International Journal of of Grid and Distributed Computing
Vol.2, No.2, June 2009

# Methodology for Penetration Testing

Farkhod Alisherov A., and Feruza Sattarova Y.

*Multimedia Engineering Department, Hannam University,*
*South Korea*
*sntdvl@yahoo.com, mymail6585@gmail.com*

***Abstract***

*Penetration testing is one of the oldest methods for assessing the security of a computer system. The idea behind penetration testing methodologies is that the penetration tester should follow a pre-scripted format during test as dictated by the methodology. A penetration testing methodology was proposed in this research. It is also important to consider a policy that should be followed by both the tester and the client to reduce financial and confidential disparities, and to bring conformity to the operations between the both parties, so this research suggests a policy that should be followed by penetration testers and clients of the penetration tests.*

***Keywords:*** *Penetration Testing Methodology, Penetration Testing.*

## 1. Introduction

Penetration testing is one of the oldest methods for assessing the security of a computer system. In the early 1970's, the Department of Defense used this method to demonstrate the security weaknesses in computer systems and to initiate the development of programs to create more secure systems. Penetration testing is increasingly used by organizations to assure the security of Information systems and services, so that security weaknesses can be fixed before they get exposed. [1] But when the Penetration test is performed without a well-planned and professional approach – it can result to what it is supposed to prevent from.

In order to protect company data, companies often take measures to guarantee the availability, confidentiality and integrity of data or to ensure access for authorized persons only. These measures include security concepts, authorization concepts and firewall systems. However, establishing these kinds of security systems is no guarantee that the legal requirements are met. Rather, the system's compliance with the legal requirements and stipulations must be checked for each individual case. Penetration tests are a suitable means of verifying the effectiveness of such measures in certain areas. [2]

The objective of the Penetration Testing service is to identify and report on security vulnerabilities to allow the Company to close the issues in a planned manner, thus significantly raising the level of their security protection. The Company understands that Internet security is a continually growing and changing field and that testing penetration testers does not mean that the Company's site is secure from every form of attack. There is no such thing as 100% security testing, and for example it is never possible to test for vulnerabilities in software or systems that are not known at the time of testing or the mathematically complete set of all possible inputs/outputs for each software component in use. Further security breaches can and frequently do come from internal sources whose access is not a function of system configuration and/or external access security issues.

There are many methodologies you can choose from, there is no such thing as “the right methodology”. Every penetration tester has his/her own approach to testing, but each one uses a methodology, in order for the test to be carried out professionally, effective and less time consuming. If a tester has no methodology to use in his test, then that might result to:

- Incomplete testing (e.g. the tester might not fulfill all of the requirements)
- Time consuming (e.g. a lot of time will be spent to re-order your test to “being-end” format)
- Waste of effort (e.g. the testers might end up testing the same thing)
- Ineffective testing (e.g. the results and the reporting might not suit the requirements of the client)

Methodology is a “map” using which you will reach your final destination (end of test) and without a methodology the testers might get “lost” (reach the abovementioned results).

## 2. Related work

Penetration testing is one of the oldest methods for assessing the security of a computer system. In the early 1970's, the Department of Defense used this method to demonstrate the security weaknesses in computer systems and to initiate the development of programs to create more secure systems. Penetration testing is increasingly used by organizations to assure the security of Information systems and services, so that security weaknesses can be fixed before they get exposed. [1] But when the Penetration test is performed without a well-planned and professional approach – it can result to what it is supposed to prevent from.

In order to protect company data, companies often take measures to guarantee the availability, confidentiality and integrity of data or to ensure access for authorized persons only. These measures include security concepts, authorization concepts and firewall systems. However, establishing these kinds of security systems is no guarantee that the legal requirements are met. Rather, the system’s compliance with the legal requirements and stipulations must be checked for each individual case. Penetration tests are a suitable means of verifying the effectiveness of such measures in certain areas. [2]

The objective of the Penetration Testing service is to identify and report on security vulnerabilities to allow the Company to close the issues in a planned manner, thus significantly raising the level of their security protection. The Company understands that Internet security is a continually growing and changing field and that testing penetration testers does not mean that the Company’s site is secure from every form of attack. There is no such thing as 100% security testing, and for example it is never possible to test for vulnerabilities in software or systems that are not known at the time of testing or the mathematically complete set of all possible inputs/outputs for each software component in use. Further security breaches can and frequently do come from internal sources whose access is not a function of system configuration and/or external access security issues.

