IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. VI (May-Jun. 2016), PP 74-77
www.iosrjournals.org

A Developed Tool Matrix for Enhancing the Penetration Testing Methodology

Ayman Al-ahwal[1]
[1](*Communication and electronics/ pyramid-institute for Engineering and Technology, Egypt)*

***Abstract**: Penetration testingis the science of insecurity that finds the vulnerabilities in the target of evaluation (ToE).Open Source Security Testing Methodology Manual (OSSTMM)is the standardof pen-testing methodology. It consists of four phases: discovery, enumeration, vulnerability mapping, and exploitation. Itsuffers from no formal, accurate way to do the pen-testing. It depends on the tool selection experience of the pen-testers who take a long time to search for the up-to-date tools that need a virtual environment to test before execution on the real environment to ensure they do not have malicious code and to verify those give the required results. Pen-testing toolsrequirean extra modification or they are not suitable for using in pen-testing phases.This paper proposesa solution to the disadvantages of pen-testing which can be summarized in the question: what are the tested, up-to-date, accurate pen-testing tools that are used in each pen-testing phase? The proposed solution is based on a survey result of more than two thousands pen-testing tools. These tools are classified in a database consists of six columns (tool ID, tool name, tool features, pen-testing phase, tool URL, operating system). It also adds several advantages to the pen-testing process: it provides a database repositoryfor pen-testing tools so that it provides a baseline which helps to know what the tools are required to search or developed? It also eliminates the pen-tester experience in the tools selection and also it reduces the search time for the tools their features, their results in virtual environmentsbefore execution in production.*

***Keywords*:** *Penetration testing, pen-testing, pen-testing phases, OSSTMM, pen-testing baseline, pen-testing tools, pen-testing limitations, pen-testing advantages.*

I. Introduction

The Penetration Testing,*pen-testing ore-assurance*is the science of insecurity that is used for investigating the security of systems through the eyes of attackers without causing system damage [1,2]. Pen-testing appeared outside of the military in 1995 when *Farmer* and *Venema* at Usenetintroduced*SecurityAnalysis Tool for Auditing Networks* (SATAN)which is first Unix-based vulnerability scanner[3]. *SATAN*was able to automatically scan computers to identify system vulnerabilities and to provide advice on how to eliminate them [4].

Pen-testing provides an attempt to prevent malicious attacks from being successful by remedy the vulnerabilities before malicious attackers can exploit them [1]. It improves the security posture of the system by correcting its vulnerabilities and minimizing the damage associated with successful real break-ins [5, 3]. It determinesthe effectiveness or ineffectiveness of the ToE security controls which improves the security controls implementation andtheresponse plan [14].In addition,itenhances the security qualifications of the IT security staff who are often unaware of the dangers presented by the attacks [15].The pen-tester seeks the answers to three basic questions[2]:

1. What can an intruder see (information) on the ToE systems?
2. What can an intruder do with that information?
3. Does anyone at the target notice the intruder's attempts or successes?

The pen-testers follow different pen-testing methodologies. *Open Source Security Testing Methodology Manual* (OSSTMM) is a standard structured methodology to test the ToE.It consists of four phases: discovery, enumeration, vulnerability mapping, and exploitation phase [18].

The *Discovery* phaseis called the *reconnaissance*or *passive information gathering phase*. It is used to gather *passively*as much information as possible about the ToE[5]. By searching through the publicly available news, groups,*Electronic Data Gathering, Analysis and Retrieval* (EDGAR) to get articles written about the vulnerabilities in the software that the ToE system may be running or bydumping the web site offlineto obtain valuable data e.g. the reference links for other web sites, clear passwords, type of authentication…etc.pen-tester can locate the ToE network IP addresses, reverse DNS, Routing Registry Information, authentication details, services patching levels, and names and versions of operating systems of the TOE infrastructure [5].

The *Enumeration* phase is called *active information gathering* phase.The pen-testers *actively* probed using ToE by using mapping,scanning tools and using techniques to identify as many of the network assets as possible, maps local or remote networks and identifies OS of the network machines [10,19].Attempting to

obtain user names and groups, network shares, routing tables, SNMP information running services on servers operating systems,DNS servers,mail servers, web serverssuch as TCP and UDP,detecting open ports using port scanners tools,applications version, system banners, and any other critical information attackers can identify[4,7].

