NAG 2025

Kyberbezpečnosť

Spôsob realizácie: **CTF (Capture The Flag).**

Okruhy: **Prehľad všetkých hlavných obsiahnutých kategórií: https://ctf101.org/**

Odporúčané znalosti:

- **Základy programovania v Python a C (výhodou, ale nie nutné)**
- **Základy práce s Dockerom**
- **Používanie Linuxových príkazov**
- **Znalosti v oblasti kódovania/dátových formátov a hashovacích algoritmov: ASCII, XOR, MD5,...**

Súťažné kategórie:

1. **Kryptografia**
    a. Znalosť známych symetrických šifier
    b. Práca s kódovaním: HEX, Base64
    c. Odporúčaný nástroj: CyberChef https://gchq.github.io/CyberChef/
2. **Forenzná analýza**
    a. Steganografia – analýza obrázkov a ich metadát
    b. Extrakcia dát zo súborov a ich analýza
3. **Reverzné inžinierstvo**
    a. Práca s binárnymi súbormi: disassembler, dekompilátor
    b. Analýza strojového kódu
4. **Počítačové siete**
    a. Základy sieťových protokolov
    b. Použitie Wireshark na analýzu paketov
5. **OSINT (Open source intelligence)**
    a. Odporúčaný článok: https://xelessaway.medium.com/osint-ctf-beginner-roadmap-191d1601e48f
6. **Útoky na webové aplikácie**
    a. Používanie webového inšpektora (napr. „Inspect“ v prehliadači)
7. **Útoky na binárne súbory**
    a. Znalosť buffer overflow útokov
    b. Využitie zraniteľností v binárnych súboroch