Review on Vulnerability Assessment and Penetration Testing on Today's Digital World

Puja Rai[1], Pema Dorjee Lepcha[2], Sukman Subba[3], Shadew Rai[4], Zening Biswakarma[5], Arvind Lal[6]

Abstract- *Today's world is largely dependent on the internet, global internet users are growing more rapidly. People are more developing their skills and getting advanced in every field using internet. In the same time SECURITY has become the major issue of the internet. Sharing data from the wireless technology can be easily breach the security by hackers and access their confidential data. Vulnerability Assessment and penetration testing is a solution for problem to overcome. A Vulnerability Assessment is the process of defining, identifying the vulnerabilities. A Penetration Testing, is a process to attack in a computer system or network with an authority to evaluate and analyze the computer and network security. The purpose of this testing method is to fix the loopholes and secure the data from the skilled hackers. This paper describes the Vulnerability Assessment and Penetration Testing methods and process to overcome the security problem.*

Keywords- vulnerability assessment, penetration testing, pen testers.

I. INTRODUCTION

We know that everyone is interacts with the internet. Our world is transforming into a digital world where the security problem is increasing rapidly. Managing security is the big task where we have to stay alert in every step against our opponents well known as attackers or hackers who are highly technically skilled using different methods and techniques to exploit their targets confidential data and information without breaking a glass. To run a successful business computer is playing the most vital role in today's date. Having a computer system is not enough, they need to be connected with a network to facilitate with external business. Without internet hacking cannot take place, every year cybercrime is increasing at a high rate and cost many organizations millions of dollars every year. To solve this hacking problem ethical hackers are introduced who knows about assessing the security of a computer system and ultimate security professional. They are employed by companies to penetrate the network and computer system by aiming to fix the vulnerabilities.

II. VULNERABILITY ASSESSMENT

Vulnerabilities are an open door which leads to threat and exploit the data occurring unexpected events. Exploit code is written to target a vulnerability and cause a fault in the system in order to retrieve valuable data. Vulnerability is a security bug, flaws, errors, fault, holes, or weakness in software that is a big opportunity for attackers to exploit the system. A vulnerability assessment is the process of finding the open doorways or vulnerabilities in the systems. In order to perceive the vulnerabilities, vulnerability assessment demand to operate automated testing tools. These tools help to expose the weakness of the systems and suggest the remedies of the problem.

III. PENETRATION TESTING

A penetration testing is also known as pen testing, and testers are known as pen testers, penetration testers, or ethical hackers. Pen testing is the cyber-attack against the computer system to check the accessible vulnerabilities with permission and to increase security solution.This testing is about to know how far the attackers can breach the security system.

This testing is done after the vulnerability assessment to expose the weakness of your system which gains unauthorized access. Testers uses different types of testing methods after observing that which testing needs to applied.

White box testing – clear box testing is also known as white-box testing; It is applicable for testing the internal software. Here the testers' programming and implementation knowledge are mandatory as compare to other testing methods. This testing consumes the most time and software testing starts after detailed design document.

Black box testing – black box testing is also known as closed testing. In this testing method the internal structure/design/implementation of the item is not known to the tester. This testing is mostly done by software testers, and does not required implementation or programming knowledge, takes least time to perform.

Gray box testing – gray box testing is also known as translucent testing. In testing method internal software structure/design/implementation is partially known to tester, it is the combination of black box and white box testing. The purpose of this testing is to detect the errors caused by codes/design or improper functioning usage of an application.

IV. VAPT TOOLS

The tools that automatically identify the vulnerabilities in the network and the computer system is VAPT tools. Following are the list of best VAPT tools:

Netsparker security scanner:

It is an automated and web application security scanner that identifies security flaws and scan websites, web applications, and web services.

Metasploit:

it is a penetration testing framework used by both malicious hacker or ethical hacker that makes hacking simple. That is available in free or in paid version and installs in Windows. Windows server, Ubuntu.

NMAP:

NMAP stands for Network Mapper, it is one of the best open souse tools used for scanning the network. With the help of NMAP we can scan open source and the services running on them including their version number.

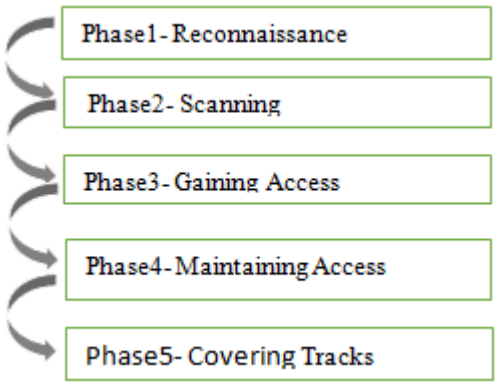
Wireshark:

It is a handy tool and useful when it comes to networking, it helps researchers to do data analyses and it also helpful for hackers when it comes to security purposes. It is an open-source system analyzer and troubleshooter.

