Learn DDoS Attacks with a Game

Jaris Johnson, Patrickson Weanquoi, Jinghua Zhang, Jinsheng Xu

***Abstract*—Distributed Denial of Service (DDoS) is an attack where the attacker overflows the victim's computer with requests, so legitimate users cannot access the victim. Currently, there is a lack of engaging ways to teach about DDoS attacks. Thus, we created a 3D game to teach the basic concepts of DDoS. The game offers a variety of debugging and visualizing tools, which can be used to examine malicious IP addresses. To evaluate the impact of the game, a pre-quiz and post-quiz will be used, which are incorporated into the game. The game is self-contained and can be deployed to different platforms.**

***Index Terms*—DDoS Attack, TCP SYN Flood, Game-Based Learning, Network Security**

I. INTRODUCTION

THE Internet has continued to develop as a gateway to massive amounts of information and services. However, with this development, there come structural vulnerabilities that may be exploited. For hackers, websites and web services are apparent targets for attacks. Having access to an organization's servers over a network is vital for legitimate users to access their requested service. However, this ability is compromised because of DDoS attacks.

Currently, there is a significant lack of engaging ways to teach about DDoS attacks. Most of the information about these attacks are limited to pictures, videos, and lectures. Beyond that, there are a few DDoS simulations that require significant technological skills to deploy. Additionally, the average person has little to no knowledge of DDoS attacks and their effects on Internet traffic and users.

Our goal is to create a 3D game that aims to help students understand what a DDoS attack is, what types exist and how they affect Internet users through visualization and gameplay. For example, one major module in our game helps students learn TCP SYN Flood, which is one of the most common DDoS attacks on the transport layer of the OSI model. It would allow them to control and visualize the attack to gain a clear understanding of the process from start to finish. Additionally, it would give players the ability to alter game elements to achieve different results, rather than the static results gained from pictures and videos. Lastly, it would present this learning opportunity in a simplified manner that anyone can use and enjoy.

Manuscript received July 23, 2018. This work was supported in part by Collaborative Research Experiences for Undergraduates (CREU) via AYUR program.

Office Setting assets are from https://assetstore.unity.com/packages/3d/props/furniture/office-cubicle-kit-25082

Server/Computer assets are from https://assetstore.unity.com/packages/3d/props/electronics/server-rack-computer-servers-73133

Jaris Johnson, Patrickson Weanquoi and Jinghua Zhang are with Winston-Salem State University, Winston-Salem, NC 27110. (Email: zhangji@wssu.edu)

Jinsheng Xu is with North Carolina A&T State University, Greensboro, NC 27411.

II. BACKGROUND AND RELATED WORK

Some research focused on projects that strayed from the conventional picture, video, or lecture format. Most, however, were simulation based. Garrido presented a model of a DDoS attack on a network through object-oriented modeling and simulation [3]. The DDoS network simulation model was implemented in the OOSimL simulation language because one of his goals was to develop new simulation tools and approaches for education [3]. This was similar to our goal of educating, except we chose not to use simulation due to the possible complexity. Some researchers discussed the detection and mitigation of DDoS attacks, such as in [2]. This work emphasized the concerns that cyber-attacks, such as DDoS, will manifest in magnitude and complexity in a smart grid AMI network. Such attacks will range from a delay in the availability of end user's metering data to complete denial in the case of a grounded network. This lead to the proposal of a cloud-based firewall for the mitigation and prevention of DDoS attacks. Whereas Diovu and Agee approached the issue from a defensive system standpoint [2], our approach was more aligned with educating about cause and effects of DDoS. Wright et al [8] used moving target, whose strategies typically work by relocating targeted services over time. This increases uncertainty for attackers, while also trying not to disrupt legitimate users or gain excessive costs. Zuybadi et al. [9] went an alternate path, discussing Software Defined Networking (SDN), which is an emerging technology in communication systems. Lastly, others focused on DDoS defense [1,4,5,6,7]. Booth et. al. described a critical infrastructure network DDoS defense by using cognitive learning. The researchers used a cognitive approach, which was derived from Cognitive Radio Network (CRN) to provide an anti-DDoS defense. Design Science research (DSR) methodology was also used to provide an anti-DDoS defense [1]. These ideas were incorporated in our research to show the movement of packets from client to server. Manoja et. al. presented a prevention technique against DDoS attacks in the cloud environment [4].

