TARTU ÜLIKOOL
teaduskool

CTF TECH

Course name: **CYBER BATTLE OF ESTONIA CYBER COURSE**

Target Group: 15-24. years old

Course dates: **Cyber course and regional pre-qualifier round**

City	Form of study	Dates
Paide	onsite	7. – 8. May 2022 (Sa, Su)
Narva	onsite	21. – 22. May 2022 (Sa, Su)
Tartu	onsite	4. – 5. June 2022 (Sa, Su)
Tallinn	onsite	11. -12. June 2022 (Sa, Su)
Pärnu	onsite	18. – 19. June 2022 (Sa, Su)
Regional pre-qualifier round	online	27. august 2022 (Sa)

Onsite course times: 10:00 – 16:15 (7 ac/h)/both days
Regional pre-qualifier round: 10:00 – 14:00 (5 ac/h)
Independent work: 20 ac/h
EAP: 1,5 EAP

Course locations: Locations for onsite trainings TBD

Lecturer(s): **Dmitri Stoljarov**, CybExer Technologies cyber security expert
Rain Nõmmsalu, CTF Tech cyber security expert

Course teaching method: **Theoretical part**: cyber course material and independent work
Practical part: solving tasks in a cyber range

Objective: **The aim of the course is to give young people knowledge about:**
- cyber vocabulary
- cyber wisdom
- cyber threats, their identification and ethical hacking
- prevention of cyber threats (Facebook, Instagram, etc.)
- beyond the cyber world, incl. the consequences of using the knowledge gained for unethical purposes
- programs and learning environments

knowledge is passed on by experts in the field using a simplified and playful learning environment. The knowledge acquired in the course will help to raise the awareness of young people in the cyber world, regardless of the specialty they take in the future.

Description: **Topics covered in the two-day cyber course:**
Linux Basics, Port scanning, DNS and Web server enumeration, Brute-forcing, Metasploit, Cyber Security and Cyber Wisdom, Steganography, Cryptography, Web Hacking, Security Vulnerabilities

Learning outcomes: **After completing the course:**
- you know why it's important to be on the good side, or an ethical hacker
- have an overview of Linux Basic commands and know how to use them
- have an overview of potential cyber threats
- can detect IP addresses and read DNS and web server logs
- you know what Metasploit is and how to use it
- have a basic knowledge of steganography and cryptography
- have knowledge of vulnerabilities in online environments and be able to identify them at an early stage
- you have knowledge of programs used to ensure, detect, and improve cyber security

Prerequisites: **following prerequisites must be met:**
- desire and wish to expand one's knowledge in the cyber world through a playful learning environment to be able to defend oneself and not attack others
- a passion for adventure in the world of computing
- basic knowledge of English language is useful

CYBER COURSE SUMMARY

Cyber Course **DAY 1**	**1. LINUX BASICS** in this module, you will understand Linux architecture in general. You will learn how to create and edit text files, delete, copy, and move files and directories. - History of Linux - Basic commands of Linux - Advanced Linux commands - Connecting processes with pipes - File processing commands - Help command **2. PORT SCANNING** you will learn how to identify available IP addresses, hosts, and ports. - Overview of **Nmap** network scanner - Basic usage of **Nmap** network scanner - Port scanning techniques and algorithms **3. NETWORK TRAFFIC ANALYSIS** in this module, you will understand how to identify and read different network protocols. Also, will learn how to reconstruct network intrusions and extract information, such as credentials, images, etc. from network traffic packet capture files. - Overview of various network protocols - Network traffic analysis with graphical tool **wireshark** - Network traffic analysis with command-line tool **tcpdump** - Extraction of information from network captures **4. DNS AND WEB SERVER ENUMERATION** you will learn how to conduct DNS and Web server enumeration. - DNS scanner -**fierce** - Brute-forcing URIs including directories and files with **gobuster** - Scanning web content with **dirb** - Web server vulnerability scanner - **nikto**

Cyber Course **DAY 2**	**5. BRUTE-FORCING** in this module, you will learn how to conduct brute-force attacks against different files and services. - Brute-forcing hashes and encrypted files with **John-the-Ripper** - Using **patator** to brute-force password protected files - **Hydra** - finding passwords for different services (Web, e-mail, FTP, etc.) - **Wi-Fi** traffic analysis and hacking **6. METASPLOIT** in this module, you will learn how to use the most popular exploitation framework Metasploit. - Introduction to **Metasploit** - **Metasploit** fundamentals - Vulnerability scanning with **Metasploit** - The exploitation of different services (Web, mail, etc.) **7. STEGANOGRAPHY** this module teaches you how to hide or extract secret messages from different media files. - Hiding text into pictures with **steghide** - Extracting hidden messages with **steghide** - Password brute-forcing **8. CRYPTOGRAPHY** this module teaches you the ways how to keep data secure and ensure that existing solutions remain robust enough. - Overview of symmetrical encryption - Overview of asymmetrical encryption **9. WEB HACKING** this module introduces you tool-driven process to identify the most widespread vulnerabilities in Web applications. - Analysing web page source code to find useful information - Identifying website security misconfigurations - Finding SQL injections with **'sqlmap'** - Finding broken authentication
Regional pre-qualifier round 27. August 2022	- Individual pre-qualifier round, in which real-life challenges based on the topics covered in the cyber course are solved within a given time frame - Based on the results, the organizer of the pre-qualifier round will form teams of three to five members based on the region, who will be able to represent their region in the final competition, which will take place on **October 29th, 2022** in Tartu.

Additional materials and reading:
DATA PROTECTION AND INFORMATION SECURITY LICENSE- https://akit.cyber.ee
COMPUTER SECURITY MATERIALS BY THE UNIVERSITY OF TARTU -
https://courses.cs.ut.ee/2021/turve/spring/Main/Praktikumid

GRADING

Grading criteria:	passed/not passed
Certificate/Proof:	- Upon passing the cyber course and the regional pre-qualifier round, a **Certificate** will be issued. - Upon completion of the cyber course ONLY, a **Proof** of completion of the cyber course will be issued. **NB!** You can also take part in the pre-qualifier round if you have not completed a cyber course. Find out more at www.ctftech.com