Study System Infiltration And Related Problems

Jitendra Gaikwad
Jit.gaikwad@gmail.com

Dr. Supriya Nagarkar
Assistant Professor, Department of computer Science
Tilak Maharashtra Vidyapeeth,Pune-37

Abstract:

A comprehensive security programme must now include penetration testing. Ethical hackers use pen tests to simulate the tactics and movements of the attacker. This challenging work requires creativity, therefore you must fully comprehend it. The customer is subsequently supplied with all security issues found together with an evaluation of their impact on the system and in the corporate business scenario, as well as a technical remedy for abilities mitigation. This paper explores several Kali Linux penetration testing tools, how todeploy them, and how to utilise them to carry out various assaults, including attack methodology and defence tactics. Technically, using virtualized systems, tools, and private networks, we will carry out various penetration tests. assaults carried out included traffic spoofing, sniffing, and man-in-the-middle (MITM) assaults. Other attacks included Blue tooth hacking and camera espionage.

Keywords: System Penetration, Network Security, Hacking, Penetration Testing.

I. Introduction

Penetration testing simulates an attack in order to evaluate the security of a system or environment. This test can be carried out physically using hardware or socially engineered methods. The purpose of this test is to evaluate how systems, networks, or personnel devices behave under difficult conditions in order to find their flaws and vulnerabilities. Tools for penetration testing include both those that merely analyse a system and those that actually attack it in order to uncover weaknesses. Penetration testing differs from port scanning, which is what some people believe it to be. Port scanning is like looking through binocular sat doors and windows to detect potential access points if a network or host system were a house. The next level up would be vulnerability assessment/management, which in this case would entail sending a home inspector with an emphasis on security to the house. The inspector would examine various elements of the house and provide feedback and suggestions for ways that they may be made better security analysis.

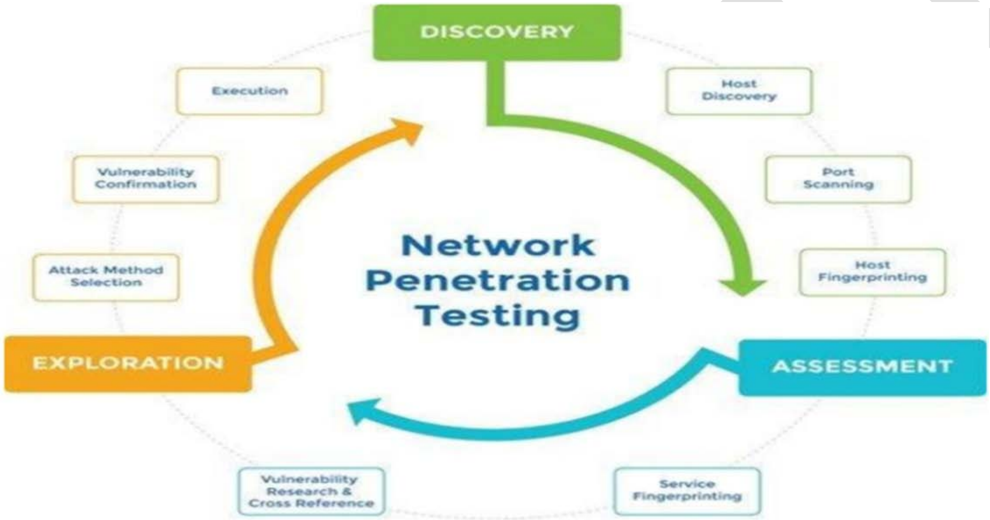
In this case, penetration testing is actually attempting to break into the property in order to identify the weak spots and security flaws. Penetration testing can be carried out manually or automatically using software programmes. In either case, the procedure entails discovering potential entry points and conducting reconnaissance of the target system before the test.

Points, making an attempt to break in (either virtually or physically), and reporting what is discovered. Finding security holes is the core goal of penetration testing. A penetration test can also be used to 1) assess an organization's ability to respond to security problems, 2)employee security knowledge, and 3)compliance with security policies.

Penetration testing generally falls into one of four categories: external, internal, blind, or double blind. A company's publicly accessible servers and equipment, such as firewalls, email servers, domain name servers (DNS),and Web servers, are the focus of an external test. In this instance, the goal is to determine whether an outside attacker may obtain unauthorized access and, if so, to what degree. An internal test replicates an internal assault by a legitimate user
with ordinary access privileges, behind the firewall. A blind test severely restricts the amount of information that is provided to the person or team conducting the test before hand in order to imitate

the actions and procedures of a real attacker. Only a select few people within the organisation would be aware that a test is being run in double blind testing, which extends the blind test even further. Penetration testing can be done using a wide variety of tools. There are plenty on the market that one can utilise for free download. Many of them—known as "Open Source tools"—can even be modified. For instance, the testing tool Kali Linux comes with its own set of in-built penetration tools, but you can also download and add more tools to it. Only a small number of these programmes are being created for Windows or Mac, with the majority being built for Linux. Additionally, one can buy a variety of penetration testing software. Some of them have licence fees as low as $10, while others might be thousands of dollars.

