CTF Framework and Virtual Environment for Cybersecurity Education

Jadiel Colón, Naileen Berríos, Alfredo Cruz
Polytechnic University of Puerto Rico
colon_96814@students.pupr.edu, berrios_98093@students.pupr.edu,
cruz_706010@students.pupr.edu

Problem Statement

When studying cybersecurity or other computer-related technical careers, a common problem among the students is the lack of hands-on experience. This can be solved by participating in internships, conferences, and competitions. Internship opportunities and local conferences are very limited, and not every student has the flexibility to leave their homes, families, and in some cases, even day jobs for a prolonged period. We feel that the best remedy for these situations is to incorporate a virtual environment that includes exercises somewhat like a capture the flag competition [1].

BACKGROUND

A large number of competitions are organized around the world as capture the flag (CTF) events. They require students and/or participants to solve problems, earn points, and thus demonstrate their skills in different areas of cybersecurity [2]. They consist of a series of challenges that vary in their degree of difficulty, and require participants to apply different sets of skills. We are developing a learning environment framework in the form of a CTF competition. As part of the creation and validation of the framework, three CFT frameworks were analyzed and only one was chosen and we chose Mellivora. The number of frameworks are: Facebook capture the Flag, CTFd, and Mellivora.

We chose to go with a CFT based on the Mellivora framework for a number of reasons: simple to use, light, very fast, and fits our required needs. For a long time, competitions have driven economies, research, and knowledge itself. We would like to incorporate it into an environment that is directly related to what students are learning in class. The challenges are expected to include: network traffic analysis, steganography, open source intelligence, cryptography, among others.

PROJECT GOALS & SIGNIFICANCE

Capture the flag challenges can result in an increase interest from students into cybersecurity. Our implemented framework will serve as a means to allow these students to immerse themselves into hands-on exercises within different levels of difficulty: beginner, intermediate, and advanced . It will provide them with the ability to use and gain important insight for a number of different cybersecurity softwares: Metasploit, Nmap, Wireshark and others. The framework will be an essential tool for participants and it will fulfil the following goals.

- Assist participants in developing a solid foundation of cybersecurity related threats and concepts.
- Assist participants in developing a high level of proficiency in a number of cybersecurity software tools.
- Provide participants from diverse backgrounds and experience with an adequate difficulty level.
- Encourage participants to enroll into regional and international Capture The Flag competitions.

PROJECT APPROACH

To implement this project, we deployed the first virtual machine in Kali Linux machine environment that serves as the exploiting machine. Some of the tools that are being used include nmap, metasploit, OpenVAS, among others. For the purpose of teaching the students how to browse the common

vulnerabilities and exposures database, scanning networks and also exploiting vulnerable services on other machines, a metasploitable 2 machine is also deployed on the network. The identification of vulnerabilities is crucial to the effective use of security measures [3] [4]. In Figure 1, we can see an nmap scan of the metasploitable VM with some of the available vulnerabilities. We can see the open ports with the services and service versions that are running on the VM. Some of the techniques that the students have to leverage in order to exploit the machine also include password cracking, SQL injection, and cross-site scripting. Finally, for the purpose of teaching about policies, network traffic analysis and computer forensics, a windows VM is also included, in which the cyberpatriot challenge is included, as well as WireShark, the Forensic Toolkit, tools for steganography and cryptography, as well as several other tools .

A separate server will host the CTF Framework along with the scoreboard, which will be protected from attacks. Once an individual challenge is resolved, the player is given a "flag" and they send this flag to the CTF server to earn points. CTF events are usually timed, and points are added once the time has expired. We feel this dynamic can be incorporated in a week-by-week basis, as new topics are discussed in class, and new challenges are unlocked and older ones expire. In Figure 2, we see the frameworks scoreboard and interface. We can see the points awarded to participating students, as well as some of the medals awarded for being among the first to complete a given challenge in the CTF. In addition, the CTF is a recognized tool to help students with real-life problems in the area of computer security when it comes to CTF tasks. Those Scoreboard are from students who practice in the CTF when we are developing, you can see too the points, the points earn are when the students answer the challenge who have 100 points each ones. Because the Framework could technically be used as part of course grade assignments, hacking it or modifying it could constitute a violation of the university's honor code.

