International Journal of Advances in Software Engineering & Research Methodology– IJSERM
Volume 2: Issue 2 [ISSN : 2374-1619]
Publication Date : 30 October, 2015

A Comparative Overview on Penetration Testing

S M Salim Reza, Wahidul Hasan, S M Saleh Reza, Sajib Chakraborty

***Abstract*— This paper provides a brief impact on penetration testing and the methodology used. The paper also renders an overview of use of IPv6 has on remote penetration testing of servers and web applications. Testing penetration is a very common and familiar method for measuring and assessing the security of a network or information. A penetration tester should follow certain topology so that, one can identify successfully the threats faced by an organization's network or information assets from a hacker and cut-down an organization's IT security costs by taking steps a better return on security investments.**

Keywords— ***Network Penetration Testing, Hacker, Vulnerability, Exploit, IPv6, Security.***

I. Introduction

In modern phenomena of any information systems arena, security is one of the major issues. The growing connectivity of computers through the internet, the increasing extensibility of systems, and the unbridled growth of the size and complexity of systems have made software security a bigger problem now than in the past [1]. Thereto, it is a business imperative to adequately protect an organization's information assets by following a comprehensive and structured approach to provide protection from the risks an organization might face [2]. In an attempt to solve the security problem and comply with the mandated security regulations, security experts have developed various security assurance methods including proof of correctness, layered design, software engineering environments and penetration testing. Penetration testing is a comprehensive method to test the complete, integrated, operational, and trusted computing base that consists of hardware, software and people [1]. The process involves an active analysis of the system for any potential vulnerability, including poor or improper system configuration, hardware and software flaws, and operational weaknesses in the process or technical countermeasures [3]. Penetration testing is different from security functional testing. The latter demonstrates the correct behavior of the system's security controls while penetration testing determines the difficulty for someone to penetrate an organization's security controls against unauthorized access to its information and information systems. It is done by simulating an unauthorized user attacking the system using either automated tools or manual method or a combination of both. This authorized attempt to evaluate the security of a network or an infrastructure by safely attempting to exploit the vulnerabilities helps in finding the loop holes in the network. These loopholes may allow an attacker to intrude and exploit the vulnerabilities. Penetration tests can have serious consequences for the net-work on which they are run. If it is being badly conducted it can cause congestion and systems crashing. In the worst case scenario, it can result in the exactly the thing it is intended to prevent. This is the compromise of the systems by unauthorized intruders. It is therefore vital to have consent from the management of an organization before conducting a penetrations test on its systems or network. [4]

II. Necessity of Network Penetration Test

- IT section is very vast area and its infrastructure is becoming more complex and wider. The internal networks have been given access over the internet to the legitimate users along with the user credentials and the privilege level, of course located outside the firewall.
- Identity of type of resources are exposed to the outer world, determining the security risk involved in it, finding the possible types of attacks and make obstacle to prevent those attacks.

A. *Benefits of Penetration Testing*

1. Proactive determination of the criticality of the vulnerabilities and false positives given by the automated scanners. This helps in prioritizing the remedy action, whether the vulnerability is to be patched immediately or not based on the criticality.
2. Penetration testing helps adherent the audit regulatory standards like PCI DSS, HIPAA and GLBA. This avoids the huge fines for non-compliance.

Depending on the needs, there are two types of penetration testing:

1. External Penetration Test – This test shows what a hacker can see into the network and exploits the vulnerabilities seen over the internet. Here the threat is from an external network from internet. This test is performed over the internet, bypassing the firewall.
2. Internal Penetration Test – This test shows risks from within the network. For example, what threat an internal disgruntled employee can pose to the network. This test is performed by connecting to the internal LAN.

Depending on the knowledge, there are three types of penetration testing, Black box, White box and Gray box. [6]

1. Black Box – This test is carried out with zero knowledge about the network. The tester is required to acquire knowledge using penetration testing tools or social engineering techniques.
2. White Box – This test is called complete know-ledge testing. Testers are given full information about the target network. The information can be the host IP addresses, Domains owned by the company, Applications and their versions, Network diagrams, security defenses like IPS or IDS in the network.

S M Salim Reza
Assistant Professor
Faculty of Science & Technology, Bangladesh University of Professionals (BUP)
Dhaka, Bangladesh

Wahidul Hasan
Department of Electrical & Electronic Engineering, Independent University
Dhaka, Bangladesh

S M Saleh Reza
Faculty, Daffodil International University
Dhaka, Bangladesh

Sajib Chakraborty
Independent University, Bangladesh;
Dhaka, Bangladesh;

3. Gray Box – The tester simulates an inside employee. The tester is given an account on the internal network and standard access to the network.

