MD-2045, CHIȘINĂU, STR. STUDENȚILOR, 9/7, TEL.: (+373) 22 509-905, www.fcim.utm.md

REGULAMENTUL CONCURSULUI

UTM-CTF/2020

An de an, luna octombrie este dedicată **Securității cibernetice**. Luna europeană a securității cibernetice este o campanie anuală a Uniunii Europene menită să sensibilizeze cetățenii și organizațiile cu privire la securitatea cibernetică prin furnizarea de informații la zi din domeniul securității prin intermediul educației și al schimbului de bune practici.

În acest context, studenții de la Programul de studii Securitate informațională a Departamentului Ingineria software și Automatică, organizează anual concursul UTM-CTF, în format Capture the Flag (CTF).

Concursurile Capture the Flag (CTF) sunt modalități populare de a dezvolta cît mai mult cunoștințele și abilitățile practice de securitate prin rezolvarea unor provocări pe teme precum web, criptare, inversare, exploatare.

Se spune ca nu esti cu adevarat specialist în securitate cibernetică daca nu te-ai implicat cel putin o dată intr-o competiție **Capture the Flag** (*Andrei Avădănei, fondator DefCamp*).

Competiția urmărește testarea creativității și a capacității echipelor de elevi, studenți și masteranzi de a utiliza cunoștințe specifice pentru a gestiona probleme concrete de securitate cibernetică. Obiectivul principal constă în stimularea interesului participanților pentru problematica securității cibernetice și evaluarea capacității acestora de a face față provocărilor de securitate cibernetică actuale.

Concursul constă în găsirea unui numar anumit de coduri (flags) prin penetrarea unor aplicaţii web sau sisteme cu vulnerabilităţi induse. Flag-urile sau soluțiile care trebuiesc să fie identificate în cadrul exercițiilor propuse este un cod unic care poate fi găsit atunci cand se reușește să fie rezolvate task-uile din concurs. In principiu formatul de flag este ***utmCTF{some-text}***.

Concurenţii vor utiliza soluţii de conectare de la distanţă la o platformă informatică dedicată. Fiecare problemă rezolvată va aduce un punctaj, iar după finalizarea probelor va fi automat generat un clasament al echipelor participante.

Concursul este deschis elevilor, studenților și masteranzilor instituțiilor de învățământ din Republica Moldova. Este necesară înregistrarea în concurs prin completarea unui formular de participare. Pot participa echipe formate din 4 membri, și un mentor. Unul dintre membrii echipei va avea rolul de șef de echipă. Mentorul trebuie să fie cadru didactic în instituția din care sunt participanții.

Pentru cei care participă pentru prima dată la un astfel de concurs, ar trebui să știți că soluția constă în a găsi flag-ul, atunci când rezolvați un task. Nu există o procedură standard pentru a le găsi, deci este recomandat să faceți mai multe teste și să nu vă limitați gândirea pentru a le obține. În cele din urmă, veți înțelege dinamica acestui tip de concurs CTF și cum să rezolvați rapid provocările.

Comportament care va duce la descalificare din concurs poate fi considerat următorul:

- Cooperea între echipe prin conturi independente, colaborarea sau schimbul de soluții cu alte echipe este interzisă
- Atacarea infrastructurii concursului sau a clasamentului – va duce la descalificare
- Sabotarea altor echipe concurente sau împiedicând în vreun fel progresul lor independent
- Generarea de trafic excesiv - nu este permisă, DOS / DDOS este strict interzis – va aduce cu sine descalificarea din concurs
- Republicarea provocărilor sau a oricărei părți a exercițiilor, postarea de soluții / flag-uri pe alte website-uri/forumuri, IRC

Se va lua în considerate următoarele, în mod obligatoriu:

- Dacă apar întrebări despre taskuri și exerciții, se va întreba organizatorii, prin chat (https://t.me/joinchat/H1WcXhggfLSjotgVsLAQ8A)
- Dacă sunteți sigur ca ați identificat soluția corectă (flag-ul este 100% corect), dar sistemul nostru nu acceptă să-l transmiteți, informați organizatorii prin chat
- Dacă identificați erori în infrastructură de concurs, la fel, informați organizatorii prin chat
- Avem un clasament dinamic ceea ce înseamnă ca cu cat mai multe echipe rezolva o provocare, cu atat punctajul problemei scade.

Recomandări:

Sistemul de operare Kali Linux;

Reverse Engineering - Linux Gdb, Radare2;

Volatility;

John the Ripper;

Wireshark;

Ingineria socială - Sherlock;

Functii hash și criptare;

File explorer, Notepad, Google…

Alte materiale educaționale și instrumente recomandate găsiți pe:

https://www.cybersecuritychallenge.ro/etapa-national/

În special puteți să va antrenați pe:

https://cyberedu.ro/