Jurnal EVOLUSI

Please cite this article as: Rukhiyah Adnan, & Wan Asiah Wan Muhammad Tahir (2023). Implementing Penetration Testing in Simulation Environment. Jurnal Evolusi, Vol 4 Issue 2, 2023

IMPLEMENTING PENETRATION TESTING IN SIMULATION ENVIRONMENT

Rukhiyah binti Adnan* (a), Wan Asiah binti Wan Muhamad Tahir (b)
Corresponding Author*

Faculty of Computing & Multimedia, Universiti Poly-Tech Malaysia, rukhiyah@uptm.edu.my
Faculty of Computing & Multimedia, Universiti Poly-Tech Malaysia, wanasiah@uptm.edu.my

DOI:
Received 15 November 2023, Accepted 16 November 2023, Available online 31 November 2023

ABSTRACT

Penetration testing or pen testing is crucial to protect systems from cyber risk attacks due to the vulnerabilities in information security. This article presents the implementation of basic penetration testing which focuses on the scanning phase by using two virtual machines which are Kali Linux and Metasploitable 2 installed virtually in a local machine through VirtualBox as one of the virtualization software to simulate the environment. Nmap which is one of Kali Linux tools was used to perform the scanning purpose on Metasploitable 2 as a vulnerable system or target machine. The experiment was conducted in a secured environment thus requiring a secured setting in configuring the VirtualBox. The experimental results show a list of open ports from the Metasploitable 2 machine and thus suggest basic countermeasures to secure the systems. Using Kali Linux as one of the penetration testing tools is beneficial for finding vulnerabilities and alerting pen testers to fix them before attackers can take advantage of them.

ARTICLE INFO

Keywords:

Kali,
Nmap,
Metasploitable 2,
Penetration Testing,
Vulnerabilities

1.0 INTRODUCTION

According to EC-Council (2023), penetration testing or pen testing shares certain similarities with ethical hacking in which both of the processes need to identify vulnerabilities in computing environments and to prevent different types of cyberattacks. Vulnerability is also known as a weakness in a system that can be exploited by attackers. Three types of penetration testing strategies can be used which consist of Grey Box penetration testing, Black Box penetration testing, and White Box penetration testing (Khan et al, 2012). In Grey Box penetration testing, the penetration tester has basic knowledge of the target system, such as initial access credentials or a network infrastructure map. A Black Box penetration test means the penetration tester has no prior knowledge of the target network or system. A White Box penetration test are less like a cyberattack and more like a complete scan of a system at the source code level.

Five main types of penetration tests focus on different security vulnerabilities and tools. For network penetration test, it covers areas in firewall configuration, firewall bypass testing, stateful inspection analysis, intrusion prevention system deception, and DNS-level attacks. Web application penetration test is suitable for problems associated with the insecure design, development, or coding of a web app. Client-side penetration tests will identify security vulnerabilities within an organization such as email platforms, web browsers, and Adobe Acrobat. For wireless network penetration test, it focuses on vulnerabilities in wireless devices such as smartphones while a social engineering penetration test is used for human aspects of an organization's security such as using phishing scams as part of social engineering tests.

Penetration testing phases consist of five phases which cover reconnaissance (gathering as much information about the target system), scanning (to identify open ports and check network traffic on the target system), vulnerability assessment (identifying potential vulnerabilities and determining whether they can be exploited, more powerful than scanning), exploitation (to access the target system and exploit the identified vulnerabilities) and reporting(document the findings and suggest to fix vulnerabilities found in the system).

Kali Linux is freely available and the Linux distribution system is based on Debian. It is specially designed for forensics analysis and penetration testing. It supports different virtual images for x86 and x86-64 architectures used in virtual environments like VMware or VirtualBox. Kali Linux tools such as Nmap can be used for scanning phase purposes. Scanning can be conducted in two ways either passive or active. In a passive scan such as DNS reconnaissance, the pen tester is not directly targeting any port or specific service related to a device on a network while active scanning is directly targeting specific ports or network services to obtain information to enumerate the possibility of a vulnerability existing.

For security research, learning or implementing pen testing in a secured environment, users can install a vulnerable system or machine such as Metasploitable 2 which is also free to download. Therefore, learning how to implement penetration testing in a secure environment helps to create awareness of becoming the target of cybercrimes like data breaches and hacking thus affecting confidentiality, integrity, and availability issues. If penetration testing can be performed earlier, loopholes and vulnerabilities can be identified before an attack takes place.

2.0 LITERATURE REVIEW

Many studies have been done to implement penetration testing for cyber defense. Some of the penetrating testing can be implemented without requiring high costs such as using Raspberry Pi. The tool is suitable, especially for beginners. Kali Linux together with Metasploit is also used in addition to generating the payload required to execute the application to allow a backdoor for remote access from the Raspberry Pi. Rajiv Pandey et al. (2020) proposed practical solutions to implement penetration testing using Raspberry Pi 3b+ and discussed the importance and applicability of smart devices for penetration testing and developing vulnerability assessment.

