CONDIȚII ÎNSCRIERE ROCSC

Participanții care vor să se înscrie în competiţie trebuie să îndeplinească următoarele criterii:

- vârsta de până la 25 de ani;
- cetățenie română.

Vârsta de referință este vârsta concurentului la sfârșitul anului calendaristic.

BENEFICII PARTICIPARE

Concurenții selecționați în echipa României vor beneficia de:

- Recunoaștere națională si promovare în media;
- Premii oferite de sponsori pentru participanții in echipa națională;
- Unul sau doua stagii specializate de pregătire;
- Mentorat cu specialiști din domeniu;
- Oportunități de angajare în domeniu;
- Toate costurile asigurate de sponsori;
- Participare la competiții internaționale.

MOD DESFĂȘURARE COMPETIȚIE

Jucatorii vor trebui să se transpună într-un scenariu care presupune dezvoltarea și apărarea unei infrastructuri.
Partea cea mai importantă va rămâne dezvoltarea și apărarea propriei infrastructuri, dar atacarea celorlalte echipe aduce puncte. Vor fi 3 nivele de dificultate a testelor: greu, mediu și ușor.
Jucatorii vor trebui să rezolve un scenariu care presupune dezvoltarea și apărarea unei infrastructuri. De asemenea, aveți șansa să strângeți puncte prin atacarea celorlalte echipe.
Partea cea mai importantă va rămâne dezvoltarea și apărarea propriei infrastructuri. Mai mult, este foarte important să cunoști punctele tari și slabe ale echipei tale, pentru a distribui sarcinile în mod optim.
Vor fi 3 nivele de dificultate a testelor: greu, mediu și ușor.
Testele vor fi din următoarele domenii, dar nu vor fi limitate doar la acestea:

- Securitate web;
- Criptografie;
- Inginerie inversă și investigații;
- Programare;
- Teste de penetrare;
- Atac și aparare;
- Securitate Linux/windows/macOS;
- Securitate telefoane mobile.

MATERIALE EDUCAȚIONALE RECOMANDATE.

- https://www.cyberedu.ro - Exercitiile din cadrul etapelor ROSCC si ECSC din anii anteriori, precum si alte exercitii de la alte competitii internationale

Criptografie

- https://class.coursera.org/crypto-preview
- http://cryptopals.com/
- A Graduate Course in Applied Cryptography - The book covers many constructions for different tasks in cryptography.
- An Introduction to Mathematical Cryptography - Introduction to modern cryptography.
- Crypto101 - Crypto 101 is an introductory course on cryptography.
- Cryptography Engineering - Learn to build cryptographic protocols that work in the real world.
- Handbook of Applied Cryptography - This book is intended as a reference for professional cryptographers.
- Introduction to Modern Cryptography - Introductory-level treatment of cryptography written from a modern, computer science perspective.
- OpenSSL Cookbook - The book about OpenSSL.
- Practical Cryptography for Developers - Developer-friendly book on modern cryptography (hashes, MAC codes, symmetric and asymmetric ciphers, key exchange, elliptic curves, digital signatures) with lots of code examples.
- Security Engineering - There is an extraordinary textbook written by Ross Anderson, professor of computer security at University of Cambridge.
- Serious Cryptography - A Practical Introduction to Modern Encryption by Jean-Philippe Aumasson.
- The Cryptoparty Handbook - This book provides a comprehensive guide to the various topics of the computer and internet security.
- Understanding Cryptography - Often overlooked, this book is a boon for beginners to the field. It contains plenty of exercises at the end of each chapter, aimed at reinforcing concepts and cementing ideas.

