ETHICAL HACKING – HOW IT OPERATES

Written by ***Mrittikaa Das***

Advocate at Gauhati High Court, Guwahati, Assam, India

ABSTRACT

There are many benefits to the Internet's rapid growth, such as e-commerce, banking, email, and cloud computing, but there are also drawbacks, such as hacking and backdoors. The first major challenge that governments, organisations, and regular people face around the world is hacking, which includes reading other people's emails, obtaining credit card information from an online store, and secretly transmitting secrets to the public Internet. An ethical hacker can assist persons who have been hurt as a result of hacking.

The ethical hacker operates in good conscience. People now have a widespread perception of hackers as malevolent, obsessive, criminal, and unethical. In essence, some hackers have even harmed some firms by collecting sensitive data about clients. In various government entities, highly confidential information, such as social security numbers and other classified information, has been interfered with. This clarifies the reason why hackers have a bad image. Ethical hackers' goal is to assess and investigate the system's weaknesses and flaws. A different perspective contends that without hackers, software faults and weaknesses would go undetected.

The author attempts to establish the concept of Ethical Hacking in this technologically driven world with this study. An investigation into the many tools and techniques involved in Ethical Hacking has been made.

Keywords: Hacking, Ethical Hacker, Pen Testing, Risk Assessment, Vulnerability Assessment, Information Technology

INTRODUCTION

In the era of technological advances, mankind has bagged both the positive and negative impacts of such advances. A cyber-attack is claimed to occur every 39 seconds, and the current systems are incapable of handling them. Therefore, each organization requires top-tier security measures to resist the volume and frequency of attacks that occur on a regular basis. Regular updates and enhancements to Information Technology security system are the best methods to safeguard business from this expanding threat. While cyber-attacks continue to plague organisational sector and the world, ethical hacking provides them with a medium to address these ever-growing problems. Therefore, in today's technically advanced world, Electronic Hacking has become a knight in shining armour.[i]

PENETRATION TEST

Meaning of Penetration Test

The technological signs are always threatened with the thought that whether their organisation is well equipped or have a proper management to deal with the increasing number of cyber-attacks as because the unpatched vulnerabilities always tend to invite cybercriminals. Therefore, penetration testing is considered by the technology society as one of the ways to analyse the organisation's Information Technology and security infrastructure to identify the network and system vulnerabilities.[ii]

A penetration that is also known as the pen-testing, or ethical hacking. It is basically way or a planned method or techniques that is adopted by the organisation to identify system, under the bracket of the security posture for adapting the best possible preventive measures. In connection to web application security, this test is usually adopted or executed to supplement a web application firewall.[iii]

National Cyber Security Centre describes penetration test as the strategy used for obtaining assurance in the IT security system. Though the windows by which the adverse party might enter using the tools and techniques (NCSC) the one may use (National Cyber Security centre, 2017).[iv]

In general terms the word, proactive refers to anything that foresees future damages, alteration, requirements so that immediate and necessary actions are taken in hands for cyber security. In context to cybersecurity, proactive cybersecurity measures steps in the same footing as that of the general terms. Under this cyber security measure there is an inclusion of a consistent self-driven improvements based on the test reports which differs from a non-proactive approach which causes delay in fixing or patching the vulnerabilities as they arise. Some of the instances of proactive cyber security measures are as follows:

- To identify and patch vulnerable in the infrastructure of the network.
- To prevent data and security breaches
- To monitor the security ground of the system regularly[v]

The main aim of a proactive measure as that of the pen testing is to reduce the quantity of retroactive upgrades and increase at large the organization's security front. Hence, it is said that penetration testing is highly a crucial at the same time a critical cyber security practice or method that implies high demand in many technological avenues.

Who Performs Pen Testing

Pen-tests are basically executed by ethical hackers who are experienced developers or security professionals with advance certification in pen-testing. These experts used several tools, strategies or methods or approaches by which they can locate or discover the possible focal points of entrance in the system through which attacks can take place. They basically perform a replica of a cyber-attack in order to explore the strengths and weakness of the organization's present security infrastructure.

