Introduction of Cybersecurity Vulnerability Management System for NPPs

Taejin Kim[a*], Gwang Seop Son[a], Young-Jun Lee[a], Jae Gu Song[a], Jae Hwan Kim[a]
[a] *Korea Atomic Energy Research Institute, 111, Daedeok-daero 989beon-gil, Yuseong-gu, Daejeon 305-353, Republic of Korea*
[*] *Corresponding author: taejinkim@kaeri.re.kr*

***Keywords :** cybersecurity, cyber vulnerability, vulnerability management,* cyber threats

1. Introduction

While it had previously seemed that an industrial control system (ICS) in nuclear power plants (NPPs) is considered safety from cyberattacks, the cyberattacks occurred in the nuclear facilities over the last few years highlight the necessity of implementing cybersecurity measures. In South Korea, technical standards for cyber security of nuclear facilities [1] and critical digital assets (CDAs) [2] have been established. All digital assets in NPPs must be evaluated in accordance with KINAC/RS-019 [2], and identified CDAs must comply with the cybersecurity program specified in KINAC/RS-015 [1]. Therefore, licensees have to manage vulnerabilities in critical digital assets. The vulnerability management includes a series of process to scan, analyze, and resolve vulnerabilities in digital assets. However, it is difficult to manage vulnerabilities because vulnerabilities are constantly being discovered and the results of potential vulnerability identification for digital assets can vary significantly dependent on the capabilities of each company or individual performing the assessment. Thus, systematic cybersecurity vulnerability management is essential. In this paper, we introduce a cybersecurity vulnerability management system for APR1400.

2. Review on Current Vulnerability Management System for OT environments

In operational technology (OT) environments, representative vulnerability tools are tenable OT security [3], nozomi networks guardian [4], dragos platform [5], etc. The commercial OT vulnerability tools conduct passive scanning to detect vulnerabilities. The passive scanning identifies potential vulnerabilities and generates alerts by comparing the collected software and firmware versions with Common Vulnerabilities and Exposures (CVEs), but it does not validate CVEs through direct exploitation attempts. Thus, there are limitations in finding valid CVEs when relying solely on the tools. In order to accurately identify valid vulnerabilities, cyberattacks based on CVEs must be conducted through a separate process outside the scope of the tools.

Another issue with applying commercial OT vulnerability tools to NPPs is that they only support standard Industrial Control System (ICS) devices and protocols. Since customized operating systems and protocols are generally used in NPPs, they are not properly operational. Thus, introducing commercial OT vulnerability tools to NPPs is not effective in terms of managing identification, assessment, and resolution of vulnerabilities.

3. Cybersecurity Vulnerability Management System for APR1400

A vulnerability management system can be utilized in the process of identification and assessment for targeted digital assets. Vulnerabilities of targeted digital assets should be collected in the system, and the vulnerabilities should be gathered based on operating systems of the digital assets. In this section, the cybersecurity vulnerability management system, which is developed for APR1400, is introduced.

3.1 Configuration and Function

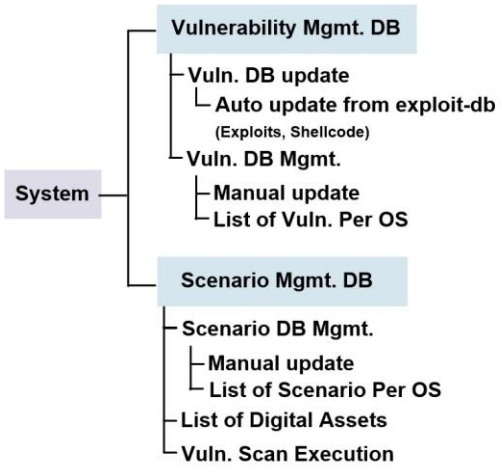


Fig. 1. Configuration of cybersecurity vulnerability management system

The configuration of the cybersecurity vulnerability management system for APR1400 is represented in Fig. 1. The system largely consists of vulnerability

management database and scenario management database and includes vulnerabilities of representative operating systems for APR1400.

The vulnerability management database gathers exploits and shellcode from Kali Linux (Exploit-db.com) and the vulnerability list can be managed by a security administrator.

The scenario database includes all scenarios which have been utilized for cyberattacks on the targeted digital assets. Also, it also lists all targeted digital assets and provides a feature for automatically executing a cyberattack with the scenarios.

3.2 Vulnerability Management Database

The vulnerability management database (DB) consists of two main pages: a) vulnerability DB update and b) vulnerability DB management. The vulnerability DB update in Fig. 2 automatically retrieves exploits and shellcodes registered in Kali Linux (Exploit-db.com) [6] and updates the list on this page. A security administrator can delete vulnerabilities on this page when necessary and download them to the vulnerability list on vulnerability DB management page.