*Vulnerability mapping*phase starts by analyzing and interpreting the information gathered during the previous phases to create a theoretical map of logical and physical topologies of the ToE systems, their potential attacks and their vulnerabilitiesby search publicly available sources of vulnerabilitythen match the identified vulnerabilities on the ToE system with a corresponding exploit [5]. The pen-testers start to do a pen-testing plan to organize the available vulnerabilities and their related exploits. It includes a high level overview of the test cases, how exploratory testing will be conducted, which components will be tested. It gives a timetable of activities, along with a list and description of deliverables, and outlines the tools needed to conduct the tests, as well as any opportunities for automated testing and which tools and techniques this testing requires.

Exploitation phase is also called *activeintrusionattempts*. It begins once the target system's vulnerabilities are mapped.It attempts to exploit the vulnerabilities on the ToEto gain privileged access to the system.There are several web sites that provide the exploitation resources that are reported daily with new exploits such as: (www.packetstormsecurity.com, www.scurityfocus.com, ftp.technotronic.com, www.cert.org).

The value of a pen-testing is in the report and briefings at the end which should be clear and easy to understood.The key elements to ensure that pen-testing gives useful results it should cover the full range of threat spectrum with using up-to-date pen-testing tools [8] to gain maximum results with minimal disruption to normal operations of the system. All the results should be recorded in a report and signed by pen-testers and the ToE responsible [4].The pen-tester should organize the available data and document of all processes to allow the pen-testing to be traced.

The pen-testing OSSTMM methodology suffers from the absenceof formal, accurate way to do the pen-testingindependentof the experience of the pen-testers [8, 13, 18], it has no security goals are defined before doing the pen-testing, and the pen-testing is a complicated process that is hard to be realized and it should cover the entire spectrum range of ToE vulnerabilities [6], so that it is a collective effort and no individual pen-tester can solve all the security problems in the system [13] alone, also the scope of pen-testing performed varies depending on the needs of the different organizations [10].In addition to there is no way to guarantee that a successful attack will not occurin the future, but pen-testing reduces substantially its probability [9]because the pen-testing process reflects the situation at a particular point in time, snapshot, while the vulnerabilities discovered daily in the systems [4].It requires determining the security testing baseline to protect the ToE against attacks.

This paper focuses on solving the limitations of pen-testing tools which are:

- The tool selection process depends on the experience of the pen-tester [7] due topen-testingmethodologies using different pen-testing tools [5, 6].
- It takes a long time to search on the Internet for the up-to-date tools then test them in virtual environment before using them in real environment [8]to be sure that there is no malicious code before executing them in the real environments.
- The pen-testing tools are different and have huge number, so that the pen-tester takes a long time to search and select the optimal tool with the suitable tool features.
- There is no way to prioritize the pen-testing process to get the maxim value of doing the pen-testing.

This research answers the following question: What are the pen-testing tools that are used in each OSSTMM pen-testing phase? The proposed solution is based on a developed pen-testing tool matrix. This matrix is a database consists of six columns: tool ID, pen-testing phase, tool name, tool feature, URL to download the tool, and the suitable operating system for running the tool. The paper has the following structure: section II the proposed pen-testing tool-matrix, section IIIresults and analysis, section IV conclusions and section V future work.

II. The Proposed Pen-testing tool matrix

The development and the selection of the pen-testing tools is one of the challenges of pen-testing process,which is different from pen-tester to another [7] because they depends on the experience of the pen-testers who are using different pen-testing tools and methodologies[5, 6].

The proposed pen-testing tool matrix is suggested as the result of survey for more than three hundreds tools.The pen-testing tools are downloaded and installed on a virtual machine then tested briefly to get the experience needed to understand their usageand evaluated based on the Internet provided material. New updates are available to the tools; that needs to be tested also before the execution on the real environment to gain maximum results with minimal disruption to normal operations.In addition, the results obtained from the

execution of one tool are often used as the basis for additional analysis and possibly as input for the execution of other tools. With the time the tools become more than three hundreds tools without classification.

These tools are regular updated with new features, also some of them are disappeared, theirInternet URL is changed, or they becamecommercial tools. Also it is difficult to know the suitable pen-testing tools between them and which are suitable for which pen-testing phase.

