HADMÉRNÖK

XIII. Évfolyam 4. szám – 2018. december

POSSIBLE CLASSIFICATION OF CYBERSECURITY PENETRATION TEST

KIBERBIZTONSÁGI PENETRÁCIÓS TESZT LEHETSÉGES OSZTÁLYZÁSA

PARÁDA István

(ORCID: 0000-0002-3083-6015)

parada.istvan@uni-nke.hu

Abstract

Nowadays, there is a lot to hear about the issue of cyber protection. Generally, everyone seeks to secure their IT and communication systems. Efforts include examining and verifying such systems. One of the aggressive control forms is the Cyber Security penetration test. Many people only identify hacking, though your test is much more than that. In order to understand the multiplicity of the test we need to be aware of the key concepts and test-related features. In this publication, the penetration test aims to present a possible classification that has been made by analyzing international standards. 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, cyber protection, IT, communication*

Absztrakt

Napjainkban rengeteget hallani a kibervédelem kérdésköréről. Általánosságban elmondható, hogy mindenki az informatikai és kommunikációs rendszereinek biztonságára törekszik. A törekvések közé tartozik az ilyen rendszerek vizsgálata, ellenőrzése. Az egyike agresszív ellenőrzési forma a kiberbiztonsági penetrációs teszt. Rengetegen csak hack-elésnek azonosítják, bár a maga a teszt sokkal több ennél. Ahhoz, hogy megértsük többrétegűségét a tesztnek tisztában kell lennünk, az kulcsfontosságú alapfogalmakkal, a tesztel kapcsolatos jellemzőkkel. Ezen felül meg kell érteni a tesztek elindításánál, milyen típusú tesztet érdemes elkezdni, és egyáltalán milyen kategóriákba sorolhatók a penetrációs tesztek. Jelen publikáció a penetrációs teszt egy lehetséges osztályzást kívánja bemutatni, melyet a nemzetközi szabványok elemzésével sikerült megalkotni. 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, kibervédelem, IT, kommunikáció*

A kézirat benyújtásának dátuma (Date of the submission): 2018.05.17.
A kézirat elfogadásának dátuma (Date of the acceptance): 2018.05.20.

INTRODUCTION

Digital is emerging as a result of the information technology revolution tools and systems are facing significant challenges. It's all the truer because all segments of everyday life are affected by communication through information technology. It is clear that these systems are a basic requirement of security. Safety can be assured by controllers, risk management, tests, and many other ways. One of these important test methods for info-communication system protection is the penetration test. This kind of complex investigation examines the attacker's perspective, follows the attacking steps and detects and exploits vulnerabilities. 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.

There are a number of international standard (for example PTES[1], OSSTMM[2], ISSAF[3], NIST[4], FedRamp[5], OWASP[6], PCI DSS[7],) recommendations for these tests, which are recommended to follow, but these different approaches often classify the tests under different points of view. Although it can be said in general that the main course is the same, flows, goals, steps, but examining the standards can be said that there are a lot of minor deviations that give rise to a self-rating. Classification has a significant role in agreements and planning, it helps to determine the nature of the test, and gives a clearer picture to the customer organization about the test.

[1] Penetration Testing Execution Standard. It is a new standard designed to provide both businesses and security service providers with a common language and scope for performing penetration testing (i.e. Security evaluations). It started early in 2009 following a discussion that sparked between some of the founding members over the value (or lack of) of penetration testing in the industry.

[2] The premise of the Open Source Security Testing Methodology Manual also known as the OSSTMM (pronounced as "awstem") It is a peer-reviewed manual of security testing and analysis which result in verified facts. These facts provide actionable information that can measurably improve your operational security.

[3] The Information Systems Security Assessment Framework (ISSAF) is produced by the Open Information Systems Security Group, and is intended to comprehensively report on the implementation of existing controls to support IEC/ISO 27001:2005(BS7799), Sarbanes Oxley SOX404, CoBIT, SAS70 and COSO, thus adding value to the operational aspects of IT related business transformation programs. It is designed from the ground up to evolve into a comprehensive body of knowledge for organizations seeking independence and neutrality in their security assessment efforts.

[4] The NIST Cybersecurity Framework (NIST CSF) provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks.

