LEARNING COMPUTER SYSTEMS' VULNERABILITIES EXPLOITATION THROUGH PENETRATION TEST EXPERIMENTS

Te-Shun Chou and Tijjani Mohammed
Department of Technology Systems
East Carolina University
chout@ecu.edu

Abstract

This paper describes a project that focused on the study of the exploitation of information systems' vulnerabilities in an intrusion detection and incidents response graduate course. The project incorporated a series of penetration testing labs and provided detailed instructions for students to conduct essential hands-on activities in a step-by-step fashion. The labs included footprinting, ARP poisoning, man-in-the-middle attack, IP spoofing, exploitation, and collecting victims' data. In this paper, these labs will be described, along with the evaluation results of the project.

Keywords: Intrusion detection and incidents response, virtualization, network security, penetration testing

1. Introduction

The major goals of teaching information security courses include delivering the theoretical knowledge across different fields and preparing students with practical skills so that they can apply what they have learnt in the real world. To tackle the second goal in an intrusion detection and incidents response graduate course, a project that comprised of hands-on activities relating to performance evaluation of intrusion detection system (IDS) was designed in and implemented [1,2]. The project was divided into six phases: creation of an intrusion detection experimental environment, attacks recording, analysis of attack signatures, generation of intrusion detection rules, collection of normal traffic, and IDS performance evaluation. Each of these phases acted as a learning development for students and raised their level of knowledge to a certain task. By successfully completing six phases, students advanced their skills and understandings in the design of IDS.

In order to broaden students' learning, we designed another project that focused on the study of hackers' behavior and information systems' vulnerabilities. The project incorporated a series of penetration testing labs and provided detailed instructions for students to conduct essential hands-on activities in a step-by-step fashion. The labs included footprinting, ARP poisoning, man-in-the-middle attack, IP spoofing, exploitation, and collecting victims' data. Network security tools were used to exploit information systems' vulnerabilities and all of the lab activities were performed in a virtual environment. The objective of this project was to help students perform security assessments and understand computer systems' vulnerabilities in an experimental environment.

This paper is organized as follows. Section 2 presents the labs used in the project. Section 3 discusses the result of the project evaluation. Finally, the conclusions and future work is presented in the last section.

2. Penetration Testing Labs

2.1. Lab Environment Setup

The project started with the creation of a virtual network using VMware as the virtualization platform. This virtual environment allowed students to install and configure multiple virtual machines that ran different operating systems in one physical machine. For performing the experiments, the virtual network included one attack host and two victim hosts. The attack host was used to launch exploration against the victim hosts. In this project BackTrack was used as the attack host and two victim hosts, Linux CentOS and Windows XP, were set up within the VMware workstation. BackTrack is a Linux-based digital forensics and penetration testing distribution for professionals to perform security assessments in an experimental environment. It organizes security tools into 12 categories: information gathering, vulnerability assessment, exploitation tools, privilege escalation, maintaining access, reverse engineering, RFID tools, stress testing, forensics, reporting tools, services, and miscellaneous [6]. In this project, we used BackTrack tools to conduct penetration testing experiments.

2.2. Labs

Penetration test involves network security assessments and the exploitation of computer systems' vulnerabilities. It attempts to exploit the vulnerabilities on computer systems and networks using simulated attacks. In this project we developed a series of labs for students to gain hands-on experiences in both network penetration testing and application security testing. A total of six labs were developed, including footprinting, ARP poisoning, man-in-the-middle attack, IP spoofing, exploitation, and collecting victims' data. Students were asked to perform the lab activities individually. Upon completion of the project, the students were required to write a short essay on each lab describing what they had learned from the project.

2.2.1. Footprinting lab

In general, Footprinting is the first step used for the security penetration test of a network. The purpose of footprinting is to collect as much information of a network as possible for the use in future hacking. It includes information gathering, determining the network range, identifying active machines, finding open ports and access points, OS fingerprinting, fingerprinting services, and mapping the network. In this lab we used a variety of tools to gather information on network infrastructures such as domain names, IP addresses, and routing information. The tools utilized include Whois, Dnsmap, Nslookup, Traceroute, Dnsenum, Dmity, Scapy, and Dnmap.

