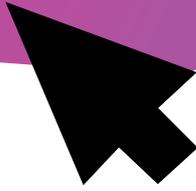




# CYBER WEEK

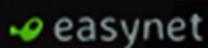


2022



easynet group  
making IT possible





I.I.S. 'A. Badoni'  
in collaborazione con  
Easynet S.P.A.  
ORGANIZZA



I.I.S. "A. Badoni"  
Via Rivolta, 10 - 23900 Lecco  
Tel: +39 0341 365339  
E-mail: [lcis00900x@istruzione.it](mailto:lcis00900x@istruzione.it)



Easynet S.p.A.  
C.so Promessi Sposi 25/D - 23900 Lecco  
Tel: +39 0341 256911  
E-mail: [info@enet.it](mailto:info@enet.it)

SETTIMANA CYBER SECURITY  
dal 28 marzo al 1 aprile



Nel corso della settimana i ragazzi delle classi quarte di Informatica e Telecomunicazioni, guidati dagli Ethical Hacker di Enforcer S.r.l. società del Gruppo Easynet, si sfideranno in una serie di attacchi e difese informatici.

Il nuovo Per-Corso ha lo scopo di introdurre studentesse e studenti alle professioni di nuova generazione indispensabili alle aziende di qualsiasi settore e previste dalle normative europee in materia di Sicurezza Informatica.

I tre professionisti della Cyber Security più ricercati dalle aziende sono: il Penetration Tester, l'Ethical Hacker ed il Security Consultant.

I Profili Professionali Cyber più richiesti secondo il rapporto CLUSID 2021 sono:

- CISO - Chief Information Security Officer
- SOC Manager
- SOC Analyst
- Penetration Tester
- Ethical Hacker
- Security System Administrator
- Security System Engineer
- Cyber Threat Intelligence Specialist
- Security Researcher
- Risk, Governance & Compliance Specialist
- Security Architect

Altre professioni molto richieste:

- Security Developer
- Machine Learning Specialist
- DPO - Data Protection Officer
- Computer Forensics

## Programma della "Cyber Week"

- Introduzione all'Ethical Hacking
- VA e PT: analogie e differenze
- Metodologie di analisi dei target (NIST, OSSTMM, OWASP)
- Scansione ed Enumerazione
- Exploit dei servizi vulnerabili
- Attacchi alle applicazioni Web e Assessment: analogie e differenze
- Enumerazione e Spidering
- Logiche Client e Server Side
- Vettori di Injection
- Falle nei sistemi di autenticazione e autorizzazione
- Vettori di Privilege Escalation
- Scenari Cross Site
- Altre problematiche
- Verifica finale attraverso un laboratorio creato ad-hoc

I partecipanti al corso impareranno a comprendere alcune delle tecniche più note di attacco e di intrusione dei criminali informatici. Saranno illustrate le metodologie OWASP e NIST.

Obiettivo del corso è quello di far apprendere ai partecipanti come viene compromessa la sicurezza dei sistemi, delle reti IT e delle applicazioni Web, utilizzando le tecniche e gli strumenti che vengono adottati dai reali attaccanti. Le competenze trasmesse permetteranno di poter decidere in piena autonomia quali contromisure sia meglio adottare per proteggere le proprie infrastrutture e applicazioni. Durante il corso non verranno elencati strumenti o exploit 0-day, ma rivelato il punto di vista che guida gli attaccanti per comprendere come difendere i propri asset al meglio.

Gli argomenti trattati verranno verificati attraverso sessioni pratiche guidate in laboratorio.