Nile Journal of Communication & Computer Science

Volume 6, December 2023

Journal Webpage: https://njccs.journals.ekb.eg

Print ISSN: 2805-2366
Online ISSN: 2805-2374

Mechanisms of system penetration: Review

Hesham. A. Sakr, Magda I. El-Afifi

Assistant Professor, ECE department, Nile Higher Institute of Engineering and Technology, Mansoura, Egypt
Artificial Intelligence Lab

Abstract

Given the escalating frequency of cyber-attacks worldwide, network security has become a pressing concern. Consequently, a substantial amount of "ethical hackers" have offered their services voluntarily to develop strategies and scripts to combat security problems. The necessity for more efficient management of security systems has led to the development of penetration testing, as it is time-consuming to maintain and monitor attacks on each hardware and software within an enterprise. Several research organisations have developed algorithms to protect networks based on their size, kind, and purpose. This study involves the construction of a simulated organisational framework to examine the practise of penetration testing within a live server-client environment. The Border Gateway Protocol (BGP) was selected as the routing protocol due to its extensive usage in contemporary networks. In addition, BGP exhibits low internal vulnerabilities, which enhances the overall security assessment. This research introduces computer-based attacks and actual network-based attacks, together with their corresponding defence methods. The article demonstrates the process of conducting penetration testing on a specific BGP network. Both internal and external network attacks are used to produce packets, exploits, and payloads. Firstly, we commence by delineating all the sub-fields within the penetration testing domain, together with its respective requirements and repercussions. This paper focuses on several techniques used to attack routers, switches, and physical client workstations in the context of educational and learning research.

Keywords: GNS3, DMZ, Python Code, LAND Attack, STP.

1. Introduction

Network security is one of the key considerations of any information system. The probability of weak configurations grows as the system grows in size, producing a security loop hole. Security weaknesses cause a slew of issues. Recent Home Depot and Target cyber security breaches, for example, resulted in cyber hackers stealing about 60 million card numbers. Similarly, JP Morgan's bank's recent network hack is predicted to result in a large financial loss. Many significant industries throughout the world should take note of these instances. The necessity to secure networks has grown considerably more crucial for all individual organisations, regardless of size or purpose, as it helps protect sensitive information and investments of their clients. It promises to create a secure networking environment that is resistant to offensive threats. The desire for a person's capacity to test a network for vulnerabilities has resulted in the emergence of a "Pentester" in recent times, which refers to a person who performs penetration testing to examine a specific network. Penetration testers can aid in the identification of vulnerabilities/threats and give the most

active means of defending specific systems by doing penetration testing. Penetration testers can aid in the identification of vulnerabilities/threats and provide the most dynamic method of protecting specific networks as shown in figure [1].

