Learn ARP Spoofing Attack in a Game

Jinsheng Xu[1], Xiaohong Yuan[1], Swathi Nallela[1], Kevin Hillard[1], Jinghua Zhang[2]

[1]Department of Computer Science
North Carolina A&T State University
Greensboro, NC, USA
{jxu, xhyuan}@ncat.edu
{snallela, kshilliard}@aggies.ncat.edu

[2]Department of Computer Science
Winston-Salem State University
Winston-Salem, NC, USA
zhangji@wssu.edu

***Abstract*—Local Area Network (LAN) access is the top vector for insider threats and misuses. It is critical for students to learn these vulnerabilities and know the common countermeasures. Although some educational tools exist that are effective in teaching ARP spoofing, they are usually hard to access and not fun enough to engage students. Gamification has been successfully used in many areas of education to engage students in learning. Gamification can provide educational and immersive experiences to the students. To our knowledge, there is no game developed to teach LAN and ARP spoofing concepts. In this paper, we present a gamification of this subject with an escape-the-room style game to teach LAN and ARP spoofing attacks. The game is developed with the Unity game engine and deployed on the world wide web. Therefore, the game is accessible anywhere on the Internet with a web browser. The game has several levels of difficulty that guide learning from the basics of LAN to the countermeasures. This game's primary learning objectives are 1) Learn how switches and hubs work, and how ARP protocol works; 2) Learn how ARP spoofing works; 3) Learn the counter measures against LAN attacks. The game would be hosted on the Web and students would be allowed to play online using the web link and provide feedback. The game is presented in the form of a 3-level building. Each level has multiple rooms where each room holds the content to learn on a different concept. The player must go through each concept and answer the quiz questions before the player can move to the next room. At the end of each level, the player will get additional challenges to complete to move to the next level. The game events which describe the player's interaction with the game will be logged and submitted for further future analysis through the GameSparks. Once the player completes all the levels, the player will enter the post-assessment stage, where they will complete a post-test and survey. The post-assessment results will be automatically collected and submitted for quantitative analysis.**

Keywords—game-based learning, educational game, security and privacy, local area network, address resolution protocol

I. INTRODUCTION

Cybersecurity is increasingly critical as we spend more of our everyday lives online. There are numerous flaws in the design of networked communication systems. Among them, LAN protocols have many vulnerabilities and most of them are very easy to exploit [20]. In Ethernet, the common vulnerabilities come from Address Resolution Protocol (ARP) and the weakness of switches that computers are connected to. It is critical for students to learn these vulnerabilities and know the common countermeasures. Although some tools have been developed that have shown to be effective in teaching ARP spoofing [1-3], they have a few problems. The first one is the difficulty in dissemination for wider adoption. Because some tools contain virtual machines that are several gigabytes in size, it will take time to download. It is also technically challenging to successfully install and configure virtual machines. The second problem is that it is difficult for students with little background knowledge in LAN. The tools lack guided learning components that can lead students to the solution gradually. The last problem is the lack of fun in these tools which may not engage.

Games have been successfully used in many areas of education to engage students in learning [6, 14]. Research shows multiple benefits of cyber security games [13, 16]. Games can provide educational and immersive experiences, which will inspire students to explore more in the security field and help students test their knowledge in authentic settings.

Many games have been used to teach cyber security concepts [4-5, 8-11, 15, 17-18]. However, to our knowledge, there is no game developed to teach LAN and ARP spoofing concepts. In this paper, we present an educational game we created to address the issues presented above. The game is developed with the Unity game engine and deployed on the world wide web. Therefore, the game is accessible anywhere on the Internet with a web browser. The game has several levels of difficulty that guide learning from the basics of LAN to the countermeasures. This game's primary learning objectives are:

1) Be able to explain how switches and hubs work, and how ARP protocol works.
2) Be able to describe how ARP spoofing works.
3) Be able to list the countermeasures against LAN attacks.