The setools, as examples, include:
KaliLinux- An Linux-based OS Linux-based suite of penetration tools.
Metasploit- A sophisticated pen-testing framework with both GUI and command-line interfaces.
Wireshark- A protocol analyzer featuring a graphical user interface.
w3af- A framework for auditing and attacking web applications.
John The Ripper– A password cracker.



Background and Initial Research

Phases of penetration testing
There are five steps in the pen testing procedure.

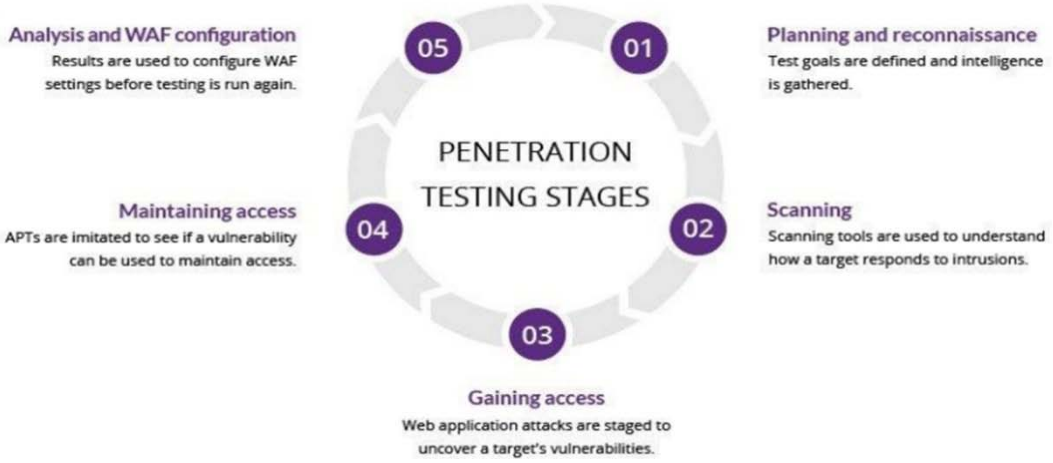

PENETRATION TESTING STAGES
01
Planning and reconnaissance
Test goals are defined and intelligence is gathered.
02
Scanning
Scanning tools are used to understand how a target responds to intrusions.
03
Gaining access
Web application attacks are staged to uncover a target's vulnerabilities.
04
Maintaining access
APTs are imitated to see if a vulnerability can be used to maintain access.
05
Analysis and WAF configuration
Results are used to configure WAF settings before testing is run again.

Figure.2 penetration testing stages

II Research And Preparation

Defining the scope and objectives of a test, including the systems to be tested and the testing techniques to be applied.

Gathering information (such as network and domain names, mail servers, etc.) to learn more about a target's operations and any potential weaknesses.

II.I Checking

Knowing how the target application will react to different intrusion attempts is the next step. Usually, this is accomplished using:

II.I.II Static Analysis

Analysing the source code of a programme to predict how it will function when it is executed. These tools have the ability to scan the entire code in a single pass.

Dynamic analysis - Examining the code of an application while it is in use. This kind of scanning is more useful because it gives a real-time glimpse into an application's performance.

II.I.III Gaining Access

This stage involves identifying a target's weaknesses via web application assaults such cross-site scripting, SQL injection, and backdoors. In order to comprehend the harm these vulnerabilities can do, After that, testers try to take advantage of them, frequently by increasing their level of access, stealing information, intercepting conversations, etc.

II.I.IV Maintaining Access

The goal of this stage is to ascertain whether the vulnerability can be utilized to create a long-lasting presence in the system under attack-long enough for a malevolent actor to gain extensive access. In order to steal the most sensitive data from an organization, advanced persistent attacks, which can frequently stay in a system for months, are imitated.

IV.Analysis

IV.I Software

VMware
GNS
Software

Figure3 Software Analysis

By using GNS-3, the network is completely designed, complete with all of its details regarding the GNS 3 programme that is used to design networks, as well as complete settings for the routers used to connect branches, as well as the switch devices used to connect devices and resources within the network, as well as the network connection's address settings. Thus, in order to complete this project, we will employ this choice, as well as VMware to create all finished-services "server, IDS/IPS, kali Linux" , and we will use GNS-3to create our network topology “routers, switches, firewall”, then we will add the end devices in to theGNS-3 network topology.