He-Jun Lu et al (2021) aimed at the vulnerability of wireless networks and proposed a method of WiFi penetration testing based on Kali Linux which is divided into four stages: preparation, information collection, simulation attack, and reporting. The experimental results show that the method of WiFi network penetration testing with Kali Linux has a good effect on improving the security evaluation of WiFi networks. Kashyap et al. (2021) discussed an overview of different penetration open-source tools available in Kali Linux. The step-by-step use of each penetration testing tool, tools analysis, and comparison based on utility and portability are also discussed in the paper. The study is useful for learning the various tools available freely to secure systems networks and web applications.

Besides the proposed methods above, Hessa et al. (2018) explained penetration tests related to factors to be considered while performing penetration test such as the process of conducting the penetration test, commonly used tools and software for conducting a penetration test, and frequently used tools such as Metasploit while Jayasuryapal et al. (2021) discussed the procedure for some of the important terms and steps to do a strong penetration testing on organizations and covered all the mechanisms including information gathering to the post-exploitation. The use of Metasploit and Kali Linux was also explained in another paper. Sudhanshu et al (2020) explained how to use a Metasploit Framework tool which is run in a Kali Linux environment and the phases involved from scanning to exploiting the systems.

Hasan et al. (2017) explained the penetration testing in system administration and the challenges faced by the industry in securing the data and information using different techniques. Various tools can be used on different services Web, database and forensics after sniffing the required information from the system or network. Alhamed et al. (2023), discussed the most common tools used for network penetration testing and potential attacks and strategies that can be used to protect the vulnerable ports by reviewing the related publications.

3.0 METHODOLOGY

Penetration testing involves five phases which are reconnaissance, scanning, vulnerability assessment, exploitation, and reporting. In this article, the experiment focuses on the scanning phase by assuming we already have information on the targeted machine, such as the IP address, which can be obtained during the reconnaissance phase. In the reconnaissance phase, online tools such as Whois can be used to gather information about targeted machines. The procedure for setting up the simulation environment is depicted in Figure 1. The main technical methods in configuring the testing include installing VirtualBox, Kali Linux, and Metasploitable 2, setting up storage size, memory size, and IP address, and ensuring both virtual machines can communicate through the ping command. During the scanning phase, the Nmap command will be performed from Kali Linux to the target machine, which is Metaspoitable2 to reveal the opening ports.

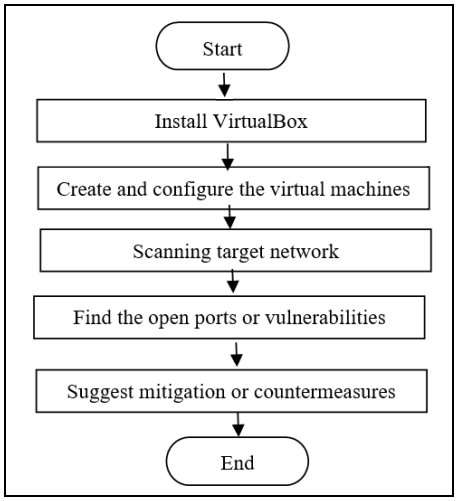

Figure 1. Simulation steps

In the scanning phase, vulnerabilities such as open ports can be exploited in the gaining access phase, thus making the targeted machine compromised, and attackers are able to perform several attacks, such as password attacks and other hacking methods.

4.0 EXPERIMENTATION AND RESULTS

In order to perform penetration testing, one needs to set up a virtual lab. The virtualization environment protects our computer from malware attacking our local host. The experimental environment consists of a physical host or local machine running Windows 11(Processor 11th Gen Intel(R) Core (TM) i7-1165G7 @ 2.80GHz and 16G RAM), two virtual machines (VM Kali Linux-attacker and VM Metasploitable 2-target). Both virtual machines use VirtualBox virtualization technology. All virtual machines are configured by using static IP address in the internal network configuration to simulate the secured environment.

- **Installing VirtualBox**

There are several virtualization software programs available to install, but for personal use, it is advisable to use VirtualBox because of its easy configuration. Figure 2 shows the main interface for VirtualBox once configuration is done.