2.2.2. Address Resolution Protocol (ARP) poisoning lab

Address Resolution Protocol (ARP) is a network layer protocol used for mapping an Internet Protocol (IP) address to its corresponding Media Access Control (MAC) address. When a device needs to send packets to a target host over Ethernet, it must have both IP and MAC addresses information of the target. The IP-to-MAC address mapping data is stored in an ARP table of each device. If the target's address mapping information is not found in a device's ARP table, the device will send an ARP request broadcast message to all computers on the subnet. The computer with the given IP address sends an ARP reply in response to the broadcast that allows the sender to be able to deliver data to the target computer. Also, the sender will update its ARP cache for future use.

An ARP table includes network devices' IP addresses and their corresponding MAC addresses. ARP poisoning, also called an ARP spoofing attack, is a type of attack that compromises the ARP table and changes the MAC address so that the IP address points to another device or the attacker itself. Attackers could then steal data from the compromised computers and eavesdrop using man-in-the middle technique. In addition, legitimate devices could be prevented from accessing the Internet or other external networks because of ARP poisoning attack. In this lab, the tool Ettercap was first used to resolve two victims' IP addresses to MAC addresses, then again used to compromise the victims' MAC addresses to the attacker's MAC address.

2.2.3. Man-in-the-middle attack lab

By intercepting legitimate communication between two computers, man-in-the-middle attacks can proceed the attacked machine in either passive or active ways. In a passive attack, the attacker intercepts the data, records it and then sends it to the destination without alternation. In an active attack, the attacker captures the data, changes its content and forges a response to the recipient the sender was originally intending to visit. In this lab, the tool Ettercap was used to perform a man-in-the-middle attack to monitor activities in the victim host XP. When a website was opened in the victim's web browser, all of the messages in the victim machine were intercepted by the attacker.

2.2.4. IP spoofing lab

IP spoofing attack impersonates a trusted host to send messages to other computer(s) with an IP address of that trusted host for gaining unauthorized access to those computers. To launch this attack, a hacker must find an IP address of a trusted host and then modify the packet headers to disguise the traffic coming from that host. In this lab we used the tool Hping in the attack host to send message to CentOS using XP's IP address. During the entire course of the experiment, the packet sniffer, Wireshark, was used to monitor the spoofing activities between the attack and the victims.

2.2.5. Exploitation lab

An exploit involves using software, data, or commands to take advantage of a bug (or vulnerability) of a computer system and the result causes the computer system to work in a manner of unexpected performance. The exploitation result, for example, could allow a hacker to gain control of a computer system, conduct privilege escalation, access a database, and become as a superuser of a system. In this lab, the tool Metasploit Framework was used to exploit a vulnerability of Mozilla Firefox that was installed in the victim XP machine. After migrating the exploited process to the victim, the victim's system information and the data can be monitored by the attacker.

2.2.6. Collecting victims' data lab

Collecting victim's data happens once the attacker has obtained unauthorized access to the victim's machine. Data could be collected to be used in further exploits if the attacker chooses to do so. Having gained access to a victim's machine in the previous lab, we used keystroke logging (keylogging) to record victim's keys keystroke data on the keyboard. By using this approach, everything the victim typed, such as username and password in an email account and a social network site, were captured by the attacker.

2.2.7. Self-study penetration testing labs

In addition to the above labs, students are asked to create and perform a penetration testing experiment by themselves for the purpose of enhancing the knowledge of the subject. Some examples from this endeavor include: 802.11 WPA-PSK key cracking by using aircrack-ng, bypassing a password protected Windows system, fingerprinting the operating system, searching for vulnerabilities on a remote system, and crashing an application on a victim's machine.

3. Project Evaluation

The project was offered online for distance education graduate students in an intrusion detection and incidents response course. An online survey with ten questions (Table 1) was designed to assess students' experiences at the end of 2013 fall semester. The objective of the survey was to evaluate the project's effectiveness in order to improve the lab manuals for future use. In the design of the questions, a five-level Likert scale was used. Available responses were: strongly disagree, disagree, neutral, agree, and strongly agree. In order to investigate attitudes of the respondents toward each question, we coded the responses accordingly: strongly disagree = 1, disagree = 2, neutral = 3, agree = 4, and strongly agree = 5. Table 2 shows the descriptive statistics result. Totally 12 questionnaires were successfully collected at the end of the course.