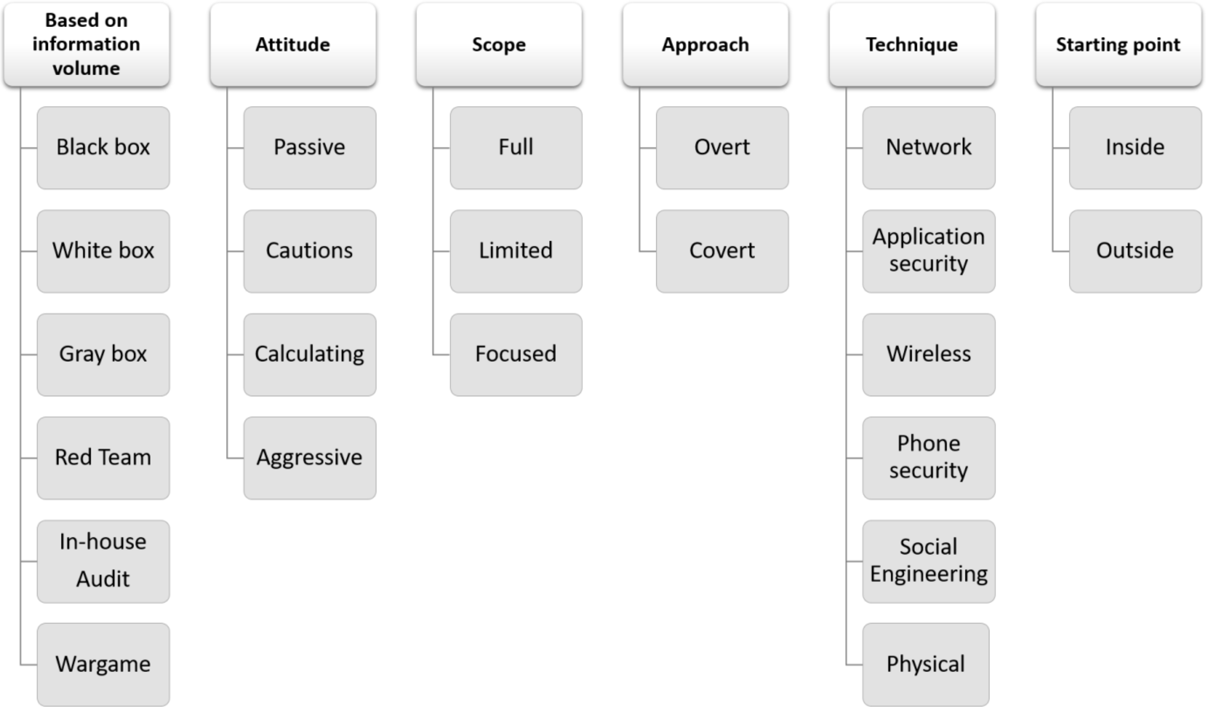
[5] The Federal Risk and Authorization Management Program (FedRAMP) is an assessment and authorization process which U.S. federal agencies have been directed by the Office of Management and Budget to use to ensure security is in place when accessing cloud computing products and services.

[6] The Open Web Application Security Project (OWASP), an online community, produces freely-available articles, methodologies, documentation, tools, and technologies in the field of web application security.

[7] The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major card schemes.

CLASSIFICATION

What criteria can you use to describe a penetration test or what differentiates one penetration from the other? Distinguishing features include, for example, the size, structure of the tested systems, the precautionary or aggressive nature of the tests, etc. Which characterize a particular penetration test - should be adapted to the purpose of the test so that an effective and effective examination can be carried out. It should be noted that not all possible combinations are a useful test, even if the classification criteria were kept in as wide a variety of ways. The aggressive test is usually identified very quickly and is therefore not ideal in combination with stealth techniques. Likewise, an open penetration test is not suitable, for example, for social engineering to obtain pre-cited confidential information. Classification can be based on many aspects and (many doctors categorize the penetration test type according to the same criteria). In the publication, he now presents a possible, more detailed classification scheme by the author.



1. Figure Possible classification of penetration test

Based on information volume

- Black Box Testing (Zero Knowledge Testing): For simulating real attacks and minimizing false results, penetration testers can choose to perform black-box testing (or zero-level knowledge testing when there is no information or help from the customer's side) and discreetly crawl the network while listing services, shared file systems, and operating systems. In addition, the penetration tester may perform award to detect available modems and detect vulnerable access points, provided that these activities fall within the scope of the project. During black-box testing, testers have no prior knowledge of the infrastructure they are testing, and do not know the internal operation of a system. This test is only performed after extensive research on the organization. The black-box test realistically simulates a typical Internet hacker attack. The tester attacks the target without knowing about defense, strengths, or communication channels. The target will not be notified of the scope of the audit, tested channels, or test vectors. The audit examines analytical skills and the preparedness of the target for unknown variables during the test. The scale and depth of the test can only be as much as the tester's knowledge and effectiveness can be. The hacker needs to examine the information required in publicly available databases. This test simulates a true hacker process. Testing the black box is time consuming and expensive. It is also known as a functional test.

