# A Study on Penetration Testing Process and Tools

Hessa Mohammed Zaher Al Shebli (NYIT, Abu Dhabi, UAE), Babak D. Beheshti, PhD (NYIT, Old Westbury, New York)

Abstract: Information is more vulnerable than ever; and every technological advance raises new security threat that requires new security solutions. Penetration testing is conducted to evaluate the security of an IT infrastructure by safely exposing its vulnerabilities. It also helps in assessing the efficiency of the defense mechanisms tools and policy in place. The Penetration testing is conducted regularly to identify risks and manage them to achieve higher security standards. In this paper we discuss the importance of penetration testing, factors and components considered while conducting a penetration test, we present a survey of tools and procedures followed, role of penetration test while implementing in the IT governance in an organisation and finally the professional ethics to be possessed by the team involved in penetration test.

*Keywords: IT security, penetration test, IT governance, vulnerability assessment, ethics for professional hacking*

## 1. Introduction:

Data and information security is in the top priority list for companies these days. All Businesses need to protect its information's to build a competitive advantage. Information are protected using standard process and well documented structured methods. It is also ensured that they follow security standards and regulations. Some of the regulations process include security assurance process, software engineering environment for security, proof of correctness and penetration tests.

Penetration testing (aka PEN test) is a structured process to test an organization computing base which includes hardware, software and people. This process includes an analysis of the entire organizations' computing system looking for vulnerabilities like system configuration, software and hardware errors, and its operational process in order to identify the weakness.

A security test helps to ensure the behavior of the system security control, whereas a PEN test helps to determine the level of difficulty for an attacker to penetrate into an organization computing network. In a PEN test an unauthorized attack is demonstrated by a user on the test target system using automatic programmed tools, manual tools or both.

This paper includes a brief overview of PEN Testing, benefits of conducting a PEN test, the process and tools available for performing a PEN test. It also discusses the vulnerability assessment, penetration test in IT security standards like ISO 27000 and personal & professional ethics of the person involved in the penetration testing process.

## 2. PEN test benefits

A penetration test is used to identify the risks that may occur when an attacker get access to the organization's computing system and networks. Performing a PEN test will help estimate the mitigation plan to close security gaps before the actual attack happens. Conducting a PEN test helps organizations to reduce financial and information loss that would have caused loss in customer trust due to security breaches.

It safeguards the organizations against failure through preventing financial loss and provide compliance to industry regulators, customers and shareholders; helping to develop trust, corporate image, and rationalize IT security investments. As penetration testing is a proactive process, it provides unassailable information that helps the organization to meet the auditing or compliance aspects of regulations [1].

One of the main objectives of PEN testing is to create IT security and its importance at all levels

in an organization through structured training and awareness programs in order to avoid security incidents that may cause damage in terms of confidentiality, integrity, relationship and customer trust.

A PEN test helps organization to evaluate the level of security awareness among its employees, effectiveness of the existing security policy and process and also the efficiency of its products. It helps in decision making process to evaluate the organizations security and hence plan for the security investment and IT strategy.

Penetration testing also helps in shaping the important aspects of information security strategy by identifying the vulnerabilities quickly and accurately. It also supports in improving test configurations to proactively eliminate identified risks. It helps business to evaluate the impacts and likelihood of the vulnerabilities. Hence the organization can priorities and implement the mitigation action plan for the vulnerabilities identified. Penetration testing consumes lots of time, efforts and knowledge depending on the complexity of the business. Therefore, penetration testing supports the enhancement of the knowledge and competency of the persons involved in the process. It is considered as a quality assurance tool that benefits both business and operations.

## 3. Penetration testing strategies

There are three methods of penetration testing methods, based on the information available: black box, white box and gray box [1].

