An Interactive Visualization Tool for Teaching ARP Spoofing Attack

Brandon Scott[1], Jinsheng Xu[2], Jinghua Zhang[3], Ariana Brown[2], Erica Clark[2], Xiaohong Yuan[2], Anna Yu[2], Kenneth Williams[2]

[1]John Hopkins University of Applied Physics Laboratory
Laurel, MD, USA
brandon.scott@jhaupl.edu

[2]Department of Computer Science
North Carolina A&T State University
Greensboro, NC, USA
{jxu, xhyuan, cshmyu, williams, asbrown10, edclark1}@ncat.edu

[3]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 according to the Verizon's Data Breach Investigations Report. Address Resolution Protocol (ARP) is often exploited by the attackers who have gained access to the LAN. It is critical for students to learn how attacks on ARP work and know the countermeasures. In an earlier work, authors developed a hands-on lab to help students learn how an ARP spoofing attack works by asking them to create and send attack packets. To enhance learning further, we present an interactive visualization tool that intuitively shows the effects of the ARP spoofing attack in real-time.**

The Hacker Graphical User Interface (HGUI) is an interactive visualization tool developed to assist students in learning how ARP Spoofing works. By modeling a controlled ARP Spoofing attack using virtual machines, we give students the ability to alter elements of the attack by interacting with the visualization. This tool was developed using Processing, an open source programming language used in many visual art communities. It runs on virtual machines installed with Kali Linux. This tool animates attack packets, normal packets, and the status of ARP cache in real-time. If students have successfully carried out the ARP spoofing attack, they can see the normal packets being routed to the attacker machine and the victim's ARP cache being poisoned. In this paper, we present the design, implementation, and evaluation of the lab. Tests were conducted to measure the performance of students before and after using this tool. We also gave students surveys after they completed the hands-on lab. The result shows that this tool can significantly enhance students' understanding of the concept of ARP spoofing attacks and motivate them in learning more about cyber security.

Keywords—Course Module; Computer Science; Cyber Security; Hands-On Lab; Visualization; Local Area Network; ARP Spoofing; Man-In-The-Middle

I. INTRODUCTION

A recent study by Verizon's Data Breach Investigations Report, states that local area network (LAN) access is the top vector for insider threats and misuses [5]. This is not surprising because LAN protocols have many vulnerabilities and most of them are very easy to exploit. 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, which include static ARP cache entries, improved ARP module in operating systems, encryption, access control, intrusion detection, and data backup.

Previously, we have developed a visual simulation tool for attacks on LAN [2]. Users can select several Man-In-The-Middle attacks including ARP spoofing, Switch Port Stealing, and Switch Port Flooding attacks and see how these attacks work with animation. Visualization and simulation can help students learn security concepts by letting them see the dynamics of changes in data structures that exist inside computers and networks. However, it lacks realness and therefore is less convincing, resulting in a lack of enthusiasm from students. Later, we developed a hands-on lab that carries out real-world ARP spoofing attacks [1]. This lab can let students enjoy the excitement of successful real-world attacks. Due to the lack of visualization components, students may not clearly understand the internal dynamics of such attacks.

There are many organizations using visualization tools to better understand real-time cyber-attacks. The Kaspersky Lab created an interactive cyber threat map that provides a real-time outlook on various cyber security incidents happening worldwide. These threats range from online scanning, detection of email and web antiviruses and other threats detected by vulnerability and intrusion detection sub-systems [6]. The Norse Intelligence Service provides another example of utilizing visual information to display attacks. This was accomplished by using over eight million sensors that mimic different applications such as laptops, ATM machines, and TV cameras to gather data on various attacks around the globe [7].

This project aims to be an aide in teaching students the inner workings of a cyber-attack. If the visualization is interactive, it could strengthen a student's learning by reinforcing the visuals with a kinesthetic hands on approach. What makes this project unique is the fact that it will also allow students to experiment and alter a real and controlled cyber-attack through the visualization.

In this paper, we present an educational tool that combines real-world ARP spoofing attack with visualization. Although, an ARP spoofing attack can be carried out by this tool, other

978-1-5090-5920-1/17/$31.00 ©2017 IEEE

tools such as Cain and Abel [8] and Ettercap [9] can also be used to send ARP spoofing packets. Through this tool students can see the effects of ARP spoofing attack on victim's ARP cache in real time. It also visualizes various types of packets being transmitted in real-time. A course module including a lab, a manual, and a quiz will be presented in this paper.

