PENETRATION TESTING – A SYSTEMATIC APPROACH

INTRODUCTION:

The basic idea behind writing this article was to put forward a systematic approach that needs to be followed to perform a successful penetration test. It has been written keeping in mind both, existing penetration testers as well as newcomers who want to make this field as a career. People responsible for maintaining security in an organization can refer to this and know what they can expect from such an exercise.

PENETRATION TEST – A BUSINESS PERSPECTIVE:

The question most commonly asked by any organization is "Why would I ever need a penetration test?" after all it costs a lot of money in hiring an external consulting firm or to invest in expensive tools to perform a penetration test. You must realize that it is very important for any organization to justify the cost involved for such an activity.

The important thing here that needs to be understood is that you may be successful in finding loads of vulnerabilities in any system, but unless those results are not analyzed thoroughly and a proper risk mitigation plan is not prepared, the test would not add any significant value to the business of any organization. Thus for giving a complete value for money, a successful penetration test would be that which would help an organization to understand the business risks arising from the vulnerabilities, and would provide a proper risk mitigation plan that fits the organizations business policy.

Agreed that a penetration test would involve a lot of risks like bringing a production system down, etc., but a properly planned penetration test would definitely add value in an organizations security framework. It should be understood that a penetration test with proper systematic approach, if included as an ongoing process in an organizations risk assessment plan, will lead to a better understanding of the current security posture of the organization and will help the organization in mitigating the risks at the proper time.

It should be noted that unlike the hype, a penetration test is not just a mere hacking exercise. It is a very essential part of the complete Risk Assessment Strategy of the organization. If used effectively, penetration test is a great tool by which any organization can measure the current security level of its network and systems. It is a good idea to have a penetration test done at regular intervals; after all you wouldn't skip your health checkup, would you?

WHAT IS PENETRATION TESTING:

"Penetration testing can be defined as a security-oriented probing of a computer system or network to seek out vulnerabilities that an attacker could exploit" [1]. The purpose of this exercise is to identify methods of gaining access to a system by using common tools and techniques used by attackers. This process involves a thorough active analysis of all the security related features of the systems in question, followed by an attempt to break into the system by breaching these security features.

TYPES OF PENETRATION TEST:

There are primarily two types of penetration tests, viz.:

- Black-Box Test
- White-Box Test

The type of penetration test usually depends upon what an organization wants to test, whether the scope is to simulate an attack by an insider (usually an employee, network/system administrator, etc.) or an external source. The difference between the two is the amount of information provided to the penetration tester about the systems to be tested.

In a black-box penetration test, the scenario is closely simulated to that of an external attacker, giving very little or no knowledge about the systems to be tested (except the IP address ranges or a domain name). The penetration tester is usually left on his own to gather as much information about the target network or systems as possible, which he can use to perform the test.

In a white-box penetration test, the penetration tester is usually provided with a complete knowledge about the network or systems to be tested, including the IP address schema, source code, OS details, etc. This can be considered as a simulation of an attack by any insider who might be in possession of the above knowledge.

METHODOLOGY:

Penetration test can be broadly carried out using a four phase methodology as shown in the figure below:

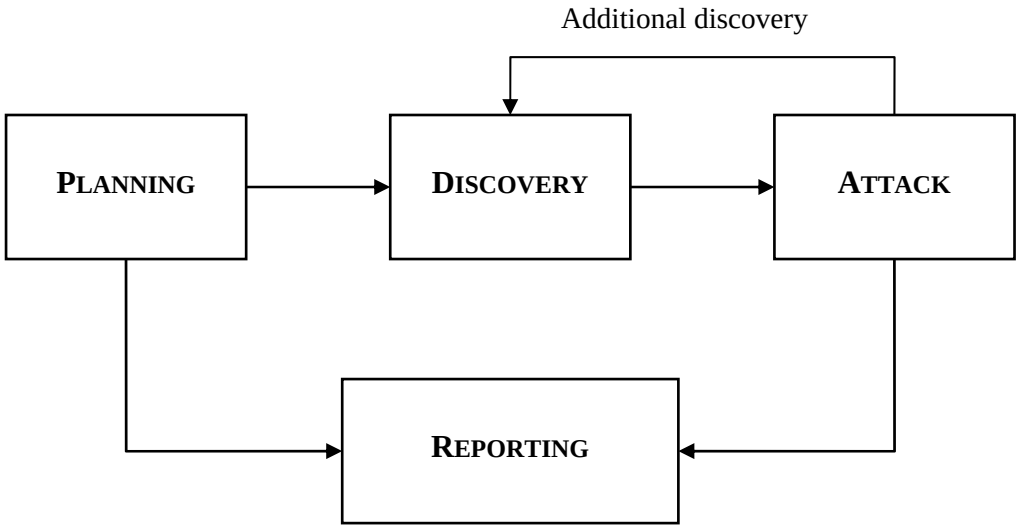

Fig. 1: Four Phase Penetration Testing Methodology [2]

PLANNING PHASE:

The planning phase is where the scope for the assignment is defined. Management approvals, documents and agreements like NDA (Non Disclosure Agreement), etc., are signed. The penetration testing team prepares a definite strategy for the assignment. Existing security policies, industry standards, best practices, etc. will be some of the inputs towards defining the scope for the test. This phase usually consists of all the activities that are needed to be performed prior to commencement of the actual penetration test.

There are various factors that need to be considered to execute a properly planned controlled attack. Unlike the hacker, a penetration tester has lots of limitations when executing a test, hence proper planning is needed for a successful penetration test. Some of the limitations are:

- Time: In a real world situation, a hacker has ample amount of time to carefully plot his attack. For a penetration tester, it is a time bound activity. He has to adhere to strict timings that are agreed upon prior to the exercise. Factors like organizations business hours need to be considered.

- Legal Restrictions: A penetration tester is bound by a legal contract, which lists the acceptable and non-acceptable steps a penetration tester must follow religiously as it could have grave effects on the business of the target organization.

There are also other limitations an organization might impose on the penetration tester, which it feels might have a business impact, like possible down-time, information leakage, etc. All these factors need to be considered during this stage.

DISCOVERY PHASE:

The discovery phase is where the actual testing starts; it can be regarded as an information gathering phase. This phase can be further categorized as follows:

- Footprinting phase
- Scanning and Enumeration phase
- Vulnerability Analysis phase

Footprinting:

The process of footprinting is a completely non-intrusive activity performed in order to get the maximum possible information available about the target organization and its systems using various means, both technical as well as non-technical. This involves searching the internet, querying various public repositories (whois databases, domain registrars, Usenet groups, mailing lists, etc.).

Many penetration testers tend to overlook this phase, but you will be surprised to see a significant amount of interesting and confidential data lying all around the internet. This information can be gathered by a penetration tester without actively probing the target systems and thus staying invisible. Useful information like IT setup details, company email addresses, device configurations, and sometimes usernames and passwords (….yes that's right .....Passwords!!!) which can be used for conducting Social engineering attacks.

A penetration tester must utilize this phase as much as possible and be creative enough in identifying various loopholes and try to explore every possible aspect that could lead to relevant information leakage about the target organization in the shortest time possible.

Many of the above procedures can be automated by writing customized scripts or small programs.

Scanning and Enumeration:

The scanning and enumeration phase will usually comprise of identifying live systems, open / filtered ports found, services running on these ports, mapping router / firewall rules, identifying the operating system details, network path discovery, etc.

This phase involves a lot of active probing of the target systems. A penetration tester must be careful and use the tools for these activities sensibly and not overwhelm the target systems with excessive traffic. All the tools used for this phase and the successive phases must be thoroughly tested in a testing environment prior to using them in a live scenario.

Various port scanners are available freely on the internet. Some of the most popular port-scanners are:

- Nmap
- SuperScan
- Hping

After successfully identifying the open ports, services behind them should be fingerprinted, either manually or by using readily available tools. It is recommended that the penetration tester confirm the exact name and version of the services running on the target system and the underlying Operating System before including the same in the final report. This will also help in identifying and eliminating various false positives found later.