The game is presented in the form of a 3-level building. Each level has multiple rooms where each room holds the content to learn on a different concept. The player must go through each concept and answer the quiz questions before the player can move to the next room. At the end of each level, the player will get additional challenges to complete to move to the next level. At the beginning of each level, the student will be given a set of instructions to play the game, how to navigate and what objective they will be learning in the level. Research shows that in-game assessments can increase the students' engagement level [12]. Therefore, the game also includes built-in assessment components. The game events which describe the player's

interaction with the game will be logged and submitted for further analysis through the GameSparks [7]. To evaluate the impact of this game on students' learning, we developed in-game assessments, a pre-survey, and a post-survey. The game events which describe the player's interaction with the game will be logged and submitted for further analysis in the future. Once the player completes all the levels, the player will enter the post-assessment stage, where they will complete a post-test and survey. The post-assessment results will be automatically collected and submitted for quantitative analysis.

This paper is organized as follows: Section II provides game design and development in detail, Section III presents the detailed assessment results, and Section IV describes the conclusion and future work.

II. Game Design and Development

Unity game engine was used to develop this game and WebGL library was used so that the game can be played from any web browser. Students can play it online at http://gamelab.wssu.edu. This game is an *escape the room* style game, where the students help the main character solve multiple challenges until the character escapes completely from the multiple room building.

This game is presented in the form of a 3-level building. Each level has multiple rooms where each room holds the content to learn on a different concept. The player must go through each concept and answer the quiz questions before the player can move to the next room. At the end of each level, the player will get additional challenges to complete to move to the next level. At the beginning of each level, the student will be given a set of instructions to play the game, how to navigate and what objective they will be learning in the level. In addition, we implemented the level control that allows the player to restart the level instead of restarting the game when necessary. Figure 1 shows the main screen of this game.

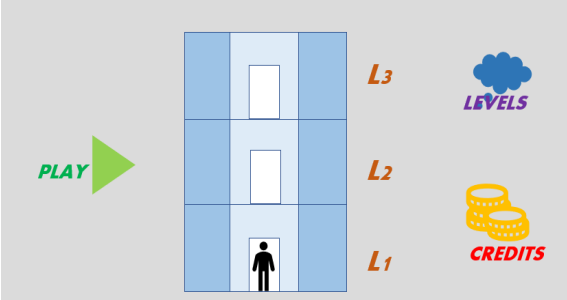

Fig. 1. Main Screen

A. Level One – Learn how LAN and ARP work

The goals of level 1 is to teach students the concepts of LAN, switches, IP address, Ethernet Frame, and Address Resolution Protocol (ARP). There are four rooms in this level. Room 1 teaches students LAN and its components; Room 2 introduces students the concept of IP address; Room 3 describes the format of Ethernet frames; Room 4 teaches students show ARP works. The following figure 2 shows the summary of learning objects presented to the students before entering the level 1.

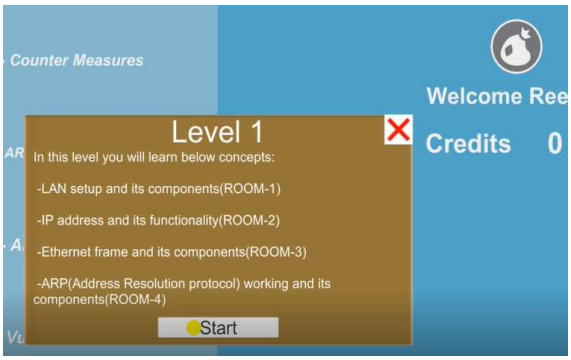

Fig. 2. Level One Concepts

Room 1 displays a Local Area Network (LAN) setup and teaches students about the components in a LAN setup and their importance in the communication. Students will learn the basic components of a LAN: switches, routers, and access points. Upon reviewing the content, students will be prompted to answer a question based on the learning they did in the Room 1. To enter the next room, the student must answer the challenge question correctly and once answered, the student will be allowed to go to the next room. Student is always allowed to go back into the room and learn the components again until they are familiar with the concept.

