RESEARCH ARTICLE OPEN ACCESS

Effectiveness of Penetration Testing Tools, Cyber Security

Prof. Alex Roney Mathew
Department of Cyber Security, Bethany College
USA

ABSTRACT

Penetrative testing is one of the oldest network security methods used in evaluating the networks systems security. The defense department has been using it since the 1970s in determining the security weaknesses in computer systems and in the initiation of development programs in coming up with security systems. The organization can use penetration testing in fixing security weaknesses before its security is compromised. Penetrative testing has been beneficial since it provides proper information services and security to the networks systems of an organization. With the help of penetration testing tools, the organization is in a position to reduce its network risks. The penetrative testing main objective is to evaluate the organization's system network security weaknesses. Penetration testing also helps in identifying security incidences and testing employee's security awareness. Consulting several penetration test tool helps in testing the systems security arrangement and identifying improvements. If done and appropriately reported, the penetration test provides knowledge of all security weaknesses and d the support and information required in removing or reducing the vulnerability.

Keywords* :- *penetrative testing, network security, system security.

I. INTRODUCTION

The risk of security for organizations, companies, and entities that deal with highly sensitive data is prevalent. In most cases, the companies are not aware of the large and complex communication structure and have little or no control over them. Additionally, the risks become higher after considering software running on their infrastructure. The uncontrolled risks may increase the frequency of security attacks that may lead to significant financial losses.

Usually, the security guarantee can achieve through various protection mechanism that includes prevention, response, and detection. Prevention involves stopping the intruders from accessing the systems resources; detection happens when the intruder has had already accessed the systems while the response is the after effect process which response to failure that occurred during the initial two steps. Its principle of operation is trying to prevent loss or future damages to the system (Stewart 76).

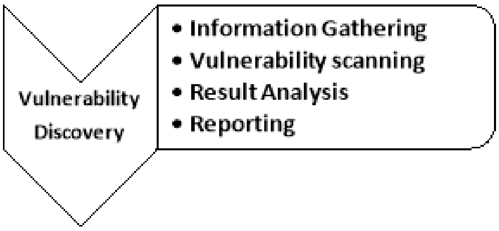
Assessing the state of security is a necessary and continuous task to help in understanding the real risks. The assessment is done using security tests; therefore, choosing the right method security testing is an essential task in minimizing the existing security risks within any corporation. Penetrative testing is one of the most common methods of assessing systems security risk (Weber et al. 37).

Penetrative testing or ethical hacking is the practice undertaken by professional hackers to identify vulnerabilities in a system before hackers attack it. It needs some bit of luck, patience, and smart thinking. Most of the professional hackers require a few particular tools to help them in getting the job done. Some of the assessment tools are freeware, while others need one to pay for a license.

Vulnerability assessment process

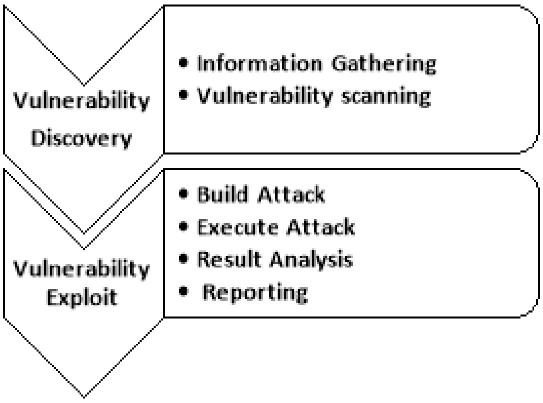
Vulnerability is a flaw in the system. The various reasons for its existence are a coding, weak password, misconfiguration or weak password, etc. attackers strive to identify vulnerability before exploiting it, this process is a systematic and proactive strategy for discovering the vulnerability. It helps in determining unknown issues within the system. It is also a requirement by industrial standards such as DSS PCI for compliance reasons. The scanner helps in conducting a vulnerability assessment. It's a hybrid process that combines expert analysis with testing.

Figure 1: vulnerability assessment process



Penetration testing process involves accessing the system security through an attack simulation. It is a systematic and proactive security assessment process. It's a two-step process.