We studied and analyzed the effectiveness of this lab on students' understanding of LAN vulnerabilities. Tests were conducted to measure the performance of students before and after using this tool. Surveys were also provided to the students after completing the hands-on lab. We will summarize the details of our findings further in this paper. This hands-on lab will also be available online to the educational community.

The following sections will introduce our background research, the development of the lab, and the evaluation of our results.

II. Background

A. Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) defined by RFC 826 [10] is a network protocol that resolves network layer addresses (e.g. IP address) into link layer addresses (e.g. MAC address). The ARP is a request and reply protocol and its range is within the boundaries of a single physical network [11]. The ARP request includes the IP address of the destination that the sender needs to resolve into the MAC address. This request is broadcasted to the entire physical network. The computer with the matching IP address will send an ARP reply message that includes its own MAC address back to the sender. The knowledge of the mapping from IP to MAC address will be stored in ARP cache. The operating system checks ARP cache and sends an ARP request message only when the entry for the destination IP does not exist.

B. ARP Spoofing Attack

ARP Spoofing attack, also called ARP Cache Poisoning, is a method by which the attacker sends a spoofed ARP message to the Local Area Network [12]. ARP is a stateless protocol, in which the receiver of ARP reply automatically saves the mapping into the ARP cache without even requesting it. Any attacker connected to the LAN can send a spoofed ARP reply message to the victim with its own MAC address associated with the IP address of the target host. Any traffic from the victim to the target will be directed to the attacker. If the target host is the router and the attacker also sends a spoofed ARP reply message to the router with its own MAC address associated with the IP address of the victim, then the attacker can potentially become the Man-In-The-Middle between the victim and all its Internet traffic.

C. ARP Spoofing Tools and Defense

There are many tools that can carry out ARP spoofing attacks: Cain and Abel [8] and Ettercap [9] are considered two of the most frequently used and they are listed as the most popular network security tools by SecTools.org [13]. Cain and Abel was developed to crack a Windows password. Ettercap is developed for Man-In-The-Middle attacks. Both have numerous features and both include an ARP spoofing attack feature. Although, it is easy to carry out ARP spoofing attack using these tools, the details of the attack is hidden from the users.

There are several ways of defending against ARP spoofing attacks. An easy solution is to make static ARP cache entries. This method, however, does not work well when the network is dynamic where hosts join and leave the network often. Another approach is to make ARP software secure in the operating systems. For example, operating systems can ignore unsolicited ARP replies. There are also tools available that detects ARP spoofing attacks by monitoring the change in the mapping of the IP address and MAC address.

III. Developing the Tool

A. Architecture

We call this tool the Hacker Graphical User Interface (HGUI). Fig.1 shows the architecture of the tool. At center, we have visualization module that interacts with users and controls other virtual machines, which can include multiple attackers and victims. Attacker and victim virtual machines send real-time data to the visualization module, which parses and visualizes the data in addition to sending commands to the attacker virtual machines to let them select targets to attack and start or stop the ARP spoofing attack. The system consists of one visualization virtual machine, one or more attacker virtual machines, and one or more victim virtual machines. All the attacker and victim virtual machines register with the visualization virtual machine. After the initial setup, users will only need to interact with the visualization virtual machine to carry out the remaining tasks. To make the process convenient, we made a single virtual machine that will be the visualizer, the attacker, or the victim.

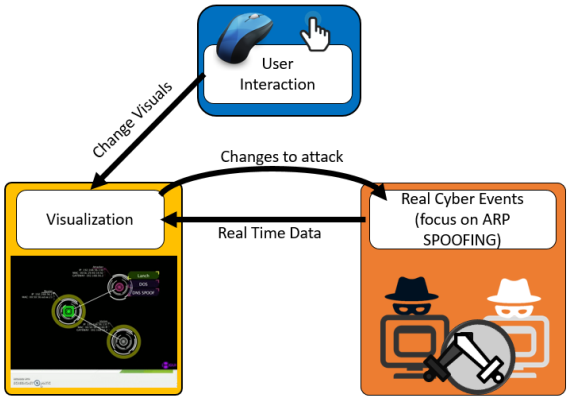

Fig. 1. The architecture of HGUI

B. Technologies Used

We used a tool called Processing to create visualizations. Processing is a flexible software sketchbook and a language for learning how to code within the context of the visual arts [14]. To create the controlled ARP Spoofing attack, a Kali Linux [15] virtual machine (a distribution of Linux used for

penetration testing) was used. Kali Linux has built-in commands that can perform ARP spoofing attacks. VirtualBox is used to run the virtual machines. Lastly, different technologies such as Apache servers, C++, PHP, HTTP, and several Linux commands and scripts were used to send data back and forth between the visualization and the virtual machines. These technologies are summarized in Fig. 2.

