

# CYBER E

CYBER EXERCISE FOR EXCELLENCE



## **Abstract**

From inception to reporting, this article provides an overview of the Cyber eXercise for eXcellence processes. It covers the terminology and life cycle of a cyber exercise, including the planning and execution parts, such as objectives, scenarios, reports, and evaluation procedures, network architectures, tools utilized, and lessons learnt from using the scenarios presented throughout the exercise. Users should be able to grasp the purpose, objectives, planning and execution processes in performing Capture the King, the major feature of Cyber eX, from reading this paper and examining the reference materials.

## Table of Contents

<b>Overview</b> .....	3
<b>Terminology</b> .....	4
<b>Exercise Planning</b> .....	8
<b>Exercise Architecture</b> .....	9
<b>Objectives</b> .....	11
<b>Exercise Participants</b> .....	12
<b>Exercise Judge eX</b> .....	12
<b>Categories of Cyber Exercises</b> .....	13
<b>User Manual</b> .....	14
<b>JUDGE eX MODULE</b> .....	31
<b><i>CTK Guidelines and Policy</i></b> .....	36
EXERCISE GUIDELINES .....	36
GENERAL.....	36
EXERCISE PROPER.....	36

## List of Figures

Figure 1. The “KNOW – DO – LEARN” Framework.....	8
Figure 2. The “CYBER eX” Framework.....	9
Figure 3 Exercise Architecture .....	10
Figure 4 Register Page .....	14
Figure 5 Register (Fill up page).....	14
Figure 6 Register (Fill up page).....	15
Figure 7 Login Page.....	16
Figure 8 Create Team.....	16
Figure 9 Join Team .....	17
Figure 10 Categories .....	18
Figure 11 Capture (button to proceed).....	18
Figure 12 Challenge scenarios.....	19
Figure 13 Challenge (Do List).....	19
Figure 14 Take Challenge .....	20
Figure 15 Download files.....	20
Figure 16 Seize The Throne (Hash format) .....	21
Figure 17 Seize The Throne (Multiple choice) .....	21
Figure 18 Conquered (Preview).....	22
Figure 19 Knowledge Well .....	22
Figure 20 Chronicles .....	23
Figure 21 Upload Files (PDF format).....	23
Figure 22 Uploaded Files (Additional Points) .....	24

Figure 23 Counter Measure ..... 25

Figure 24 Progress Bar ..... 25

Figure 25 Multiplayer Scoreboard ..... 26

Figure 26 Individual Scoreboard..... 26

Figure 27 Participant Team..... 27

Figure 28 Filter Section..... 27

Figure 29 Notification ..... 28

Figure 30 CTK Category (Change)..... 29

Figure 31 Cyber eX Articles ..... 30

Figure 32 Chat Support..... 30

Figure 33 Cyber eX Support System..... 31

Figure 34. Judge eX DASHBOARD..... 31

Figure 35. Judge eX DASHBOARD 1..... 32

Figure 36. Judge eX DASHBOARD 2..... 32

Figure 37. Judge eX PLAYERS mode..... 33

Figure 38. Judge eX MONITORING INDIVIDUAL ..... 33

Figure 39. Judge eX MONITORING TEAMS ..... 34

Figure 40. Figure 39. Judge eX - Score | View Document | Rate ..... 34

Figure 41. Figure 39. Judge eX Sample Scoring ..... 35

## List of Tables

Table 1 Terminology ..... 4

Table 2 Sub categories ..... 5

Table 3 Objectives ..... 11

Table 4. Exercise Structures ..... 13

## Overview

Cyberattacks, particularly targeted attacks, have become more common in recent years, and a huge number of cybersecurity mishaps have occurred often. Capable personnel, on the other hand, are in short supply, and enhancing systematic human resource development for cybersecurity activities is becoming a prominent issue.

The Philippine Army, in compliance with the PA Medium-Term Force Structure 2020-2021, made efforts to plan, develop and organize the activation of the Cyber Battalion, Army Signal Regiment. This is also in compliance on the provisions of the adoption of cyberspace as another domain of operations and the PA Operating Concept.

In order to enforce cybersecurity practical exercises cost-effectively and flexibility, Cyber Battalion developed Cyber eXercise for Excellence, the next generation cyber exercise training platform of the Philippine Army which simulates cyber combat training operational on a virtual environment for the use of Cybersecurity Incident Response Teams (CIRTs) of all respective PAMUs.

The structure and concept of a cyber-exercise are same throughout operations; however, the execution and scenarios differ based on the participants and objectives of the exercise. Understanding the various sorts of workouts and the purposes they serve improves exercise realism and efficacy. Once the operations have established exercise objectives, the exercise users can start looking into what kind of exercise will best complement the objectives and give an effective assessment for the team platform programs.

This playbook guides organizations as they exercise and assess capabilities in the realm of cyberspace. It details the key aspects of designing and executing exercises that pit scenario-driven threats against PA's cyberspace assets. The playbook:

- Defines terminology based on doctrine and practical implementation
- Defines objectives for executing threat scenarios to assess cyberspace operations capabilities
- Outlines threats, ranges, and best practices for operating a Cyber Exercise
- Reports on the effectiveness of cyber injects and scenarios
- Provides the necessary information to execute and assess cyber threat scenarios within an exercise
  - Exercise structures
  - Sample scenarios
  - Sample observation and incident reporting formats
  - Tools that could facilitate various scenarios

## Terminology

As the Philippine Army's reliance on networks has grown, so has the organization's reliance on collective cyberspace defense. Many exercises have the potential to cause misunderstandings about terminology and practices. Table 1 defines important terminology connected to cyber exercises for the purposes of this paper and to establish a similar vocabulary across the exercise, while Table 2 describes the different sub categories in each challenge.

*Table 1 Terminology*

Term	Definition
<b>Apprentice</b>	This category is composed of the most basic and common exercise scenarios in Cybersecurity in the Philippine Army and is relatively beginner friendly. This is automatically unlocked upon log in.
<b>Challenges</b>	Exercise scenarios under each category. These are the scenarios that must be answered correctly to be able to advance to the next level
<b>Chronicles</b>	This is where the team will submit their documentation on how they were able to answer the challenge
<b>Conquered</b>	List of teams who already solved the challenge
<b>Conqueror</b>	An extremely high number of difficulties, most of the exercise relatively above expert level. This category will automatically unlock if the Warrior category has 60% solved challenges
<b>Counter Measure</b>	This is where the team will submit the documentation on the best practices on how to solve the challenge
<b>Cyber Battlefield</b>	The gameplay of Cyber eX which the player gain extra ideas about the scenarios of the challenge to do Capture The King (CTK) which they have to enhance their team and individual requirements as it allows the teams to play and generate challenging platforms to achieve the providing basic and advanced concepts of Cyber Exercise
<b>Cyber eX</b>	The next generation cyber exercise training platform of the Philippine Army that simulates cyber combat training, designed to provide comprehensive hands-on training for Philippine Army personnel to train and improve responsive capacity in case of a cyber crisis
<b>Cyber eX Live Chat Support</b>	Real-time chat support assistance to users
<b>Cyber Smorgasbord</b>	A variety of projects which offers ideas from which you can pick and choose what information you wanted to know about Cyber eX. It contains all the varieties of Cyber Bn Projects
<b>Download Files</b>	Files needed to be able to answer a certain challenge can be downloadable in this tab.

<b>Notifications</b>	Shows the system and challenge updates and announcements
<b>Scoreboard</b>	Shows the up-to-date scores of the team during the exercise
<b>Seize the Throne</b>	This is where you will find the challenge and where you will submit your hash
<b>Team</b>	CIRT trained personnel of a Philippine Army Major Unit (PAMU) composed of one (1) officer and 4 enlisted personnel (EP).
<b>Warrior</b>	In this category, the participant understands the concept, can correctly recognize the given concept of exercise, can weigh it and related concepts as solutions to some problem, and can apply each of them correctly. This will automatically unlock if the Apprentice Category is at least 70% solved

Table 2 Sub categories

<b>Term</b>	<b>Definition</b>
<b>Active Directory Basics</b>	Active Directory is a directory service that centralizes the management of users, computers, and other objects within a network. Its primary function is to authenticate and authorize users and computers in a windows domain.
<b>Burp Suite</b>	Burp Suite is a set of tools used for penetration testing of web applications. ... It is the most popular tool among professional web app security researchers and bug bounty hunters.
<b>Computer Exploitation</b>	A computer exploit, or exploit, is an attack on a computer system, especially one that takes advantage of a particular vulnerability the system offers to intruders. Used as a verb, exploit refers to the act of successfully making such an attack.
<b>Cryptography</b>	Encryption techniques used to make sure that only the sender and recipient of a message can read it. Secret keys are used to protect this access, which are only known by the two authorized parties.
<b>Cybersecurity Threat</b>	A malicious act that seeks to damage data, steal data, or disrupt digital life in general.
<b>Incident Response &amp; Digital Forensics</b>	The field within cybersecurity focuses on the identification, investigation, and remediation of cyberattacks.
<b>Introductory Networking</b>	The aim of this room is to provide a beginner's introduction to the basic principles of networking. Networking is a massive topic, so this really will just be a brief overview; however, it will hopefully give you some foundational knowledge of the topic, which you can build upon for yourself.
<b>Linux Fundamentals</b>	All of the necessary shell and operating system commands are taught, allowing you to start and use the Linux operating system's full potential.

<b>Malicious logic</b>	Is a set of instructions that cause a site's security policy to be violated. The types of malicious logic are Trojan Horse, Virus, Logic Bomb, Time Bomb, Trapdoor, Worm and Rabbit.
<b>Malware</b>	Malicious software disrupts specific components or disables a system when a user clicks a dangerous link or email attached.
<b>Metasploit</b>	A penetration testing framework that makes hacking simple. It's an essential tool for many attackers and defenders.
<b>Network Exploitation</b>	Enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary information systems or networks.
<b>Network Services</b>	In computer networking, a network service is an application running at the network application layer and above, that provides data storage, manipulation, presentation, communication or other capability which is often implemented using a client-server or peer-to-peer architecture based on application layer network protocols.
<b>Network virus</b>	A type of file less malware that moves from computer to computer without saving files on any device but going straight into the operating system.
<b>NMAP</b>	It scans the entire system and creates a map of every aspect of it as a solution to the challenge of identifying network activity.
<b>OSINT</b>	Use publicly available information, such as Google search, news media, images, and mapping, to make a decision and find web vulnerabilities.
<b>OWASP Top 10</b>	A standard awareness document for developers and web application security. It represents a broad consensus about the most critical security risks to web applications.
<b>Ransomware</b>	Access to key components of a network is blocked until ransom is paid
<b>Shells and Privilege Escalation</b>	Exploitation to gain root shell access in the target machine and perform a sudo and superuser access.
<b>Spear phishing</b>	The fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.
<b>Spyware</b>	Hackers covertly obtain information by transmitting data from the hard drive.
<b>SQL Injection</b>	Hackers insert malicious code into a server that uses SQL, forcing the server to reveal sensitive information.
<b>Steganography</b>	The act of concealing a secret message within something that is not hidden. That something can be anything you want it to be. It entails hiding a concealed piece of text within a photograph.



<b>Trojan Horse</b>	Contains unexpected, additional functionality
<b>Upload Vulnerabilities</b>	A local file upload vulnerability is a vulnerability where an application allows a user to upload a malicious file directly which is then executed. A remote file upload vulnerability is a vulnerability where an application uses user input to fetch a remote file from a site on the Internet and store it locally.
<b>Virus</b>	Attaches itself to a program and propagates copies of itself to other programs
<b>Web Fundamentals</b>	The web's fundamental technology and principles of the TCP/IP stack, HTTP, HTML/CSS, and computer languages that include the web's structure and technologies.
<b>Windows Exploitation</b>	Scanning and enumerating Windows systems to determine underlying operating system versions and services, identifying vulnerabilities, then researching and employing exploits to get access.
<b>Windows Fundamentals</b>	A window is a rectangular area on screen with a title bar and program name at the top. Each time you launch (run) a Windows application, it is displayed in its own window. You can launch several applications and keep them all open.
<b>Cybersecurity</b>	The implementation of technologies, operations and controls to protect systems, networks, programs, devices and data from cyberspace threats.
<b>Worm</b>	Propagates copies of itself through a network
<b>Zero-day exploit</b>	After a network vulnerability has been announced but before a patch or solution has been implemented, hackers seize the opportunity to initiate an attack.

## Exercise Planning

The exercise planning process determines the participants, exercise scenario, injects and the execution order for the course of the exercise. A group of exercise planners focused on the objectives, selects the best means to reach those objectives and develops a complete exercise plan.

The structure and planning of a cyber exercise are similar across organizations; however, the execution and scenarios vary depending on the participants and objectives of a specific exercise, they will apply the **KNOW-DO-LEARN** platform basis of the Cyber EX. **“Know”** knowing your targets, discover **“Do”** implement your actual outputs by doing your actual exploits, **“Learn”** is the user gained experience and counter measure on the scenarios and procedure on how to mitigate those risk. Understanding the different categories of exercises and the objectives that each fulfills greatly increases exercise realism and effectiveness. Once an organization has established exercise objectives, the exercise planners can begin to take a more detailed look at what type of exercise would match the objectives and provide an effective assessment of the organization’s program.

For the Cyber EX, this may run as a stand-alone event on an isolated network. The planning processes must ensure the exercise both achieves the cyber objectives and supports the greater exercise objectives through controlled impacts to operational networks.

Many organizations are familiar with the concept of a Capture the King “CTK,” but associate it with different purposes. Cyber Battalion created “CTK” may consist of an integration lab where users can “play” with the Platform and test how it functions in different situations. Military personnel has a marksmanship where personnel undergo safely train, maintain, and test proficiency with their guns. Similarly, a Cyber EX can provide a controlled environment in which organizations can execute cyber eXercise for eXcellence without harming a live networks systems or operations.

A Cyber EX is a controlled electronic computing environment with systems, networks, services, and users generally isolated from a live network. Such a CTK has a defined to “Seize the Throne” that could be a hash type or any form of format. Cyber EX can provide access to participants from any Territorial Battalion’s provided by the Cyber VPN.