Various Service and OS fingerprinting tools are available on the internet. Some of them are:

- Xprobe2
- Queso
- Nmap
- p0f
- Httprint
- Amap
- Winfingerprint

More details about various port-scanning and fingerprinting techniques can be found here:

- http://www.insecure.org/nmap/nmap-fingerprinting-article.html
- http://net-square.com/httprint/httprint_paper.html
- http://www.irongeek.com/i.php?page=videos/nmap1
- http://www.irongeek.com/i.php?page=videos/nmap2

Vulnerability Analysis:

After successfully identifying the target systems and gathering the required details from the above phases, a penetration tester should try to find any possible vulnerabilities existing in each target system. During this phase a penetration tester may use automated tools to scan the target systems for known vulnerabilities. These tools will usually have their own databases consisting of latest vulnerabilities and their details.

It is important for any penetration tester to be up to date with the latest security related activities. More often than not this phase solely depends on the experience of the

penetration tester. A successful penetration tester will always keep himself updated to the latest vulnerabilities by means of joining security related mailing-lists, security blogs, advisories, etc.

Some good informational sites, mailing-lists available for references are:

- http://www.phrack.org
- http://www.securityfocus.com
- http://www.secunia.com
- http://www.pulltheplug.org/
- http://www.schneier.com/blog/
- http://taosecurity.blogspot.com/
- http://www.securityfocus.com/archive
- http://packetstormsecurity.org/
- http://www.milw0rm.com/
- http://www.securiteam.com/
- http://cve.mitre.org/
- http://www.osvdb.org/

During this phase a penetration tester may also test the systems by supplying invalid inputs, random strings, etc., and check for any errors or unintended behavior in the system output. By doing so there are many possibilities that the penetration tester may come across unidentified vulnerabilities.

It makes sense not to rely only on automated tools for this activity; as manual testing may more often than not, result in some kind of vulnerability to be discovered.

Many good vulnerability scanners, both commercial and open-source are available. Some of them are:

- Nessus
- Shadow Security Scanner
- Retina
- ISS Scanner
- SARA
- GFI LANguard

But please remember that penetration testing is not a mere tool based activity. A penetration tester must use his expertise and judgment in every possible way.

ATTACK PHASE:

This is the phase that separates the Men from the Boys. This is at the heart of any penetration test, the most interesting and challenging phase.

This phase can be further categorized into:

- Exploitation phase
- Privilege Escalation phase

Exploitation:

During this phase a penetration tester will try to find exploits for the various vulnerabilities found in the previous phase. There are many repositories on the internet that provide proof-of-concept exploits for most of the vulnerabilities.

Some of them are listed below:

- http://www.milw0rm.com/
- http://packetstormsecurity.org/assess/exploits/

It is recommended that the penetration tester has programming knowledge of C (preferably Socket Programming) or scripting languages like Perl, Python or Ruby. It helps in understanding and writing exploits and custom tools / scripts.

This phase can be dangerous if not executed properly. There are chances that running an exploit may bring a production system down. All exploits need to be thoroughly tested in a lab environment prior to actual implementation. Some organizations would require that certain vulnerabilities on critical systems should not be exploited. In such a scenario a penetration tester must give sufficient evidence by means of well documented proof-of-concepts detailing the impact of the vulnerability on the organizations business.

There are good exploitation frameworks available that would aid a penetration tester in developing exploits and executing them in a systematic manner. Few good commercial as well as open-source exploitation frameworks are:

- The Metasploit Project
- Core Security Technology's Impact
- Immunity's CANVAS

It is advised that a penetration tester make full use of the potential of such frameworks, rather than using it for merely running exploits. These frameworks can help reduce a lot of time in writing custom exploits.