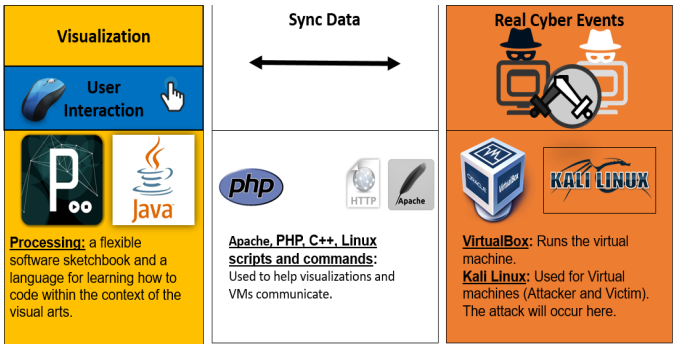

Fig. 2. Technologies used in HGUI

C. *Items to Visualize*

We want to visualize the most important items in an ARP spoofing attack. The devices that are involved in such an attack includes a router, switch, attacker, and victim. HGUI displays the IP addresses and MAC addresses of these devices (except for the switch). It also displays the contents of ARP cache of the attacker and the victim. In addition, packets moving through the network from device to device are also animated. Fig. 3 depicts the items. From top left to top right, the router, switch, attacker, and victim are represented by colored nodes with images. Packets, which are essential to the attack can be represented by colored arrows moving from node to node.

Fig. 3. Devices and Packets in HGUI.

Fig. 4 displays a typical network in HGUI, which includes a victim, attacker, and router, all connected by white lines to a switch. By clicking on these nodes students can see their expanded forms, which include a combination of their IP address, MAC address, and the IP address of gateway. An ARP table, which contains the mapping from IP addresses to MAC addresses on each row, are also shown in the expanded form of the attacker and victim. These ARP tables only include the IP addresses of the other visualized nodes in the network.

The attacker and victim virtual machines are not only broadcasting their ARP tables and IP addresses, but also all of the packets that flow to and from it. These packets are associated with their own color. Referring to the packet color legend, students will be able to determine what type of traffic from which they belong. By adjusting the packet speed slider to slower speeds, students can see additional color coded information about the packet.

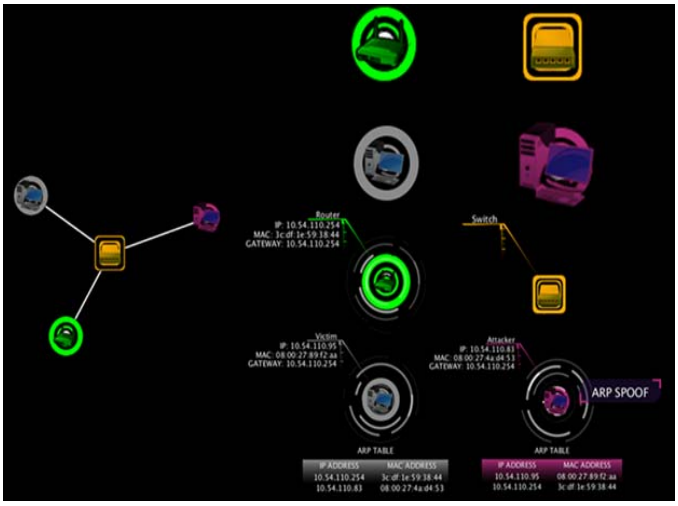

Fig. 4. A typical network in the visualization involving the victim, switch, attacker, and router

D. *ARP Spoofing Attack*

The attacker node has a button that allows the user to perform ARP Spoofing. After clicking this button, the info box will change to give students further instructions about the attack. In this case, the info box is telling the user to select two victims to perform a Man-In-The-Middle attack on. To intercept all the Internet traffic of a victim, students should select the victim's virtual machine and the router as two victims. After the user has selected two victims, an option is given to launch the attack, which when pressed, sends a command to the virtual machine which will perform the attack. Lastly, after the attack has started, an option to stop the attack is given. Fig. 5 illustrates the screenshots before and after the ARP spoofing attack.

