Y. Zh. Aitkhozhayeva¹, A. A. Ziro¹, Zh. A. Zhaibergenova¹, A. G. Baltabay²

¹Kazakh National Research Technical University named after K. I. Satpayev (Satbayev University), Almaty, Kazakhstan,
²School of Control and Computer Engineering, North China Electric Power University, Beijing, China. E-mail: ait_djam@mail.ru, ziro.aasso@gmail.com, zhanshuak@gmail.com, aliya250892@gmail.com

**PENETRATION TESTING**

**Abstract.** Detection of vulnerabilities is an important composite component of both internal and external audit of information security systems. Potential internal vulnerabilities can be revealed by testing for penetration. At the same time, both the commercial and being in the free access instruments of penetration test are used differently. The review of recognized methodologies (standards) of conducting testing for penetration is made. The list of free distribution kits of instruments of penetration test is provided. One of the widespread attacks is BackDoor allowing to receive control over the attacked system. With the help of the utility of Msfvenom which is a part of a free distribution kit of penetration test Kali Linux with methodology of PTEs the attack of BackDoor by implementation of an exploit is successfully realized. Control over the attacked virtual machine was as a result received.

**Keywords:** vulnerabilities, penetration testing methodology, BackDoor attacks.

**Introduction.** Now there was the standard international practice of support of the mode of the information security (IS), one of the stages of which is audit of the IS systems. Existence of management system of IS (Information Security Management), and in particular audit of management system of IS (Risk Management), is an indispensable condition of the organization of the IS mode at the enterprise.

IS audit is carried out by a team of security experts of enterprise systems and experts in the field of management. One of the methods in case of the active audit of information security systems is testing for penetration. Testing for penetration - the valuation method of safety of computer systems or networks of the attack of the malefactor (etic hacking - ethical hacking). Testing for penetration is an integral part of the analysis of security of any information resource. The authorized search of vulnerabilities of protection system is execute and their subsequent use for penetration into subject to protection. The purpose of penetration test is independent assessment and the expert opinion on a status of security of the critical information. The recommendations about closing (elimination) of the found vulnerabilities are whenever possible formulated. As a result, security concerns which need to be solved urgently come to light. There is a certification of CHE (Certified Ethical Hacker) for experts in the field of conducting testing for penetration which is recognized around the world today and confirms existence of appropriate level of knowledge. The certified examination of EC-Council CEH approved by the U.S. Department of Defense is one of recognized for experts of IT safety. State structures of the USA require existence of this certificate for certain positions of IS that once again emphasizes importance of penetration test as instrument of the active audit.


The offered methodologies differ on steps of conducting testing, types of testing for penetration, detailing of testing objects, determination of testing procedures, the description of utilities for conducting testing, a formulating, structure, a detail of description of a technique and purposes of penetration testing.

PCI DSS is oriented on a penetration testing for the organizations which processing, storing and transferring data of card owners. OSSTMM is one of the first techniques of complex testing of information security of the organization. In methodology of NIST different recommendations about testing types are described, there is in the separate document an operation methodology with a fire-wall (NIST SP 800-41 Guideline on Firewalls and Firewall Policy). The detailed methodology of BSI provides both technical and organizational aspects of testing, and legal aspects. ISSAF describes assessment of safety of fire-walls, routers, anti-virus systems and many other things. Methodologies of PTES and OWASP are well structured therefore they are widely used when testing for penetration. PTES is model which was used in the system of a penetration testing Rapid7 Metasploit.

Tools. Penetration test is subdivided on external and internal. External infrastructure penetration test is an analysis of perimeter from the Internet. The expert makes attempts, trying to compromise available network services and to develop the attack which main goal is to get in system. Internal infrastructure penetration test is a simulation of action of the insider. As the insider the infected node in a network can appear.

In turn external penetration test is conditionally divided into categories: network scanners, scanners in web scripts, exploits, automation of injections, debugger. There are both separate programs, and distribution kits (commercial and free) for conducting testing for penetration.

Usually distribution kits represent the processed versions existing Linux distribution kits.