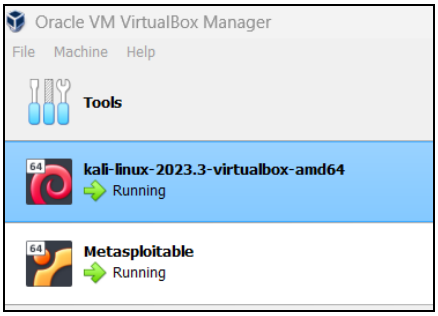

Figure 2. The main interface of VirtualBox

- **Installing Kali Linux**

Figure 3 shows the Linux distro designed for penetration testing purposes, and it uses the Debian kernel. Pen testers can download it for free from their website according to PC specifications. In this experiment, the ISO format is used and configured directly inside VirtualBox. The default login and password for Kali Linux are "kali" and "kali" respectively.

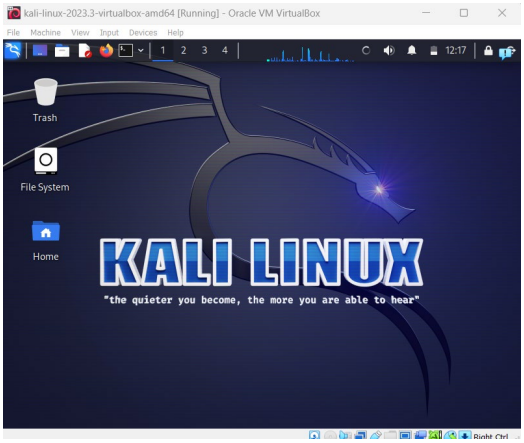

Figure 3. The main interface of Kali Linux.

- **Installing Metasploitable 2**

Another virtual machine that needs to be created is the targeted machine, which is Metasploitable 2 as depicted in Figure 4. This is also a free download from the Rapid7 website. The default login and password for Metaploitable are "msfadmin" and "msfadmin," respectively.

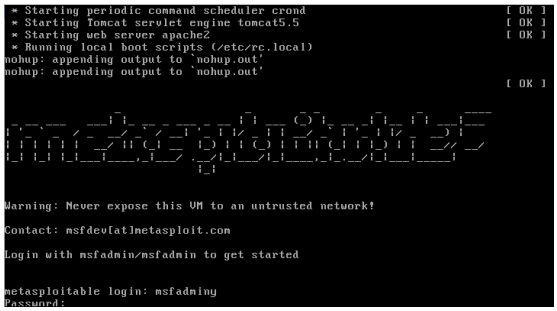

Figure 4. The main interface of Metasploitable 2

- **Performing Nmap command**

Nmap command is obtained in the Kali Linux terminal. Other useful tools are installed in the Kali Linux such as Wireshark, Social Engineering Tool and several forensics tools. To execute commands in a Kali Linux environment, the user should know the basics of bash scripting and command-line basics. Sample Nmap commands and the result from those scripts are as follows.

Figure 5 shows list of open ports starting from port 21 until 8180 together with their services after we performed scanning on a single host or an IP address (IPv4) using this script *nmap ip address*

```
└─$ nmap 10.0.2.15
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-11 22:51 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabl
ed. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.2.15
Host is up (0.0023s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 0.38 seconds
```

Figure 5. Scanning a single host

Figures 6 to 8 show output when we turn on OS (operating system) and version detection scanning script (IPv4) using this script, *nmap -A ip address*

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-11-11 22:58 EST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try
 using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.0.2.15
Host is up (0.00069s latency).
Not shown: 977 closed tcp ports (conn-refused)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.16
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      vsFTPd 2.3.4 - secure, fast, stable
|_End of status
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN,
STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ssl-date: 2023-11-12T03:59:05+00:00; -2s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
```

Figure 6. OS and version detection I