III. GAME DESIGN AND DEVELOPMENT

Unlike currently existing systems, our approach was to develop a 3D educational game that provides a self-contained experience transferable over multiple platforms that does not require high levels of technical ability to

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

download and play. Three undergraduate students in the Department of Computer Science designed and developed the prototype using the Unity game engine and C# scripting language. The game is designed to be played for around five to ten minutes per topic. To evaluate the impact of the game on students' learning, the pre-quiz and post-quiz are built into the game.

We decided to build a 3D game world to make the learning space as close to job environment as possible. The player will be immersed in the learning environment and can perform the actions as if in a real situation. 3D office space shown in Fig. 1 in the game has a server room, four cubicle sections, and a common area.

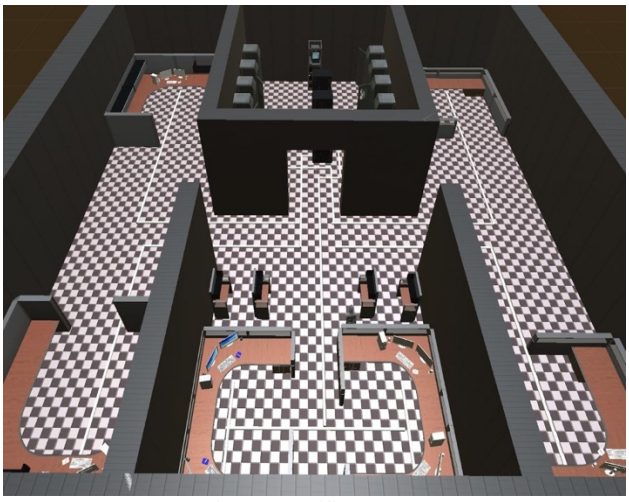

Figure 1. Office Space

The server room shown in Fig. 2 is located adjacent to the common area. It's used to host several servers and a server computer. Players can use the server room to manipulate and view changes to the servers. And also, it is easier for players to navigate and configure server features. Furthermore, cubicles in the office space allows for great mobility and easy communication. Each cubicle is designed in parallel to the others, with two cubicles on each end of the room. Lastly, there is one common area where the player spends most of the time configuring the server.

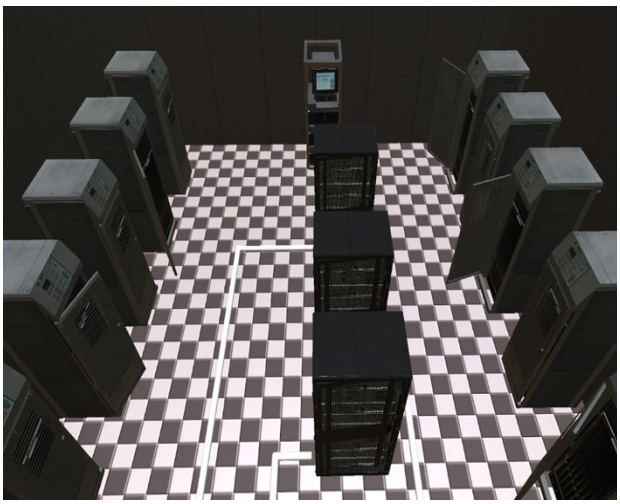

Figure 2. Server Room

The game starts with a short introduction about the game controls and game story. Once entering the play mode, the participant will enter a mandatory pre-assessment stage. This stage will include a pre-quiz to test the player's knowledge of the targeted topic and a questionnaire about the player's skills. The player's responses and the detailed game events describing the player's interaction with the game will be logged and submitted for further analysis. Once the participant completes all the learning modules, he/she will enter the post-assessment stage to complete a post-quiz and an online survey to share their feedback after playing the game.

Students are expected to explore the learning modules in order of difficulty. Fig. 3 shows the current available topics for learning. The participants will start with the Network Components module where they will learn the important components in the network such as functionality of routers, IP address etc. After that, the game unlocks the Transmission Control Protocol (TCP) learning module to help students understand the purpose of the protocol and how it works with the Internet Protocol. The third module helps participants learn about TCP SYN Flood, which is one type of DDoS attack. The game incorporates network flow and DDoS attacks. The player controls the main character (an intern in a tech company) to learn different types of DDoS attacks such as TCP SYN Flood. UDP Flood and PING Flood will be added to the learning module in future iterations. The player will interact with the boss who acts as a guide on the first day. The boss takes the intern through the server room while explaining how maintenance of the servers will work. He also explains how the intern will monitor network activity and take action once a DDoS attack is initiated. The intern then begins his/her first day where they are presented with a UI to learn how to monitor packet rates from the server room. In addition, the game provides the intern with a TCP-SYN UI which allows him/her to carry out an attack on the network and see the impact of the TCP SYN Flood.