- White Box Testing (Full Skill Testing): If the organization needs to evaluate its security to achieve a specific attack or a specific goal. In this case, you can provide full information about the organization's network to the penetration tester. The information provided may include network topology documents, asset inventory and valuation information. Typically, an organization chooses this when full control of security is the goal. It is important to note that, nevertheless, the information security process and the penetration test give a snapshot of the security position of an organization at that time. You can do a white box test with or without IT staff. White box testing is also called complete knowledge testing. The tester has various pieces of information about the body before white box testing. The analyst attacks the target because of his defense and tools as well as the complete knowledge of the communication channels. The goal is notified in advance about the scope and duration of the audit, but not the tested channels or test vectors. Width and depth depend on the quality of information about the analyst and target analysis, as well as from the tester's knowledge. Testing the white box often gives the following information to the tester:
  - Organizational infrastructure: This includes information about the various organizational units of the organization. Information about hardware, software and controllers is also disclosed by the penetration tester.
  - Network Type: Network type information may be for the organization's LAN[8] and the topology that implements the system's connection. Information about remote networks and access to the Internet may be.
  - Current security implementations: Current security implementations are the various security measures that the organization has adopted to protect vital information against any damage or theft.
  - IP address/firewall/IDS[9] data: This information includes details of the IP address of the organization using firewalls that protect the data against unauthorized users and other important technical details about the network. Firewall and IDS policies are available for the penetration tester.
  - Corporate Policies: The various business policies that an organization has adapted to perform a business depends on the nature of the test. Security policies, legal policies, and labor policies all can be useful to the penetration tester.
- Gray-box testing: The most common method for the testing vulnerability is the penetration testing of the gray box. This testing process works like a black box test. Both the tester and the normal user have the same privileges. The purpose of the tests is to simulate a malicious insider attack. The gray box penetration test includes a safety assessment and internal testing; the test process examines insiders' access to the

[8] A local area network (LAN) is a computer network that interconnects computers within a limited area such as a residence, school, laboratory, university campus or office building.

[9] Intrusion detection system (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported either to an administrator or collected centrally using a security information and event management system.

organization's network. Here, the tester usually has limited information. The tester targets the target with limited control over his defense and tools as well as the communication channels. Gray box testing tests the analytical skills. The nature of the test is efficiency. Width and depth depend on the quality of the information provided by the analyst prior to the test and the applicable knowledge of the analyst

- War - The tester attacks the target without knowing about defense, strengths, or channels of communication. The goal is to prepare for verification, knowing all the details of the check. The test primarily tests the analytical skills. The scope and depth of the audit can only be as much as the analyst's applicable knowledge and effectiveness.
- In-house Audit - The tester and the target are prepared for the check, both of you can advance all the details of the check. The tandem audit tests the target's protection and control. However, you cannot test the preparedness of the target for unknown variables. The width and the depth depend on the analyst's quality of the information (transparency) and the applicable knowledge of the analyst
- Red Team Practice - The tester has full knowledge of its purpose and its operational safety, but the goal knows nothing about what, how or when the analyst will test. The true nature of this test is to check the preparedness of the target against unknown variables and vectors. Width and depth depend on the knowledge and creativity of the tester and the quality of the information transmitted. [1] [2]

Attitude

In order to allow for a sufficiently fine distinction, four levels of aggression have been identified for the purpose of the study:

- At the lowest level, test objects are only passively tested, meaning that the detected vulnerabilities are not exploited.
- Identified vulnerabilities of the second level - cautious - can only be exploited if the tested system does not harm or disrespect the tester's best knowledge
- Calculating the next level - the tester will also try to exploit the vulnerabilities that could lead to system failures. This includes, for example, the automatic testing of passwords and the utilization of known buffer overflows in precisely defined target systems. Before doing so, the tester will examine how likely the attacks are to be successful and how serious the consequences are.
- The highest level - aggressive - the tester tries to take advantage of all possible vulnerabilities, eg. buffer buffers are also used on unidentified target systems or deactivate security systems with deliberate overload (DoS[10]) attacks. The tester should be aware that in addition to the tested systems, adjacent systems or network components may be harmed as a result of the tests. [3]

