Acta Scientific COMPUTER SCIENCES

Volume 2 Issue 11 November 2020

Review Article

An Analytical Study on Penetration Testing and Vulnerabilities

Aroosh Amjad* and Adeel Munawar

Computer Science, Lahore Garrison University, Pakistan

***Corresponding Author:** Aroosh Amjad, Computer Science, Lahore Garrison University, Pakistan.

Received: October 15, 2020

Published: October 28, 2020

Abstract

With the new invention in technology, computer security is most often concerned for government agencies and organizations. Multiple organizations have a bulk amount of data over the internet which provides efficiency to access. But at the same time, security issues are enlightening which cannot be denied. This paper presents the detailed taxonomy of security issues which perhaps handled by penetration testers. We have discussed their scope and multiple phases of penetration testing through which every penetration tester has to go through. Additionally, some of the common vulnerabilities are analyzed with their detailed description. The paper concludes that while the technology is growing up rapidly, attacks are becoming more enthusiastic so mitigating these types of attacks security researchers are playing a vital role and this critical analysis gives a detailed report on the role of security researchers or penetration testers with the deep discussion of finding loopholes.

Keywords: Web Attacks; Vulnerabilities; Open Ports; Network Security; Web Security

Introduction

Penetration Testing is considered as security testing that unleashes the loopholes, vulnerabilities, different types of threats, risks within the web application, software, network that an attacker can exploit. The foremost purpose of pen testing to uncover the abnormalities or weak points of the website or network in order to make the organization alert.

Attacker disrupts or gets unauthorized access to any system that contains a tremendous amount of data through vulnerability, which is a risk [1]. Most of the vulnerabilities occur during the implementation process and most probably in the development phase. These vulnerabilities include software errors, configuration errors and design bugs.

Penetration testers

Usually, different organizations hire penetration testers from outside often referred to as ethical hackers as they are being hired to breach into the system positively or with the permission of an organization's vendors who are supposed to hire them for the sole purpose to merely secure the organization from unauthorized access. Pen testing must be performed by the ones who have little-to-no prior knowledge because they may be able to find out the blind errors that been missed by the developers while designing the system [2].

Most probably ethical hackers are self-taught, but on the other hand, many of them are experienced with their field and they can find the hidden loopholes easily which were ignored by the developers.

Types of penetration testing

Penetration testing is usually divided into six main categories [3]:

- Black box penetration testing
- White box penetration testing
- Grey box penetration testing
- Covert penetration testing
- External penetration testing
- Internal penetration testing.

Black box penetration testing

Considering a black box penetration testing, a tester has no prior knowledge about the system which is to be tested but he is the one who is responsible for collecting information regarding the website [3]. Merely, this testing is also known as blind testing, the hacker regarding this, having no background at all additionally, the hacker is provided with null information besides the only name of the targeted company

White box penetration testing

This is another sort of penetration testing which includes the hacker to be provided with some little information and time regarding the targeted company's security information. In this testing, the tester is provided with the full fledge information and details about the targeted system which includes IP address, source code, and operating system details [3].

Grey box penetration testing

In grey box penetration testing, a tester is aware of half of the knowledge about the targeted system**.** An attacker can be considered as an external hacker who had to gain illegal access to an organization's network [3].

Covert penetration testing

This type of penetration test is considered as 'double-blind test', the process of convert pen testing in which most probably no one is known about the process of pen testing either it is happening or not, including all those Security and IT professionals who tend to respond towards the attack Importantly, the hacker must know the scope and all other details in writing beforehand in order to avoid any sort of issue with law enforcement [4].

External penetration testing

As an external penetration test, the ethical hacker works up against the company's external technology, such as their external network servers and websites. In many cases, the hackers are not supposed to enter the company's building but this case tends to give access within the company [3]. This means placing any attack from a remote location.

Internal penetration testing

The internal test is considered as a test performed by an ethical hacker from the company's internal network. This test is useful in the condition when the company wants to know the loss or damage they have been bared.

Penetration testing phases

There are four different phases through which penetration testers have to go within [5]. Penetration testing is kind of impossible without applying these four phases during the test.

- Planning phase
- Discovery phase
- Attack Phase
- Reporting phase

Figure 1: Penetration testing phases.

Planning phase

This phase is the most important and thus creates the strategy and scope of the project that have been allotted to the pen testers. Furthermore, there are some pre-defined rules and policies that define the scope of the project.