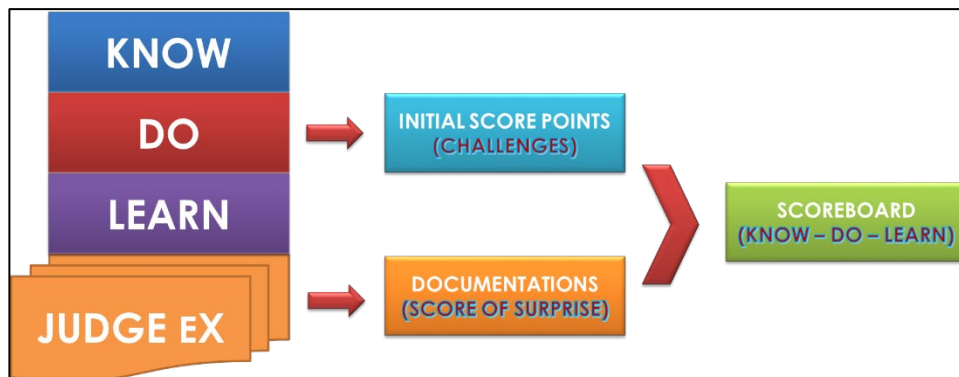


Figure 1. The “KNOW – DO – LEARN” Framework

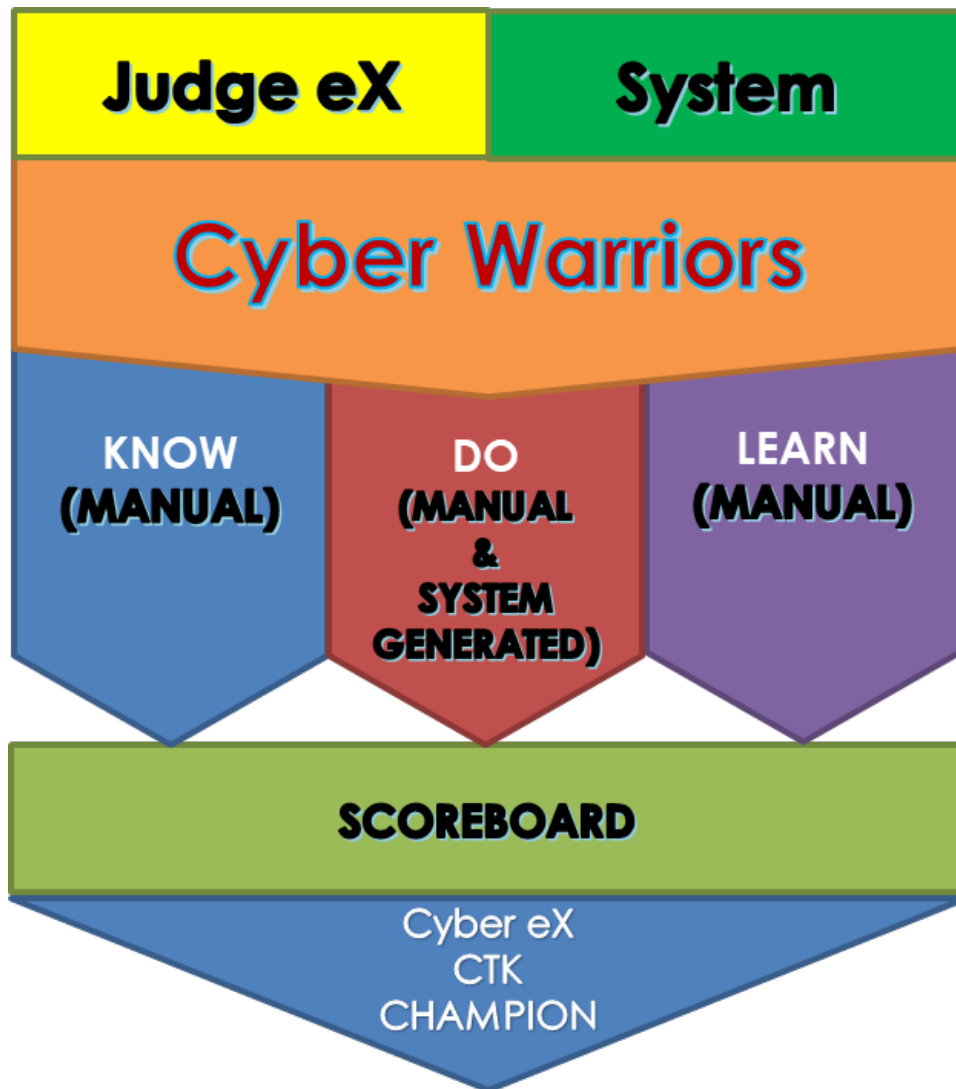


Figure 2. The "CYBER eX" Framework

## Exercise Architecture

The Cyber eX platforms consist of different systems such as VPN Servers, Live Machines (Target Machines) and the Cyber eX Server Website. CIRT participants connect using the VPN tunneling, to fully run the Cyber eX platform. Cyber eX used the combination of Layer 2 Tunnel Protocol/ Internet Protocol secure, to encrypts the connection between two or more computers. Cyber eX network has an isolated local network consists of servers that are connected in an environment. This environment provides well defined physical, network and security characteristics.

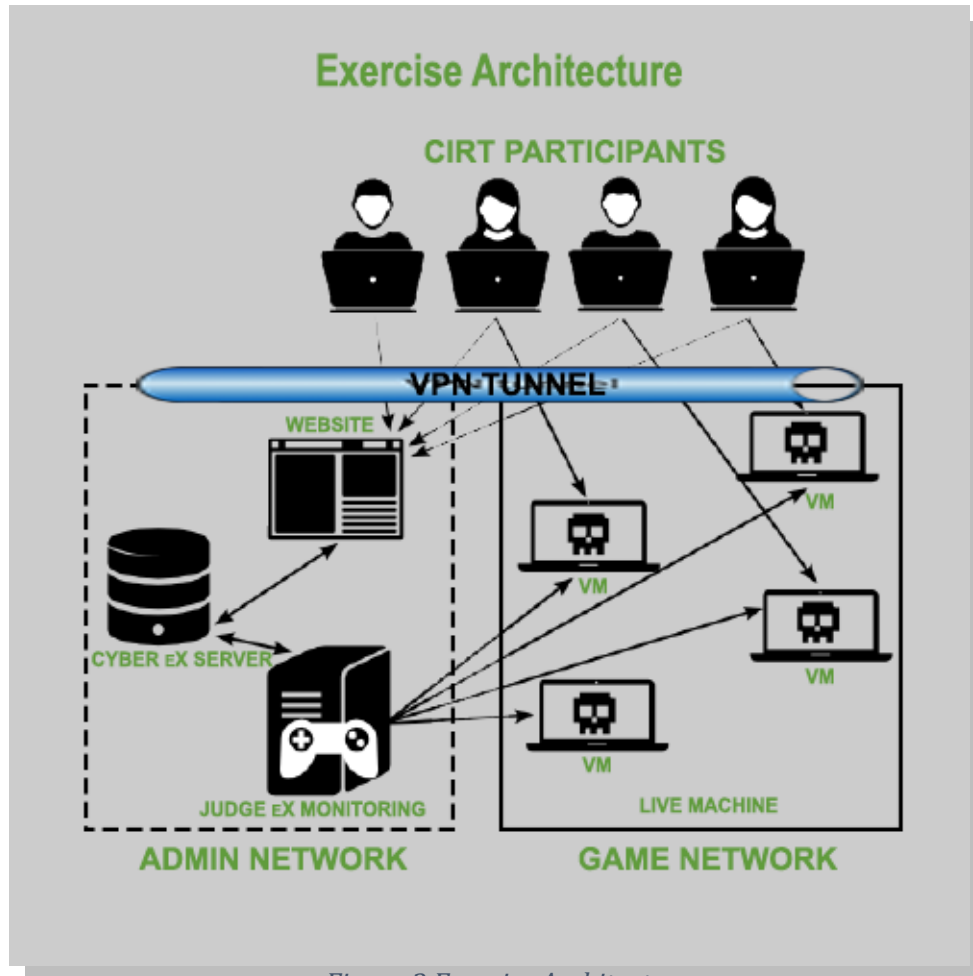


Figure 3 Exercise Architecture

## Objectives

The overarching objective of executing cyber training scenarios is to ensure that information systems and networks successfully operate in support of the exercise scenario. This provides the basis for exercise planners to begin building a cyber scenario centered on a coalition network that must be defended in order to accomplish a mission. Table 3 outlines a minimum set of objectives that planners consider throughout the lifecycle of an exercise, to include training, execution, validation, and reporting; it does not represent a comprehensive list.

*Table 3 Objectives*

ID	Objective
01	Determine the knowledge and ability of all CIRT trained personnel towards cyber incident responses
02	Assess effectiveness of the exercise's incident reporting and analysis guides for remedying deficiencies
03	Improve CIRT response to future cyber attacks in the PA Network
04	Assess ability of the personnel to detect and properly react to cyber related incidents in the PA Network
05	Assess the personnel's capability to determine operational impacts of cyber-attacks and implement proper recovery procedures for the exercise
06	Expose and correct weaknesses in cyber security systems
07	Expose and correct weaknesses in cyber operations policies and procedures
08	Determine what enhancements or capabilities are needed to protect an information system and provide for operations in a hostile environment
09	Enhance cybersecurity awareness, readiness, and coordination

## Exercise Participants

Since the Philippine Army has started adopting the cyberspace as another domain of operations, established, secured, and defended networks has just begun. Some units of the PA are mostly newbie in the field of cybersecurity and only few personnel have quite advanced cybersecurity practices and different approaches to the execution of such. This, combined with a reliance on commercial services and limited exposure to cyberspace operations, can pose a challenge to future cyber scenarios in exercises with the various nations.

For the Cyber EX, exercise customers will be all Cybersecurity Incident Response Team (CIRT) trained personnel of the Philippine Army Major Units, including Post and Territorial Signal Battalions of the Army Signal Regiment.

## Exercise Judge eX

Judge eX is a part of Cyber eX Directorates to give evaluation or make grading decision on the documentation submitted by the players. Each Judge eX has an own account that they can use to reviews and evaluate the KNOW – DO – LEARN.

Designed to provide independent grading system for the CTK player and improve responsive support in case of a cyber situation.

A systematic platform and powerful way of monitoring the player's status on the game and quick response.

**Cyber Exercise for Excellence is composed of three Documentation to be evaluate by Judge eX:**

**Knowledge Well (KNOW)** – This part of the challenge is where the players inputs Links, Video and any other references that they strategized as necessary during the duration of the CTK.

**Chronicles (DO)** – This is where the actual results of the exploits from the challenge are laid down. More of, added also on this part are the screenshots that were found during the steps done by players during the challenge.

**Counter Measure (LEARN)** – This is where all the user gained experiences, comments and counter measure on the scenarios and procedure on how to mitigate those risk for improvement suggestions are emphasized. This mainstream can serve as basis for more futuristic and for more modern technology designs raised for the system. Understanding the different categories of exercises and the objectives that each fulfills greatly increases exercise realism and effectiveness.

## Categories of Cyber Exercises

Cyber exercises take different forms. For Cyber EX, there will be three categories in which exercise customers need to engage. Table 5 summarizes some characteristics of different exercise categories and their usage.

*Table 4. Exercise Structures*

Category	Description	Complexity
<b>Apprentice</b>	This category is composed of the most basic and common exercise scenarios in Cybersecurity in the Philippine Army and relatively beginner friendly.	This type of exercise can be planned and executed quickly, depending on the number of challenges involved.
<b>Warrior</b>	Participant understands the concept, can correctly recognize the given concept of exercise, can weigh it and related concepts as solutions to some problem and can apply each of them correctly.	This type of exercise requires more planning and longer execution times.
<b>Conqueror</b>	An extremely high number of difficulties, most of the exercise relatively above expert level.	This type of exercise requires detailed coordination and planning.

Ideally, as PA matures, it will progress through the different exercise structures in a “crawl, walk, run” fashion. This approach allows PAMU’s to step their way from beginner category up to the advanced category. As with most new processes, planners must absorb lessons and must clearly write out sub-processes to make improvements and design meaningful and successful challenges.

# User Manual

Navigate to "Register Page" to create a Player Account.

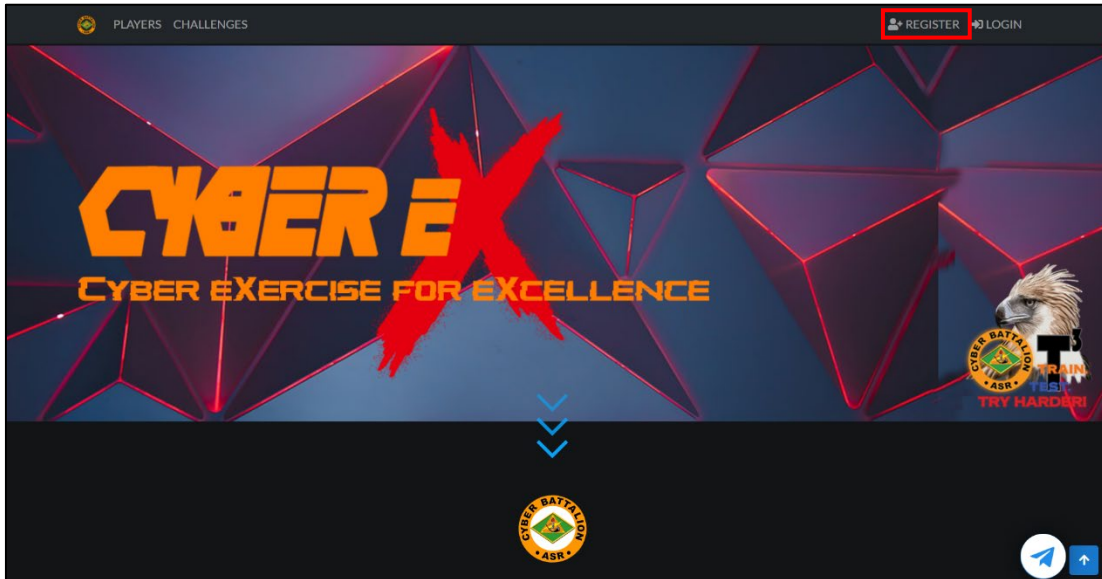


Figure 4 Register Page

Fill up all required information and click "Submit" to Register.

