Mesopotamian journal of Cybersecurity
Vol.2023, **pp**. 93–103
DOI: https://doi.org/10.58496/MJCS/2023/014, ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/CyberSecurity

Research Article

A Process of Penetration Testing Using Various Tools

Dr. Deepika Kongara[1,*], Shivani Krishnama[1,]

[1]*Information Technology, Kakatiya Institute of Technologies and Science, Warangal, India.*

ARTICLE INFO

Article History
Received 7 Feb 2023
Accepted 20 April 2023
Published 26 April 2023

Keywords
Testing, Vulnerability
Kali
Exploit
Nmap
Metasploit
Google dorks
Information Gathering
Hacking.

ABSTRACT

In the present world, information and data are the greatest assets one can possess. If one cannot secure their information from cyber-attacks, they would lose everything in the blink of an eye. Penetration testing can help reduce this cyber-risk exposure of clients' data and protect them. Penetration testing (also called "pen testing") is a part of ethical hacking that exposes the weak areas, vulnerabilities, or loopholes in the core of a PC, its networks, and its applications with the purpose of securing the system. The main idea of pen testing is to find vulnerabilities in systems and fix them before attackers can take advantage of them. These vulnerabilities are identified, exploited, and analyzed in five phases: information gathering, scanning, gaining access, maintaining access, and covering tracks. Penetration testing is done regularly in order to maintain high-security standards. As it pertains to any organization's secrecy and privacy, this testing is also constrained by a number of legal agreements. The work provided by many researchers in the field of penetration (PEN) testing is reviewed and analyzed in this paper. This report gives a detailed description of the process and tools used to conduct penetration testing.

1. INTRODUCTION

There are occasional news reports of a significant IT company becoming the target of cybercrimes like data breaches and hacking. These companies are losing confidential information and disclosing the private information of their customers due to security flaws in their systems, which can be resolved. If penetration testing is performed on these systems, loopholes or vulnerabilities can be identified even before an attack takes place [1]. **Penetration testing** can be defined as a cyberattack performed on a personal computer, networks, application, or the web to find loopholes in the system and exploit them with the client's consent. For every client, the duties and scope of a pen tester differ according to the security levels of the company. The budget, time, and scope of the organization's penetration testing are all important considerations for every pen tester when selecting the ideal tool for each stage of the process. At the end of penetration testing, the analysis and outcome of the testing report are given to the client. Suggestions are also included in the report to avoid further cyberattacks. A Penetration test is only performed with a license and official agreement with the client organization which is the only difference between this attack and an actual cyber-attack [2].

1.1 Penetration Testing Strategies

There are 3 fundamental approaching strategies for performing penetration testing. Each approach here is differentiated based on the level of knowledge the penetration tester has about the client's network or system.

1.1.1. Grey Box Penetration Testing

In Grey Box Testing the pen tester has finite knowledge and access to internals. In this case, the tester has basic information about the client, such as their IP addresses, hostnames, emails, URLs, etc. In this approach, the tester is given access to design the documents, and the testing is done from the user's perspective rather than that of the creator. Grey box testing is faster compared to white box testing.

*Corresponding author. Email: b20it012@kitsw.ac.in

1.1.2. Black Box Penetration Testing

In black box testing (also called closed box testing), the tester has no information about the target. This kind of approach takes a lot of time compared to any other approach due to the lack of knowledge and access to internals. This type of testing can only be performed by skilled testers. In this approach, only a limited number of test cases are executed. Here the tester performs from the perspective of a potential hacker.

1.1.3. White Box Penetration Testing

In white box testing, the pen tester has all the information about the client, even their logins. As the tester is provided with most of the information, it saves a lot of time, and they can perform many test cases. The tester performing white box testing must have good programming and logical skills. This type of testing is faster and less expensive than any other testing approach.

