Journal of the Korea Academia-Industrial cooperation Society
Vol. 18, No. 7 pp. 1-8, 2017

https://doi.org/10.5762/KAIS.2017.18.7.1
ISSN 1975-4701 / eISSN 2288-4688

시스템 취약점 개선의 필요성에 따른 효율적인 점검 방법을 통한 종합 보안 취약성 분석 시스템 설계

민소연[1], 정찬석[2], 이광형[3*], 조은숙[3], 윤태복[3], 유승호[2]
[1]서일대학교 정보통신공학과, [2](주)엔오비즈, [3]서일대학교 소프트웨어공학과

Design of Comprehensive Security Vulnerability Analysis System through Efficient Inspection Method according to Necessity of Upgrading System Vulnerability

So-Yeon Min[1], Chan-Suk Jung[2], Kwang-Hyong Lee[3*], Eun-Sook Cho[3], Tae-Bok Yoon[3], Seung-Ho You[2]

[1]Dept. of Information and Communcation Eng., Seoil University
[2]N.O.BIZ Co. Ltd., [3]Dept. of Software Eng., Seoil University

요 약 IT 환경 발전되고 융합서비스가 제공됨에 따라서 다양한 보안위협이 증가하고 있으며, 이로 인해 사용자들로부터 심각한 위험을 초래하고 있다. 대표적으로 DDoS 공격, 멀웨어, 웜, APT 공격 등의 위협들은 기업들에게 매우 심각한 위험요소가 될 수 있으므로 반드시 적절한 시간 내에 적절한 조치 및 관리가 되어야 한다. 이에 정부는 '정보통신기반보호법'에 따라 국가안보 및 경제사회에 미치는 영향 등을 고려하여 중요 시스템에 대해 주요정보통신기반시설로 지정 관리하고 있다. 특히 사이버침해로부터 주요정보통신기반시설을 보호하기 위하여 취약점 분석·평가, 보호대책 수립 및 보호조치 이행 등의 지원과 기술가이드 배포 등의 관리감독을 수행하고 있다. 현재까지도 '주요정보통신기반시설 기술적 취약점 분석 평가방법 가이드'를 베이스로 보안컨설팅이 진행되고 있다. 적용하고 있는 항목에서 불필요한 점검항목이 존재하고 최근 이슈가 되는 APT공격, 악성코드, 위험도가 높은 시스템에 대해 관리부분이 취약하다. 실제 보안 위험을 제거하기 위한 점검은 보안관리자가 따로 기획해서 전문업체에게 발주를 주고 있는 것이 현실이다. 즉, 현재의 시스템 취약점 점검 방법으로는 해킹 및 취약점을 통한 공격에 대비하기 어려움이 존재하여 기존의 점검방법과 항목으로는 대응하기가 힘들다. 이를 보완하기 위해서 본 논문에서는 시스템 취약점 점검의 고도화 필요성을 위해 효율적인 진단 데이터 추출 방법, 최근 트렌드를 반영하지 못한 점검 항목을 최신 침입기법 대응에 관하여 기술적 점검 사례와 보안위협 및 요구사항에 대해서 관련 연구를 수행하였다. 국내·외의 보안 취약점 관리체계 및 취약점 목록을 조사 후 이를 기반으로, 효율적인 보안취약점 점검 방법을 제안하며 향후, 제안방법을 강화하여 국외의 취약점 진단 항목을 국내 취약점 항목에 연관되도록 연구하여 개선하고자 한다.

