ASSESSING THE SECURITY OF AN IT&C SYSTEM USING SCAN TESTS

Valentin PAU[1], Dorina Luminița COPACI[2], Constantin Alin COPACI[3]

Abstract. *Cyber security has become a topic of strategic importance both internationally and nationally. In order to protect against cyber threats, it is essential to have an appropriate cyber security management system. The purpose of the present paper is to assess the confidentiality, integrity and availability as well as the security of information by identifying vulnerabilities in the network, in order to comply with the security requirements in accordance with the ISO/IEC 27001 standard.*

Rezumat. *Securitatea cibernetică a devenit un subiect de importanță strategică atât la nivel internațional, cât și la nivel național. Pentru a se proteja împotriva amenințărilor cibernetice, este esențial să se dispună de un sistem adecvat de gestionare a securității cibernetice. Scopul prezentei lucrări este de a evalua confidențialitatea, integritatea și disponibilitatea, precum și securitatea informațiilor prin identificarea vulnerabilităților din rețea, pentru a respecta cerințele de securitate în conformitate cu standardul ISO/IEC 27001.*

Keywords: security, sistem IT&C system , vulnerability, scan tests

DOI [10.56082/ANNALSARSCIENG.2024.2.24](https://doi.org/10.56082/ANNALSARSCIENG.2024.2.24)

1. Introduction

The information security control must be permanent, centralized and specialized in order to deal with the complexity and high danger of information security threats from various sources.

The SR ISO/CEI 27001:2013 standard provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an information security management system [1].

The paper aims at assessing the integrity, confidentiality, availability and security of information, taking into account the security requirements in accordance with the ISO/IEC 27001 standard.

The IT&C infrastructure has the following characteristics:

- 25 computer systems, 5 servers and about 10 specific applications developed with internal and/or external resources and various other commercial applications provided by third-party manufacturers (Adobe Systems Incorporated, Corel

[1]Professor, PhD Academy of Romanian Scientists;
[2] PhD, Titu Maiorescu University, Bucharest;
[3] Engineer, ANCOM, Bucharest;

Corporation, Abbyy, McAfee Inc.). Their number is constantly changing due to ongoing projects.
- it is based on a solution consisting of a virtualized environment with VirtualBox technology.
For practical research, we have used VirtualBox [2] as an implementation of virtualization at the level of the operating system for Linux [3].
In order to identify vulnerabilities in the network, we have used the specialized tools of Tenable Nessus Expert software, version 10.7.3, for Linux [4]. The present paper is based on the results of the scanning process performed using the management solutions of the vulnerabilities in the Nessus application.
The present paper ends with a set of conclusions down from the analyses carried out in the light of the proposed objectives.

2. Identifying threats

This part of the paper identifies the sources of threat to the analyzed system and compiles a list of possible threats that can affect the company.

In the following table, there are indicated some threats and their effects on the functions of security (confidentiality, integrity and availability of information).

Threats	The cyber security objectives that are affected		
	Privacy	**Integrity**	**Availability**
Natural threats			
Earthquake			•
Fire			•
Flooding			•
Storm			•
Deliberate human threats			
Interception and espionage	•		
Introduction of destructive codes	•	•	•
Intentional destruction of data		•	•
Sabotage		•	•
Unauthorized access to data	•	•	
Use of pirated software			•
Identity fraud	•	•	
Unintentional human threats			
Absence of key personnel	•	•	•
Wrong forwarding of messages	•	•	•
Programming errors	•	•	•
Technical defects		•	•
Transmitted errors		•	•
Threats from the operational environment			

Contamination with hazardous substances			•
Voltage drops in power supply			•
Power voltage fluctuations	•		•
Fire/ Flooding			•

3. Types of vulnerabilities and threats that may exploit them

The identification of vulnerabilities and the method used for this purpose depend both on the operational environment of the analysed system as well as on the stage at which the analysed system is located (planning stage, implementation stage, implementation stage, operational phase). The purpose of this step is to identify vulnerabilities and compile a list of them.

Vulnerability is a breach in the design and implementation of network security or in the applied security measures that could be exploited, accidentally or intentionally, by a threat to the system.

In the table below, there are presented some types of vulnerabilities and threats that can exploit them, along with the types of system assets that may be affected.

