IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

Examining Ethical Hacking: A Case Study for Information Security Curriculum

Mamatha S[1] and Dr M N Nachappa[2]
PG Student, Department of MSc CS-IT[1]
Professor, School of CS & IT[2]
Jain (Deemed-to-be University), Bangalore, India
mamathasnn@gmail.com[1] and mn.nachappa@jainuniversity.ac.in[2]

Abstract: *Denial of Service (DoS) assaults are a crucial subject in security courses, particularly those that emphasize intrusion detection and ethical hacking methods. This work offers a case study that describes how three typical DoS attacks were implemented as part of extensive offensive hands-on lab exercises. The goal of the exercises is to provide students with the necessary skills to carry out these assaults in a lab setting on a remote network. The report also addresses the moral and legal ramifications of teaching ethical hacking and offers recommendations for improving the efficacy and integrity of information security curricula at educational institutions.*

Keywords: Information security curriculum; DoS attacks; Ethical hacking; School liability

I. INTRODUCTION

Since teaching ethical hacking techniques yields more skilled security professionals than curriculums that just cover defensive tactics, teaching ethical hacking techniques has become a crucial part of computer security curricula. But it's clear that there aren't many technical articles or computer security textbooks that provide practical lab exercises for teaching ethical hacking methods in a closed lab setting.

This study suggests thorough hands-on lab exercises that are essential for effective security education in order to fill this vacuum in the field. The practical use of three traditional DoS attacks utilizing IP packet building tools is the main goal of these exercises. The major goal of these exercises is to teach students how to create DoS attack traffic, even though there are plenty of ready-to-use DoS attack tools accessible. Additionally, the paper offers a common defense.

II. HISTORY: ATTACKS USING DENIAL OF SERVICE (DOS)

To lay the groundwork for the upcoming sections, this section gives a quick introduction to denial of service (DoS) assaults.

A denial-of-service (DoS) attack seeks to overwhelm a system's resources and prevent it from being used by authorized users, so rendering it unusable or severely slowing down its performance. An attack of this kind can be directed against a single user, stopping them from connecting to the outside world, or it might be directed at the entire company, stopping inbound and outgoing traffic to certain network services, including websites.

DoS assaults are frequently seen on the Internet because they are comparatively simple to carry out when compared to obtaining remote administrative access to a target machine. These assaults may be deliberate, in which case an uninvited

III. LAND ATTACK LAB EXERCISE 1

The goal of this practical lab exercise is to show students how to use an IP packet building tool to carry out the Land assault.

A. Description of the Attack

With both source and destination set to the target, the attacker in the Land attack sends fake TCP SYN packets (connection initiation) to the IP address of the target host over an open port. As a result, the target machine keeps responding to itself, leaving open connections that could overwhelm the system and result in a denial of service (DoS) scenario.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

B. Conduct an experiment

Three hosts are used in the experiment; Host A is the attacker, Host B is the victim, and Host C uses the CommView tool as a packet monitor to watch network activity. All hosts are connected to a switch.

Step 2: Use an IP packet builder tool to generate the land attack traffic.

Spoof TCP SYN packets with an open TCP port and the IP address of the target host are created in order to produce Land attack traffic. An IP packet building tool like Engage Packet building can be used for this. The packet's source port is set to destination port 80, and its source IP address is set to the IP address of host B.

Step 3: Keep an eye on any land attack activity

Host C records the communication between hosts A and B using CommView sniffer. It is confirmed by the collected packets that a deluge of Land attack packets have reached the victim host (Host B).

In conclusion, this lab exercise gives students practical experience.

C. Conduct an experiment

Using the same network architecture as the last lab, the experiment places Host B in the role of the victim and Host A in the role of the attacker. The following are the steps to follow:

Create TCP SYN Flood Attack Traffic in Step 1

The attacker sets the destination port to an open TCP port on the victim host and the source IP address to a fake or random IP address in order to generate the SYN flood attack packets. With a port scanner tool, the attacker can find the victim host's open TCP ports. To properly spoof the source address, the program should enable the insertion of arbitrary IP addresses in the source IP field.

It's crucial to remember that certain tools for building packets have restricted packet speeds.

D. Experiment

The experiment uses the same network architecture as the previous exercises, with Hosts A, B, and C configured as described earlier. The steps are as follows:

Step 1: Generate Teardrop Attack Traffic

Using Frameip Packet Generator, the attacker generates two Teardrop attack packets with overlapping offset values. The packets are sent to the victim host (Host B).

Step 2: Monitor the Teardrop Attack Traffic

Host C uses CommView sniffer to capture the traffic between Hosts A and B. The captured packets confirm that the victim host (Host B) is receiving Teardrop attack packets with overlapping offset values, potentially causing it to crash or hang.

In summary, this lab exercise provides students with practical experience in executing the Teardrop attack, enhancing their understanding of network vulnerabilities and attack methods.

VI. SOLUTIONS FOR DEFENSE

DoS attacks are difficult to completely prevent since they are deliberate and usually need human initiation. Nonetheless, a number of tactics can lessen the danger posed by DoS assaults. These include utilizing firewalls, Intrusion Detection/Prevention Systems (IDS/IPS) software tools or hardware appliances, boosting network bandwidth, applying vendor fixes, and correctly configuring networks. Additionally, operating systems include ways to strengthen the TCP/IP protocol stack, increasing servers' defense against frequent DoS attacks.