FIGURES

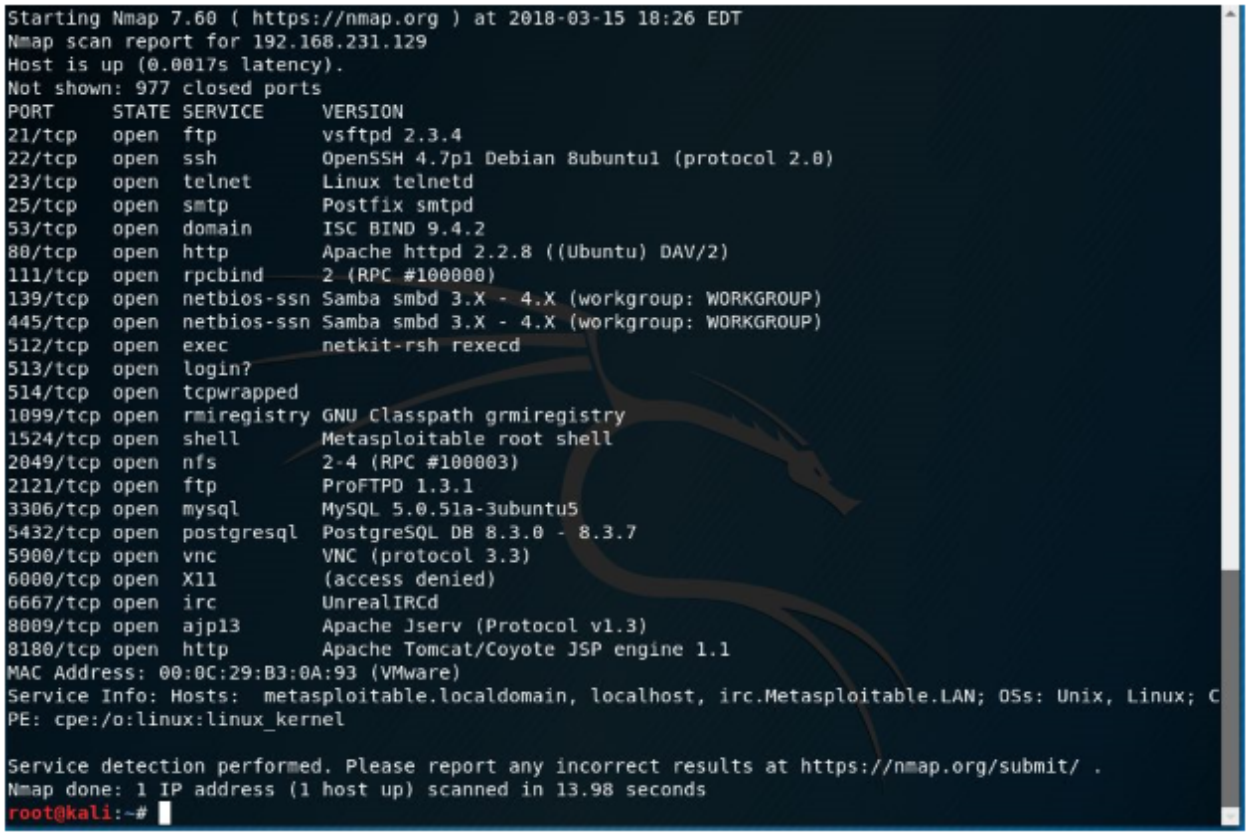

Figure 1: nmap scan of the metasploitable 2 machine performed from inside the Kali Linux machine

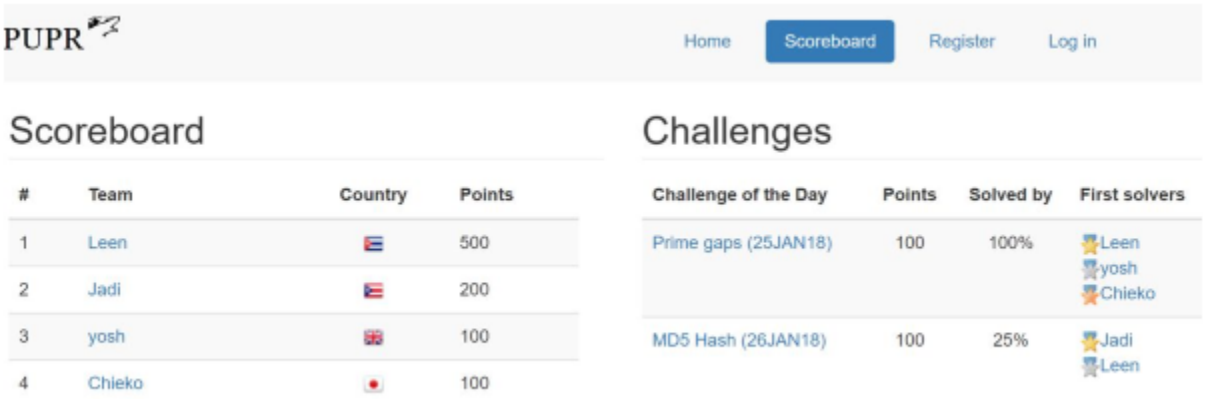

Figure 2: Framework Interface is very user-friendly. Allows to set timed challenges and max number of attempts per challenge.

ACKNOWLEDGEMENT

This material is based upon work supported by, or in part by the National Science Foundation Scholarship for Service (NSF-SFS) award under contract/award #1563978

REFERENCES

[1] Leune, K., & Petrilli, S. J. (2017). Using Capture-the-Flag to Enhance the Effectiveness of Cybersecurity Education. Proceedings of the 18th Annual Conference on Information Technology Education - SIGITE '17 . doi:10.1145/3125659.3125686

[2] Ford, V., Siraj, A., Haynes, A., & Brown,E.(2017).CapturetheFlagUnplugged.Proceedingsofthe 2017 ACM SIGCSE Technical Symposium on Computer Science Education - SIGCSE '17 .doi:10.1145/3017680.3017783

[3] Idika, N. C., Marshall,B.H.,&Bhargava,B.K.(2009).Maximizingnetworksecuritygivenalimited budget. The Fifth Richard Tapia Celebration of Diversity in Computing Conference on Intellect, Initiatives, Insight, and Innovations - TAPIA '09 . doi:10.1145/1565799.1565803

[4] Venter, H., & Eloff, J. (2003). Assessment Of Vulnerability Scanners. Network Security , 2003 (2), 11-16. doi:10.1016/s1353-4858(03)00211-3