Scope

When a penetration test is first performed, a full test must be carried out to ensure that the safety loopholes in the non-tested systems are ignored. The time required for the penetration test is usually directly related to the scope of the systems being tested. The same and nearly

[10] Denial-of-Service attack, a type of network computer attack that attempts to render a particular service (e.g. web site) unavailable to its audience.

identical systems are often tested in a single test, but as there are different configurations, each system must be handled separately:

- Focused: If only one particular subnet, system or service is to be tested, the penetration test must be considered focused for the purposes of this test. This test scope adjusts, for example, after modifying or extending the image of the system. Such a test can, of course, only provide information about the tested system; does not provide general information on IT security.
- Limited: A limited number of systems or services are tested in a limited penetration test. For example, systems containing all systems or functional units in DMZ[11] can be tested.
- Complete: The entire test covers all available systems.

Approach

If, in addition to primary security systems, secondary systems such as IDS, organizational or personal structures (eg escalation processes) have to be tested, the test approach should be amended accordingly:

- Uncovered/Overt: Penetration tests on secondary security systems and existing escalation procedures must at least initially be secretive, so in the initial assessment phase, only methods that cannot be directly identified by attempts to attack the system are used. It involves simulations and implementations of attacks, but in this case, we do not have any information about that organization. The Covert Test tests the ability of the internal security team to detect attacks and respond to attacks. This type of test covers more time and money and requires much more knowledge and ability. In a Penetration tester's eye, this kind of measurement is preferable, as this is the closest to simulating a real attack. There are no significant vulnerabilities in this test, but the easiest way to access the system is unexpectedly revealed.
- Covered/Covert: If the hidden approach fails to generate a response or the tester performs a white box test in cooperation with the system, open methods can be used such as searching for extensive ports with direct connections. Customers can join the team in an open white box test. This is especially recommended for extremely critical systems because it means that testers are able to respond more quickly to unexpected problems. When co-operating with the organization to identify potential security threats. One of the great advantages is that you have the ability to initiate the desired access and internal knowledge attacks without the risk of blocking. On the other hand, it is a disadvantage for the identification of the security program, ie how to detect certain attacks. [4]

Technique

In a traditional penetration test, systems are attacked only through the network. In addition, physical attacks and other types of social engineering techniques can be used to attack systems.

[11] Demilitarized zone (sometimes referred to as a perimeter network) is a physical or logical subnetwork that contains and exposes an organization's external-facing services to an untrusted network, usually a larger network such as the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network, an external network node can access only what is exposed in the DMZ, while the rest of the organization's network is firewalled. The DMZ functions as a small, isolated network positioned between the Internet and the private network.

- Networking: A network-based penetration test simulates a typical method of attacking a typical hacker attack. Most IT networks currently use TCP / IP[12], so these tests are also called IP-based penetration tests. The network security test identifies risks and vulnerabilities that could damage network and security policies. Provides information on network security decisions. Testing network penetration is critical to your organization's computer network. It is designed to evaluate network and system security risks and vulnerabilities from an attacker perspective. Network penetration testing uses processes and tools to investigate network vulnerability and helps organizations develop security policies. This test tries to compromise systems on the network as an attacker and then make a detailed statement of the findings. It detects network security issues that lead to data or equipment manipulated by Trojans, DoS attacks, and other intruders. This test ensures that the security implementation actually provides the protection your business requires whenever an attack occurs on the network, usually by exploiting the vulnerability of an organization's system.
- Application Security: It is not possible to prevent a weak application from being aware of the organization's assets, even in a well-established and secure infrastructure. This type of testing is intended to ensure that the application does not detect or provide access to central servers within a network and software. Software testing is an essential part of the software development process and helps to determine the accuracy and completeness of the software versions developed. In other words, software testing provides trouble free and reliable software. Testing applications involve testing software applications and testing web applications. Web application vulnerabilities can be identified by testing web applications. The best way to perform this test is by utilizing various vulnerabilities in the application through a series of regular and repetitive tests. Some important aspects of application testing:
  - Review Source Code: Revision of source code helps to ensure that the software does not contain any important information an attacker can use to exploit an app. For example, an available software code may include test requests, names, or clear text passwords that may contain relevant data or information for the tester.
  - Licensing Testing: Licensing Testing tests systems for commencing and maintaining user sessions. This includes testing login credentials, cookie security, and exclusion testing to ensure that valid sessions cannot be diverted. Licensing tests are performed to identify the authorization status of notified systems and to help identify unauthorized access.
  - Functionality Testing: Functionality testing tests the systems that are responsible for the functionality of the application. This includes testing the validation of characters and specific URLs inputs.

