Introduzione alla Cybersicurezza

Corso di formazione avanzato
per docenti delle scuole secondarie di II grado
(Iniziativa formativa ID. 68611)
Edizione ID. 112847

Indice

CINI Cybersecurity National Lab
c/o DIAG – Sapienza Università di Roma
Via Ariosto, 25 – 00185 Roma RM

https://cybersecnatlab.it

Contatti:
Email: info@cybersecnatlab.it;
segreteria.cybersecurity@consorzio-cini.it
Cell: +39 338 780.2181

1. Presentazione

Il corso è organizzato dal Laboratorio Nazionale Cybersecurity[1] del CINI[2] (Consorzio Interuniversitario Nazione per l'Informatica) nell'ambito del programma CyberHighSchools[3].

Rivolto in primis ai docenti delle scuole secondarie di II grado che hanno aderito al programma, il corso mira ad approfondire tematiche avanzate di sicurezza informatica legate a:

1. Crittografia
2. Web security
3. Network security
4. Software security
5. Hardware security

attraverso un opportuno mix di lezioni e di esercitazioni pratiche, tutte fruibili in remoto e su piattaforme ufficiali del Laboratorio.

Il corso è gratuito, è tenuto da collaboratori esperti del Laboratorio ed ha una durata complessiva di 30 ore ed è fruibile in modalità remota tramite la piattaforma Zoom.

2. Obiettivi

Il corso mira a far crescere la sensibilizzazione verso le problematiche di sicurezza nell'uso di strumenti e tecnologie informatiche, attraverso un opportuno mix di lezioni e di esercitazioni pratiche, tutte fruibili in remoto.

3. Organizzazione

- Il corso prevedere 30 ore complessive di impegno, di cui:
  - 14 h di lezione, fruibili da remoto, in modalità e-learning, tramite lezioni video-registrate;
  - 16 h di tutoraggio on-line.
- L'erogazione del corso avverrà nell'arco di 8 settimane e prevede, tra l'altro:
  - Questionari anonimi per l'analisi delle competenze in ingresso e in uscita
  - Esercitazioni pratiche su piattaforma di addestramento del Laboratorio
  - Rilascio di un attestato di superamento del corso, anche sotto forma di Open Badge[4].

[1] https://cybersecnatlab.it
[2] https://www.consorzio-cini.it
[3] https://cyberhighschools.it
[4] https://openbadges.org

4. Modalità di erogazione e fruizione

- Le lezioni vengono erogate on-line, tramite la piattaforma Zoom, a una classe di max 100 discenti.
- Tutte le lezioni sono preregistrate e messe a disposizione dei discenti.
- Gli incontri iniziale/conclusivo e tutti i tutoraggi sono erogati in modalità on-line live.

5. Programma

Settimana 1 - Incontro Introduttivo:

- In modalità on-line live [1 h – Gaspare FERRARO]
  - Introduzione al corso
  - Presentazione del Laboratorio Nazionale di Cybersecurity
  - La filiera OliCyber > CyberChallenge > TeamItaly
  - Questionario di ingresso

Settimana 2 – Network Security:

- Lezione 2 – in modalità preregistrata
  - Fondamenti di reti di calcolatori
  - Analisi del traffico di rete con Wireshark
- Tutoraggio on-line [2 h – Giulia MARTINO]

Settimana 3 – Crittografia 1:

- Lezione 3 – in modalità preregistrata
  - Introduzione alla crittografia
  - Storia della crittografia
  - Segretezza perfetta e one-time pad
  - Stream ciphers
  - Block ciphers nel mondo reale
- Tutoraggio on-line [2 h – Matteo ROSSI]

Settimana 4 – Web Security 1:

- Lezione 5 – in modalità preregistrata
  - Introduzione a http
  - Il browser web
  - Autenticazione
  - Sessione utente
- Tutoraggio on-line [2 h – Riccardo BONAFEDE]

Settimana 5 – Crittografia 2:

- Lezione 4 – in modalità preregistrata

  - Problema dello scambio delle chiavi
  - Cenni di teoria dei numeri
  - Problemi facili e problemi difficili
  - Scambio di chiavi Diffie-Hellman
  - Crittografia a chiave pubblica e RSA
  - Integrità, Autenticazione e Non-ripudio
- Tutoraggio on-line [2 h – Matteo ROSSI]