To know the suitable tool for each phase of OSSTMM pen-testing (discovery, enumeration, vulnerability mapping, and exploitation) a database table is developed with the following attributes:

1. *Tool ID*: is a unique sequential number used as tool index to identify the tool in the table.
2. *Pen-testing phase*: contains one of the OSSTMM phases (discovery, enumeration, vulnerability mapping, and exploitation).
3. *Tool Name*: represents the tool name. The tool matrix should be up-to-dated tools from the hacking books, hacking Web sites, mailing lists, or published papers…etc.
4. *Tool Feature*: includes the description of the tools and their basic characteristics. This field should be also up-to-date because the tools are always change with time to have new features and also for vulnerability scanning tools there are a daily new lists of vulnerabilities are discovered. The tool should be updated with new vulnerabilities scanners that are very useful in the results.
5. *Tool URL*: URL to download and to update the tool from the Internet. The tool version is always needs to be up-to-dated, the tool manual can be downloaded from the Internet.
6. *Operating System*: to known the pen-testing tool victim operating system, and from which operating system the tool is running from Windows, Linux, UNIX…etc.

A sample of the developed pen-testing tool matrix is as follows in table (1):

Tool ID	Pen-Testing Phase	Tool Name	Tool Feature	Tool URL	Operating System
1	discovery	ARIN	• American Register for Internet Numbers. • Get the DNS for North America, parts of the Caribbean, and subequatorial Africa.	www.arin.net	Windows UNIX
2		RIPE	• Résolutions IP Européens Network Coordination Centre (RIPE) for Europe.	www.ripe.net	Online Web Site
3	vulnerability mapping	Nmap	• An abbreviation of 'Network Mapper'. • Open source hacker's tool. • Network discovery, network inventory, open ports, managing service upgrade schedules, monitoring host or service uptime and security auditing. • Uses raw IP packets in creative ways to determine what hosts are available on the network, what services those hosts are offering, what operating systems and what type and version of packet filters/ firewalls are being used.	https://nmap.org	Linux, Microsoft Windows, OpenBSD, Solaris, Mac OS X, HP-UX, NetBSD, Sun OS.
4	exploitation	Metasploit	• An exploitation framework. • Provides several tools, utilities, and scripts to execute and/or develop exploits against ToE remote machines. • Used to cover the phases of Penetration. • Includes a large number of exploits for several different applications, protocols, and operating systems.	http://www.metasploit.com/	Linux, Microsoft Windows

Table (1): *Sample of the proposed tool matrix*

The tool matrix is designed to collect the pen-testing tools, to check the toolsupdates which change very fast in features and the tools version. The pen-testers always update the tool matrix with the tested pen-testing tools in virtual environments before executed them in the real environments. So that when the pen-test starts it is easy to search about the optimal tool for each phase of the pen-testing phases.

III. Results and Analysis

This paper focuses on how to do a pen-testing with a systematic way independent on experience of pen-testers in the selection of the pen-testing tool. In other words it answers the question: what are the pen-testing tools that are used in each phase of the OSSTMM pen-testing methodology?By sorting the pen-testing tools in a database according the pen-testing phases provides several advantages as follows:

- Provides a *Repository* of pen-testing tools.
- Reduces the time required to research about pen-testing tools because the tools are sorted and classified according to the pen-testing phases.
- Reduces the need for experience of pen-tester for the tool selection.
- Enables the execution of the pen-testing tools in the virtual environment before executing them in real time applications.

- Provides a baseline for pen-testing tools that are required to allow the pen-tester to look at ToE through the eyes of a potential intruder in each phase of pen-testing.
- If a tool is not present should be requested to be developed for appropriate cases.

On the other hand after adding the proposed pen-testing tool matrix to the pen-testing it still suffers from several disadvantages as follows:

- It has no prioritization for the pen-testing process in consideration to get the maxim value of testing ToE.
- It has no prioritization for the countermeasures implementation process based on the risk assessment techniques.
- It has no quantitatively estimation about the risk and its potential impact on the ToE.
- No relation between the pen-testing goals and the prioritization process of doing the pen-testing process.
- It provides available tools to the public, which increases the hacking process that introduces the risk that someone will use for malicious purposes.

