Analysis of Network Vulnerability through Pen Testing

Foram Suthar, Samarat V.O. Khanna

Abstract: Now a day internet becomes a mandate for the people. The usage of the internet is increasing rapidly. Every year new devices are connected to the internet and store their data with positively increase of the usage in the technology and internet also having the dark side of security breaches and cyber-attacks which negatively affect the organization. Security of the system and network is now a topmost priority for the people. Many methodologies and techniques have been used to identify the flaws and vulnerabilities in the system to prevent cyber-attacks. Pen testing is one of the proper processes of getting the loophole of the network. In this paper, we have analyzed network-related vulnerabilities using a black box and white box testing. We have used different pen testing tools to find the loopholes and simulate privilege escalation attacks in the network.

Keyword: Vulnerability, Cyber Attack, Pen testing,

I. INTRODUCTION

Cyber Security is now a day one of the big challenges for organizations. The Growing connectivity of computers being difficult to secure the information and data. Internet becomes mandate for the people now. The global internet population has been increasing from 3.0 billion to 4.5 billion between the years 2014-2020, which is reach 59% of the world's population [16]. People are directly and indirectly releveling the data over the internet which increaser the cyber-attacks. Internet is one of the common way to get sensitive data. Each second, the data being uploaded to the internet is 24,000 GB [17]. The attacker always the connected deceives over the internet and try to identify vulnerability and loophole into the system and web application for accessing sensitive data.

Many cyber-attacks are being reportedin a covid-19 pandemic situations due to vulnerabilities, lack of security training, etc. that cause a major impact on private and government organizations. Many vulnerability detection and prevention techniques are available. A penetration test is a process of systematically and actively testing a network to determine what vulnerabilities may be present and to create reports to resolve these vulnerabilities. The aim of this research is to detect vulnerabilities and flaws in the system through different penetration-testing. Two main pen testing modes have been focused here I. Black Box Testing II. White Box Testing.

In black-box testing tester have basic information about the company, like the company name. The tester will try to get detailed information after doing the fingerprinting process. In white box testing tester have details information about the company.

This paper is organized as follows. Section II discussed literature review. The Proposed methodology discussed in section III. Section VI illustrates the lab work and result about analysis of experiment work shows in section V.

II. LITERATURE REVIEW

Salam et al. [15] provided a broad idea of cloud infrastructure and security threats in the system. The author has implemented a private cloud and applied some pen testing techniques to identify the vulnerabilities and flaws. They have worked on man-in-cloud attacks, DoS attacks, and OpenStack Components attacks. The author has only focused on network-based vulnerabilities and risk.

DORTKARDES et al. [10] have applied various pen-testing techniques in the system to identify the vulnerabilities. The author have created automated pen testing tool and compare the result with the manual test of seven different environments. They mainly focus on to detecting the weakness of social engineering techniques with an automated application tool. The main gap in this research is that they focus more on pen-testing tools instead of vulnerabilities of the system.

Cloud infrastructure is now targeted by different types of attacks because of the diversity of cloud computing models and their security risks. Detailed explanation on Cloud infrastructure and different Cloud models which are available is given by Ali et al. [11].Its emphasis on Virtual network vulnerabilities, security threats targeting the communication layer, and also on user's limited control on their data.

To support testers and overcome white box technique shortcomings, another methodology is called black-box testing. The testers of black-box use no internal knowledge of the web application coding. Nonetheless, many researchers [9, 10] have effectively analyzed and shown constraints and limitations of the Black Box scanner to prevent web vulnerability

III. METHODOLOGY

Penetration testing is the process of evaluating the security of a network or an information system by applying attack to find out vulnerabilities that an attacks cloud exploit. Penetration testing involves an active analysis of system configurations, technical flaws, design implementation weaknesses and loopholes.

Manuscript received on 10 April 2021 | Revised Manuscript received on 20 April 2021 | Manuscript Accepted on 15 May 2021 | Manuscript published on 30 May 2021.

* Correspondence Author

Foram Suthar*, Student, Department of Computer Engineering, Indus University, Gujarat, India. Email: Foram.suthar9@gmail.com

Samarat V.O. Khanna, Former Director of IICT, Indus University, Gujarat, India, Email: drsokhanna@yahoo.com

© The Authors. Published by Lattice Science Publication (LSP). This is an open access article under the CC-BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

It is not only point out the vulnerabilities but also documents how the weakness can be exploited. It is an approach to assessment that encompasses the security audit and vulnerability assessment.