Web application hacking

- Hacker101 - Written by hackerone.
- The Daily Swig - Web security digest - Written by PortSwigger.
- Web Application Security Zone by Netsparker - Written by Netsparker.
- Infosec Newbie - Written by Mark Robinson.
- The Magic of Learning - Written by @bitvijays.
- CTF Field Guide - Written by Trail of Bits.
- The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws de Dafydd Stuttard

Reverse Engineering

- Practical Malware Analysis de Michael Sikorski
- The IDA Pro Book
- Reverse Engineering for Beginners
- Assembly Language for Intel-Based Computers (5th Edition)
- Practical Reverse Engineering
- Reversing: Secrets of Reverse Engineering
- Practical Malware Analysis
- Malware Analyst's Cookbook
- Gray Hat Hacking
- The Art of Memory Forensics
- Hacking: The Art of Exploitation
- Fuzzing for Software Security
- Art of Software Security Assessment
- The Antivirus Hacker's Handbook
- The Rootkit Arsenal
- Windows Internals Part 1 Part 2
- Inside Windows Debugging
- iOS Reverse Engineering
- The Shellcoders Handbook
- A Guide to Kernel Exploitation
- Agner's software optimization resources

Exploitation

- Gray Hat Hacking The Ethical Hacker's Handbook, Fourth Edition de Daniel Regalado
- Hacking: The Art of Exploitation, 2nd Edition de Jon Erickson
- Hacking - The art of exploitation
- A bug Hunter's Diary: A Guided Tour Through the Wilds of Software Security
- The Shellcoder's Handbook: Discovering and Exploiting Security Holes

- Sockets, shellcode, Porting, and coding: reverse engineering Exploits and Tool coding for security professionals
- Writing Security tools and Exploits
- Buffer overflow attacks: Detect, exploit, Prevent
- Metasploit toolkit for Penetration Testing, exploit Development, and vulnerability research
- https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/
- https://www.corelan.be/index.php/2009/07/23/writing-buffer-overflow-exploits-a-quick-and-basic-tutorial-part-2/
- https://www.corelan.be/index.php/2009/07/25/writing-buffer-overflow-exploits-a-quick-and-basic-tutorial-part-3-seh/
- https://www.corelan.be/index.php/2009/07/28/seh-based-exploit-writing-tutorial-continued-just-another-example-part-3b/
- https://www.corelan.be/index.php/2009/08/12/exploit-writing-tutorials-part-4-from-exploit-to-metasploit-the-basics/
- https://www.corelan.be/index.php/2009/09/05/exploit-writing-tutorial-part-5-how-debugger-modules-plugins-can-speed-up-basic-exploit-development/
- https://www.corelan.be/index.php/2009/09/21/exploit-writing-tutorial-part-6-bypassing-stack-cookies-safeseh-hw-dep-and-aslr/
- https://www.corelan.be/index.php/2009/11/06/exploit-writing-tutorial-part-7-unicode-from-0x00410041-to-calc/
- https://www.corelan.be/index.php/2010/01/09/exploit-writing-tutorial-part-8-win32-egg-hunting/
- https://www.corelan.be/index.php/2010/02/25/exploit-writing-tutorial-part-9-introduction-to-win32-shellcoding/
- https://www.corelan.be/index.php/2010/06/16/exploit-writing-tutorial-part-10-chaining-dep-with-rop-the-rubikstm-cube/
- https://www.corelan.be/index.php/2011/12/31/exploit-writing-tutorial-part-11-heap-spraying-demystified/
- https://www.corelan.be/index.php/2010/01/26/starting-to-write-immunity-debugger-pycommands-my-cheatsheet/
- https://www.corelan.be/index.php/2010/03/22/ken-ward-zipper-exploit-write-up-on-abysssec-com/
- https://www.corelan.be/index.php/2010/03/27/exploiting-ken-ward-zipper-taking-advantage-of-payload-conversion/
- https://www.corelan.be/index.php/2011/01/30/hack-notes-rop-retnoffset-and-impact-on-stack-setup/
- https://www.corelan.be/index.php/2011/05/12/hack-notes-ropping-eggs-for-breakfast/

- https://www.corelan.be/index.php/2011/07/03/universal-depaslr-bypass-with-msvcr71-dll-and-mona-py/
- https://www.corelan.be/index.php/2011/11/18/wow64-egghunter/
- https://www.corelan.be/index.php/2012/02/29/debugging-fun-putting-a-process-to-sleep/
- https://www.corelan.be/index.php/2012/12/31/jingle-bofs-jingle-rops-sploiting-all-the-things-with-mona-v2/
- https://www.corelan.be/index.php/2013/02/26/root-cause-analysis-memory-corruption-vulnerabilities/
- https://www.corelan.be/index.php/2013/01/18/heap-layout-visualization-with-mona-py-and-windbg/
- https://www.corelan.be/index.php/2013/02/19/deps-precise-heap-spray-on-firefox-and-ie10/
- https://www.corelan.be/index.php/2013/07/02/root-cause-analysis-integer-overflows/