Settimana 6 – Web Security 2:

- Lezione 6 – in modalità preregistrata
  - Back-end
  - Database e SQL
  - Iniezioni
  - SQL Injections
  - Command Injections
- Tutoraggio on-line [2 h – Riccardo BONAFEDE]

Settimana 7 – Software Security:

- Lezione 7 – in modalità preregistrata
  - Memory space
  - Tecniche di reverse engineering
  - Buffer overflows
- Tutoraggio on-line [2 h – Giulia MARTINO]

Settimana 8 – Hardware Security:

- Lezione 8 – in modalità preregistrata
  - Security vs Safety
  - Generazione di Numeri Casuali
  - Il ruolo dell'hardware nella Security
  - Vulnerabilità Hardware
- Tutoraggio on-line [2 h – Paolo PRINETTO]

Incontro Conclusivo:

- In modalità on-line live [1 h – Gaspare FERRARO]
  - Analisi dell'andamento del corso
  - Attività future
  - Questionari di uscita

6. Docenti

- Le lezioni e i tutoraggi sono svolti da docenti universitari e afferenti del Laboratorio Nazionale di Cybersecurity:
  - Paolo PRINETTO (Politecnico di Torino)
  - Gaspare FERRARO (Laboratorio Nazionale di Cybersecurity)
  - Riccardo BONAFEDE (Laboratorio Nazionale di Cybersecurity)
  - Matteo ROSSI (Politecnico di Torino)
  - Giulia MARTINO (Università degli Studi di Genova)

7. Costi

- Il corso viene offerto gratuitamente dal Laboratorio Nazionale di Cybersecurity del CINI ai docenti delle scuole superiori di II grado.

8. Prerequisiti

- Competenze base di informatica e programmazione

9. Iscrizioni

- Dal 19/09/2022 al 30/09/2022
- Tramite la piattaforma S.O.F.I.A. del Ministero dell'Istruzione (Iniziativa formativa ID. 68611 – Edizione 112847)

10. Periodo di erogazione

- dal 03/10/2022 al 05/12/2022

Il programma dettagliato degli incontri on-line live, tramite la piattaforma Zoom, è il seguente:

Data	Orario	Docente	Oggetto
03/10/2022	18:00 -19:00	FERRARO Gaspare	Incontro introduttivo
10/10/2022	17:00 -19:00	MARTINO Giulia	Tutoraggio on-line Network Security
17/10/2022	17:00 -19:00	ROSSI Matteo	Tutoraggio on-line Crittografia 1
24/10/2022	17:00 -19:00	ROSSI Matteo	Tutoraggio on-line Web Security 1
07/11/2022	17:00 -19:00	BONAFEDE Riccardo	Tutoraggio on-line Crittografia 2
14/11/2022	17:00 -19:00	BONAFEDE Riccardo	Tutoraggio on-line Web Security 2
21/11/2022	17:00 -19:00	MARTINO Giulia	Tutoraggio on-line Software Security
28/11/2022	17:00 -19:00	PRINETTO Paolo	Tutoraggio on-line Hardware Security
05/12/2022	18:00 -19:00	FERRARO Gaspare	Incontro conclusivo

11. Materiale didattico

- Registrazione delle lezioni
- Copia delle slide utilizzate
- Esercitazioni pratiche su piattaforma del Laboratorio Nazionale di Cybersecurity
- Puntatori a materiali di approfondimento.

12. Punti di forza

- Contribuire a far crescere, nel corpo docente della scuola secondaria di II grado, la sensibilizzazione verso le problematiche di sicurezza nell'uso delle tecnologie informatiche
- Qualificazione del soggetto erogante
- Modalità di fruizione remota, supportata da docenza e tutoraggio qualitativamente significative
- Valorizzazione e diffusione dei programmi CyberChallenge.IT[5] e OliCyber.IT[6]
- Partecipazione gratuita, con rilascio di un attestato di superamento, anche sotto forma di Open Badge.

[5] https://cyberchallenge.it
[6] https://olicyber.it