There are certain responsibilities that an ethical hacker should possess while performing a pen-testing. Some of them are listed below:[vi]

- Accessing threats through threat analysis on various application of the system.
- Security audits are required to be look upon
- The security controls should be properly implemented and planned
- To review and update the security policies
- Provide suggestions how to fix the gaps in the system's infrastructure

- After conducting the test, it shall be the responsibility of the tester to consolidate all the finding of the test in a concise manner and document it in a form of a report

What aappens after Pen-Testing

As already mentioned above that once the pen-testing is over, it shall be the duty of the Ethical hacker to consolidate all the findings of the test in a report. After preparing the report, the tester shall share the findings with the security team of the organization. The organization use this finding for further examinations and assessment under the umbrella of a security posture. At this point, the stakeholders and the organization's security team participate together to fix the loopholes of the security gaps efficiently and within a proper time frame.[vii]

STAGES OF PENETRATION TESTING

The stages of Penetration Testing is depicted below in the given figure:

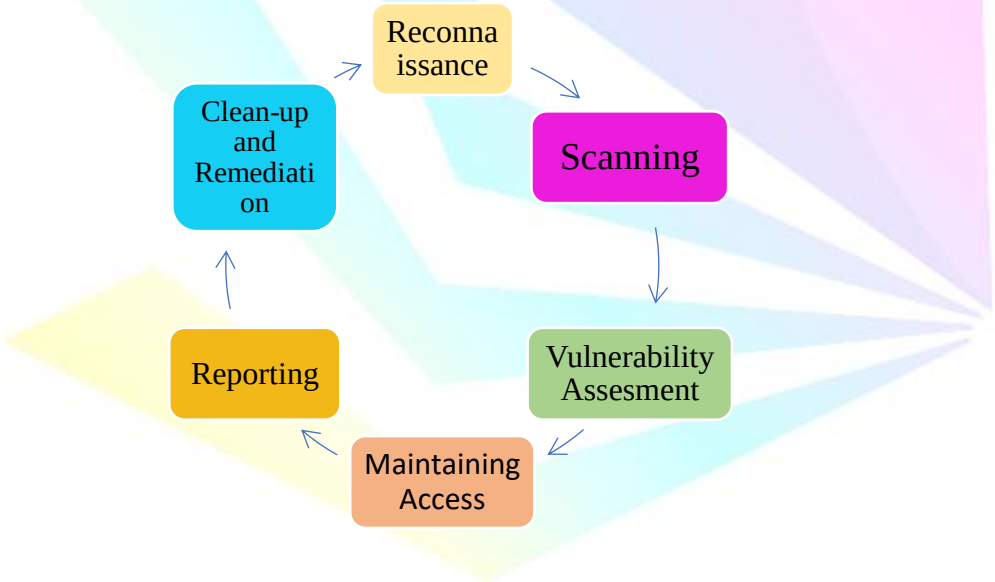

Fig 2 : Stages of Penetration Testing

Reconnaissance

Reconnaissance is the first and preliminary stage of a penetration testing or an ethical hacking. This stage is the preparatory stage as because, the tester here gathers as much as information possible from all sorts of sources including private and public related to the targeted system.[viii]

The tester uses competitive intelligence to learn about the target at this phase. It could be a future point of return, highlighted for ease of entrance for an attack, where more about the target in a large scale is known clients, workers, operations, networks, and systems of the target organization may be included in the reconnaissance target range.

There are two types of reconnaissance under this stage:

- Active Reconnaissance

Under this type of reconnaissance once the tester looks for gathering information related to the target network, the targeted server or any advanced application used under the system. Once he enters the network, he tries to discover individual hosts, IP address and network services. Thus, this process is called as "rattling the doors."[ix]

- Passive Reconnaissance

From the perspective of the tester under this Reconnaissance, his focal point is all about gathering information about the company's key members important facts of the system, IP addresses of the system or any other crucial piece of information related to the organization's system.

