Automated Penetration Testing : An Overview

Conference Paper · April 2018

DOI: 10.5121/csit.2018.80610

CITATIONS
13

READS
11,931

2 authors:

Farah Abu-Dabaseh
Princess Sumaya University for Technology
2 PUBLICATIONS **22** CITATIONS
SEE PROFILE

Esraa Alshammari
Princess Sumaya University for Technology
6 PUBLICATIONS **46** CITATIONS
SEE PROFILE

AUTOMATED PENETRATION TESTING: AN OVERVIEW

Farah Abu-Dabaseh and Esraa Alshammari

Department of Computer Science
Princess Sumaya University for Technology, Amman, Jordan

ABSTRACT

The using of information technology resources is rapidly increasing in organizations, businesses, and even governments, that led to arise various attacks, and vulnerabilities in the field. All resources make it a must to do frequently a penetration test (PT) for the environment and see what can the attacker gain and what is the current environment's vulnerabilities. This paper reviews some of the automated penetration testing techniques and presents its enhancement over the traditional manual approaches. To the best of our knowledge, it is the first research that takes into consideration the concept of penetration testing and the standards in the area.This research tackles the comparison between the manual and automated penetration testing, the main tools used in penetration testing. Additionally, compares between some methodologies used to build an automated penetration testing platform.

KEYWORDS

Penetration test, Automation, Exploitation, Ethical hacker, Penetration testing standards.

1. INTRODUCTION

Penetration testing is used to check the exploitations and the vulnerability of the organization's system and help the developers to build a protected system that meets the needs. It's very important to any organization and company to protect their data and information from outside attackers and keep monitoring to the prioritize the severity of the security issues. Determining the priorities can help the developers to determine the needed devices in the allocation of the budget for security issues. Additionally, can be used to find the financial loss expected and risks if the attackers achieve their goals and exploited the system and how to mitigate that. The data generated from the test considered confidential and private data because it shows approximately all the holes in the system and how they could be exploited. [1]

PT can be done by attacking the system similar to the action of the outside attackers and find out what can be obtained [2]. The attack might not be as easy as exploiting one vulnerability, many vulnerabilities may be used to achieve the goal by making a sequence of attack chain (Multi-step attack) [3]. It's also considered as a risk assessment and can be used to check the network safety. When penetration test is done, the roles of engagement for that test should be set also, to set the goals and the methodology of the test.

Dhinaharan Nagamalai et al. (Eds) : NATL, CSEA, DMDBS, Fuzzy, ITCON, NSEC, COMIT - 2018
pp. 121–129, 2018. © CS & IT-CSCP 2018 DOI : 10.5121/csit.2018.80610

Penetration tests companies can be classified into three different types: gray hat, black hat, and white hat. In the white hat, the tester is an ethical hacker that respects the rules of the organization and the employees can help to perform the testing. While the black hat is mainly used to find how the employees interact with the undesired attack, in this approach the administrators are only the ones who know the test is underway. Moreover, we can do a Gray hat which is a combined approach to the previous types into a custom test plan [4].

Penetration testing should be considered as a standard frequent process within the security roadmap. Traditionally, the organizations used to perform the penetration testing only when they have a product release or a major upgrade. [5]

However, it's suitable to perform the test in these situations:

- New installed software
- Applied system upgrades
- User policy modification
- Applied Security patches
- New infrastructure is added

Although it's important to have a penetration testing in the organization, it's hard to implement too. Since it should include a security expert with the capability to do such a complex job. That could be an overhead on the organization and could waste time and money without the desired result in the case that the security team wasn't as professional as they must. So, the automated approach has seen the light; done by an expert security team in the field.

The contribution of this research will consider the standards of penetration testing, the tools used for each phase in the penetration test, the comparison between the automated and manual approaches and the comparison between some of the current approaches for the automated penetration test.

The rest of this research is as follows: in section two the Penetration testing standards will presents. While the comparison between manual and automated techniques in penetration testing are provided in section three. Section four shows an overview of the current automated penetration testing. Finally, the conclusion and future works are presented in section five.

2. PENTRATON TESTING STANDARDS

Standards for penetration testing aimed to provide a basic outline and definition of the penetration testing. Also to give an outline of the steps used for it, many standards are out there having various pros and cons [6]. Choosing one of them should be based on the goal of having the test.

There are currently various standards that could be followed, such as ISAAF (Information Systems Security Assessment Framework), the OSSTMM (Open-Source Security Testing Methodology Manual), the NIST SP 800-115, and the PTES (the Penetration Testing Execution Standard), the OISSG (Open Information Systems Security Group) [6].