There are many methodologies you can choose from, there is no such thing as “the right methodology”. Every penetration tester has his/her own approach to testing, but each one uses a methodology, in order for the test to be carried out professionally, effective and less time consuming. If a tester has no methodology to use in his test, then that might result to:

- incomplete testing (e.g. the tester might not fulfill all of the requirements)
- time consuming (e.g. a lot of time will be spent to re-order your test to “being-end” format)
- waste of effort (e.g. the testers might end up testing the same thing)

- ineffective testing (e.g. the results and the reporting might not suit the requirements of the client)

Methodology is a “map” using which you will reach your final destination (end of test) and without a methodology the testers might get “lost” (reach the abovementioned results).

## 3. Proposed methodology

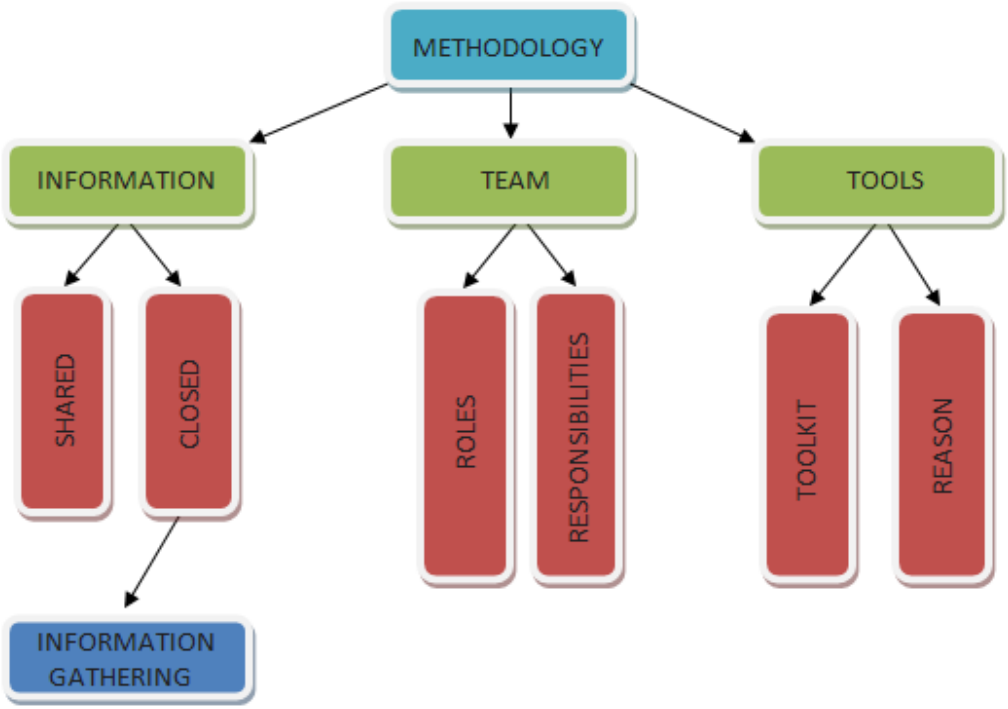


Figure 1. Proposed methodology model

While there are several available methodologies for you to choose from, each penetration tester must have their own methodology planned and ready for most effectiveness and to present to the client. In the prosposed methodology planning, there are 3 main figures that must be fully understood and followed:

**1. Information.**

Information gathering is essentially using the Internet to find all the information you can about the target (company and/or person) using both technical (DNS/WHOIS) and non-technical (search engines, news groups, mailing lists etc) methods. Whilst conducting information gathering, it is important to be as imaginative as possible. Attempt to explore every possible avenue to gain more understanding of your target and its resources. Anything you can get hold of during this stage of testing is useful: company brochures, business cards, leaflets, newspaper adverts, internal paperwork, and etc. Information gathering does not require that the assessor establishes contact with the target system. Information is collected (mainly) from public sources on the Internet and organizations that hold public information (e.g. tax agencies, libraries, etc.)

Information gathering section of the penetration test is important for the penetration tester. Assessments are generally limited in time and resources. Therefore, it is critical to identify points that will be most likely vulnerable, and to focus on them. Even the best tools are useless if not used appropriately and in the right place and time. That's the reason why experienced testers invest an important amount of time in information gathering. [4]

There are commonly 2 types of penetration testing:

• When the information about the organization is Closed (Black box) - the pen-tester performs the attack with no prior knowledge of the infrastructure, defence mechanisms and communication channels of the target organization. Black box test is a simulation of an unsystematic attack by weekend or wannabe hackers (script kiddies).

• And when the information is Shared (White box) - the pen-tester performs the attack with full knowledge of the infrastructure, defence mechanisms and communication channels of the target organization. White box test is a simulation of a systematic attack by well prepared outside attackers with insider contacts or insiders with largely unlimited access and privileges.

