CONSORZIO
UNIVERSITARIO
HUMANITAS

Corso di Alta Formazione

FAD Asincrona

INTRODUZIONE ALLA CYBERSECURITY

Direzione scientifica

GIANLUIGI ME

PIERLUIGI PERRONE

GIUSEPPE GIULIO RUTIGLIANO

DIREZIONE SCIENTIFICA

Gianluigi Me
Docente Università Luiss Roma

Pierluigi Perrone
Docente Università Luiss Roma

Giuseppe Giulio Rutigliano
Responsabile Telematica Armamento ed Equipaggiamenti Speciali , Arma dei Carabinieri

PRESENTAZIONE

Il corso di CyberSec (Cyber Security) è progettato per fornire agli studenti una comprensione completa dei principi della sicurezza informatica unita ad una conoscenza introduttiva delle tecniche e degli strumenti utilizzati maggiormente negli attacchi informatici con l'obiettivo di comprendere come adottare le opportune contromisure difensive. Il corso copre argomenti come gli attacchi tramite Social Engineering, crittografia, virus e malware, firma digitale, contesto normativo.
Il corso è suddiviso in moduli, ognuno dei quali copre un aspetto specifico della Cyber Security, comprendenti lezioni teoriche affiancate da lezioni pratiche di laboratorio. Ad esempio, un modulo potrebbe concentrarsi sulle tecniche di attacco basate sull'utilizzo di tecniche di Social Engineering. Un altro modulo potrebbe essere incentrato sull'acquisizione dei principali concetti legati alla crittografia.
Alla fine del corso gli studenti avranno l'opportunità di applicare le tecniche apprese durante il corso per risolvere problemi e raggiungere obiettivi specifici, anche sotto forma di Capture the Flag. In questo modo, gli studenti possono comprendere meglio come utilizzare le tecniche e gli strumenti della Cyber Security in situazioni reali.

OBIETTIVI

Il principale obiettivo del corso CyberSec (Cyber Security) è quello di illustrare agli studenti i concetti fondamentali della sicurezza informatica, nonché le metodologie e tecnologie per la protezione dei sistemi, delle reti, delle applicazioni e dei dati. Per poter meglio comprendere finalità e modalità di impiego delle metodologie di cybersecurity illustrate, queste saranno precedute dalla descrizione dei corrispondenti attacchi e minacce nei vari contesti.
Alcuni degli obiettivi specifici potrebbero includere:

- Apprendere i principi fondamentali della sicurezza informatica;
- Acquisire una corretta awareness relativamente ai rischi legati agli attacchi informatici;
- Comprendere le basi degli attacchi basati sul social engineering;
- Imparare i principi legati alla protezione dei dati con crittografia;
- Conoscere le più note forme di attacco tramite virus e malware;
- Avere un inquadramento del contesto normativo italiano e europeo
- Acquisire i concetti principali di firma digitale

RICONOSCIMENTI

Attestato di partecipazione

DESTINATARI

Il Corso è destinato principalmente ai laureati in Giurisprudenza, Psicologia, Ingegneria e altre discipline tecnico/scientifiche, nonché a tutti i professionisti e agli operatori di settore: direttori ICT di imprese private e Pubbliche Amministrazioni, manager, imprenditori e professionisti, consulenti operanti nel settore della sicurezza e intelligence, funzionari dello Stato, avvocati e praticanti legali, consulenti legali.

MODALITÀ

L'attività didattica sarà svolta con lezioni live in videoconferenza e in presenza per quanto riguarda la parte teorica mentre la parte riguardante le lezioni pratiche di laboratorio sarà erogata mediante sessioni preregistrate in modalità asincrona.

PROGRAMMA

Principi sulla sicurezza informatica

- Introduzione alla sicurezza
- Cybersecurity – Definizione e Rilevanza
- I Pilastri della Security
- Cybersecurity – Vulnerabilità

Principi funzionamento sistemi informatici

- Reti
- Web
- Sistemi operativi

Tecniche di Social Engineering

- Tecniche di attacco
- Web application security
- Phishing
- Security awareness e prevenzione

Metodi per restare anonimi sul web e cercare vulnerabilità

- TOR
- Shodan
- NMAP

Principi sulla Crittografia

- Simmetrica
- Asimmetrica
- Firma digitale

Attacchi principali

- Cracking password
- Xss
- Sqli
- Privilege escalation

Contesto normativo

- Italiano
- Europeo

COSTO

- 80 €

MODALITÀ DI PAGAMENTO

Bonifico bancario intestato a Consorzio Universitario Humanitas – Intesa San Paolo
Codice IBAN:
IT34 N030 6905 2381 0000 0002 173
(Causale: nome, cognome, titolo del corso).

MODALITÀ DI ISCRIZIONE

Seguire la procedura guidata cliccando sul pulsante "iscriviti ora" della pagina web del corso, disponibile sul sito www.consorziohumanitas.com