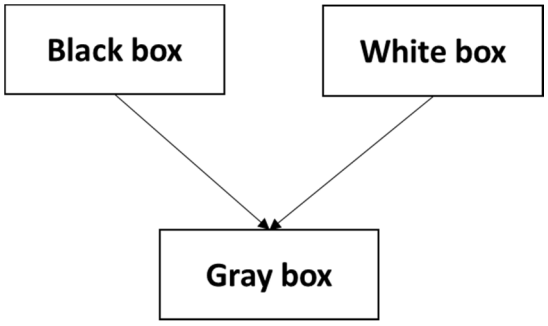


*Figure 1: Penetration testing methods*

In the black box penetration testing, the team has no information about the tested target. The possibilities for security breaches are identified from scratch.

In a white box penetration testing, the testers are given all the information about the test target.

Gray box penetration testing, the testers are provided with partial information about the tested target and the rest are for identification.

### 3.1. External testing

External testing is to perform an attack from outside the organization on the tested target. It helps to identify how, if an outside attacker gets in to the network and how far he can get access once taking controls.

### 3.2. Internal testing

In the internal testing, an attack is performed on the organization computing network as an internal user having standard access privileges. By doing internal testing, the tester can estimate the damages that may be caused by unhappy employee in the organization. In this process the test target is tested by penetrating a system and identifying the causalities as a user having standard access privileges.

### 3.3. Router Penetration

Router Penetration is testing the misconfiguration of router for specific vulnerabilities. Routing devices are used to direct network traffic, and if one router is misconfigured it can be used to manipulate network traffic. A compromise on routing device compromises the entire network traffic.

### 3.4. Firewall Penetration

Firewall Penetration is to perform an attempt to penetrate the firewall and host on the test target to look for vulnerabilities across the firewall security software, configuration settings and operating system itself. The results will help to identify the misconfigurations and eliminate poorly implemented security policies in the organization.

### 3.5. Application Penetration

Application Penetration is to perform conscientious testing of an applications to check for code related or back end vulnerabilities that provided access to the application itself, the

underlying operating system, or the data that the application can access. organizations employ experts to perform application penetration and security assessment testing online trade portals or other applications like games, antivirus and embedded applications.

**Intrusion Detection System**

Intrusion Detection System Penetration is to attempts and penetrate IDS from outside as well as inside to find loop holes due to weak security policies. Though it is unlikely to have complete information on the rule set of existing IDS, many hackers and security consultants do understand the common IDS rule set, including typical threshold values. They develop their penetration strategy around bypassing the common IDS configuration. The test should help to identify holes in IDS rules, signatures or thresholds to avoid IDS.

### 3.6. Password Cracking Penetration

Password Cracking Penetration is to extract password and shadow files in Linux or extract SAM files in windows and use cracking tools. Some of the passwords cracking tools are john the ripper, pwdump3, l0phtcrack. The process is to identify the target person's personal profile and try various password cracking tools to break password protected files. Then the password cracking team makes a report and presents it to the organization.

### 3.7. Social engineering

Social engineering is a term used to describe an attack that relies entirely in human error. It gathers valuable and sensitive information through the use of psychological manipulation to trick legitimate users. This kind of attack is very dangerous since users' mistakes are less predictable.

PEN testing helps the organization evaluate their staff adherence to the organizations' policies and procedures. It also helps in improving the security training provided for the employees.

**PEN test process**

To conduct a penetration test and document its outcome it needs a systematic approach which are circulated to different organization units and management level in the organization. The Penetration testing is conducted in three phases [2]:

1. Test preparation.
2. Test implementation.
3. Test analysis.

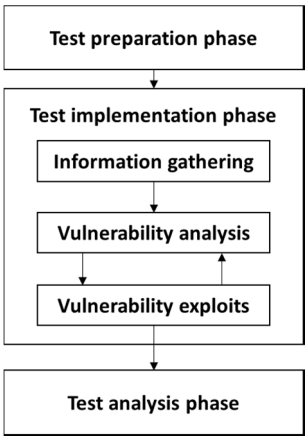


*Figure 2: Phases of penetration test*

### 4.1. Test preparation

In test preparation the documents are collected and finalized. In this phase the scope of the system components, objective of the test, test duration and time are identified, agreed and documented. Predicted incidents like information leakage, downtime is also identified and are documented in the legal documents and are agreed and signed by both sides.