Table 1. Survey Questions

No.	Question
1	The steps of labs shown in the assignment are clear and easy to follow.
2	The assignment provides all of the necessary information in order to conduct lab activities.
3	The learning objectives of labs are clearly described.
4	I would rate the overall quality of the project as high.
5	I would rate the technical difficulty of the labs as difficult.
6	BackTrack is a good tool for learning penetration testing.
7	I have a better understanding of penetration testing after finishing the labs.
8	It's a good strategy to simulate network attacks in a virtualization environment, instead of using physical network devices.
9	I believe I am able to apply the knowledge of penetration testing to my future career.
10	I spent excessive time working on this project.

Table 2. Survey Statistics Result

Question	Strongly Disagree (1)	Disagree (2)	Neutral (3)	Agree (4)	Strongly Agree (5)	Mean	Standard Deviation
1				4 (33.33%)	8 (66.67%)	4.67	0.49
2			1 (8.33%)	4 (33.33%)	7 (58.33%)	4.50	0.67
3			1 (8.33%)	3 (25.00%)	8 (66.67%)	4.58	0.67
4		1 (8.33%)		4 (33.33%)	7 (58.33%)	4.42	0.90
5		1 (8.33%)	7 (58.33%)	2 (16.67%)	2 (16.67%)	3.42	0.90
6					12 (100.00%)	5.00	0.00
7			1 (8.33%)	3 (25.00%)	8 (66.67%)	4.58	0.67
8			1 (8.33%)		11 (91.67%)	4.83	0.58
9			1 (8.33%)	3 (25.00%)	8 (66.67%)	4.58	0.67
10		2 (16.67%)	3 (25.00%)	2 (16.67%)	5 (41.67%)	3.83	1.19

Overall the average of the ten questions was approximately 4, which shows the students had generally positive attitudes toward the course. Over 90% of students selected "strongly agree" and "agree" on the survey questions except questions 5 and 10. All of the students agreed that BackTrack is a good tool for learning penetration testing. Students affirmed that the lab instructions were clear and very well written. After finishing the labs, students had a better understanding of penetration testing concepts. They agreed that the project provided valuable information on penetration testing and plan to apply what they have learnt in their future careers.

In addition to the 10 questions, students were also asked to provide one example where they have added to their knowledge from this project. Some of responses were: "*I haven't had the chance to use BT5 and I really enjoyed learning the footprinting tools and I think that they will be very* *useful to me throughout my personal life and career.*", "*I gained a great deal of knowledge on the concepts behind attack strategies.*", "*I feel like this assignment provides good details and requires the student to really get to know BackTrack and its abilities.*", "*I have had some experience with the tools inside of BackTrack, this experiment increased my knowledge of the tools capabilities which has been a great experience for my understanding of the potential attacks that could occur.*", and "*I've been through many network security classes, but this series of assignments really helped me understand the actual processes that take place when and IDS is put into place and working.*"

4. Conclusions and Future Work

In this project created a virtualized network environment that included three different virtual machines using VMware. The environment provided students with a confined place to carry out penetration testing activities. Students studied information systems' vulnerabilities exploitation and conducted security assessments using a variety of network security tools. This project helped the students to gain a better understanding of the characteristics and nature of information systems vulnerabilities. It also helped students become better prepared for career opportunities in the field of network security.

We plan to continue revising and upgrading the lab activities based on the feedback received from students. In addition, this project could be used as a foundation for developing more penetration testing labs to help broaden students' aspect of security awareness and assessment.

Acknowledgement

The authors would like to thank the summer funding support from College of Technology and Computer Science at East Carolina University.

References

[1] Chou, Te-Shun, "Understanding Computer Network Vulnerabilities and Security Threats via Packet Signature Analysis," *American Society for Engineering Education (ASEE) The Computers in Education Journal*, Volume XXIII, Number 3, (2013).

[2] Chou, Te-Shun, "Development of an Intrusion Detection and Prevention System Project Using Virtualization Technology," *International Journal of Education and Development using Information and Communication Technology*, Volume 7, Issue 2, 46-55, (2011).

[3] Vmware: http://www.vmware.com/ (Last browsed in March 2014)

[4] Linux CentOS: http://www.centos.org/ (Last browsed in March 2014)

[5] Windows XP: http://www.microsoft.com/windows/windows-xp/default.aspx (Last browsed in March 2014)

[6] BackTrack: http://www.backtrack-linux.org/ (Last browsed in March 2014)