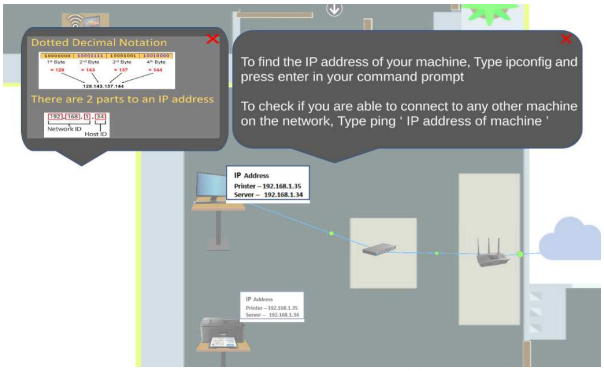

Fig. 3. Level 1 Room 2: IP Address

In Room 2, where they would learn about Internet Protocol (IP) Address. Figure 3 shows a snapshot from the IP address learning component. Students will learn dotted decimal notation, network address/host address, and how to get the IP address of the current machine and test connective to other IP address via *ping* command.

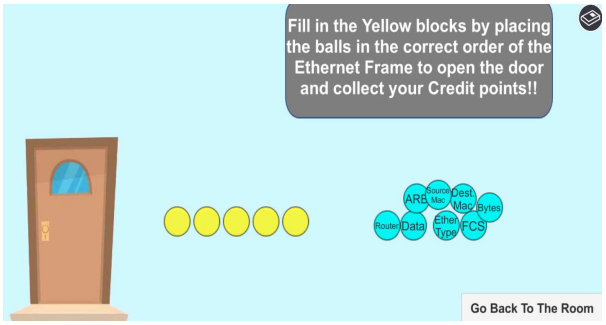

Fig. 4. Level 1 Room 3: Ethernet Frame Challenge

In Room 3, students will learn the format of Ethernet frames. To make it interesting, we have animated a moving Ethernet packet, where the student must click on each moving component to learn about it. The qualifying question for this component would be in the form of a simple game where the students must place the balls in the correct order for the door to open and let them pass through to the next room as shown in Figure 4.

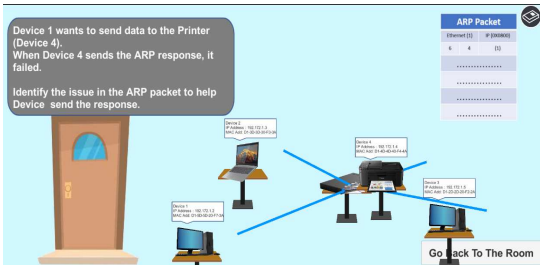

Fig. 5. Level 1 Room 4: ARP Challenge

In Room 4, students will learn how ARP works. Students would be asked to click on a simulation to see how ARP packets are formed and how ARP caches change. Students click on each part of the ARP Packet to learn more about fields in the packet. Fig 5 shows the challenge students must solve to exit the room.

B. Level Two – ARP Spoofing Attack

This level teaches students how ARP spoofing works. Because this is quite complex process, we created a virtual character called Joe who guides students throughout the learning process. Figure 6 shows the environment of the setup with three computers: A, B, and Attacker. The goal of this level is to use the Attacker computer to do ARP Spoofing attacks so that Attacker can intercept the traffic between A and B, thus becoming the Man-In-The-Middle. The IP addresses and the MAC addresses of all these computers are shown. The ARP caches of A and B are also shown.

