HADMÉRNÖK

XIII. Évfolyam 3. szám – 2018. szeptember

BASIC OF CYBERSECURITY PENETRATION TEST

KIBERVÉDELMI PENETRATION TESZT ALAPJAI

PARÁDA István

(ORCID ID: 0000-0002-3083-6015);

parada.istvan@uni-nke.hu

Abstract

Nowadays it is common and self-evident that organizations strive to secure their IT and communications systems. Part of this is testing and checking systems. One of the most important elements of cyber security testing is the penetration test. Penetration tests show the extent to which IT security is threatened by attackers. Attacks and security measures can provide adequate IT security. Measures to improve IT security are needed to overcome the threats. In line with corporate IT security policy, all such measures are described in the IT security concept for the entire organization. It is important to understand the process of penetration testing within cage protection and that it is not equal to public hacking. Penetration Test is a complex process that technically provides a comprehensive and realistic picture of the vulnerabilities of the infocommunication system. This article describes the basics of the penetration test, the location and role of the vulnerability analysis, and the basic parameters of the test.

The work was created in commission of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled „Public Service Development Establishing Good Governance.

Keywords: *cybersecurity, penetration test, vulnerability analysis*

Absztrakt

Napjainkban általános és magától értetődő dolog, hogy a szervezetek az informatikai és kommunikációs rendszereik biztonságára törekszenek. Ennek egy része a rendszerek vizsgálata és ellenőrzése. A kiberbiztonsági tesztek egyik legfontosabb eleme a penetrációs teszt. A penetrációs tesztek azt mutatják, hogy az informatikai biztonságot milyen mértékben fenyegetik a támadók. A támadások és a biztonsági intézkedések képesek-e megfelelő informatikai biztonságot nyújtani. A fenyegetések leküzdéséhez az informatikai biztonság javítására irányuló intézkedésekre van szükség. A vállalati IT biztonságpolitikával összhangban minden ilyen intézkedést az egész szervezetre vonatkozó informatikai biztonsági koncepció ír le. Fontos megérteni a kibervédelmen belül a penetrációs tesztek folyamatát, és hogy nem egyenlő a köztudatban megjelent hack-eléssel. A penterációs teszt egy összetett folyamat, mely technikai úton átfogó és reális képet ad az infokommunikációs rendszer sérülékenységeiről. Ez a cikk bemutatja a penetráció teszt alapjainak meghatározását, a sebezhetőségi elemzés helyét és szerepét, valamint a teszt alapvető paramétereit. A mű a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú, „A jó kormányzást megalapozó közszolgálat-fejlesztés” elnevezésű kiemelt projekt keretében, a Nemzeti Közszolgálati Egyetem felkérésére készült.”

Kulcsszavak: *kiberbiztonság, penetrációs teszt, sérülékenységelemzés*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.07.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.05.19.

INTRODUCTION

Penetration testing has been in use for years and there are several methods for testing the technical security of the system. However, it is easy to confuse other forms of technical security testing, especially vulnerability analysis. Many organizations offer security features and terms such as security audit, network or risk assessment, and overlapping test overlays or application. Security surveys are a risk assessment, that is, services to identify the vulnerability of systems, applications and processes. Penetration testing has been in use for years and there are many methods to test the technical security of the system. However, it is easy to coordinate technical security tests in other forms, especially vulnerability analysis.

Nowadays there are many free and commercial security scanners, most of which contain updated databases due to known hardware and software failures. These tools are suitable to identify the vulnerability of the systems under investigation and therefore determine the risks associated with them. Typically, information provided by such devices includes a technical description of security vulnerability and provides instructions on how to eliminate weak points or points by changing configuration settings or updating system components. [1]

