WorldSkills Malaysia (WSM)
University Challenge 2021

TECHNICAL DESCRIPTION

Cybersecurity (CTF Modul)

ORGANIZED BY:
JABATAN PEMBANGUNAN KEMAHIRAN, KEMENTERIAN SUMBER MANUSIA
UNIVERSITI KUALA LUMPUR – MALAYSIA FRANCE INSTITUTE (UNIKL MFI)

1. INTRODUCTION

Cyber Security is one of the new skilll set contested in skill competition across the level, from the World Skills Malaysia Belia (WSMB), ASEAN Skills Competition (ASC), World Skills Asia (WSA) to World Skills Competition (WSC). Skill Competition actively promoting its values, with particular attention to popularizing vocational professions among the younger generation, and facilitating improvement of professional training standards. Thus, Cybersecurity skill in the WORDLSKILL MALAYSIA (WSM) UNIVERSITY CHALLENGE 2021 has an objective to unearth talent in the field of CyberSecurity among youths under the age of 25 to represent the country at various levels of competition

2. TECHNICAL DESCRIPTION

In recent years there has been an explosive growth in online business transactions, the Internet of Things (IoT) and cloud computing. Simultaneously, IT has become an official and unofficial political tool, as well as a means of new types of warfare. Many countries now deliver essential services online, to the extent that citizens without access to IT may become isolated and disadvantaged. This growing collective and individual dependency on IT places a significant obligation on IT service providers to safeguard their systems and users from intentional and unintentional breaches to the security of data and whole systems. As a result, the importance of the Cyber Security Professional cannot be overstated.

In this WORDLSKILL MALAYSIA (WSM) UNIVERSITY CHALLENGE 2021 the cybersecurity skill competition has adopted the challenge of Capture The Flag (CTF) to assess the skillset of the competitor in this domain. In CTF challenge the competitor is asked to solve task of different level of difficulties while finding hidden “Flags” which maybe in the form of hidden phrases, text, or image. To solve these task contestants are required to exercise different skill sets including reverse-engineering, packet sniffing, protocol analysis, system administration, programming,

cryptoanalysis, and writing exploits, among others. Additionally, contestants also require using tools that are in fact used by industry experts in the cybersecurity and knowing the knowledge to use these tools are a leverage to them in the industry. The challenges are based on different areas of penetration testing but not limited to

1st Day

- Enumeration
- Web Based Attacks
- Database Attacks
- Windows Attacks
- Root Access
- Cryptography
- Steganography

2nd Day

- Reconnaissance
- Application Detection
- Exploits
- Drive by download malware
- Reverse Engineering
- Forensic

The Competitors are given access to a CTF system which the URL will be given during the competition. *VPN

3. Hardware and software requirement (Competitor)

- Desktop computer / Laptop
- Web camera 1 unit (Refer Appendix 1)
- High speed internet connection
- Browser to access the monitoring system and CTF competition

4. Workflow

Instructions for the competitor :

- Every day the competition will start from 0900 to 1700.
- Each competitor will be given a unique account to the CTF competition system based on the email given during registration.
- The CTF challenge requires each competitor to login into the CTF competition system for the task.
- The system held all the task and some of the tasks requires the competitor to download a file as part of the task.
- The marks are given by finding something called “cyBLOCKS”. A cyBLOCK is basically a flag and it is represented in the following format.

  MSC2021{<flagvalue>}

  This format may be hidden or even obfuscated in some challenges. So, look out for something that is interesting and pops out.
- Once the flag is found, competitor is required to key in the flag in the CTF competition system.
- Competitors need to take notes the Do and Don’t of the competition

Do not

- Competitor will be disqualified if found
- Executing Malicious scanning, DDoS and ARP Poisoning to the server or other machine
- The competitor seek help from anyone in solving the task.

Do

- Any question can be fowarded to the committee
- Competitor are allowed to use any tool available in order to solve the specific task

5. Marking Scheme

Each solved task from the domain covered in the competition will contribute a point to the competitor. The final marking scheme will be announced during the briefing of the competition

6. Competition Briefing

An online competition briefing will be held a day before the competition through

Zoom/Webex. Link will be given to email provided during the registration.

The Scope of the briefing are.

- Competitor registration and validation
- Hardware and software checking
- Competition briefing

APPENDIX 1 – Web camera setup

WEBCAM