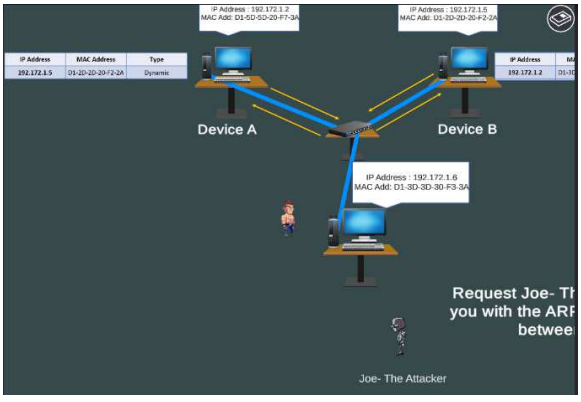

Fig. 6. Level 2: ARP Spoofing Setup

Using the Left and Right arrow buttons, the student can control the conversation between the player and Joe. Joe instructs students step by step on how to do the ARP spoofing attack. Students will fill out fields in the ARP reply packets according to the instructions. The fields would show in green color if the values are correct and they would show in red if the entered values are wrong. Once the player enters the correct values, a simulation is generated which shows the ARP packets moving to the victims and that device ARP Cache table poisoned. Figure 7 shows the screenshot of animation when ARP spoofing is successful.

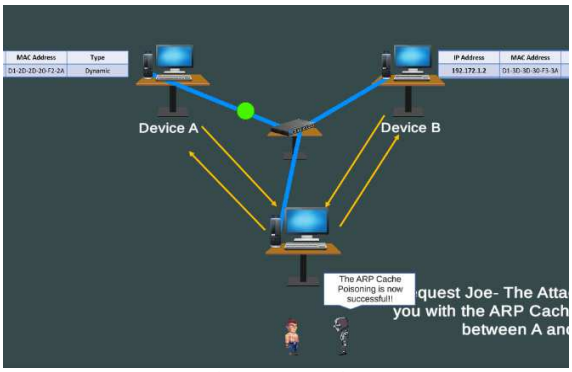

Fig. 7. Level 2: ARP Spoofing Animation

As part of the evaluation in this level, the player is provided with a challenge to perform the ARP spoofing attack by entering the correct IP address and MAC address values for two ARP reply packets needed to become successful Man-In-The-Middle as shown in Figure 8. In the second evaluation problem, the player would be asked to arrange the steps in order to perform an ARP spoofing attack. The player would drag and drop in the correct order in the blocks. Once the blocks are arranged correctly, the player would have successfully completed the module.

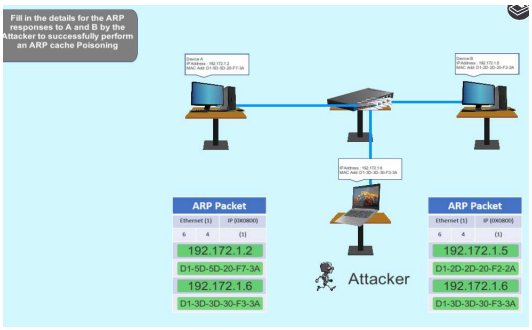

Fig.8. Level 2: Challenge

C. Level Three – Countermeasures

This level teaches students how to protect against the ARP spoofing attacks. While there are several methods of ARP spoofing attacks, this game focus on static ARP cache. The setup is the same as in the Level 2 with three computers: A, B, and Attacker. The player would be given option to control the conversation with Joe using the Left and Right arrow buttons. The learning component would be in the form of the Joe explaining the concept of Static ARP to the player. Joe also teaches the Player command line to set the ARP cache with static entry. Then, students will be asked to carry out the same attack as they did in level 2. This time, students will notice that ARP cache of the victims did not change because of static ARP cache. For the challenge, we ask the user to make ARP cache static for a different setup.