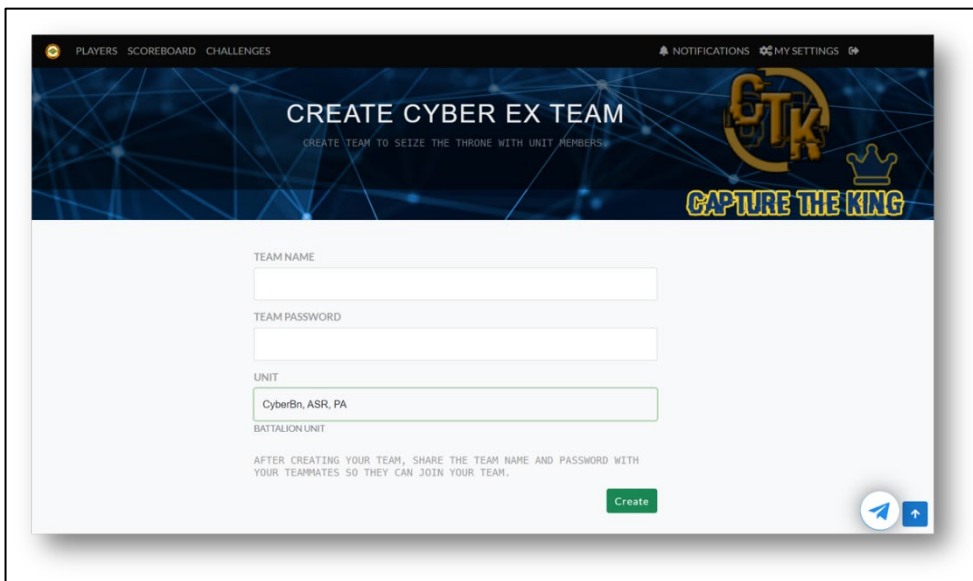


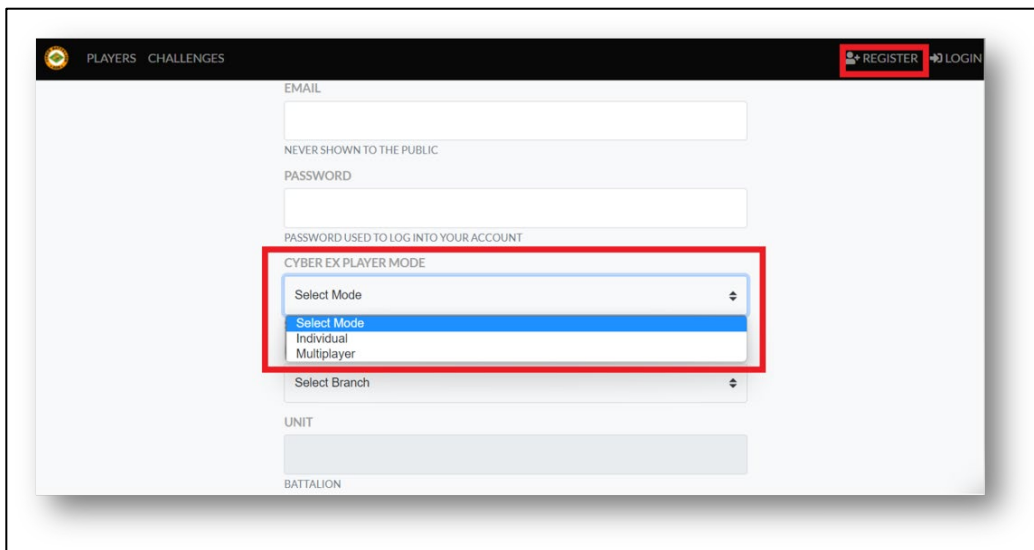
Figure 5 Register (Fill up page)

Fill up the required field in the form.



- i. **Username**
- ii. **Email**
- iii. **Password**
- iv. **Cyber EX Player Mode**
- v. **Major Unit**
- vi. **Battalion**
- vii. **Unit**

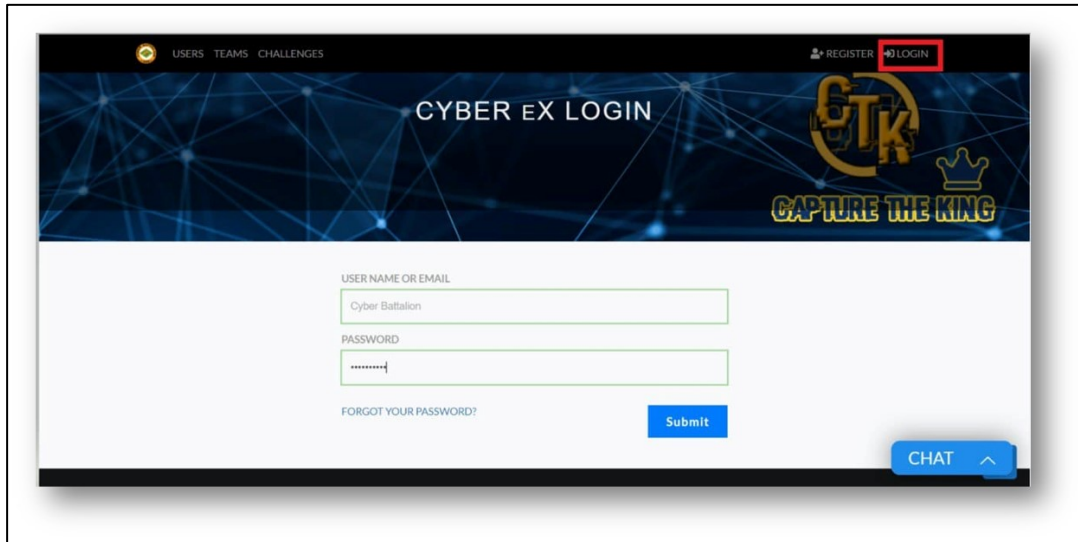
**Note: Remember your Team Name and Password as you share to your Team Mates to Join to your Team.**

A screenshot of a web registration form. The form is titled 'REGISTER' and 'LOGIN' in the top right corner. It contains several input fields: 'EMAIL', 'NEVER SHOWN TO THE PUBLIC', 'PASSWORD', 'PASSWORD USED TO LOG INTO YOUR ACCOUNT', 'CYBER EX PLAYER MODE', 'Select Branch', 'UNIT', and 'BATTALION'. The 'CYBER EX PLAYER MODE' dropdown menu is highlighted with a red box, showing options: 'Select Mode', 'Individual', and 'Multiplayer'. The 'Individual' option is currently selected.

*Figure 6 Register (Fill up page)*

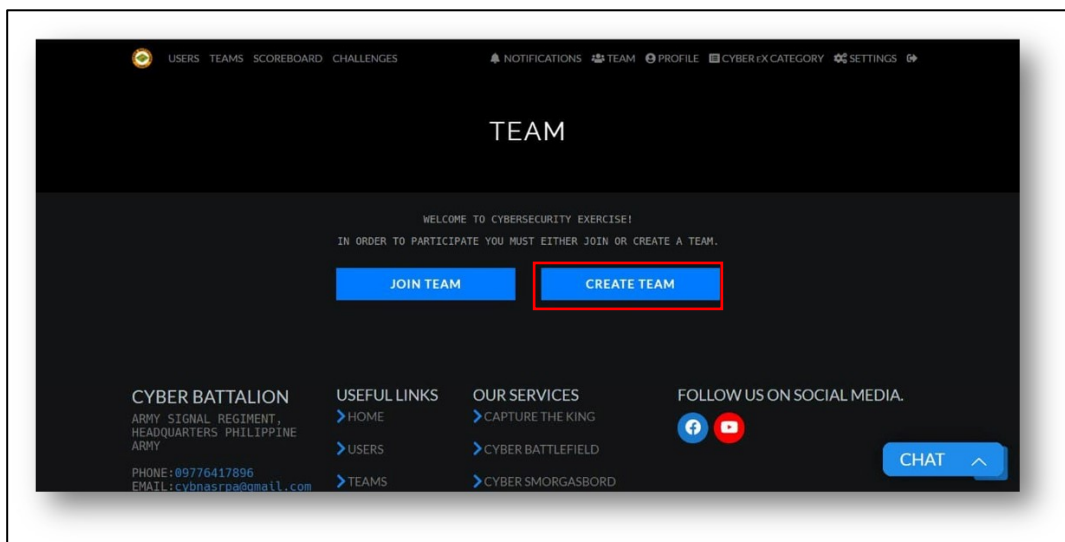
Individual or Multiplayer mode selector at **Register** page.

**Login to your account by navigating to "Login" Page.**



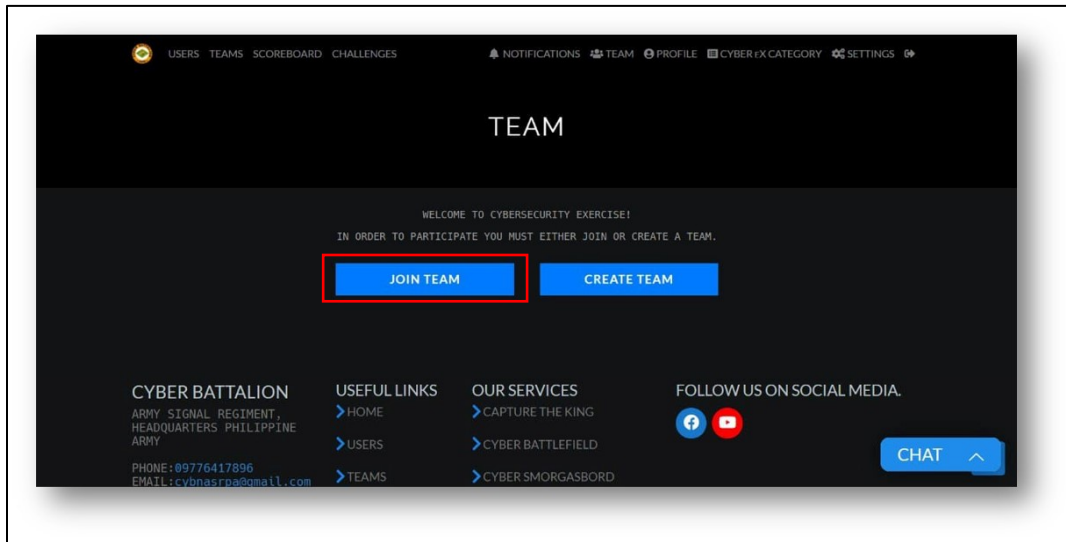
*Figure 7 Login Page*

**Create a Team for those who doesn't have an existing Team Account. To create, click "Create Team"**



*Figure 8 Create Team*

**To join the Team, Choose the "Join Team" and provide you Team Name and Password.**



*Figure 9 Join Team*

The Cyber EX category Composed of 3 major Categories which is the Apprentice, Warrior and Conqueror. Apprentice is automatically unlocked to proceed for the Challenges. Warrior will be unlocked after Apprentice is captured by the players for minimum of 70% and Conqueror will unlock if Warrior Reached 60% solved by Team Players.

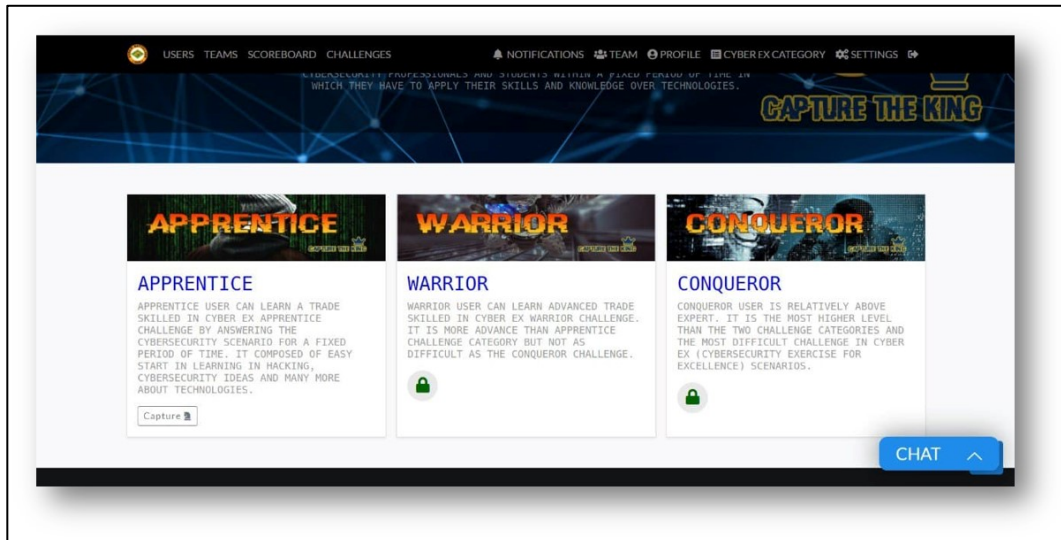


Figure 10 Categories

Click the "Capture" button to proceed.