No. crt.	Vulnerability	Threat	Affected types of goods
1.	Existence of flammable materials	Fire	Auxiliary installations Hardware Data
2.	Lack of backup files	Earthquake Fire Flooding Electronic interference Power fluctuations	Data
3.	Inadequate wiring	Transmission errors	Data
4.	Improper training of staff regarding antivirus protection	Computer hacking	Data
5.	Poor maintenance of auxiliary installations	Technical malfunctions	Hardware
6.	Inappropriate Firewall policies	Unauthorized data access Data destruction Unauthorised Software Theft and fraud	Data
7.	Absence of identification and authentication mechanisms	Unauthorized access	Hardware Software Data
8.	Lack of physical security	Fire Data destruction	Hardware Data

In order to identify computer vulnerabilities, it is used the CVE - Common Vulnerabilities and Exposures public database representing the Standard for the Name of Computer Security Vulnerabilities [5].

4. Method of security analysis and evaluation

For security testing, security penetration tests have been performed using the specialized tools of the Tenable Nessus Expert version 10.7.3 application.

In the present paper, reference will be made to the results of the scanning process performed with Nessus vulnerability management solutions.

The operating system on which Tenable Nessus Expert has been installed is Linux Debian (Figure1):

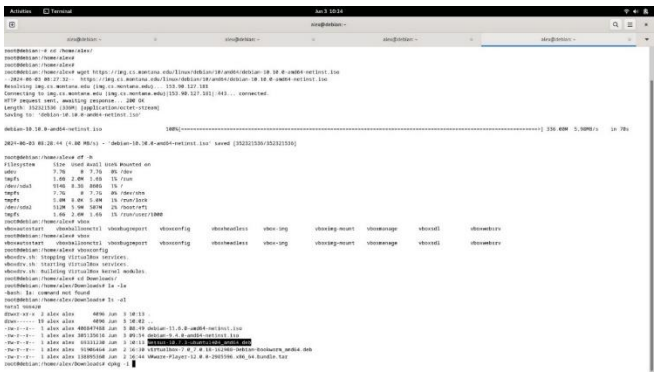

Figure 1. Tenable Nessus Expert Installing

A number of CVE-compatible vulnerabilities (Common Vulnerabilities and Exposures) have been identified.

Different software versions, missing upgrades, expired security certificates are some of the IT problems, but they are also part of security in general. If exploited, they may affect the credibility of the institution in the eyes of third parties.

In the Nessus reports, in addition to CVE vulnerabilities, there is also general information aimed at raising a red flag or informing.

The test result in the case of each publicly scanned IP highlights the number of identified vulnerabilities, their type, their manner of realization, their CVE code, as well as the primary recommendations for remediating vulnerabilities.

One of the VirtualBox virtual machines, which is going to be scanned, is configured as a database server on Linux Debian 10 operating system. On another virtual machine, Apache2 has been installed on Debian 11 as a web server.

High, medium, low level vulnerabilities are identified for the chosen IPs (Figure 2, Figure 3, Figure 4).