2. LITERATURE SURVEY

Bishop [1] argued that a computer system or network need not be the "aspect" being tested. It might also be a building, a team of people working in an office, or a network of computers. He further described the resources needed for testing and the knowledge possessed by attackers by using suitable examples. Rajiv Pandey et al.'s [2] aim is to implement penetration testing in a controlled environment. In this case, a Raspberry Pi 3B+ is used to investigate, evaluate, and detect network flaws. They have designed a portable, minimal, and cheaper VAPT device using the Raspberry Pi 3B+. This is done in a Kali Linux environment. Aileen G. Bacudio et al. [3] utilized two web applications named TuneStore and BOG to explain the procedure for performing web application penetration testing. Using a fingerprinting attack and the fiddler tool, HTTP headers for TuneStore are obtained for information gathering. Further SQL injection vulnerabilities are tested and exploited. They have concluded that TuneStore has an XSS vulnerability using WebScarab's buzzer feature. They also showed that by exploiting this vulnerability, one can get their hands on important data, which is achieved by creating a fake website and including material that entices users to input private data. Hessa Mohammed Zaher Al Shebli and Babak D. Beheshti [4] explained different approaches to penetration testing, penetration testing advantages, the procedure to follow while performing a penetration test, its phases, and frequently used tools such as NMap, Cain and Abel, BeEF, Metasploit, and Nessus with their applications. He also discussed individual ethics and organizational procedures for managing the vulnerabilities identified. Jayasuryapal et al. [5] discuss the procedure for conducting network penetration testing in strong organizations. According to them, enumeration is the focal point of the entire testing phase, where a tester cross-checks their information from the information gathering phase and decides whether further information is accurate or not. The tester will draw conclusions about the results and determine how to take advantage of the target firm if it is They concluded that a penetration tester can execute reliable and high-quality network testing if they have a superior technique. Parvin Ami and Ashikali Hasan [6] proposed a penetration testing model that offers a precise, organized, and planned approach for performing a pentest in seven steps. This strategy allows the tester to accomplish more in less time, securing more systems without compromising the overall standard of their testing. They suggested this approach to small IT companies due to its lower cost and automated guidance, which offers services and tools to both novice and expert pen testers.

V.V.N. Suresh Kumar [7] made comparisons between manual and automated penetration testing and concluded that, if correctly used, automated technologies may be more productive and efficient. He also compared external and internal testing and concluded that internal testing would be a better choice. He further explained different penetration testing strategies and how ethical hackers use their network expertise and experience to find vulnerabilities in systems and safeguard them. Sudhanshu Raj and Navpreet Kaur Walia [8] explained how to use a Metasploit Framework tool for the Android operating system using a test case with detailed procedures at each phase of testing along with the commands (syntax) to be executed once access to the target is gained. This process is carried out in a Kali Linux environment. They have pointed out many security flaws and identified potential dangers that could allow hackers to access a system, particularly on smartphones. Matthew Denis et al. [9] demonstrated various penetration tests that make use of private networks and their potential defense mechanisms in the Kali Linux environment. They have insisted that testers should be particularly prepared for man-in-the-middle attacks, and MITM attacks are successful due to a lack of OS hardening and patching. They came to the conclusion that the same techniques used to thwart attacks could also be used to gather information and exploit They also suggested that without knowing or understanding vulnerabilities, one cannot prevent cyberattacks. Penetration testing, according to Budiarto et al. [10], provides a bird's-eye view of the state of security. Their aim was to make a model for security experts to understand penetration testing. Unlike software engineers, security experts don't have a common model of guidelines to utilize while performing penetration testing. The currently used methodology places a strong emphasis on specifics, which vary depending on the situation. The proposed model is made up of commonly employed techniques that follow a similar trend or pattern. R. Sri Devi and M. Mohan Kumar [11] gathered data from different organizations and IT industries. Then, using the hostname or ID, vulnerability analysis and assessment were carried out for several websites. Using various tools such as Nikto, Nmap, Netcraft, and OWASP’s Zed in a Kali environment, all these tools are analyzed and compared. Their