III. Steps in Penetration Testing Methodology

B. *Preparation for a Network Penetration Test*

To carry out an exhaustive penetration testing and make it a success, there should be a proper goal defined for a penetration tester. A meeting between the penetration tester and the organization which requires a penetration test must be held. The meeting should clearly define the scope and the goal of the test.

B. *Reconnaissance or Information Gathering*

This is a very important step a Pen tester must follow. A Pen tester must gather information from an attacker's perspective.

□ Network Diagrams
□ IP Addresses
□ Domain names
□ Device type

IV. How to Conduct Penetration Testing

It should provide a clear and concise direction on how to secure an organization's information and information systems from real world attacks. One critical factor in the success of penetration testing is its underlying methodology. Generally, penetration testing has three phases: test preparation, test, and test analysis as shown in Figure 1.

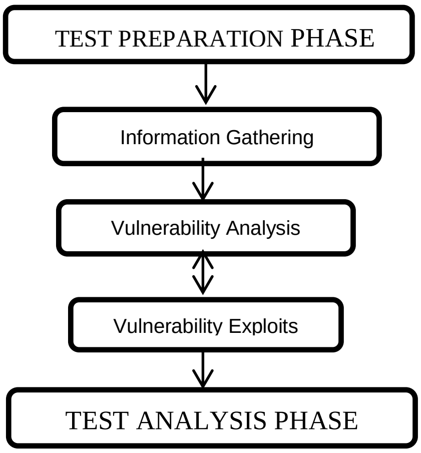

Figure 1. Penetration Testing Methodology

All the necessary documents for the test are organized and finalized during the test preparation phase. The testers and the organization meet to decide the scope, objectives, timing, and duration of the test. Issues such as information leakages and downtime are resolved and put into legal agreement document. Other legal agreements that are deemed necessary are concluded and signed during this phase. The information gathering step requires that the tester scan the physical and logical areas of the test target and identify all pertinent information needed in the vulnerability analysis phase. Depending on the information gathered or provided by the organization, the tester then analyzes the vulnerabilities that exist within the target's network, host and application. The tester may opt to use the manual method to do this step but automated tools also exist to help the tester. [9]. Table 1 lists some of these tools. This phase involves the following steps: information gathering, vulnerability analysis, and vulnerability exploits.

Table1. Penetration Testing Tools

Name of Tools	Specific Purpose	Cost	Portability
Nmap [10]	□network scanning □port scanning □OS detection	Free	Linux, Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac
Hping [11]	□port scanning □remote OS fingerprinting	Free	OpenBSD, Solaris, Mac OS X Linux, FreeBSD, NetBSD
SuperScan [12]	□detect open TCP/UDP ports □ run queries like whois, ping, and hostname lookups	Free	Windows 2000 XP Vista Windows 7
Xprobe2 [13]	□remote active OS fingerprinting	Free	Linux and all updated OS
p0f [14]	□OS fingerprinting □firewall detection	Free	Linux,FreeBSD,NetBSD OpenBSD,MAC OS X,Solaris
Httprint [15]	□ web server fingerprinting □ detect web enabled devices	Free	Linux, Mac OS X, FreeBSD, Win32 (command line and GUI)
Nessus [16]	□detect vulnerabilities that allow remote cracker to control or access sensitive data □detect misconfiguration	Free Non-enterprise Edition	Mac OS X, Linux, FreeBSD, Oracle Solaris, Windows,Apple
Scanner [17]	□detect network vulnerabilities,	Free trial version	Windows but scan servers built on any platform

V. Web Application Penetration Testing

Penetration testing is the systematic probing of a system that could be any combination of applications, hosts, or networks [6]. The general methodology of penetration testing described in Section 4 is a useful process to uncover and resolve security weaknesses of applications, especially web applications.

A. *Impact of IPv6 on the current penetration testing process*

In this section we discuss the components of Pine's current penetration testing process that either need to be changed in order to be applicable to IPv6, or become obsolete and can be removed from the process. We go through the three phases described in the previous section, and discuss the activities that take place. For each of these activities, we analyze its dependencies to see if it relies on features specific to IPv4. We only discuss those items that would need change or can be removed.