[12] TCP/IP, in full Transmission Control Protocol/Internet Protocol, standard Internet communications protocols that allow digital computers to communicate over long distances. The Internet is a packet-switched network, in which information is broken down into small packets, sent individually over many different routes at the same time, and then reassembled at the receiving end. TCP is the component that collects and reassembles the packets of data, while IP is responsible for making sure the packets are sent to the right destination. TCP/IP was developed in the 1970s and adopted as the protocol standard for ARPANET (the predecessor to the Internet) in 1983.

  - Web penetration testing: Web penetration testing includes verifying Web-based texts in languages such as J2EE[13], ASP.NET[14], and PHP[15]. In this test, testers receive reports of applications with different levels of authority, allowing testers to find OWASP vulnerabilities. Web penetration testing helps identify vulnerabilities in the web application, such as SQL[16] injection problems, XSS[17], XSRF[18], weak authentication and source code discovery.
- Wireless: A wireless / remote access security test deals with the security risks associated with wireless devices. Some wireless devices are under security threats over the 802.11 wireless network and broadband Internet access. Precautions should be taken to ensure the architecture, design and installation of such solutions are safe. The wireless / remote access survey is used to assess the security level of an organization using mobile workforce. To ensure the efficient management of a unified risk management, it is essential to contribute to the design and installation of the architecture, solutions.
- Phone Security: In addition to TCP / IP networks, other communication networks that can be used for an attack can also be used. These include telephone and fax networks, mobile wireless networks. The telephone security test deals with voice security issues considering technologies. Penetrating testers may try to make calls to the PBX[19] at the expense of the target, or check the installation and security of the mailbox, voice over (VoIP[20]) integration, unauthorized modem usage, and related risks. Telephone Security Assessment helps you assess security issues related to company sound technologies. There are many modem vulnerabilities, such as the modem's permission

[13] Java Platform, Enterprise Edition (Java EE), formerly Java 2 Platform, Enterprise Edition (J2EE), is a set of specifications, extending Java SE with specifications for enterprise features such as distributed computing and web services. Java EE applications are run on reference runtimes, that can be microservices or application servers, which handle transactions, security, scalability, concurrency and management of the components it is deploying.

[14] ASP.NET is an open-source server-side web application framework designed for web development to produce dynamic web pages. It was developed by Microsoft to allow programmers to build dynamic web sites, web applications and web services.

[15] PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language. Originally created by Rasmus Lerdorf in 1994, the PHP reference implementation is now produced by The PHP Group. PHP originally stood for Personal Home Page, but it now stands for the recursive acronym PHP: Hypertext Preprocessor.

[16] Structured Query Language is a domain-specific language used in programming and designed for managing data held in a relational database management system or for stream processing in a relational data stream management system.

[17] Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications. XSS enables attackers to inject client-side scripts into web pages viewed by other users.

[18] Cross-site request forgery, also known as one-click attack or session riding and abbreviated as CSRF or XSRF, is a type of malicious exploit of a website where unauthorized commands are transmitted from a user that the web application trusts. There are many ways in which a malicious website can transmit such commands; specially-crafted image tags, hidden forms, and JavaScript XMLHttpRequests, for example, can all work without the user's interaction or even knowledge.

[19] A PBX (Private Branch Exchange) is a system that connects telephone extensions to the Public Switched Telephone Network and provides internal communication for a business. An IP PBX is a PBX with Internet Protocol connectivity and may provide additional audio, video, or instant messaging communication utilizing the TCP/IP protocol stack.

[20] Voice over Internet Protocol (also voice over IP, VoIP or IP telephony) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet.

and unauthorized use. For example, Wardialisation[21] allows malicious users to detect and access modems. Abuse by unlawful outsiders to the bundle is by way of calling for the target costs, an important element of the telephone penetration test.