main goal was to discuss security flaws in network infrastructure and web applications and describe them in detail via penetration testing. They concluded that when the Nikto and ZAP tools' results were compared, Nikto revealed more vulnerability. Gurline Kaur and Gurpreet Kaur [12] described penetration testing as a test performed by any organization that attacks itself in order to find its loopholes. They further described different types of penetration testing techniques and various tools used for conducting penetration testing, and they differentiated ethical hacking from penetration testing. Aar et al. [13] described four port scanning tools (Map, Unicornscan, Dmitry, and Hping3) and compared them using eight criteria. They concluded that Dmirty scans faster than any other tool while providing OS and service identification. And Hping3 required the most time for port scanning. Nmap and Hping3 found the majority of open ports, while Dmitry found the least number of them. Aleksandar Hudic et al. [14] refer to the root as a superclass that is divided into six child nodes that are each designated as a subclass. The framework and its subclasses were created and organized. The subclasses created are information gathering, utility, application domain, technology, physical security, and compliance. Ge Chu and Alexei Lisitsa [15] suggested an approach using the belief-desire-intention (BDI) agent model, which can even interact with dynamic, unpredictable, and complicated targets for the purpose of automating penetration testing. They used the BDI reasoning cycle to describe the penetration testing process. They concluded that local buffer overflow attacks cannot be performed by the BDI agent, while remote buffer overflow attacks using the BDI agent were successful.

3. PROPOSED METHODOLOGY

The proposed methodology implies five phases: information gathering, scanning, gaining access, maintaining access, and covering tracks. All these phases are conducted in a Kali Linux environment. The procedure for conducting penetration testing is as follows: Fig. 1.

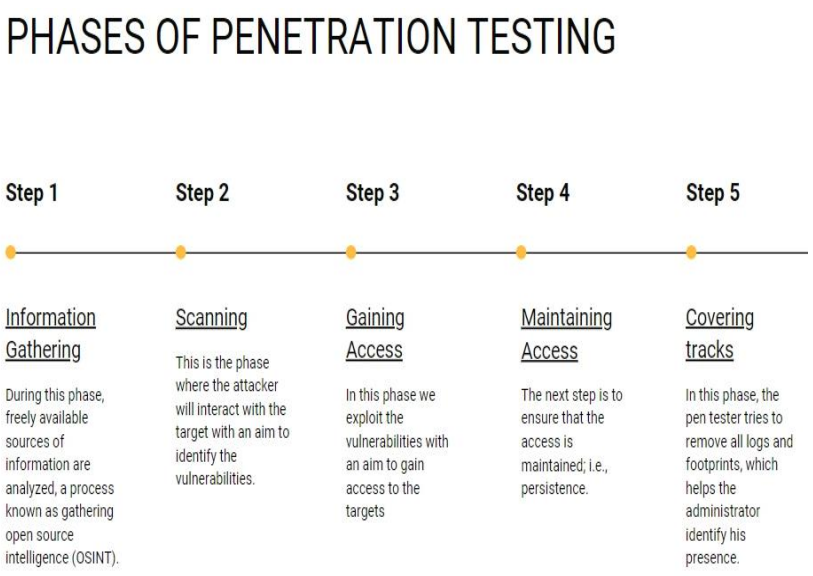


Fig. 1. Phases of Penetration Testing.

Testers need to perform all five phases of penetration testing and generate a report on their findings through this process. Tools such as Kioptrix, Metasploit, Nmap, and nslookup are used for penetration testing during each phase to find, exploit, and analyze vulnerabilities. In the information-gathering phase, the tester collects useful data about the target from both online sources and Kali Linux tools. Popularly used online sources are whois, ip2location, hunter.io, dnschecker.org, and shodan.io. Popularly used kali tools are harvester, and redhawk. In the scanning phase, vulnerabilities such as open ports of the target are found using a scanner. The vulnerabilities found from this phase are exploited in the gaining access phase. Once the target PC is compromised, the tester needs to maintain access to work further, which is done in the maintaining access phase. Then, in covering tracks phase tester cleans all the paths through which they could get caught.

4. EXPERIMENTATION AND RESULTS

To perform penetration testing and use particular tools to perform testing, one needs to set up a virtual lab. This also protects your PC from malicious outputs resulting from testing (like viruses from malware analysis).

Installing Kali- One can choose their vulnerable machine according to their preferences, targets, and usage type (personal or professional). Some of the best available software programs are VMware and VirtualBox, while VirtualBox is preferable for personal use. After the installation of VirtualBox or VMware, the pen testing is performed in the Kali Linux environment which is to be installed from the internet. Once Kali is installed, it is imported into VirtualBox. The default login and password for Kali Linux are "kali" and "kali" respectively.

