Proceedings of Online International Conference on Advances in Technology, Social Sciences and Humanities
Organized by Novateur Publications, Pune, Maharashtra, India
JournalNX- A Multidisciplinary Peer Reviewed Journal
ISSN: 2581-4230, Website: journalnx.com, July 11th and 12th 2020.

DETECTING VULNERABILITIES IN CORPORATE NETWORKS

Makhmudov Abdukhalil,
[*]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi,
Faculty of Vocational Education in the field ICT, student
maxmudovabduhalil@gmail.com

Aliyeva Zarina
[**]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi,
Faculty of Vocational Education in the field ICT, student
zarina_aliyeva_97@bk.ru

Annotation. The main purpose of security systems is to determine vulnerabilities of network. These systems perform extensive research to specify the vulnerabilities that may lead to security policy breaches. The article discusses some of the vulnerabilities in the system, their origin, level of risk and ways to overcome them.

Key words: vulnerabilities, snapshot, passive, active, hacking, security analysis systems, scan, banner check, active checking, exploit check

Nowadays the results of the security analyzing methods represent a "snapshot" of system's protective status. As these systems cannot detect an attack during their development, they can define potential abilities for the attack. Security analyzing technology is an effective way to implement network security policies before breaking of organization outside or inside. One of the options of classifying vulnerabilities can serve to reflect as a classification of the information system's life cycle stage. (Table 1)

Table 1

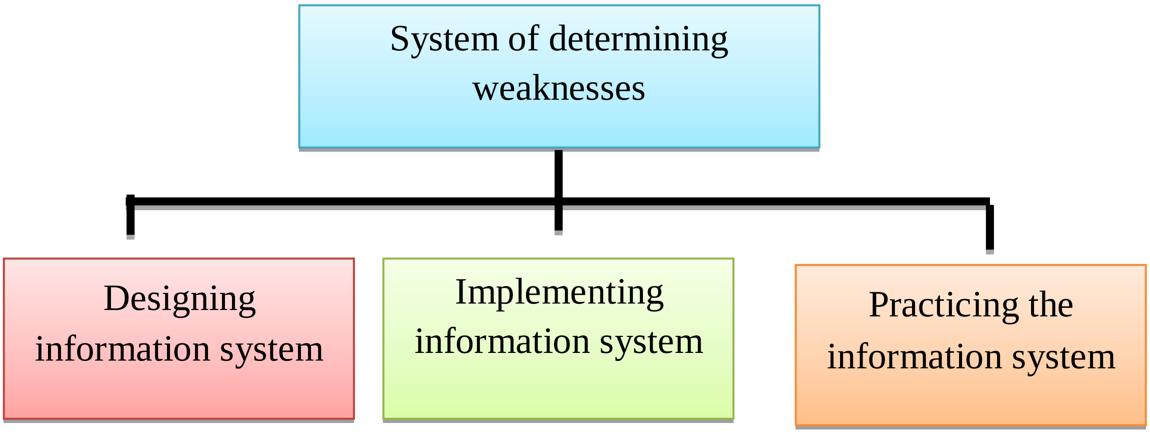
	Planning stages of the Information system	Possible weaknesses in the information system.
1	Designing the Information system	Weaknesses in the designing process
2	Implementing information system	Weaknesses in implementation
3	Practicing the information system	Weaknesses in software or hardware configuration

The weaknesses in the designing process is one of the most troublesome vulnerabilities, identifying and eliminating these kinds of vulnerabilities are very difficult. In this case, the vulnerability is inherent to the project or algorithm and therefore implementing it perfectly (in principle not possible) will not eliminate the vulnerability that is imposed on it.

The second kind of weakness is an algorithmic errors in a software or errors of hardware. Identifying and eliminating these kinds of vulnerabilities are very easy. It may be eliminated by renewing a digital code or changing source text of the weak software.

