IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
Volume 8, PP 25-28

Proactive Security Analysis in Network

Tanvi Kapdi[1], Priya Porwal[2]
[1](Computer Department, Atharva College of Engineering/ Mumbai University, India)
[2](Computer Department, Atharva College of Engineering/ Mumbai University, India)
Corresponding Author: Tanvi Kapdi

Abstract: *With the advent of new technology and modernization today most of the organizations opt for multilayer network architecture and heterogeneous server environments in order to fulfill the organization's increasing demands. But the major concerns for those organizations are "security" and thus every organization should have a build in set of policies that must comply with the goals and objectives of the organization.*
To meet up with these goals and objectives the optimal solution is through penetration testing. The process of penetration testing involves an active analysis of the system for any potential vulnerability. This analysis is carried out by considering oneself as the active attacker and exploiting the security of the system. Effective penetration test will couple this information with an accurate assessment of potential impacts to the organization and outline a range of technical and procedural countermeasures to mitigate the risk.
Though being such an exclusive approach still there are certain technical problems in the current penetration testing system which needs a detailed study of the penetration test methodology to overcome the challenges faced by the information security industry.
Keywords - *penetration testing, network security, ethical hacking, proactive security policy.*

I. Introduction

There is a considerable amount of confusion in the industry regarding the differences between vulnerability scanning and penetration testing as the two phrases is commonly interchanged. However, their meaning, and implications are very different. A vulnerability assessment simply identifies and reports noted vulnerabilities, whereas a penetration test attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing typically includes network penetration testing and application security testing as well as controls and processes around the networks and applications, and should occur from both outside the network trying to come in (external testing) and from inside the network.

Penetration testing, often called "pen testing or "security testing", is the practice of attacking your own or your clients' IT systems in the same way a hacker would to identify security holes. Of course, you do this without actually harming the network. The person carrying out a penetration test is called a penetration tester or pen tester.

Let's make one thing crystal clear: Penetration testing requires that you get permission from the person who owns the system. Otherwise, you would be hacking the system, which is illegal in most countries. In other words: The difference between penetration testing and hacking is whether you have the system owner's permission. Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents. Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in.

II. Requirement and Goals

The main objective of penetration is to determine security weaknesses. A pen test can also be used to test an organization's security policy compliance, its employees' security awareness and the organization's ability to identify and respond to security incidents.

- ✓ To improve information security awareness
- ✓ To assess risk
- ✓ To mitigate risk immediately
- ✓ To reinforce the IS process
- ✓ To assist in decision making processes

Each organization's management must continuously seek for the maximum information input and reevaluate their security policy in an endless loop. This approach will form a truly proactive security policy which is carefully redefined in a regular basis, taking into account every possible parameter (social, technical, environmental) might affect it [3].

The remainder of the paper is organized as follows. Section II discusses network attack taxonomy, by dividing the threats into classes according to their operational model. We present
the proposed penetration testing methodology and working framework in Section III. In Section IV we analyze the case study scenario and finally, Section V summarizes and concludes this paper.

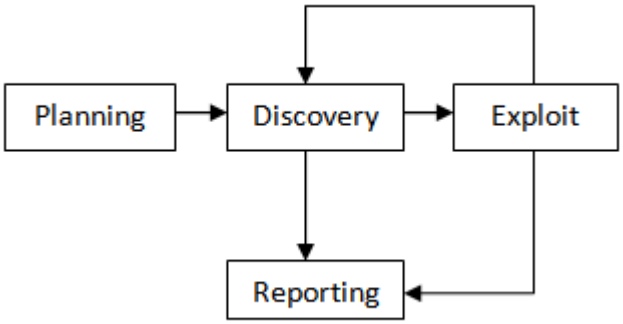

Figure 1: Penetration testing mythology

II. Attacker goals can be divided into four main classes: interruption, interception, modification and fabrication as shown in figure 1. An interruption attack aims to make network or system resources unavailable by carrying out large or special crafted amounts of information packets. It is an attack on availability mainly expressed by denial of service (DoS) attacks [8,9]. The second class is the interception attacks, where the attacker tries to gain unauthorized access to a network or system. A major example is a simple eavesdropping [10] on a communication channel where sensitive data are transmitted through it. Modification attacks aim to modify information that is transferred during a communication session of two or more parties. This class mainly includes network spoofing attack [11] where the information source and data fields are altered Pretending to originate from another source. Finally, the fourth class contains fabrication attacks which aim to bypass authenticity checks by mimicking or impersonating information.

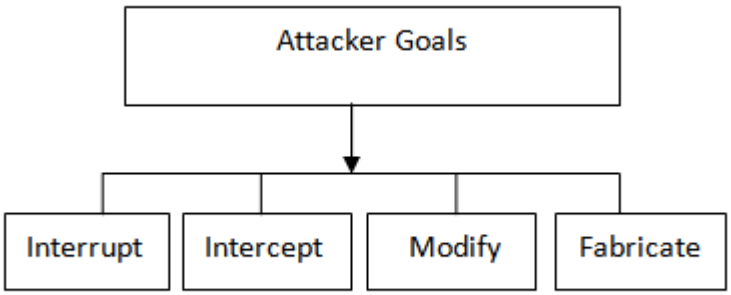

Figure 2: Classification of attacker goals

Keeping the above attacker goals in mind, there are two main types of attacks whose aim is to compromise the security of a network – passive and active attacks. During a passive attack the attacker simply monitors the transmission between two parties and captures information that is sent and received. The attacker does not intend to interrupt the service, or cause an effect, but to only read the information. If information is encrypted or obfuscated, it will be more difficult to interpret it. Although, the attacker simply observes the data flow and tries extract useful information about the evolved parties. Passive attacks are usually harder to detect as there is little or no impact. On the other hand, an active attack aims to cause disruption, and is usually easily recognized. Unlike a passive attack, active attacks modify information, interrupt services and aim to gain unauthorized access to the network systems.