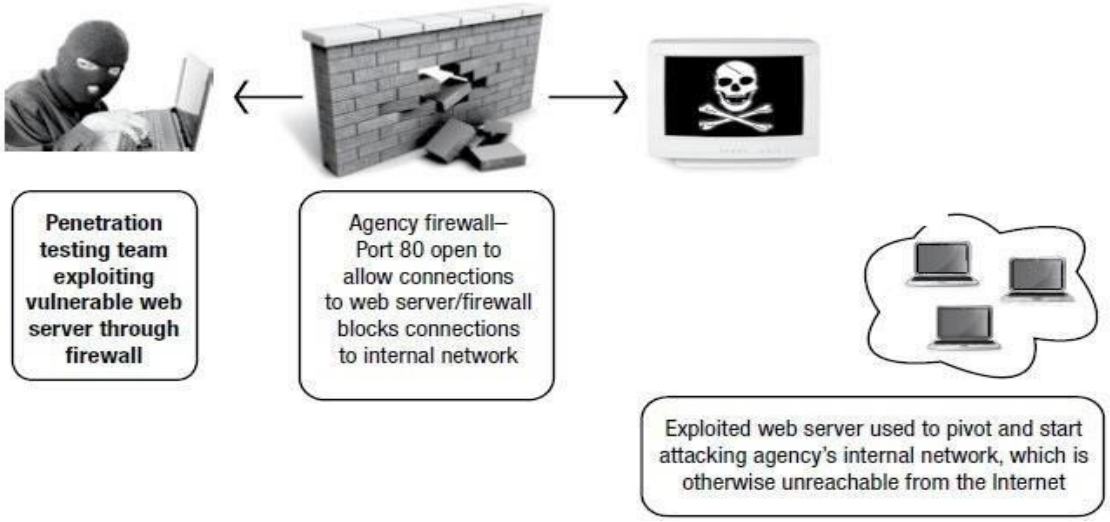

Figure 1: A Procedure Prototype for Pen Testing [1]

2. Related work

Penetration testing is a method used to understand and evaluate the security capabilities of a network by simulating fictional attacks and flaws. This information enhances the advancement of any organization's security system. This chapter provides an overview of various approaches and focuses of penetration testing. Block diagrams are used to illustrate the many stages of penetration testing. This text offers a concise overview of the diverse tools employed by a penetration tester. Figure 2 illustrates the objectives and advantages of this testing procedure towards its conclusion.

Penetration testing is categorised into three types: black box, white box, and grey box, depending on the utilised approach. This also simplifies the classification into two main categories: external and inside. In essence, the outcome hinges on whether the attacking system is situated within or outside the network.[4-2]

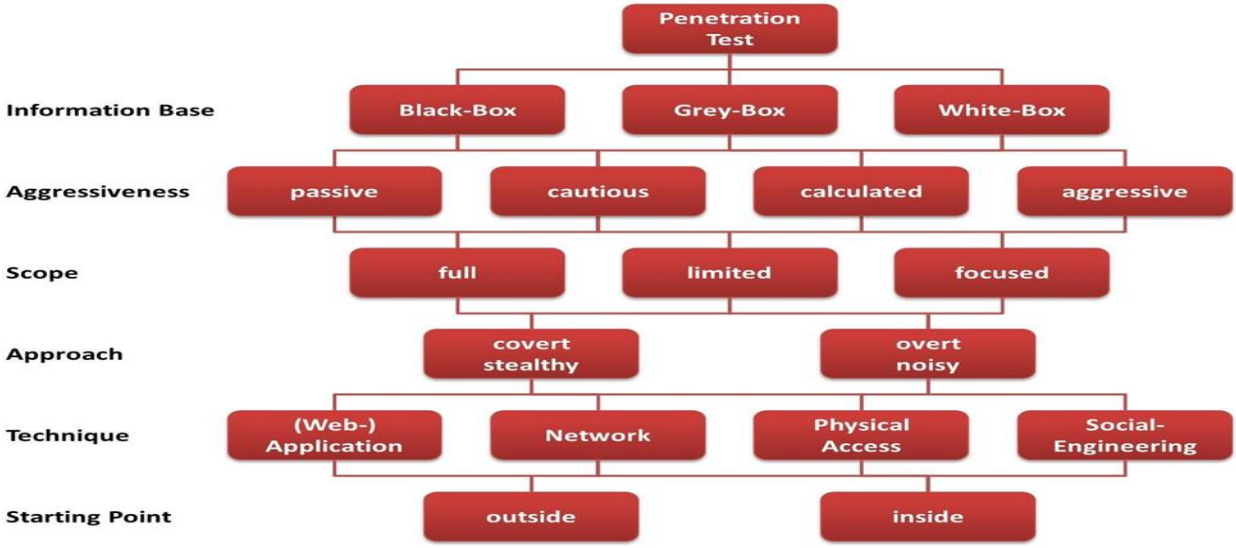

Figure 2: Penetration Testing Layout [5]

3. Contribution

The research focuses on the following critical problem statements:

•Types, phases, and applications of penetration testing

•Conducting Border Gateway Protocol testing in the laboratory

• Assessing vulnerabilities in network equipment

• Weaknesses in different apps installed on the host machine

4. Techniques

There is a wide array of tools in the market that aid penetration testers and network administrators in evaluating and building a secure network infrastructure for offensive security purposes. Most of these tools are freely available, open-source software designed for ethical hacking and specifically designed to work efficiently on Linux machines. By employing the essential tools, numerous stages of penetration testing can be executed. There exist several tools such as scanning tools, testing tools, working platforms, and vulnerability detection tools. The methodologies employed to demonstrate this security evaluation are enumerated in Table 1 [7-10].