Fig. 2. Kali Linux Environment through VirtualBox.

After the Kali Linux installation, the user needs to install all the other tools required to perform pen testing. Some of the useful virtual machines to be installed prior to tools are:

- Metasploitable
- Kioptrix level 1.0
- Kioptrix level 1.2
- Mr. Robot

Some of the useful tools that are to be installed in the environment are as follows:

- Ncat
- Netcat
- Wireshark
- Nessus
- Discover Tool

To perform operations or execute commands in a Kali Linux environment, the user should know the basics of bash scripting and command-line basics. One of the best features of Kali Linux is that it has Cherrytree, which is for keeping notes. It has some amazing features. It is important to keep track of findings for a pen tester. The code from Kali Terminal can be directly copied and pasted onto these notes.

4.1. Information Gathering

Information gathering is the most important phase of pen testing. A person who has little to more knowledge of ethical hacking would spend most of the time in this phase. Some of the free online websites used for information gathering are archieve.org, whois.com, and netcraft.com. More the information the more and easier the findings.

4.1.1. Archive.org

The Wayback Machine (Archive.org) website is just like a time travel to know about how our desired target website looked through the years and the information it has on its website through the years. One can even inspect the code and check

for the coding done from time to time. Once the user gives the target website's address on the website, snapshots of the target website are displayed. In this way, information can be gathered.

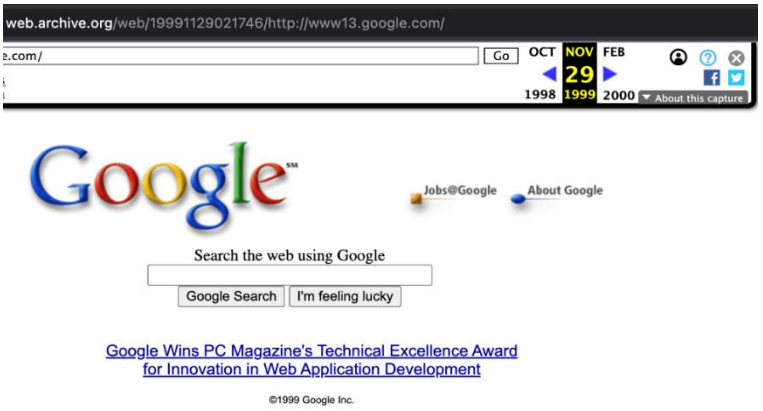


Fig. 3. Snapshot of Google in 1999 using archive.org.

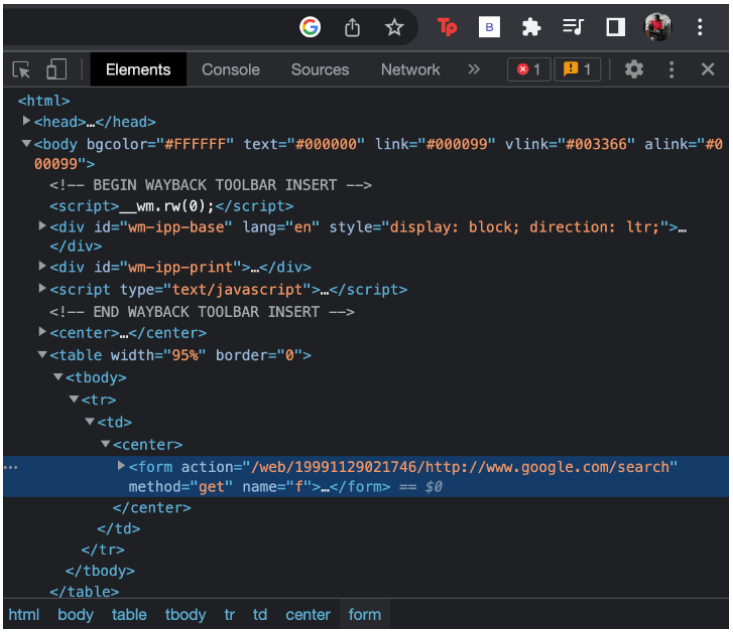
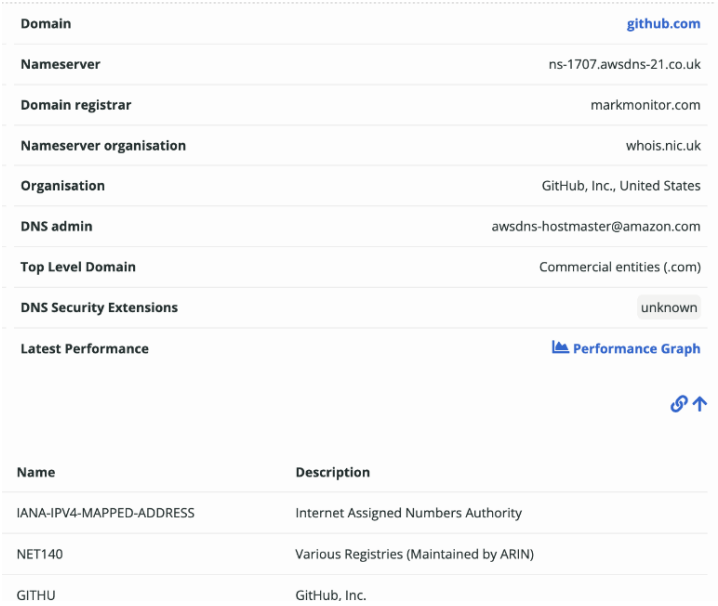