If the penetration testers are using the "Black Box" approach, then Information gathering must be planned out, because information gathering is one of the most important processes in penetration testing and it's one of first phases in security assessment and is focused on collecting as much information as possible about a target application. This task can be carried out in many different ways: by using public tools (search engines), scanners, sending simple HTTP requests, or specially crafted requests, it is possible to force the application to leak information, e.g., disclosing error messages or revealing the versions and technologies used [5].

If the penetration testers are using the "White Box" approach, then the tester should target the information gathering procedure based on the scope (e.g. the clinet might give all the required information, and might not want the testers to search for other information)

Basically there are 4 phases to information gathering:

**Phase 1.** The first step in information gathering is - network survey. A network survey is like an introduction to the system that is tested. By doing that, you will have a "network map", using which you will find the number of reachable systems to be tested without exceeding the legal limits of what you may test. But usually more hosts are detected during the testing, so they should be properly added to the "network map". The results that the tester might get using network surveying are:

- Domain Names
- Server Names
- IP Addresses
- Network Map
- ISP / ASP information
- System and Service Owners

Network surveying can be done using TTL modulation(traceroute), and record route (e.g. ping -R), although classical 'sniffing' is sometimes as effective method

**Phase 2.** 2nd phase is the OS Identification (sometimes referred as TCP/IP stack fingerprinting). The determination of a remote OS type by comparison of variations in OS TCP/IP stack implementation behavior. In other words, it is active probing of a system for responses that can distinguish its operating system and version level. The results are:

- OS Type
- System Type
- Internal system network addressing

The best known method for OS identification is using nmap[3]

**Phase 3.** Next step is port scanning

Port scanning is the invasive probing of system ports on the transport and network level. Included here is also the validation of system reception to tunneled, encapsulated, or routing protocols. Testing for different protocols will depend on the system type and services it offers. Each Internet enabled system has 65,536 TCP and UDP possible ports (incl. Port 0). However, it is not always necessary to test every port for every system. This is left to the discretion of the test team. Port numbers that are important for testing according to the service are listed with the task. Additional port numbers for scanning should be taken from the Consensus Intrusion Database Project Site. The results that the tester might get using Port scanning are:

- List of all Open, closed or filtered ports
- IP addresses of live systems
- Internal system network addressing
- List of discovered tunneled and encapsulated protocols
- List of discovered routing protocols supported

Methods include SYN and FIN scanning, and variations thereof e.g. fragmentation scanning

**Phase 4.** Services identification. This is the active examination of the application listening behind the service. In certain cases more than one application exists behind a service where one application is the listener and the others are considered components of the listening application. A good example of this is PERL installed for use in a Web application. In that case the listening service is the HTTP daemon and the component is PERL. The results of service identification are:

- Service Types
- Service Application Type and Patch Level
- Network Map

The methods in service identification are same as in Port scanning

There are two ways using which you can perform information gathering:

1. 1st method of information gathering is to perform information gathering techniques with a 'one to one' or 'one to many' model; i.e. a tester performs techniques in a linear way against either one target host or a logical grouping of target hosts (e.g. a subnet). This method is used to achieve immediacy of the result and is often optimized for speed, and often executed in parallel (e.g. nmap).

2. Another method is to perform information gathering using a 'many to one' or 'many to many' model. The tester utilizes multiple hosts to execute information gathering techniques in a random, rate-limited, and in non-linear way. This method is used to achieve stealth. (Distributed information gathering [4])

**2. Team.** Penetration testing is most effective if it's a team of professional, which all have their roles and responsibilities appointed and all know what he/she must do and how to do it. In penetration testing, as in any sphere, each team member must know his/her part of the team, and should follow the affixed procedure (e.g. network administrator, should not be searching for vulnerabilities through the web-site) in order for the test to be quick, efficient and less time consuming. (e.g. security consultant is responsible to make the report clear and understandable, in order for the technicians to be more focused on testing rather than reporting)

**3. Tools.** And the last most important part of the test is the toolkit. Each penetration testers have their "toolset" to perform a penetration test. These tools are usually chosen in order to make their work most effective (a test cannot be effective if the owner of the system assigns tools, which the testers are not familiar with). There are many tools available, and many of them are available for free usage, but the penetration testers must have excellent usage at least with some of them, rather that know most of them on an average level.

It is also vital for the testers to choose their toolkits wisely, since this not only one area to perform a penetration test in (software development, network). For example, network vulnerability scanners that try to evade detection by IDS and IPS devices would normally not be useful for software development. So the testers should choose the toolkit with features that are suitable for them (e.g. Configurability, Extensibility).

