Ministry of Education of the Republic of Belarus
Educational institution
Belarusian State University of Informatics and Radioelectronics

UDC 528.854.2

Nguyen Cong An

TECHNIQUE OF VULNERABILITIES MANAGING IN INFORMATION SYSTEMS

Abstract to master degree thesis

Specialty 7-06-0611-02 Information Security

_____

Supervisor:
Boiprav O.V., Cand. Of Sci. (Tech),
Associate Professor

_____

Minsk 2025

GENERAL DESCRIPTION OF WORK

The Research Aim and Objectives

The purpose of the work is to configure, use the vulnerability scanners OpenVAS, ScanOVAL and analyze the scanning results.

To achieve this goal, it is necessary to solve the following main tasks:

1. Analysis of several vulnerabilities, their assessment.
2. Familiarization with the software for searching for vulnerabilities.
3. Installation and configuration of the OpenVAS vulnerability scanner.
4. Installation and configuration of the ScanOVAL vulnerability scanner.
5. Scanning vulnerabilities.
6. Analysis of the scanning results.
7. Remediation vulnerabilities.

Work Connection with Priority Areas of Scientific Research

The topic of the thesis corresponds to paragraph 6 Ensuring the security of humans, society and the state (means of technical and cryptographic information protection, cryptology and cybersecurity) of the list of priority areas of scientific, scientific-technical and innovative activities for 2021–2025, approved by the Decree of the President of the Republic of Belarus dated 07.05. 2020 No. 156.

Thesis Results Approbation

The main results of the dissertation were reported and discussed at the 59th and 60th Scientific Conference of Graduate Students, Master Students and Students of BSUIR (Minsk, April 17–21, 2023; Minsk, April 22–26, 2024), XXI Belarusian-Russian Scientific and Technical Conference “Technical Means of Information Protection” (Minsk, June 06, 2023).

INTRODUCTION

In the twenty-first century, information resources are becoming the driving force and the main object of all human activities, and the state of channels, networks and server security are gradually becoming the basis for economic development. Complex network technologies are quite vulnerable and therefore very often become a target for attacks by intruders. All this poses new problems for developers and builders of information infrastructure. Some modern forms of business are completely based on network technologies (e-commerce, IP telephony, network providers, etc.) and for this reason are especially vulnerable.

The presence of vulnerabilities in information systems, infrastructure nodes or elements of the information security complex is a big problem for IT and information security departments. Of course, searching for gaps can be done manually, but this will be an extremely labor-intensive process that will take a lot of time with a high probability of not noticing something. Therefore, it is best to use automatic tools to search for vulnerabilities and weak points in the enterprise's information infrastructure, such as security scanners or vulnerability scanners. This paper will consider one of the methods of network security analysis using the widely used vulnerability scanners OpenVAS and ScanOVAL.

The purpose of the work is to configure, use the vulnerability scanners OpenVAS, ScanOVAL and analyze the scanning results.

To achieve this goal, it is necessary to solve the following main tasks:

1. Analysis of several vulnerabilities, their assessment.
2. Familiarization with the software for searching for vulnerabilities.
3. Installation and configuration of the OpenVAS vulnerability scanner.
4. Installation and configuration of the ScanOVAL vulnerability scanner.
5. Scanning vulnerabilities.
6. Analysis of the scanning results.
7. Remediation vulnerabilities.

OpenVAS and ScanOVAL help security engineers detect and manage vulnerabilities in information systems, thereby promptly fixing and closing vulnerabilities to help prevent external attacks and ensure system safety.

MAIN PART

The first chapter introduces the concept of vulnerabilities in information systems, common types of vulnerabilities today, and learns more about specific vulnerability information through the "CVE dictionary". This chapter also introduces some software analysis for vulnerability detection in information systems such as: Nessus, Max Patrol, OpenVAS, ScanOVAL. OpenVAS and ScanOVAL are chosen for development in this study.

The second chapter presents the configuration procedure for the OpenVAS vulnerability scanner. This chapter details the steps to download, install, and run a scan on a Windows server using VirtualBox and on Kali Linux. The appliance can use two different approaches to scan a target: Simple scan or authenticated scan using local security checks. The following steps have to be executed to configure a simple scan:

– Step 1. Creating a target.

