelle firme digitali
- Funzionamento di un Time Stamping Authority (TSA).

modulo 08

DISPOSITIVO QUALIFICATO DI FIRMA E FIRMA REMOTA

4 ORE

- Compliance normativa

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

Esercitazione su protocolli di autenticazione federata (SAML2 e Open-ID Connect) e SSI.

Sessioni pratiche per sviluppatori sull'integrazione di soluzioni di identità digitale (SAML SSO, OpenID Connect, OAuth2.0, WebAuthn).

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

RISK MANAGEMENT & EVALUATION FRAMEWORKS

16 Common Criteria for Information Technology Security Evaluation 76

17 Framework e Standard open per Cyber Risk Assessment 80

18 Framework e Standard commerciali per Cyber Risk Assessment 84

CORSO 16

COMMON CRITERIA FOR INFORMATION TECHNOLOGY SECURITY EVALUATION

Il modulo offre una panoramica approfondita sullo standard internazionale per la valutazione della sicurezza dei sistemi IT, con particolare attenzione agli aspetti teorici e pratici del framework. Vengono introdotti i concetti fondamentali, analizzando termini essenziali come Target of Evaluation (TOE), Security Functional Requirements (SFRs) e Security Assurance Requirements (SARs). Viene quindi spiegata la struttura del framework e come questa si applica nei diversi contesti di valutazione. Un focus specifico è dedicato al Protection Profile (PP), ossia il documento che definisce i requisiti di sicurezza generici per una categoria di prodotti, evidenziandone l'importanza e il processo di creazione. Il modulo quindi approfondisce la definizione e il ruolo del Target of Evaluation, l'insieme specifico di funzioni di sicurezza e tecnologie sottoposte a valutazione. Attraverso esempi pratici, i partecipanti imparano a identificare le caratteristiche principali del TOE e come documentarle efficacemente.

Una parte significativa del programma riguarda il processo di valutazione stesso, spiegando le sue fasi principali: dalla pianificazione iniziale, passando per la verifica tecnica, fino alla certificazione ufficiale. Vengono analizzati i ruoli e le responsabilità di tutti gli attori coinvolti, inclusi sviluppatori, valutatori e organismi di certificazione.

Infine, il corso fornisce strumenti pratici per applicare i Common Criteria in contesti reali, preparando i partecipanti a sviluppare, valutare o certificare prodotti in linea con i requisiti dello standard, con l'obiettivo finale di garantire sicurezza, affidabilità e conformità normativa.

Il modulo è organizzato su due parti da seguire a distanza da 20 ore ciascuno per un totale di 40 ore più 16 ore di attività di laboratorio in presenza.

argomenti

- ISO e i principali standard internazionali collegati ai Common Criteria
- Target of Evaluation, Security Target e Protection Profile
- CAP e TOE composto
- Valutazione Assurance Continuity
- Schemi di valutazione nazionali e europei e EUCC

target

- Laboratori di valutazione, inseriti nello Schema nazionale per la valutazione e la certificazione della sicurezza delle tecnologie dell'informazione ai fini della tutela delle informazioni classificate concernenti la sicurezza interna e esterna dello Stato" (DPCM del 11/4/2002) gestito dalla PCM, nello "Schema nazionale per la valutazione e certificazione della sicurezza nel settore della tecnologia dell'informazione, ai sensi dell'art.10c1 del DL n.10/2002" (DPCM del 30/10/2003) gestito da OCSI, o in quello del Perimetro di Sicurezza Cibernetica Nazionale (D.Lgs del 21.09.2019, n. 105) gestito da ACN
- Aziende che si vogliono inserire nel mercato per fornire prodotti e sistemi ICT e che intendono certificarli. Personale specializzato è essenziale affinché sia in grado di guidare il processo di sviluppo di prodotti o sistemi e di integrazione degli stessi affinché la qualità delle misure di sicurezza sia tale da superare agevolmente superare i test che una valutazione ai fini della certificazione di sicurezza richiede