Rezolvări probleme de CTF

- https://github.com/ctfs
- https://github.com/CCSIR/dctf-2017
- https://github.com/CCSIR/dctf16-finals
- https://club.securityespresso.org/writeups/

Alte cursuri

- http://www.cs.fsu.edu/~redwood/OffensiveComputerSecurity/lectures.html
- https://github.com/isislab/Hack-Night
- http://www.opensecuritytraining.info/Exploits1.html
- http://ocw.cs.pub.ro/courses/cns

Tool-uri recomandate:

Reverse Engineering

- Ida Freeware / Radare
- WinDbg
- OllyDbg v1.10
- OllyDbg v2.01
- OllySnD
- Olly Shadow
- Olly CiMs
- Olly UST_2bg
- x64dbg

- gdb
- vdb
- lldb
- qira
- Unicorn
- APKtool
- dex2jar
- Bytecode Viewer
- CFF Explorer
- Cerbero Profiler // Lite PE Insider
- Detect It Easy
- PeStudio
- PEiD
- MachoView
- nm - View Symbols
- file - File information
- codesign - Code signing information usage: codesign -dvvv filename
- dnSpy
- Bytecode Viewer
- Bytecode Visualizer
- Volatility

Exploitation

- Gdb + Peda
- OllyDbg
- WinDbg
- Mona.py

Web application hacking

- Burp Suite Free Edition
- sqlmap - Automatic SQL injection and database takeover tool.
- https://www.arachni-scanner.com/

Operating System

- Kali Linux

Probleme online

- https://wechall.net
- https://attackdefense.com/

- https://www.vulnhub.com/
- http://www.hacker.org/
- https://pentestbox.org/
- OSX Crackmes
- ESET Challenges
- Flare-on Challenges
- Github CTF Archives
- Reverse Engineering Challenges
- xorpd Advanced Assembly Exercises
- Virusshare.com
- Contagio
- Malware-Traffic-Analysis
- Malshare
- Malware Blacklist
- Malwr
- Vxvault
- Protostar
- Fusion

REGULI TESTARE:

- orice tentativă de atac prin metode de tip Denial Of Service a scoreboard-ului sau a celorlalte servicii va conduce la descalificare;
- clasificarea câștigătorilor se face după punctajul total la sfârșitul competiției naționale;
- în caz de egalitate, departajarea se va face după timpul de execuție a task-urilor.

INFORMAȚII TESTARE:

- task-urile testează următoarele capitole de securitate: Reverse Engineering, Exploitation, Forensics, Web Application hacking, Crypto;
- anumite taskuri pot avea componente din mai multe capitole;
- scopul fiecărui task este de a obține o informație (denumită în mod tradițional "flag") la care nu am avea acces, în mod obișnuit, dată fiind protecția oferită de sistemele de securitate. În fiecare task există o problemă de securitate care ne permite (prin analiza de cod și exploatarea sa) să ajungem la flag;
- un flag poate fi recunoscut după forma următoare: flag{sha256 random};
- fiecare task are un număr de puncte în funcție de dificultatea sa;
- unele task-uri ar putea fi blocate în prima fază, dar vor fi pornite ulterior (până la încheierea perioadei de competiție);
- descrierile task-urilor și fișierele aferente fiecăruia vor putea fi copiate de pe un site anexa numit rocsc23.cyberedu.ro;

- pe rocsc23.cyberedu.ro se vor introduce flagurile și se va putea vizualiza progresul fiecărei persoane înscrise;
- vor exista task-uri offline (care se pot rezolva pe calculatorul personal, pentru validare, trimițându-se doar flagul pe scoreboard) și task-uri online (va exista un IP și un PORT prin care sa se faca interacțiunea cu server-ul);
- Este interzisa folosirea de tool-uri automate ce pot impacta disponibilitatea sistemelor informatice sau a problemelor date, cu exceptia precizari acestora la o problema specifica.