Introduzione alla Crittografia

Corso di formazione avanzato
per docenti delle scuole secondarie di II grado
(Iniziativa formativa ID. 88892)
Edizione ID. 133723

Indice

CINI Cybersecurity National Lab
c/o DIAG – Sapienza Università di Roma
Via Ariosto, 25 – 00185 Roma RM
https://cybersecnatlab.it

Contatti:
Email: segreteria@cybersecnatlab.it
Cell: +39 338 780 2181

1. Presentazione

Il corso è organizzato dal Cybersecurity National Lab[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 alla crittografia attraverso un opportuno mix di lezioni e di esercitazioni pratiche, tutte fruibili in remoto e su piattaforme ufficiali del Laboratorio.

Il corso è gratuito, tenuto da collaboratori esperti del Laboratorio ed ha una durata complessiva di 16 ore.

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, con particolare attenzione a schemi e protocolli crittografici.

3. Organizzazione

- Il corso prevedere 16 ore complessive di impegno, di cui:
  - 6h di lezione, in modalità e-learning, tramite lezioni video-registrate e materiali didattici online;
  - 10h di tutoraggio on-line.
- L'erogazione del corso avverrà nell'arco di 5 settimane e prevede:
  - Questionari anonimi per l'analisi delle competenze in ingresso e in uscita
  - Esercitazioni pratiche su piattaforma di addestramento del Laboratorio

4. Modalità di erogazione e fruizione

- Le lezioni vengono erogate on-line, a una classe di massimo 100 discenti.
- Lezioni preregistrate e materiale didattico sono messi a disposizione dei discenti.
- L'incontro iniziale e tutti i tutoraggi sono erogati in modalità on-line live.

5. Programma

Settimana 1 – Introduzione e Motivazioni

- Lezione 1 – Materiale didattico online
  - Introduzione alle gare "Capture The Flag"
  - Setup dell'ambiente di lavoro
  - Basi di programmazione in Python
- In modalità on-line live

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

  - Introduzione al corso
  - Presentazione del Cybersecurity National Lab
  - Presentazione dei programmi di formazione
  - Questionario di ingresso

Settimana 2 – Crittografia Simmetrica 1

- Lezione 2 – 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
  - Scripting in Python: operazioni di base
  - Challenge introduttive di crittografia simmetrica

Settimana 3 – Crittografia Simmetrica 2

- Tutoraggio on-line
  - Scripting in Python: la libreria pycryptodome per la crittografia simmetrica e l'interazione con i server remoti
  - Challenge avanzate di crittografia simmetrica dal programma OliCyber.IT

Settimana 4 – Crittografia Asimmetrica 1

- 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
  - Scripting in Python: la libreria pycryptodome per la crittografia asimmetrica
  - Challenge di introduzione alla crittografia asimmetrica

Settimana 5 – Crittografia Asimmetrica 2

- Tutoraggio on-line
  - Challenge avanzate di crittografia asimmetrica dal programma OliCyber.IT
  - 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 Cybersecurity National Lab:
  - Gaspare FERRARO (Cybersecurity National Lab)
  - Francesco FELET (Cybersecurity National Lab)

7. Costi

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

8. Prerequisiti

- Competenze base di informatica e programmazione
- Consigliata programmazione Python

9. Iscrizioni

- dal 28/10/2023 al 18/01/2024
- Tramite la piattaforma S.O.F.I.A. del Ministero dell'Istruzione (Iniziativa formativa ID. 88892 – Edizione 133723)

10. Periodo di erogazione

- dal 23/01/2024 al 27/02/2024

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

Data	Orario	Docente	Oggetto
23/01/2024	17:00 - 19:00	FERRARO Gaspare	Introduzione e Motivazioni
30/01/2024	17:00 - 19:00	FELET Francesco	Crittografia Simmetrica 1
06/02/2024	17:00 - 19:00	FELET Francesco	Crittografia Simmetrica 2
20/02/2024	17:00 - 19:00	FELET Francesco	Crittografia Asimmetrica 1
27/02/2024	17:00 - 19:00	FELET Francesco	Crittografia Asimmetrica 2

11. Materiale didattico

- Registrazione delle lezioni
- Copia delle slide utilizzate
- Esercitazioni pratiche su piattaforma del Cybersecurity National Lab
- 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[4] e OliCyber.IT[5]
- Partecipazione gratuita, con rilascio di un attestato di superamento con riconoscimento delle ore ai fini didattici.

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

CINI Cybersecurity National Lab
c/o DIAG – Sapienza Università di Roma
Via Ariosto, 25 – 00185 Roma RM
https://cybersecnatlab.it

Contatti:
Email: segreteria@cybersecnatlab.it
Cell: +39 338 780 2181