## 4. Policy

**1. The Company must provide the penetration tester with certain required information regarding the scope and range of the tests and all information provided must be true and accurate.**

This is done for the purpose of:

- Accuracy; e. g. with the defined scope the test will be "pin-pointed", and the tester will have a "test-map" which to follow throughout the test

- Confidentiality; e. g. with the defined ranges of the test, the tester will not be testing and/or acquiring the information which is confidential even for the tester

- Resource saving; e. g. with the defined scope and range, the tester will not be spending time and human resources on testing non-required targets

**2. Penetration tester must gather all the information required for the testing only within the defined boundaries of the test and all of this information must be reported completely at the end of the test.**

Purpose:

- Privacy; e. g. all of the gathered information must be reported so that there will be no "information leaks"

**3. The Company and the tester must agree upon a timing table of the tests**

Purpose:

- Safety; e. g. so that tests will be carried in a non-harmful for them period (a DoS attack will not be carried out in a busy network period)

**4.1 The penetration tester must be held responsible for all the damage that occurs to the reason of testing.**

The penalty for the damage (data loss, equipment destruction) should be agreed upon and stated in the contract prior to the testing.

**4.2 The damage that has occurred not to the fault of the test is the responsibility of the Company**

There are also cases that damage is occurred which is not the responsibility of the tester, for example the DoS attack was carried out, which led to financial loss (because of no service), but the timing of the DoS attack was not agreed upon. This is why timing is important (refer to policy rule #3)

**5. The Company and the penetration tester must keep all the information of the test, including the contract as confidential.**

No information about contract, terms, fees should be released by either party. Information about the Company's business or computer systems or security situation that the tester obtains during the course/and after the completion of the test must not be released to any third party without prior written approval.

**6. The provider may assign or sub-contract all or any part of its rights and obligations under a contract to third parties without the Company's prior written consent.**

Some penetration testing companies assign different stages of testing to third-parties, this does not have to be approved by the client. The penetration tester utilizes a team approach employing experts to test different security aspects. All sub-contractors employed by the penetration tester shall, however, be bound by the terms and conditions of a same contract as between the Company and the penetration tester.

**7.1 The penetration tester and the Company may from time to time impart to each other certain confidential information relating to each other's business including specific documentation.**

There are times when tester might need additional information (contacts, accounts), and/or the client might provide additional information (e. g. passwords, user accounts) during the testing. All of this information should keep confidentiality as information given prior to the test, or acquired during the testing (refer to policy rule #5)

**7.2 Each party must use such confidential information only for the purposes of the test and that it must not be disclosed directly or indirectly to any third party**.

**8. After the completion of the testing and reporting the provider has no rights to the information or the data of the Company, unless approved by the Company.**

During the testing, the penetration is granted access, and/or acquires access to confidential information. After the completion of the test, the tester no longer has right to the information, or any further "testing", unless the client of the test approves.

**9. The penetration tester holds no responsibility for the loss and/or damage that is occurred in case if a "real" attack is occurred during the testing period.**

If a "real" attack occurred during the testing period, the tester holds no responsibility to that attack, however if that attack occurred to the result of information leak from the tester, then the tester is responsible for the damage.

## 5. Conclusion

One of the crucial factors in the success of a pen-test is the underlying methodology. Lack of a formal methodology means no consistency, and the client wouldn't want to be paying and watching the testers testing cluelessly. While a penetration tester's skills need to be specialized for the job, the approach shouldn't be. In other words, a formal methodology should provide a disciplined framework for conducting a complete and accurate penetration test, but need not be restrictive - it should allow the tester to fully explore his/her intuitions.
A penetration test is useless without a well-implemented security policy. In order for the testing service to bring conformity between penetration testers and clients of the penetration test, a penetration testing policy was suggested in this research. Methodology makes the testing service more effective, while Policy – will reduce financial and confidential disparities between the two parties of the testing service.

## Acknowledgements

This work was supported by the Security Engineering Research Center, granted by the Korean Ministry of Knowledge Economy.

## References

[1] http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1083683,00.html
[2] http://www.weblaw.co.uk/templates_agreements/ethical_hacking_penetration_testing/
[3] http://www.infosecinstitute.com/blog/ethicalhacking_computer_forensics.html
[4] http://www.oissg.org/wiki/index.php/PENETRATION_TESTING_METHODOLOGY
[5] http://searchnetworking.techtarget.com/generic/0,295582,sid7_gci1083715,00.html