Developing and Evaluating a Hands-On Lab for Teaching Local Area Network Vulnerabilities

Jinsheng Xu[1], Xiaohong Yuan[1], Anna Yu[1], Jung Hee Kim[1], Taehee Kim[2], Jinghua Zhang[3]

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

[2]Department of Human Development and Services
North Carolina A&T State University
Greensboro, NC, USA
tkim@ncat.edu

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

***Abstract*—Verizon's Data Breach Investigations Report states that local area network (LAN) access is the top vector for insider threats and misuses. In Ethernet, the common vulnerabilities come from Address Resolution Protocol (ARP). It is critical for students to learn these vulnerabilities, understand the mechanisms of exploits, and know the countermeasures, which include static ARP cache entries, improved ARP module in operating systems, encryption, intrusion detection, and data backup. In this paper, we introduce a hands-on lab to help students learn how ARP spoofing attack works. The objective of this lab is to let students successfully become a Man-In-The-Middle by manually creating attack packets. Although tools exist that carry out ARP spoofing attack automatically, asking students to create raw ARP spoofing packets themselves can help them understand the mechanisms of this attack method much deeper than with the automatic tools. We have studied the effectiveness of this lab on the students' understanding of LAN vulnerabilities. Tests were conducted to measure the performance of students before and after using this tool. We gave students surveys after they completed the hands-on lab. A few students were selected for an interview by an independent evaluator. The result shows that this tool can help students understand 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; Local Area Network; ARP Spoofing; Man-In-The-Middle

I. INTRODUCTION

National Cyber Security and Communications Integration Center (NCCIC) recently published an article titled "Combating the Insider Threat" [1]. This article quoted a recent study result by Verizon's Data Breach Investigations Report stating that local area network (LAN) access as the top vector for insider threats and misuses [2]. 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 computer are connected to. Wireless networks have more vulnerabilities of their own in addition to the ones Ethernet already has. 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 on attacks on LAN [10]. 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. Although simulation can help students understand the dynamics of ARP spoofing attacks, students cannot feel the excitement in carrying out successful real world attacks. Several tools exist that can do real world ARP spoofing attacks [3,4]. 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 a switched network. 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. We believe that letting students create their own ARP spoofing packets can help them understand this mechanism much deeper. It can also give them more confidence and motivation on learning related cyber security concepts.

In this paper, we introduce a hands-on lab to help student learn how ARP poisoning attack works. The goal of this lab is to let students successfully become a Man-In-The-Middle and understand the vulnerabilities of LAN. This lab will ask students to create Ethernet frames that carry out an 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 manually enter all fields of an ARP Reply packet.

We have studied 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. We have given student surveys after they completed the hands-on lab. A few students were selected for interview by an independent evaluator. We will present the details of our findings. We will also share this hands-on lab with the education community by providing a URL for downloading.

In the following sections, we will introduce our background research, the development of the hands-on, and the evaluation results.

II. BACKGROUND

A. Address Resolution Protocol (ARP)

The Address Resolution Protocol (ARP) is a network protocol that resolves network layer addresses (e.g. IP address)

into link layer addresses (e.g. MAC address). ARP was defined by RFC 826 [5]. IP Datagrams must be encapsulated in Ethernet Frames for delivery in Ethernet. Therefore, ARP is needed to resolve MAC addresses from IP addresses. The ARP is a request and reply protocol and its range is within the boundaries of a single physical network. 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. 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 [6]. ARP is a stateless protocol, in which the receiver of ARP reply automatically saves the mapping into the ARP cache even without 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, 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 [3] and Ettercap [4] are two of the most popular ones among them. They are listed as the most popular network security tools by SecTools.org [7]. Cain and Abel is developed for cracking the Windows password. Ettercap is developed for Man-In-The-Middle attacks. Both have numerous features and both include ARP spoof 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 spoof 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 frequently. Another approach is to make the ARP software secure in the operating systems. For example, operating system can ignore unsolicited ARP replies. There are also tools available that detect ARP spoofing attacks by monitoring the change in the mapping of IP address and MAC address.

III. DEVELOPING THE HANDS-ON LAB

We have developed tools with which students are asked to carry out a successful Man-In-The–Middle attack on a switched network. The first tool named "sendarp" is programmed to send an arbitrary ARP reply message. Students are asked to provide information such as MAC addresses of the source and the target in ARP reply message, the IP addresses of the source and the target in ARP reply message, and the destination and source MAC addresses in the Ethernet frame header. Students can successfully carry out this attack only with a clear understanding of Ethernet frames, ARP message format, and goals of ARP poisoning. 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 interval. This program was developed on Windows with WinPcap library. The source code is included in the provided virtual machine.