Quite often, successful exploitation of a vulnerability might not lead to root (administrative) access. In such a scenario additional steps need to be taken, further analysis is required to access the risk, that particular vulnerability may cause to the target system. This is represented in the feedback loop in Fig. 1 between the Attack and Discovery phase. This loop can be graphically explained as follows:

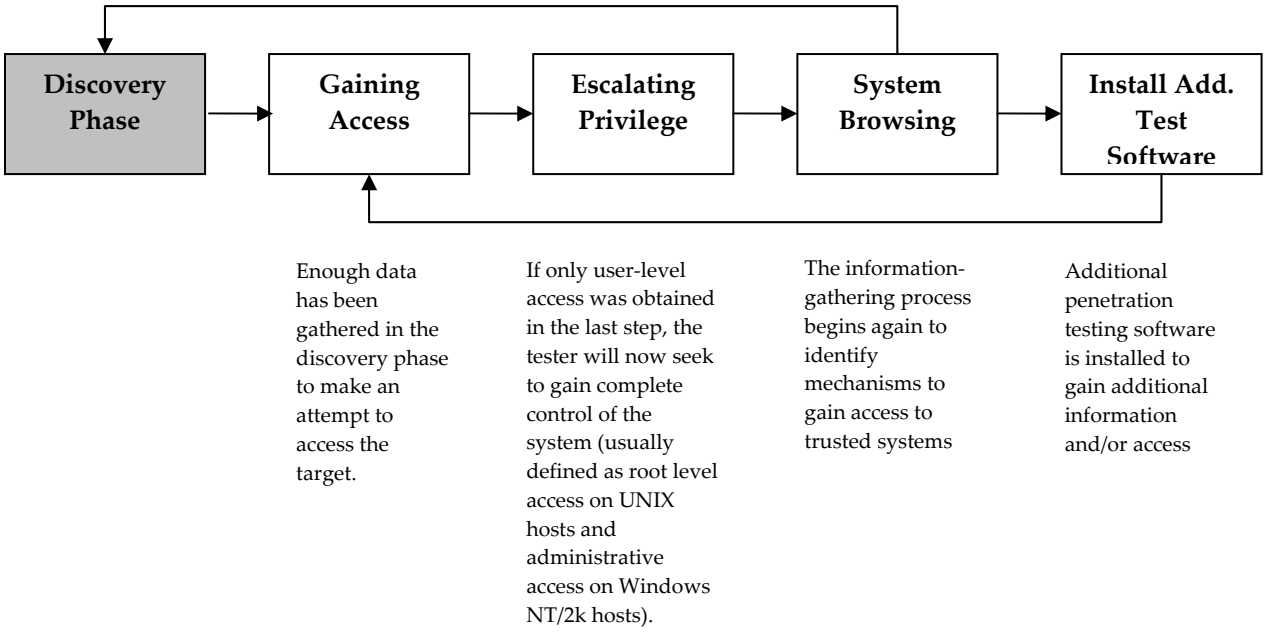

Fig. 2: Attack Phase Steps with Loopback to Discovery Phase [3]

Privilege Escalation:

As mentioned above, there are times when a successful exploit does not lead to root access. For example, for a particular vulnerability, the penetration tester might acquire user level access. An effort has to be made at such point to carry further analysis on the target system to gain more information that could lead to getting administrative privileges, e.g. local vulnerabilities, etc.

As shown in Fig. 2 above, a penetration tester might need to install additional software that might help in getting a higher level of privilege. This process is called privilege escalation.

Penetration testers should also consider pivoting through targeted systems on successful exploitation. Pivoting is a process in which a penetration tester uses the compromised (target) system to attack other systems in the target network. This will also help in explaining better, the business impact of a successful exploit on the organizations security.

But a penetration tester must be careful and get prior permission from the target organization before proceeding further.

A good penetration tester will always keep logs of all the activities performed, as these could help in the reporting stages and also act as the proof of the activities performed.

REPORTING PHASE:

The last stage in the entire activity is the reporting stage. This stage can occur in parallel to the other three stages or at the end of the Attack stage. Many penetration testers do not concentrate on this stage and follow a hurried approach to make all the submissions.

But this stage is probably the most important of all the phases, after all the organization is paying you for this final document. The final report must be prepared keeping in mind both Management as well as Technical aspects, detailing all the findings with proper graphs, figures, etc. so as to convey a proper presentation of the vulnerabilities and it's impact to the business of the target organization. An executive summary, probably a one page document, describing in brief, the activities performed, findings, and high level recommendations should be given. Based on these findings the cost of implementation of the recommendations will eventually be made.