Discovery phase

In the phase of discovery, Penetration testers collect information as much as possible about the targeted system which includes encoded data like, usernames and even though passwords. This process of discovering information regarding the system is also known as fingerprinting.

This process of fingerprinting scans the whole system or the network and makes analysis of open and closed ports [4]. Eventually, this process contains a complete analysis of the vulnerabilities of the internal system. It may scan the whole system including open and close ports, different types of services and the operating system running at the targeted system.

Attack phase

In the case of penetration testing, the attack phase thus finds out the common vulnerabilities and loopholes in order to get privileged access to the targeted side to exploit [5].

Reporting phase

The last but most crucial phase is making a report of all the scanned devices or findings of the targeted system. Penetration testers have to make a complete documentation based report against

the targeted system [5]. It may include the risks of different vulnerabilities found and their impact on the business organization.

Tools for penetration testing

Recon-ng

Recon-ng is a Web reconnaissance framework based on python. It includes independent modules with light interaction of databases. It may have built-in convenient functions [5]. It helps the user to work with the user interactive mode. Recon-ng thus provides an interactive source and a much powerful environment to work within.

Recon-ng looks like a Metasploit framework perhaps it works in a different way. This framework is not intended to compete with others as it is designed exclusively and with the sole purpose of reconnaissance.

Recon is a full and fledge modular framework and makes even easier for python developers as beginners. Therefore, all the libraries are been there for backend work. The built-in modules are always there for efficient work [5].

Sparta

Sparta is based on GUI application that makes the pen testers to work on a more convenient way. It simplifies the whole network infrastructure in order to aid pen testing in the phase of scanning and enumeration. It provides an opportunity for the testers to save their time by point-and-click access to the toolkit and by displaying the output in a more convenient way.

The tester does not need spent much time by setting the commands and getting interaction with the tool, instead of setting up commands more time can be provided in analyzing the results [4].

Zen map

Zen map is the new version of the Nmap scanner GUI present within Kali Linux. Although it is multiplatform including Linux, Windows, macOS X, Ubuntu, fedora. It is an open-source and free application that provides efficient working and even more flexibility. Nmap is much easy for the beginner level users with advanced features for those who are handy with Nmap [4].

Literature Review

Many authors have contributed their efforts while describing the term of hacking, one of them is: K. Bala Chowdappa *et al*, they have done the survey analysis on different types of hackers. The author had verily discussed the roles of malicious and ethical hackers in the field of security [6].

The author in this paper [1], describes a wide range of high-level ethical hacking, he describes the full details that why many companies hack their own companies. Moreover, by taking real-world examples, penetration testing and different countermeasures had been implied. Some real-world based scenarios have been discussed in order to understand why ethical hacking is considered to be important in the field of technology.

Another author had discussed the dissatisfaction of employee in a company as statistics shows how devastating it can be if any of employees try to get the advantage for the sake of curiosity. The author had recommended a vulnerability analysis of internal and external network which stores sensitive information. In case, a hacker successfully gained access to the WiFi network he would have probably the same rights as network administrator does. He would have the chance to implement open data mining, privilege escalation. As per the author's observation, an internal vulnerability assessment can take place at the customer's office without any physical link to the local area network [2].

Shubham Goel, in his research [3] declared that hacking is the first issue that has been faced by government agencies, companies, and many private citizens. Hackers are invading the user's privacy such as: reading emails, stealing debit or credit cards, getting access to E-commerce websites. The author helps the common users and those who are UN aware of the hacking system, they must understand the concept of loopholes and must know how to prevent themselves in case of being hacked [3].

Asoke, in this paper [2], had primarily discussed how the user can prevent his or her computer system from being hacked. Ethical hacking which is done by white hat hackers is also known as penetration testing which includes some tools and techniques by using Linux OS or its family, that most probably used by hackers. Ethical hacking is performed with a vulnerability assessment to discover different loopholes from a hacker's point of view so that the system can be even better security. Ethical hacking also ensures that service providers must claim about the security of their services are authentic or not [2].

Nabie Y conteh, describes a complete theory of cybercrime and its impact on organizations. The author had described the expan-

sion of cybercrime also the role of social engineering and its effect on normal users. The paper concludes the process of vulnerability assessment, social engineering attacks. The author helps others in reducing the bad impact of social engineering, the vulnerability resides with the behavior of humans that can ruin the career [4].