PENETRATION TEST KEY CONCEPTS

Definition of penetration test

Penetration testing uses several manual and automated techniques to simulate an organization's security information systems attack. This must be done by a qualified and independent penetration testing expert, sometimes referred to as an ethical security tester. Penetration testing takes advantage of known vulnerabilities, but it also needs testing expertise to identify specific weaknesses in the organization's security systems - unknown vulnerabilities. [2] The penetration testing process is an active analysis of the target system due to possible vulnerabilities that result from incorrect or incorrect system configuration, known and unknown hardware or software failures, and operational weaknesses in process or technical countermeasures. This analysis is typically carried out in the perspective of a potential attacker and could include the exploitation of vulnerabilities. So, the penetration test is a way to simulate methods an attacker can use to take over security management of our system or access it to a higher level of access. The process itself involves filtering and collecting vulnerabilities and security risk factors, then exposing them to attack by exploiting them. The penetration test more than, test runs over scanners or automated tools and then writes a report about it. The penetration test evaluates whether the vulnerability is real or false. For example, an audit or a survey may use scanning tools that result in hundreds of possible vulnerabilities on multiple systems. The penetration test attempts to attack these vulnerabilities in the same way as a malicious hacker to check which vulnerabilities are real, reducing the realistic list of system vulnerabilities for some security deficiencies. The most effective penetration tests are those that target a very specific system that has a very specific purpose. [3]

Penetration testing, often abbreviated as pentest, is a process that is performed to thorough safety assessment or audit. The methodology defines rules, practices, and procedures followed and implemented by the information security audit program. The penetration testing methodology defines a timetable, that provides practical ideas and best practices that can be tracked when assessing the true security situation of a network, application, system, or any combination thereof. Penetration testing can be performed individually or as part of an IT security risk management process that can be integrated into the regular development lifecycle. It is essential to note that product safety is not only dependent on factors related to the IT environment but also relies on product-specific security practices. This includes the implementation of appropriate security requirements, risk analysis, code surveys, and operational safety measurements. The penetration test is the last and most aggressive form of security assessment. They must be trained by qualified professionals and can be performed with or without prior knowledge of the targeted network or application. The penetration testing output usually consists of a report that is divided into several parts that address the weaknesses found in the current state of the target environment and then recommend potential countermeasures and other recovery suggestions. The use of the methodological approach has extensive benefits for the tester to understand and critically analyze the integrity of the current defense throughout each stage of the testing process. The reason behind the penetration testing methodology is the fact that most attackers follow a common approach, when they enter the system. In the penetration test, the tester is limited by resources: time, skilled resources and access to equipment as outlined in the penetration testing agreement. The penetration test simulates the methods used by the intruder that give unauthorized access to the organization's network and compromise them. This includes the use of own and open source tools. In addition to automated techniques, intrusion tests include manual techniques for testing targeted systems and ensuring that there is no security vulnerability that has not been detected before. [4]

Vulnerability scanners

Vulnerability Analysis (also known as "Scanning") is the use of automated tools to identify well known security vulnerabilities in the system. Vulnerability assessment tools investigate information systems to determine whether security settings are turned on and applied, and that appropriate security patches have been applied. The vulnerability test is typically used to validate the minimum level of security - and is often the forerunner of a more specialized penetration test. It does not use the identification of attacks to re-engage the real attack and does not consider the general security of system-based management processes and procedures. This is the process of scanning network devices, operating systems, and applications to identify known and unknown vulnerabilities. Vulnerability is a gap, error, or weakness in system design, use, and protection. If a vulnerability is exploited, it may result in unauthorized access, prerogative, denial of service on the device, or other results. Vulnerability surveys typically break when a vulnerability has been found, so the tester does not perform an attack on the vulnerability to make sure it is real. The vulnerability assessment results with potential recovery steps as well as possible risks associated with any vulnerability. There are a number of solutions, such as Kali Linux, which can investigate vulnerabilities based on system / server type, operating system, open ports, and other devices(for exaple OpenVAS[1], MBSA[2] Secunia PSI[3], Nipper[4], Retina[5], Nexpose[6] GFI Lan Guard[7].)[5]

[1] The Open Vulnerability Assessment System (OpenVAS) is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. The actual security scanner is accompanied with a daily updated feed of Network Vulnerability Tests (NVTs), over 33,000 in total (as of December 2013). All OpenVAS products are Free Software. Most components are licensed under the GNU General Public License (GNU GPL). The OpenVAS is available for FREE and for Linux, Windows and other operating systems.

[2] The Microsoft Baseline Security Analyzer provides a streamlined method to identify missing security updates and common security misconfigurations. MBSA 2.3 release adds support for Windows 8.1, Windows 8, Windows Server 2012 R2, and Windows Server 2012. Windows 2000 will no longer be supported with this release. MBSA is a FREEWARE and is available only for Windows operating system.