The types of penetration testing depend on the amount of information a pen tester is given about the organization. We are going to focus broadly on two main types of penetration testing.
They are as follows:

1. Black-Box Testing

- Here in black box testing, pen-tester having limited information about the organization. Tester uses different methods like fingerprinting, footprinting to gather more information about the organization. The external attacker got simulated with the help of Black box testing. Test case designingis also difficult without having clear information about the inputs. Black box testing is subdivided into blind testing and double-blind testing.

2. White-Box Testing

- In white-box testing, the organization gives complete details about the network to the pen tester. The information can include network-topology documents, asset inventory, and valuation information. A tester can perform pen-testing with or without the knowledge of IT staff.

The framework is suggested based on our methodology. Different phases of the Framework are shown in figure 1.

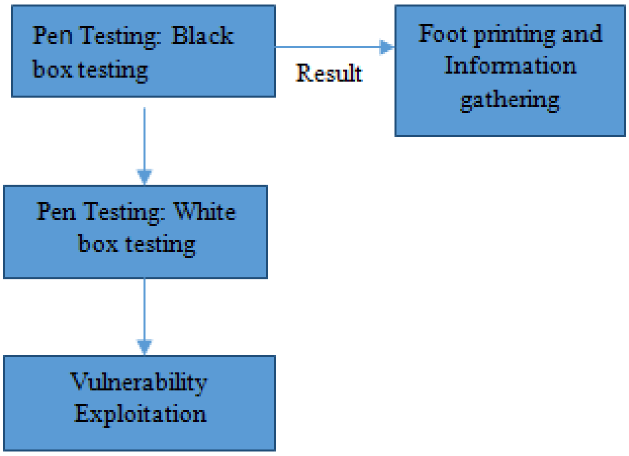

Pen Testing: Black box testing
Result
Foot printing and Information gathering
Pen Testing: White box testing
Vulnerability Exploitation

Figure 1. Framework

IV. LAB EXPERIMENT

An experimental scenario based on the proposed Framework and different phases is shown below:

A. Experimental Scenario

1) Lab Infrastructure:Ubuntu Server 12.04 is used to create this Infrastructure and is fully patched as of early September 2012.It is a boot to root virtual machine based on Linux with SSH and NFS configuration weaknesses. The system architecture is x86 and 512MB RAM.

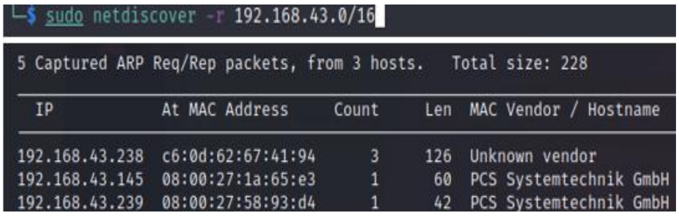
2)Port and Network Scanning: We have used Nmap and netdiscovry for host discovery. These tools will help us to get information of the system such as version, OS, open ports, etc.***3)Penetration Testing Tools:*** We have used Kali Linux for exploitation with Nessus vulnerability scanner. Another tool is used for brute-forcing is hydra. Hydra do brute force attack to get login credentials of the system

Nessus is the apopular tool in vulnerability and scanning and management. This tool scan the system activity and gives a detail report of the weakness and loophole existing in the system or web application.

B. Framework Phases

Phase One: Black box pen testing

In this phase,the first step is to discover the host through footprinting and network scanning process. Netdiscovery command used to get the IP address of the system, which connected in the network. The result of the netdiscovery command have been show in the figure 2. Scanning the network with netdiscovery shows the three different IP addresses where 192.168.43.239 is the IP address of the attacking machine. After getting theIP address of the system next step is to get port-related information. Nmapis used for port and network scanning. The result of the Nmapis shown in Table 1 which indicate that how many ports are open in the system and which services are running on the particular port address. Open port, version and services will always disclose the vulnerabilities, which allows someone for the system or network-based attacks. We have also scanned the system using the Nessus scanner and get some information about the system.