Another author has discussed the poor protection of the internet. Due to the formal verification or less testing while releasing software. The author has mainly discussed the role of ethical hackers; they tend to find errors and bugs. They better scan networks in order to detect bugs and loopholes. Additionally, the author describes the two different modes of ethical hackers, an ethical hacker from any university is doing services for the internet community and on the other hand ethical hacker can be the malicious ones doing illegal things as well [3].

Suresh kumar *et al,* discussed the overview of ethical hacking and how ethical hacker disrupts the security. The author has also studied the different phases of hackers as hacking is categorized into three major hack terms, namely, white hat hackers, black hat hackers, grey hat hackers. Finally, the author had to make a comparison while doing penetration testing [5].

Proposed methodology

The basic approach that has been used while testing is as follows.

Scanning

By using vulnerability scanners within Linux, each host would be tested for vulnerabilities. The result would be used for further analysis that could be exploited to gain access to the target site on a network.

Reconnaissance

In this phase of Reconnaissance, as much as information is to be collected from the targeted website or network.

Reconnaissance can be active and passive. An active form of reconnaissance could be more intrusive and show up in audit logs and can be considered as a type of social engineering attack. A passive attack is probably the best starting point for intrusion detection systems and other forms of protection.

Enumeration

There are as many fingerprinting tools to determine whether the hosts are alive or not, which type of services hosts are using and how many operating systems running out there. These types of research can be carried out through enumeration.

Obtaining access

After the complete knowledge about the target host and tested vulnerabilities, the result would be analyzed. The weak points are found throughout the scanning and exploit found within the application, Operating system and different services running at host side could be attempted by using brute force.

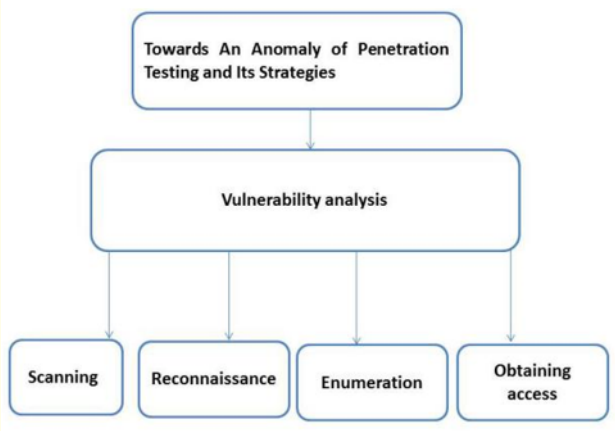

Figure 2: Proposed vulnerability analysis.

Vulnerability assessment report

Table 1 depicts the summary of findings by using Nessus, this table shows the port IDs and their types with explained description about vulnerabilities.

Pen-test technical summary

The experimental setup shows the common vulnerabilities found through Nessus.

Figure 3

Port.no	Types	Description
42873	SSL Medium Strength Cipher	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that use the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.
65821	SSL RC4 Cipher Suites	The remote host supports the use of RC4 in one or more cipher suites. The RC4 cipher is flawed in its generation of a pseudo-random stream of bytes so that a wide variety of small biases are introduced Into the stream, decreasing its randomness. If plaintext is repeatedly encrypted e.g., HTTP
11219	Nessus SYN scanner	Protect your target with an IP filter
95631	SSL certificate signed	Contact the certificate authority
104743	TLS version 1.0 protocol detected	Enable support for TLS 1.1 and
121010	TLS Version 1.1 Protocol	Enable support for TLS 1.2 and/or 1.3, and disable support for TLS 1.1.

Table 1: Summary of findings.

The description in the figure 3 above shows that the port named, tcp 443 HTTP server is opened at the destination end. Nessus, being as a professional tool determine the server type and version of destination end.

Figure 4

This figure 4 determine the tcp based port 80, This port verifies the HTTP protocol. According to the complete analysis this is ought to know the protocol version HTTP/1.1 and SSL is not implemented at the destination end. Moreover, it is witnessed that context type is used as simple HTML text.

In this figure 5, it is detected that the remote host detected Jquery. The web server on the host, uses Jquery with the version of 3.3.1. As the concerned URL shows that the J.