Vulnerabilities are only useful when calculating the risk. The disadvantage of many security audits is the result of vulnerability testing, which makes security checks longer, without providing real value. Many vulnerable scanners show false results or identify vulnerabilities that do not really exist. This is because they are incorrectly identifying the operating system or looking for special fixes to fix vulnerabilities, but they do not investigate interchangeable fixes (multiple minor fixes) or software modifications. This means that the vulnerabilities reported by the automatic devices must be checked. Vulnerability Assessment is a process that can measure internal and external security audits by identifying threats that severely affect your organization's assets. Internal vulnerability assessment provides assurance of internal systems while external vulnerability assessment demonstrates border protection. In both test criteria, all elements of the network are strictly tested against multiple attack vectors to identify unattended threats and quantify reactive actions. Depending on the type of assessment to be performed, unique testing processes, tools and techniques are used to automatically detect and identify the vulnerability of information assets. This is achieved through an integrated vulnerability management platform that provides up-to-date security vulnerabilities and can test various types of network devices while retaining the integrity of configuration and change management. [6]

Penetration test vs vulnerability analysis

The key difference between vulnerability and penetration testing is that penetration tests go beyond the level of vulnerability identification that leads to exploitation process, increasing entitlements, and maintaining access to target systems. On the other hand, evaluation of vulnerability provides a broad picture of system errors, without considering the impact of these errors on the system being tested. The other two significant differences between the two terms are that the penetration test is much more rough than evaluating vulnerability and aggressively uses all the technical methods to take advantage of the IT environment. The vulnerability assessment process, however, carefully identifies and quantifies all known vulnerabilities in a non-invasive manner.

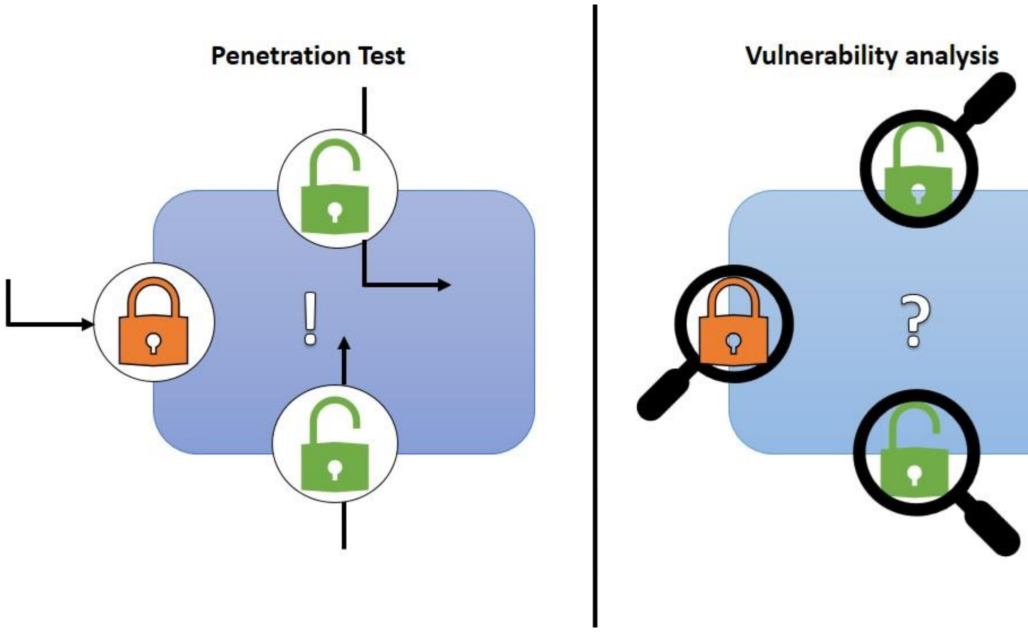
[3] The Secunia Personal Software Inspector (PSI) is a free security tool designed to detect vulnerable and out-dated programs and plug-ins, which expose your PC to attacks. Once installed, the Secunia PSI can help you patch vulnerable programs and stay secure. Secunia PSI is available for free and works only with Windows operating system.

[4] Nipper (short for Network Infrastructure Parser, previously known as Cisco Parse) audits the security of network devices such as switches, routers, and firewalls. It works by parsing and analyzing device configuration file which the Nipper user must supply. This was an open source tool until its developer (Titania) released a commercial version and tried to hide their old GPL releases (including the GPLv2 version 0.10 source tarball). Nipper is available for Windows, Apple MAC OSX, Linux and is a PAID software.