Burp Suit:

It is a java-based web penetration testing framework, which is mostly used by security professionals to identify various security flaws. It is also called an interception proxy tool. It is available in Windows, Linux, and MAC

V. ANATOMY OF AN ATTACK



Reconnaissance-

Reconnaissance is a computer attack in which attackers attempt to gather information about their target as much as possible because in hacking information gathering about the network and system is the first step to proceed. Reconnaissance can either be active or passive reconnaissance. Active reconnaissance attacker will directly engage with the computer system to gather information about the target, using this process gathered information can be gained accurate. In this reconnaissance there is a high chance of getting detected, if we tried without permission. If got detected, then the system admin can take server action against the attacker.

Scanning

The purpose of the scanning phase after reconnaissance is to find the open ports and find vulnerable to hacking. Scanning refers to collecting more information of target by using complex techniques by detecting live machines on the target network, identifying the operating system, identifying which TCP and UDP services are running.

Gaining access

In this phase attackers will look at gaining access to the computer device- a phone, a laptop, a tv, a network, a router, a website, a server. Mention each device has an OS, in which attackers access the OS and can launch attacks like denial of service attack, buffer overflow attacks, and application base attacks,

SQL injection.

Gaining access can be done by two methods one is the server-side and the other is the client- side. On the server-

side, the attacker has zero interaction with the user, and the client-side has to interact with the user.

Maintaining access:

After gaining access to the system, the attackers work hard to maintain that access. An attacker who wants to remain undetected they tries to secure their presence by removing their evidence of entry. To gain repeat access they can use a black door or installing software trojan horse or root kits at the kernel level to gain super user access. A trojan horse gain access at the application level and rootkit at the operating system level and both the systems depends on users to install them.

Covering tracks:

This is the final phase of the attack**,** after finishing all his work, attacker needs to erase all the evidence which can lead to trouble by covering tracks (by covering all the little clues). Its purpose is to remain obscure and evade trace back

VI. COMPARISION TABLE

VULERABILITY ASSESSMENT VS PENETRATION TESTING

Basis	VA	PT
Definition	It is the process of defining, identifying, classifying prioritizing vulnerabilities in computer systems, applications and network infrastructure.	It is the process of hacking a system with the permission from the owner of that system, to evaluate security, hack value, attacks, exploits, zero-day vulnerability & other components such as threats, vulnerabilities, and daisy chaining.
Types	Active Passive Host based Internal External Network Wireless network application	Black box Grey box White box

VII. LITERATURE REVIEW

[1] Irfan Yaqoob1, Syed Adil Hussain2, Saquib Mamoon3, Nouman Naseer4, Jazeb Akram5, Anees Ur Rehman6, “Penetration Testing & Vulnerability Assessment”, Volume: 7 issue: 8 | August-2017.

The main objective of this research paper is to identify common network threats and define countermeasures to prevent these threats.This gives the best overview of the VAPT and describes the different process and methodology of vulnerability assessment and penetration testing.

[2] Gurline Kaur1, Gurpreet Kaur2, “Penetration Testing: Attacking oneself to Enhance Security”, Volume: 5 issue: 4| April-2016.

The objective of this paper is to know about what penetration testing is, how it is done, and also about the various tools available. There are a number of tools available for such purpose;a few of them are explained.

[3] Jignesh Doshi1, Bhushan Trivedi2, “Comparison of Vulnerability Assessment and Penetration Testing”, volume: 8, No.6 April-2015.

This paper provides a comparison of two approaches vulnerability assessment and penetration testingBoth solutions are different and complementary to each other. And explained that penetration testing is better compare to vulnerability assessment as it exploits the vulnerability.

[4] Chanchala Joshi1, Umesh Kumar Sing2, “Security Testing and Assessment of Vulnerability Scanner in Quest of Current Information Security Lanscape”, Volume: 145, No.2, July-2016.

This paper explains the difference measure to secure the application significantly. The results of web application evaluation identify the most challenging vulnerabilities for the scanner to detect, and compare the effectiveness of scanners.

[5] Korra manasa1, L. Venkateswara Reddy2, “Designinga Web Application & Detecting Vulnerabilities using Vega Vulnerabilities Scanner” Volume: 5, Issue: -8, pp-227-232(2016),

In this paper, they used the Vega tool that can observe the web that can help the developer tofind vulnerabilities in the web and fix the holes before developer online the website. After developing a web application, thedeveloper explained about testing the website using the scanner and the result will be analyzed.

[6] Pawan Kesharwani1, Sudhanshu Shekhar Pandey2, Vishal Dixit3, Lokendra Kr. Tiwari4,” A Study on Penetration Testing using Metasploit Framework”, Volume: 05 Issue: 12 | Dec-2018.

