Titolo Progetto	**HACKER PER UN GIORNO: scopri come attaccare e come difenderti!**			
ENTE PROPONENTE Comitato Scientifico in collaborazione con ITS Academy Fondazione Rizzoli ed azienda Easynet	MODALITA' E BREVE DESCRIZIONE Sai cosa fa un Ethical Hacker? Oggigiorno, la sicurezza informatica è diventata una priorità per le aziende di ogni settore. La presenza costante di minacce informatiche come, per esempio, i **malware** o gli attacchi di phishing, rendono necessario adottare soluzioni efficaci per proteggere i propri dati e la propria reputazione online. Tra le figure esperte di sicurezza informatica si può trovare l'**Ethical Hacker**, un professionista con sofisticate conoscenze in ambito **Cyber Security**, in grado di individuare e prevenire le vulnerabilità che possono minacciare un'infrastruttura informatica. Conosciuto anche con il nome di **White hat** (antagonista dei cosiddetti **Black hat**), l'**Ethical Hacker** è un esperto di sicurezza informatica capace di **simulare, anticipare e prevenire attacchi informatici**. Più nello specifico, l'**Ethical Hacker** simula attacchi al sistema informatico dell'azienda di riferimento al fine di individuare eventuali falle; è dunque in grado di infiltrarsi in reti protette (**penetration test**), di testare l'efficacia dei sistemi di sicurezza aziendale e di valutare l'efficacia delle misure adottate fino a quel momento. Pertanto potrai essere protagonista per un giorno. Ecco le attività proposte: **Parte Teorica** (2 ore) Che cos'è l'hacking: tipologie di attacchi (virus, trojan, spyware etc), tecniche di social engineering, vulnerabilità sistemi. Profili di hacker: black hat, white hat e gray hat. Introduzione all'etica hacker e ai concetti di privacy e sicurezza informatica. **Simulazioni Pratiche** (4 ore) Sessioni controllate di attacchi con tecniche di phishing per ottenere credenziali	OBIETTIVI E DESTINATARI Per quanto riguarda gli obiettivi, questi sono quelli che affiancano l'acquisizione delle DIGITCOMP 2.0 previste a livello europeo. In aggiunta si cercherà di sensibilizzare maggiormente gli studenti affinché possano: **a. Identificare Vulnerabilità:** individuare e documentare le vulnerabilità nei sistemi informatici e nelle reti. Questo processo implica una valutazione completa dei sistemi per scoprire potenziali debolezze; **b. Proteggere Dati Sensibili:** per garantire che i dati sensibili e le informazioni personali rimangano al sicuro da intrusioni e accessi non autorizzati. Questo è particolarmente importante per le aziende e le organizzazioni che gestiscono grandi quantità di dati; **c. Prevenire Attacchi Futuri:** Oltre a identificare le vulnerabilità attuali, si cercherà di a prevenire futuri attacchi. Ciò implica la creazione di piani di sicurezza e il rafforzamento delle difese informatiche. **Questo progetto è dedicato a tutti gli studenti del triennio (un invito particolare agli studenti dei corsi LS e Musicale), fino al raggiungimento di un massimo di 50 alunni.**	DURATA La durata del progetto è **10 ore** Questo si svolgerà presso i laboratorio di informatica dell'Istituto nelle seguenti date: **05 marzo 2024 ore 14.00 - 16.00** **12 marzo 2024 ore 14.00 – 18.00** **26 marzo 2024 ore 14.00 – 16.00** **02 aprile 2024 Ore 14.00 – 16.00**	INFO ISCRIZIONE E SCADENZA **PRE-ISCRIZIONI AL LINK: https://forms.gle/DhUHiWcuuUsChP518** **ENTRO VENERDI' 19 Gennaio 2024** **CODICE CLASSROOM:** **sw5uooj**

	Tentativi di intrusione tramite vulnerabilità note su servizi/protocolli (simulazione attacchi reali come exploit SMB, RCE) Uso di keylogger per registrazione di quanto digitato sulla tastiera Cifratura simulata di filesystem con ransomware Contromisure: utilizzo antivirus, patch di sistema, blocco tentativi di intrusione tramite IPS **Esercitazioni Cyber-Hygiene** (2 ore) Identificazione mail di spear-phishing Simulazione risposta ad attacchi di social engineering via telefono Impostazione password sicure e utilizzo password manager Riconoscimento siti fraudolenti e contenuti non sicuri **Discussione Finale** (2 ore) Confronto guidato sull'esperienza: considerazioni etiche suscitate dalle simulazioni Analisi di casi reali di cronaca per valutare le diverse implicazioni e conseguenze di cyber-crimini Take-home messages: importanza di sviluppare consapevolezza, senso critico e responsabilità come "cyber-cittadini"			

COME ISCRIVERSI

-Preiscriversi utilizzando il link indicato e iscriversi alla classroom del progetto.

- Dopo la scadenza, il tutor comunicherà sulla classroom l'elenco definitivo degli iscritti
- L'iscrizione si dovrà completare poi con la consegna del modulo di adesione e del **patto formativo** sulla classroom stessa in formato pdf.

Informazioni al link:
https://ethicalhackeritaliani.it/

Firmato digitalmente da CARMELA MERONE