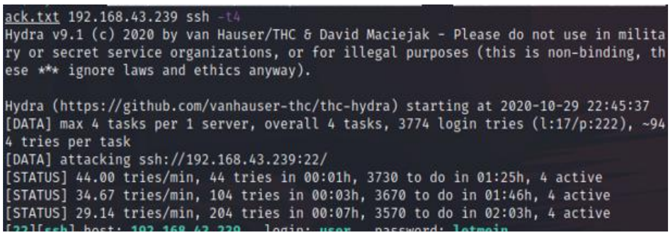
```
└$ sudo netdiscover -r 192.168.43.0/16

 5 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 228
 ______________________________________________________________________
   IP            At MAC Address     Count     Len  MAC Vendor / Hostname
 ______________________________________________________________________

 192.168.43.238  c6:0d:62:67:41:94      3     126  Unknown vendor
 192.168.43.145  08:00:27:1a:65:e3      1      60  PCS Systemtechnik GmbH
 192.168.43.239  08:00:27:58:93:d4      1      42  PCS Systemtechnik GmbH
```

Figure 2. Result of netdiscovery command

Table 1: Nmap Result

Open Port	Services/ Version
22/tcp	ssh/ OpenSSH 5.9p1 Debian 5ubuntu1
25/tcp	smtp/Postfix smtpd
79/tcp	finger/Linux fingerd
110/tcp	pop3/Dovect pop3d
111/tcp	rpcbind/2-4
143/tcp	imap/Dovecot imapd
512/tcp	exec/netkit-rshrexecd
513/tcp	login
514/tcp	tcpwrapped
993/tcp	ssl/imps?
995/tcp	ssl/pop3s?
2049/tcp	nfs_acl

Hydra usefor brute forcing attack. Brute-force attacks is the trial-and-error to guess the login credential of the account. Here we have brute forced the ssh port 22 and cracked the user name ‘user’ and password ‘letmein’ shows in figure 3. fasttrack.txt world list has been created having a combination username and password.

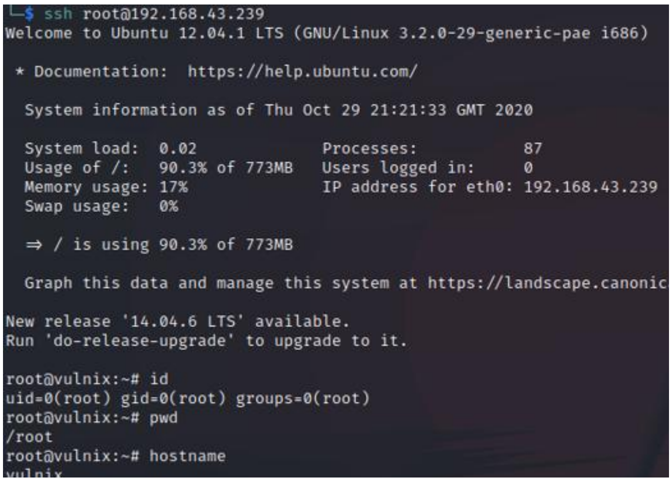


```
ack.txt 192.168.43.239 ssh -t4
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in milita
ry or secret service organizations, or for illegal purposes (this is non-binding, th
ese *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-10-29 22:45:37
[DATA] max 4 tasks per 1 server, overall 4 tasks, 3774 login tries (l:17/p:222), ~94
4 tries per task
[DATA] attacking ssh://192.168.43.239:22/
[STATUS] 44.00 tries/min, 44 tries in 00:01h, 3730 to do in 01:25h, 4 active
[STATUS] 34.67 tries/min, 104 tries in 00:03h, 3670 to do in 01:46h, 4 active
[STATUS] 29.14 tries/min, 204 tries in 00:07h, 3570 to do in 02:03h, 4 active
[22][ssh] host: 192.168.43.239   login: user   password: letmein
```