Fig. 4. Inspecting Code of Google Website in 1999 through archive.org.

4.1.2. Netcraft.com

Through this website, information such as hosting companies, origin, IPv4 and IPv6 addresses, hosting history, and other information about the target can be known.



Domain	**github.com**
Nameserver	ns-1707.awsdns-21.co.uk
Domain registrar	markmonitor.com
Nameserver organisation	whois.nic.uk
Organisation	GitHub, Inc., United States
DNS admin	awsdns-hostmaster@amazon.com
Top Level Domain	Commercial entities (.com)
DNS Security Extensions	unknown
Latest Performance	**Performance Graph**

Name	Description
IANA-IPV4-MAPPED-ADDRESS	Internet Assigned Numbers Authority
NET140	Various Registries (Maintained by ARIN)
GITHU	GitHub, Inc.

Fig. 5. Site report on Github through Netcraft.

4.1.3. Google Dorks

Google dorks that come in handy for efficient search in google are-

1. For titles, use the keyword intitle: "desired title search."
2. For URLs, use the keyword inurl: "desired search."
3. For text, use the keyword intext: "desired search."
4. For caching, use the keyword cache: "desired search."
5. For related, use the keyword related: "desired search" gives the alternative or related searches for our desired search.
6. For live camera access, use the keywords view.shtml, network camera, live view, axis, guest images, and more.

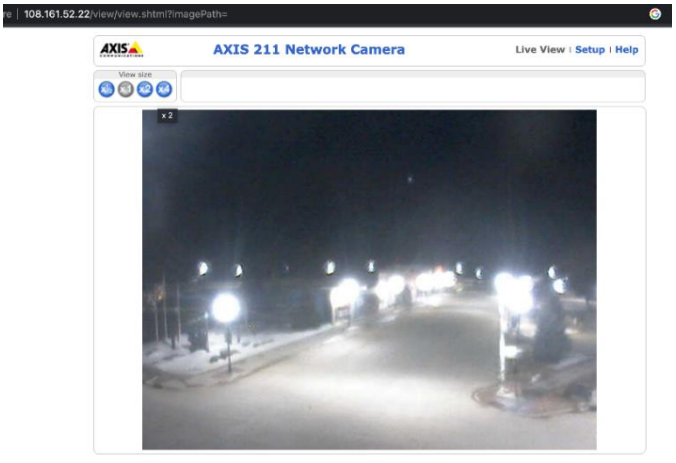


Fig. 6. Live camera access through Google.

Being a pen tester, one just can't rely on only online sources and the information gathered from them. Instead, other tools are used to gather information.