OSSTMM v3 covers the whole parts of the penetration test and have three classes of attacks: Communications Security, Spectrum Security and Physical Security. This standard was published in 2010 and is very mature since the first version which was released in 2000.[6]

On the other hand NIST (SP800-115) standard provides guidelines for planning and conducting information security testing and assessments. Additionally, to analyze the findings and developing mitigation strategies. It's not purposed to give an overall testing or assessment program but to give an overview of the key elements in both security testing and assessment with assurance on specific techniques showing their benefits and limitations. in addition to that, it also gives recommendations and reports for their use.

On the other hand NIST (SP800-115) standard provides guidelines for planning and conducting information security testing and assessments. Additionally, to analyze the findings and developing mitigation strategies. It's not purposed to give an overall testing or assessment program but to give an overview of the key elements in both security testing and assessment with assurance on specific techniques showing their benefits and limitations. in addition to that, it also gives recommendations and reports for their use.

As (SP800-115) NIST standard, the penetration testing process can be divided into the following four processes shown in (Figure.1) [7]:

Figure.1: The Phases of Penetration Testing (NIST) Standard

The third standard in penetration testing is ISSAF methodology which aimed to help the administrator to evaluate your application, system and network controls. It consists of three phases and nine steps [8]. As shown in Figure 2:

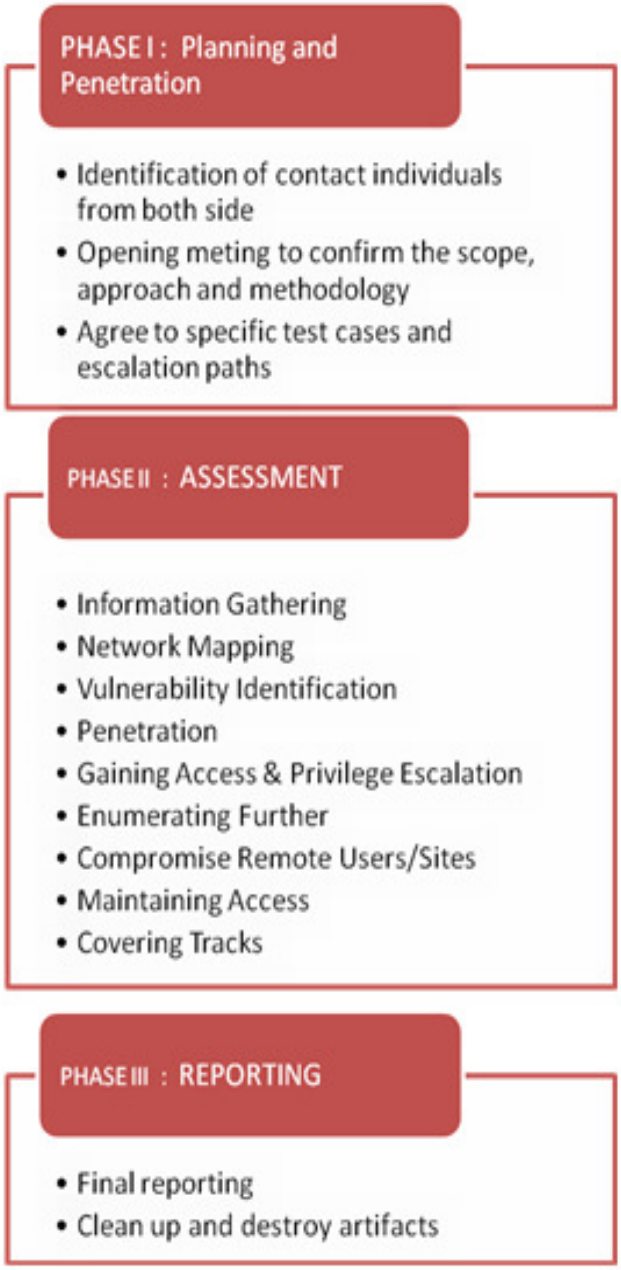

Figure 2: The Phases of Penetration Testing (ISSAF) Standard

The final standard to be considered is the PTES, the Penetration Testing Execution Standard is a completely new standard that started to be developed in 2010. One of its main features is that the industry experts in specific areas have developed it [9]. the steps covered in the PTES are shown in (Figure.3) [6].

Figure 3: Steps of Penetration Testing Execution Standard

3. MANUAL VS. AUTOMATED PENETRATION TESTING

Until recently, Penetration testing has been restricted to advanced security specialist that having many years of relevant experience to do the complex manual process. but in fact, the proficient penetration testers are not highly available and the manual process is time and money consuming. A team of experts can gather to build a professional automated tool that can be a combination of experience of the expert penetration testers. so that the non-expert users can substitute the penetration team with the automated tools to get an inclusive view of the security situation on the organization's system.