Figure 3. Hydra Result

Phase Second: White box pen testing

After black box testing we have identified the vulnerability and weakness existing in the system. Now we have detailedinformation ,including login credentials. By using this information, we can perform some white box pen testing using a different tools. Privilege escalation is one of the common attacks in the network. In this phase, we have tried to escalate the privilege using Nmap and some networking command to get root access, which is shown in figure 4.



```
└─$ ssh root@192.168.43.239
Welcome to Ubuntu 12.04.1 LTS (GNU/Linux 3.2.0-29-generic-pae i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Thu Oct 29 21:21:33 GMT 2020

  System load:  0.02              Processes:           87
  Usage of /:   90.3% of 773MB   Users logged in:     0
  Memory usage: 17%               IP address for eth0: 192.168.43.239
  Swap usage:   0%

  ⇒ / is using 90.3% of 773MB

  Graph this data and manage this system at https://landscape.canonic

New release '14.04.6 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

root@vulnix:~# id
uid=0(root) gid=0(root) groups=0(root)
root@vulnix:~# pwd
/root
root@vulnix:~# hostname
vulnix
```

Figure 4. Successfully logged in into root user.

V. RESULTS AND ANALYSIS

Privilege escalation happens, when the attacker get root access into the system. After getting root access to the system malicious users, can easily access the sensitive data and change the security setting of the system. Getting access to the system is an important phase in hacking. After this phase attacker always tries to deploy some malicious software, do remove the track of the activities. This is possible only because of some vulnerability and open ports in the system as shows in the Nmap results. This paper shows various ways to find vulnerabilities and check the security level of the system using different pen testing techniques.

REFERENCES

1 Wani, Abdul Raoof, Q. P. Rana, and Nitin Pandey. "Analysis and countermeasures for security and privacy issues in cloud computing." *System performance and management analytics*. Springer, Singapore, 2019. 47-54.

2 Singh, Saurabh, et al. "A comprehensive study on APT attacks and countermeasures for future networks and communications: challenges and solutions." *The Journal of Supercomputing* 75.8 (2019): 4543-4574.

3 Singh, Shravan, and Ankit Kumar. "Detection and prevention of sql injection." *International Journal of Scientific Research & Engineering Trends* 6.3 (2020): 1642-1645.

4 Maraj, Arianit, ErmirRogova, and GencJakupi. "Testing of network security systems through DoS, SQL injection, reverse TCP and social engineering attacks." *International Journal of Grid and Utility Computing* 11.1 (2020): 115-133.

5 Kakouros, Nikolaos. "A cheat detection system for an educational pentesting cyber range: an intrusion deficit approach." (2020).

6 Radoglou-Grammatikis, Panagiotis, et al. "Implementation and Detection of Modbus Cyberattacks." *2020 9th International Conference on Modern Circuits and Systems Technologies (MOCAST)*. IEEE, 2020.

7 Raj, Sudhanshu, and Navpreet Kaur Walia. "A Study on Metasploit Framework: A Pen-Testing Tool." *2020 International Conference on Computational Performance Evaluation (ComPE)*. IEEE, 2020.

8 Chaudhary, Sumit, ForamSuthar, and N. K. Joshi. "Comparative Study Between Cryptographic and Hybrid Techniques for Implementation of Security in Cloud Computing." *Performance Management of Integrated Systems and its Applications in Software Engineering*. Springer, Singapore, 2020. 127-135.

9 Suthar, Foram, S. Khanna, and Jignesh Patel. "A Survey on Cloud Security Issues." *Int. J. Comput. Sci. Eng* 7 (2019): 120-123.

10 DORTKARDES, Volkan, and İbrahim SOGUKPINAR. "Adaptive Penetration Test Method."

11 Ali, M., Khan, S. U., &Vasilakos, A. V. (2015). Security in Cloudcomputing:Opportunities and challenges. Information Sciences, 305,357-383

12 Jason Bau, ElieBursztein, Divij Gupta, John Mitchell, "State of the Art: Automated Black-Box Web Application Vulnerability Testing", 2010

13 Adam Doup´e, Marco Cova, and Giovanni Vigna, "Why Johnny Can't Pentest: An Analysis of Black-box Web Vulnerability Scanners", July 2010

14 Khalid, Muhammad Noman, Kamran Rasheed, and Malik MuneebAbid. "Web Vulnerability Finder (WVF): Automated Black-Box Web Vulnerability Scanner.

15 Salam,Omar,Huwida "Analysis of cloud computing attacks and countermeasures", January 2016

16 https://www.domo.com/learn/datanever-sleeps-8

17 https://www.webfx.com/internet-real-time/

Published By:
Lattice Science Publication

© Copyright: All rights reserved.