This paper is reviewing the steps involved in preparing for and performing penetration testing. The Intended audience for this paper is the project director or managers whomight be considering having a penetration test performed.

[7] Leena Jacob1, Virginia Mary Nadar2, Madhumita Chatterjee3, "Web Application Security: A Survey" Volume: 7(1), 2016.

In this paper, they have presented few of the attacks such as SQL Injection, Cross-Site Scripting (XSS), insecure Direct Object References (IDOR), Sensitive Data Exposure, and using components with a known vulnerability. And also, they have described the detection and prevention.

[8] Kyle Coffey1, Richard Smith2, Leandros Maglaras3, Helge janicke4, "Vulnerability Analysis of Network Scanning on SCADA System", Volume: 2018, Article ID 3794603, 21 pages, Published 13 march-2018.

The objective of this paper is to explore, test and critically analyze the use of network scanning against bespoke Supervisory Control and Data Acquisition equipmentto identify the issues with conducting asset discovery or service detection on Supervisory Control and Data Acquisition systems with the same tools used on conventional IP networks.

[9] Martin Tomanek1 Tomas Klima2, "Penetration Testing in Agile Software Development Project" Volume: 5 No.1 March-2015.

Theobjective of this paper is to introduce the enriched Scrum agile software development framework that includes the security requirements and execution of automated and manual penetration tests. This concept has been introduced and validated in various software development projects in the global logistics company.

[10] Gitanjali Simran T1, Sasikala D2, "Vulnerability Assessment of Web Application using Penetration Testing" Volume: 8, Issue: 4 Nov-2019.

This paper aim is to elucidate the overview of vulnerability assessment and penetration testing introduced the most efficient open- source tools used to perform this test.

[11] Grusha Kaur Sahni1, K. Ravindranath2, "VSTAAS-An Integrated pen-testing tool" Volume: 9, Issue: 2, Dec-2019.

In this paper, it offers strong, actionable intelligence with RPA, machine learning, and AI automation concerning Security Requirements across the SDLC.

[12] Jai Narayan Goel1, BM Mehtra2,"Vulnerability Assessment and Penetration Testing as a Cyber Defence Technology", Procedia Computer Defence Technology, Volume 57, 2015, Pages 710-715.

The objective of this paper is to describe the complete life cycle of Vulnerability Assessment and Penetration Testing on systems or networks and stop possible attacks. And also, they have described prevalent Vulnerability assessment techniques and some famous VAPT tools.

REFERENCES

[1] Irfan Yaqoob1, Syed Adil Hussain2, Saquib Mamoon3, Nouman Naseer4, Jazeb Akram5, Anees Ur Rehman6, "Penetration Testing & Vulnerability Assessment", Volume: 7 issue: 8 | August-2017.

[2] Gurline Kaur1, Gurpreet Kaur2, "Penetration Testing: Attacking oneself to Enhance Security", Volume: 5 issue: 4| April-2016.

[3] Jignesh Doshi1, Bhushan Trivedi2, "Comparison of Vulnerability Assessment and Penetration Testing", volume: 8, No.6 April-2015.

[4] Chanchala Joshi1, Umesh KumarSing2, "Security Testing and Assessment of Vulnerability Scanner in Quest of Current Information Security Lanscape", Volume: 145, No.2, July-2016.

[5] Korra manasa1, L. Venkateswara Reddy2, "Designing a Web Application & Detecting Vulnerabilities using Vega Vulnerabilities Scanner" Volume: 5, Issue: -8, pp-227-232(2016),

[6] Pawan Kesharwani1, Sudhanshu Shekhar Pandey2, Vishal Dixit3, Lokendra Kr. Tiwari4," A Study on Penetration Testing using Metasploit Framework", Volume: 05 Issue: 12 | Dec-2018.

[7] Leena Jacob1, Virginia Mary Nadar2, Madhumita Chatterjee3, "Web Application Security: A Survey" Volume: 7(1), 2016.

[8] Kyle Coffey1, Richard Smith2, Leandros Maglaras3, Helge janicke4, "Vulnerability Analysis of Network Scanning on SCADA System", Volume: 2018, Article ID 3794603, 21 pages, Published 13 march-2018.

[9] Martin Tomanek1 Tomas Klima2, "Penetration Testing in Agile Software Development Project" Volume: 5 No.1 March-2015.

[10] Gitanjali Simran T1, Sasikala D2, "VulnerabilityAssessment of Web Application using Penetration Testing" Volume: 8, Issue: 4 Nov-2019.

[11] Grusha Kaur Sahni1, K. Ravindranath2, "VSTAAS-An Integrated pen-testing tool" Volume: 9, Issue: 2, Dec-2019.

[12] Jai Narayan Goel1, BM Mehtra2, "Vulnerability Assessment and Penetration Testing as a Cyber Defence

Technology", Procedia Computer Defence Technology, Volume 57, 2015, Pages 710-715.