ICT Berufsbildung
Formation professionnelle
Formazione professionale

Cyber Security | Skill 54

General description

Introduction

The Cyber Security | Skill 54 competitions presents a unique opportunity for aspiring cybersecurity professionals to demonstrate their expertise and skills in the field of offensive security as well as cyber defense. Within a jeopardy style Capture the Flag (CTF) format, participants are required to solve a wide range of challenges, testing both their theoretical knowledge and practical application in various cybersecurity domains.

A competition consists of several tasks that need to be solved (also referred to as challenge). A challenge counts as solved as soon as a “flag” is retrieved and submitted on the platform. The flag is usually in the format of “flag{something_something_1337}” and can be retrieved by compromising a system or exploiting an application.

The competition language is English.

RegioSkills (Swiss Hacking Challenge)

The regional skills is a collaborative competition between the Swiss Hacking Challenge and ICT-Berufsbildung. Everyone can sign up for free and solve the challenges remotely within the time span of 2 months.
Find out more at Swiss Hacking Challenge (swiss-hacking-challenge.ch)

ICTSkills / SwissSkills

The ICTSkills and/or SwissSkills competition is a one-day competition where contestants need to solve as many challenges as possible during a 7- to 8-hour period. The ICTSkills/SwissSkills competition is an on-site event.

Knowledge

Participants should be well-versed in areas such as (but not limited to):

Cryptography:

- Classical ciphers (Caesar, Vigenère, etc.)
- Modern cryptographic algorithms (AES, RSA, etc.)
- Cryptanalysis techniques

Web Security:

- Cross-Site Scripting (XSS)
- SQL Injection
- Cross-Site Request Forgery (CSRF)
- Server-side vulnerabilities and misconfigurations
- Web session management

Binary Exploitation:

- Buffer overflows
- Return-oriented programming (ROP)
- Heap exploitation
- Reverse engineering of binaries

Forensics:

- Disk and memory forensics
- Network traffic analysis (packet captures)
- Steganography
- File format analysis

Networking:

- Protocols (TCP/IP, UDP, HTTP, FTP, etc.)
- Network scanning and enumeration

Operating Systems:

- Privilege escalation techniques
- System vulnerabilities and misconfigurations

Programming and Scripting:

- Writing scripts to automate tasks or solve challenges (Python, Bash, etc.)
- Understanding of various programming languages (C, Java, JavaScript, etc.)

Mobile Security:

- Android and iOS vulnerabilities
- App reverse engineering
- Mobile network vulnerabilities

Scoring

Challenges are categorized based on difficulty, with each carrying a specific point value. Completing a challenge earns participants its respective points. The more contestants solve a challenge, the more points are deducted for each solver. No partial points are given for solutions. Solutions are automatically graded based on the flags submitted on the platform.

A live leaderboard provides real-time rankings, reflecting participants' performance. Contestants with the same score will be ranked by the time difference of submitting the flag.

Tools

Contestants are required to bring their own devices with their tools of choice preinstalled. It's recommended for beginners to use Kali Linux since it already has most of the tools preinstalled.
If you are a Windows user, it is recommended to have at least WSL installed.

Rules

Violation of any competition rules will result in immediate disqualification:

- Do not attack the organizers infrastructure
- No outside communication
- No teams allowed (unless stated otherwise)
- No sharing hints or solutions
- No flag hoarding

Preparation Tasks

If you need preparation tasks, there are plenty of CTFs and challenges on:

- SHC Library (m0unt41n.ch)
- picoCTF
- CTFtime.org
- TryHackMe
- Hack The Box
- Cyberdefenders
- Blue Team Labs

Remarks

Details for Fairness etc. see in the General-Informations for the ICT Champion-ships.