[5] With over 10,000 deployments since 1998, Beyond Trust Retina Network Security Scanner is the most sophisticated vulnerability assessment solution on the market. Available as a standalone application or as part of the Retina CS unified vulnerability management platform. Retina Security Scanner enables you to efficiently identify IT exposures and prioritize remediation enterprise-wide.

[6] Nexpose, the vulnerability management software, proactively scans your environment for mis-configurations, vulnerabilities, and malware and provides guidance for mitigating risks. Experience the power of Nexpose vulnerability management solutions by knowing the security risk of your entire IT environment including networks, operating systems, web applications, databases, and virtualization.

[7] GFI LanGuard scans and detects network vulnerabilities before they are exposed, reducing the time required to patch machines on your network. GFI LanGuard patches Microsoft ®, Mac® OS X®, Linux® and more than 50 third-party operating systems and applications, and deploys both security and non-security patches. GFI Lan Guard is a paid software and only works on Windows operating.



1. Figure Penetration test versus vulnerability analysis

So by scanning the vulnerability you will find individual vulnerabilities; penetration testing, however, tries to verify whether these vulnerabilities can be exploited in the target environment. Penetration testing in the area of security assessments goes one step beyond the vulnerability tests. Vulnerability Testing - a process that examines the security of individual computers, network devices, or applications - the penetration test evaluates the security model for the entire network. Penetration testing reveals the potential consequences for network administrators, IT managers, and executives for a real attack on the network. Penetration tests highlight the typical safety deficiencies that have been omitted during the vulnerability test. The penetration test points out the vulnerabilities and documents that these weaknesses can be exploited. It also shows that an attacker can exploit a number of minor vulnerabilities that compromise computers or the network. Penetration testing highlights the lack of organizational security modeling and helps organizations strike a balance between technical performance and business functions for potential security injuries. This information is also useful for disaster recovery and business continuity planning.[7]

Most vulnerabilities are evaluated only by software and do not evaluate other types of potential security issues. Human factors and processes can be important sources of vulnerabilities, just as technology or software vulnerabilities. By using social engineering techniques, intrusion tests may reveal whether employees can routinely allow people to enter into enterprise facilities without unauthorized access and unauthorized access to a computer system. Exercises applied during the patch management cycle can be evaluated during the penetration test. The penetration test is an ethical attack simulation designed to demonstrate or enforce the effectiveness of security controls in a given environment through exploitable vulnerabilities that pose real risks. It is built around a manual testing process that aims to move on through general responses, false positive results, and incomplete automated app ratings (such as tools used in vulnerability assessments). [8]

MAIN PARAMETERS

Objectives

In the case of a successful penetration test for the customer's expectations, a clear definition of the goals is indispensable. If the goals can not be achieved or are not effectively achieved, the tester should inform the customer during the preparatory phase and recommend alternate procedures. The result of the IT penetration test should therefore be more than just a list of existing vulnerabilities; Ideally, it should also provide concrete solutions and suggestions.

Intrusion testing is performed by an organization to achieve the following goals:

- Improving the safety of technical systems
- Identify vulnerabilities
- Confirming IT security by an external third party
- Improving the security of organizational and personnel infrastructure
- Test and confirm the safety and control efficiency
- Ensure availability of the organization's internal and external vulnerabilities
- Provide useful information to audit teams that collect data to comply with legislation
- Minimizing the costs of security controls by providing comprehensive and detailed, realistic evidence of business capability
- Promote the relevance of relevant patches for reported or known vulnerabilities
- Disclosing the existing risks of the organization's networks and systems
- Evaluating the effectiveness of network security tools, such as firewalls, routers, and web servers
- Develop a comprehensive approach to prepare for preventing future exploitation
- Find out if any existing software, hardware or network infrastructure needs to be modified or upgraded

Most penetration tests are commissioned to improve the safety of technical systems. Tests are limited to technical systems such as firewalls, routers, web servers, etc. The organizational and personnel infrastructure is generally not specifically tested. The penetration test can also be performed for confirmation from an independent external third party. It is important to note that the penetration test reflects the situation only at a certain point in time and can not, therefore, give a statement about the future security level. [9]

What makes a good penetration test?