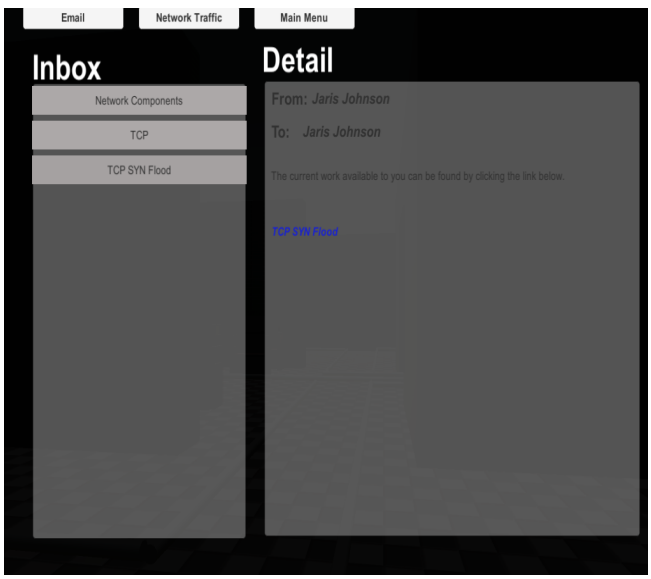

Figure 3. Current Modules

There are many varieties of DDoS attacks; we chose to first focus on the concept of TCP SYN Flood. TCP SYN Flood is a basic form of DDoS attack where the client computer initiates connection with the host server, but the connection is never established. The module helps the

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

player understand how this form of attack holds valuable resources of the host's computer at a standstill. The player will be able to send and receive packets to see the impact of the TCP SYN Flood attack as shown in Fig. 4. There is also an option for the player to control the rate of data flow and monitor the effect it has on the network.

Figure 4. TCP SYN Flood UI

Fig.5 shows one of the tools that the player can use to find potential problems in the network. When it is configured, active connections are visible. Malicious IP is detected and removed based on the information provided. This tool is activated by interacting with the server through the network topology shown in Fig. 6. TCP SYN Flood UI will be unlocked after completing the review session, providing an interactive illustration of the TCP SYN flooding.

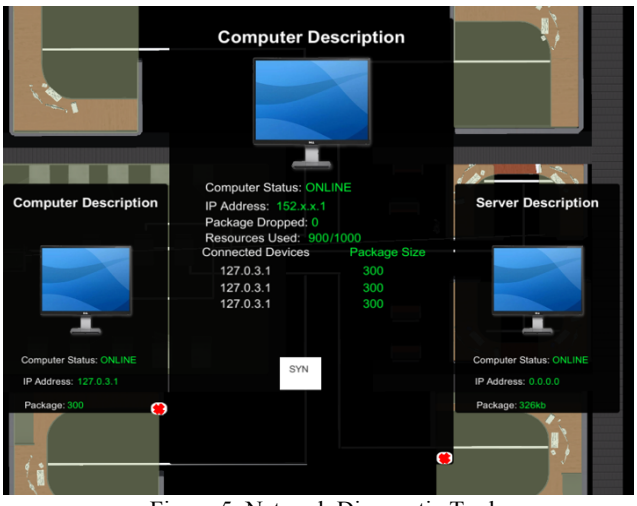

Figure 5. Network Diagnostic Tool

Finally, the player is presented with an overlay of the office that signals the server rooms current status based on network activity as shown in Fig. 7. When the server room flashes red, it indicates that there is a TCP SYN Flood attack in progress. The topology tool is the first indication the server is under attack. Network topology could be analyzed to debug the root cause of the problem and eliminate it. To find out the status of each computer on the network shown in Fig. 6 and Fig. 7, the player can click the icon of the computer to view the detailed activities. The IP address that caused the attack will be blocked from sending access requests to the server.

