BLOOMING

Inclusion and Diversity in STEAM

# Planul de lecție

## Securizarea viitorului: înțelegerea securității rețelei și a criptografiei

---

Obiectiv:

- Elevii vor învăța elementele de bază ale securității rețelei, inclusiv amenințările comune, importanța criptării și metodele de protecție a datelor în timpul transmisiei. Lecția va introduce concepte cheie precum criptografia, securitatea rezistentă la cuantum și detectarea atacurilor în timp real.

Materiale:

- Proiector pentru diapozitive despre concepte de securitate a rețelei
- Documente despre atacurile comune de rețea (man-in-the-middle, denial of service, phishing etc.)
- Laptop-uri sau computere pentru exerciții simulate de securitate a rețelei
- Instrumente/software de securitate a rețelei (de exemplu, Wireshark, instrumente de criptare de bază)
- Acces la Internet pentru cercetarea vulnerabilităților și apărării rețelei

Co-funded by the European Union

Erasmus+
Enriching lives, opening minds.

BLOOMING

Inclusion and Diversity in STEAM

---

Informații generale:

Securitatea rețelei se referă la practicile și tehnologiile concepute pentru a proteja integritatea, confidențialitatea și disponibilitatea datelor pe măsură ce acestea sunt transmise prin rețele. Pe măsură ce atacurile cibernetice devin tot mai sofisticate, este esențial să implementați măsuri de securitate robuste, cum ar fi criptarea, firewall-urile și detectarea atacurilor în timp real. Amenințările emergente, cum ar fi calculul cuantic, pun noi provocări pentru metodele criptografice tradiționale, făcând criptografia rezistentă la cuantică un domeniu important de studiu.

1. Introducere în securitatea rețelei (15 minute):
   - Începeți cu o privire de ansamblu asupra motivului pentru care securitatea rețelei este crucială în era digitală de astăzi. Explicați modul în care rețelele sunt vulnerabile la diferite tipuri de atacuri, inclusiv atacuri man-in-the-middle (MITM), denial of service (DoS) și phishing.
   - Introduceți termeni de bază precum criptarea, firewall-urile și protocoalele de rețea și discutați despre importanța asigurării că datele transmise prin rețele sunt sigure.
   - Menționați provocarea emergentă a calculului cuantic, care amenință sistemele criptografice tradiționale.

2. Atacuri și apărări comune în rețea (20 de minute):
   - Împărțiți clasa în grupuri mici și atribuiți fiecărui grup un atac comun de rețea (de exemplu, MITM, DoS, phishing sau injecție SQL).
   - Cereți fiecărui grup să cerceteze și să prezinte următoarele:
     - Cum funcționează atacul

    - Daunele potențiale pe care le poate provoca
    - Metode de prevenire sau atenuare a atacului (de exemplu, folosind criptare, firewall-uri sau autentificare cu mai mulți factori)
- După fiecare prezentare, discutați despre importanța protocoalelor de securitate care pot detecta și preveni aceste tipuri de atacuri.

3. Activitate practică: Simularea traficului în rețea și detectarea atacurilor (30 de minute):

- Configurați o rețea simulată utilizând un instrument de securitate a rețelei precum Wireshark.
- Cereți elevilor să observe traficul de rețea normal și rău intenționat pentru a înțelege cum pot fi detectate atacuri precum MITM și DoS.
- Instruiți elevii să identifice potențialele vulnerabilități în rețeaua simulată și să sugereze posibile apărări, cum ar fi criptarea mai puternică sau segmentarea rețelei.
- Ghidați elevii prin criptarea datelor (de exemplu, folosind software-ul de criptare de bază) și demonstrați modul în care datele criptate sunt protejate în timpul transmiterii.

4. Explorarea criptografiei rezistente la cuantum (15 minute):

- Introduceți conceptul de calcul cuantic și de ce reprezintă o amenințare pentru metodele actuale de criptare (criptografia tradițională precum RSA și ECC).
- Discutați despre criptografia rezistentă la cuanți și modul în care aceasta utilizează algoritmi proiectați să reziste atacurilor la nivel cuantic.

- Explicați modul în care cercetători precum Dr. Anca Jurcut dezvoltă acești algoritmi rezistenți la cuanți pentru a asigura viitorul comunicațiilor securizate.

Vizualizați și discutați:

- După simulare, utilizați un flipchart sau o tablă albă pentru a crea o hartă vizuală a diferitelor straturi de securitate a rețelei (firewall-uri, criptare, sisteme de detectare a intruziunilor etc.). Discutați modul în care aceste straturi lucrează împreună pentru a crea o rețea sigură.
- Cereți elevilor să ia în considerare modul în care protocoalele de securitate ar putea evolua pe măsură ce tehnologii precum calculul cuantic devin mai răspândite și modul în care detectarea atacurilor în timp real va juca un rol cheie în securitatea viitoare a rețelei.

Puncte suplimentare de discuție:

- Aplicații ale securității rețelei: discutați despre modul în care securitatea rețelei este esențială în diferite sectoare, cum ar fi bancare, asistență medicală, guvern și chiar uz personal (de exemplu, securizarea tranzacțiilor online, a e-mailului și a rețelelor sociale)
- Viitorul criptografiei: Implicați studenții într-o discuție despre viitorul potențial al criptografiei și despre modul în care algoritmii rezistenți la cuanți vor proteja datele în era calculului cuantic.
- Hacking etic: introduceți conceptul de hacking etic, în care experții în securitate testează în mod intenționat rețelele pentru vulnerabilități pentru a consolida apărarea.

Evaluare:

- Cereți elevilor să scrie o reflecție despre:
    1. Ce atac de rețea l-au considerat cel mai periculos și de ce.
    2. Cum protejează criptarea datelor în timpul transmisiei.
    3. De ce calculul cuantic reprezintă o provocare pentru metodele actuale de criptare și cum criptografia rezistentă la cuantică ajută la depășirea acestei provocări.
- Evaluați prezentările de grup și participarea la activitatea practică. Evaluați capacitatea lor de a detecta atacuri și de a propune apărări.