4.1.4. Nslookup

The nslookup tool is pre-installed in both windows and Kali Linux. For a simple command using this tool, the syntax is **nslookup target_domain**. If the tester needs it to be more interactive, the tester can declare the types as type=mx, where mx means Mail eXchange. There are many types, and according to what type of result the tester needs, the type can be chosen.

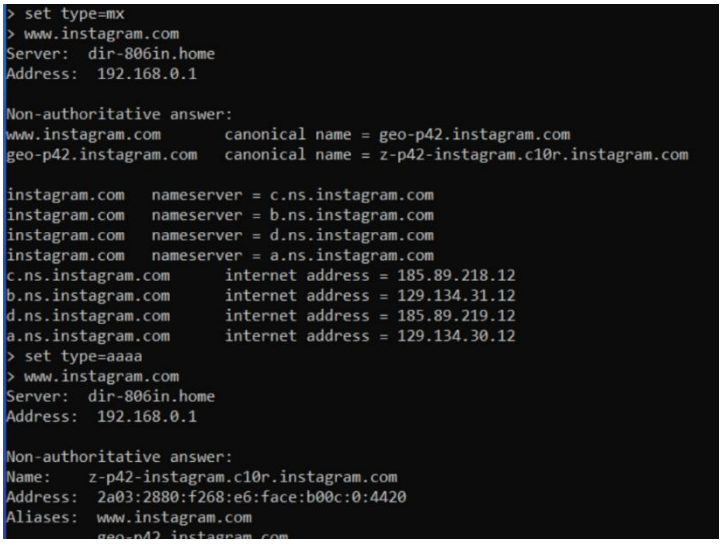


Fig. 7. Nslookup Tool in Kali Linux.

4.1.5. theHarvester

theHarvester tool is pre-installed in Kali Linux. This tool is used to recover emails from our target domain. To start this tool, execute the harvester command in Kali Terminal. Then the tester enters into theHarvester tool. Syntax - **theHarvester -d abc.com -l 200 -b source_name**

Here, d represents the domain, while abc.com is the target domain, l represents the limit of the search, and b represents the source from which information is to be gathered. For general purposes, **all** are preferred. In order to break online login credentials or obtain access to a person's email account, this tool is utilized. Employee names can also be extracted using google, Linkedln, or any other open-source using this tool. Due to its effectiveness, simplicity, and ease of use, it is also intended to assist the pen tester at an earlier stage.

Fig. 8. The Harvester Tool in Kali Linux.

4.1.6. Discover tool

The Discover tool is not pre-installed. This tool is available on github which can be copied and cloned onto Kali terminal to initialize it. To use this tool, the first step is to change directories to discover. The discover tool has plenty of options to scan, which are more helpful to pen testers than any other tools.

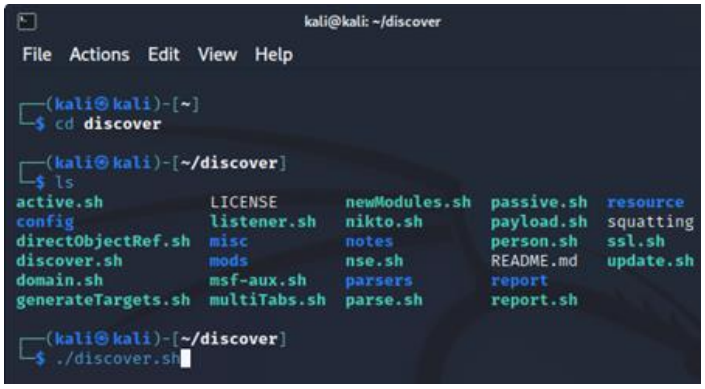


Fig. 9. Basic commands in the Discover tool.