III. The process of penetration testing as shown in Fig. 1, can be broadly divided into four phases: planning, discovery, exploitation and reporting. Initially at the planning phase, the scope for the assignment is defined. Management approvals, documents and agreements like NDA (Non Disclosure Agreements) are signed under the guidance of responsible legal departments and lawyers. After the management consent, the penetration testing team gathers crucial input about the organization operational procedures and security policies, towards defining the scope for the test. Following the initial planning, the actual penetration test starts with the discovery phase, also known as information gathering phase. During the information gathering process the penetration testing team launches scanning and enumeration procedures to gain as much information as possible about the target network and the participating systems and services. The gathering phase can be further divided into non-intrusive (public repositories, documents, mailing lists, web profiles etc) and intrusive (port scanning, firewall rules, matching OS fingerprints etc) inspection processes. Having adequate amount of information the testing team can profile the target network and enumerate possible exploitable vulnerabilities using relative public or personal security knowledge bases. The third and most import phase of a penetration test is the exploitation phase. Using as input the discovered vulnerabilities arriving from the previous phase, the penetration testing team revises matching proof-of-concept exploits that may lead to a network or service security bridge. Depending on the agreement with the management and the exploitation implication level, the attacks can be launched either in an identical network simulation lab or in the actual network using adequate security prerequisites. While exploiting network vulnerabilities and mis-configurations, the testing team might discover additional information that can feedback the discovery phase, resulting in new attack scenarios and exploits. This interaction between the discovery and exploitation phases is continuous throughout the actual test. The last phase that completes a penetration test process is the reporting phase. The report writing can begin in parallel to the other three stages, although must finish after exploitation phase has been completed. A successful report details all the findings and their impacts to the organization by taking into account both the technical and management aspects in its format. It is very important to conduct a fully detailed and well documented report in order to inform the management about the security risks and provide technical details and high level recommendations to the ICT department. Figure 1. Penetration testing methodology diagram.

IV. Let us understand the whole process with the help of a case study. The client requested to conduct a penetration test including exploitation (where possible) of discovered vulnerabilities against some of their public facing IP addresses as well as the internal network. In addition, the company requested to review their wireless network security.

Analysis of the public facing network revealed that the majority of accessible devices were reasonably well configured; however, two of the devices exhibited high-risk vulnerabilities.

One device contained copies of the Windows Command Interpreter in the /scripts folder. These files acted as a functional back door and could be used to execute a wide range of commands. As a demonstration, the tester created a folder called C:\demo on the server. The fact that these files existed on the server may have indicated that the server had been compromised in the past by an attacker or other malicious software (such as a worm). The tester then recommended that an investigation be conducted as to how these files came to exist on the server and advised a complete rebuild of the server from clean media may be required.

During this assignment, it was also found that the customer's web server suffered from a SQL Injection flaw. This flaw was caused by poor validation of input accepted by the web server application. The application took the input from the end user and passed it to the backend SQL server without validation. It was also possible for an attacker to login as any user in the database, or worse, to obtain any information contained within the database, including all user transactions, contact details and more. The web application operated with an account that had too many privileges on the SQL server; when this flaw was combined with the SQL Injection flaw it was possible for an attacker to execute any commands on the server. A complete application test was not completed against this server as this was out of scope, but it was recommended that a complete review of the application be conducted.

The internal network analysis revealed several vulnerabilities; they were predominantly caused by default, weak or missing passwords and the fact that numerous critical security patches were not installed. These weaknesses made it possible for the consultants to obtain access to sensitive data and information, including passwords for all services on the network and hence recommended that strong passwords be in place for all services and that all devices be properly hardened, regardless of whether they were public facing or not.

Both of the wireless networks found implemented WEP encryption. Unfortunately, weaknesses in the WEP implementation made it possible for an attacker to execute an attack that revealed the key (password). This fact was demonstrated and the key was retrieved within an hour. Both wireless networks broadcasted their identifier.

We have analyzed a case study on penetration testing over a network and based on the study we concluded that network security issues, concerns and trends are rapidly evolving posing a major challenge to the organization's business operations. Vendor updates are necessary although not enough for a proactive and efficient security policy. Thus the current state of penetration testing is far more from optimal and automating them will bring them to a new level of quality and overcoming the technical problems may be a challenge for the information security industry in the near future.

References

[1] Khidzir, N.Z., Mohamed, A. and Arshad, N.H.H., "Information Security Risk Management: An Empirical Study on the Difficulties and Practices in ICT Outsourcing", NETAPPS 2010.
[2] Kshetri, N., "The simple economics of cybercrimes", IEEE Security and Privacy (2006), Volume: 4, Issue: 1.
[3] Kotenko, I. and Bogdanov, V., "Proactive monitoring of security policy accomplishment in computer networks", IDAACS 2009
[4] Hamisi, N.Y., Mvungi, N.H., Mfinanga, D.A. and Mwinyiwiwa, B.M.M., "Intrusion detection by penetration test in an organization network", ICAST 2009.
[5] Bishop, M., "About Penetration Testing", IEEE Security and Privacy (2007), Volume: 5, Issue: 6.
[6] CERT Coordination Center Statistics, "http://www.cert.org/stats".
[7] S. Hansman and R. Hunt, "A taxonomy of network and computer attacks", Computers Security (2005), Volume: 24, Issue: 1, Publisher: Elsevier, Pages: 31-43.
[8] Long, M., Chwan-Hwa Wu, Hung and J.Y., "Denial of service attacks on network-based control systems: impact and mitigation", IEEE Transactions on Industrial Informatics (2005), Volume: 1, Issue: 2.