Abstract As the IT environment becomes more sophisticated, various threats and their associated serious risksare increasing. Threats such as DDoS attacks, malware, worms, and APT attacks can be a very serious risk to enterprises and must be efficiently managed in a timely manner. Therefore, the government has designated the important system as the main information communication infrastructure in consideration of the impact on the national security and the economic society according to the 'Information and Communication Infrastructure Protection Act', which, in particular, protects the main information communication infrastructure from cyber infringement. In addition, it conducts management supervision such as analysis and evaluation of vulnerability, establishment of protection measures, implementation of protection measures, and distribution of technology guides. Even now, security consulting is proceeding on the basis of 'Guidance for Evaluation of Technical Vulnerability Analysis of Major IT Infrastructure Facilities'. There are neglected inspection items in the applied items, and the vulnerability of APT attack, malicious code, and risk are present issues that are neglected. In order to eliminate the actual security risk, the security manager has arranged the inspection and ordered the special company. In other words, it is difficult to check against current hacking or vulnerability through current system vulnerability checking method. In this paper, we propose an efficient method for extracting diagnostic data regarding the necessity of upgrading system vulnerability check, a check item that does not reflect recent trends, a technical check case for latest intrusion technique, a related study on security threats and requirements. Based on this, we investigate the security vulnerability management system and vulnerability list of domestic and foreign countries, propose effective security vulnerability management system, and propose further study to improve overseas vulnerability diagnosis items so that they can be related to domestic vulnerability items.

Keywords : Diagnosis Script, Information Communication Infrastructure, Security, Vulnerability Inspection, Vulnerability Management System

본 연구는 중소기업청에서 지원하는 2016년도 산학연협력기술개발사업 C0397609의 연구수행으로 인한 결과물임을 밝힙니다.
*Corresponding Author : Kwang-Hyong Lee (Seoil Univ.)
Tel:+82-10-7327-4118 email: dreamace@seoil.ac.kr
Received June 2, 2017 Revised June 27, 2017
Accepted July 7, 2017 Published July 31, 2017

1. 서론

최근의 IT 보안 위협은 지속적으로 증가되고 급속히 확산되고 있으며 본질적으로 끊임없이 변화되고 있다. 그 이유는 기업들의 IT 인프라가 매우 복잡하며 다양한 시스템들을 사용하고 있기 때문에 기업들이 직면한 보안 위협들의 다양한 위협들에 대해서 적절한 조치를 취하기에는 역부족이다[1-6].

이에 따라 기업들은 정기적으로 “시스템 취약점 점검”을 통해 더 큰 보안사고가 발생하는 것을 방지하고 있다. 하지만 10년 전이나 지금이나 똑같은 기준과 항목을 이용하여 시스템 취약점 점검을 실시하고 있으며, 적용하고 있는 항목에서 불필요한 점검항목이 존재하여 현재 이슈가 되는 APT공격, 악성코드, 위험도가 높은 시스템 취약점에 대해서는 소홀히 점검되거나 법적으로 진행되는 형식적인 점검으로 생각하고 자체적인 점검항목을 추가하여 부족한 항목 점검에 대하여 보완하고 점검하고 있다[8,12,13,21].

이에 따라 기술적 점검은 시스템 취약점 점검보다 모의해킹을 통한 시스템보호에 비중을 높게 두고 있는 것이 현실이다. 이는 근본적으로 취약점 점검에 대한 접근방법이 잘못되었거나 필요성을 느끼지 못하기 때문이라고 판단된다[8].

본 논문에서는 시스템 취약점 점검의 필요성에 따른 진단 데이터 추출 방식과 효율적인 점검 방법에 대해서 연구하도록 한다. 제안된 논문은 현재 취약점 점검 방법의 문제점과 신규 취약점에 대응하여 새로운 점검항목 반영 등 현재 점검 방법에서 국내 설정에 맞는 취약점 진단 방식에 적합하게 수행할 수 있는 신뢰성 있는 방법에 대하여 제안 한다.

본 논문은 5장으로 구성되어 있다. 2장에서는 시스템 취약점 분석 방법과 문제점에 대해서 관련연구를 수행한다. 3장에서는 시스템 진단 스크립트, Vulnerability Management Program에 대한 데이터 처리, 자동화 처리에 대하여 설계하고 4장에서는 이에 대해 제안방식의 시간당 처리량, 취약점 분석 항목 평가에 따라 Vulnerability Management Program 효율성을 평가한다. 5장에서는 결론과 향후 연구방향성을 제시한다.