The table below, summaries the comparison between manual and automated penetration testing:

Table 1: Comparison of manual and automated testing[1] [10]

	Automated	Manual
Testing process	Fast, standard process; Easily repeatable tests;	Manual, non-standard process; capital intensive; High cost of customization;
Vulnerability /attack Database management	Attack database is maintained and updated attack codes are written for a variety of platforms;	Maintenance of database is manual; Need o rely on public database; Need re-write attack code for functioning across different platforms;

Exploit Development and Management	Product vendor develops and maintains all exploits. Exploits are continually updated for maximum effectiveness. Exploits are professionally developed, thoroughly tested, and safe to run. Exploits are written and optimized for a variety of platforms and attack vectors	Developing and maintaining an exploit database is time-consuming and requires significant expertise. Public exploits are suspect and can be unsafe to run. Re-writing and porting code is necessary for cross platform functionality.
Reporting	Reports are automated and customized	Requires collecting the data manually
Cleanup	Automated testing products offer clean-u solutions	The tester has to manually undo the changes to the system every time vulnerabilities found
Network modification	System remain unchanged.	Often results in numerous system modification
Logging/ Auditing	Automatically records a detailed record of all activity.	Slow, cumbersome, often inaccurate process
Training	Training for automated tools is easier than manual testing	Testers need to learn non-standard ways of testing ; training can be customized and is time consuming

4. CURRENT AUTOMATED PENETRATON TESTING OVERVIEW

Recently, penetration testing has been used to find the vulnerabilities exists in the system to know how to mitigate them. the test usually simulates various types of attacks on the target system. by this test, the administrator will have an organized and controlled way to identify the security shortcomings. The resources and time needed for comprehensive testing will make penetration testing price intensive. Consequently, such tests are sometimes solely performed throughout necessary milestones. during [5] project have been automated the penetration testing method for many protocol-based attacks. their automated penetration testing, application covers many attacks which support hypertext transfer protocol (HTTP), SIP and TCP/IP. the target of this work is to supply a quick, reliable and automated testing tool, that is additionally easier to use than existing tools.

In research [6], The purpose behind this research was to contribute a tool to the community that may be won't to improve the potency of current penetration testing companies, so that they will expand coverage of the testing to grant customers a additional in depth read of their current security ways and wherever they have to enhance. the most purpose behind this tool is to prove that automated testing isn't a hindrance to the security community however is very a tool that should be leveraged throughout testing.

In the other hand project [11] was developed to facilitate the vulnerability analysis and penetration testing in Indian banks. It's a big threat to the bank to do the penetration testing an vulnerability assessment using third party tools. this approach is fully automated and interactive so that it doesn't require a high experience and technical sills from the users. the tool has been developed using python libraries and without any third party software's, it's a reliable option to find the vulnerabilities associated to the applications and services running on the target system. After that, the tool produces a vulnerability list with the severity level associated to each vulnerability. it also used to detect the SQLI vulnerability on the target system.

In [3], the known mathematical model of partially observable Markov decision processes (POMDP) have been used to tackle the problem of the research. the solution proposed automatically produce generation of multi-step plans for a penetration test, the plans are robust to uncertainty during execution. this work focuses on remote test with uncertainty in both information gathering and exploit actions, by developing probabilistic metrics to find the effective probability that an exploit can be executed and the overall probability that the attacker can successfully execute it a summary for the comparison between these approaches can be found in table 2. Paper [5] will be considered as A , paper [6] will be considered as B while paper [11] will be C and paper [3] will be D.

Table 2: Comparison between current methodologies of automated penetration testing

	Target	Tools	Phases	Method of implementation	Aim
A	HTTP / TCP/IP and session initiation protocol (SIP) attacks	Hping3 to perform TCP DOS attack	Input parameters based on the web interface then routing the params to appropriate module then finally implement the attack	The application was developed using PHP and the attack scripts is implemented using JAVA and shell scripting , the design implemented on Linux	Perform automated easy to use with web interface, penetration testing toolkit
B	All protocols and services	Harvester, Metagoofil, NMAP, ZAP, Metasploit, Nessus (pynessus)	Insert arguments , run scanning tools then parse the output from these tools and finally exploit with Metasploit and start the manual process if needed	Uses script to link the tools to each other's and to parse the output from them.	Optimizing the process by automating the running of any tool that is used commonly on the penetration test
C	Database	No third party tools has been used here	Information gathering, scanning, then	Developed using core python packages/Libraries and	Find user credentials , Email ID and

			vulnerability detection and mapping and in the final step Exploitation and report generation is done	no third party software has been used	other details from the database using SQLI
D	All services and protocols	Exploiting tools	Information gathering then vulnerability assessment and the final step is penetration test planning	Used partially observable marker decision process (POMDPs) and demonstrate the use of an effective approximation algorithm that satisfies the performance requirement of penetration testing planning , then a script is used to link the components	Find a way to do remote penetration testing with uncertainty of tools used.