The second tool, 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 a Wireshark [8] 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. The 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 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 generate traffic for students to capture. Alternatively, students can manually generate traffic from the victim to verify if these traffic can be intercepted by the attacking virtual machines. In each of the virtual machines, "sendarp", "mim" and Wireshark are installed. We also included the source code for "sendarp" and "mim" in the virtual machine.

Fig. 1. The architecture of Hands-on Lab

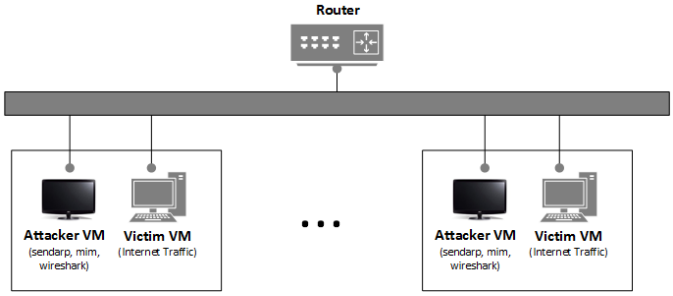


Figure 2 shows the screenshot of a successful ARP spoofing attack on the victim with the "sendarp" program. The attacker sends ARP reply message to the victim 78:e3:b5:68:0c:a9 (192.168.1.13) with its own MAC address associated to the router's IP address 192.168.1.1. Figure 3 shows the screenshot of 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. 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 the "mim" program to forward the intercepted IP datagram to the destination.

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

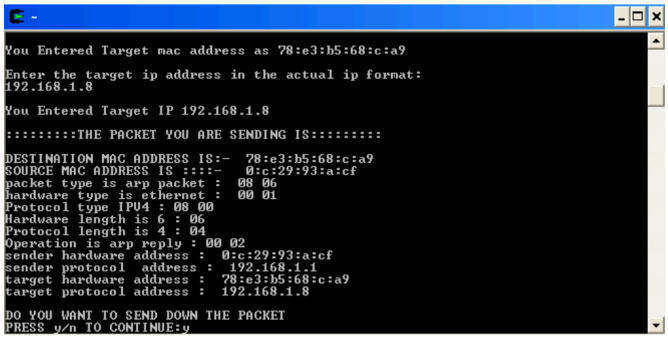
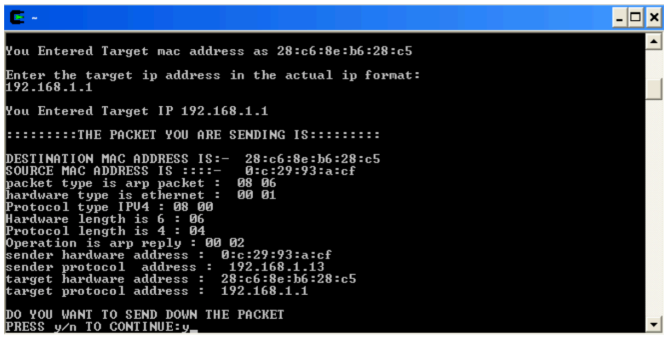


Fig. 3. Screenshot of ARP spoofing attack on router with *sendarp* program



IV. Evaluation and Results

This hands-on tool was first developed in 2008 by the Department of Computer Science at North Carolina A&T State University to let students get hands-on experience and increase student interests and confidence in Information Assurance knowledge and skills. Along with other tools, it was first distributed at the 2008 Faculty Development Workshop on Cyber Games and Interactive Simulation [9]. The workshop took place in June of 2008 at University of North Carolina at Charlotte. Eighteen faculty members from different universities attended the workshop. We presented this tool to attendees and let them get hands-on experience. At the end of the workshop, we conducted a survey on the quality of the tool. Sixty seven percent gave excellent ratings and eleven percent gave good ratings on this tool.

Since then, this tool has been continuously used in Network Security class, which is offered once in every year to both undergraduate and graduate students at North Carolina A&T State University. This tool has inspired one graduate student to do a Master's Project on creating a tool that visualizes the ARP spoofing attacks in real time by monitoring the traffic of the network and the ARP cache status of the victim hosts. Recently, we have expanded the application of this tool to the undergraduate Computer Networks class, a required class, to enhance cyber security education to more students. We know students generally enjoyed this hands-on lab and was motivated by the fact that they can successfully finish it. However, we do not exactly know how effective this lab is in helping students understand the concept of ARP and ARP spoofing. Therefore, we decided to measure it and disseminate this tool in a conference.