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo **01**

MODULO INTRODUTTIVO

20 ORE

- Introduzione generale
- La valutazione e la certificazione
- Termini tecnici di base (TOE, PP, SFR, SAR, EAL/CAP, VA&PT)
- Schemi nazionali, europei e accordi multinazionali
- Perimetro Sicurezza Nazionale Cibernetica (PSNC)
- Accreditamento laboratori

modulo **02**

MODULO AVANZATO

20 ORE

- Termini specifici dei CC e struttura documenti
- Struttura dei documenti
- Principali SFR
- Svolgimento valutazione a EAL1 e EAL2 e differenze
- Rapporto Finale di Valutazione (RFV)

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

- L'obiettivo è prendere confidenza con gli strumenti del II volume dei Common Criteria sulle SFR al fine di scrivere i documenti a supporto dei prodotti/sistemi sviluppati o integrati e del III volume dei Common Criteria sulle SARsistemi ICT; svolgere piccole attività di valutazione a livello EAL1 e a EAL2 con l'impiego del CEM
- Modulo esercitativo Ore Approfondimento, esempi ed esercizi di scrittura di ST/PP (CC Vol. II e IV)

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

CORSO 17

FRAMEWORK E STANDARD OPEN PER CYBER RISK ASSESSMENT

Il modulo presenta alcuni dei principali metodi open per l'assessment (non trattamento) dei rischi cyber, dal modello NIST all'approccio europeo di ENISA, fino allo standard ISO/IEC 27001:2022. Il modulo si compone di una prima parte teorica e di una seconda parte orientata ad analizzare molteplici contesti applicativi sia in ambito IT sia in ambito OT. Il modulo è organizzato su due parti da seguire a distanza: il primo teorico di 16 ore; il secondo pratico da 24 ore per un totale di 40 ore.

argomenti

Cyber risk assessment del NIST; Cyber risk assessment di ENISA anche per PMI; Cyber risk assessment dello standard ISO/IEC 27001:2022; Almeno due casi applicativi in ambito IT; Un caso applicativo in ambito OT industriale; Un caso applicativo in ambito OT civile (es., smart city).

target

- **PERSONALE AZIENDALE E DELLA PA DI ORGANIZZAZIONI DEL PERIMETRO NAZIONALE, DELLA NIS2 E DI DORA**
- **STUDENTI DI MASTER E DOTTORATO**
- **PERSONALE DI INFORMATICA E INGEGNERIA INFORMATICA OVVERO DI ALTRI AREE GESTIONALI, ECONOMICHE E TECNOLOGICHE**

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

CYBER RISK ASSESSMENT – NIST

16 ORE

- Introduzione al NIST Cybersecurity Framework (CSF): Core, Implementation Tiers, e Profiles
- Identificazione dei rischi: asset criticality, threat intelligence e valutazione delle vulnerabilità
- Categorizzazione dei controlli: identità e gestione degli accessi, protezione, rilevazione, risposta e ripristino
- Metriche e indicatori di performance per il monitoraggio del rischio
- Simulazione di un framework di rischio per una piccola organizzazione IT (es. azienda di servizi SaaS)

modulo 02

CYBER RISK ASSESSMENT – ENISA

16 ORE

- Linee guida di ENISA per la gestione dei rischi
- Adattamento dell'approccio ENISA alle PMI: semplicità e scalabilità
- ENISA per il risk management (Cybersecurity Threat Landscape)
- Focus sui contesti europei e il supporto alle PMI per soddisfare i requisiti normativi
- Valutazione del rischio per una piccola impresa manifatturiera (ambito OT). *(Esempio applicativo)*
- Identificazione delle vulnerabilità principali e prioritarizzazione degli interventi