B. *Preparation Phase*

In the preparation phase, little activity involving the target systems of the penetration test takes place. Normally the customer will give an exact list of IP addresses that form the scope of the penetration test.

In section V of the paper, an algorithm for host discovery in IPv6 networks is described in general terms. Due to the size of IPv6 subnets, host discovery by simply scanning all the addresses in a given range has become infeasible. In the paper, an algorithm was described that makes use of external sources for address information and assumptions about assignment to perform host detection in IPv6 networks.

The algorithm is depicted in Figure 2. The boxes indicate an action that is performed; the arrows indicate the information flow between the actions. Unless otherwise indicated, the information that travels between boxes consists of IPv6 addresses. The following information is given as input to the algorithm:

1. Given DNS names, IPv4/IPv6 addresses and IPv4 port scan results. When a customer specifies a target for a penetration test, some information (a URL or IPv4 addresses for instance) is given.
2. Prefix information. When the customer has specified a network that is the target of a penetration test, this prefix is fed to the algorithm. In some cases, prefix information can be retrieved from external sources such as WHOIS databases.
3. Wordlists. When generating candidate addresses, a list of possible hex-words (such as babe, cafe, 1337, b00b) is used.

The algorithm shown in the figure performs the following numbered steps:

1. **DNS resolving:** Any DNS names that were given as input are resolved to IPv6 addresses.

2. **DNS info gathering:** From DNS, more addresses can be gathered. By using brute force, or AXFR when available, more addresses from a target domain can be retrieved. When DNSSEC is in use with NSEC, the whole zone can be retrieved as with AXFR. In case NSEC3 is deployed, more effort must be made, but still large parts of the zone can be retrieved. The last technique is PTR traversal.

3. **Web info gathering:** From online search engines and directories, extra information on possible DNS names and addresses is gathered. Search engines may have pages in cache that were served on the target network in the past. Online directories record visible DNS changes and overviews of virtual hosts hosted on different addresses.

4. **Address pool:** The addresses that have been found so far are stored as well as used in the next steps.

5. **Subnet guessing:** From the addresses that are known so far, subnets can be guessed. Ad-dresses in the same network will have an overlap, starting at the MSB. An organization has a network range that it can use (a prefix), and within which it can create different subnets. By comparing the addresses found so far, assumptions about the prefix and subnets can be made. The part of the found addresses that is constant across all addresses and starts at the MSB, is probably the prefix. If multiple addresses have an overlapping part after the prefix, one can assume this is the subnet. The subnets are needed when new candidates for alive detection are generated: guesses will be appended to known subnets.

6. **Vendor-ID extraction:** If SLAAC addresses have been found, the Vendor-ID can be extracted from the last 64 bits, which are in modified EUI-64 format. This format includes the MAC address of the network interface the address belongs to, with the sequence 0xfffe inserted between the OUI and the NIC. The assumption can be made that more hardware from the same vendor is used, so only the NIC identifier of 24 bits needs to be guessed.

7. **Candidate address generation:** This is the heart of the algorithm. From the found prefixes, vendor IDs, and addresses, new addresses can be generated that might be in use. The assumptions on numbering schemes that are mentioned in the paper are transformed into candidate addresses. The following rules can be used:
   - Generate new subnets by numbering around the current subnet numbers;
   - Generate IPv4-address based candidates in each subnet for all known IPv4 addresses of the site;
   - Generate service-based candidates for well-known services and services that have been found in the IPv4 scan if present;
   - For found addresses which have a at least 16 bits of consecutive zeroes in the last 64 bits, generate sequential addresses around them. Random generated addresses have an extremely small chance of containing 16 bits of zeroes, while sequential addresses often do. If the addresses were given out using DHCPv6 or sequentially by hand, this may result in finding surrounding hosts;
   - For found OUIs, generate candidates for the last 24 bits of the ad-dress in the prefixes where SLAAC addresses were found.

8. **Alive detection**
   The candidate addresses that are generated in the

previous step are tested for aliveness. Multiple methods for alive detection are used, since no single method can guarantee detection of an alive host. Combining methods still does not give guarantee, but gives a higher chance of detecting alive hosts.

9. **Service discovery**
   On hosts that were found in the previous step and that were in the ad-dress pool, service discovery is performed. This takes place in the same way as for IPv4, by probing all TCP ports and certain UDP ports.