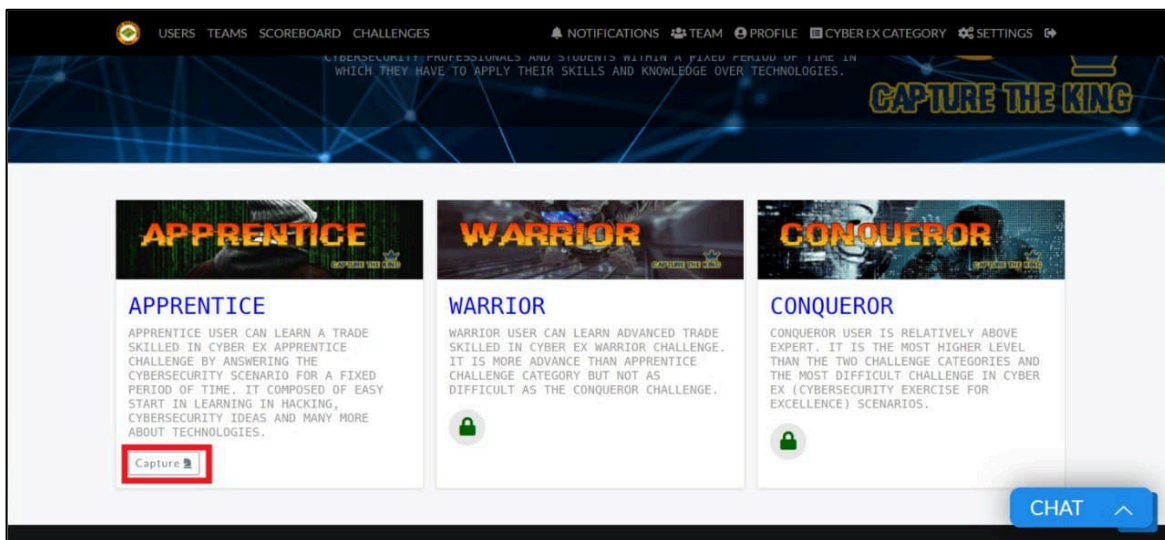


Figure 11 Capture (button to proceed)

Challenges are sorted out by Challenge Categories. Click a category to display the list of challenges.

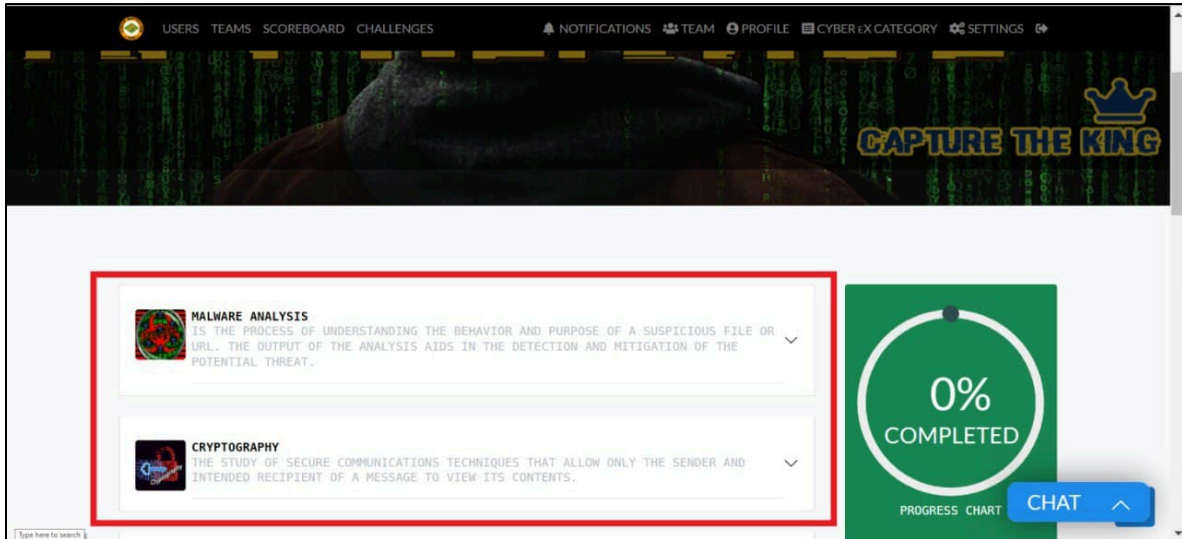


Figure 12 Challenge scenarios

To view the challenge to-do list and description, click the challenge to toggle down the list.

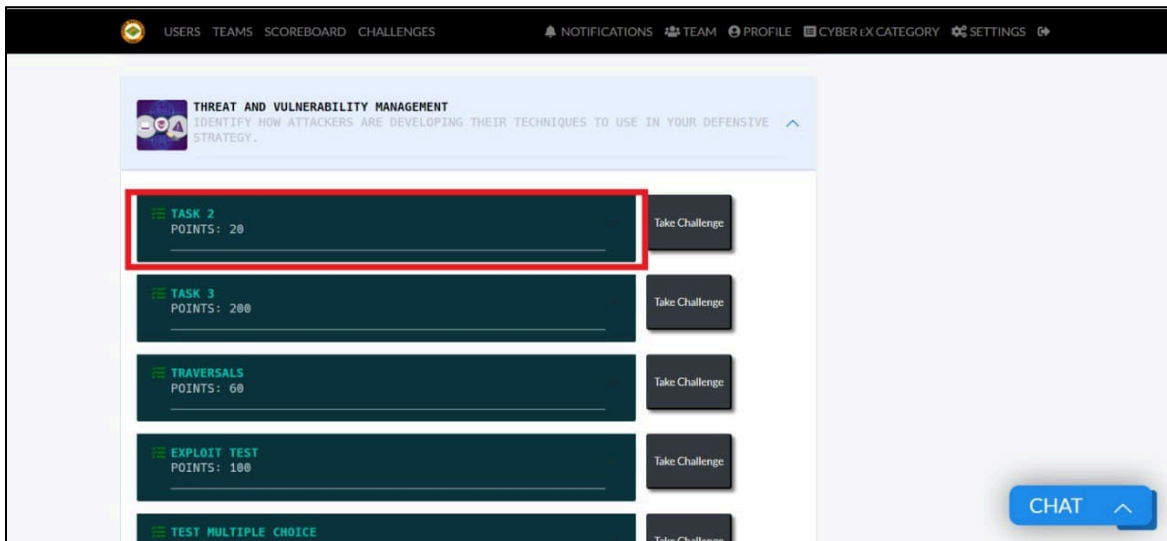


Figure 13 Challenge (Do List)

View the challenge description and Instructions and Click "Take Challenge" button to Seize the Throne.

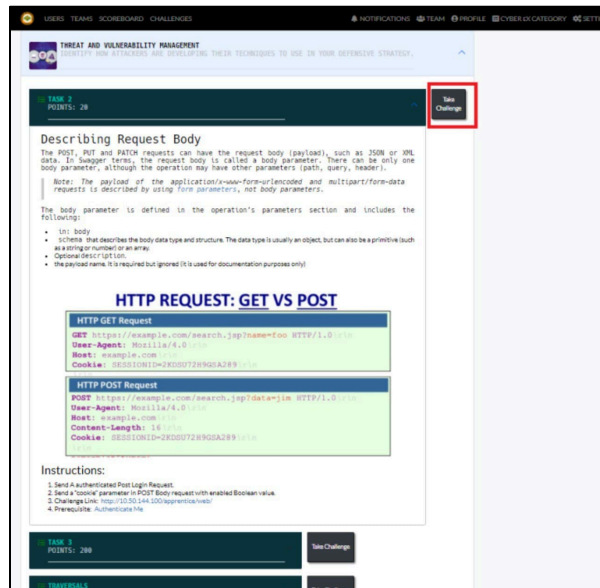


Figure 14 Take Challenge

Navigate to "Download Files" to Download required Files to Take the Challenge.

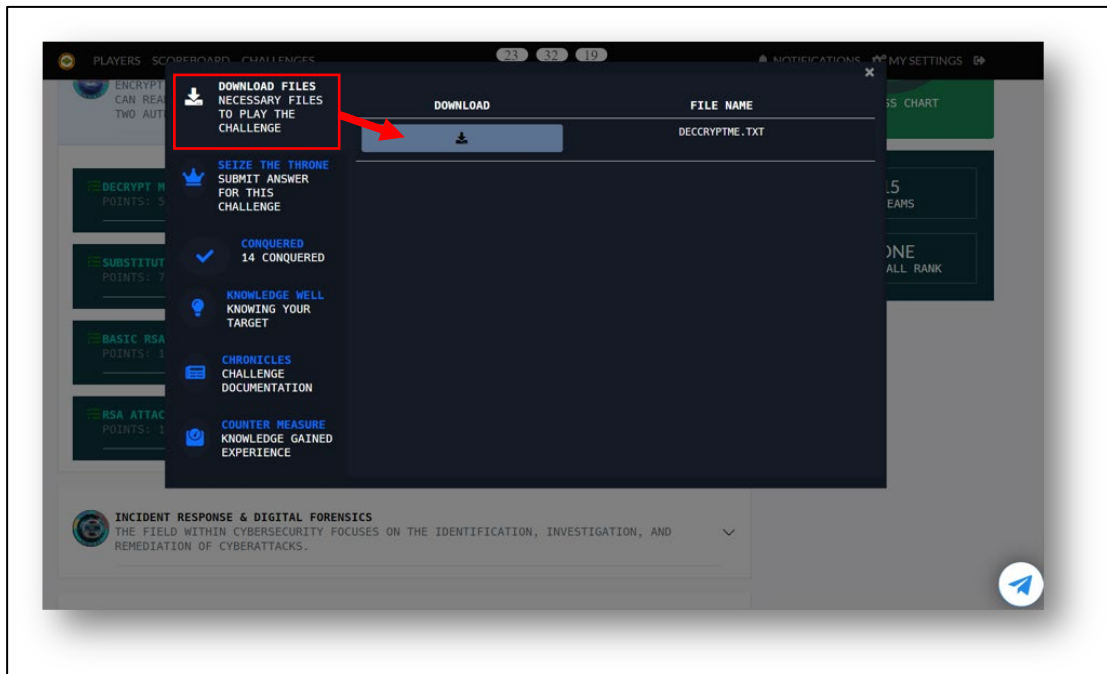


Figure 15 Download files

After the Team solves the problem and captured. The Hash is required to the challenge.

Input the Hash to "Hash Submission" text field. Be aware to Attempts indicator as will limit the hash submission per teams.

The "Hints" Button will help to Seize the Throne but will accumulate minus points from your team.

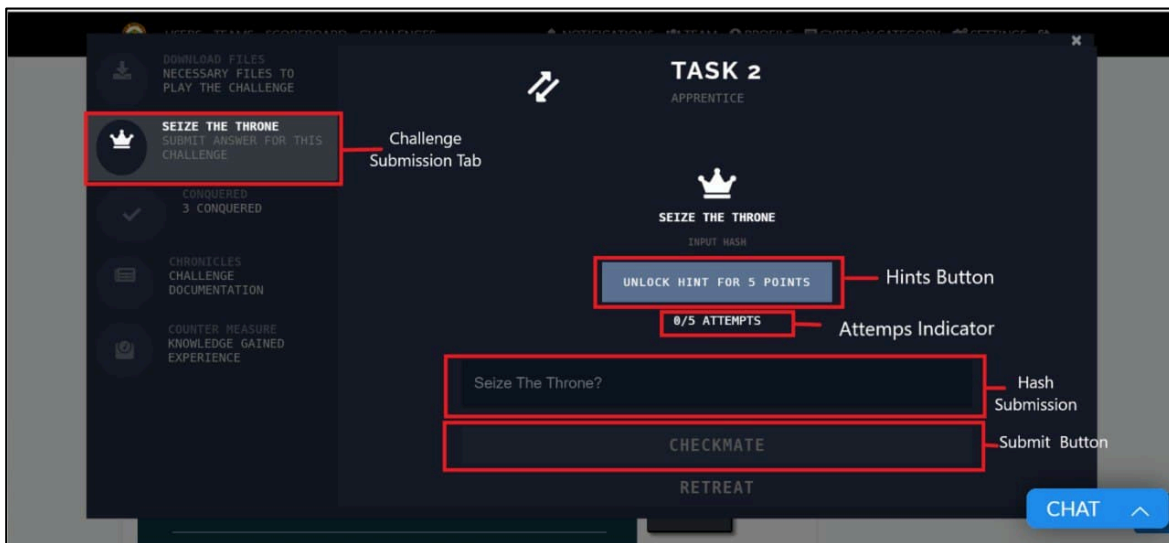


Figure 16 Seize The Throne (Hash format)

The challenge consists of questions with Multiple-Choice answers which accept one submission attempt only. Click the radio button to select your best answer.

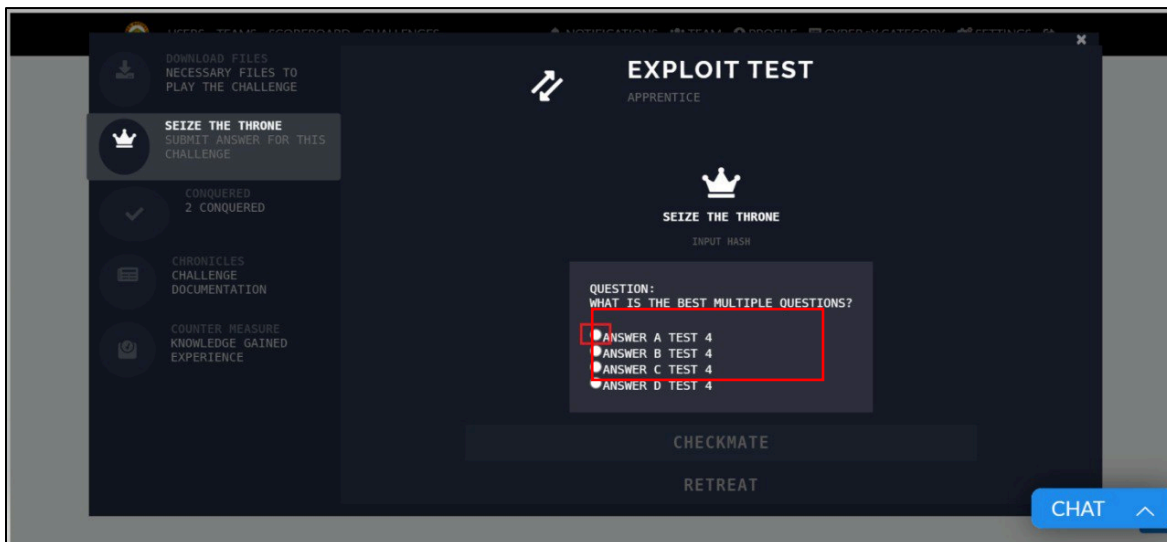


Figure 17 Seize The Throne (Multiple choice)

Navigate to “Conquered” tab to view the list of Team Players who already solved the challenge.

