

Test Project Cyber Security

Module C *Capture the Flag - Attack*

Submitted by:
Jay Krishna

Contents

Contents	2
Introduction.....	3
Description of project and tasks.....	3
Marking Scheme.....	4
Workflow.....	4
Mark Summary Form	6
Appendix A.....	7

Introduction

The objective of Capture the Flag (CTF) is to present cybersecurity in an exciting and engaging context and enable security professionals to hone their skills in simulated cyber security attack scenarios.

During the competition, the teams will compete to take down enemy servers, expose vulnerabilities, and win flags while defending their home ground against enemy attacks. The participants were exposed to a range of new tools, skills, and situations.

The Capture the Flag (CTF) is divided into 2 areas. Day 3 is for Attack and Day 4 is for Defense. This document gives the introduction to the player for Attack activities on Day 3.

- Red Team (Attacking): Learn various offensive mechanisms to stay updated with current attack trends and get into the hacker mindset to improve your defense strategy
- Blue Team (Defensive): Learn to defend your organization against distributed denial of service (DDoS), advanced persistent threat (APT), web application threats, and other attacks launched by skilled malicious aggressors

The CTF platform presented in real-time a dashboard of key performance indicators for teams to learn from scenario success rates, red team performance and blue team performance.

Description of project and tasks

STRUCTURE OF THE CTF

The Competitors are given access to a system with Kali Linux 2019 version with all the required tools for completing the exercise successfully.

There will NOT be internet access for the CTF system. All the competitors are expected to use the tools provided. You can refer to the man pages of the tools for their syntax etc.

The Kali Linux machines are accessible to a set of vulnerable machines as targets. Each team has their own set of isolated vulnerable machines so that there will not be any access to a different team. Please refer to the logical network diagram in Appendix A.

CHALLENGES FOR RED TEAM ACTIVITIES:

The challenges are based on different areas of penetration testing but not limited to

- Enumeration
- Web Server Attacks
- Database Attacks
- Windows Attacks
- Root Access.
- Cryptography
- Steganography.

The IP addresses for various servers/devices can be found in Annex B.

Marking Scheme

According to the WorldSkills Standards Specifications within current Technical Description all marks for this Day 3 Test Project module has a maximum mark of 25. Marking scheme is also divided into 7 sub criteria as defined in the areas of penetration testing above. Each sub criterion has the same weight. However, 50% of the aspects within each section will have more than 70% weightage. The remaining 50% of the aspects will only get 30% weightage. You need to submit cyBLOCK (basically a flag) to get the mark. So, it is important to achieve the aspects for all sub criteria to gain maximum marks.

A bonus mark will be given if you have achieved 5 or more sub criteria.

Workflow

Instructions for the team

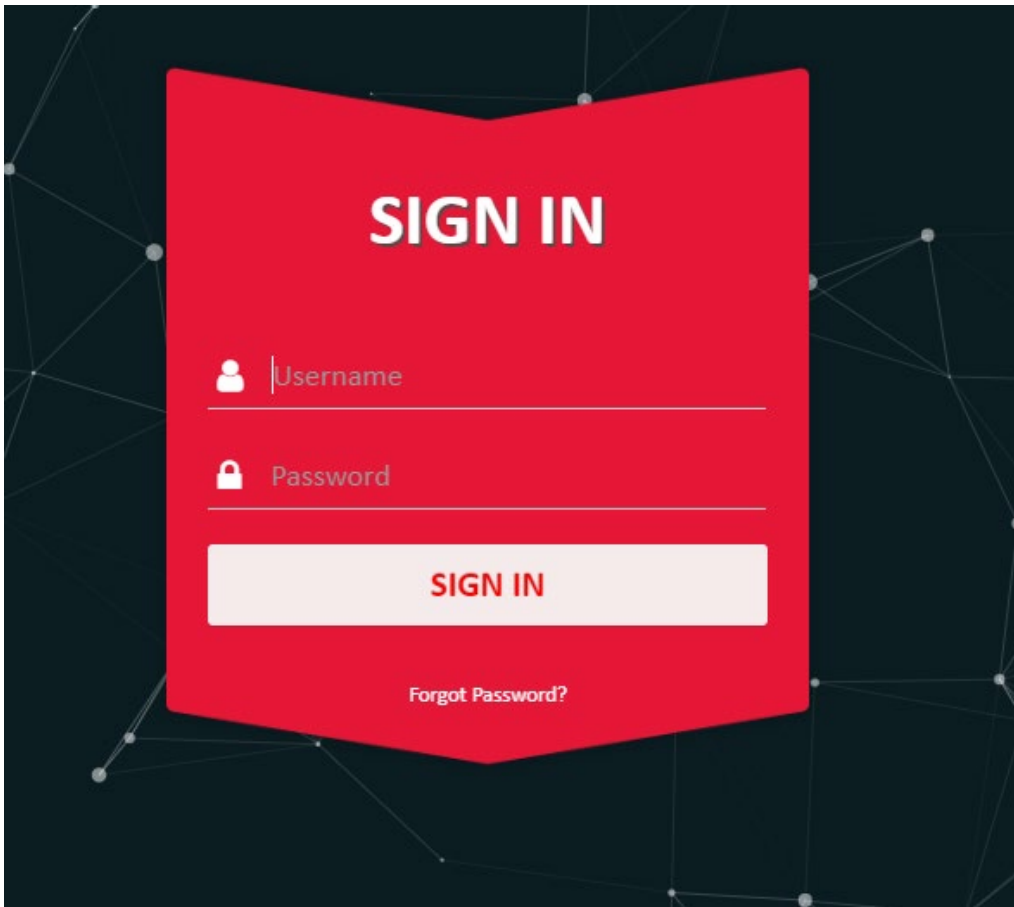
You are playing a role of a security penetration test engineer who is responsible for identifying the security risks of an organizations critical servers by finding ways to understand and gain access to the machines.