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

modulo 03

CYBER RISK ASSESSMENT - STANDARD ISO/IEC 27001:2022

16 ORE

- Panoramica delle modifiche introdotte nella versione 2022
- Processo di risk assessment ISO: identificazione, analisi, valutazione e trattamento del rischio
- Risk ownership e monitoraggio continuo del rischio
- Ruolo di Annex A nel rafforzare la sicurezza operativa
- Analisi del rischio ISO per una rete aziendale complessa con accessi remoti (es. azienda multinazionale)

laboratorio

16 ORE

Elaborazione casi applicativi

- Caso Applicativo 1:
  IT – Azienda di e-commerce
  Obiettivo: Creare un cyber risk assessment per un'azienda di e-commerce
- Caso Applicativo 2:
  Infrastruttura Cloud
  Obiettivo: Applicare le linee guida ENISA a un ambiente cloud
- Caso Applicativo 3:
  OT Industriale
  Obiettivo: Realizzare un cyber risk assessment per un impianto industriale OT
- Caso Applicativo 4:
  OT Civile – Smart City (es. gestione traffico)
  Obiettivo: Valutare i rischi in un contesto smart city

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

CORSO 18

FRAMEWORK E STANDARD COMMERCIALI PER CYBER RISK ASSESSMENT

Il modulo presenta due dei principali metodi commerciali per l'assessment (non trattamento) dei rischi cyber. Il modulo si compone di una prima parte teorica e di una seconda parte orientata ad analizzare molteplici contesti applicativi. Il modulo è di 24 ore da seguire a distanza, in cui vi è una parte teorica di 8 ore e una seconda di casi applicativi di 16 ore.

argomenti

I due metodi da prendere in considerazione sono a libera scelta dell'RTI così come l'organizzazione dei contenuti.
Si suggerisce di presentare ciascun metodo in 4 ore di lezione teorica e di dedicare 8 ore per ciascun metodo ai contesti applicativi. Si può anche ipotizzare di considerare uno stesso contesto a cui si applicano i due metodi.

target

- **PERSONALE AZIENDALE E DELLA PA DI ORGANIZZAZIONI DEL PERIMETRO NAZIONALE, DELLA NIS2 E DI DORA**
- **STUDENTI DI MASTER E DOTTORATO**
- **PERSONALE DI INFORMATICA E INGEGNERIA INFORMATICA OVVERO DI ALTRI AREE GESTIONALI, ECONOMICHE E TECNOLOGICHE**

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

METODO FAIR (FACTOR ANALYSIS OF INFORMATION RISK)

16 ORE

- Introduzione al metodo FAIR: principi e struttura generale
- Comprensione dei rischi: asset, minacce, vulnerabilità, perdita
- Processo FAIR: identificazione del rischio, quantificazione, analisi
- Applicazione del framework FAIR al contesto aziendale
- Analisi del rischio per un'azienda IT con focus sull'impatto finanziario di una violazione dei dati

modulo 02

METODO OCTAVE (OPERATIONALLY CRITICAL THREAT, ASSET, AND VULNERABILITY EVALUATION)

24 ORE

- Introduzione a OCTAVE: panoramica e obiettivi del framework
- Identificazione degli asset critici e delle vulnerabilità
- Valutazione dei rischi operativi e pianificazione delle contromisure
- Confronto tra OCTAVE e altri approcci
- Utilizzo di OCTAVE per un sistema SCADA in un contesto industriale

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

Elaborazione casi applicativi

IT – Rete aziendale

Attività con FAIR

- Identificazione degli asset critici (es. database clienti, server)
- Valutazione delle minacce: phishing, malware, DDoS
- Quantificazione del rischio: probabilità e impatto economico
- Output: Report FAIR con grafico di priorità dei rischi

Attività con OCTAVE

- Identificazione delle vulnerabilità specifiche della rete aziendale
- Mappatura degli asset e delle interazioni
- Analisi del rischio con OCTAVE, evidenziando minacce critiche

Output: Piano d'azione OCTAVE per mitigare i rischi prioritari

OT – Impianto Industriale

Attività con FAIR

- Identificazione dei componenti critici (PLC, sensori, reti)
- Valutazione delle minacce: manipolazione dei dati, interruzioni di servizio
- Quantificazione del rischio per l'impianto, con focus sull'impatto operativo
- Output: Analisi FAIR con priorità dei rischi per i processi industriali

Attività con OCTAVE

- Analisi delle vulnerabilità specifiche di SCADA e dispositivi OT
- Identificazione di attacchi mirati (es. ransomware)
- Creazione di un piano di mitigazione basato su OCTAVE

Output: Report OCTAVE con raccomandazioni per la sicurezza OT.