– Step 2. Creating a task.

– Step 3. Running the task

This chapter also details the vulnerabilities scanned on Windows 7 and Windows 10, and analyzes the results achieved. OpenVAs provides reports for scanned results in many different formats such as html; xml; pdf... to help save for easy management.

The third chapter presents the installation, setup and scanning steps of the vulnerability scanner ScanOVAL. The detailed steps are as follows:

– Installation and Launch of the Program ScanOVAL;

– Install vulnerability descriptions formatted in the "*scanoval.xml*" file;

– Vulnerability detection;

– Analysis of scan results.

The detected vulnerabilities can be viewed in more detail by clicking on the vulnerability ID, which redirects to the Information Security Threat Database. The program allows you to save the scan results in HTML format on your local computer or any location accessible from your system.

The fourth chapter presents methods to remedy vulnerabilities. In general, the remedy of vulnerabilities will follow the following 4 basic steps: Finding; Prioritizing; Fixing; Monitoring. This chapter also discusses the solutions that OpenVAS and ScanOVAL offer to help remedy vulnerabilities and prevent network attacks from outside as well as inside.

CONCLUSION

During the writing of the thesis, a methodology for searching and analyzing vulnerabilities in information systems was developed [1–A, 2–A]. This methodology shows the procedure for installing the OpenVAS tool on a virtual box and on Kali Linux, which performs scanning on target machines in the local network.

As a result of scanning 2 computers with Windows 7 and Windows 10, 4 vulnerabilities were detected: 2 high-risk vulnerabilities: SMB logins (name and password are the same), SMB server (ms17–010) with port 445/TCP; 1 medium-risk vulnerability (reason – DCE/RPC service with port 135/TCP); 1 low-risk vulnerability (reason – timestamps of packets transmitted via TCP). OpenVAS provides the ability to generate reports on the results of the scan, as well as a connection to the CVE database describing known vulnerabilities. The CVSS system is used to assess vulnerabilities. There are three levels of vulnerability severity: high, medium, and low. Most of the scanned nodes contained medium severity vulnerabilities that could allow a denial of service attack. It is worth understanding that even low severity vulnerabilities can allow an attacker to use them to successfully implement their plans. Timely detection of vulnerabilities and their detailed assessment help us prevent cyber attacks on computers or a company's local network.

ScanOVAL program for automatic software vulnerability testing is provided by ФСТЭК России. The software uses OVAL-descriptions of the information security threat database ФСТЭК России (БДУ ФСТЭК России). Not only that, ScanOVAL also provides reports in HTML format to help individuals or managers easily manage and prevent attackers from attacking the information system.

OpenVas and ScanOVAL both provide solutions to fix and close discovered vulnerabilities, the solutions are classified as follows:

– Vendor fix: An official fix or patch released by the vendor that fully resolves the vulnerability;

– Workaround: A configuration change or deployment tweak to avoid exposure until a proper fix is available;

– Mitigation: A change or setting that reduces the risk but does not eliminate the vulnerability;

– Will Not Fix: No fix will be released, often due to the product being deprecated or unsupported.

These solutions are very practical to overcome vulnerabilities, helping to manage information systems safely.

LIST OF OWN PUBLICATIONS

1–A. Nguyen, K.A. Methodology for searching and analyzing vulnerabilities in information systems / K.A. Nguyen // Collection of Abstracts of Reports of the 59th Scientific Conference of Postgraduates, Master's Students and Students of BSUIR, Minsk, April 17–21, 2023. – P. 46–47.

2–A. Nguyen, K. A. Techniques for analyzing information system vulnerabilities / K. A. Nguyen // Technical Means of Information Protection: Abstracts of Reports of the XXI Belarusian-Russian Scientific and Technical Conference, Minsk, June 6, 2023 / editorial board: T. V. Borbotko [et al.]. – Minsk: BSUIR, 2023. – P. 8.

3–A. Nguyen, K. A. Technique of information systems vulnerabilities management / K. A. Nguyen // Information Security: Collection of Abstracts of Reports of the 60th Scientific Conference of Postgraduate, Master's and Undergraduate students of BSUIR, Minsk, April 22–26, 2024. – P. 19–21.