The following activities ensure good penetration:

- Define the parameters of the penetration test, such as goals, limitations, and justification for the procedures
- Recruit highly trained and experienced professionals
- Appoint a legal penetration tester who follows the rules in the termination agreement
- Select a suitable test package that balances costs and benefits
- Follow up a well-designed methodology with documentation and documentation that documents the results carefully and makes them understandable to the customer. An intruder tester should be available to answer any questions when needed.
- The final report provides a clear description of the findings and recommendations

Limits

Performing penetration test runs will help you examine some of your security measures and improve your development, but there are limitations. For example, a penetration test:

- It covers only the targeted application, infrastructure, or the selected environment
- Focuses on the discovery of technical infrastructure,
- It covers only a small part of the human resources screening, specifically (social enginnering)
- Just snapshot from a system at a given time
- By legal or commercial considerations, the width or depth of the test can be limited
- You cannot detect all security weaknesses, for example due to limited scope or inappropriate testing
- Provides results that are often of a technical nature and need to be interpreted in a business context

Challenges

In general, organizations have encountered the following difficulties:
Determining the depth and width of the test coverage

- Determine what type of penetration test is required
- Understand the difference between vulnerability and pentest
- Identify the risks associated with possible system failures and disclosure of sensitive data
- Frequency of goals and tests
- To improve the vulnerabilities discovered during the penetration test, the system will really be "safe"

The need

The main drivers of penetration testing include a high level of concern about:

- Increasing compliance requirement
- The impact of serious (often Internet) security attacks on similar organizations
- Utilize the number and variety of outsourced services
- Significant changes in business processes
- Awareness raising about potential cyber security attacks. [10]

CONCLUSIONS

The summary should briefly summarize the conclusions, the results, possible suggestions and other new research orientations. The summary is also a mandatory element of the publications. The cybersecurity penteration test provides a thorough study of IT systems. As a result of today's trends, this choice of test methods provides complex analysis that covers the system and the organization's IT-related questions. It shows significant differences in testing vulnerabilities but provides a more comprehensive approach from the attacker's point of view. With this test, the identified safety deficiencies are not only collected but also exploited. the attacker goes on to exploit the vulnerability analysis as it may go further, get new information, and do more attacks. Then a comprehensive report is prepared, including suggestions.

Penetration Test is one of the most important technical tests of cyber security to ensure system security. Considering a number of international standards, however, there are many definitions and rounding differences. Standards are, of course, a major direction, but there are a lot of differences. This is because, on the one hand, these are recommendations, are not binding. On the other hand, the penetration test itself depends on the attacking nature and expertise, so it can be said to try the objective test, but there are subjective elements in it. That is why I thought it important to define basic definitions, goals and features. This publication has collected the basic understanding of the penetration test, the differences between the fragility test and the penetration test. This includes the benefits, goals, and limitations associated with the test.

BIBLIOGRAPHY

[1] FEDERAL OFFICE FOR INFORMATION SECURITY (BSI) STUDY: *A Penetration Testing Model;* Bonn p.8.

[2] JASON C, IAN G.: *A guide for running an effective Penetration Testing programme* April (2017) p.8.

[3] GEORGIA W.: *Penetration testing A Hands-On Introduction to Hacking*; San Francisco ISBN-10: 1-59327-564-1 ISBN-13: 978-1-59327-564-8 (2014) pp.31-36.

[4] LEE A, TEDI H, SHAKEEL A.: *Kali Linux – Assuring Security by Penetration Testing*, Birmingham ISBN 978-1-84951-948-9; (2014) pp. 51-52.

[5] EC-COUNCIL CERTIFI ED SECURITY ANALYST PRESS*: Penetration Testing Procedures and Methodologies* ISBN-13: 978-1-4354-8367-5 ISBN-10: 1-4354-8367-7, USA (2011) p.23.

[6] JOSEPH M, AAMIR L.: - *Web Penetration Testing with Kali Linux;* Birmingham. ISBN 978-1-78216-316-9 (2013) p.13.

[7] LEE A, TEDI H, SHAKEEL A.: *Kali Linux – Assuring Security by Penetration Testing,* Birmingham ISBN 978-1-84951-948-9; (2014) pp. 53-54.

[8] JASON C, IAN G.: *A guide for running an effective Penetration Testing programme* April (2017) p.9.

[9] EC-COUNCIL CERTIFI ED SECURITY ANALYST PRESS: *Penetration Testing Procedures and Methodologies* ISBN-13: 978-1-4354-8367-5 ISBN-10: 1-4354-8367-7, USA (2011) p.24.

[10] JASON C, IAN G.: *A guide for running an effective Penetration Testing programme* April (2017) pp.10-12.