The most known of them which are in the free access [9]:
- BlackArch Linux, a distribution kit is based on Arch Linux. Includes 1359 utilities for testing for penetration, it is intended for professionals, maintains architecture of i686 and x86_64;
- Parrot Security OS, is based on Debian Linux, the easy and effective testing tool on penetration, idle time in mastering;
- BackBox, is based on Ubuntu Linux, is convenient for private use, and has rather good functionality for daily use;
- Pentoo, is based on Gentoo Linux, contains a set of security-utilities;
- Network Security Toolkit, is based on Fedora Linux, intended for the analysis of safety of a network, gives simple access to a wide set of the opened network applications, many of which are included in one hundred the best security aids recommended by the website insecure.org;
- DEFT Linux, is founded on Lubuntu, has the convenient graphic interface, includes antivirus, the systems of information search in a browser cache, network scanners and utilities for detection of rootkits, tools for search of the hidden data on a disk;
- Samurai Web Security Framework is intended for testing for penetration of different web applications. It is delivered in the form of an image of the virtual machine which contains the most popular Open Source of the utility for information collection and carrying out different attacks to web applications;
- Santoku Linux, is based on Ubuntu Linux. It is intended for the analysis of mobile devices and applications: carrying out the analysis of safety, extraction of data, the reverse engineering, forensic, also contains development tools. It is provided only for the X64 platform;
- WifiSlax, is based on Slackware Linux, intended for check of safety of the WiFi networks systems and carrying out the criminalist analysis. It is used for audit of Wi-Fi of networks as the majority of popular utilities for the analysis of security of wireless networks are included in it, maintains the majority creates network interface cards;
- Kali Linux, is based on Debian Linux, includes more than 600 security-utilities (Wireshark, Nmap, Armitage, Aircrack, Burp Suite, etc.) and multilingual support. There are several types of this distribution kit for different platforms: x86 and ARM systems, systems of virtualization, mobile platforms (Kali Net hunter).
Results. Kali Linux – the most popular and advanced distribution kit for conducting testing for penetration and security audit today [10]. The special kernel of Kali Linux is protected from injections that allows to book audit of wireless networks safely. Kali Linux maintains a large number of wireless devices, is compatible to USB and other wireless devices.

In [11] risks and threats of virtualization and results of detection of vulnerabilities of the virtual machines by port scanning by means of the utility of Wireshark from the Kali Linux distribution kit were presented.

Also the utility of Msfvenom is a Kali Linux part by means of which it is possible to realize the attack of BackDoor, having created an exploit. Successfully realized attack of BackDoor allows to implement on the attacked computer the small program through which it is possible to collect confidential data, to control far off an operating system and the computer in general, to use the cracked computer for scanning of a network, carrying out network attacks of network hacking. Usually in case of this attack two programs are used. The program of control is installed on the computer of the tester and controls other program which is illegally set on the attacked computer.

The exploit uses vulnerabilities of the attacked system to violation of its safety. There is an open database of exploits (The Exploit Database) and the appropriate vulnerable software. The basis is created and supported for testers on penetration and researchers of vulnerabilities. There are also closed databases in which the most interesting exploits are collected. Access to them can be or paid, or for a certain circle of people. To one of examples can serve the tool for testing for penetration – Metasploit Exploitation Framework. It contains a big basis of exploits. There are two Metasplot versions, free and paid. There are websites on search of exploits, such as The Exploit Database, WPScan Vulnerability Database (a fresh basis of exploits for Wordpress) and Packet Storm (the most different fresh exploits).

With the help of the utility of Msfvenom which is a part of a free distribution kit of penetration test Kali Linux with methodology of PTES the attack of BackDoor was organized. As attacked the virtual machine was used. With the help of Msfvenom the special program - an exploit (exploit) with the .exe format is created. Implementation of this program in the attacked computer, gives to the malefactor access to the virtual machine and means of the user.

During creation of an exploit it is necessary to specify the IP address of the attacking machine, the port and the place of saving the file of an exploit in the attacking machine. To learn the IP address, it is possible to use the ifconfig command. This command will issue information on a configuration of the attacking machine, including the IP address - 192.168.209.138 (figure 1).