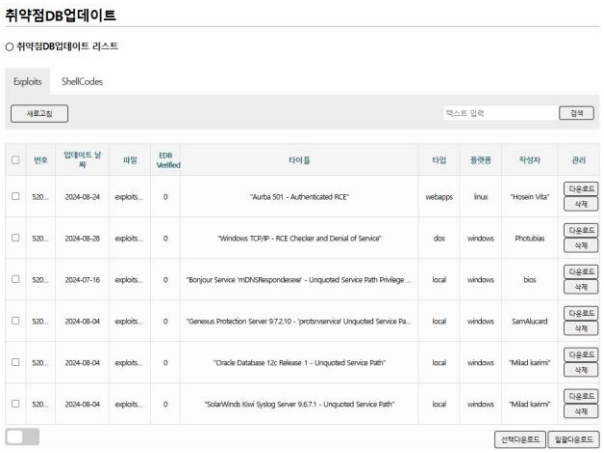


Fig. 2. Vulnerability DB update page

The vulnerability DB management in Fig. 3 is updated from the vulnerability list on the vulnerability DB update upon an approval of a security administrator. Vulnerabilities of each operating system are categorized into separate tables. It also has a provision to manually add vulnerabilities. For example, a security administrator can manually add vulnerabilities, such as those from NIST's National Vulnerability Database (NVD), using excel format.

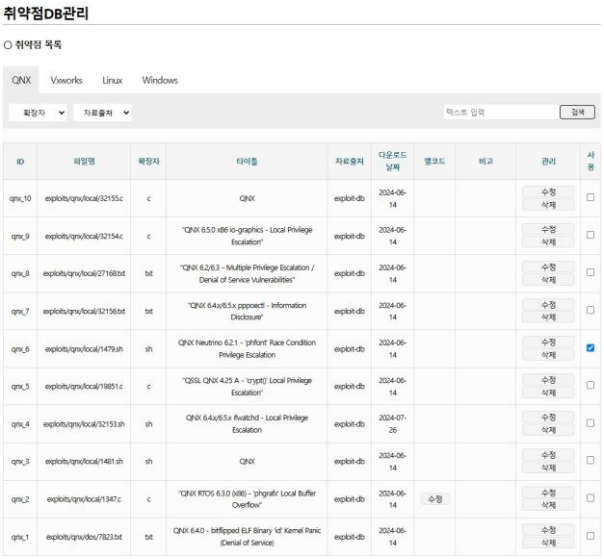
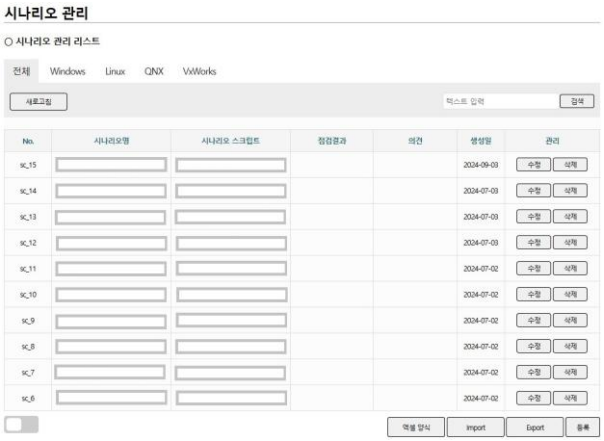


Fig. 3. Vulnerability DB management page

3.3 Scenario Management Database

The scenario management database consists of three main pages: a) Scenario DB management, b) List of digital assets, and c) Vulnerability scan execution. The scenario DB management Fig. 4 include scenario scripts which can be used to attack targeted digital assets. The scenario scripts have been developed through penetration testing for each digital asset. The list of scenario scripts is manually managed by a security administrator.



- For security reasons, the scenario title has been masked

Fig. 4. Scenario DB management page

The list of digital assets in Fig. 5 contains targeted digital assets along with their IP addresses and port numbers for cyberattack testing. In this page, basic attacks such as Nmap scans, flooding, and others can be executed.

Fig. 5. List of digital asset page

The vulnerability scan execution in Fig. 6 provide a function to execute cyberattack using a selected scenario. A cyberattack test can be manually executed after a security administrator calls a scenario and selects a targeted digital asset.

- For security reasons, the scenario title has been masked

Fig. 6. Vulnerability scan execution

4. Conclusions

During the research on developing detection technologies to cyber threats for APR1400, this cybersecurity vulnerability management system is developed. Although this system must be very carefully managed for security reasons, it can be very helpful to manage cyber vulnerabilities for digital assets of nuclear power plants if utilities have this system. Specifically, it can manage existing vulnerabilities and update the latest ones so it can reduce the cost and effort required for penetration testing by distinguishing which vulnerabilities have been tested in digital assets. Also, managing scenario database can enhance the penetration testing level above a certain threshold by avoiding redundant efforts and focusing on the areas that need it. Thus, in the long term, it will contribute to enhance security of nuclear power plants and be economically beneficial.

ACKNOWLEDGEMENT

This work was supported by the National Research Foundation (NRF) using the financial resource granted by the Ministry of Science and ICT of the Republic of Korea. (No. RS-2022-00144287).

REFERENCES

[1] KINAC/RS-015, Technical Standard for Security on Computer and Information Systems in Nuclear Facilities, 2023.
[2] KINAC/RS-019, Technical Standard for Critical Digital Asset Identification, 2015.
[3] https://www.tenable.com/products/ot-security
[4] https://ko.nozominetworks.com/products/guardian
[5] https://www.dragos.com/cybersecurity-platform/
[6] https://www.kali.org/