### 4.2. Test implementation

This phase involves the following steps:

- information gathering.
- vulnerability analysis.
- vulnerability exploits.

During the information gathering step it is required to scan and identify all logical and physical areas and all possible information required for the analysis of vulnerability analysis. Depending on the information collected, the tester, analysis and assess the vulnerabilities exists [4]. The test can be conducted using automated testing tools or manual testing tools or both sometimes.

In the vulnerability assessment step, the penetration tester will receive the challenge to evaluate and find the necessary security defeats from the target. This task requires complete attention in process of the penetration testing. It is very important to ensure that each task, functions, and processes followed in specific and proper way step by step. In the proposed model of penetration testing this phase expands in two main procedures: Code Analysis and Vulnerability Analysis

Code Analysis is used to find security flaws by analyzing source code. Usually analysis like this would automatically find security flaws with a high degree.

This vulnerability analysis is divided into two areas. Identifying and reducing the number of new vulnerabilities before the software is deployed. With vulnerability discovery, it strives to help engineers understand how vulnerabilities are created and found. Main goal is that, with this education, engineers will learn how to detect and eliminate and eventually avoid vulnerabilities in software products before the products are shipped. The unfortunate reality is that many software products are being shipped with vulnerabilities that attackers may be able to exploit [3].

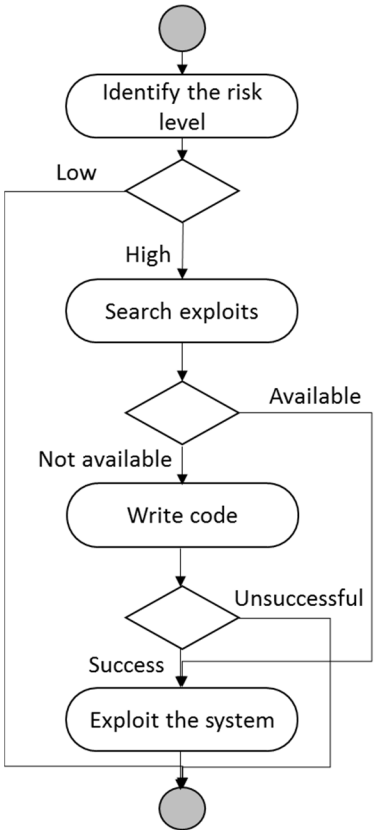


*Figure 3: Logical model of a penetration test process*

This vulnerability remediation process involves a comprehensive approach to protecting systems using below equation

Total Vulnerability = (CA + VA)

Where CA =Code Analysis and

VA=Vulnerability Analysis.

In the last step the tester exploits for the vulnerabilities found in the vulnerability analysis step. Exploitation is the process to gain access by taking advantage of vulnerabilities which received previously through analysis phase. Generally, this phase performs if client is agreeing to evaluate impact of risks due to existing vulnerability because this phase contains high risk and may damage the targeted system. However, using this task penetration tester can evaluate the perfect solutions and impacts of existing vulnerability. An exploit is a set of commands that takes advantage of vulnerability and may cause unintended behavior to software, hardware, or something electronic. This include privilege escalation, DoS denial of service attacks and gaining control to restricted parts. Sometimes

exploits when investigated do not results to what it was intended and hence may require more analysis, which is usually feedback process or self learning process between vulnerability analysis and exploits.

### 4.3. Test analysis.

Reporting, when penetration testing process has been compiled at same time the next process is to provide advisory and various reports to senior management through reporting process, IT management and IT technical staff will all likely see the report, or at least part of it. The report has sections: core Summary, Technical detail, assessment Findings, Risk Level indication overview, Patch information advisory, Budget information and Time Estimation etc... Using this report penetration tester can represent the entire process to the IT management so that the final solution can be obtain and implement. A mitigation plan is prepared after the penetration testing.