On the other hand, if we look from the lens of the hackers, information about the target is obtained without the awareness of the target firm or individual. It could be accomplished easily by searching the targeted information on the internet or bribing an employee if the targeted organization to diverge and offer essential information to him.[x]

Scanning Phase

The next move after the Reconnaissance stage is the scanning step. Based on the previous gatherings in the initial stage, the tester in this stage uses various scanning tools in order to delve into the system to fix weak spots. Under this stage of the pen-testing, the tester uses several scanning tools to detect the vulnerabilities, which are later shortlisted for exploitation.[xi] The tools which are used by the tester for scanning includes:

- War Diallers
- Port Scanners

- Security Vulnerability Scanners
- Network Mappers

Vulnerability Assessment

The third step is the vulnerability assessment, under which all the data that which collected by the tester in the previous two stages are used in this stage to pick out the budding vulnerabilities and find out whether they can be exploited or not.

One of the resources that the tester use under this assessment is the National Vulnerability Database (NVD). The NVD is the US government repository for standards-based vulnerability management data represented by the Security Content Automation Protocol (SCAP). This data enables vulnerability management, security measurement and compliance to the automated. The NVD under this stage helps the tester by analysing the software vulnerability that are mentioned under the Common Vulnerability and Exposures (EVE) database. [xii]

Maintaining Access

This stage makes sure that the tester stays connected with the targeted system for a much larger time so that it is much easier and more possible for the tester to exploit the vulnerabilities for most of the infiltrated data diffusion.

One such tool that is used by the tester to exploit the vulnerability is Metasploit. It helps the tester in scanning the system vulnerabilities. Metasploit basically is executed through a piece of code, which when executed in a system, triggers the vulnerability at the target.[xiii]

Reporting Stage

This is the last stage of the pen-testing, where the tester after exploiting the vulnerability of the targeted system prepares a report documenting the testing's findings[xiv]. The reports rule out the following details of the testing:

- The vulnerabilities exploited by testers.
- Type of the sensitive information or gatherings accessed by the testers.
- Time required in gaining and staying connected to the target.

Clean-Up and Remediation

When the testing is finished, the pen tester should erase any traces of the tools and process used in the preceding steps to prevent a real-world threat actor from using them as an anchor for system invasion. During this step, organizations should begin addressing any flows discovered in their security controls and infrastructures.

TYPES OF PENETRATION TESTING

White Box Testing

This testing provides a penetration tester or ethical hacker to gai knowledge about the systems internal structure along with the various code in the system is known as White Box Testing.[xv]

Under this technique, the tester is provided with all the internals of the system which includes the software, internal structure design and internal working of all the codes of the systems which need, to be tested. As the test, makes the code visible to the examiners or tester this test is also known as clear box testing, open box testing, code base testing or glass ox testing.

Thus, the terms of white box is used under this technique because of the theme of see through box concept which helps the tester to have a sneak peek of the internal working through the basis of the software's outer shell or box.

The main objective of the tester under this test is to detect all the kinds of errors which include logical design and typographical error.[xvi]

White Box testing calls for the testing for the following software codes:

- The security holes of the internal proceedings
- The codes which are defective in structure
- The improper running of the specific inputs through the codes and likewise.

Advantages of White Box Testing

- Redefining of the codes that conceal errors
- It can be easily operated

- White Box Testing involves specific and in-depth testing dealing with the codes internal paths.

Disadvantages of White Box Testing

- It is complex in nature as well as expensive
- This testing requires professional implications as the testing requires intensive understanding of the codes
- As the testing is complex it is time consuming as bigger applications are implemented in this testing.