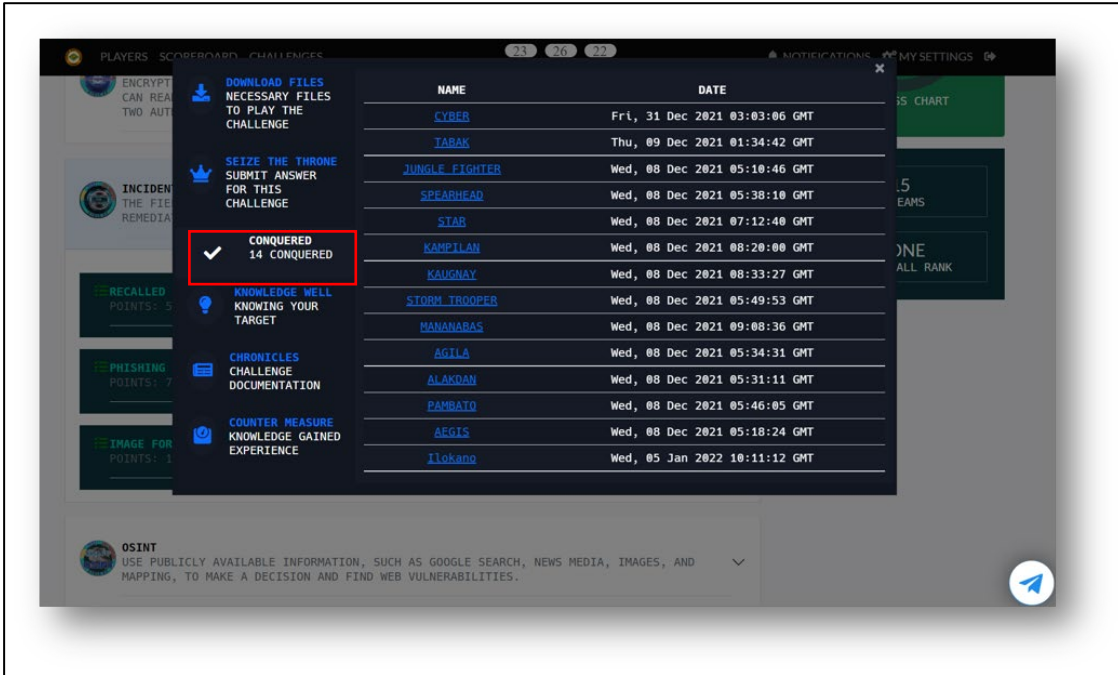


Figure 18 Conquered (Preview)

Navigate to “Knowledge Well” tab submit documentation. This will indicate the references and the links on how the Teams know the target challenge.

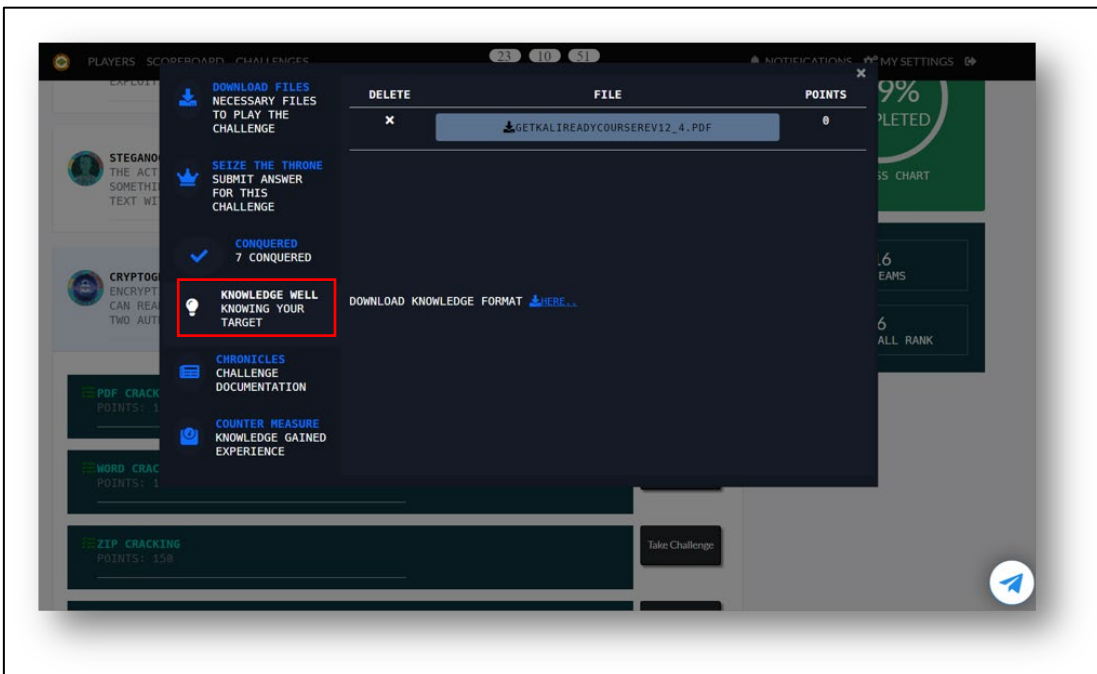


Figure 19 Knowledge Well



Navigate to the “Chronicles” tab to submit documentation. This will show steps on how the Teams solved the challenge.

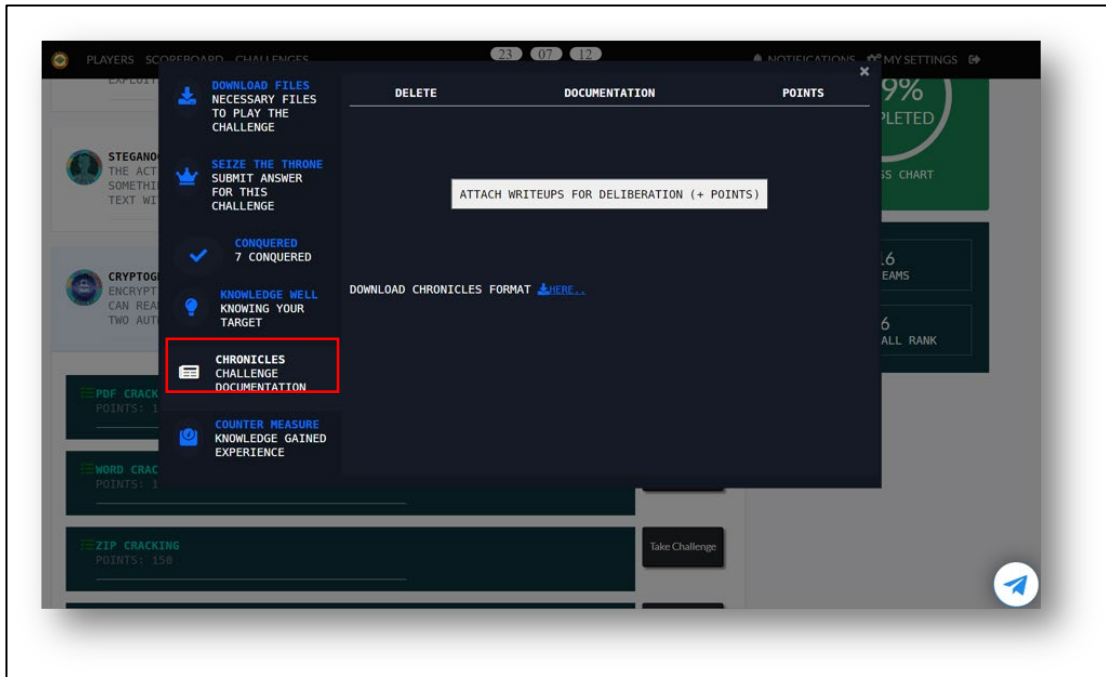


Figure 20 Chronicles

To upload your file, drag your file or click the “Drag files area” to browse from your folder, which is specified from your documentation.

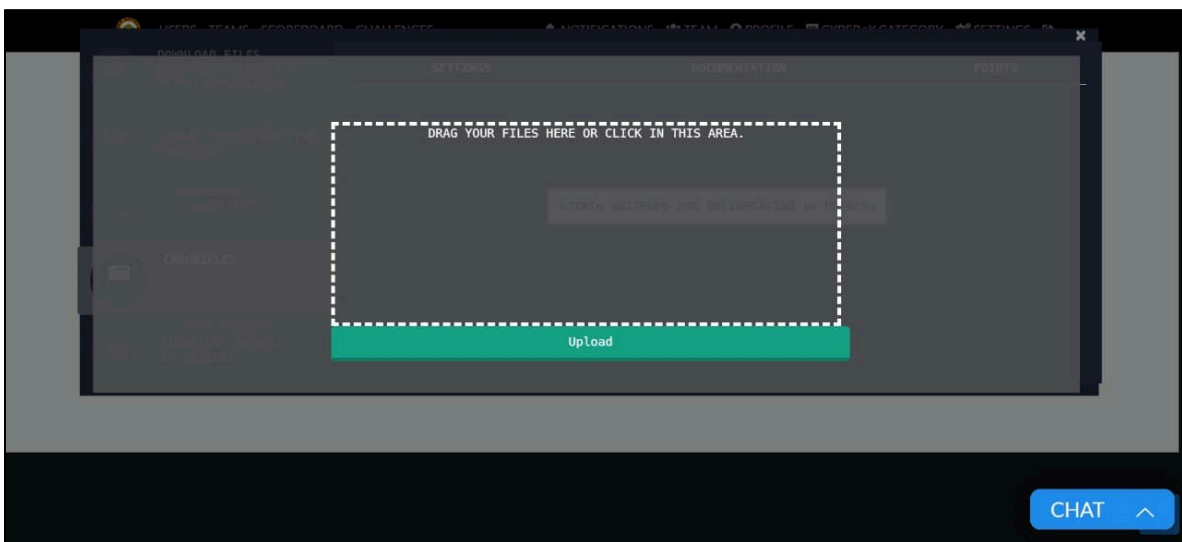


Figure 21 Upload Files (PDF format)

After browsing click the "Upload" button and will wait for the Judge EX to Check the Submitted documentation.

Additional Points will be given and will automatically add to your challenge points.

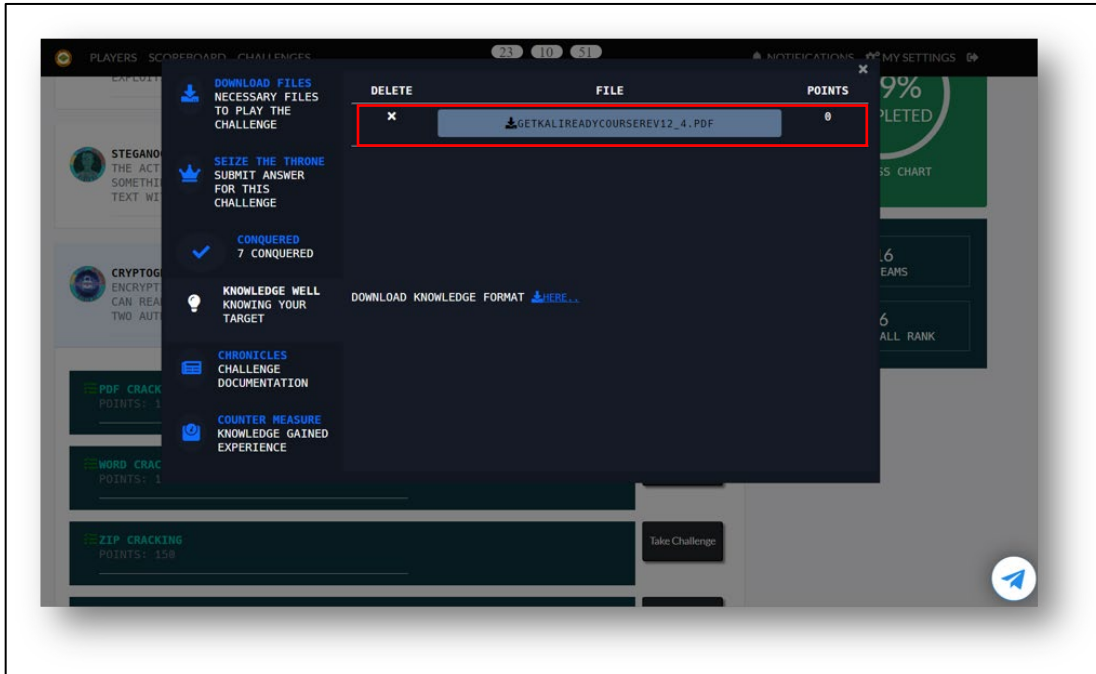


Figure 22 Uploaded Files (Additional Points)

Navigate to the "Counter Measure" tab to upload documentation for your challenge gain experience with how the team solved the problems.

Counter Measure shows the best practices on solving the challenge.

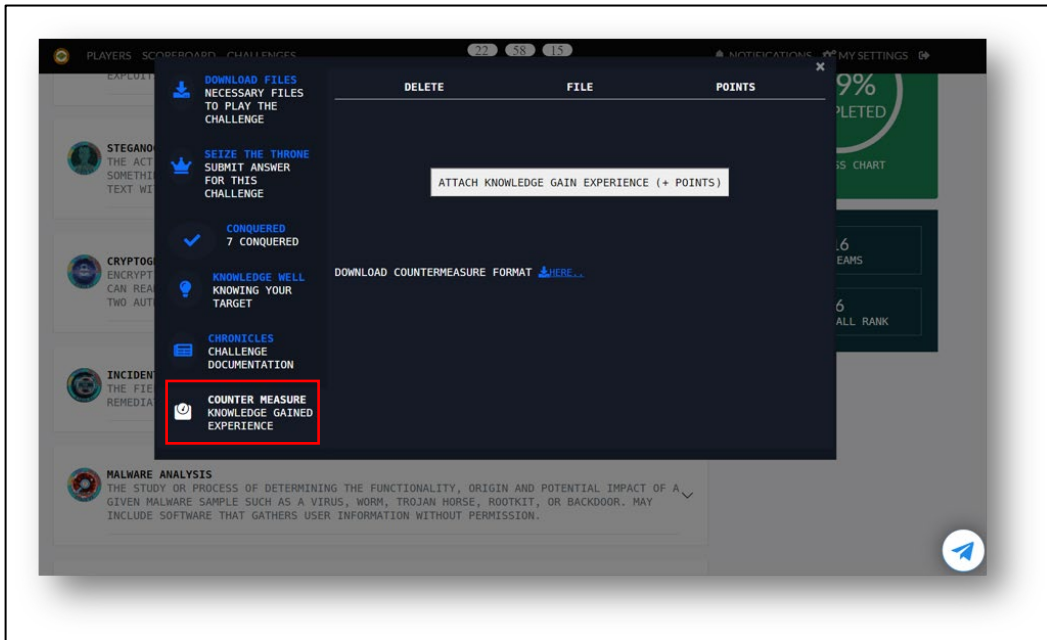


Figure 23 Counter Measure

The Challenge page consists of Progress Bar which indicates the team solved progress and a Teams indicator that displays the total teams registered in the Cyber EX platform and the Current Team Ranking.

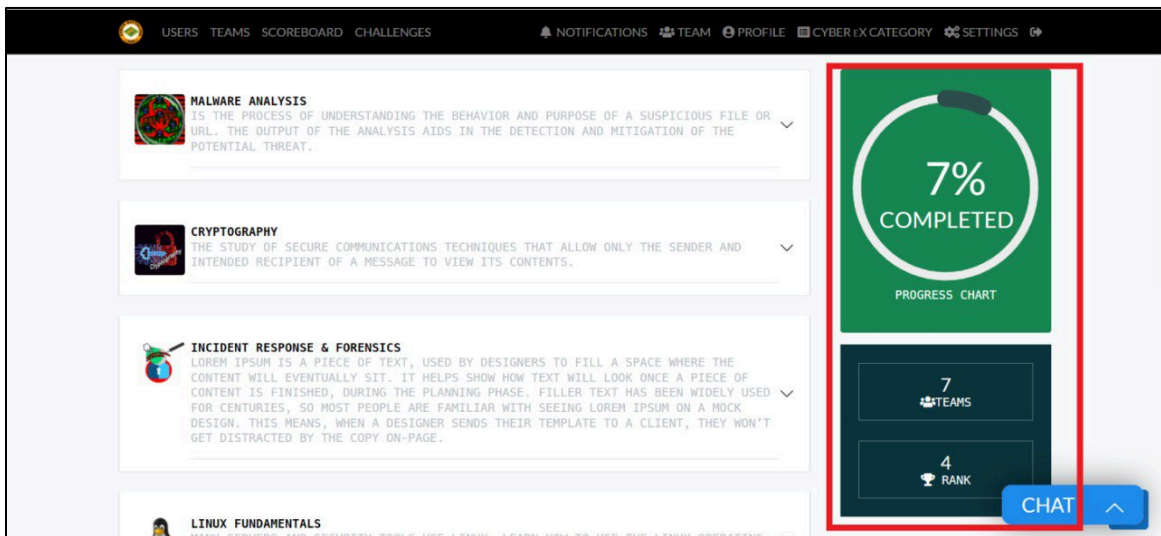


Figure 24 Progress Bar

To check the team’s scoreboard, navigate to the “Scoreboard” menu.

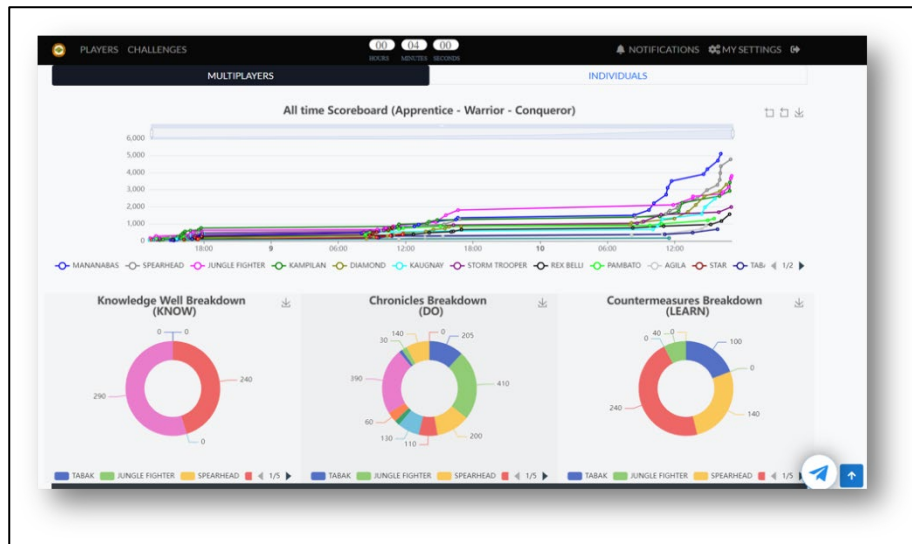


Figure 25 Multiplayer Scoreboard

Navigate to the “Landing” page to check Chronicle’s total Accumulated points per team.

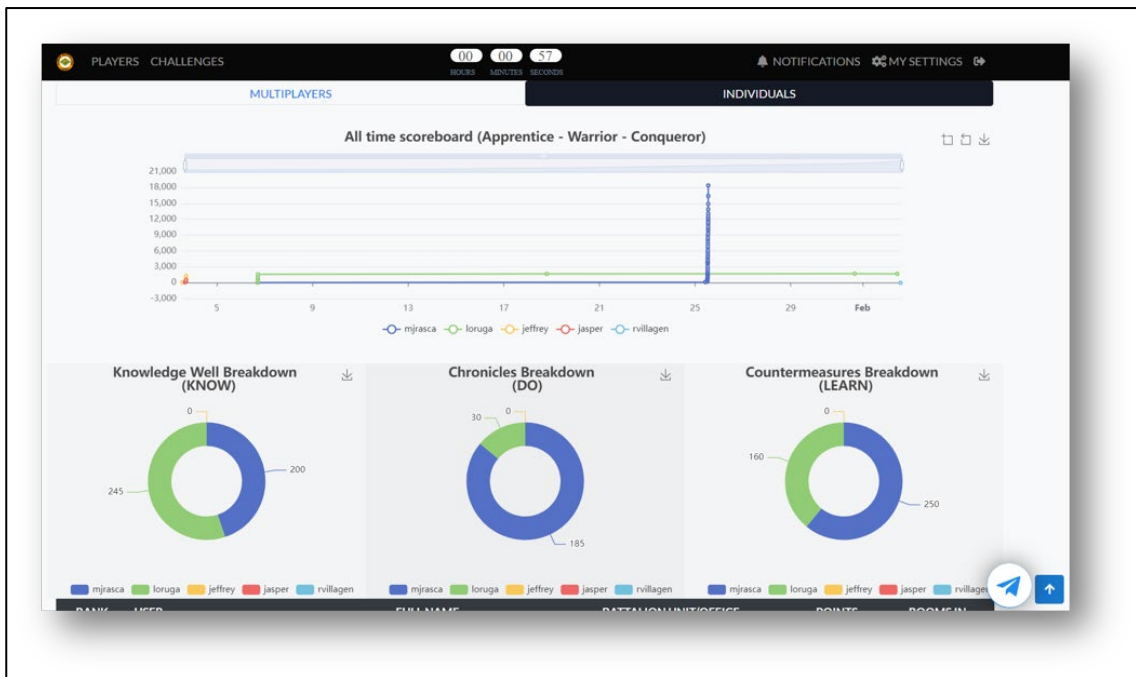


Figure 26 Individual Scoreboard

Navigate to the “Teams” menu to check teams’ composition.

Click the “team link” to check the scoreboard summary per team.

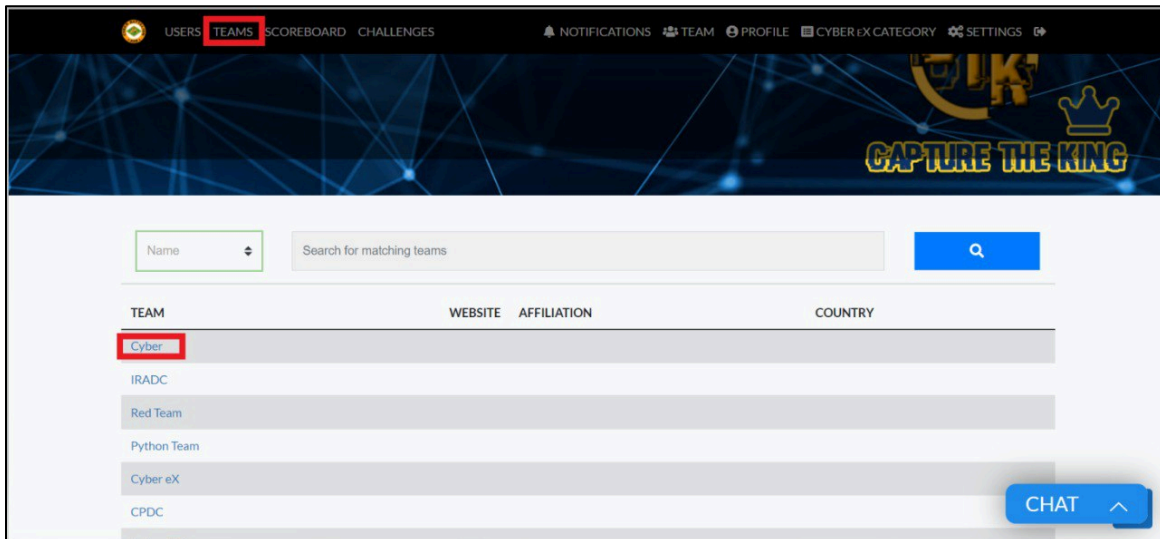


Figure 27 Participant Team

Select from the “filter section” to display the sort summary from Apprentice, Warrior, and Conqueror

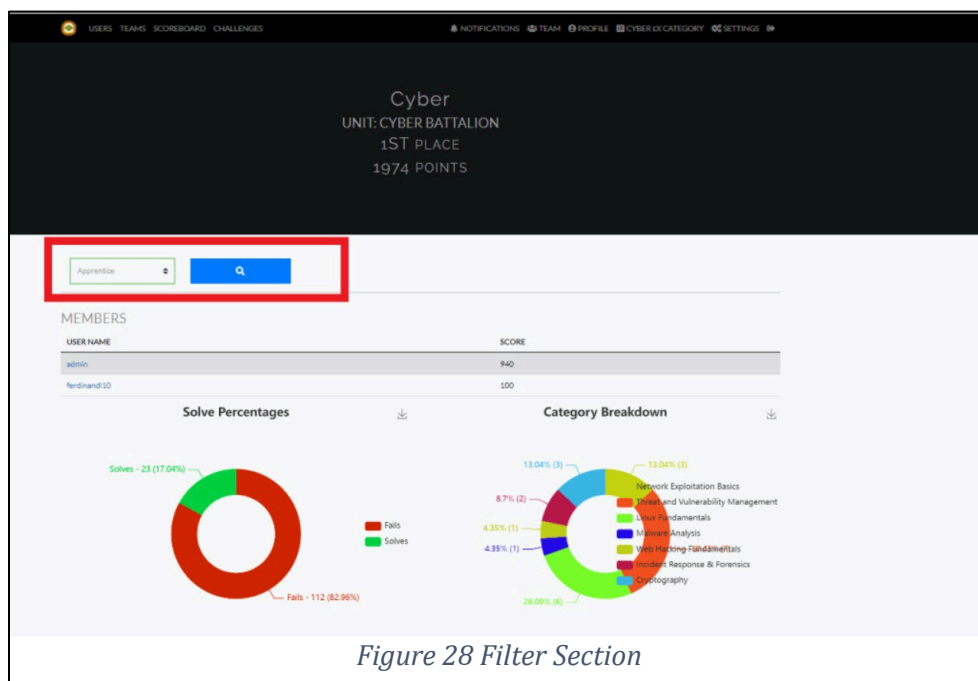


Figure 28 Filter Section

To check updated system and challenges updates and announcements, just navigate to the “Notifications” page.