5. CONCLUSION AND FUTURE WORK

Many organizations need penetration testing to discover the most vulnerabilities that have in their system. To apply the penetration test, there are two approaches that the organizations used to discover the bugs, one is automated penetration test and the other is manual penetration test. The automated pen test is the easiest way to figure out the whole vulnerabilities in the system by implementing a tool that has some patterns to find the vulnerabilities. While the manual test is the way to discover the vulnerabilities manually through analyzing the system and distinguish the abnormal behavior.

Hence, this paper has been done to shows the importance of the penetration testing as well as the importance of automating this process. Additionally, some standards in the penetration testing have been highlighted to help the researchers find the suitable standards to use. Even more, the comparison between the manual and automated penetration testing has been provided in term of the testing process, vulnerability and attack database management, exploit development and management reporting, clean up, network modification, logging, and training. And the result shows that the automated penetration testing is better than the manual penetration in all of the above process, except finding the new or zero day exploits. So that many organizations may go for the automated approach because it seems the better and cheaper way to maintain security in the systems as most of the vulnerabilities that the attackers used to exploit the system are well defined in the automated tools.

Although writing own exploits may be time-consuming as well as ineffective in terms of money. But, the attackers can conceal their activity through their own scripts. Thus, the automated tools still have limitations and vulnerabilities.

To the best of our knowledge, this research is a step forward to the other researchers who interested in the automated penetration testing. The next step is to study the impact of the penetration testing toward the hunting threats. Even more, to study the applicability of building automated tool that takes into consideration the general limitations in the current automated tools.

REFERENCES

[1] Y. Stefinko, A. Piskozub and R. Banakh, "Manual and automated penetration testing. Benefits and drawbacks. Modern tendency," 2016 13th International Conference on Modern Problems of Radio Engineering, Telecommunications and Computer Science (TCSET), Lviv, 2016, pp. 488-491. doi: 10.1109/TCSET.2016.7452095

[2] Xue Qiu, Shuguang Wang, Qiong Jia, Chunhe Xia and Qingxin Xia, "An automated method of penetration testing," 2014 IEEE Computers, Communications and IT Applications Conference, Beijing, 2014, pp. 211-216.
doi: 10.1109/ComComAp.2014.7017198

[3] L. Greenwald and R. Shanley, "Automated planning for remote penetration testing," MILCOM 2009 - 2009 IEEE Military Communications Conference, Boston, MA, 2009, pp. 1-7.
doi: 10.1109/MILCOM.2009.5379852

[4] Gula, Ron. “Broadening the Scope of Penetration Testing Techniques.” Jul. 1999. URL: www.forum-intrusion.com/archive/ENTRASYS.pdf (6/14/12)

[5] Samant, Neha. Automated penetration testing. Diss. San Jose State University, 2011.

[6] K. P. Haubris and J. J. Pauli, "Improving the Efficiency and Effectiveness of Penetration Test Automation," 2013 10th International Conference on Information Technology: New Generations, Las Vegas, NV, 2013, pp. 387-391.doi: 10.1109/ITNG.2013.135

[7] Souppaya, Karen Scarfone Murugiah, Amanda Cody, and Angela Orebaugh. "Technical Guide to Information Security Testing and Assessment." Recommendations of the National Institute of Standards and Technology (2008).

[8] "Open Information Systems Security Group", Information systems security assessment framework, 2006.

[9] Pentest-standard.org. (2018). The Penetration Testing Execution Standard. [online] Available at: http://www.pentest-standard.org/index.php/Main_Page [Accessed 31 Mar. 2018].

[10] Mirjalili, Mahin, Alireza Nowroozi, and Mitra Alidoosti. "A survey on web penetration test." International Journal in Advances in Computer Science 3.6 (2014).

[11] Shah, Sugandh, and B. M. Mehtre. "An automated approach to Vulnerability Assessment and Penetration Testing using Net-Nirikshak 1.0." Advanced Communication Control and Computing Technologies (ICACCCT), 2014 International Conference on. IEEE, 2014.