worldskills

Test Project Cyber Security

Module D

Capture the Flag - Defense

Submitted by:
Jay Krishna

Contents

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 Defense activities on Day 4.

- 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 an instance of

- Fortinet NGFW with the following features.
    - Threat Detection
    - Intrusion Prevention System (IPS)
    - Data Loss Prevention (DLP)
- Splunk Enterprise 7 with Fortinet app.

There will **NOT** be internet access for the CTF system. All the competitors are expected to use the tools provided.

The attacks to the network will be automated. The attacks will be only present during a certain time, so its important to identify and work on the alerts timely.

CHALLENGES FOR BLUE TEAM ACTIVITIES:

The challenges are based on different areas of security monitoring but not limited to

- Reconnaissance and Application Detection
- Malware/Exploits
- Phishing
- Lateral Propagation /Botnet
- Data Leakage
- Reverse Engineering
- Digital Forensics

Marking Scheme

According to the WorldSkills Standards Specifications within current Technical Description all marks for this Day 4 test project module has a maximum mark of 25. Marking scheme is also divided into 7 sub criteria as defined in the areas of security monitoringg 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 achieve 5 or more sub criteria.

Workflow

Instructions for the team

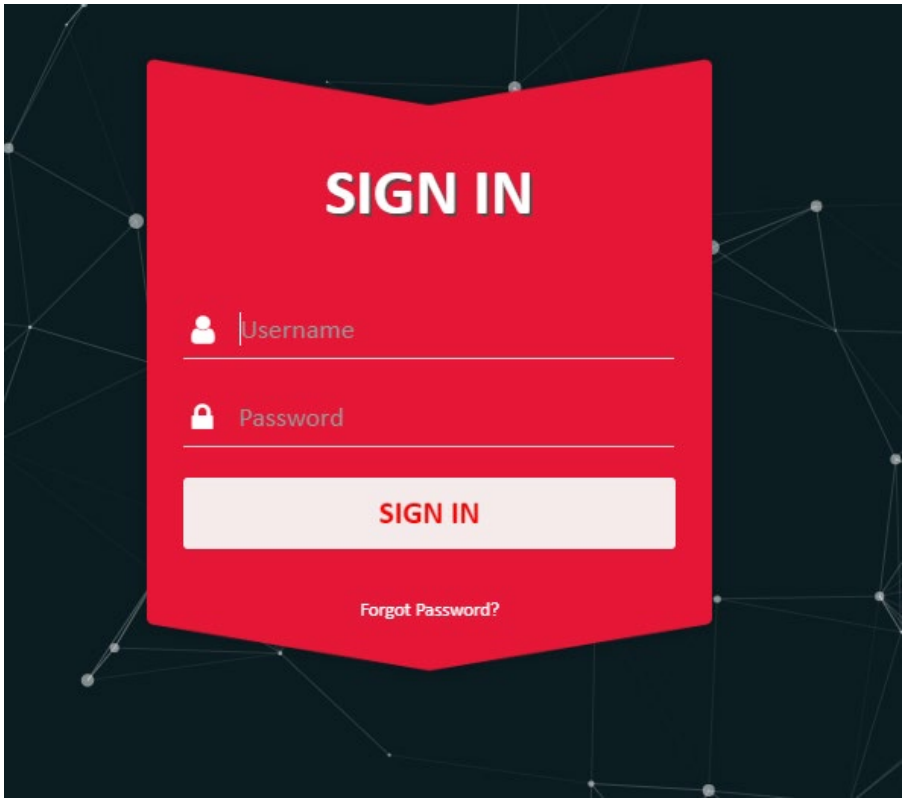
You are playing a role of an SoC analyst and Network Security Engineer who is responsible to identify the attacks targeted on the network.

