Kennesaw State University
DigitalCommons@Kennesaw State University

KSU Proceedings on Cybersecurity Education, Research and Practice

2018 KSU Conference on Cybersecurity Education, Research and Practice

Oct 20th, 10:30 AM - 10:55 AM

Evaluating Two Hands-On Tools for Teaching Local Area Network Vulnerabilities

Ariana Brown
North Carolina A&T State University, asbrown10@aggies.ncat.edu

Jinsheng Xu
jxu@ncat.edu

Xiaohong Yuan
North Carolina A & T State University

Brown, Ariana; Xu, Jinsheng; and Yuan, Xiaohong, "Evaluating Two Hands-On Tools for Teaching Local Area Network Vulnerabilities" (2018). *KSU Proceedings on Cybersecurity Education, Research and Practice*. 2.
https://digitalcommons.kennesaw.edu/ccerp/2018/education/2

Abstract
According to the Verizon's Data Breach Investigations Report, Local Area Network (LAN) access is the top vector for insider threats and misuses. It is critical for students to learn these vulnerabilities, understand the mechanisms of exploits, and know the countermeasures. The department of Computer Science at North Carolina A&T State University designed two different educational tools that help students learn ARP Spoofing Attacks, which is the most popular attack on LAN. The first tool, called Hacker's Graphical User Interface (HGUI), is a visualization tool that demonstrates ARP Spoofing Attack with real time animation. The second tool is a hands-on (HandsOn) tool that asks students to perform an ARP Spoofing Attack by manually creating ARP reply packets. It was demonstrated in previous research that both tools enhanced students' learning.

In this paper, we are going to scientifically evaluate and compare the effectiveness of these two tools. We divided the class of forty-five students randomly into two groups. Group A was assigned HGUI lab and the Group B was assigned the HandsOn lab. The labs were assigned as a one and half week homework assignments. Both groups were given a pre-survey and a pre-quiz before the lab. After they submitted the lab, we gave them a post-survey and a post quiz. The analysis shows that prior to the labs, students in both groups have almost identical background in the knowledge of ARP Spoofing. After the lab, both groups made statistically significant improvements. Although group A did better on survey and group B did better on quiz, it is not statistically significant enough to draw a definitive conclusion according to the student's t-test result. Also, in analyzing survey results, we found that actively reading cyber security related articles is a more significant contributing factor in students' knowledge in the subject matter than other factors including having formal training or taking cyber security classes.

Location
KC 400

Disciplines
Educational Methods | Higher Education | Information Security | Technology and Innovation

INTRODUCTION

Local area network (LAN) access is the top vector for insider threats and misuses by a recent study by Verizon's Data Breach Investigations Report (Verizon 2014). This is not surprising because LAN protocols have many vulnerabilities and most of them are very easy to exploit. Using 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, North Carolina A&T State University's Computer Science Department developed a visual simulation tool that demonstrates attacks on LAN (Baxley et al., 2006). 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. Several tools exist that can do actual ARP spoofing attacks. However, the technical details are hidden from the users. For example, "Cain & Abel" implements APR (ARP Poison Routing) which enables Man-In-The-Middle attacks to be carried out easily on switched networks. However, students cannot learn the details of becoming Man-In-The-Middle which include poisoning the router's ARP table, poisoning the victim's ARP table and forwarding the packets between the router and the victim.

In this paper, we present two tools that will assist students with learning about ARP spoofing attacks. Tool A is the Hacker Graphical User Interface or HGUI. The purpose of HGUI is to utilize visualization to illustrate an ARP spoofing attack (Scott et al., 2017). 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. Tool B is a hands-on lab used to help student learn how ARP poisoning attack works (Xu et al., 2016). The goal of this lab is to let students successfully become a Man-In-The-Middle and understand vulnerabilities in LAN. This lab will ask students create Ethernet frames that do ARP poisoning attack. One of the frames will poison the ARP cache of the victim while the other one poisons the ARP cache of the router. Students also need to set up the IP forwarding between the router and the victim to successfully capture the whole traffic session. Students will have to manually enter all fields of an ARP Reply packet.

In the past, both of the tools were tested separately in different classrooms and different semesters. The HandsOn tool has been used as a homework assignment for the Network Security course for the past three years. The HGUI tool was first tested in a classroom in the Computer Networks course in the spring of 2016 (Xu et al., 2016). Although, it was reported that both of these tools enhanced students' learning, the evaluation was carried out on small sample sizes without rigorous analysis. Because HGUI is focused on using visualization and GUI while HandsOn tool is based on manually creating ARP Spoofing frames with command line, it is interesting to compare pros and cons of these tools in a common setting. The evaluation result can give insight on how to create and improve educational tools.