Also detailed technical descriptions of the vulnerabilities and the recommendations to mitigate them should be documented in this report. All the security holes found and exploited must be accompanied with proper Proof-of-Concept by means of screenshots of the successful exploits, or any other such methods.

The report must be precise and to the point. Nothing should be left to the client's imagination. Clear and precise documentation always shows the ability of a successful penetration tester.

For example the necessary things that the report should consist of are:

- Executive Summary
- Detailed Findings
- Risk level of the Vulnerabilities found
- Business Impact
- Recommendations
- Conclusion

CONCLUSION:

In this article we have tried to demonstrate an approach that can be taken to perform a successful penetration test, describing each stage in detail and points that need to be remembered while performing each stage. The whole approach can be summarized graphically as follows:

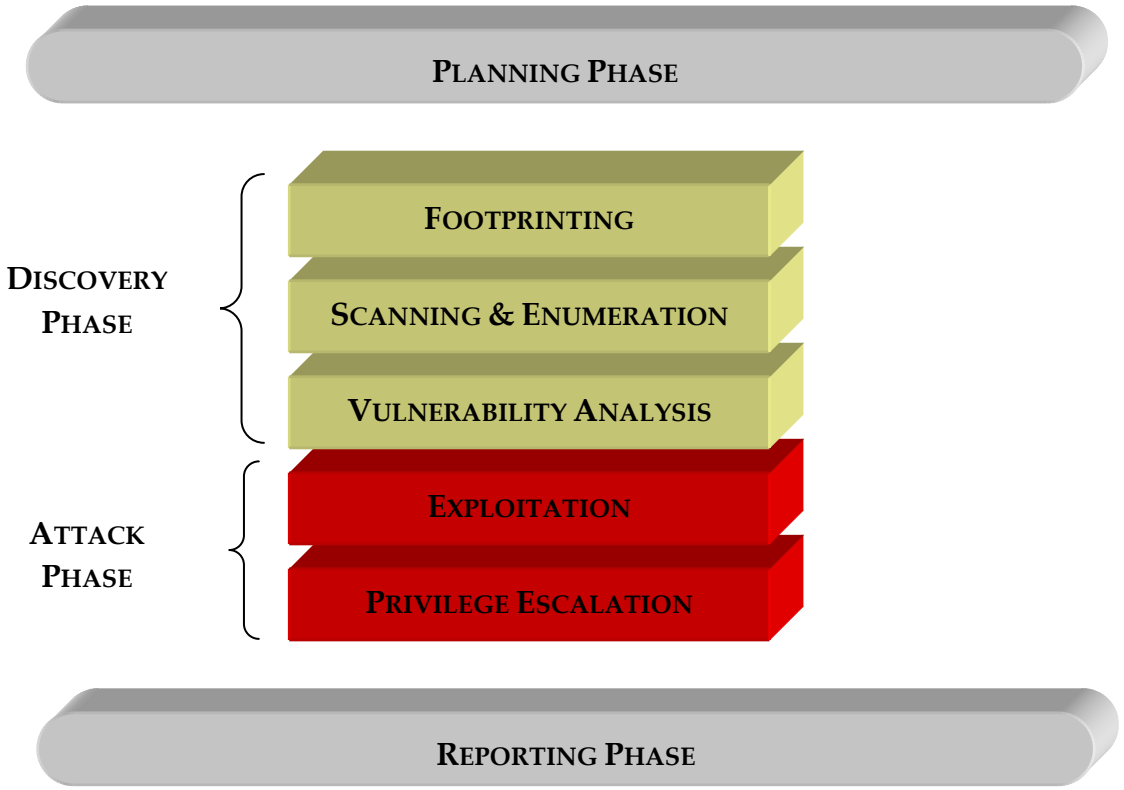

Fig. 3: Penetration Testing Approach

REFERENCES:

[1] http://searchsecurity.techtarget.com/sDefinition/0,290660,sid14_gci929671,00.html
[2, 3] http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf