**What will you learn?**

1. What is Capture The Flag Competition and its Types?

2. Challenges Types

3. Skills Required to Play CTFs

**Introduction**

Capture the Flag (CTF) is one of the most interesting ways to learn cybersecurity. Learning through playing is an effective way to boost your skills and start in the cybersecurity field.

We will discuss the basic information about capture the flag (CTF) competitions, challenges, tools, and resources for starting in capture the flag (CTF) competitions.

This lesson is designed to help the newcomers to these types of competitions and provide them with the skills required to get started in cybersecurity or seek a new career in infosec.

**What is Capture The Flag Competition and its Types?**

CTF stands for Capture The Flag. This is a type of cybersecurity competition or game with the purpose to locate a particular piece of text called a flag that may be on the server or behind a web page.

Capture The Flag (CTF) competition is simulating the real-world scenarios of hacking a remote site or exploiting a vulnerability on a specific application.

**There are two common types of CTFs:  Jeopardy and Attack-Defense:**

**Jeopardy CTF**

This type includes problems (challenges) like web, digital forensics, reverse engineering, and others. Teams or individuals will gain points for any correct challenge they solve.

Points are defined depending on challenges difficulty, challenges labeled as hard will help you to gain more points.

**Attack-Defense**

Here each team has its network of insecure devices (or just one host). Your staff typically has time to repair the infrastructure and fix vulnerabilities.

So you will defend your own services for defense points and hack opponents for getting attack points.

**Challenge Types**

Jeopardy-style CTFs challenges are typically divided into different categories. You will find below the most common types:

**Cryptography**

It includes understanding the different encryption algorithms.

**Digital Forensics**

It includes file format analysis, steganography, memory dump analysis, or network packet capture analysis.

**Reverse Engineering**

It includes the process of taking compiled code like .exe files or .apk or others and trying to convert it back into a more human-readable format.

**Web Security**

It includes discovering vulnerabilities in web applications.

**Exploitation**

It includes exploiting a service to find the flag, the reverse engineering techniques are also applied here in order to analyze the structure and behaviors of the binaries.

**Network Security**

It includes analyzing traffic data like pcap files and others.

**Open Source Cyber Intelligence**

It includes using open source tools to gather information.

**Skills Required to Play CTFs**

Playing capture the flag (CTF) competitions might need some basic prerequisite skills.

You will need to have some basic knowledge of networking like subnetting, TCP/IP, routing, and similar.

Also, it is important to know some Linux commands which will help you in using command-line tools on Kali Linux.

In addition to this, basic programming skills are also needed. You might not need to write code in some types of challenges but at least you need to know how to read code and understand it.

The most important skill you need to have is to be persistent, you won’t be able to solve challenges from the first day. You will need to practice days and nights to be able to solve your first group of challenges. So, don’t give up easily and keep trying.