The marks are given by finding something called "cyBLOCKS". A **cyBLOCK** is basically a flag and it is represented in the following format.

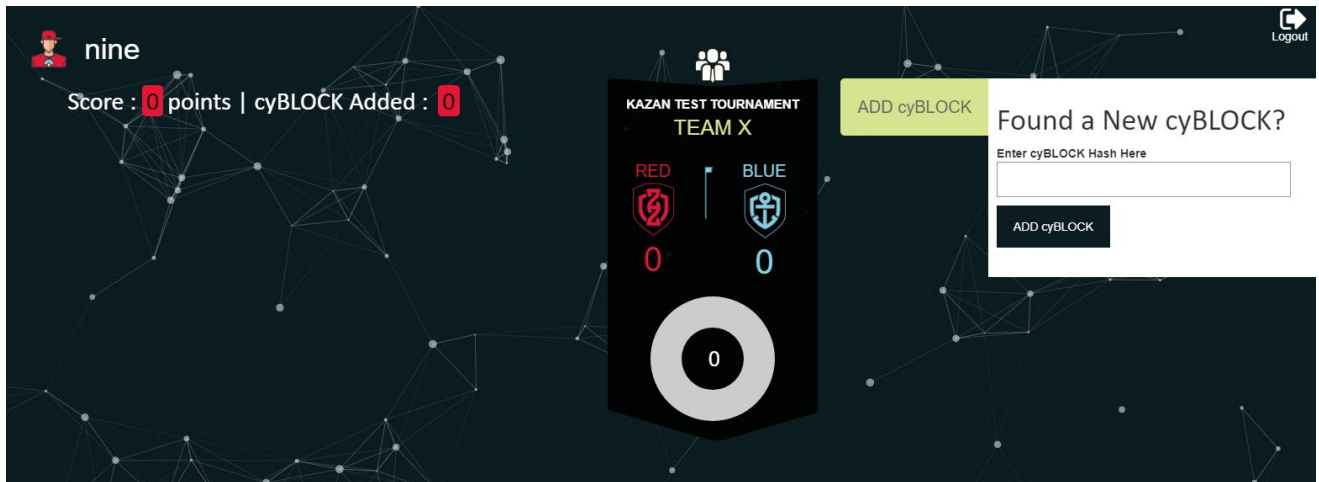
```
icc{<flagvalue>}
```

This format may be hidden or even obfuscated in some challenges. So, look out for something that is interesting and pops out.

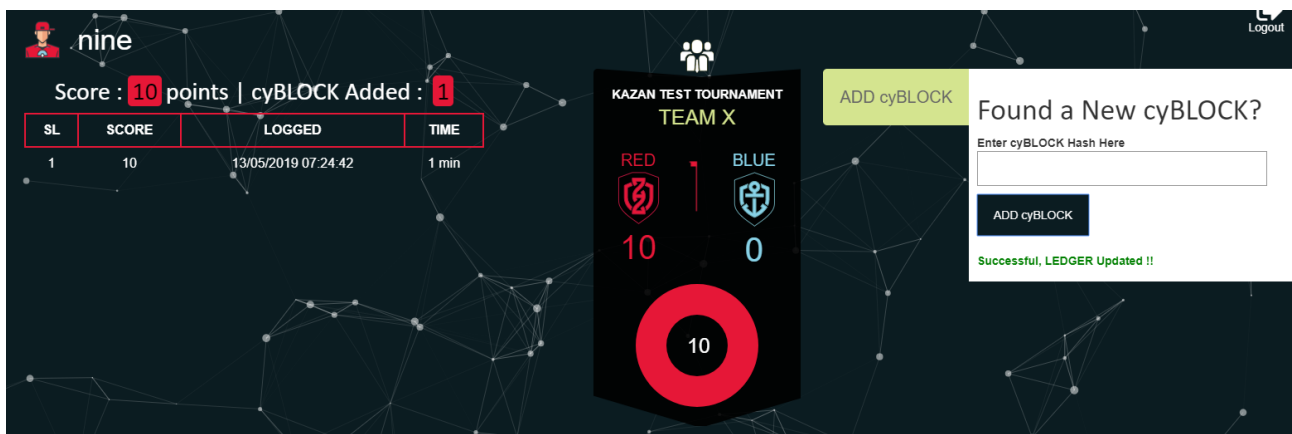
You are also given login access to the scoring system. Each team is given one login so you will have to use the same login for both of the Competitors.



Once you login to the tournament, you will have the ability to enter cyBLOCKS.



Place the flag value in the field for instant validation and score.



Important: Please DO NOT DDoS or perform any attacks to the scoring system or you WILL be disqualified in the game. The server is monitored by a dedicated IPS with alerts.

Mark Summary Form

ID	Description	Mark Summary
C	Capture The Flag (Attack)	25.00
C1	Enumeration	3.50
C2	Web Based Attacks	3.50
C3	Database Attacks	3.50
C4	Windows Attacks	3.50
C5	Root Access	3.50
C6	Cryptography	3.50
C7	Steganography	4.00

Appendix A