Figure 5

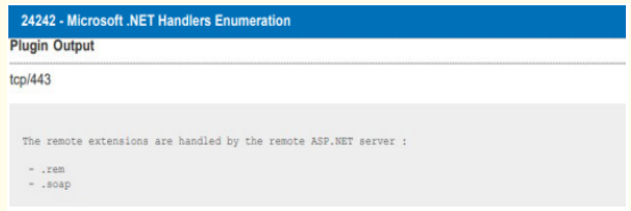

Figure 6

This vulnerability is quite at low risk shown in figure 6. This results provide false positive report. The vulnerability Microsoft. NET handlers provides the highest accuracy rate however, hackers have an idea about the abnormality of this vulnerability. It is the most common vulnerability founded but for attackers it is low hanging fruit.

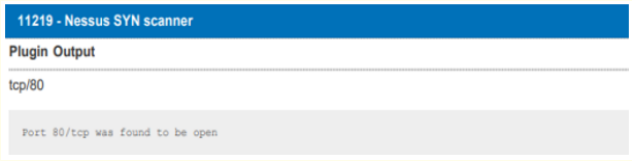

Figure 7

This figure 7 displays that SYN scanning is a tactic, that malicious access can use it in order to determine the active states of ports without generating a connection. This approach can be used to attempt Denial of service attacks. So this type of vulnerability contain medium risk because Dos attacks are reversible attacks.

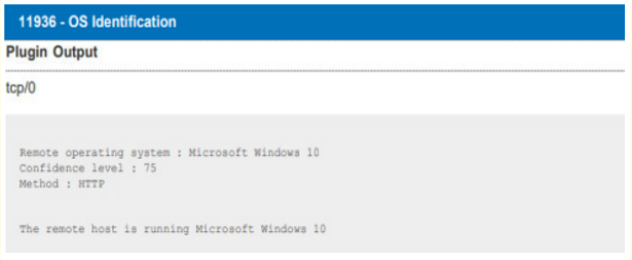

Figure 8

This Scan is used to identify the operating system. According to the plugin 11936, it uses the output by other plugins in order to identify the targeted operating system. There are multiple plugins that are automatically responsive by the plugin 11936, This plugin requires information regarding the target host's operating system. Besides of this plugin other plugins are also logged in to detect the operating system by using fingerprinting technique which includes SSL analysis, Script injections, HTTP response and requests, ICMP pings.

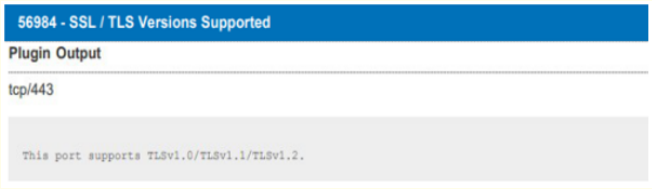

Figure 9

This figure 9 shows that SSL and TLS both are used in every browser widely in order to provide http services in a secured way. This plugin output shows the result after complete analysis that the destination end uses SSL and TLS version 1.0.

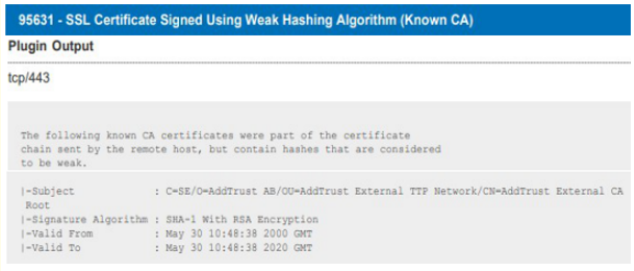

Figure 10

This figure 10 shows the SSL certificates which is used by weak algorithm of hashing. The destination end uses the browser which have signed SSL certificate but with weak hashing crypto based algorithm.

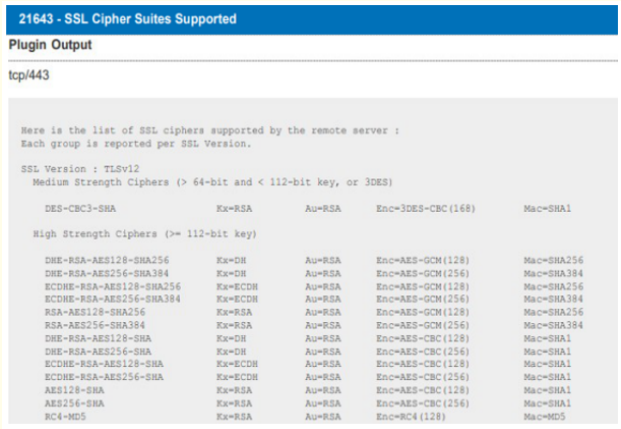

Figure 11

This plugin output 21643 in figure 11, displays the output as SSL cipher suites supported at the backend. The port 443 is opened and thus required a list of all SSL certificated that the host side supports.