In this paper, we are going to evaluate and compare these two tools in large classroom setting and evaluate them scientifically. The following sections introduce related work, the development of the lab, the evaluation results, and the conclusions.

RELATED WORK

As the world of computer security continues to evolve, there's a strong need for more security professionals who are knowledgeable in the field. While this demand begins to increase, so does the expectation of delivering more hands-on exercises in the classroom, which explains why many universities have created and added more interactive tools to their curriculum. For instance, the Department of Technology at UAE University developed a hands-on lab exercise that focuses on Min-in-the-middle and DoS attacks using ARP cache poisoning (Trabelsi 2011). Between 2006 and 2008 this lab was not offered to students who were enrolled in the course. They began incorporating the hands-on portion beginning in the fall of 2008. During all years the course was offered students completed quizzes that were closely correlated with ARP cache poisoning. Starting with the fall of 2008 class, overall grade averages began improving in comparison to previous classes who didn't have the ability to participate in the hands-on exercises. Vigna (2003) offered a hands-on environment for students to gain the necessary skills for attack prevention and defense by utilizing network testbeds. This lab was tested on a graduate-level Network Security and Intrusion detection course at the University of California, Santa Barbara. The testbeds were created with ten hosts and multiple operating systems. Once created, the students were given the opportunity to experiment with various types of attacks and defense techniques during an instructional educational activity. Murph (2009) developed experiments using different tools in order to educate and give students more hands-on experience. The security experiments and tools included steganography, windows password hashes, MBSA, Security Cookies and History, PGP, Nessus, Nikto, and Phishing.

Other institutions have also used games as a means of adding an interactive approach to learning. The Naval Postgraduate School created CyberCIEGE, which is an active learning video game that reinforces lectures and materials that have been taught in an introduction to computer security course (Thompson & Irvine, 2011). The game consists of more than twenty scenarios that covers multiple computer and network security topics. Instructors are even given the ability to create and customize scenarios in the game as well. While playing the game students can experience attacks such as trojan horses, trap doors, insiders, configuration errors, unpatched software flaws, weak procedural policies, and poorly trained users. D'Apice, Claudia, Rossella, Luca (2015) introduced a security video game called SIRET Security Game. In the game, a player portrays the role of an employee at an organization who has to defend the company's data from adversaries and spies. There are a series of missions to be completed in order to become a Computer Security Officer in the game. They used surveys to determine how effective the games were. Craig, Knapp, Mitchell, Claypool, and Fisler (2011) presented a game-type environment for practicing and learning security skills called CounterMeasures. CounterMeasures is a single player game that consists of various missions that teaches different security concepts. They gave students a preliminary questionnaire that tested their basic computer security knowledge before and after they played the game.

Japan Advanced Institute of Science and Technology created a cyber range that is able to provide the tools necessary for deep learning on IT security (Pham, Tang, Chinen, and Beuran, 2016). The name of their tool is Cyber Range Instantiation System (CyRIS). CyRIS is an instantiation system that creates and manages environments used for cyber security training courses. In order to utilize CyRIS instructors created a definition of their desired training content. CyRIS will take the instructors file submission and create the desired environment. Du et. al. and Kaabi et. al. created tools that enabled students to have access to different labs in one place while allowing instructors to choose the content they are focusing on. Syracuse University developed a laboratory environment called SEED (SEcutiry Education) (Du and Wang 2008). The SEED environment uses Minix and Linux to provide a platform for the labs. These labs cover a large spectrum of security principles so that students can develop essential computer security principles. The labs the have been implemented in the SEED environment are divided into three classes: design implementation labs, exploration labs, and vulnerability labs. The College of Information Technology at UAE University created an educational platform that depicts a denial of service attack called DoS_Lab (Kaabi, Kindi, Fazari, and Trabelsi 2016). DoS_Lab allows students to interact with a graphical user interface that provides different hands-on labs that are associated with DoS attacks.

Our work is focused on teaching how ARP spoofing works with two different tools and compare how their impact on students' learning outcomes.

EDUCATIONAL TOOLS

In this section, we introduce two education tools we have developed. They are Hands-On ARP Spoofing tool and HGUI.

Hands-on ARP Spoofing Learning Tool

We have developed programs with which students are asked to carry out a successful Man-In-The–Middle attack on a switched network. The first program, named “sendarp”, is programmed to send an arbitrary ARP reply message. Students are asked to provide such information as MAC addresses of the source and the target in ARP reply message, IP addresses of the source and the target in ARP reply message, and destination and source MAC addresses in the Ethernet frame header. Students cannot carry out successful attack without clear understandings of Ethernet frames, ARP message format, and ARP poisoning attack. This program needs to be executed twice to poison both the router and the victim. To increase the chance of success, the program repeatedly sends the ARP reply message with fixed time intervals. This program was developed on Windows with WinPcap library. The source code is included in the provided virtual machine.

