Cybersecurity V: Laboratori virtuali di Cybersecurity

La **Sicurezza Informatica** è la branca dell'informatica che si occupa di proteggere sistemi, reti, programmi e dati dagli attacchi digitali. Questi attacchi possono mirare a rubare informazioni sensibili, interrompere servizi, danneggiare dispositivi o chiedere riscatti e quindi sono compiuti principalmente da gruppi criminali, ma in realtà chiunque grazie a internet può diventare hacker con la giusta dose di passione e impegno.

Un hacker non è necessariamente un attore malevolo: nel mondo della cybersecurity **un hacker è un esperto di sicurezza** che può sfruttare le sue conoscenze per difendere i sistemi informatici dagli attacchi (defensive security) e può contribuire a questo obiettivo anche imparando ad attaccare questi stessi sistemi (offensive security) per trovare ed evidenziare le falle di sicurezza.

Imparare ad attaccare un certo sistema, infatti, vuol dire imparare a conoscerlo, imparare le sue caratteristiche e i suoi difetti ma, soprattutto, vuol dire impararare il funzionamento di computer, programmi e reti; in pratica, è una porta d'accesso verso l'informatica tout cour. Per questo è molto importante **parlare di sicurezza informatica a scuola**: è un altro punto di vista interessante, sicuramente con un certo appeal verso gli studenti, per avvicinarli allo studio dell'informatica o, se non altro, condurli alla conoscenza del mondo digitale che li circonda, in tutte le sue sfaccettature.

News

IMPARARE DIVERTENDOSI

L'offensive security e l'hacking sono aspetti importanti della cybersecurity che hanno una certa visibilità pop, pensiamo a come nelle serie TV e nei film gli hacker sono generalmente descritti come individui in grado di fare virtualmente qualsiasi cosa; anche se non è proprio così, di certo **la figura dell'hacker genera un certo fascino**. Perché non sfruttare quindi questa componente intrigante per coinvolgere gli studenti in attività che li avvicinino a questa disciplina?

Uno dei metodi più efficaci per coinvolgere i giovani studenti nella cybersecurity è la **gamification**: utilizzare il gioco per insegnare concetti di sicurezza rende l'apprendimento più interessante e interattivo. Ci sono molti siti web che offrono laboratori pratici per acquisire esperienza diretta. Questi **laboratori virtuali** possono essere anche usati in classe seguendo l'approccio del learn by doing per trattare i temi più disparati: la programmazione web, le basi di dati, le tecniche crittografiche, i protocolli di rete e così via…

CTF – CAPTURE THE FLAG

Una categoria a sé, oltre che forse l'alternativa più semplice per iniziare, è data dai siti che organizzano e che allenano a svolgere le Capture The Flag (CTF), ovvero delle **competizioni** in cui gli studenti devono risolvere delle sfide di sicurezza. Ogni sfida comporta il superamento di problemi tecnici, come trovare vulnerabilità in un sistema, decrittare informazioni o bypassare misure di sicurezza. L'obiettivo è trovare una "flag", cioè una stringa di testo nascosta, che prova la riuscita della sfida. I CTF sono usati sia per allenare le competenze tecniche che come gare tra esperti e praticanti di hacking etico. Molti eventi CTF sono progettati per principianti e possono essere un modo eccellente per apprendere le basi.

Un sito in inglese molto interessante per sperimentare questo tipo di sfide è PicoCTF. Nella sezione *Compete* si può trovare il calendario delle future competizioni in aggiunta agli scoreboard delle gare passate. Nella sezione Practice è possibile invece allenarsi sui quesiti delle vecchie competizioni potendo selezionare sia la difficoltà sia la categoria. Il sito inoltre mette a disposizione un'interessante funzionalità che permette di creare delle classi (dal menu Classrooms) invitando i propri studenti a partecipare a una selezione di sfide appositamente scelte dall'insegnante.

Una valida alternativa italiana è il sito di OliCyber, in cui da un lato sono presenti tutte le informazioni e le date degli eventi relativi alle Olimpiadi Italiane di Cybersicurezza organizzate dal **Cybersecurity Nationl Lab** e dall'altro un ricco portale di addestramento pieno di sfide CTF. Le sfide sono divise per categoria e per ognuna è indicato un punteggio proporzionale alla difficoltà e il numero di persone che l'hanno risolta.

ALTRE RISORSE FORMATIVE

In aggiunta ai CTF che possono essere un ottimo modo per iniziare e appassionarsi all'argomento, esistono dei siti che permettono di svolgere dei **veri e propri corsi**, in parte gratuiti, e di mettersi alla prova in contesti di hacking più realistici ed elaborati.

Un sito interessante a cui è possibile iscriversi è TryHackMe; qui si possono trovare diversi percorsi formativi il cui completamento permette di guadagnare punti e badge e incrementare la propria posizione nella classifica del portale. Nella sezione Practice sono presenti moltissimi laboratori caratterizzati da un diverso livello di difficoltà.

Un altro sito utile per fare esperienza e avviarsi verso lo studio della Cybersecurity è HackTheBox. Questo portale, molto usato anche a livello professionale, fornisce una Academy con diversi corsi gratuiti, un sito di sfide CTF e molte altre risorse utili, tra le quali spicca il portale dei laboratori pratici di penetration testing, in cui vengono messe a disposizioni delle macchine virtuali che gli studenti possono provare a "bucare". Anche qui la risoluzione dei corsi e delle diverse sfide attribuisce un punteggio che permette di migliorare la propria posizione nella classifica virtuale.

IN CONCLUSIONE

L'approccio pratico e interattivo all'apprendimento è estremamente efficace nell'insegnamento dell'Informatica. Questo approccio, unito alla gamification proposta dalle diverse piattaforme che promuovono l'insegnamento della cybersecurity, è molto stimolante per gli studenti poiché li porta ad affrontare gli argomenti, anche teorici, dell'informatica attraverso la risoluzione di una serie di giochi e rompicapo che rendono il compito più divertente e gratificante.