Advisory, the final phase of penetration model includes security solution and patched information against all found risks such as Preparation of Countermeasures, Budget Estimation, Time Estimation, Creating Advisory Map, Discussion with the Client, Recheck the implemented Solution etc… this is the task where penetration tester must give definitive and conclusive advisory report for various solutions and the cost. In many instances when the penetration testing is completed, it is essential for the client to install the suitable patches. In such cases, security solution should be provided in both open source and paid solutions. The advisory phase is dependent on reporting phase because advisory must be prepared after complete review of all different reports. Advisory mainly direct to include three major components to install.

1. Advice to install the patch if available
2. Advise to install the open source patch if available
3. Advise to install paid patches and software

## 4. Tools for penetration testing

There are a wide variety of tools that are used in Penetration Testing and the important tools are [3]:

### 5.1. NMap

NMap is also called Network Mapper In order to develop network services and maps, NMap sends specifically crafted packets to the target host and then analyses the responses. NMap supports the scanning of the various types of protocols and most of the existing systems.

### 5.2. BeEF

BeEF is stands for The Browser Exploitation Framework focuses on the web browser. It works on Linux, Apple Mac OS X and Microsoft Windows. BeEF allows the professional penetration tester to assess the actual security posture of a target environment. It investigates the exploitability in the context of web browsers.

### 5.3. Metasploit

Metasploit is test tools that test for weaknesses in operating systems and applications. This penetration testing tool is based on the concept of ‘exploit’. It runs a set of code on the test target creating framework for penetration testing. It works on Linux, Apple Mac OS X and Microsoft Windows [3].

### 5.4. Nessus

Nessus is a penetration testing tool and remote security scanner, typically run on one machine to scan the services offered by a remote machine. Nessus is the world’s most popular vulnerability scanner that is used in over 75,000 organizations worldwide. This tool allows the user to script and run specific vulnerability checks. These checks provide a lot of control where most products do not.

### 5.5. Cain and Abel

Cain and Abel mostly used for password cracking. It uses network sniffing, Dictionary attack, Brute-Force and Crypt analysis attacks, and routing protocol analysis methods to accomplish this. This is entirely for Microsoft operating systems.

## 5. Information Security Management System (ISMS)

Information Security Management System (ISMS) which specifies the requirements for the implementation of security controls customized to the needs of organizations to minimize assets risks and ensure business continuity [6]. The ISMS is designed to protect the information assets from any security breaches. ISO27k is a series of international standards for Information security management. This standard covers all types of organizations: commercial business, government agencies and non-profit organizations, all sizes from micro-businesses to multinational business.

The services taken into consideration are (C-I-A) traits:

- Information Confidentiality,
- Information Integrity
- Service availability.

Information Security Management System is based on the PDCA model also known as Plan Do Check and Act model, which is applied to structure its processes.

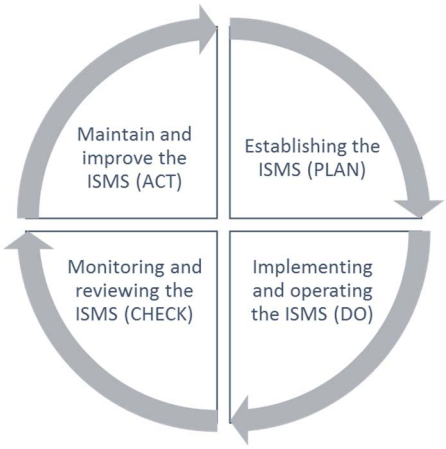


*Figure 4: Plan-Do-Check-Act (PDCA) model*

The results of the tests will help to identify weaknesses within information security and provide information on how these weaknesses can be penetrated by an attack [2]. These can then be used as part of the risk assessment and steps implemented to enable remedial action.