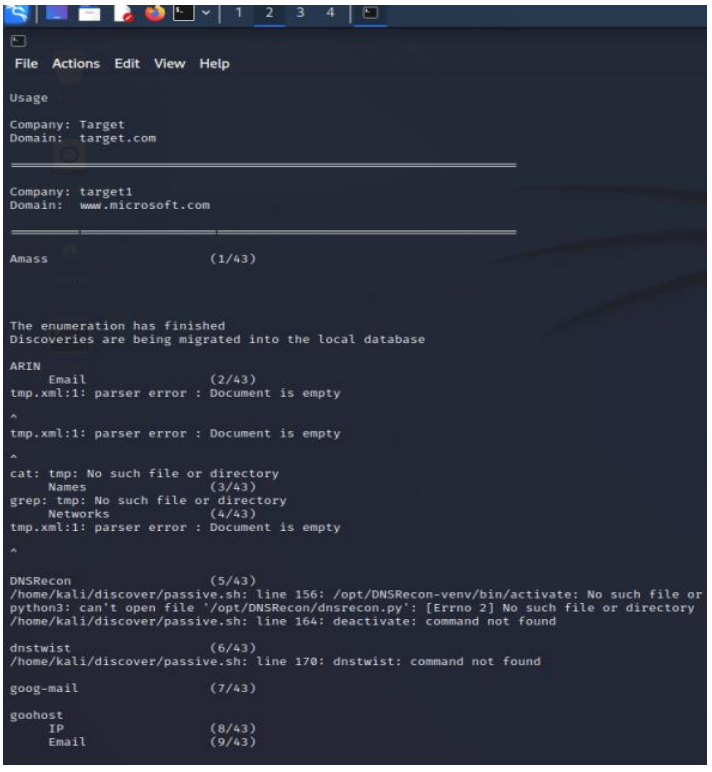


Fig. 10. Discover tools using different tools such as whois, Metasploit, Google, and others.

4.2. Scanning

In the scanning phase, different scanners and network mappers are used to identify vulnerabilities or loopholes. Some of the scanners used are Metaploit scanning, Nmap scanning, and Nessus scanning.

4.2.1. Nmap scan

Nmap scanning has various options for scanning. Through this tool, one can find the open ports through which exploitation is done. To know the different options available the command **nmap** is used in Kali terminal. Selecting any of the options, scan the target as **nmap -sn 10.5.2.0/24,** where sn is the option to stop port scanning after host discovery. This is also known as "ping scanning." Scan reports are generated once scanning is complete.

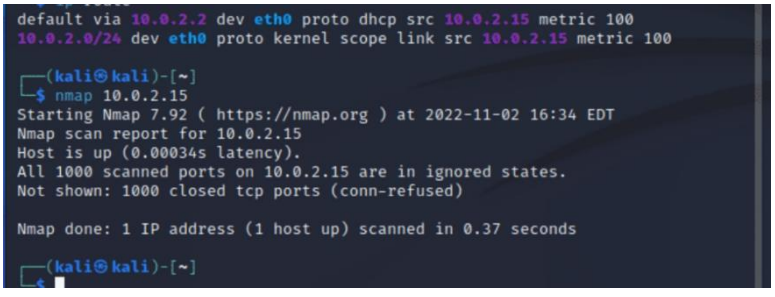


Fig. 11. Nmap Tool in Kali Linux.

4.2.2. Metasploit scan

To initialize, go for the command - **msfconsole** which is metasploit framework console. For scanning, the command "**search portscan**" is used. Then, using a scanner, one can set ports, rhosts, threads, and much more. Then ports are scanned to look for open ports. In this way, all the ports are scanned.

4.3. Gaining Access

In the gaining access phase, the vulnerabilities (open ports) that were found in the previous phase are exploited, and access to the target is gained. Tools used for gaining access are Metasploit and Nmap.

A nmap command through which a tester can gain access is **hydra -t 4 -v -f -l ab -p cd,** where -**v** is verbose mode, -t is the total number of parallel connects, **-l** is the login name if the login name is not known, a text file of logins can be included using option -**L**, and the same goes for p password.

4.4. Maintaining Access

The importance of this phase is that once the tester gets control over the target system through gaining access phase then if the target shuts down their system or reboots the system as soon as the tester gains access, the temporary access would be lost. To prevent this, the tools used are-

- Metasploit
- **Keylogging:** In this approach, all the activities done on the keyboard are recorded and stored in a text file for which we assign a time.
- **Backdoor**: This is one of the best approaches for maintaining access. Through a backdoor, an application is installed onto target system by which the access would remain. This approach is hardly noticeable.
- **Remote access**: in this approach, remote access from the target is enabled when access is gained. A person who has little to medium knowledge of system networks would notice this attack. So this approach is not suggested.