III. Classroom Experience Report

We conducted a pre-survey to evaluate the participants' background knowledge in the related subject and post-survey to collect the participants' opinions on this game in the undergraduate network security class. Twenty one responses were recorded for the pre-survey and sixteen responses were recorded for the post-survey. The pre-survey began by analyzing the students' prior experience with cybersecurity. The results are shown in table 1. 39% of students have taken cybersecurity courses or training prior to playing the game. These courses and training include Applied Network Security, Fundamentals of Information Assurance, Web Security and CodePath's cybersecurity course. 91% of students had never had prior experience with a cybersecurity educational game, however. 73% of students were concerned about cybersecurity incidents, with 82% of students spending at least 1-2 hours learning about cybersecurity each week. Finally, 62% of students were interested in ARP concepts prior to playing the game. Table 2 shows the post survey result. Interest in ARP grew 26% from the pre-survey. 88% of students felt the ARP game was an engaging way to learn the topic, and felt more confident in describing the concepts learned. In addition, all students enjoyed using the game to learn the material and expressed interest in seeing more cybersecurity topics taught using games. Students were asked to rate their level of knowledge or skills in several categories on a five-point scale, ranging from None to Excellent. Table 3 shows the questions asked, the mean of the results from the pre-survey and post-survey, and the percentage of Excellent and Good responses from each survey. Overall, students feel that their skills in each area have improved after playing the game.

When asked for open-answer feedback, students praised the interactivity of the game and the detailed explanations in each level. Suggestions for improvement included increasing the number of levels in the game, making the text bigger and easier to read, and allowing the clicking function, used for movement and interacting with objects.

Table 1. Pre-Survey

Question	
Have you taken cybersecurity course(s) or formal training (e.g. workshops, certification training, etc.) on common cybersecurity practices?	39% (YES)
Do you have prior experience with a Cybersecurity Education Game?	9% (YES)
How frequently do you read cybersecurity-related newsletters or articles?	41% Frequently
I am concerned about cybersecurity incidents.	73% Agree
I am interested in learning about Address Resolution Protocol (ARP).	62% Agree

Table 2. Post-Survey

Question	Strongly Agree/Agree
I am interested in learning about the topic of Address Resolution Protocol (ARP).	88%
The ARP Game engaged me in learning this topic.	88%
I enjoyed the learning experience of this topic using the ARP Game.	100%
I think the learning experience with the ARP Game is effective.	100%
I am satisfied with the level of effort the ARP Game requires for learning this topic.	94%
After using the ARP Game, I have more confidence in describing the concepts learned.	88%
I wish more cybersecurity topics will be taught using games.	100%

Table 3. Learning Object Survey

Question	Pre-Survey Mean	Post-Survey Mean	Pre-Survey Excellent/ Good	Post-Survey Excellent / Good
Explain different components of LAN	2.95	3.94	19%	75%
Use the 'ipconfig' command.	2.71	4.25	14%	100%
Explain what an Ethernet is.	3.76	4.31	57%	94%
Explain the different parts of an Ethernet Frame.	3.00	4.00	29%	81%
Explain the workings of Address Resolution Protocol (ARP).	2.05	3.94	10%	75%
Explain the different parts of an ARP packet.	2.10	4.13	14%	88%
Explain the steps in ARP Cache poisoning.	1.90	3.75	5%	75%
Understand the countermeasures for ARP Cache Poisoning.	1.81	3.81	0%	63%
Use the command arp -s.	1.71	3.94	0%	75%

IV. Conclusions and Future Work

We designed and built game that teaches LAN, ARP spoofing, and the countermeasures. The game is built to the WebGL format and made available online. Through the integration of GameSparks IDE, we can continuously collect and analyze player data to improve user experience and ensure the quality of the game.

Based on the initial assessments, students not only enjoyed this game, but also improved learning. We will keep improving this game based on feedback collected. In addition, more assessments will be carried out in the future.

ACKNOWLEDGEMENTS

This work is supported by NSF under the grant DUE-1821960 and 1821965. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of NSF.

REFERENCES

[1] Xu, J., Yuan X., Yu, A., Kim, J. Kim, T. Zhang, J., "Developing and Evaluating a Hands-On Lab for Teaching Local Area Network Vulnerabilities", IEEE Frontiers in Education, 2016.