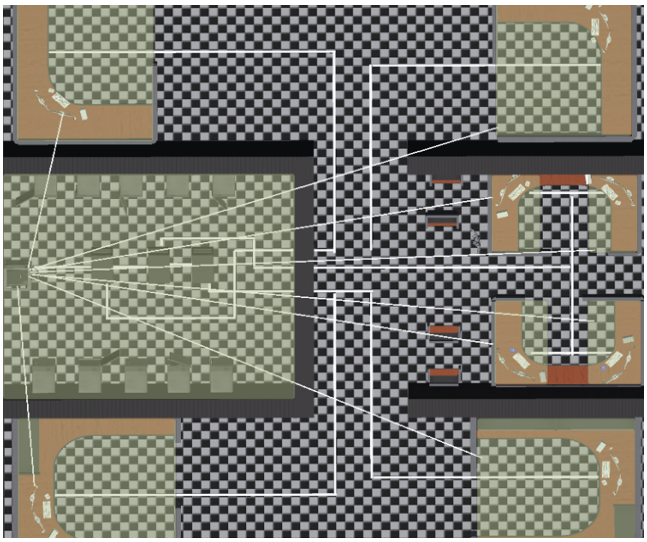

Figure 6. Network Topology

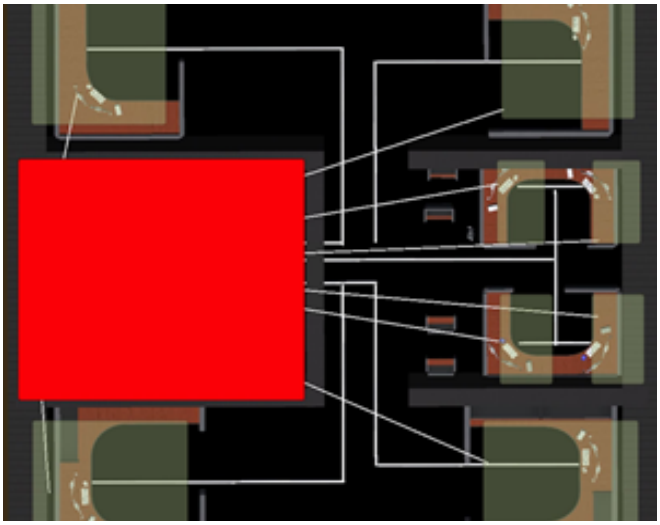

Figure 7. DDoS Overlay Signaling SYN Flood Attack on Servers

IV. RESULTS AND FUTURE WORK

In summary, we developed a 3D game environment using the Unity game engine and C# to help students understand TCP SYN Flood - one basic form of DDoS attacks. A pre-quiz shown in Fig. 8 and post-quiz shown in Fig. 9 are built into the game and will be used to evaluate the impact of the game on the students' learning. Each quiz consists of five multiple choice questions, allowing students to quickly reinforce the new information they have attained. After the game play, students will take an online survey to provide feedback.

This game will be used in lower level computing courses. We will refine the game based on student feedback, as well as add more modules to teach other forms of DDoS attacks, such as UDP Flood attacks.

