Creating a capture the flag (CTF) to teach cybersecurity basics

Eugen Dunca
Mentored by Jarick Commarado

Introduction

Cybersecurity is a very deep field of computer science with the depth of many different techniques and information being expanded on constantly. A common way for most people to learn cybersecurity is through completing Capture the Flags (CTF). CTFs are a gamified simulation of something similar one would encounter in a realistic situation. Each level is structured to apply a unique technique which the user could already know or would have to research to be able to find the password to move onto the next level. The goal of this project was to create a unique CTF to act as an intro to Cybersecurity for beginners.

There are many levels of difficulty for CTFs with national competitions consisting of some of the hardest CTFs. A known national competition is the iCTF competition, which is held most years. In Figure 1, the network topology is shown with the teams start at the access point and moving through webserver to get access to the firewall. Afterwards, the teams could pick either the development or financial path to reach the bomb. The bomb required each team to write their own code that would disarm the bomb. At first, the competition seemed like a race, but was organized with a point system so that the progress could be better monitored and would shed light on the different strategies employed by each team (Childers et al., 2010). This project's CTF focuses on the basic foundations of operating command line and with some special challenges for some levels.

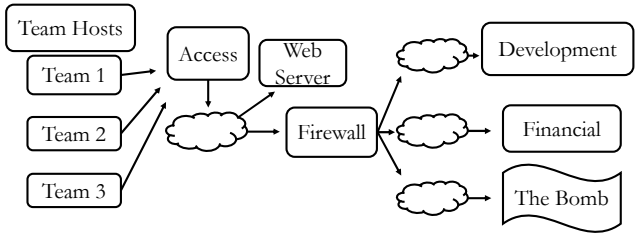

Figure 1 (above): The 2008 iCTF Network Topology, having the users move through from the access point and getting passwords to move forward from each server to the next. The final goal was to defuse the bomb.

Materials and Methods

Before starting any aspect of the project, online CTFs were completed. A CTF known as bandit provided basic skills and quickly moves onto moved onto more complicated concepts throughout the machine. The process of creating the project went through three phases. These phases were design, implementation and alpha testing. The start of the project had a document outline the CTF with skills that were to be covered and giving an overall structure to the CTF through establishing goals, a scope and a design for each level. This makes the implementation easier since the level's plan is written out.

Materials and Methods (cont.)

In the documentation, criteria was established to consider a level successful, including teaching a new concept or a challenge level, giving a reason to include that level in the CTF.

Following the documentation comes the implementation. The application used to create the machine was Oracle VM VirtualBox. A virtual machine (VM) was created to simulate a system running Linux Debian that was run locally. The machine consisted of twelve users, each being their own separate level with the password to the user hidden as the flag for the previous level. Figure 2 shows the layout for the second level, one of the first levels teaching the user about hidden directories (more commonly known as folders) and a hidden file.

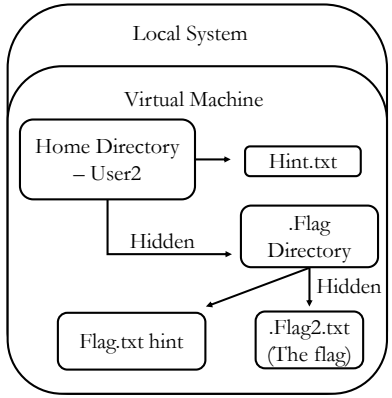

Figure 2 (left): The graphic shows how the virtual machine is running within your local system. The home directory has a hint which explains to the user about hidden directories and files and that there is a way to find and access them. Within the hidden directory is a hint reminder that hidden files exist to enforce that hidden files could exist and that should be checked for. Many levels show a similar structure with a hint teaching a new concept to find the location of the flag, which is not obvious at first.

Different levels include different skills used to complete the level, ranging from an encrypted image, cryptology and some interaction with executable files. All home directories for each level have a text document made to help the participant gain some guidance. This documents helps identify what skills the participant must learn and what direction to start looking for the flag.

After the implementation, alpha testing was conducted. Having some volunteers complete specific parts of the CTF to reveal any problems that might have been overlooked. From our alpha testing, we realized that the start of the CTF had the participant with almost no guidance for a beginner. To solve this issue, a safety document was added to provide information directly to the user for the first two levels so that they would understand which direction to move in.

The CTF is transportable to users through a snapshot of the VM. Snapshots are a compressed save point in the game, which can be sent as a file and imported into any VirtualBox application. Once imported, the CTF can run from the snapshot and can be interacted with as intended. Once the participant moves through all twelve levels, the CTF gives a congratulating message and the CTF is concluded.

Results

The CTF was completed with twelve levels that each focused on a new skill. After alpha testing, there were some adjustments made for the CTF to have better guidance for beginners to cybersecurity.

Figure 3 shows user2 within the Debian terminal, the environment that the CTF is hosted within. The CTF's functionality was working properly through some alpha testing with new features being added to provide better guidance and make the CTF more understandable for beginners. The CTF was also very accessible through the file being able to be compressed to a file which can be send to anyone who wants to complete the CTF.

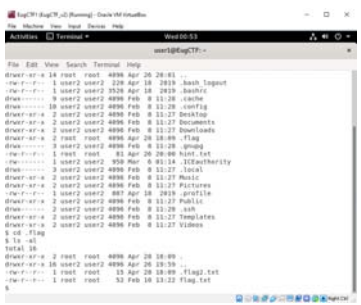

Figure 3 (left): The Debian operating system showing the flag2 and hidden flag directories.

Conclusion

The purpose of the project was to create a CTF that could be used as a learning tool. The CTF acts as a good starting place for beginners and gradually gets more difficult as they progress. By progressing through the CTF, the participant learn new concepts which they might have not encountered from other beginner CTFs. The CTF can be used as a starting place for anyone with not a lot of cybersecurity background.

CTFs were designed as a gamified version of a realistic cybersecurity situation. Most situations will need the user to find information in specific locations or manipulate permissions in a way for them to receive more access than intended. With the field of cybersecurity gaining depth and a need for higher skilled individuals, there must be a foundation. CTFs are a fun, attractive form of learning Cybersecurity with the environment feeling less stressful due to the level design. With completing this CTF, one could move onto more advanced CTFs and advance their cybersecurity knowledge and later apply it to offensive or defensive realistic situations.

References

Childers, N., Boe, B., Cavallaro, L., Cavedon, L., Cova, M., Egele, M., & Vigna, G. (2010). Organizing Large Scale Hacking Competitions. *2010 Detection of intrusions and malware, and vulnerability assessment*, *6201*, 132–152. https://doi.org/10.1007/978-3-642-14215-4_8

Chung, K. & Cohen, J.(2014). Learning obstacles in the capture the flag model. *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education*, 1–7. https://www.usenix.org/conference/3gse14/summit-program/presentation/chung