This is another SSL based certificate which is root based and includes authority based information. This root certificate shows the validity of certificates and signature algorithm which is used at the browser of targeted site.

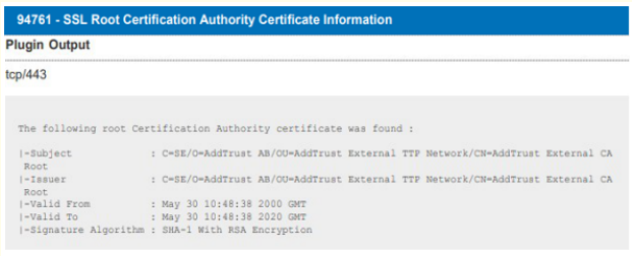

Figure 12

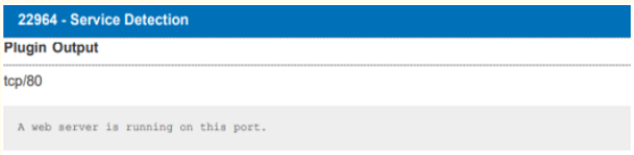

Figure 13

This plugin output is just a service detection that display the services used at the targeted host. This plugin shows the open port tcp/80 and the web server is running at this port.

Figure 14

The plugin output 10287 shows the complete trace route of network which displays a list of ip addresses shown in the above figure 14, The tracert is network command that is used to show the all routes from source to destination by just using the simple ICMP based message [7-15].

Conclusion

The practice of testing any system, network or any web application is to find out the flaws and vulnerabilities that an attacker can exploit. Penetration testing can be performed manually or by some means of software. It is a process of attempting in order to evaluate the security of infrastructure within information technology. Moreover, vulnerabilities could be of any type, it may include within an operating system, services of any flaw within web application most important the misconfiguration that may exist within a system while development. This research paper is eventually based on the security issues that multiple organizations are facing nowadays. We had to find out some common vulnerability and show a detailed description of malicious vulnerabilities that have a high impact.

Bibliography

1. A Mukhopadhyay R and Nath. "Ethical hacking: scope and challenges in 21st century". *International Journal of Innovative Research in Advanced Engineering* (2014): 11.

2. B Akanksha. "Ethical hacking and social security". *Journal of Radix International Educational and Research Consortium* (2012): 10.

3. Bansal A and Arora. "Ethical hacking and social security". *Radix International Journal of Research in Social Science* (2012): 16.

4. Chowdappa K B., *et al*. "Ethical hacking techniques with penetration testing". *International Journal of Computer Science and Information Technologies* (2014): 3389.

5. Conteh N Y and schmick PJ. "Cyber security: risks, vulnerabilities and countermeasures to prevent social engineering attacks". *International Journal of Advanced Computer Research* (2016): 23.

6. D, Yurcik B and Doss. "Ethical hacking: The security justification". In ethics of electronic information in the 21st century. (2001): 10.

7. D.M, Hafele. "Three different shades of ethical hacking: black, white and gray". (2004): 10.

8. Faily S. "Ethical hacking assessment as a vehicle for undergraduate cyber security education". (n.d.). farsole A A kashikar and A, G. "E-hacking". *International Journal of Computer Applications* (2010): 14.

9. Farsole Ajinkya A, Amurta G, Kashikar and Apurva Zunzunwala. "Ethical Hacking". *International Journal of Computer Application* (2010): 20.

10. Goel S., et al. "Ethical hacking and its countermeasures ". *International Journal* (2014): 3.

11. Prasad ST. "Ethical hacking and types of hackers". *International Journal of Emerging Technologies in Computer Science* (2014): 11.

12. ST Prasad. "Ethical hacking and its types". *International Journal of Emerging Technology in Computer Science and Electronics* (2014): 11.

13. saleem, S. A. "Ethical hacking as a risk management technique". 3rd annual conference on information security curriculum development (2006).

14. V Kumar. "Ethical hacking and penetration testing strategies". *International Journal of Emerging Technology in Computer Science and Electronics* (2014): 11.

15. Xynos K., *et al*. "Penetration testing and vulnerability assessments L A professional approach". (2010): 8.