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

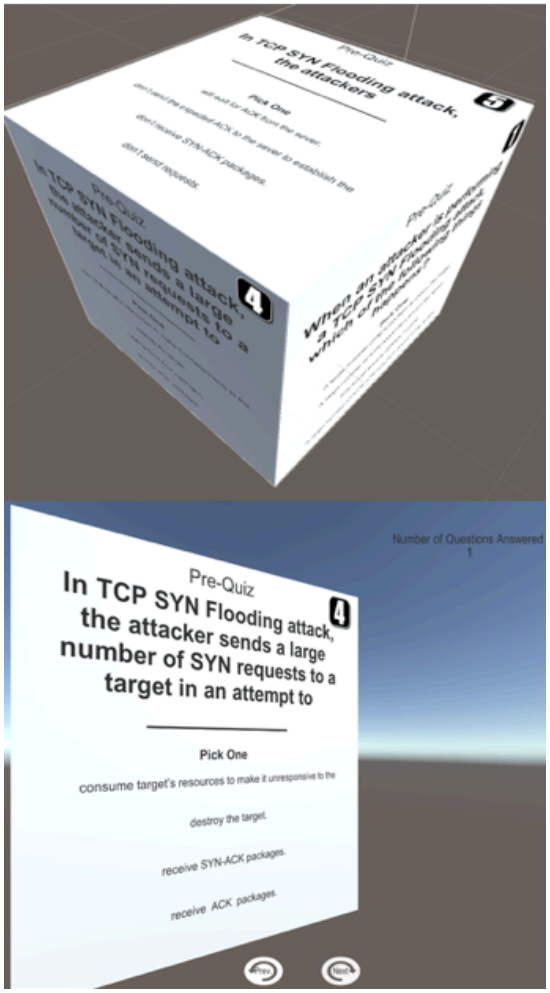

Figure 8. Pre-Quiz

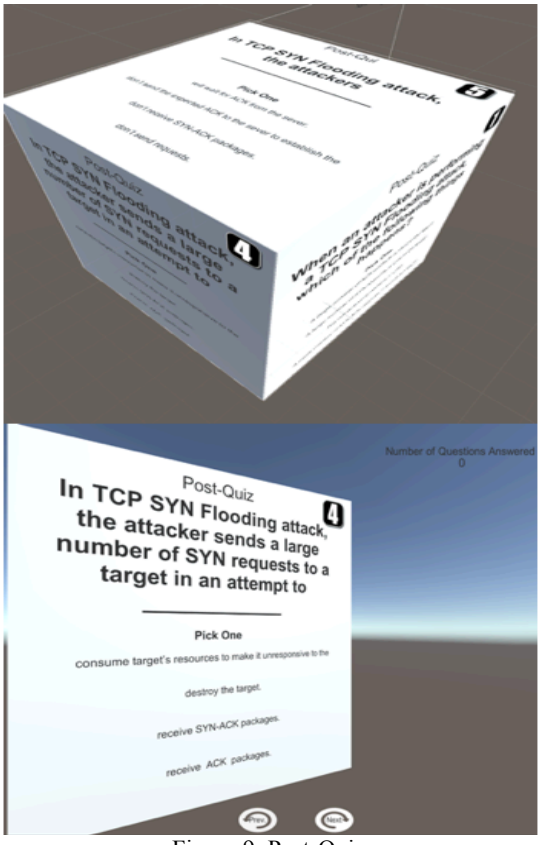

Figure 9. Post-Quiz

REFERENCES

[1] Booth, T., and Andersson, K.. 2017. "Critical Infrastructure Network DDoS Defense, via Cognitive Learning." 2017 14th IEEE Annual Consumer Communications & Networking Conference (CCNC), doi:10.1109/ccnc.2017.8013423

[2] Diovu, R. C., and Agee, J. T. "A Cloud-Based Openflow Firewall for Mitigation against DDoS Attacks in Smart Grid AMI Networks." 2017 IEEE PES PowerAfrica, 2017, doi:10.1109/powerafrica.2017.7991195

[3] Garrido, J.M. 2009. Understanding distributed denial of service with object-oriented simulation. In Proceedings of the 47th Annual Southeast Regional Conference (ACM-SE 47). ACM, New York, NY, USA, Article 8, 4 pages. DOI=http://dx.doi.org.courseinfo.wssu.edu:2048/10.1145/1566445.1566456

[4] Jiao, J., et al. 2017. "Detecting TCP-Based DDoS Attacks in Baidu Cloud Computing Data Centers." 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), doi:10.1109/srds.2017.37.

[5] Manoja, I., et al. 2017. "Prevention of DDoS Attacks in Cloud Environment." 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC), doi:10.1109/icbdaci.2017.8070840.

[6] Petana, E., and Kumar, S.. "TCP SYN-Based DDoS Attack on EKG Signals Monitored via a Wireless Sensor Network." Security and Communication Networks, vol. 4, no. 12, 2011, pp. 1448–1460., doi:10.1002/sec.275.

[7] Rashidi, B., and Fung, C.. "CoFence: A Collaborative DDoS Defence Using Network Function Virtualization." 2016 12th International Conference on Network and Service Management (CNSM), 2016, doi:10.1109/cnsm.2016.7818412

[8] Wright, M., et al. 2016. "Moving Target Defense against DDoS Attacks." Proceedings of the 2016 ACM Workshop on Moving Target Defense - MTD'16, doi:10.1145/2995272.2995279

[9] Zubaydi, H. D., et al. "Review on Detection Techniques against DDoS Attacks on a Software-Defined Networking Controller." 2017 Palestinian International Conference on Information and Communication Technology (PICICT), 2017, doi:10.1109/picict.2017

ISBN: 978-988-14048-1-7
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)