2. 관련연구

2.1 시스템 취약점 분석 방법

시스템 취약점 점검은 시스템 설정 또는 서비스를 통해 공격자에 의해 공격당하지 않도록 보안점검 항목을 정의하고 점검을 실시하여 취약점을 제거하는 행위를 말한다[7,8,13].

이는 시스템 취약점 점검 항목에 의해 현황을 파악하고 보안 기준에 부합하도록 설정을 유지하여 안정적인 서비스와 보안 위험으로부터 보호하기 위함이다[12]. 시스템 취약점 점검 주요 범위는 [Table 1]과 같다.

Table 1. Main scope of system vulnerability inspection

Category	Contents
Account settings	Check administrator / user account privilege management policy
File permissions	Check whether to abuse system / important files
Service	Enable unnecessary service Check part and setting
Application settings	Confirm setting of whether to use main application
Log Management	Collect system logs and check access rights
Security management	Security patch and Management check

우리나라의 주요정보통신은 정보통신기반보호법(이하 “동법”)에 근거를 두고 있다[12].

동법에서 규정한 지정기준에 따라 ‘주요정보통신기반시설’의 운영기관(관리기관) 및 관계부처 등이 사이버보안을 위해 해야 하는 일련의 행위 및 제반 사항을 규정하고 있으며, 주요 정보통신기반시설 취약점 분석·평가 방법은 주요정보통신기반시설의 안정적 운영을 위협하는 사이버보안 점검항목과 항목별 세부 점검항목으로 도출하여 발견된 취약점에 대한 위험등급 부여, 개선방향 수립 등의 유기적인 평가를 수행해야 한다[7].

대부분의 취약점점검컨설팅은 ‘주요정보통신기반시설 취약점 분석·평가 방법’을 기준으로 취약점을 점검하고 취약점을 진단함으로써 해킹 위협으로부터 안전성 여부를 판단함과 동시에 보안 대응책을 강구함을 목적으로 한다.

대표적인 취약점 평가 기준인 ‘금융분야 취약점 분석·평가 기준’과 ‘주요정보통신기반시설 취약점 분석·평가 기준’은 취약점 항목 매칭이 가능하다.

하지만 대다수의 기업들은 시스템 취약점 점검은 형

식적으로 진행되며, 실제 위험을 제거하기 위한 항목은 따로 점검항목을 분석 및 작성하여 관리하도록 한다. 즉, 현재의 시스템 취약점 점검 방법으로 해킹이나 취약점을 통한 공격에 대비하기 힘들기 때문에 지금의 점검 방법과 점검항목 외에 효율적인 점검 방법이 필요한 현실이다[8,17-19].

2.2 시스템 취약점 진단 방법 및 문제점

취약점 점검 방법은 자동화된 진단 도구를 사용하여 계정권한, 파일권한, 설정현황 등을 텍스트 형태의 보고서 파일로 작성하여 점검자에게 제공한다. 점점자는 보고서의 결과를 분석 후 결과를 작성한다[8].

자동화된 진단 툴에 의한 텍스트형태의 결과 값은 [Fig. 1]과 같다.

```
================================================================================
                        [W-4] 계정 잠금 임계값 설정
================================================================================
- 계정 잠금 임계값이 5 이하의 값으로 설정되어 있지 않은 경우 취약
- Lockout threshold 값이 5이하이면 양호

Lockout threshold:                                Never

[W-4] END
[W-4] RESULT=[Fail]
================================================================================
                        [W-5] 해독 가능한 암호화를 사용하여 암호 저장
================================================================================
- "해독 가능한 암호화를 사용하여 암호 저장"을 사용 하는 경우 취약
- ClearTextPassword 값이 "사용안함" 상태인 0이면 양호

ClearTextPassword = 0

[W-5] END
[W-5] RESULT=[success]
================================================================================
```

Fig. 1. Text result by script

수동진단의 경우 자동화된 도구를 사용하지 못하거나 자동화를 수행할 수 없는 항목에서는 직접적으로 시스템에 접근 후 현황을 파악한다. 이후 파악된 현황을 기반으로 결과를 분석 및 진단한다[8].