![Figure 1 – Configuration of hacking machine](image)

We use data retrieved during creation of an exploit: we specify the IP address of the attacking machine (192.168.209.138), the port (5566), the place of saving and file name of an exploit (attack.exe). The exploit is created on the x86 platform, file size 73802 bytes (figure 2).

After creation of an exploit we will send it to the virtual machine Windows 7 via the Internet. For example, through e-mail, explaining attacked that it is the useful program.

Further on the attacking machine we will launch metasploit framework (figure 3).

Then we register the IP address of the attacking machine and on what port there will be a connection with the implemented exploit (figure 4).

Attacked launches an exploit by the machine, thinking that it is the useful program.
Figure 2 – Creation of exploit

Figure 3 – Start of metasploit framework

Figure 4 – Configuration of linking with exploit

Figure 5 – Link with exploit

Figure 6 – Messages from exploit
By this time by the attacking machine it is necessary to open a session of connection with an exploit (figure 5).

Now the virtual machine under monitoring of the attacking machine (figure 6).

Conclusion. Innovation, organization, and sophistication - these are the tools of cyber attackers as they work harder and more efficiently to uncover new vulnerabilities [12]. With the help of testing for penetration it is possible to be ahead of malefactors, having revealed and having eliminated vulnerabilities before real cyber-attack. Now penetration test is a mandatory component of both internal and external audit. Free products of penetration testing are easy to use. They allow identifying vulnerabilities on the channel, network and transport layers, having built-in expert systems. When solving problems at the application level, these products unusable. In this case necessary to use commercial solutions (commercial versions Nessus and Rapid 7 NeXpose, Xspider 7, Retina Nenwork Security Scanner, SAINT and etc.) [13-16]. Commercial products of the penetration testing use more advanced technologies and have extended capabilities compared to free ones. This provides additional opportunities in assessing risks and threats. Penetration testing should be performed on both the channel, network and transport layers, and at the application level.

REFERENCES


TESTIROVANIE NA PRONIKNOVENIE

Annotation. Vывление уязвимостей является важной составной компонентой как внутреннего, так и внешнего аудита систем информационной безопасности. Потенциальные внутренние уязвимости могут быть выявлены тестированием на проникновение (пентест). При этом испытываются различные, как коммерческие, так и находящиеся в свободном доступе инструменты пентеста. Сделан обзор признанных методологий (стандартов) проведения тестирования на проникновение. Приводятся перечень бесплатных дистрибутивов инструментов пентеста. Одной из распространенных в России является атака BackDoor, позволяющая получить контроль над атакуемой системой. С помощью утилиты Msfvenom, входящей в состав бесплатного дистрибутива пентеста kali Linux, по методологии PTE5 реализована атака BackDoor путем внедрения эксплойта. В результате был получен контроль над атакуемой виртуальной машиной.

Ключевые слова: уязвимости, методологии тестирования на проникновение, атаки BackDoor.

Information about authors:
Aitkhazhayaeva Yevgeniya – associate professor of the Department of Information Security, Candidate of Technical Sciences, Kazakh National Research Technical University named after K. I. Satpayev, Almaty, Kazakhstan; ait_djam@mail.ru; https://orcid.org/0000-0002-5961-8556
Ziro Aasoo – Master of Technical Sciences, senior-lecturer of the Department of Information Security, Kazakh National Research Technical University named after K. I. Satpayev, Almaty, Kazakhstan; ziro.aasoo@gmail.com; https://orcid.org/0000-0002-5952-877X
ZHaibergenova Zhanshuak – Master of Technical Sciences, tutor of the Department of Information Security, Kazakh National Research Technical University named after K. I. Satpayev, Almaty, Kazakhstan; zhanshuak@gmail.com; https://orcid.org/0000-0002-4775-8877
Baltabai Aliya – Master of Military Sciences, master student at North China Electric Power University, Beijing, China; aliya250892@gmail.com; https://orcid.org/0000-0002-9145-0992