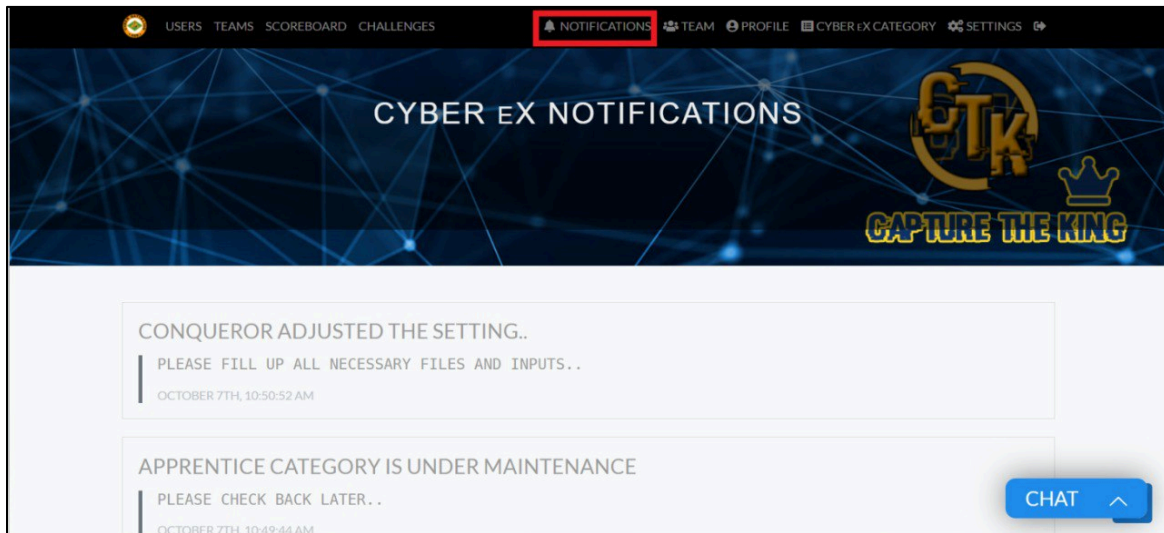
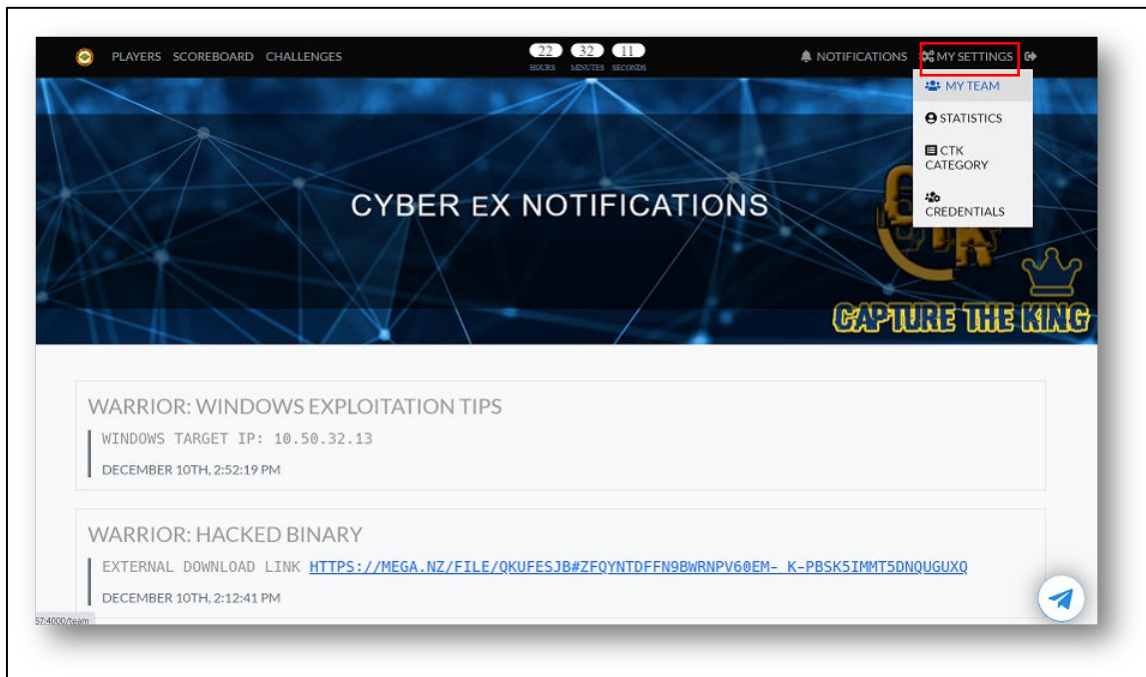


Figure 29 Notification

To check your team scoring and setting up Team Captain and awards given, navigate to the “Team” menu and “Profile” to update your profile.



To switch between Cyber EX Challenge Categories, navigate to the "My Settings" menu and click the "CTK" button.

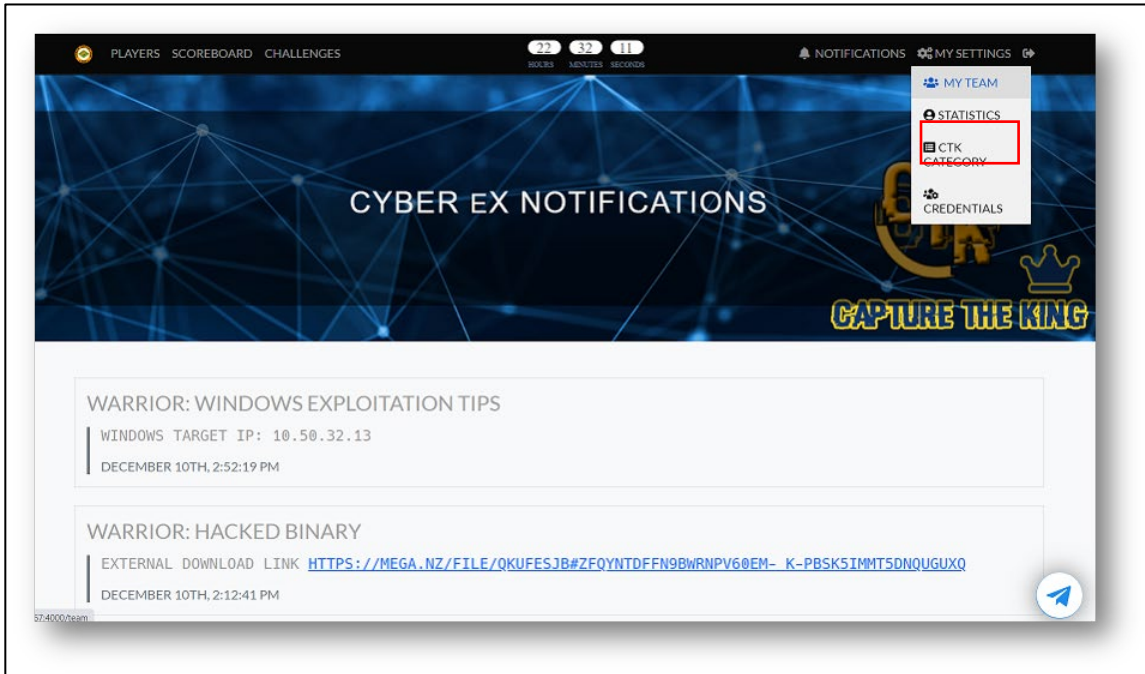


Figure 30 CTK Category (Change)

To read the Cyber EX Articles, explore to “Home” page and choose the preferred article.

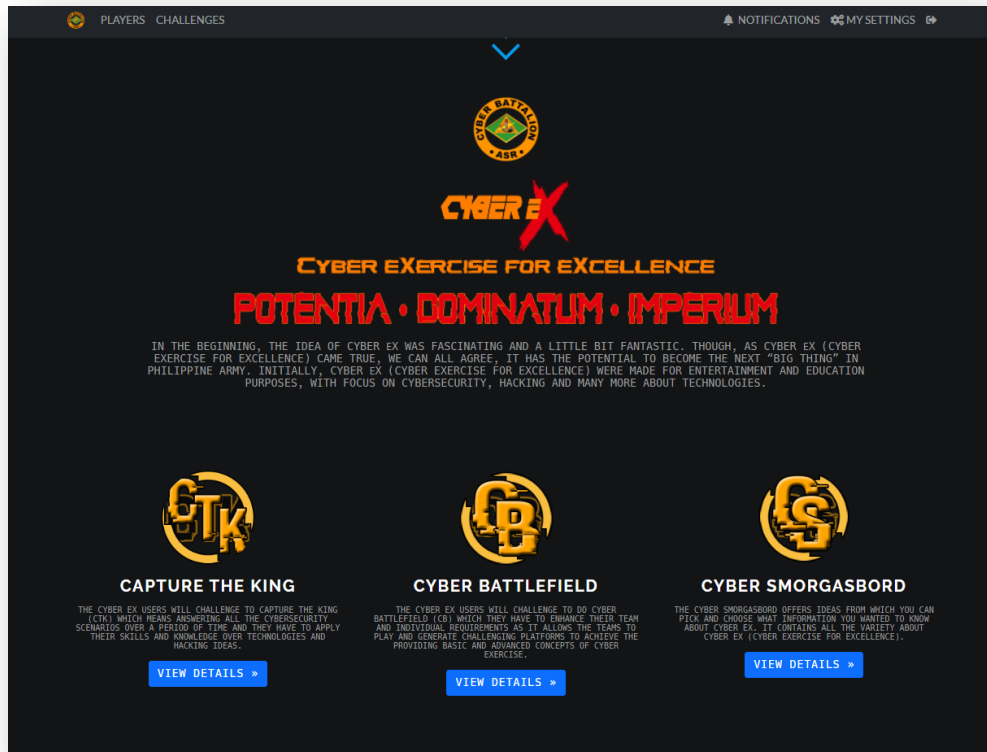


Figure 31 Cyber eX Articles

For any system concerns and experienced errors from challenges, click the “Telegram icon” floating button

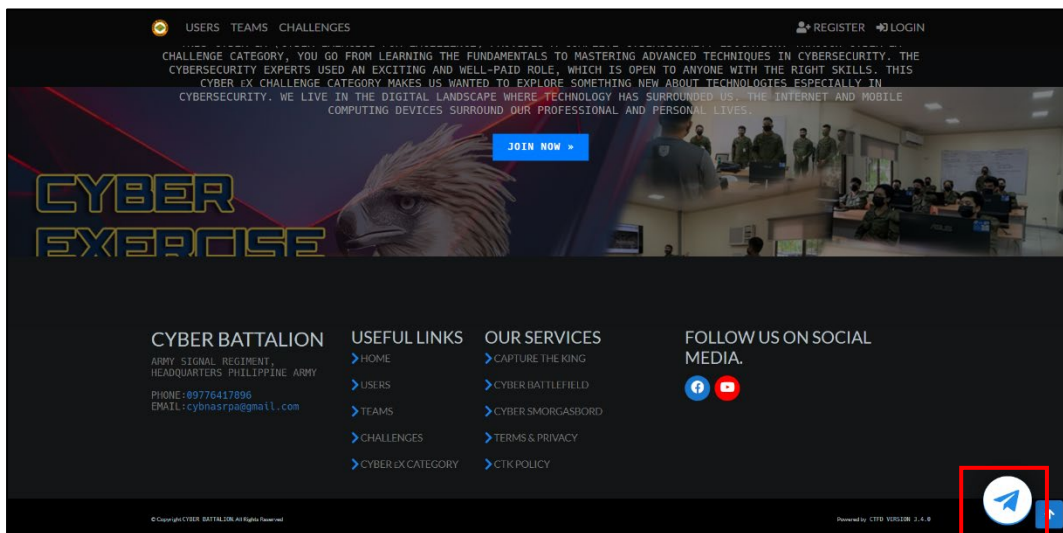


Figure 32 Chat Support



Use the Cyber EX Chat Support system for real-time assistance.