IV.II Project Phases

1. Network Design.
2. Configurations.
3. Penetration attacks.
4. Mitigation and defending.

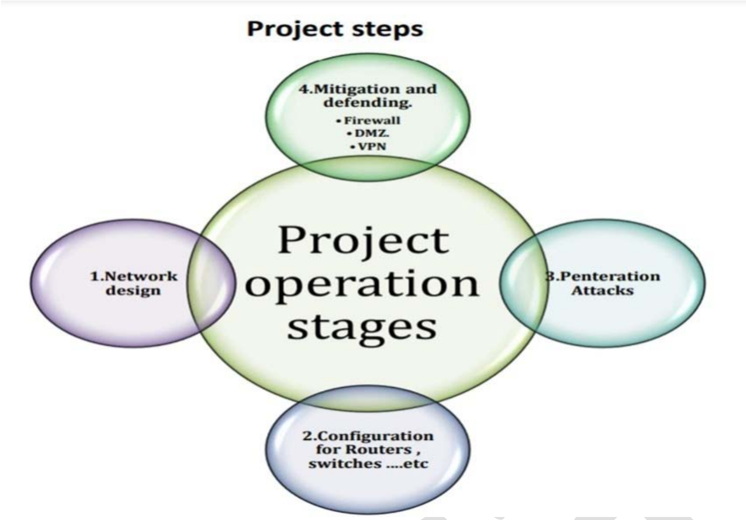


Figure4 Project Steps

V. Design

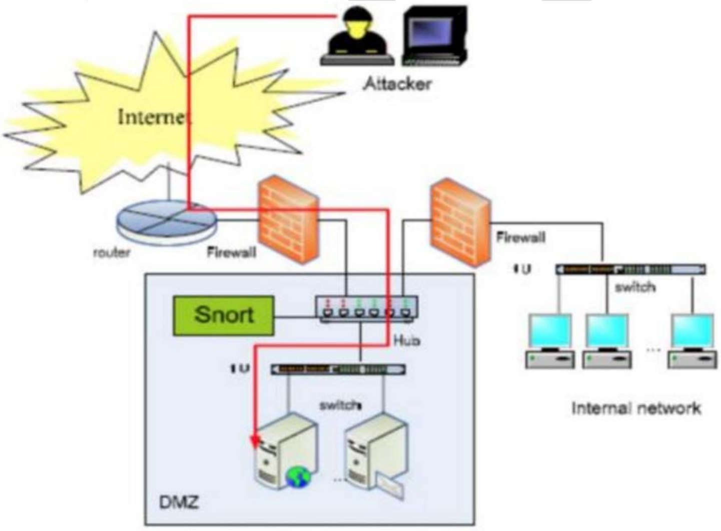


Figure 5 Network Block Diagram

VI. Mitigation Policies:

Although finding tools and tactics to test for vulnerabilities after an application has beendeployed is the primary goal of this paper, there has also been a lot of work done on patching vulnerabilities in applications before they are distributed. This is done during the software development life cycle's design, development, and testing phases. As a result, this section discusses some of the works that aim to eliminate vulnerabilities by primarily using testing techniques. The articles listed in this section were not discovered through an SMS, which is essential to note because this could be the subject of a brand-new study. The present methodology for security testing vary widely in terms of their traits, goals, and methods; never theless, because they are made specifically for different reasons, these methodologies also have restrictions on target scenarios. Due to the wide range of target situations, we think that none of the so-called "standard" approaches could be employed to run Pentest. Given that it provides an open problem in the domain of security testing, this may be regarded as one of the core lessons of this methodical mapping. Future research in security could potentially take a fresh turn by developing a new methodology or approach that could handle the variety of target scenarios and the advantages and weaknesses of any existing technique.

VII. Conclusion:

From a research perspective, it is obvious that penetration testing (Pentest) is relevant. Since there have been more faults and vulnerabilities in recent years, testing and safety researchers have focused a lot of attention on this topic. This article concentrated on mapping the Pen test field, finding application scenarios, common tools and approaches in various contexts, the key contributions, and associated difficulties. On the techniques or methodologies used for vulnerability assessment, network scanning, pre-invasion, post-invasion, and web analytics, certain conclusions could be drawn. The outcomes from that can assist testers in defining, within the scope of their testing, whatever tools or methodologies are suggested based on the context or scope they will be applied.

VIII.Future Scope:

Dynamics and test processing: Since a Pentest necessitates the exploitation of the identified vulnerabilities, the test activities might be changed in accordance with the outcomes of this exploitation. This modification immediately influences the dynamics and flow of the test, and several judgements made throughout the execution of the activities rely on the tester's discernment. However, a criticism raised in this systematic mapping that is not taken into account in the associated studies refers to the adaptability of security testing software coupled with worries about reprocessing test stages. In this regard, a continual assessment of the completed activities with the goal of implementing verification cycles may lead to an improvement in test efficacy or efficiency.

5. References

1. Santhi, V., Dr K. Raja Kumar, and BLV Vinay Kumar. "Penetration Testing using Linux Tools: Attacks and Defense Strategies." pub. in International Journal of Engineering Research & Technology(IJERT)5.12 (2016).
2. Denis, Matthew, Carlos Zena, and Thaier Hayajneh. "Penetration testing: Concepts, attack methods, and defense strategies." 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT).IEEE, 2016.
3. Rahman, Chowdhury Mofizur, et al. "Attacks classification in adaptive intrusion detection using decision tree."(2010).
4. Al-Jarrah, O., & Arafat, A. (2015). Network intrusion detection system using neural network classification of attack behavior. Journal of Advances in Information Technology Vol, 6(1).