The last cause of vulnerabilities is an errors of configuration in software or hardware for example , using old versions of telnet service, "weak" passwords or passwords less than 6 symbols, incorrect settings on servers, unnecessary ports open, and the others. Determining and fixing these kind of vulnerabilities do not take much time

Security analyzing systems can be classified according to the types of vulnerabilities which are identified by them (scheme 1)


System of determining weaknesses
Designing information system
Implementing information system
Practicing the information system

Scheme 1

The second and the third classes of security analyzing systems are most common among users. There are several additional classifications for these systems. For example, testing software and managing analyzes of source text and executable code of system, and so on.

Software codes which are open, is not given to the organization. That is why the systems of searching vulnerabilities are more important

The attack simulation systems detect not only their vulnerabilities, but also detect vulnerabilities in their exploitation. Security analyzing systems, particularly implementing and detecting vulnerabilities in exploitation, can be in all levels of any company's infrastructure of information, including network level, operating system, software level. It is the most common way of analyzing network services and protocol security. It depends on versatility of protocol which is used. In spite of the high-level software, studying and using protocols such as TCP / IP, etc. allows to check the security of corporate network The second most common system is analyzing security of operating systems. It also deals with the versatility and deployment of some operating systems (such as UNIX and Windows). However, as each manufacturer makes its own changes to the operating system (the obvious example is many varieties of the UNIX operating system), OS security analyzing methods primarily analyze the parameters of the whole OS family.

Security analyzing is carried out in two stages:

Passive – an operating system which carries out about application level, analyzes configuration files and system registers for invalid parameters, passwords that do not correspond to security policies, and other system objects for the violations of security policy

Active – often carries out about network level, where scenario of attack is generated, and organized attack to the network, and analyzed the response of system to this attack.

Security analysis systems are mainly used for:

- ➢ Appraising security level of organization;
- ➢ Monitoring the effectiveness of the network, system and software configuration;
- ➢ For testing and certification of software and hardware.

New vulnerabilities always appear and the database of security analyzing systems must be regularly updated for identifying them effectively. Ideally, there should be no distinction between the emergence of vulnerability data and the filling of the detection system database in some **"hacking"** sources. But however how often the vulnerability database is updated, there is a time limit for reporting and checking new vulnerabilities.

Another way to detect vulnerabilities is scanning. **Scan** is a passive analysis mechanism — which tries to detect a vulnerability without any real confirmation. This method is the fastest and easiest to implement. This method is called "logical conclusion" (inference) by the point of view of ISS. According to Cisco, this process identifies open ports which are found on each network device and collects banner-related headings which are found on each port scan.

Every received title is compared to a table of identifying rules, network devices, operating systems, and potential vulnerabilities. On the basis of comparison it will be concluded are there any weaknesses or not.

These mechanisms are implemented in several ways in practice (table 2)

Table 2

Banner check	This mechanism is a series of checks, such as Scan, which gives to conclude based on information of agent's request for its title. A typical example of such verification is analyzing the titles of the Sendmail or FTP server, It helps to know their version and concludes that there is a weakness in it based on this information. However, please note that the administrator can change the title of text which is returned for request.
Active checking	besides it is based on the "scanning" mechanism which are based on "digital scanning" comparing a piece of software with some specific weakness. Similarly, antivirus systems compare scanned software components with virus signatures stored in a dedicated database. The diversity of this method is scanning sums which is carried out by agents who work at the operating system level or checking scanned software
Exploit check	it must find the time of appearing weaknesses to detect some of them. Attacking the system is one of the effective way of identifying weaknesses. "Exploit check" gives an opportunity to simulate real attacks, that is why it is more efficient to detect vulnerabilities in scanned nodes (but speed may decrease).

References

1. Nadeem Ahmad, M. Kashif Habib "Analysis of Network Security Threats and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution". Sweden 2010
2. Steve Manzuik, André Gold, Chris Gatford "Network Security Assessment FROM VULNERABILITY TO PATCH". Canada 2007
3. В.В. Бондарев "Анализ защищенности и мониторинг компьютерных сетей Методы и средства" . Москва 2017