The following tools were initially tested to work virtually with Cisco equipment.

• Graphical Network Simulator; Cisco Configuration Expert.

• Professional VMware Workstation 15.

If Windows XP is used as the target machine for application penetration testing:

• Establish a physical connection between the routers using the suitable cables.

• Establish a physical connection between the LAN interfaces of the routers and the corresponding switches.

• Establish a connection between the PCs and the switches.

• Follow the instructions to set up the IP addresses for the PCs and routers.

• Following a successful configuration, the personal computers should have the capability to establish a connection and exchange network packets with one another using the ping command.

Many tools and frameworks used by operating systems to conduct experiments [11-15].

5. Methodology

A successful penetration testing methodology incorporates a step-by-step procedure for a tester to follow. Our work is depicted in the same way as the steps in this methodology as shown in figure 3.

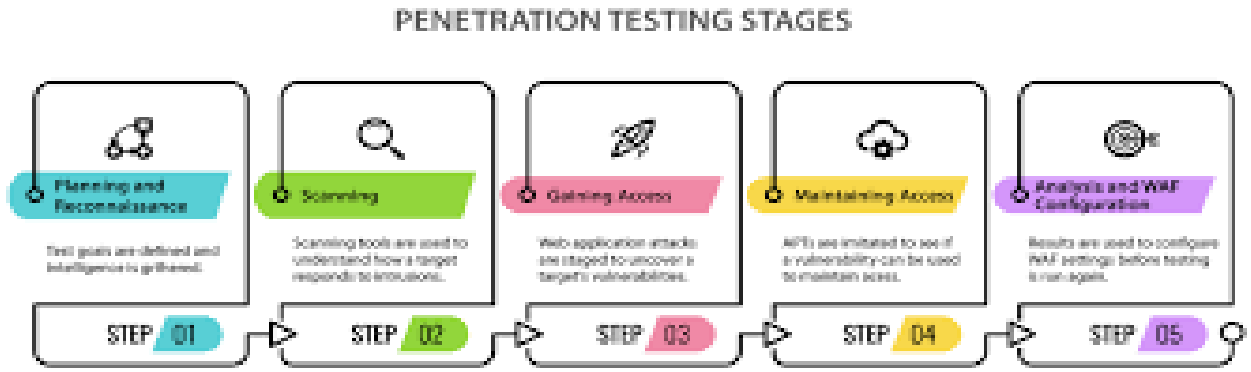

Figure 3: Step by Step Pen Testing

Based on this article, the most pertinent future endeavour would involve exploiting vulnerabilities in the BGP protocol to intercept network traffic by transmitting malicious packets among trusted peers. Utilise the Ruby programming language to develop Metasploit scripts with the innovative objective of executing potent exploits against safeguarded vulnerabilities in various Windows configurations. Moreover, the study and construction of fuzzer code is both stimulating and enables the sending of manipulated packets to many susceptible applications. By viewing penetration testing as a regular software application, businesses may effectively and confidently secure their network with minimal knowledge. In addition, social engineering is often disregarded, leading to an undetected vulnerability. Implementing logical strategies to enhance confidentiality at social gatherings and on online platforms might effectively reduce an attacker's ability to obtain information [16-22].

6. Results

For formal customer reasons, results must be prepared. Mitigation techniques must also be included in this document. The following are some of the most effective mitigations for this type of intruder attack.