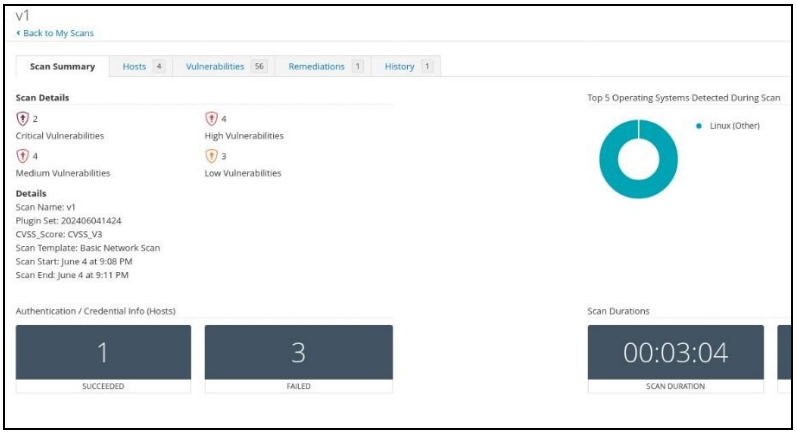

Figure 2. General information about scanned items

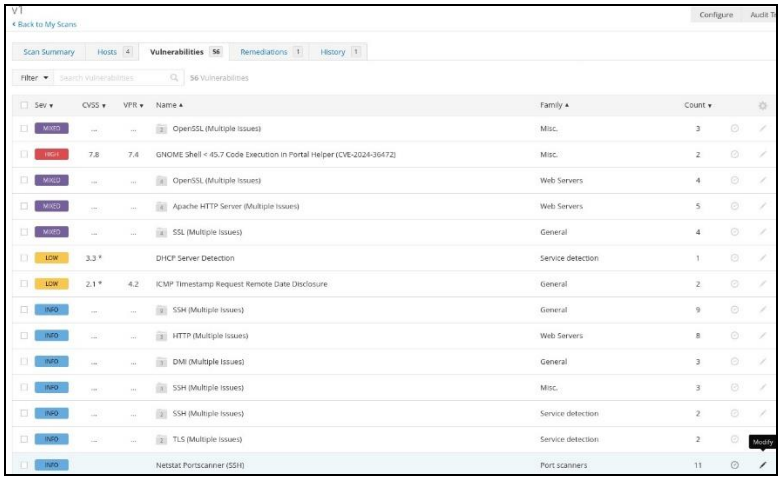

Figure 3. Vulnerabilities discovered after scanning

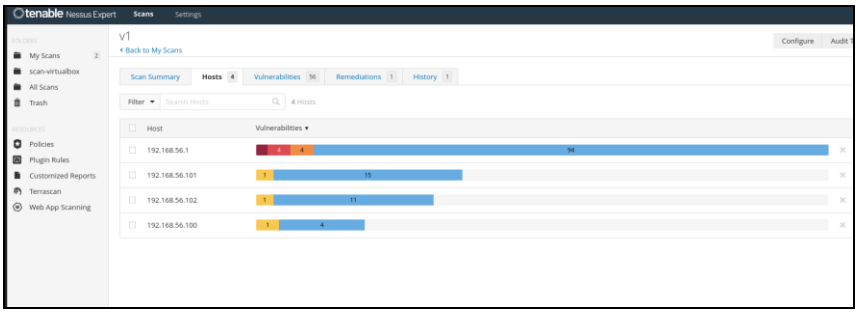

Figure 4. Vulnerabilities found on every scanned IP

For example, in the case of IP 192.168.56.1, 1 critical vulnerability, 3 high-grade vulnerabilities, 4 medium-grade vulnerabilities were found.

The critical vulnerability is 182259 – OpenSSL SeoL (1.0.2.x) and it refers to an old OpenSSL version installed on this machine. It is recommended to update the OpenSSL version (Figure 20).

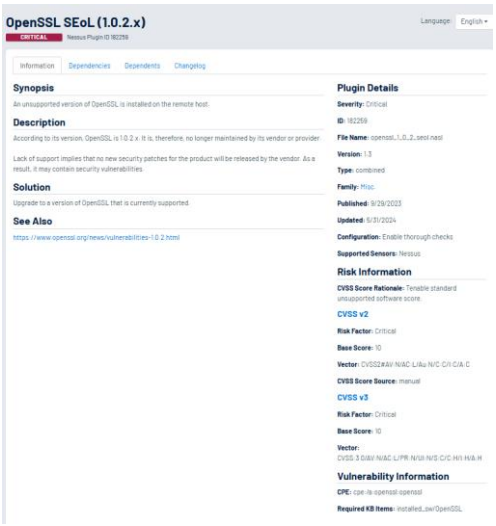

Figure 20. Critical vulnerability OpenSSL SeoL (1.0.2.x)

The main identified vulnerabilities refer especially to very old versions of the software which has been installed in routing/switching equipment or on servers that have not been updated /maintained.

The main recommendations are: more recent versions of the installed software, upgrades, closure of some services as a result of an internal analysis which validates this approach, checking rights and access, etc.

5. Conclusions

The present paper presents simulation scenarios regarding the security assessment of an IT&C system, using network scanning tests.

The scanning tests carried out have revealed a high number of vulnerabilities with major, medium and minor risks that require a proper approach, an implementation of security measures as well as the repetition of these security measures in the coming period.

R E F E R E N C E S

[1] ISO/IEC 27001:2013. Information technology - Security techniques - Information security management systems – Requirements;

[2] Oracle VirtualBox User Manual Version 4.3.40" (PDF). Retrieved 2023-11-10. https://download.virtualbox.org/virtualbox/4.3.40/UserManual.pdf;

[3] "Linux kernel licensing rules". Linux kernel documentation. Archived from the original on September 6, 2022. Retrieved June 17, 2022. https://www.kernel.org/doc/html/v4.18/process/license-rules.html;

[4] https://docs.tenable.com/nessus/Content/InstallNessusLinux.htm;

[5] http://cve.mitre.org/;

[6] https://www.virtualbox.org/ ;

[7] https://docs.tenable.com/nessus/Content/InstallNessusLinux.htm;

[8] https://legislatie.just.ro/Public/;

[9] https://www.iso.org/standard/27001;

[10] V. Pau, D.L. Copaci, C. A. Copaci: “Cyber security: an attack graphs perspective”, Vol. 15, Number 2/2023, Annals of the Academy of Romanian Scientists Series on Engineering Sciences, Series on Engineering Sciences, ISSN 2066 – 8570.