IV. Conclusion

The proposed methodology adds several advantages to the pen-testing process: it provides tools storage which are sorted and classified according to the pen-testing phases. It provides a way to modify tools for the absent features in the database. In addition it reduces the time required to test the tool in virtual environment while the pen-testing takes place and it also provides a baseline for pen- testing tools which are classified according to the pen-testing phases. In addition toit eliminates the pen-tester experience dependence in the selection of the process and there is no way to guarantee that a successful attack will not occur in the future. In the other side there is no way to prioritize the pen-testing process.

V. The Future work

The pen-testing suffers from there is no priority to do the pen-testing process according predefined goals. The future plan will be extending the research to answer the questions: Is the attack modeling techniques helping in doing the pen-testing prioritization process of the TOE? How to link between the pen-testing goals and pen-testing prioritization process? In addition to How to prioritize the countermeasures based on the pen-testing? Then how to determine the potential impact of risk on the ToEbased on analyzing the threats, and vulnerabilities of the TOE? And how to prioritize the implementation process of countermeasures based on the risk assessment techniques?

References

[1] Herbert H. Thompson, “Software Security Assurance,” Security innovation (SI), Inc. The application Security Company, www. securityinnovation.com, November 2006.

[2] A. Vorobiev and J. Han, "Specifying Dynamic Security Properties of Web Service Based Systems," SKG2006, Guilin, China, 2006.

[3] Stuart McClure, Joel Scambray, and George Kurtz, “Hacking Exposed: Network Security Secrets and Solutions,” Osborne/McGraw-Hill, Fifth Edition, USA, 2006.

[4] John Chirillo, “Hack Attacks Revealed,” Wiley computer publishing, USA, 2001.

[5] Helen J. Wang, Chuanxiong Guo, Daniel R. Simon, and Alf Zugenmaier, " Shield: Vulnerability Driven Network Filters for Preventing Known Vulnerability Exploits," Microsoft Research, SIGCOMM’04, ACM conference, USA, 2004.

[6] Daniel Geer and John Hartshorne, "Penetration Testing: A Duet," Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC.02), IEEE, 2002.

[7] Federal office of information security (BSI), “Study: a Penetration Testing Model,” USA, http://www.bsi.bund.de, 2005.

[8] Steven Splaine, “Testing Web Security-Assessing the Security of Web Sites and Applications,” Wiley Publishing, Inc., USA, 2002.

[9] Avishai Wool, "Why Security Standards Sometimes Fail," Vol. 45, communications of the ACM journal, USA, December 2002.

[10] Giovanni Vigna, Fredrik Valeur, Jingyu Zhou, and Richard A. Kemmerer, "Compostable Tools for Network Discovery and Security Analysis," Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC.05), IEEE, USA, 2005.

[11] John Steven, and Gunnar Peterson "Security Testing of Internal Tools," IEE Security & Privacy conference, IEEE Computer Society, 2007.

[12] A. El Ahwal, S. El Kassas, M. E. Allam, and H. Abdel Kader, "Methodology and Limitations of Penetration Testing", Ain Shams University Academic Magazine, 2008.

[13] Internet Security Systems, Inc., “Network Intrusion and Penetration Techniques,” USA, August 2006.

[14] Richard Bejtlich, “The Tao of Network Security Monitoring Beyond Intrusion Detection,” Addison Wesley, USA, July 2004.

[15] Information Technology Advisory Committee Staff, ”Using an Ethical Hacking Technique to Assess Information Security Risk," The Canadian Institute of Chartered Accountants (CCTI), Canada, http://www. Icca.ca/ccti, 2003.

[16] Filippo Ricca, Paolo Tonella, "Analysis and testing of web applications," Proceedings of the 23rd international conference on Software engineering, IEEE Computer Society, 2001.

[17] Bazaz, A., Arthur, J.D. and J.G. Tront, “Modeling Security Vulnerabilities: A Constraints and Assumptions Perspective,” The 2nd IEEE International Symposium on Dependable, Autonomic and Secure Computing, Indianapolis, USA, October 2006.

[18] Gunter Ollmann, “Passive Information Gathering, the Analysis of Leaked Network Security Information,” NGS Insight Security Research (NISR) Publication, USA, 2004.

[19] Johnny Long and others, "Penetration Tester's open source toolkit", Syngress Pub., 2008.