Turn off any superfluous services.

• Regular updates on operating systems

• Enabled firewall • Trustworthy anti-virus • Server-side IDS/IPS configuration and a strong DMZ

7. Conclusion

This paper proposes a technique for doing penetration tests on a live network. Vulnerabilities are discovered through the use of a range of tools and programmes, regardless of operating system or usability. The study is followed by a full introduction to various penetration testing, BGP, testing tools, and frameworks. The applicability and practicality of the penetration testing approach were supported throughout the study. A prototype of an organisational network based on the present primary internet domain protocol (BGP) is demonstrated in the lab. Finally, penetration testing is the most secure level [27-23].

This is a network evaluation since it examines elaborated vulnerabilities in a physical network, which aids in mitigation. Despite network equipment and server makers' best attempts to prevent known vulnerabilities, new threats arise on a regular basis. Vulnerabilities are unavoidable since developments in sophisticated technology are unavoidable. Successful penetration testing employing suitable methods on a regular basis maintain the security of any organisation, winning consumer trust.

Using this article as a basis, the most relevant future work would be to attack BGP protocol weaknesses to capture traffic by sending malicious packets among trusted network peers. Using the Ruby programming language, create Metasploit scripts with the novel purpose of launching effective exploits against protected flaws in diverse Windows settings. Furthermore, fuzzer code is exciting to learn and build, and it facilitates in the transmission of forged packets to a range of vulnerable applications. Most significantly, treating penetration testing as if it were any other software application will enable organisations to confidently secure their network with little understanding. Furthermore, social engineering is usually overlooked, resulting in an undiscovered back door. Logical techniques of emphasising secrecy during social gatherings and on websites will aid in reducing an attacker's information collecting.

8. Reference

[1]. Kali Linux Tools.” Kali Linux Tools. N.p., n.d. Web.25 sep. 2014.

[2]. THE METASPLOIT PROJECT” Metasploit. Rapid7, 20 Oct. 2010. Web. 01 Oct. 2014.

[3]. Maynor, David, K. K. Mookhey, Jacopo Cervini, Fairuzan Roslan, and Kevin Beaver. "Metasploit Toolkit for Penetration Testing Exploit Developement." (2007): n. pag. Www.syngress.com. SYNGRESS. Web. 3 sep. 2014.

[4]. Silberman. "Metasploit: Reconstructing the Scene of the Crime." BHUSA, 2009. Web. 10 Sept. 2014.

[5]. Miller, M. "Metasploit's Meterpreter." (2004:(n. pag. Web. 25 Sept. .2014

[6]. https://dev.metasploit.com/documents/meterpreter.pdf.<

[7]. Become an Kali linux OpenStack Expert." The Leading OS for PC, Tablet, Phone and Cloud.

[8]. Canonical Ltd, n.d. Web. 08 Sept. 2014.

[9]. Lyon, Gordon. "Nmap - Free Security Scanner For Network Exploration & Security Audits." Nmap - Free Security Scanner For Network Exploration & Security Audits. Secure Software Developer, n.d. Web. 12 Sept. 2014.

[10]. M. Abdel-Azim, M., Awad, M. M., & Sakr, H. A.,” VoIP versus VoMPLS Performance Evaluation”, International Journal of Computer Science Issues (IJCSI), 11(1), 194, 2014.

[11]. Mohameda, M. A., M. M. Awadb, and H. A. Sakrc. "RSVP BASED MPLS VERSUS IP PERFORMANCE EVALUATION." The Mediterranean Journal of Computers and Networks 10.2 (2014).

[12]. H.A.Sakr, and M.A.Mohamed, “Performance Evaluation Using Smart: HARQ Versus HARQ Mechanisms Beyond 5G Networks”, Wireless. Pers. Communication (Springer), pp.1-26, ISSN:1572-834X, June 2019.