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

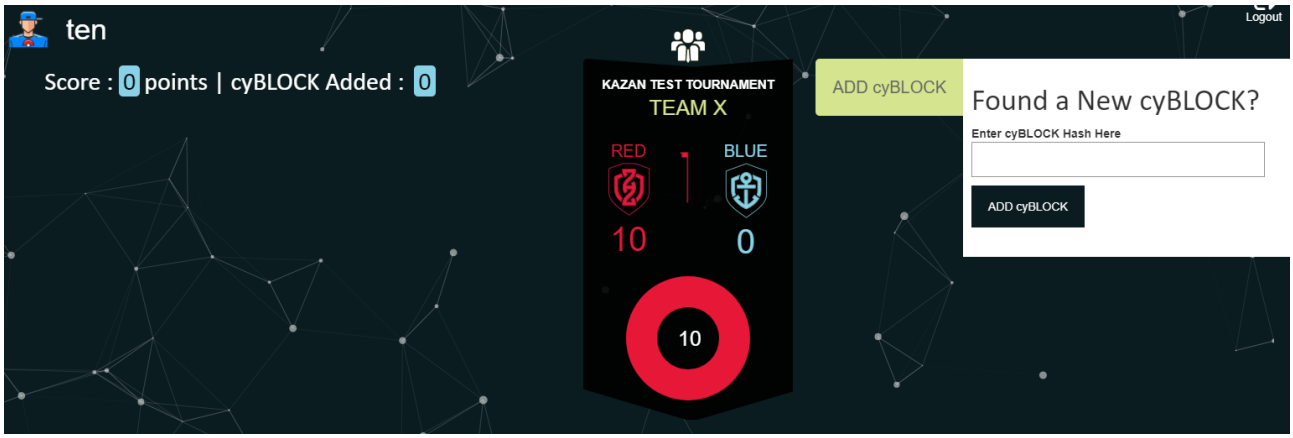
icc{<flag value>}

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

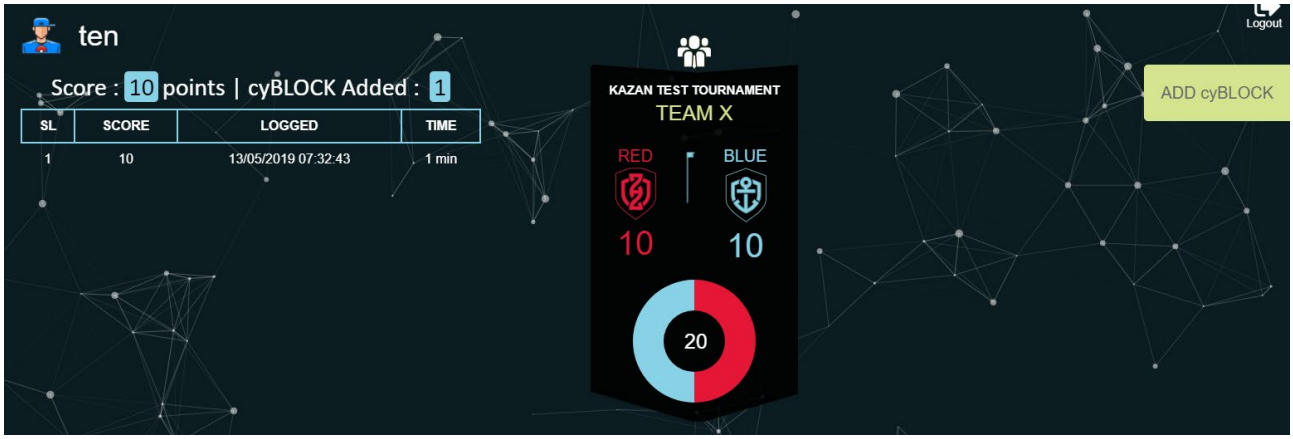
You are also given login access to the scoring system. Each team is given one login so you will have to use the same login for both of the students.



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.

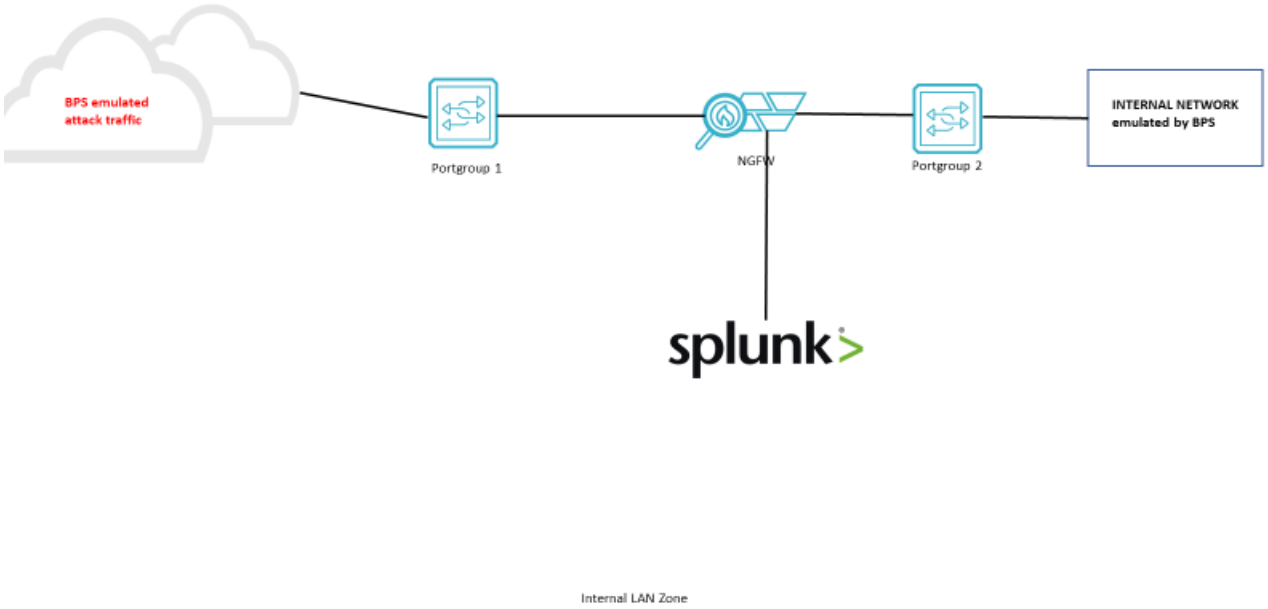


Important: Please DO NOT DDoS or perform any attacks to the scoring system or you WILL be disqualified in the game. The server is monitored by a dedicated IPS with alerts.

Mark Summary Form

ID	Description	Mark Summary
D	**Capture The Flag (Defence)**	**25.00**
D1	Reconnaisance and Application Detection	3.50
D2	Malicious URL	3.50
D3	Exploits, Drive by download malware	3.50
D4	Botnet	3.50
D5	Data Leakage	3.50
D6	Reverse Engineering	3.50
D7	Forensic	4.00

Appendix A


BPS emulated
attack traffic
Portgroup 1
NGFW
Portgroup 2
INTERNAL NETWORK
emulated by BPS
splunk>
Internal LAN Zone