[2] Scott, B., Xu, J., Zhang, J., Brown, A., Clark, E., Yuan, X., Yu, A., Williams, K., An interactive visualization tool for teaching ARP spoofing attack, IEEE Frontiers in Education, 2017.

[3] Baxley, T., Xu, J., Yu, H., Zhang, J., Yuan, X., Brickhouse, J., "LAN attacker: A visual education tool", Proceedings of the 3rd annual conference on Information security curriculum development, 2006.

[4] Compte, A. L., Elizondo D., and Watson, T. (2015) "A Renewed Approach to Serious Games for Cyber Security", *Proceedings of* the *7th International Conference on Cyber Conflict: Architectures in Cyberspace:* 203-16, 2015.

[5] Cullinane, I., Huang, C., Sharkey, T. and Moussavi, S. (2015) "Cyber security education through gaming cybersecurity games can be interactive, fun, educational and engaging" *J. Comput. Sci. Coll. 30, 6. June 2015, pp. 75-81.*

[6] Eagle, M., Barnes, T., "Wu's castle: teaching arrays and loops in a game", Proceedings of the 13th annual conference on Innovation and technology in computer science education, June 30-July 02, 2008, Madrid, Spain

[7] GameSparks, https://www.gamesparks.com/.

[8] Guimaraes, M., Said, H. and Austin, R. "Using Video Games to Teach Security." Proceedings of the 16th Annual Joint Conference on Innovation and Technology in Computer Science Education - ITiCSE '11(2011): 346.

[9] Herr, C. and Dennis, A. (2015) "Video Games as a Training Tool to Prepare the Next Generation of Cyber *Warriors*", *Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research* - SIGMIS-CPR '15, Newport Beach, CA, 2015.

[10] Irvine, C., Thompson, M. and Allen, K., "CyberCIEGE: Gaming for Information Assurance", IEEE Security & Privacy, vol. 3, no. 3, 2005, pp. 61–64

[11] Jordan, C., Knapp, M., Mitchell, D., Claypool, M. and Fisler, K. "CounterMeasures: A Game for Teaching Computer Security." 2011 10th Annual Workshop on Network and Systems Support for Games.

[12] Lee, M., Ko, A. and Kwan, I. (2013), "In-game Assessments Increase Novice Programmers' Engagement and Level Completion Speed," In Proceedings of the Ninth Annual International ACM Conference on International Computing Education Research (ICER '13). ACM, New York, NY, USA, 153–160.

[13] Pusey, P., Tobey, D. and Soule, R., "An Argument for Game Balance Improving Student Engagement by Matching Difficulty Level with Learner Readiness ". In 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14). USENIX Association, San Diego, CA

[14] Repenning, A., loannidou, A., "Broadening participation through scalable game design ", ACM SIGCSE Bulletin, v.40 n.1, March 2008

[15] Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E., "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish, " Symposium on Usable Privacy and Security (SOUPS), 2007.

[16] Tobey, D. H., Pusey, P. and Burley, D. L., Engaging Learners in Cybersecurity Careers: Lessons from the Launch of the National Cyber League. ACM Inroads 5, 1 (2014), 53–56.

[17] Williams, L., Meneely, A. and Shipley, G., "Protection Poker: The New Software Security 'Game', " IEEE Security & Privacy, vol. 8, no. 3, 2010, pp. 14–20.

[18] Zhang, J., Yuan, X., Johnson, J., Xu, J., Vanamala, M., "Developing and Assessing a Web-Based Interactive Visualization Tool to Teach Buffer Overflow Concepts", FIE 2020, October 21-24, Uppsala, Sweden.

[19] Silowash, G., Cappelli, D., Moore, A., Trzeciak. R., Shimeall, T.J., Flynn, L., "Common Sense Guide to Mitigating Insider Threats", 4th Edition, CMU/SEI-2012-TR- 012, 2015.

[20] Verizon 2014 Data Breach Investigations Report (DBIR, 2014), http://www.verizonenterprise.com/DBIR/2014/, 2014. Retrieved from URL.