UDC 004.056

TECHNIQUE OF INFORMATION SYSTEMS VULNERABILITIES MANAGEMENT

C.A. Nguyen

group 367311

Belarusian State University of Informatics and Radioelectronics, Minsk, Belarus

Scientific supervisor: Boiprav O.V. – Cand. of Sci. (Tech.), Ass. Prof of Department of IP

Annotation. The report presents the results of the justification and development of the technique
of vulnerabilities searching and analyzing in information systems. This technique is based on the use of the OpenVAS vulnerability scanner and Windows or Kali Linux operating system.

Keywords: vulnerabilities, scanner OpenVAS, network security, CVE, NVD, Windows, Kali Linux.

Introduction. Vulnerabilities, in the context of cybersecurity and software engineering, refer to weaknesses or flaws within a system that could be exploited by attackers to compromise
the security of the system. These vulnerabilities can exist in various components of software, hardware, networks, or even human processes. They create opportunities for unauthorized access, data breaches, denial of service attacks, or other malicious activities. Vulnerabilities have been registered by MITRE as a CVE (Common Vulnerability or Exposure), and assigned a Common Vulnerability Scoring System (CVSS) score to reflect the potential risk it could introduce to your organization. This central listing of CVEs serves as a reference point for vulnerability management solutions.

A vulnerability scanner is a software tool designed to assess computers, networks, or applications for security weaknesses or vulnerabilities. These tools typically automate the process of identifying potential vulnerabilities by scanning for known security flaws in software, configurations, or network infrastructure. Vulnerability scanners can be either passive or active. Passive scanners observe network traffic and analyze it for potential vulnerabilities without interacting with the target system directly, while active scanners actively interact with the target system to identify vulnerabilities.

Several well-known commercial vulnerability scanners are widely used in the cybersecurity industry to assess the security posture of networks, systems, and applications: Nessus, GFI LANguard, XSpider (MaxPatrol). These scanners offer advanced features, comprehensive vulnerability databases, and professional support services. Unlike the listed scanners, OpenVAS, which stands for Open Vulnerability Assessment System, is an open-source vulnerability scanning and management tool. OpenVAS conducts comprehensive scans of network infrastructure, including servers, endpoints, and network devices, to identify security vulnerabilities. It employs various scanning techniques, including remote and authenticated scanning, to detect vulnerabilities in both online and offline systems. The OpenVAS vulnerability database includes about 52,000 checks, the so-called Network Vulnerability Tests (NVTs), as well as a connection to the CVE database, which describes known vulnerabilities. OpenVAS integrates with the National Vulnerability Database (NVD) and other sources of vulnerability intelligence to maintain an extensive database of known vulnerabilities. This enables it to provide up-to-date information on security flaws in software, operating systems, and third-party applications. Due to the indicated advantages of OpenVAS compared to other vulnerability scanners, this software tool was chosen as a tool for developing the technique [1–5].

Main Part. The OpenVAS vulnerability scanner can be installed using VirtualBox as a virtual machine. To do this you need to follow these steps.

Step 1. Set the following parameters of the virtual machine to be installed in VirtualBox: operating system – Other Linux, RAM – 5120 MB, processors – 2, video memory – 9 MB, media – downloadable OVA file, network – network bridge.

Step 2. Complete the virtual machine installation process.

Step 3. Start installed machine and log in using the following login information: login – admin, password – admin.

Step 4. Create a new web administrator account.

Step 5. Open the web browser and enter the IP-address of virtual machine.

Step 6. Log in with the web administrator account created during the installation of the virtual machine.

The OpenVAS vulnerability scanner can also be installed in the Kali Linux operating system distribution. To do this, you need to follow the following steps.

Step 1. Completely upgrade your Kali Linux system by using the: sudo apt update && sudo apt upgrade -y command.

Step 2. Run the following command to download OpenVAS: sudo apt install openvas.

Step 3. Run the OpenVAS installer by running the following command: sudo gvm-setup.

Step 4. Generate a password for the first login.

Step 5. Check the OpenVAS settings by using the following command: sudo gvm-check-setup.

Step 6. Generate a new administrator password.

Step 7. Open the web interface: http://localhost:9293 or http://127.0.0.1:9392.

Step 8. Log in using the following credentials: username – admin, password – the new administrator password generated during installation

Generally speaking, 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.

Conclusion. During testing of the developed technique on 4 computers with operating systems Window 7 and Window 10, 4 vulnerabilities were discovered: 2 high risk vulnerabilities: SMB Brute Force Logins with Default Credentials (username and password are the same), Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (Microsoft MS17-010); 1 medium risk vulnerabilities: DCE/RPC and MSRPC services enumeration reporting; 1 low risk vulnerabilities: TCP timestamps.
It should be noted that OpenVAS provides the ability to generate reports based on the results of the scan performed. Reports can be displayed in the web interface and downloaded in a variety of formats making it easy for developers to use to fix vulnerabilities as well as monitor.

References

1. What are Vulnerabilities, Exploits, and Threats? [Electronic resource]. – Access mode: https://www.rapid7.com/fundamentals/vulnerabilities-exploits-threats/. – Date of access: 09.03.2024.

2. Best Vulnerability Scanning Tools. [Electronic resource]. – Access mode: https://thectoclub.com/tools/best-vulnerability-scanning-tools/. – Date of access: 09.03.2024.

3. OpenVAS. [Electronic resource]. – Access mode: https://www.bugcrowd.com/glossary/openvas-vulnerability-scanner/. – Date of access: 09.03.2024.

4. Greenbone Enterprise Appliance with Greenbone OS 22.04 – Manual // Greenbone AG. 2024. Chapter 5, chapter 10.

5. Kali Linux Install Guide – Greenbone Community Documentation. [Electronic resource]. – Access mode: https://greenbone.github.io/docs/latest/22.4/kali/index.html – Date of access: 09.03.2024.