- Physical: Nowadays security systems such as firewalls, etc. They are widespread and the configuration of these systems usually provides a high level of security, which means that it is extremely difficult, but it is not impossible for such systems to have an attack to have an adverse effect. It is often easier and faster to obtain the required or required data if these systems can be avoided by a direct physical attack. Physical attack, such as data, directly accesses a non-password-protected workstation after unauthorized access to the building and/or server space.
- Social Engineering: People are often the weakest link in the security chain, so social engineering techniques that take advantage of inadequate security skills or insufficient security awareness are often successful. Such tests are appropriate after the introduction of a general security policy, for example, to examine the extent of its implementation and/or acceptance. Fake assumptions about the alleged effectiveness of the security policy often result in security risks that, if the situation is accurately assessed, can be mitigated by taking further steps. Social engineering is a technique that attackers use to exploit human vulnerabilities within the network. Social engineering is a process where people use weaknesses and friendships. Testers can use techniques such as eavesdropping, crawl of employees' passwords, and access to access codes through people's observation. Social engineering is the use of influence and persuasion to mislead people into information exchange. Often people call hacking. Social engineering techniques use psychological tricks to obtain sensitive information such as contact addresses, passwords, usernames, and credit card information. The human tendency for help and trust can be utilized in a variety of ways to gather information. Depending on the environment or the circumstances, social engineering is implemented through a computer-based or direct relationship. The information can come from the garbage or from a street sweeper. Some social engineering tricks include, for example, false phone calls, email fraud, and phishing. Techniques include making counterfeits such as offering cash or prizes in a mailbox or questioning seemingly innocent questions that can reveal personal information. A good social engineering conducts background research at the organization to get acquainted with the basic nature of the company and even the name of a few employees. Such information will help attackers gain physical access to the organization's information systems by circumventing controls by stealing important information. [5]

Starting point

The starting point of the penetration test, that is where the penetration tester's computer is connected to the network or where attack attempts come from, may be inside or outside the client's network or building.

[21] War dialing or war dialing is a technique to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for modems, computers, bulletin board systems (computer servers) and fax machines. Hackers use the resulting lists for various purposes: hobbyists for exploration, and crackers – malicious hackers who specialize in breaching computer security – for guessing user accounts (by capturing voicemail greetings), or locating modems that might provide an entry-point into computer or other electronic systems. It may also be used by security personnel, for example, to detect unauthorized devices, such as modems or faxes, on a company's telephone network.

- Most hackers are attacked through the network's Internet connection. The penetration test can detect and assess the potential risk of such an attack from the outside. Usually, the firewall and system of DMZ and RAS[22] connections are tested in such tests.
- From the inside of the intrusion test, the tester should not normally overwrite firewalls or access controls to access internal networks. Therefore, an internal test can assess the impact of a firewall configuration, a successful attack on the firewall, or attacks on people who have access to the internal network. [6] [7]

CONCLUSIONS

Everyday use of the information society and info communication tools and the basic existence of security requirements is a general thing. This is the consciousness, the armed mind of public finances, education, finance and almost every organization. Ensuring the security of info communication networks is ensured in a fundamental part of the systems. One of the most popular test methods, which is mainly a technical and technological approach, is to penetrate the test. This publication based on and examining international standards, contains a self-classification approach for the penetration test. Possible classification will hopefully facilitate the preparatory phase of such tests and suggest a test for the relevant info communication system.

Of course, in the first place, it is necessary to understand the basic concepts, characteristics, and types of tests that can be performed during a penetration test. The classification method published in the publication is not mandatory, it only gives one possible categorization to promote the tests.

BIBLIOGRAPHY

[1] OSSTMM 3 – The Open Source Security Testing Methodology Manual, December 14, 2010. p.37.

[2] 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.

[3] FEDERAL OFFICE FOR INFORMATION SECURITY (BSI) STUDY: *A Penetration Testing Model;* Bonn p.15.

[4] FEDERAL OFFICE FOR INFORMATION SECURITY (BSI) STUDY: *A Penetration Testing Model;* Bonn p.16.

[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) pp.27-30.

[6] Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1A ,2006

[7] Information Systems Security Assessment Framework (ISSAF) Draft 0.2.1B , Penetration testing Framework (PTF), 2006

[22] A remote access services (RAS) is any combination of hardware and software to enable the remote access tools or information that typically reside on a network of IT devices. A remote access service connects a client to a host computer, known as a remote access server. The most common approach to this service is remote control of a computer by using another device which needs internet or any other network connection.

[8] Karen Scarfone Murugiah Souppaya , Amanda Cody, Angela Orebaugh -Technical Guide to Information Security Testing and Assessment, Special Publication 800-115 Computer Security Division Information Technology Laboratory National Institute of Standards and Technology Gaithersburg, MD 20899-8930 September 2008