```
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|_    SSL2_RC4_128_WITH_MD5
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/st
ateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
53/tcp   open  domain      ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      37486/udp   mountd
|   100005  1,2,3      37499/tcp   mountd
|   100021  1,3,4      43248/tcp   nlockmgr
|   100021  1,3,4      45045/udp   nlockmgr
|   100024  1          41262/udp   status
|_  100024  1          49297/tcp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  ◆           Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
```

Figure 7. OS and version detection II

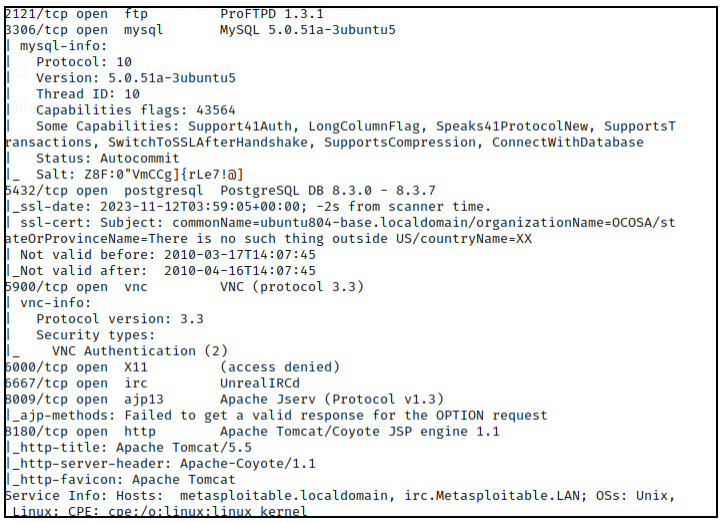

Figure 8. OS and version detection III

Figures 5 to 8 are the results from the scanning process which display all the open ports, operating systems and their services that are vulnerable for attackers to exploit. Thus, several mitigations or countermeasures need to be applied to harden the Metasploitable 2 machine such as by turning off unused ports and server hardening through some configuration in server settings, applications or services that can eliminate directory traversal attacks. Those configurations also require the user to be familiar with Linux script since the operating system running in the Metasploitable 2 is Ubuntu. Any default passwords in the system should be modified as well by using at least 12 characters with combinations of alphanumeric and special characters to avoid password cracking.

5.0 CONCLUSION

Through this experiment, users can practice ethically conducting penetration testing to learn how to find loopholes in systems and how attackers exploit them. The penetration testing of the target machine is carried out through a simulation experiment in a secured environment by using the virtualization concept. The results show that performing basic penetration testing with Nmap in Kali Linux can display all open ports and we can take action on what ports are supposed to be closed or fixed. This also gives ideas on the types of attacks that can be performed according to the ports and services. Overall, various Kali Linux tools can be tested in the future which are suitable for each penetration testing phase and mitigation methods for Metasploitable 2.

REFERENCES

Adamovic, S. (2019), *Penetration testing and vulnerability assessment: Introduction, phases, tools and methods*. In *Sinteza 2019-International Scientific Conference on Information Technology and Data Related Research*; Singidunum University: Belgrade, Serbia, 2019; pp. 229–234.

Alhamed, M., & Rahman, M. M. H. (2023). *A Systematic Literature Review on Penetration Testing in Networks*: Future Research Directions. Applied Sciences, 13(12), 6986. MDPI AG. Retrieved from http://dx.doi.org/10.3390/app13126986

Fatimah, A. (2023). *Impact and Research Challenges of Penetrating Testing and Vulnerability Assessment on Network Threat*. 2nd International Conference on Business Analytics for Technology and Security, ICBATS 2023

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

Hasan, Muhammad Zulkifl & Hussain, Muhammad Zunnurain & Chughtai, Muhammad. (2017). *Penetration Testing In System Administration*. International Journal Of Scientific & Technology Research Volume 6, Issue 06.

H. M. Z. A. Shebli & B. D. Beheshti,(2018).*A study on penetration testing process and tools*. IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 2018, pp. 1-7,doi: 10.1109/LISAT.2018.8378035.

He-Jun Lu, Yang Yu,(2021).*Research on WiFi Penetration Testing with Kali Linux*. Complexity, vol.Article ID 5570001, 8 pages, 2021. https://doi.org/10.1155/2021/5570001

J. N. Goel and B. M. Mehtre,(2015).*Vulnerability Assessment & Penetration Testing as a Cyber Defense Technology,* Procedia Computer Science, vol. 57, pp. 710-715, 2015.

Kashyap, Kajal & Noor, Arti & Saraswat, Rekha & Sharma, V. (2021). *Learning of Penetration Testing Using Open Source Tools for Beginner*. 10.35629/5252-031212871305.

M. E. Khan & F. Khan, (2012). *A comparative study of white Box, Black Box and grey Box testing techniques*. *International Journal of Advanced Computer Science & Applications*, vol. 3, no. 6, pp. 1–12.

P. S. Shinde and S. B. Ardhapurkar, (2016). *Cyber security analysis using vulnerability assessment and penetration testing. In Futuristic Trends in Research and Innovation for Social Welfare*, (Startup Conclave) World Conference on, pp. 1-5, 2016.

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

Shebli, A.; Mohammed Zaher, H.; Beheshti, B.D. *A Study On Penetration Testing Process And Tools. In Proceedings of the 2018 IEEE Long Island Systems*, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, 4–8 May 2018.

S. Raj & N. K. Walia (2020). *A Study On Metasploit Framework: A Pen-Testing Tool*. International Conference on Computational Performance Evaluation (ComPE), 2020, pp. 296-302.

Shariqueb Reza, Feon Jaison. (2021), *A Comparative Study between Vulnerability Assessment and Penetration Testing*, International Journal of Trend in Scientific Research and Development (IJTSRD) 2021

What is penetration testing or pentest?: Types, tools, Steps & Benefits: EC-Council. (2023). Retrieved from https://www.eccouncil.org/cybersecurity/what-is-penetration-testing/