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

SECURITY OF CLOUD & EMERGING TECHNOLOGIES

19 Orchestratori distribuiti e applicazioni “Cloud Native” 90

CORSO 19

ORCHESTRATORI DISTRIBUITI E APPLICAZIONI “CLOUD NATIVE”

Il corso offre una panoramica sugli aspetti operativi e di sicurezza dell’orchestratore Kubernetes e le caratteristiche delle applicazioni cloud native. Il modulo si divide in tre parti: la prima della durata di 8 ore illustra l’architettura e le scelte progettuali dietro all’orchestratore, la seconda della durata di 20 ore coinvolgerá invece delle lezioni pratiche sull’installazione, operazione, manutenzione sia di applicativi che dell’orchestratore stesso. Il terzo modulo di 12 ore approfondisce le tematiche di sicurezza, tra cui la gestione dei segreti, la gestione della rete, le pratiche di osservabilità e la simulazione e il rilevamento di potenziali attacchi.

argomenti

Architettura di Kubernetes, nodi, stato distribuito, modello a Pod, networking model; installazione e manutenzione di Kubernetes in ambienti baremetal, controllori integrati, service discovery, gestione traffico nord-sud, operatori, gestori di pacchetti per Kubernetes; gestione dei segreti, policy di rete, monitoraggio, logging, auditing, detection di movimenti laterali (pivot) ed evasione dalle sandbox.

target

- **AZIENDE DI MEDIE E GRANDI DIMENSIONI** che stanno effettuando una transizione verso architetture cloud native
- **SOCIETÀ DI CONSULENZA IT** che necessitano di formare il proprio personale sulle tecnologie container
- **STARTUP TECNOLOGICHE** che intendono scalare le proprie infrastrutture
- **SYSTEM INTEGRATOR** che devono gestire deployment complessi per i propri clienti
- **PROFESSIONISTI IT, DEVOPS ENGINEER, SYSTEM ADMINISTRATOR E SVILUPPATORI SOFTWARE** che desiderano acquisire competenze approfondite su Kubernetes e le architetture cloud native

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

articolazione del corso

modulo 01

ARCHITETTURA E SCELTE PROGETTUALI

8 ORE

- Architettura di Kubernetes
- Nodi
- Stato distribuito
- Modello a Pod
- Networking model

modulo 02

TECNICHE DI INSTALLAZIONE, OPERAZIONE E MANUTENZIONE

20 ORE

- Installazione e manutenzione di Kubernetes in ambienti baremetal
- Controllori integrati
- Service discovery, gestione traffico nord-sud
- Operatori
- Gestori di pacchetti per Kubernetes

modulo 03

TEMATICHE DI SICUREZZA

12 ORE

- Gestione dei segreti
- Policy di rete
- Monitoraggio
- Logging
- Auditing
- Detection di movimenti laterali (pivot) ed evasione dalle sandbox

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

laboratorio

16 ORE

Tutti i contenuti del modulo due si terranno sotto forma di esercitazioni guidate all’interno di macchine virtuali, permettendo agli allievi di fare esperienza pratica con le tecnologie prese in esame.

Le durate dei moduli sono indicative, da confermarsi in fase di microprogettazione

Finanziato
dall'Unione europea
NextGenerationEU

Ministero
dell'Università
e della Ricerca

Italiadomani
PIANO NAZIONALE
DI RIPRESA E RESILIENZA

SERICS
SECURITY AND RIGHTS IN THE CYBERSPACE

serics.eu

serics.eu/academy academy@serics.eu