Figure 2: Penetration testing process



II. PENETRATIVE TESTING TOOLS

Here are 7 of the best penetrative testing tools that may help in performing penetrative actions. While some are free and others require one to pay for licenses, all of these are good for use

1. **Metasploit** is a very popular collection of different penetration tools. Expects and cybersecurity professionals have applied it for many years to achieve different objectives such as managing security evaluations, discovering vulnerabilities, and coming up with defense methodologies. Metasploit tools are applicable on servers' networks, online-based applications once a new exploit or security vulnerabilities are detected, and the utility is in a position to identify it. Metasploit is very useful in ensuring the security of infrastructures in older vulnerabilities (Wrycza 45).

2. **Nmap** is known as network mapper. It's an open source and free tool used in scanning networks or systems for vulnerabilities. The tool helps in carrying out other activities such as monitoring service or host uptime and network attack surface mapping. It runs on every major operating system and is best suited for scanning small and large networks. With Nmap utility, the ethical hacker can understand the different characteristics of the target network such as type of the operating systems, types of firewall or packet filters available, and available hosts.

3. **Wireshark** tools help in understanding the minutest detail of the activities occurring in a network. It's an actual network sniffer, network analyzer, or network protocol analyzer that allows in assessing vulnerabilities for network traffic in real time. Wireshark is used widely in scrutinizing traffic network details at different levels from the pieces constituting data packet to the connection level. Capturing of data packets allows one to investigate individual packet different characteristics such as their origin, the protocol used, and the destination. With such detailed information, the ethical hacker can quickly identify security weakness in a system's network.

4. **Aircrack-ng** is a comprehensive utility collection used in analyzing the wifi network weaknesses. The tool allows one to monitor the wifi network security through data packets capturing and converting them to text format for additional analysis. Wifi cards performance verification occurs through injection and capture. It's beneficial in assessing the WPA-PSK and WEP key reliability. This tool helps in cracking these keys.

5. **John, the ripper**-use of traditional passwords is one of the most common cybersecurity risks. Attackers usually compromise users' password and use it in stealing necessary credentials, cause damage to access sensitive systems. Therefore, password cracking is a very critical penetration testing aspect. John, the ripper, is one of the best penetrative testing tools for this type of vulnerability. It's a primary free tool used in blending different password crackers to a single package. It automatically identifies various forms of password hashes and is accompanied by a customizable cracker. Pen testers usually use the tool in launching attacks to identify password weaknesses in databases or systems.

6. **Nessus** is a common paid for a tool used for scanning vulnerabilities in networks or computing systems (Singh 15). It is quite easy to use, offers accurate and fast scanning, and provides one with networks weaknesses comprehensive outlook just by clicking a button. Nessus scans for loopholes that hackers may exploit to damage its infrastructure. Some of the vulnerabilities identified by Nessus include open ports, improper passwords, and misconfiguration errors

7. **Burpsuite** is a commonly used tool for checking the web-based security applications. It comprises of different tools that can be applied when performing various security tests such as mapping the application surface attack, analyzing responses and requests happening between the destination servers, browsers, and web-based crawling application. There are two versions of the burp suite penetrative tool. The free version has the critical manual tools used for performing scanning activities. One may take into consideration the professional version when advanced web penetration testing capabilities are required.

Penetrative testing tools give automatic methods for searching for vulnerabilities to avoid the tedious and repetitive task of performing hundreds or thousands of tests for every type of vulnerability. The previous study indicates that these tools effectively in web service are very poor. Authors of this study tested four commercial tools that included two different versions of a specific brand in identifying the security flaws in over 300 web services available in the public domain. The vulnerability differences detected by every too and low coverage for the two scanners was less than 20 percent (Munea et al. 46). The false positives high number was 40 percent and 35 percent in both cases. These results were an indication of the upper limit for these tools. (Chandola 24)

Checking for web vulnerabilities requires a short amount of time. When faced with time constraints, developers have to choose between considering other forms of testing, such as static code analysis and penetrative testing. Other than regular penetrative testing plan, the test should occur whenever: a new network infrastructure is installed to the system, a system is updated, new software installed, the office is relocated, a new end-user policy is a setup or whenever the security system identifies new threats. Every business works uniquely, and the value of conducting penetrative testing is unique in each case.