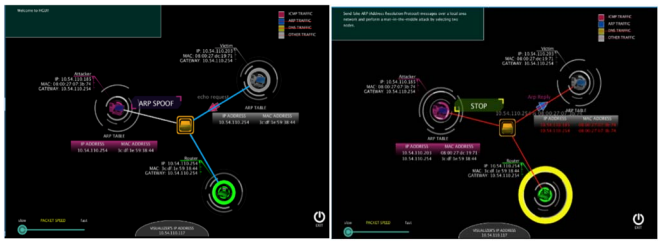

Fig. 5. Screenshots of HGUI before and after the attack

IV. Designing and Evaluating the Lab

A. Lab Desgin

This hands-on tool was first developed in 2016 by the Department of Computer Science at North Carolina A&T State University to allow students to gain hands-on experience and increase student interest and confidence in Cyber Security knowledge and skills. We have designed a corresponding lab associated with this tool. The components of the lab contains this tool, manual of the tool, a step by step demonstration, lab problems, and a quiz. This lab can be used as a two-hour lab session or as a homework assignment. Fig. 6 shows the lab questions students were required to answer and Fig. 7 shows the quiz questions related to ARP spoofing attacks.

1. **Answer the following questions:**
   a. What are the IP address and MAC addresses of the Attacker, Victim, and Router?
   b. Print all entries of ARP cache table in the Victim before the attack.
   c. Print all entries of ARP cache table in the Victim after the successful attack.
   d. What values has changed from step b to step c? Explain the impact of the change.
   e. Use Wireshark to capture the ARP spoofing packets sent by the attacker. List all the fields in the ARP spoofing packets.
2. **Start the ARP spoof attack on the visualizer then Launch a browser from the victim and visit a popular website and answer the following questions**
   a. Did the web page load on the victim's browser?
   b. Create a screenshot that shows the traffic of the website is being captured by the attacker. Explain what happened to the traffic.
   c. What happens if the attacker stopped ARP Spoofing attack? Go to another website. Does it still go to attacker? Create screenshots that shows what happened to the traffic.
3. **Launch another HGUI VM and make it an attacker. Let this attacker attack the same victim. Answer the following questions:**
   a. Did both attackers get all the traffic of the victim?
   b. Launch Wireshark on the attackers to verify your answer in step a.
   c. Explain the result you get from step b and step c.

Fig. 6. Lab Questions

1. ARP protocol resolves _____.
   A. IP address from domain name
   B. A domain name from IP address
   C. MAC address from IP address
   D. IP address from MAC address

2. On Ethernet, what should be the destination MAC address of an ARP Request?
   A. 255.255.255.255
   B. ff:ff:ff:ff:ff:ff
   C. 192.168.0.1
   D. 00:00:00:00:00:00

3. In ARP spoofing attack, to intercept the traffic from the victim to the Internet, the attack should _____.
   A. Poison the router's ARP cache
   B. Poison the victim's ARP cache
   C. Poison the attacker's ARP cache
   D. Poison the switch's ARP cache

4. In ARP spoofing attack, to intercept the traffic from the Internet to the victim, the attack should _____.
   A. Poison the router's ARP cache
   B. Poison the victim's ARP cache
   C. Poison the attacker's ARP cache
   D. Poison the switch's ARP cache

5. Which of the following is the best counter measure against ARP Spoofing attack?
   A. Upgrade Ethernet hubs to switches
   B. Set important entries in ARP cache static.
   C. Upgrade to wireless Ethernet
   D. Use firewall to block ping requests

Fig. 7. Quiz Questions

B. Evaluations

We used this lab in a Computer Networks class during the Spring of 2017. There were eleven total participating students. Students had a lecture on ARP before the two-hour lab session. In the first lab session, students were given the quiz questions before teaching assistants helped students set up the lab and finished a step-by-step demonstration of the tool. Then, students were asked to independently finish the lab questions. Ten minutes before the lab ended, we gave post lab quizzes and surveys. The pre-lab and post-lab quiz performance for each student is shown in Fig. 8. Seven out of eleven students showed big improvements in their scores. The scores for three students remained unchanged. For some reason, one student performed better in the pre-test. Overall the results are promising. Table I shows the summary of the quiz evaluation. The average of the pre-lecture is 2.82 and the average of the post-lab quiz is 3.91. The p-value of two-tailed paired t-test is 0.01421, showing statistically significant improvement from pre-lab to post-lab.