## 6. Professional Standards and Ethical Competency

Penetration testing is effective when it is a team of professionals, where all have their roles and responsibilities appointed and everyone what must done and how [9]. While conducting a penetration test on a system or protocol, there are several ethical and competency issues faced by the person involved. Explicitly including or significant omission could possibly be dangerous to the organisation [6]. Always the tester employees is ethically and legally complied to meet the customers requirement and hence ensure that these test do not lead false or misleading issues.

There are Code of Conduct and Best Practice laid by professional bodies, but while conducting the test the individual is often required to take an informed decision and hence should possess the necessary procedural, ethical and technical training such as:

- IEEE, 2010
- IEEE Computer Society IEEE CS
- BCS British Computer Society
- BCS - The Chartered Institute for IT, 2010
- BCS Information Security Specialist Group BCS-ISSG
- Institute of Information Security Professionals (iisp)

## 7. Professional Standards and Technical Competency

Professional bodies set industrial standards to distinguish members and non-members. It is called code of conducts and mark as a guide to the penetration tester.

The common codes of conducts are:

- EC Council or EC Council, 2010
- ISC2 code of ethics of The ISC 2 code of ethics

All testers and personals involved in the PEN test have to keep up their knowledge and update on the tests and development. It is important to

constantly develop skills and understanding of new system that are being developed and used.

OSSTMM Open Source Security Testing Methodology Manual are used in developing technical skills and knowledge.

OWASP Open Web Application Security Project are used for internet based applications

## 8. Conclusion

In this paper, we have discussed penetration test, factors to be considered while performing penetration test, the process of conducting penetration test, commonly used tools and software for conducting a penetration test. The process becomes effective if the actions are taken to solve the vulnerabilities identified. Finally, is comes to the organisational process and personal ethics in managing the risk and vulnerabilities. Hence in this paper we have also discussed the role of the Information Security Management System (ISMS), professional Ethical and technical Competency required for performing the penetration test.

## 9. References


[1] X. Y. B.-T. B. C. M. J. Aileen G. Bacudio, "AN OVERVIEW OF PENETRATION TESTING," *International Journal of Network Security & Its Applications (IJNSA),* vol. 3, no. 6, 2011.

[2] V. S. KUMAR, "Ethical Hacking and Penetration Testing Strategies," *International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE),* vol. 11, no. 2, pp. ISSN 0976-1353, 2014.

[3] P. Ami and A. Hasan, "Seven Phrase Penetration Testing Model," *International Journal of Computer Applications,* vol. 59, no. 5, p. ISSN: 0975 – 8887, 2012.

[4] K. ,. K. K. Ankita Gupta, "Vulnerability Assessment and Penetration Testing," *International Journal of Engineering Trends and Technology-,* vol. 4, no. 3, 2014.

[5] G. K. Gurline Kaur, "Penetration Testing: Attacking Oneself to Enhance Security," *International Journal of Advanced Research in Computer and Communication Engineering ,* vol. 5, no. 4, pp. ISSN: 2278-1021 , 2016.

[6] M. Z. H. M. T. A. C. Muhammad Zunnurain Hussain, "Penetration Testing In System Administration," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH,* vol. 6, no. 6, pp. ISSN 2277-8616, 2017.

[7] A. B. a. T. M. William Knowles, "Analysis and recommendations for standardization in penetration testing and vulnerability assessment," BSI group, London, 2014.

[8] S. S. M. A.-J. R. Q. F. M. a. F. D. Awni Itradat, "Developing an ISO27001 Information Security Management System for an Educational Institute: Hashemite University as a Case Study," *Jordan Journal of Mechanical and Industrial Engineering ,* vol. 8, no. 2, pp. 102-108, 2014.

[9] J. M. a. C. I. S. Faily, "Ethical Dilemmas and Dimensions in Penetration Testing," in *Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015)* , London, 2015.

[10] A. G. J. a. M. J. W. Justin D. Pierce, "PENETRATION TESTING PROFESSIONAL ETHICS: A CONCEPTUAL MODEL AND TAXONOMY," *Australasian Journal of Information Systems,* vol. 13, no. 2, 2006.