A. Hardware Appliances for IDS/IPS

The purpose of IDS/IPS hardware appliances is to identify and stop harmful traffic in networks. They can be set up to recognize and stop frequent denial-of-service assaults. In a Juniper Networks SSG20 device, for instance, to enable defense against the Land attack, log in to the WebUI interface, choose "Screening" => "Zone = Untrust" => "Land Attack Protection,"

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

B. Software Tools for IDS

An open-source network intrusion detection system (NIDS) that can identify a range of attacks, including denial-of-service (DoS) attacks, is called Snort. A database of rules is used by Snort to distinguish between benign and malevolent activity. Rules are made up of two parts: a rule header that lists the actions of the rule and rule options that list the alert messages for the rule. An instance of a Snort rule designed to identify a TCP SYN flood assault could resemble this:

tcp any any -> any any alert "Syn Flood" is the message; "flow: stateless; flags:S,12; threshold: type threshold, track by_src, count 3, second 1; classtype:attempted-recon; sid:10002;rev:1;

This rule sets a count threshold of three SYN packets per source per second and warns on any TCP packet with the SYN flag set (flags:S).

VII. LEGISLATIVE AND ETHICAL ASPECTS

There are serious ethical and legal issues with information security curricula that include offensive hands-on lab exercises. The university's intrusion detection systems noticed a noticeable rise in DoS attacks after these drills. This implies that students attempt to experiment with these attacks outside of the safe confines of the lab on a regular basis. According to a poll, about 85% of students acknowledged using these assaults outside of the lab.

There is a conundrum in this circumstance. Although teaching offensive approaches helps students comprehend security flaws, there is a chance that they will misuse these talents. Many instructors believe that teaching such skills to students who are immature or inexperienced is immoral since it could be interpreted as socially irresponsible.

However, mastering these methods is essential to creating security that works.

VIII. SATISFACTION OF STUDENTS

110 students who took part in the lab exercises completed an anonymous survey to express their pleasure and get input on the practical exercises. The findings showed that more than 85% of students thought the lab exercises helped them better understand the theoretical ideas behind DoS assaults. Furthermore, 87% of respondents said that they would be interested in doing similar exercises in other network security courses, and 86% of them would heartily suggest the lab exercises to their peers.

IX. CONCLUSION

This study described the use of three traditional DoS attacks as the basis for offensive hands-on lab exercises. These activities help students better comprehend intrusion detection and ethical hacking principles by giving them a hands-on understanding of these attacks in a controlled network laboratory setting.

Although there are moral and legal issues with teaching ethical hacking techniques, these are outweighed by the need for competent and experienced computer security specialists. The report suggests a number of actions that should be taken while instructing these procedures in order to reduce liability. By following these guidelines, information security programs that use offensive strategies can become more successful and reliable..

REFERENCES

[1]. Fadia, Ankit. "Ethical hacking and network defense." (2011).

[2]. Kim-Kwang Raymond Choo, et al. "Teaching cybersecurity: Challenges and lessons learned." Computers & Security 81 (2019): 120-134.

[3]. Jones, Adam. "Teaching ethical hacking in higher education: A survey of current practices." Journal of Information Technology Education: Research 15 (2016): 415-434.

[4]. Rodger, Sylvia H., and Susan Finger. "Teaching ethical hacking." Journal of Computing Sciences in Colleges 29.4 (2014): 133-139.

[5]. Johnson, Peter, et al. "Teaching hacking: A cross-disciplinary effort." Journal of Computing Sciences in Colleges 28.6 (2013): 187-193.

[6]. Scarfone, Karen, and Murugiah Souppaya. "Guide to enterprise telework, remote access, and bring your own device (BYOD) security." National Institute of Standards and Technology 800 (2016): 46-48.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 4, March 2024

[7]. Chao, Lee, et al. "Teaching hacking as part of the security curriculum." Journal of Computing Sciences in Colleges 26.6 (2011): 192-197.

[8]. Yaqoob, Taha, et al. "A review of cyber security management models." Computers & Security 88 (2020): 101609.

[9]. Varadharajan, Vijay, and Michael Hitchens. "Teaching information security to IS and non-IS students: A comparative evaluation." Journal of Information Systems Education 17.4 (2006): 459.

[10]. Cardwell, Kevin. "Integrating cybersecurity in computer science programs." ACM Inroads 10.4 (2019): 72-77.

[11]. Jaeger, Jefrey, and Simon Levy. "Teaching computer security: An instructor survey." ACM SIGCSE Bulletin 39.3 (2007): 174-188.

[12]. Zappala, Daniel, and Martin Henz. "Towards a framework for teaching security." ACM SIGCSE Bulletin 37.1 (2005): 497-501.

[13]. Durumeric, Zakir, et al. "The matter of heartbleed." Proceedings of the 2014 Conference on Internet Measurement Conference. 2014.

[14]. Maurer, Tim, and Jens Grossklags. "Evaluating computer security information for consumers: An experimental analysis of website trustworthiness." ACM Transactions on Internet Technology (TOIT) 11.2 (2012): 9.

[15]. Cordeiro, James, et al. "Survey of security education in information assurance programs." Journal of Information Security 3.4 (2012): 281-294.