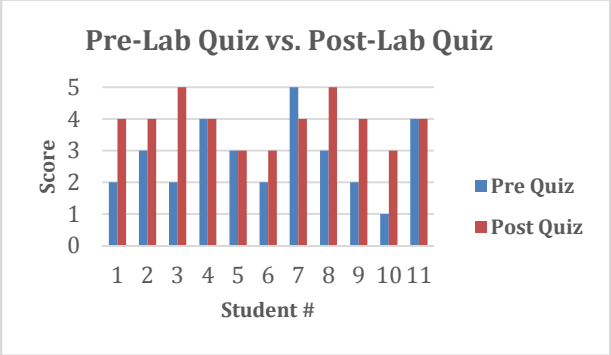

Fig 8. Pre-Lab Quiz vs. Post-Lab Quiz

TABLE I. SUMMARY OF QUIZ EVALUATIONS

Average of Pre-Lab Quiz	2.82
Average of Post-Lab Quiz	3.91
Two tailed p-values of t test	0.01421

C. Survey

After successful completion of the pre-quiz, lab and post-quiz we conducted a survey of four questions. The answer to each survey question ranged from 1 to 5. With 1 being the least effective and 5 being the most effective. The mean score of students' opinion on the worthwhileness of the lab is 4.42 with standard deviation of 0.67. The mean score of the students' opinion on the quality of organization of the lab is 4.17 with standard deviation of 0.94. When asked about their motivation on learning network security, students gave mean score of 4.08 with standard deviation of 0.99. The mean score of students' opinion on the usefulness of the lab in learning ARP spoofing is 4.67 with standard deviation of 0.65. Overall, students thought positively about the lab. The organization of the lab can be improved based on the experiences gained from previous experiments.

V. CONCLUSIONS

In this paper, we introduced an interactive visualization tool for learning ARP spoofing attacks and presented our evaluation results. The results show that this tool was very helpful to students in learning this topic and motivated them in learning more on related topics. This hands-on tool will be made available at: http://williams.comp.ncat.edu/IA_visualization_labs/.

REFERENCES

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

[2] Baxley, T., Xu, J., Yu, H., Yuan, X., Brickhouse, "LAN Attacker: A Visual Education Tool", Proceedings of 2006 Information Security Curriculum Development Conference, 2006.

[3] Yu H., Williams K., Xu J., Yuan X., Chu B., Kang. B., Kombol, T., "Interactive Simulation Tools for Information Assurance Education", Proceedings of the Second Annual Conference on Education in Information Security (ACEIS 2009), 2009.

[4] Silowash, G., Cappelli, D., Moore, A., Trzeciak, R., Shimeall, T.J., and Flynn, L. "Common Sense Guide to Mitigating Insider Threats", 4th Edition, CMU/SEI-2012-TR- 012. Retrieved on March 23, 2015 from http://resources.sei.cmu.edu/asset_files/TechnicalReport/2012_005_001_34033.pdf.

[5] Verizon 2014 Data Breach Investigations Report (DBIR, 2014), Retrieved on March 23, 2015 from http://www.verizonenterprise.com/DBIR/2014/

[6] Real Threats in Real Time: Kaspersky Lab Launches Worldwide Interactive Cyberthreat Map, Retrieved on April 21, 207 from https://usa.kaspersky.com/about/press-releases/2014_real-threats-in-real-time-kaspersky-lab-launches-worldwide-interactive-cyberthreat-map

[7] Norse Attack Map, Retrieved on April 21, 207 from http://map.norsecorp.com/

[8] Cain & Abel, Retrieved on April 23, 2016 from http://www.oxid.it/cain.html

[9] Ettercap, Retrieved on April 23, 2016 from https://ettercap.github.io/ettercap/

[10] David C. Plummer (November 1982). "RFC 826, An Ethernet Address Resolution Protocol -- or -- Converting Network Protocol Addresses to 48.bit Ethernet Address for Transmission on Ethernet Hardware". Internet Engineering Task Force, Network Working Group.

[11] Address Resolution Protocol, Retrieved on April 23, 2016 from https://en.wikipedia.org/wiki/Address_Resolution_Protocol

[12] ARP Spoofing, Retrieved on April 23, 2016 from https://en.wikipedia.org/wiki/ARP_spoofing

[13] Top Network Security Tools, Retrieved on April 23, 2016 from http://sectools.org/

[14] Processing is a flexible software sketchbook and a language for learning how to code within the context of the visual arts, Retrieved on April 21, 2017 from https://processing.org/

[15] Kali Linux | Penetration Testing and Ethical Hacking Linux Distribution, Retrieved on April 21, 2017 from https://www.kali.org/

[16] Wireshark, Retrieved on April 23, 2016 from, https://wireshark.org