The different techniques used in White Box Testing are:

- Data Flow Testing
- Branch Testing
- Path Testing
- Statement Coverage

Black Box Testing

The pen-testing strategy which deals specially or is concerned purely of the systems output in reciprocation of the selected inputs and execution conditions is called or known to be the Black Box Testing. [xvii]

The Black box testing is also called as the functional testing as because this test takes hold of only the functional applicability of the system by completely pushing aside the structure of the program. Hence, the tester is mainly focussed with substantiating of the output rather than knowing how the outputs are produced.[xviii]

Therefore, a black box software into which known inputs we supplied and known outputs are expected, the system performs the transformation of known inputs to known outputs, which is not tested in this type of testing. The transformation process system is referred to as the black box. [xix]

The different Black Box techniques are:

- Equivalence Class Testing

- Boundary Value Testing
- Decision Table Testing

Advantages of Black Box Testing

- It facilitates identification of contradictions and vagueness in functional specifications.
- Tester is free from any pressure of knowledge of specific programming languages to test the reliability and functionality of an applications.
- Test cases can be designed immediately after completion of specifications.

Disadvantages of Black Box Testing

- Results might be overestimated at times.
- Testing every possible input stream is not possible because it is time consuming.
- Cannot be used for testing complex segments of code.

Grey Box Testing

Grey Box testing is a software testing which is a combination of Black Box Testing technique and White Box Testing Technique. The interior structure of the item being tested is unknown to the tester in the Black Box testing technique, whereas the internal structure is known to the tester in the White Box testing technique. Grey Box Testing provides some insight into the internal structure. This includes gaining access to internal data structure and algorithms in order to construct test cases.[xx]

Grey Box Testing is so named because the software programme resembles a semi-transparent or grey box inside which the tester can only view a portion of it. It frequently focuses on content-specific mistakes linked to web systems. It is based on requirements test case creation since it contains of all the criteria supplied before the programme is tested.

The Techniques used for Grey Box testing are:

- Matrix Testing
- Regression Testing
- Orthogonal Array Testing
- Pattern testing

Advantages of Grey Box Testing

- This is mostly done by the user perspective
- It is a non-intrusive testing
- It is unbiased in nature and avoids conflicts between a tester and developer.

Disadvantages of Grey Box Testing

- This test is not suitable for algorithm testing
- It provides limited access to internal structure which leads to limited access for code paths traversal.
- Defect association is difficult when grey testing is performed for distributed systems.

REASONS TO CONDUCT PEN-TESTING

A penetration test put forwards the perception into the most accessible aspects of a system. It is used as a alienation technique by the organisations to close the diagnosed holes or gaps before the process of the system gets started.

The prime reasons are highlighted below:

1. Risk Assessment

At the edge of technological era, cyberattacks like DDoS, phishing and ransomware are at a rapid increase which puts the companies at risk. Such attack causes in the loss of millions of dollars of revenue. For example: a ransomware attack is the attack which blocks a company from accessing the data, devices, network, and servers it relies on the conduct business.

The main task of pen tester is to identify and prevent the cyber security risks before they are exploited, hence it provides a great help to the IT leaders to upgrade the security holes and reduce the possible cyber-attacks.

2. Security Awareness

As technology advances, so do the strategies used by cyber criminals. Companies must be able to upgrade their security measures at the same rate in order to successfully protect themselves

and their assets from these threats. The downside is that it is frequently difficult to determine which approaches hackers are employing and how they might be employed in an attack. Organizations on the other hand, can rapidly and effectively identify, update, and replace the components of their system that are most vulnerable to modern hacking tactics by employing skilled ethical hackers.

3. Reputation

A data breach can jeopardise a company's reputation, especially if it becomes public. Customers may lose faith in the company and cease purchasing its products, while investors may be hesitant to invest in a company that does not take cyber defence seriously. Penetration testing safeguards reputation by providing proactive mitigation strategies.

4. Compliance

Healthcare, banking, and service providers, for example take compliance and regulation seriously and include pen testing as part of their compliance operations.