A. Evaluations

We measured this tool with two different methods. The first one is to see how effective this tool is in supplementing the classroom lecture. The second one aimed to see if this tool can replace a classroom lecture. To achieve this, we evaluated the tool in two stages on two different groups of students.

The first evaluation was done in Fall of 2015. There were seven students in the Computer Networks class participated in the study. The lecture contained the topics on the vulnerabilities of LAN and Man-In-The-Middle attacks. ARP Spoofing attack was covered in the lecture. We designed a quiz that contained five questions and administered the quiz three times: before the lecture, after the lecture, and after the hands-on lab. Figure 4 shows the evaluation quiz questions. The average of the quiz scores for pre-lecture, after-lecture, and after-lab are 2.7, 3.1, and 3.4 respectively. All the scores are out of five. From the result we can see the steady improvement from the lecture to the hands-on lab.

Fig. 4. Evaluation quiz 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 attacks is not an MITM attack?
   A. ARP Spoofing
   B. DNS Spoofing
   C. Switch Port Stealing
   D. TCP SYN Flooding

In the second evaluation, we carried out the hands-on lab without giving students lectures on ARP spoofing attacks. However, students are aware of the ARP protocol because it is part of the topics in Computer Networks. This evaluation was given in Spring 2016 semester. There were eleven students who participated in this evaluation. The average quiz scores before the lab and after the lab are 2.8 and 4.0 respectively. The average quiz score before any learning was very similar to the result of stage 1. However, stage 2 students performed much better after the hands-on lab. One possible reason is that

we had two people (instructor and TA) helping students in stage 2. Therefore, each student got more attention compared to those in stage 1. Another reason could be more experience in keeping students focused during intensive fifty minutes of lab time. Table 1 summaries the results of the two quiz evaluations. From the results we can see that Stage 2 was much more successful, not only in the improvements of average quiz grades, but also in statistical significance as shown by the t-test results. This was achieved without giving lectures on ARP spoofing to the students.

Table. 1. Summary of Quiz Evalutions

	Average of Pre-Lecture Quiz	Average of Post-Lecture Quiz	Average of Post Lab Quiz	Two tailed P values of t test
Stage 1	2.7	3.1	3.4	0.1824
Stage 2	2.8	N/A	4.0	0.0189

B. Survey

Four students participated in a survey after the course in Fall 2015. The following is the mean scores for students' motivation, satisfaction, enjoyment, and perceived difficulty. All the scores are out of five. Regarding different types of students' motivation, the mean score of students' intrinsic motivation is M=3.38 with SD=.83, and that of students' identified motivation is M=4.50 with SD=0.61, that of students' external motivation is M=2.75 with SD=0.96, and that of students' amotivation is M=1.43 with SD=0.88.

Regarding students' satisfaction, enjoyment, and perceived difficulty, students' satisfaction, the mean score of students' satisfaction is M=4.00 with SD= .84. Also, the mean score of students' enjoyment is M=4.42 with SD= 0.69, and that of students' perceived difficulty is M=1.85 with SD= 1.43.

C. Focus Group Interview

To understand effectiveness of hands-on activities on students' learning processes and motivation in the courses, focus-group interviews were conducted in Fall 2015. Two students participated in the focus group interview. Based on the focus group interviews, several themes were emerged regarding students' improving competence and motivation on the topic, their preference of hands-on activities, and their future career interest in the field. More specifically, the following themes were found:

- The importance of practical use in learning
- Motivation to learn more about the topic
- Desire for more hands-on activities in the course

Overall, students explained how hands-on activities helped them see the importance of practical use of theory in learning. For instance, one of the students repeated the importance of practical use by stating "apply what we learned" and "be able to apply theory" as a reason to like hands-on activities in class. Especially, a student mentioned that his motivation has increased, saying "it raises more questions (while doing hands-on activities), and definitely get you more engaged, and (have) motivation to dig deeper". In line with that, the other student mentioned that the hands-on activity "sparks interest" in the topic because he could see the practical implication of the topic.

V. CONCLUSIONS

In this paper, we introduced a hands-on lab on learning LAN vulnerabilities and presented our evaluation results. The results show that this tool is helpful to students in learning this topic and motivated them in learning more and deeper on related topics. Currently, we are working on adding real time visualization component to this tool, so that students can visualize in real time the effects of their work by seeing the traffic being diverted to the attacker and the ARP cache of the victim being modified. This hands-on tool will be made available at: http://williams.comp.ncat.edu/IA_visualization_labs/.

REFERENCES

[1] 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.

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

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

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

[5] 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.

[6] Whalen, S., "An introduction to ARP spoofing," 2600: The Hacker Quarterly, vol. 18, no. 3, Fall 2001

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

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

[9] 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.

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