CTF are for Nerds : A Popular myth

Parinay Bansal Follow
Oct 6 · 5 min read

I have been a student of Security for over 12 years now. About 3 years ago, I was introduced to the world of CTFs.

CAPTURE THE FLAG

History of CTFs

Capture the flag (**CTF**) is a traditional outdoor game where two teams each have a flag and the objective is to capture the other team's flag, located at the team's "base," and bring it safely back to their own base. Enemy players can be "tagged" by players in their home territory and, depending on the rules, they may be out of the game, become members of the opposite team, sent back to their own territory, or frozen in place ("in jail") until freed by a member of their own team. That's traditional CTF.

Defining CTF in Computer Security

> *Hackers' always want it their way. To hack literally means to open by force.*

Unlike the notoriously popular belief that hackers are bad people, with a lot of tattoos, long hairs and a hooded T-Shirt, hackers are just enthusiast. In the true sense, the word hacker should be accepted as a synonym to headstrong.

In computer security, Capture the Flag (CTF), a type of wargame, is a computer security competition. CTF contests are usually designed to serve as an educational exercise to give participants experience in securing a machine by breaking the existing security, as well as conducting and reacting to the sort of attacks found in the real world (i.e., bug bounty programs in professional settings). Reverse-

engineering, network sniffing, protocol analysis, system administration, programming, and cryptanalysis are all skills which have been required by prior CTF contests at DEF CON. There are three main styles of capture the flag competitions: attack/defense, hardware challenges and Jeopardy!.

In an attack/defense style competition, each team is given a machine (or a small network) to defend on an isolated network. Teams are scored on both their success in defending their assigned machine and on their success in attacking the other team's machines. Depending on the nature of the particular CTF game, teams may either be attempting to take an opponent's flag from their machine or teams may be attempting to plant their own flag on their opponent's machine. The most prominent attack/defense CTF is held every year at DEF CON, the largest hacker conference.

Hardware challenges usually involve getting a unknown piece of hardware and having to figure out how to bypass part of the security, e.g. using debugging ports or using a Side-channel attack.

Jeopardy!-style competitions usually involve multiple categories of problems, each of which contains a variety of questions of different point values and difficulties. Teams attempt to earn the most points in the competition's time frame (for example 24 hours), but do not directly attack each other. Rather than a race, this style of game play encourages taking time to approach challenges and prioritizes

quantity of correct submissions over the timing.

There is a fourth type of CTF, most commonly referred to as King of the Hill (KotH). King of the Hill is similar to Attack/Defend, but instead of everyone having their own machine (or small network) to defend, there are only preconfigured ones, which require all teams to exploit them. Once your team has successfully taken over the machine, the focus shifts to defending the machine from other teams attacks. Score is usually determined by a score reporting service on the machine, that reports a team token. When one team is able to gain access, they will remove the other teams token, and insert their own, thus making them the King of the Hill.

Certain CTF Platforms Encourage teams, others require Individuals to participate, that just depends on the kind of competition that one is participating and the rules of the game therein.

Its Definitely for the bad guys : MYTH

Knowing the definition but not understanding the underlying culture, I often am looked down upon by peers and family alike, because I like paying CTFs in my free time. I am not a great player, but yes I manage to stay in the game. I always wanted to be a hacker, that used to be a taboo to talk about some time ago, but not today.

The Community of hackers is all about problem solving, finding new

problem statements and (re)searching for answers is what the hackers do. Well scientists do the same, so essentially hackers are scientists in the computer world.

Whats in Store for ME?

> *For companies its all about the talent they hold. Any company or an employee would stand out for his Out-of-the box thinking, Uniqueness and of course knowledge.*
> *A student can gain knowledge, a company would gain understanding of the latest kinds of problems the hackers have been able to solve and the latest kinds of attacks that have been discovered.*
> *To top it up, the developers would understand security.*

Today any company across the world suffers from a cyber security threat that could be either external or internal. A bad guy, who would want to harm you will try and find a hundred way to breach you, and he needs succeed only once. But you on the other hand, need to find 101 ways you can be hacked, and plug them before he can. So you need to be ahead in the game.

CTFs provide a ready made solution for that. You can learn and play at the same time. The makers for these CTFs bear two things in mind while making CTFs : What are the currently niche ways to break code apart, what are the common and un-common mistakes the

developers are making these days and how to challenge the mind of the hacker playing the game.

> *The time for the CTFs are generally set in a manner that they challenge every nerve in the player's brain.*

That being said, you as management / developers / team leaders / researchers / CxO / any other portfolio have a plethora of knowledge to gain from the CTFs. You will know, whats current, whats bubbling and who knows you might even end up with a CVE of your own, because the idea behind the CTF is to challenge you and make you think out-of-the-box.

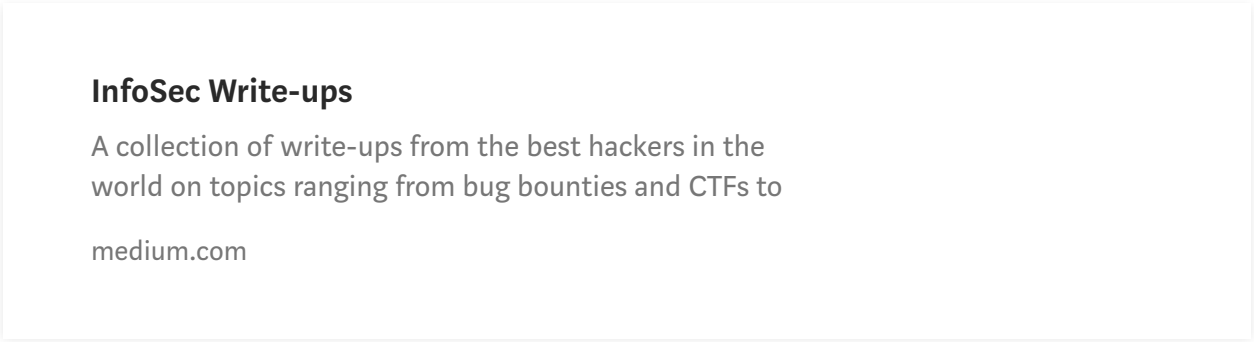
OK I am interested, Where should I being?

That's a good question.

Just head out to https://ctftime.org and find yourself a CTF that is ongoing. There are some for students, some for the pros, make your pick and just start. A CTF will generally pose problems relating to Web, Crypto, Forensic, Exploit Development, Riddles and many more. So at the end of the competition, which generally last for only a weekend, will have you gained knowledge of all of these. Isn't it quick?

I don’t have the time for it…..

Well, I suffer from similar shortage at times. Need not worry, just head over to any good site that you follow. Personally, I like to follow https://medium.com/bugbountywriteup.



Just scroll up and down the write-ups in your free time, while traveling or in the loo. And review after a month. You would see that you have become a lot wiser.

HAVE FUN……