Pen- testing is required to follow common standards such as a Service organization Control 2 (SOC 2), HIPAA and the Payment card industry Data Security standard (PCIDSS). Organization can keep in top of their compliance demands by doing frequent planned pen testing.

DIFFERENCE BETWEEN PENETRATION AND VULNERABILITY ASSESSMENTS

- ***Penetration Testing***

Penetration testing is performed to identify vulnerabilities, malicious information, defects, and dangers. It is done to strengthen the organisation's security system in order to protect the IT infrastructure. Pen testing is another name for penetration testing. It is an official practise that can be considered beneficial rather than damaging. It is a part of an ethical hacking approach that focusses solely on infiltrating the information system.

- ***Vulnerability Assessment***

Vulnerability assessment is the process of identifying and quantifying security flaws in each environment. It is a comprehensive examination of the information security situation. It is used to identify potential flaws and gives the necessary mitigation steps to either eliminate or reduce the risk level.

The difference between Penetration Technique and Vulnerability Assessment is illustrated below:

SL.No.	Penetration Testing	Vulnerability Assessment
1.	This is meant critical real time system.	This is meant for non-critical systems.
2.	This is a goal-oriented procedures that should be carried out in a controlled manner.	This cost-effective assessment method is often considered safe to perform.
3.	It is a simulated cyber-attack carried out by experienced Ethical Hackers in a well-defined and controlled environment.	It is a automated assessment performed with the help of automated tools.
4.	The focus is to discovers unknown and exploitable weakness in normal business processes.	The focus is to list known software vulnerabilities that could be exploited.
5.	It gathers targeted information of the system.	It allocates quantifiable value and significance to the available resources.
6.	It determines the scope of an attack.	It makes a directory of assets and resources in each system.
7.	It only identifies the exploitable security vulnerabilities.	It identifies, categorizes, and quantifies security vulnerabilities.

ENDNOTES

[i] INVENSIS LEARNING, https://www.invensislearning.com/blog/penitration-testing-methodology/
[ii] EC COUNCIL, https://www.eccouncil.org/cybersecurity/what-is-penetration-testing/
[iii] ibid.
[iv] ibid.
[v] THREAT INTELLIGENCE, https://www.threatintelligence.com/blog/proactive-cybersecurity#:~)
[vi] EC COUNCIL, https://www.eccouncil.org/cybersecurity/what-is-penetration-testing/
[vii] TECH TARGET, https://techtarget.com/searchsecurity/definition/penetration-testing
[viii] INFO SAVVY, https://infosavvy.com/5-phases-of-hacking/
[ix] INVENSIS LEARNING, https://www.invensislearning.com/blog/phases-of-ethical-hacking/
[x] Bhawana Sahare, Study of Ethical Hacking, 2, INTERNATIONAL JOURNAL OF COMPUTER SCIENCE TRENDS AND TECHNOLOGY, 6, 8 (2014)
[xi] TECH TARGET, https://techtarget.com/searchsecurity/definition/penetration-testing)
[xii] NATIONAL VULNERABLE DATABASE, https://nvd.nist.gov/
[xiii] PACKT PUB, https://subscription.packtpub.com/book/security/9781788297134/1/ch01lvl1sec9/the-fundamentals-of-metasploit#:~:
[xiv] TECH TARGET, https://techtarget.com/searchsecurity/definition/penetration-testing
[xv] ECONOMIC TIMES, https://m.economictimes.com/defination/white-box-testing/amp
[xvi] ECONOMIC TIMES, https://economictimes.indiatimes.com/definition/white%20box%20testing
[xvii] ECONOMIC TIMES, https://m.economictimes.com/b/black-box-testing/amp_profileshow/51698917.cms
[xviii] ibid
[xix] Ibid
[xx] GEEKS FOR GEEKS, https://www.greeksforgreeks.org/grey-box-testing-software-testing/