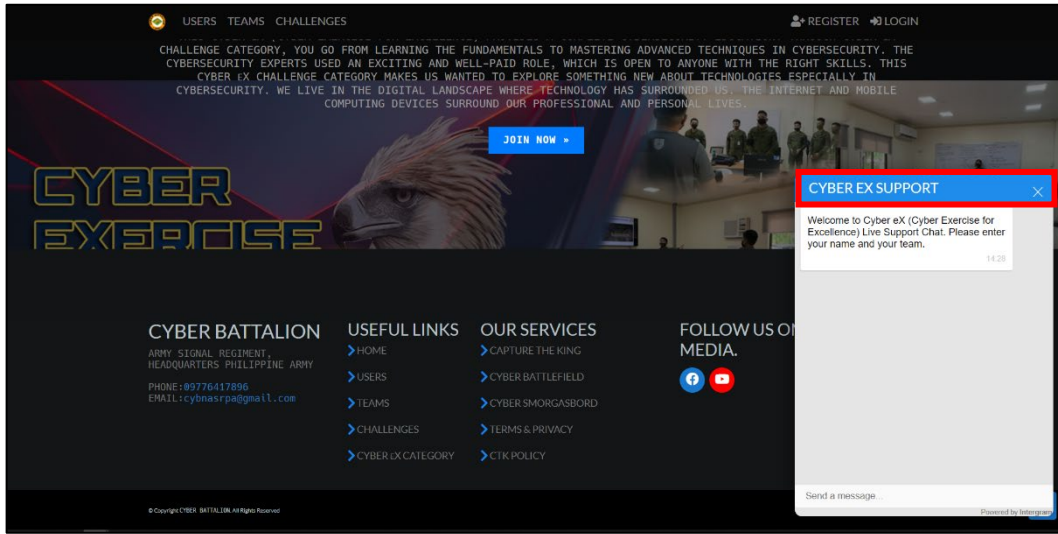


Figure 33 Cyber eX Support System

JUDGE eX MODULE

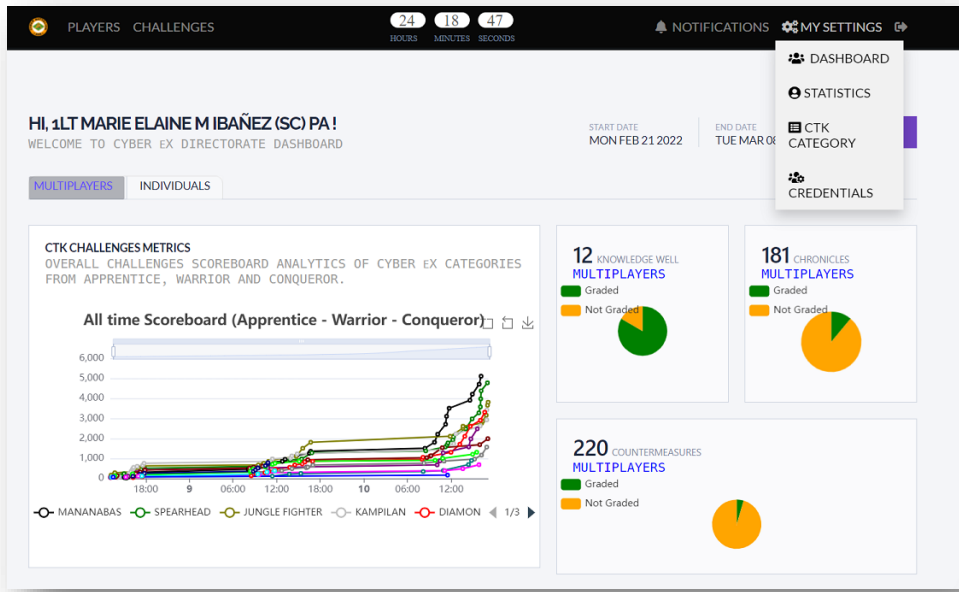


Figure 34. Judge eX DASHBOARD

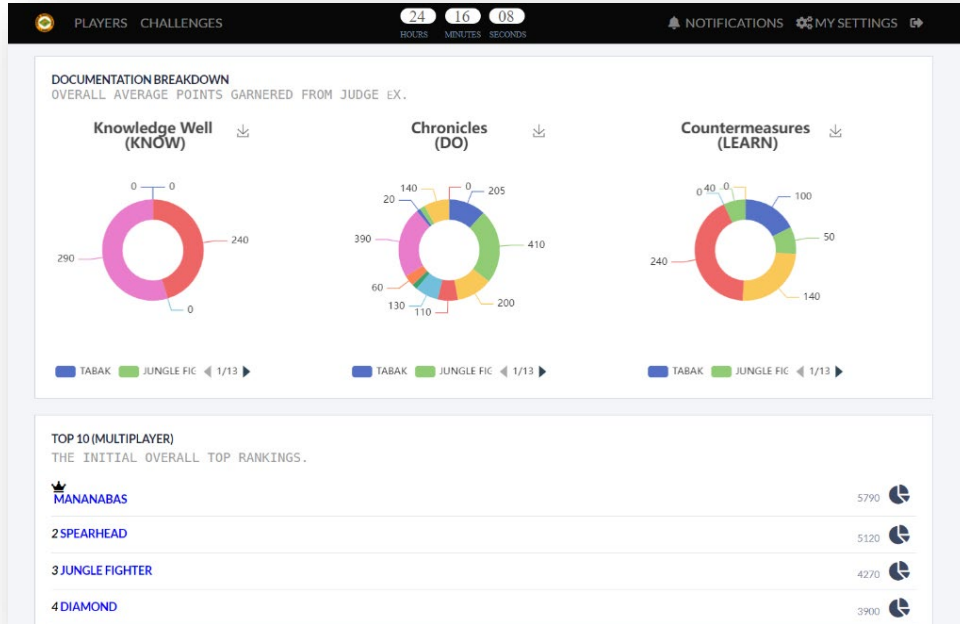


Figure 35. Judge eX DASHBOARD 1

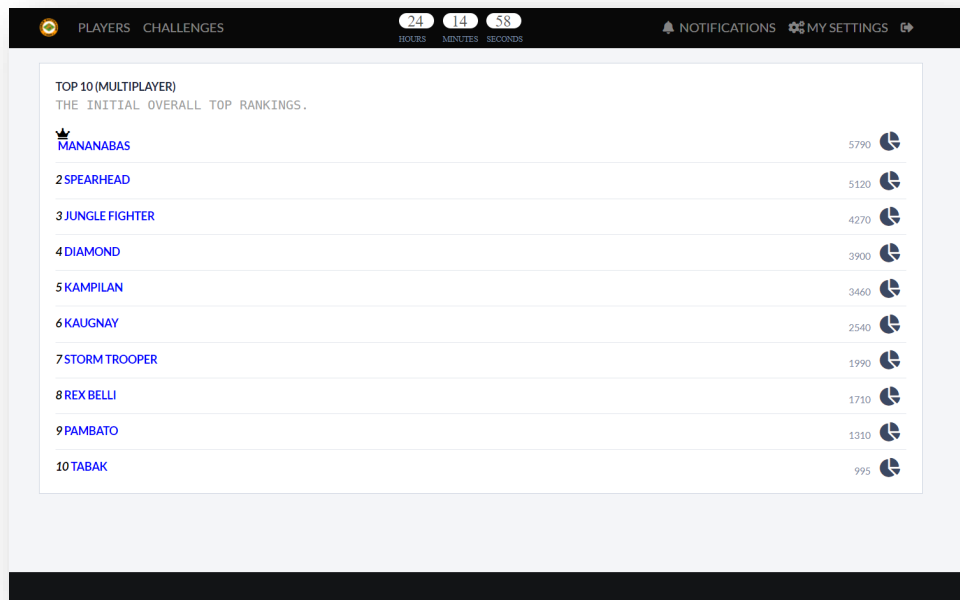


Figure 36. Judge eX DASHBOARD 2

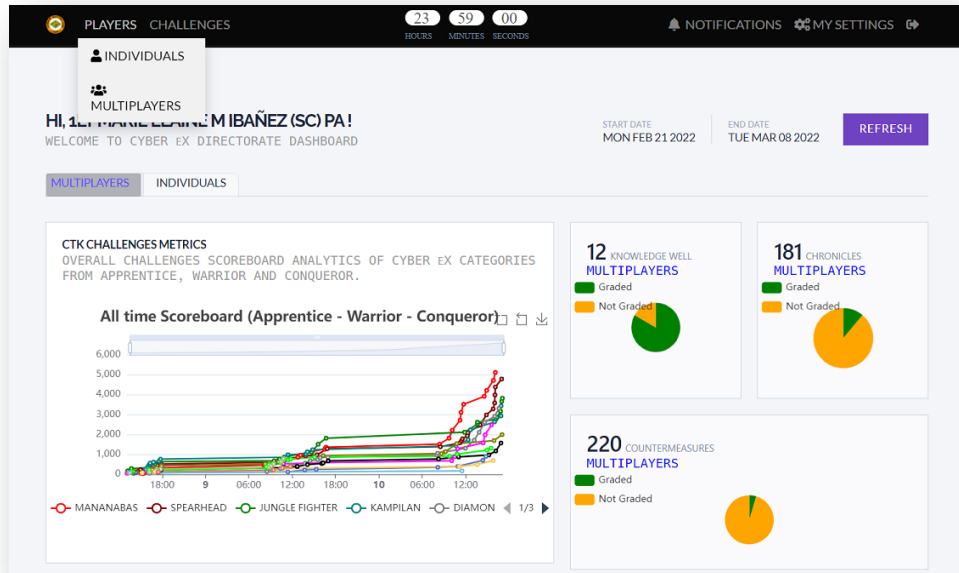


Figure 37. Judge eX PLAYERS mode

USER	FULL NAME	BATTALION UNIT/OFFICE	KNOW	DO	LEARN	COUNTRY
<a href="#">jeffrey</a>	JEFFREY P LAZARTE	CYBER BATTALION	0/0	0/0	0/0	
<a href="#">jasnct</a>	JASPER JOHN TALINTING	CYBER BATTALION	0/0	0/0	0/0	
<a href="#">mirasca</a>	MARK JEROME U RASCA	CYBER BATTALION	3/3	4/4	5/5	
<a href="#">loruga</a>	LOUIE ORUGA	2ND SIGNAL BATTALION	3/4	1/2	0/2	
<a href="#">mina</a>	PVT AARON JONES C MINA (INF) PA	CYBERBN, ASR, PA	0/0	0/0	0/0	
<a href="#">villagen</a>	RYAN VILLAGEN	45INFBN, 1BCT, PA	0/0	0/0	0/0	
<a href="#">eresse</a>	GLADYS KRISTINE O ERESE	1MIBN, AD, PA	0/0	0/0	0/0	

Figure 38. Judge eX MONITORING INDIVIDUAL

TEAM	BATTALION UNIT/OFFICE	KNOW	DO	LEARN	COUNTRY
<a href="#">TABAK</a>	15BN, ASR, PA	0/0	4/6	2/14	PH PHILIPPINES
<a href="#">JUNGLE FIGHTER</a>	25BN, ASR, PA	0/0	5/17	1/57	PH PHILIPPINES
<a href="#">SPEARHEAD</a>	35BN, ASR, PA	0/0	0/19	2/23	PH PHILIPPINES
<a href="#">DIAMOND</a>	45BN, ASR, PA	5/6	2/32	5/54	PH PHILIPPINES
<a href="#">STAR</a>	55BN, ASR, PA	0/0	3/8	0/14	PH PHILIPPINES
<a href="#">KAMPILAN</a>	65BN, ASR, PA	0/0	0/19	0/33	PH PHILIPPINES
<a href="#">KAUGNAY</a>	75BN, ASR, PA	0/0	0/4	0/0	PH PHILIPPINES
<a href="#">STORM TROOPER</a>	85BN, ASR, PA	0/0	0/16	0/4	PH PHILIPPINES
<a href="#">MANANABAS</a>	95BN, ASR, PA	5/6	6/18	0/0	PH PHILIPPINES
<a href="#">AGILA</a>	105BN, ASR, PA	0/0	0/8	0/0	PH PHILIPPINES
<a href="#">ALAKDAN</a>	115BN, ASR, PA	0/0	0/8	0/2	PH PHILIPPINES
<a href="#">REX BELLI</a>	OG6, AAR, PA	0/0	0/14	0/0	PH PHILIPPINES
<a href="#">PAMBATO</a>	ARMOR	0/0	0/0	0/0	PH PHILIPPINES
<a href="#">AEGIS</a>	OG6, 1BCT, PA	0/0	0/12	0/19	PH PHILIPPINES
<a href="#">ARMY</a>	CYBERBN, ASR, PA	0/0	0/0	0/0	PH PHILIPPINES

Figure 39. Judge eX MONITORING TEAMS

KNOWLEDGE WELL

NO KNOWLEDGE WELL SUBMITTED YET

CHRONICLES

CHALLENGE	CATEGORY	SCORE	VIEW	MORE INFO
<a href="#">DECRYPT ME</a>	CRYPTOGRAPHY	0		
<a href="#">DECRYPT ME</a>	CRYPTOGRAPHY	0		
<a href="#">PHISHING 101</a>	INCIDENT RESPONSE & DIGITAL FORENSICS	0		
<a href="#">PHISHING 101</a>	INCIDENT RESPONSE & DIGITAL FORENSICS	0		
<a href="#">REQUEST TIER 1</a>	WEB FUNDAMENTALS	0		
<a href="#">IMAGE FORENSICS 101</a>	INCIDENT RESPONSE & DIGITAL FORENSICS	0		
<a href="#">SUBSTITUTE ME</a>	CRYPTOGRAPHY	0		
<a href="#">BASIC P&amp;A</a>	CRYPTOGRAPHY	0		

Figure 40. Figure 39. Judge eX - Score / View Document / Rate

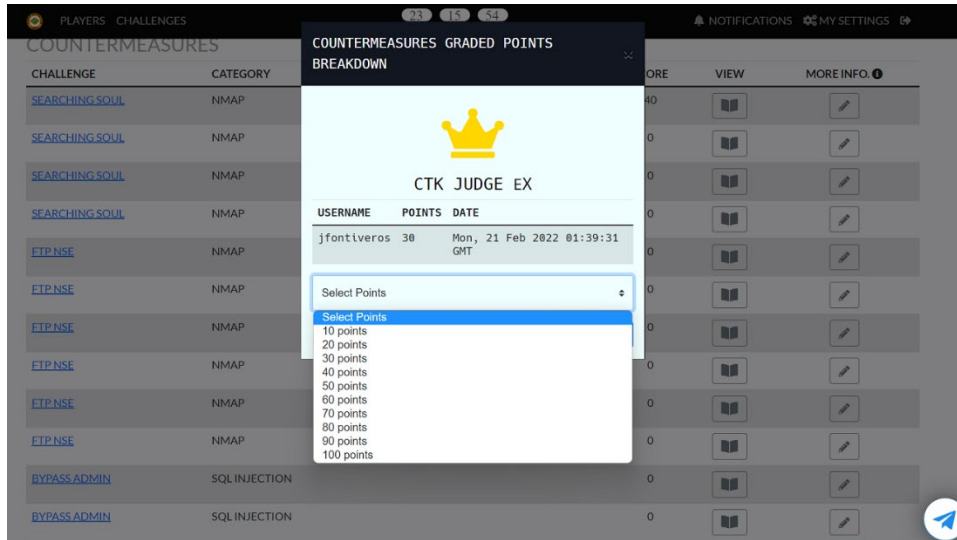


Figure 41. Figure 39. Judge eX Sample Scoring

## ***CTK Guidelines and Policy***

### EXERCISE GUIDELINES

#### GENERAL

1. A registration will be provided to the CIRT participants. Only CIRT participants who completed the activity will be given certificate of participation.
2. Each CIRT participants shall be composed of five (5) members and must be officer led.
3. All CIRT members shall attend the Cyber EX orientation. Participant who failed to attend the orientation is not allowed to access the platform as part of ensuring the security and operation of the system.
4. CIRT shall prepare their respective vtc platform. For the duration of activity, CIRT shall ensure that their camera is always open, and their microphone is functional. They must set-up their work area in a way that they can be seen in the monitor by the ED.
5. CIRT shall ensure their connectivity during the activity.

#### EXERCISE PROPER

1. CIRT participants shall follow the set guidelines in the conduct of exercise. CIRT who will violate each guideline will be given corresponding deduction of **fifty percent (50%)** points to their over-all **“DO”** score.
2. The scoring point to be used in the exercise is the one provided by the training platform.
3. In case of tie, the team who reached first the higher score will be declared as the winner.
4. Each exercise will be given a time period to be determined by the exercise directorate.
5. In case of uncontrolled connectivity problem such as power interruption, the team will be given time to complete the exercise.
6. None CIRT members of different units are not allowed to join in answering the problem exercise.
7. Only scores for the challenges will be visible to the participants.
8. ED will individually score the knowledge well, chronicles and counter measures submitted by the participants. Its average will be the final score for the said documentation.
9. Scores of the documentation will be published after all the challenges has been answered and the timeline has been completed. This is the score of surprise concept.
10. Any activity outside the competition, including probing or attacking the system and any disclosure of public IP address of the system is subject for disqualification and tantamount to investigation and severe punishment.
11. Following are the criteria for each team to reach the 3 major categories of Cyber EX.
  - **APPRENTICE** – *Automatically unlocked upon the start of the Challenge.*
  - **WARRIOR** – *Will be automatically unlocked upon completing 70% of the Challenges at APPRENTICE category.*
  - **CONQUEROR** – *Will be automatically unlocked upon completing 60% of the Challenges at WARRIOR category.*