4.5. Covering Tracks

In this phase, the tester would erase all the tracks or information left in any phase through which one could reach him. After completion of all phases, a report is made of all findings, which is then submitted to the client.

The notes from CherryTree for Kali Linux can also be included. The report should contain an introduction, the scope of the penetration test, all the findings or results from the five phases, a description of the risk found through penetration testing, and an estimation of the loss that would occur if an attacker actually exploited the client system, network, and application. A report should also contain suggestions for avoiding such loopholes or vulnerabilities in the future.

5. CONCLUSION

Penetration testing is the process of finding loopholes in systems and exploiting them. For maintaining security standards and to avoid financial loss, data loss, and reputation loss, penetration testing is preferred. The strategy to follow can be decided according to the information presented by the tester. An overview of the tools and process required to perform penetration testing is given in the paper. The tools differ from client to client according to the target systems and scope of the network. One cannot expect to find all the vulnerabilities in a single pen testing session in a limited amount of time. In this paper, using suitable tools, vulnerabilities are explored and exploited in five phases (information gathering, scanning, gaining access, maintaining access, and covering tracks), and basic commands are specified.

Funding

None.

Conflicts Of Interest

The authors declare no conflicts of interest.

Acknowledgment

None.

References

[1] M. Bishop, "About penetration testing," IEEE Security & Privacy, vol. 5, no. 6, pp. 84-87, 2007.

[2] R. Pandey, V. Jyothindar, and U. K. Chopra, "Vulnerability assessment and penetration testing: a portable solution Implementation," in 2020 12th International Conference on Computational Intelligence and Communication Networks (CICN), 2020, pp. 398-402.

[3] A. G. Bacudio, X. Yuan, B. T. B. Chu, and M. Jones, "An overview of penetration testing," International Journal of Network Security & Its Applications, vol. 3, no. 6, pp. 19, 2011.

[4] H. M. Z. Al Shebli and B. D. Beheshti, "A study on penetration testing process and tools," in 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2018, pp. 1-7.

[5] G. Jayasuryapal, P. M. Pranay, and H. Kaur, "A Survey on Network Penetration Testing," in 2021 2nd International Conference on Intelligent Engineering and Management (ICIEM), 2021, pp. 373-378.

[6] P. Ami and A. Hasan, "Seven phrase penetration testing model," International Journal of Computer Applications, vol. 59, no. 5, pp. 16-20, 2012.

[7] V. S. Kumar, "Ethical Hacking and Penetration Testing Strategies," International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), vol. 11, no. 2, pp. 0976-1353, 2014.

[8] S. Raj and N. K. Walia, "A study on metasploit framework: a pen-testing tool," in 2020 International Conference on Computational Performance Evaluation (ComPE), 2020, pp. 296-302.

[9] M. Denis, C. Zena, and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies," in 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 2016, pp. 1-6.

[10] R. Budiarto, S. Ramadass, A. Samsudin, and S. Noor, "Development of penetration testing model for increasing network security," in Proceedings. 2004 International Conference on Information and Communication Technologies: From Theory to Applications, 2004, pp. 563-564.

[11] R. S. Devi and M. M. Kumar, "Testing for security weakness of web applications using ethical hacking," in 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI), 2020, pp. 354-361.

[12] G. Kaur and G. Kaur, "Penetration Testing: Attacking Oneself to Enhance Security," in 2016 International Journal of Advanced Research in Computer and Communication Engineering, vol. 5, issue 4.

[13] P. Aar and A. K. Sharma, "Analysis of Penetration Testing Tools," International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), vol. 7, no. 9, pp. 36, 2017.

[14] A. Hudic, L. Zechner, S. Islam, C. Krieg, E. R. Weippl, S. Winkler, and R. Hable, "Towards a unified penetration testing taxonomy," in 2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Conference on Social Computing, 2012, pp. 811-812.

[15] G. Chu and A. Lisitsa, "Poster: Agent-based (BDI) modeling for automation of penetration testing," in 2018 16th Annual Conference on Privacy, Security and Trust (PST), 2018, pp. 1-2.