For effective penetrative testing, security experts recommend regular use of penetration testing tools. There are also some experts who think penetration testing is not effective and a waste of time and money. Both of these views are wrong; the reality is that penetration testing is nuanced and complicated (Rountree 113). The process is expensive and generates a lot of reports after the testing. That's where the problem lies; research indicates that once penetrative testing tools create a report on the level of system insecurity, most clients lack the financing to fix all of them. Most people always discard the tentative testing report to avoid legal issues for failing to fix the security loops which they had identified before.

With enough money and time, penetrative testing is effective in finding vulnerabilities. If one will is not ready to fix all the weaknesses, then there is no point of identifying them. For effective penetration testing, there has to be protection, detection, the response. All three aspect is critical for a secure system (Sinha 36).

The effective penetrative system should be conducted to exploit severe vulnerabilities frequently. Penetrative testing is a unique business. Within the field of system security, there is an organization that solves the same problem as the penetrative testing tools using manual methods such as the military. Now the big question is, can't businesses do the same thing? Is the use of penetrative tools away from hiring burglars to break into organizations systems? Is it a way of committing fraud against oneself? The big answer to this is a no (EC-Council 34).

Penetration testing is currently a big business since the system is poorly understood and complicated. Many people know about fraud, kidnapping, and burglars but lack information on computer criminals. People don't understand the dangers they face, and they will be facing in the future, and therefore, hiring of the penetrative tester is critical in understanding such risk. For the penetrative testing tools to be effective, people should be ready to implement the action recommended in the reports generated by these tools (Engebretson 17).

III. CONCLUSIONS

Penetrative testing tools are very effective in identifying system vulnerabilities before they are attacked by hackers. However, the level of effectiveness is dependent on various factors. For effective pen test process, the process should be conducted by qualified testers. ISO standards require system owners and managers to do a regular penetration test and system reviews. Effective penetrative testing tools should detect multiple attacks which should be responded to immediately. If an intrusion is detected, the forensic and security teams should immediately respond to the threat, penetration testers should also be blocked followed by immediate removal of their tools. Attacks should be detected automatically, reports generated, and action taken in line with the company's internal procedures. Effective penetrative testing tools should not only asses risk from the client side but also the risks from the client interface.

REFERENCES

[1] Chandola, Sagar. *A Tour Of Ethical Hacking: Perfect guide of ethical hacking for beginners*. Sagar Chandola, 2014.

[2] EC-Council. *Ethical Hacking and Countermeasures: Attack Phases*. Cengage Learning, 2016.

[3] Engebretson, Patrick. "What is Penetration Testing?" *The Basics of Hacking and Penetration Testing*, 2013, pp. 1-18.

[4] Munea, Tewodros L., et al. "Network protocol fuzz testing for information systems and applications: a survey and taxonomy." *Multimedia Tools and Applications*, vol. 75, no. 22, 2015, pp. 14745-14757.

[5] Rountree, Derrick. "System Security." *Security for Microsoft Windows System Administrators*, 2011, pp. 109-134.

[6] Singh, Pawan. "Metrics for Quantification of the Software Testing Tools Effectiveness." *American Journal of Software Engineering and Applications*, vol. 4, no. 1, 2015, p. 15.

[7] Sinha, Sanjib. "Python 3 and Ethical Hacking." *Beginning Ethical Hacking with Python*, 2016, pp. 37-38.

[8] Stewart, J. M. *Network Security, Firewalls and VPNs*. Jones & Bartlett Publishers, 2013.

[9] Weber, Rolf H., and Dominic Staiger. *Transatlantic Data Protection in Practice*. Springer, 2017.

[10] Wrycza, Stanisław. *Information Systems: Development, Learning, Security: 6th SIGSAND/PLAIS EuroSymposium 2013, Gdańsk, Poland, September 26, 2013, Proceedings*. Springer, 2013.