[13]. Abeer Twakol Khalil, A. I. Abdel-Fatah and Hesham Ali sakr, “Rapidly IPv6 multimedia management schemes based LTE-A wireless networks", International Journal of Electrical and Computer Engineering (IJECE),vol. 9, no.pp. 3077-3089,2018.

[14]. H. A. Sakr, A. I. Abdel-Fatah, A. T. Khalil, “Performance Evaluation of Power Efficient Mechanisms on Multimedia over LTE-A Networks”, International Journal on Advanced Science, Engineering and Information Technology, (IJASEIT), vol. 9, no. 4, pp.1096-1109, 2019 .

[15]. H.A. Sakr and M.A. Mohamed, ‘Handover Management Optimization over LTE -A Network using S1 and X2 handover', Proc. of The Seventh International Conference on Advances in Computing, Electronics and Communication – ACEC 2018, ISBN: 978-1-63248-157-3 doi: 10.15224/978-1-63248-157-3-11, pp. 58–64, 2018.

[16]. Sakr, A., Magda I. El-Afifi, and Plvar Team. "Intelligent Traffic Management Systems: A review." Nile Journal of Communication and Computer Science 5.1 (2023): 42-56.

[17]. Sakr, H. A., Ibrahim, H. M., & Khalil, A. T. (2022). Impact of Smart Power Efficient Modes on Multimedia Streaming Data Beyond 5G Networks. Wireless Personal Communications, 1-37.

[18]. . Soomro, A. M., Naeem, A. B., Senapati, B., Bashir, K., Pradhan, S., Maaliw, R. R., & Sakr, H. A. (2023, January). Constructor Development: Predicting Object Communication Errors. In 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T) (pp. 1-7). IEEE.

[19]. Soomro, A. M., Naeem, A. B., Senapati, B., Bashir, K., Pradhan, S., Ghafoor, M. I., & Sakr, H. A. (2023, January). In MANET: An Improved Hybrid Routing Approach for Disaster Management. In 2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T) (pp. 1-6). IEEE.

[20]. Mansour, Nehal A., and Hesham A. Sakr. "The Role of data mining in healthcare Sector." Nile Journal of Communication and Computer Science 4.1 (2023): 1-11.

[21]. Ibrahim, M., Bajwa, I. S., Sarwar, N., Hajjej, F., & Sakr, H. A. (2023). An Intelligent Hybrid Neural Collaborative Filtering Approach for True Recommendations. IEEE Access.

[22]. A. A. Eladl, M. I. El-Afifi, M. A. Saeed, & M. M. El-Saadawi, Optimal operation of energy hubs integrated with renewable energy sources and storage devices considering CO2 emissions. International Journal of Electrical Power & Energy Systems, 2020,117, 105719.

[23]. A. A. Eladl, M. I. El-Afifi, M. M. El-Saadawi, & B. E. Sedhom, A review on energy hubs: Models, methods, classification, applications, and future trends. Alexandria Engineering Journal, 2023, 68, 315-342.

[24]. M. I. El-Afifi, M.M. Saadawi, & A. A. Eladl, Cogeneration Systems Performance Analysis as a Sustainable Clean Energy and Water Source Based on Energy Hubs Using the Archimedes Optimization Algorithm. Sustainability, 2022,14(22), 14766.

[25]. A. A. Eladl, A. A., M. E. El-Afifi, & M. M. El-Saadawi, Communication technologies requirement for energy hubs: a survey. In 2019 21st International Middle East Power Systems Conference (MEPCON), 2019, (pp. 821-827).

[26]. A. A. Eladl, A. A., M. E. El-Afifi, & M. M. El-Saadawi, Optimal power dispatch of multiple energy sources in energy hubs. ERJ. Engineering Research Journal, 2018, 41(4), 279-287.

[27]. A. A. Eladl, M. I. El-Afifi, M. M. El-Saadawi, & B. E. Sedhom, Distributed optimal dispatch of smart multi-agent energy hubs based on consensus algorithm considering lossy communication network and uncertainty. CSEE Journal of Power and Energy Systems., 2023.