The second program, named “mim”, forwards the packets between the router and the victim. To become a successful Man-In-The-Middle without being detected by the victim, the attacker must forward the intercepted packet either to the victim or to the router and let victim continue communicating without interruption. This tool dumps the intercepted traffic into a file in tcpdump format which can later be viewed using Wireshark or other packet analyzers. This program asks students under which condition a packet should be forwarded to the router or the victim. Students need to know the format of the IP datagrams intercepted by the attacker to correctly forward the packets.

To assist the lab, we developed a shell script that runs on the victim and constantly contacts a web server that computes a simple mathematical function on the random number sent by the victim. Students need to intercept enough traffic to successfully guess the function computed by the web server.

Figure 1 shows the architecture of the Hands-On lab. This tool can be used in a lab setting where a group of students can work on the ARP spoofing attack at the same time. Multiple identical attacking virtual machines are connected to the same LAN. These virtual machines are used by students to carry out ARP spoofing attacks. The rest of the virtual machines are used as victims, which constantly generates traffic for students to capture. Alternatively, students can manually generate traffic from the victim to verify if this traffic can be intercepted by the attacking virtual machines. In each of the virtual machines, “sendarp” and "mim" and Wireshark are installed. We also included the source code for "sendarp" and "mim" in the virtual machine.

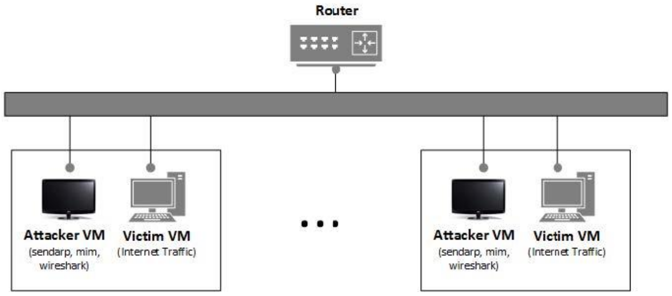
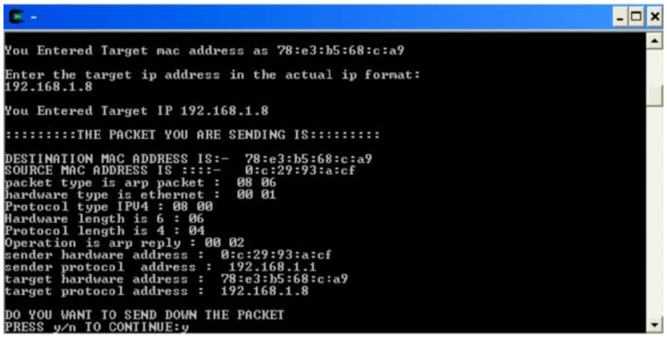


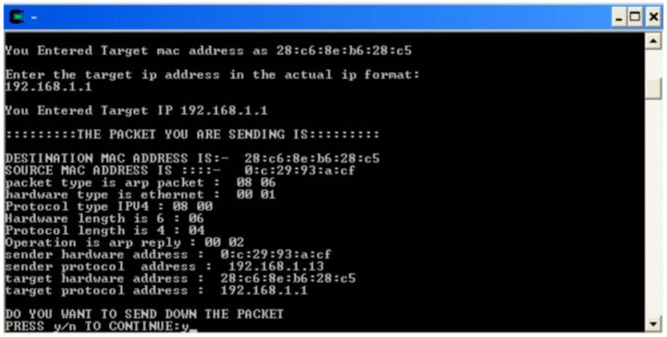
Figure 1. The architecture of Hands-On Lab