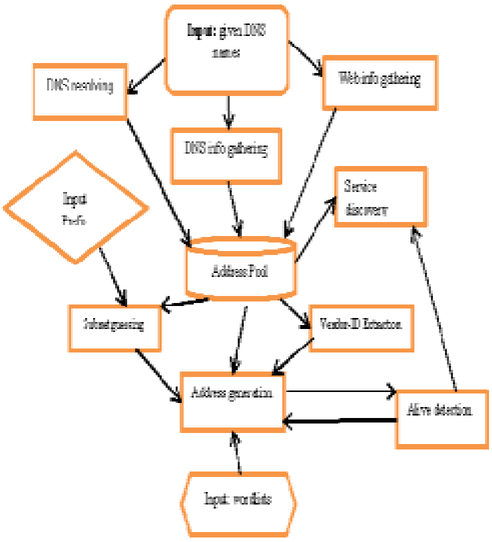

Figure 2: IPv6 host discovery algorithm

VI. Conclusion

To identify the vulnerabilities in a system there should be a penetration testing in a comprehensive method. In this comparative overview, it has been estimated that it offers benefits such as prevention of financial loss; compliance to industry regulators, customers and shareholders; preserving corporate image; proactive elimination of identified risks. The testers can choose from black box, white box, and gray box testing depending on the amount of information available to the user. The testers can also choose from internal and external testing, depending on the specific objectives to be achieved. There are three types of penetration testing: network, application and social engineering. This paper describes different types of methodology consisting of test preparation, test, and test analysis phase.

References

[1] McGraw, G. (2006). *Software Security: Building Security In*, Adison Wesley Professional.

[2] The Canadian Institute of Chartered Accountants Information Technology Advisory Committee, (2003) "Using an Ethical hacking Technique to Assess Information Security Risk", Toronto Canada. http://www.cica.ca/research-and guidance/documents/it-advisory-committee/item12038.pdf, accessed on Jun. 13, 2015.

[3] Mohanty, D. "Demystifying Penetration Testing HackingSpirits, http://www.infosecwriters.com/text_resources/pdf/pen_test2.pdf, accessed on Jun. 13, 2015.

[4] "Penetraion Testing Guide", http://www.penetration-testing.com/

[5] iVolution Security Technologies, "Benefits of Penetration Testing," http://www.ivolutionsecurity.com/pen_testing/benefits.php, accessed on Jun. 13, 2015.

[6] Shewmaker, J. (2008). "Introduction to Penetration Testing," http://www.dts.ca.gov/pdf/news_events/SANS_Institute-Introduction_to_Network_Penetration_Testing.pdf,

[7] "Application Penetration Testing," https://www.trustwave.com/apppentest.php,

[8] Mullins, M. (2005) "Choose the Best Penetration Testing Method for your Company," http://www.techrepublic.com/article/choose-the-best-penetration-testing-method-for-your-company/5755555, accessed on Jun. 13, 2015

[9] Saindane, M. "Penetration Testing – A Systematic Approach," http://www.infosecwriters.com/text_resources/pdf/PenTest_MSaindane.pdf, accessed on Jun. 13, 2015

[10] "Nmap – Free Security Scanner for Network Explorer, http://nmap.org

[11] Sanfilippo, S. "Hping – Active Network Security Tool," http://www.hping.org/

[12] Superscan,http://www.mcafee.com/us/downloads/free-tools/superscan.aspx,.Xprobe2, http://www.net-security.org/software.php?id=231, accessed on Jun. 13, 2015

About Author (s):

S M Salim Reza has been serving as Assistant Professor of the Department of ICT, Faculty of Science and Technology (FST) in Bangladesh University of Professionals, Mirpur Cantonment, Dhaka, Bangladesh

Wahidul Hasan has completed his B.Sc Engg in EEE from Independent University, Bangladesh (IUB) and he is doing his MS in EEE at same institution. Presently, he has been working as Research Assistant (RA) in the Dept. of EEE of Independent University, Bangladesh (IUB), Dhaka, Bangladesh.

S M Saleh Reza is currently teaching at Daffodil International University. He has completed his MBA with a major in Human Resources Management from North South University, Bangladesh. He is also a PhD researcher at Bangladesh University of Professionals.

Sajib Chakraborty received his Bachelor of Science in Electrical and Electronic Engineering from Independent University, Bangladesh. Currently, he is studying Master of Science (Power) in Independent University, Bangladesh. His research interests include hybrid power system, sustainable energy and high voltage engineering.