Figure 2 shows the screenshot of a successful ARP spoofing attack on the victim with the "sendarp" program. The attacker sends ARP reply message to the victim 78:e3:b5:68:0c:a9 (192.168.1.13) with its own MAC address associated to the router's IP address 192.168.1.1. Figure 3 shows the screenshot of a successful ARP spoofing attack on the router with the "sendarp" program. The attacker sent an ARP reply message to the router 192.168.1.1 with its own MAC address associated to the victim's IP address 192.168.1.13. Please note that in Figure 2, the target protocol address is set to 192.168.1.8, which is not the same as the victim's IP address 192.168.0.13. Nevertheless, the victim accepted this and updated its ARP cache with the spoofed MAC address of the router. This shows that ARP module in the victim's machine does not even check that ARP reply is targeted to itself. After these two steps, both the victim and the router have spoofed MAC addresses for each other in their ARP caches. All the traffic from the victim to the Internet and from the Internet to the victim will be sent to the attacker. To become Man-In-The-Middle and continuously monitor the traffic between the victim and the Internet, the attacker needs to use "mim" program to behave as a router by doing IP forwarding.



```
You Entered Target mac address as 78:e3:b5:68:c:a9

Enter the target ip address in the actual ip format:
192.168.1.8

You Entered Target IP 192.168.1.8

:::::::::THE PACKET YOU ARE SENDING IS:::::::::

DESTINATION MAC ADDRESS IS:-  78:e3:b5:68:c:a9
SOURCE MAC ADDRESS IS ::::-   0:c:29:93:a:cf
packet type is arp packet :  08 06
hardware type is ethernet :  00 01
Protocol type IPV4 : 08 00
Hardware length is 6 : 06
Protocol length is 4 : 04
Operation is arp reply : 00 02
sender hardware address :  0:c:29:93:a:cf
sender protocol  address :  192.168.1.1
target hardware address :  78:e3:b5:68:c:a9
target protocol address :  192.168.1.8

DO YOU WANT TO SEND DOWN THE PACKET
PRESS y/n TO CONTINUE:y
```

Figure 2. Screenshot of ARP spoofing attack on victim with sendarp program



```
You Entered Target mac address as 28:c6:8e:b6:28:c5

Enter the target ip address in the actual ip format:
192.168.1.1

You Entered Target IP 192.168.1.1

:::::::::THE PACKET YOU ARE SENDING IS:::::::::

DESTINATION MAC ADDRESS IS:-  28:c6:8e:b6:28:c5
SOURCE MAC ADDRESS IS ::::-   0:c:29:93:a:cf
packet type is arp packet :  08 06
hardware type is ethernet :  00 01
Protocol type IPV4 : 08 00
Hardware length is 6 : 06
Protocol length is 4 : 04
Operation is arp reply : 00 02
sender hardware address :  0:c:29:93:a:cf
sender protocol  address :  192.168.1.13
target hardware address :  28:c6:8e:b6:28:c5
target protocol address :  192.168.1.1

DO YOU WANT TO SEND DOWN THE PACKET
PRESS y/n TO CONTINUE:y_
```

Figure 3. Screenshot of ARP spoofing attack on router with sendarp program

HGUI

Figure 4 shows the architecture of the tool. At center, we have visualization modules that interact 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 creates visuals of the data. The visualization module also sends 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 of 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 it convenient, we made a single virtual machine that will be the visualizer, the attacker, or the victim.

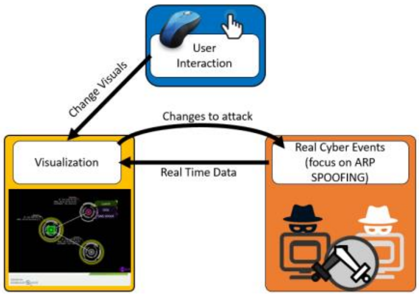
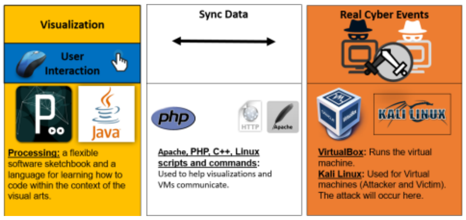


Figure 4. The architecture of HGUI

We used software 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 (Processing.org). To create the controlled ARP Spoofing attack, a Kali Linux 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 VMs. These technologies are summarized in Figure 5.



Processing: a flexible software sketchbook and a language for learning how to code within the context of the visual arts.

Apache, PHP, C++, Linux scripts and commands: Used to help visualizations and VMs communicate.

VirtualBox: Runs the virtual machine.
Kali Linux: Used for Virtual machines (Attacker and Victim). The attack will occur here.

Figure 5. Technologies used in HGUI

We want to visualize the most important items in an ARP spoofing attack. The devices that are involved in an ARP spoofing attack includes 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. Figure 6 depicts the items to visualize in the HGUI. 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.

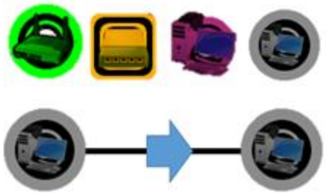
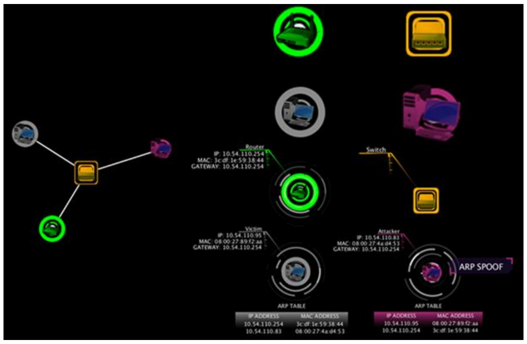


Figure 6. Devices and Packets in HGUI.

Figure 7 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, you can see their expanded forms, which include a combination of their IP address, MAC address, and IP address of gateway. An ARP table, which is a table linking 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, you will be able to determine what type of traffic from which they belong. By adjusting the packet speed slider to slower speeds, you can also see additional color coded information about the packet.



Router
IP: 10.54.110.254
MAC: 3c:df:1e:59:38:44
GATEWAY: 10.54.110.254

Switch

Victim
IP: 10.54.110.95
MAC: 08:00:27:89:f2:aa
GATEWAY: 10.54.110.254

Attacker
IP: 10.54.110.83
MAC: 08:00:27:4a:d4:53
GATEWAY: 10.54.110.254

ARP TABLE

IP ADDRESS	MAC ADDRESS
10.54.110.254	3c:df:1e:59:38:44
10.54.110.83	08:00:27:4a:d4:53

ARP TABLE

IP ADDRESS	MAC ADDRESS
10.54.110.95	08:00:27:89:f2:aa
10.54.110.254	3c:df:1e:59:38:44

Figure 7. A typical network in the visualization involving the victim, switch, attacker, and router

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 you further instructions about the attack. In this case, the info box is telling the user to select two victims to successfully perform a Man-In-The-Middle attack on. To intercept all the Internet traffic of a victim, students should select 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. Figure 8 illustrates the screenshots before and after the ARP spoofing attack.

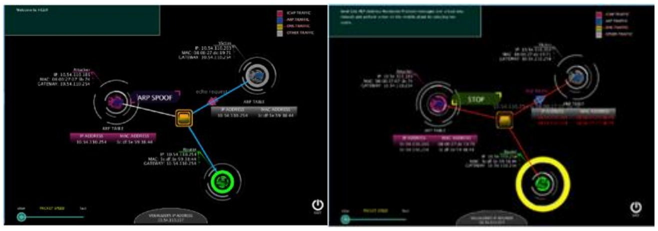
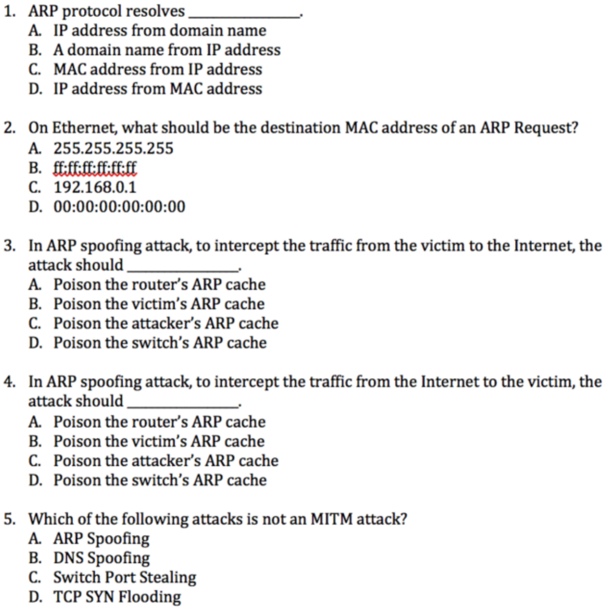


Figure 8. Screenshots of HGUI before and after the attack

EVALUATING THE TOOLS

Evaluation Process

We evaluated these two labs on a Network Security class at North Carolina A&T State University, which includes both undergraduate and graduate students. There were 45 students in the class, among which, 22 students were assigned to group A, and 21 students were assigned to group B. Group A students were assigned the HGUI lab, group B students were assigned the HandsOn lab. Before the lab started, we gave them a pre-quiz and a pre-survey. All students were given one and a half weeks to complete the labs. A post quiz and a post survey were given after students turned in their assignment. The pre-quiz and post-quiz have the identical questions. It is shown in Figure 9.



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 attacks is not an MITM attack?
   A. ARP Spoofing
   B. DNS Spoofing
   C. Switch Port Stealing
   D. TCP SYN Flooding

Figure 9. Evaluation Quiz Questions

In the pre-survey, we asked students the following background questions: 1) Have you taken cybersecurity courses for academic credit? 2) Have you received formal training (e.g., workshops, certification training, etc.) on common cyber security practices? 3) How frequently do you read cybersecurity-related newsletters or articles? 4) Do you have other prior experience with cybersecurity than the above mentioned? 5) Are you interested in learning about various topics of cyber security? 6) Are you interested in pursuing a career in cyber security? We also asked their subjective opinion about knowledge on subject matter as follows: 1) Explain how ARP works; 2) Explain how packet sniffing works; 3) Explain Man-In-The-Middle Attacks; 4) Explain how ARP Cache Poisoning works; 5) Explain how ARP Spoofing works; 6) Explain how to prevent ARP Cache Poisoning.

In the post-survey, we asked the same questions on their subjective opinion of their knowledge on the subject matter. This allows us to evaluate how they feel about their knowledge gain before and after the labs. In addition we asked the following questions on the labs: 1) Was the course module useful to help you understand cyber security concepts? 2) Were the learning objectives of this course module met? 3) Was he level of difficulty of this course module appropriate? 4) Did you enjoy learning this course module? 5) Were the lab instructions clear? 6)

Approximately, how many hours did you spend on the lab? 7) Was the time you spent on the lab worthwhile? 8) Are you motivated to learn more about cyber security as a result of this course module? 9) Are you interested in pursuing a career in cyber security as a result of this course module? 10) What was the most important thing you learned from this course module? 11) What problems did you encounter in learning with this course module? 12) Provide general comments about this lab.

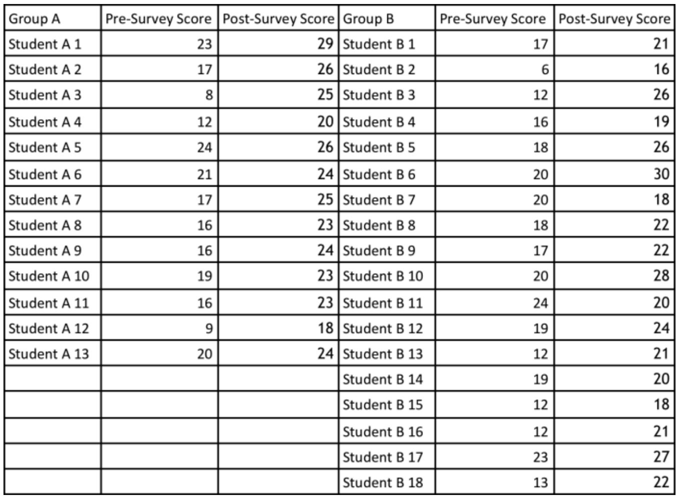
Evaluation Results

Because the surveys were voluntary, not all students turned them in. Some students only submitted their pre-survey while other students only turned in the post-survey. There were 13 students in group A and 18 students in group B, who turned in both pre-survey and post survey.

Students background before the labs

At the start of our analysis, we compared the two groups of students to determine if they had similar backgrounds before completing the labs. Because we randomly assigned students to two different groups and the samples were large enough, we had reason to believe students should have almost the same background knowledge on the subject matter before they started the lab.

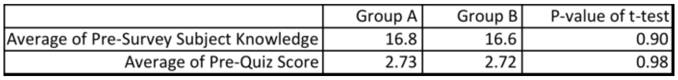
We compared students' subjective opinion on the subject matter in the pre-survey. Table 1 shows the survey results of groups A and B on the 6 subjective opinions of their knowledge on the subject matter respectively. The score of each question ranges from 1 to 5 with 1 meaning the minimum knowledge and 5 meaning the maximum knowledge. This tables shows the total scores students received on 6 subjective questions.



Group A	Pre-Survey Score	Post-Survey Score	Group B	Pre-Survey Score	Post-Survey Score
Student A 1	23	29	Student B 1	17	21
Student A 2	17	26	Student B 2	6	16
Student A 3	8	25	Student B 3	12	26
Student A 4	12	20	Student B 4	16	19
Student A 5	24	26	Student B 5	18	26
Student A 6	21	24	Student B 6	20	30
Student A 7	17	25	Student B 7	20	18
Student A 8	16	23	Student B 8	18	22
Student A 9	16	24	Student B 9	17	22
Student A 10	19	23	Student B 10	20	28
Student A 11	16	23	Student B 11	24	20
Student A 12	9	18	Student B 12	19	24
Student A 13	20	24	Student B 13	12	21
			Student B 14	19	20
			Student B 15	12	18
			Student B 16	12	21
			Student B 17	23	27
			Student B 18	13	22

Table 1. Pre and Post Survey Result of Subject Matter Questions for Group A and B

We also compared the pre-quiz scores for group A and group B. Table 2 shows the average of pre-survey scores and pre-quiz scores for both groups. The averages are very close for both groups. We calculated a two tailed t-test on the pre-survey and pre-quiz results. Hypothesizing that there is no significant difference between two groups in the knowledge of the subject matter. The p-value for pre-survey t-test is 0.90 and the p-value for pre-quiz t-test is 0.98. Both results strongly accept the null hypothesis.

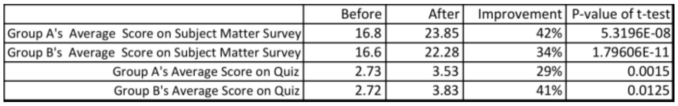


	Group A	Group B	P-value of t-test
Average of Pre-Survey Subject Knowledge	16.8	16.6	0.90
Average of Pre-Quiz Score	2.73	2.72	0.98

Table 2. Comparison of Group A and B Students

Improvement after the labs

Table 1 shows the post-survey result on the subject matter questions for group A and group B respectively. Both groups have improved significantly. Table 3 shows the comparison of improvements before and after the labs in survey and quiz results. Group A improved 42% in survey result; Group B improved 34% in survey result. Group A, who used the HGUI visualization tool seemed to feel they knew more about the subject matter than Group B students did. However, interestingly in the objective quiz results, group A improved 29% while group B who did HandsOn lab improved 41%. We calculated the t-test on all of the results with a null hypothesis that there was no significant change to students' performance before and after the labs. In all these cases, the p-value are extremely small, strongly rejecting the null hypothesis. Therefore, we can conclude that both labs have significantly improved students' knowledge in ARP Spoofing Attacks.

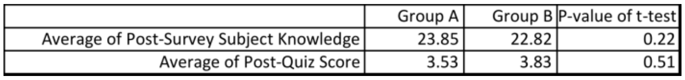


	Before	After	Improvement	P-value of t-test
Group A's Average Score on Subject Matter Survey	16.8	23.85	42%	5.3196E-08
Group B's Average Score on Subject Matter Survey	16.6	22.28	34%	1.79606E-11
Group A's Average Score on Quiz	2.73	3.53	29%	0.0015
Group B's Average Score on Quiz	2.72	3.83	41%	0.0125

Table 3. Comparison of Improvement before and after the labs

Evaluating which educational tool is more effective

In the previous section, we showed that both tools have significantly improved students' knowledge in ARP Spoofing. In addition, students who did the HGUI lab improved more on the subjective self-evaluation on the topic, while students who did the HandsOn lab improved more on the objective quiz scores. To determine if the differences were significant enough, we performed a t-test on the post-survey and post-quiz results. The null hypothesis for these tests was there is no significant difference in the performance of students in group A and group B after their respective labs. Table 4 shows that the p-value of the t-test for post survey results on group A and group B is 0.22; the p-value of the t-test for post quiz results on group A and group B is 0.51. These fairly large p-values suggest that the null hypothesis cannot be rejected. Therefore, we cannot definitively conclude which tool is superior by survey or quiz measures.

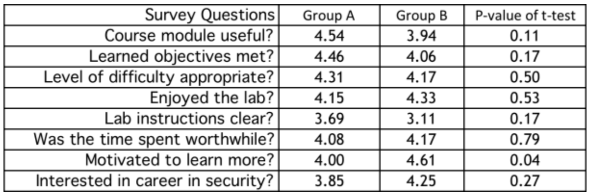


	Group A	Group B	P-value of t-test
Average of Post-Survey Subject Knowledge	23.85	22.82	0.22
Average of Post-Quiz Score	3.53	3.83	0.51

Table 4. Comparison of Improvement for Group A and B

Post-Survey Results

We analyzed the post-survey results for both groups. Each question has scores from 1 (strongly disagree) to 5 (strongly agree). Table 5 shows the results. For group A students, the best response came from the usefulness of the lab and the worst response came from the clearness of the lab instructions. Group B students also considered lab instructions were not clear enough. This result shows that we need to improve the lab instructions in the future. Group B's best response was the motivation to learn more about cyber security. We conducted the unpaired t-test to find out if difference in two groups' response to the same question is statistically significant. The smallest p-value (0.04) came from the question about the motivation to learn more about cyber security. Students in group B showed statistically significant better response to this question than students in group A. This is hard to explain because group B students considered their lab was less useful than group A students. More tests are needed in the future to confirm or deny this observation. Students' answers to other free response survey questions were very positive. Students also gave suggestions and bug reports.

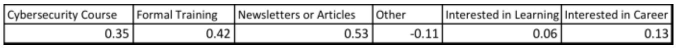


Survey Questions	Group A	Group B	P-value of t-test
Course module useful?	4.54	3.94	0.11
Learned objectives met?	4.46	4.06	0.17
Level of difficulty appropriate?	4.31	4.17	0.50
Enjoyed the lab?	4.15	4.33	0.53
Lab instructions clear?	3.69	3.11	0.17
Was the time spent worthwhile?	4.08	4.17	0.79
Motivated to learn more?	4.00	4.61	0.04
Interested in career in security?	3.85	4.25	0.27

Table 5. Post-Survey Results

Other Observations

We were interested in finding out if the students' background has an impact on their existing knowledge on ARP Spoofing before they did the labs. We measured this by analyzing the pre-survey results and computing the correlation between the specific background and the sum of scores on the pre-survey. Table 6 depicts the correlation results. Students who read newsletters or articles on cyber security had the strongest positive correlation with the knowledge on ARP Spoofing followed by having had formal training and having taken cyber security courses. However, interest in learning cyber security and interest in pursuing career had almost no correlation with their knowledge. Interestingly, reading newsletter or articles are the most active forms of learning compared to other backgrounds.



Cybersecurity Course	Formal Training	Newsletters or Articles	Other	Interested in Learning	Interested in Career
0.35	0.42	0.53	-0.11	0.06	0.13

Table 6. Correlation between background and knowledge

CONCLUSIONS

In this paper we introduced two different educational tools for teaching ARP spoofing attacks. The first one is based on visualization and simulation; the second one is focused on hands-on practice. These two tools were evaluated in a network security class with 45 students. Students were randomly divided them two groups and comprehensive pre-survey, post-survey, and pre and post quizzes were conducted in the evaluation process. The results show that both tools have significantly improved the students' knowledge in the subject matter. Although, there is difference in the performance of students in these two groups, it is not statistically significant enough draw conclusion that one is better than the other. Interestingly, students who used the hands-on lab showed significant higher motivation in learning more about cyber security. More research needs to be done in the future to verify or reject this result. If verified, an analysis is also needed to explain the reason for this result. Another interesting observation is that actively reading cyber security related articles is a more significant contributing factor in students' cyber security knowledge than other factors including formal training and taking cyber security classes.

ACKNOWLEDGMENT

This work is partially supported by the National Security Agency (NSA) under the award H98230-17-1-0332. 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 the NSA.

REFERENCES

Baxley, T., Xu, J., Yu, H., Yuan, X., Brickhouse J, (2006). LAN Attacker: A Visual Education Tool, *Proceedings of Information Security Curriculum Development Conference*.

Craig J., Knapp M., Mitchell D., Claypool M., Fisler K. (2011). CounterMeasures: A Game for Teaching Computer Security, *Annual Workshop on Network and Systems Support for Games*.

D'Apice, C., Claudia G., Rossella P., Luca L. (2015). Dms2015short-2: Advanced Learning Technologies for Elearning in the Enterprise: Design of an Educational Adventure Game to Teach Computer Security. *Journal of Visual Languages and Computing, 31:260–66*.

David C. Plummer (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*.

Du W., Wang R. (2008). SEED: A Suite of Instructional Laboratories for Computer Security Education, *Journal on Educational Resources in Computing, v8 n1 Article 3*.

Kaabi S., Kindi N., Fazari S., Trabelsi Z. (2016). Virtualization based Ethical Educational Platform for Hands-on Lab Activities on DoS Attacks, *IEEE Global Engineering Education Conference (EDUCON), pp 273-280*.

Murthy N. (2009). Teaching Computer Security with a Hands-On Component, *IFIP World Conference on Information Security Education, vol 406. Springer, Berlin, Heidelberg*.

Pham C., Tang D., Chinen K., Beuran R. (2016). CyRIS: A Cyber Range Instantiation System for Facilitating Security Training, *ACM International Conference Proceeding Series*.

Processing is a flexible software sketchbook and a language for learning how to code within the context of the visual arts (n.d.). *Retrieved from https://processing.org/*

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

Thompson, M., Irvine, C. (2011). Active learning with the CyberCIEGE video game, *Proceedings of the 4th conference on Cyber security experimentation and test*.

Trabelsi Z. (2011). Hands-on Lab Exercises Implementations of DoS and MiM Attacks Using ARP Cache Poisoning, *Proceedings of the 2011 Information Security Curriculum Development Conference*.

Verizon (2014). Verizon Data Breach Investigations Report. *Retrieved from http://www.verizonenterprise.com/DBIR/2014/*

Vigna G. (2003). Teaching Hands-On Network Security: Testbeds and Live Exercises, *Journal of Information Warfare*.

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