시스템에 접근하여 Shell 명령어를 통한 결과 값은 [Fig. 2]과 같다.

```
C:₩>net accounts
만료 시간이 지난 얼마 후에 강제 로그오프하시겠습니까?:    아님
최소 암호 사용 기간 (일):                          0
최대 암호 사용 기간 (일):                          42
최소 암호 길이:                                    0
암호 기록 개수:                                    없음
잠금 임계값:                                       아님
잠금 기간 (분):                                    30
잠금 관찰 창 (분):                                 30
컴퓨터 역할:                                       WORKSTATION
명령을 잘 실행했습니다.
```

Fig. 2. Results from shell command

마지막으로 자동화 진단 및 수동진단을 할 수 없는 경우 담당자를 통해 시스템의 현황을 파악 후 이를 기반으로 분석한다[8].

시스템 취약점 진단을 효율적으로 진행하기 위해서는 자동화된 진단 도구를 통해 최대한 많은 데이터를 수집하고 담당자 인터뷰 등 수동진단항목을 최소화 시키는 것이 필요하다.

그렇기 때문에 대다수의 점검자는 “주요정보통신기반시설 취약점 분석·평가 방법”을 기준 항목에 맞게 자동화된 진단 도구를 통해 원하는 결과데이터를 얻을 수 있도록 수정보완하고 있는 것이 사실이다.

또한 고객사의 요청에 의해 시스템 취약점 진단 항목이 추가 또는 변경 요청이 된다면 진단스크립트를 수정해서 진행하고 있다.

자동화된 진단 스크립트를 통한 시스템 취약점 진단 방법은 가장 효율적인 방법으로 점검자의 작업시간을 절약할 수 있다는 장점이 있다.

하지만 자동화된 진단 진단스크립트를 통한 점검 방식도 텍스트 형태의 파일의 결과물은 최종보고서 문서파일 형태로 작성해야 하는 문제점이 발생한다.

이는 점검자의 진단시간을 확실히 줄일 수 있지만 반복 작업 등의 문제점은 여전히 존재하는 것이 사실이며, 효율적인 진단 방식을 위해서는 작업자의 반복 작업의 최소화와 진단스크립트를 통해 최대한 많은 시스템의 정보의 결과 값을 확보하는 것이 필요하다.

3. 제안 취약점 점검 방법

3장에서는 시스템 취약점 개선의 필요성에 따른 효율적인 점검에 따른 효율적인 점검 방법에 대하여 제안한다.

제안하는 취약점 점검 방법은 시스템 진단 스크립트, 점검자, Vulnerability Management Program으로 구성되어 있다.

점검자는 시스템에서 산출된 스크립트 텍스트 결과물을 사용하여, Vulnerability Management Program을 이용, 진단 결과를 결과보고서 형태로 변환하여 점검자가 시스템 취약점 보고서 작성 시에 필요한 데이터 작업을 최소화하여 수행하는 방식이다. 제안된 취약점 점검 방법 개념도는 [Fig. 3]과 같다.

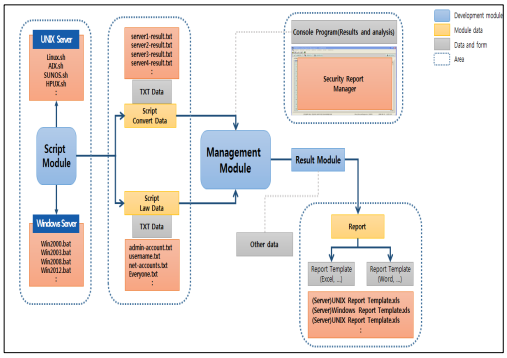

Fig. 3. Vulnerability Analysis

3.1 점검 스크립트 개선 방법

시스템 점검 스크립트의 경우 기존 자동화 진단 방식에서 사용되는 Script Convert Data의 활용과 진단 항목이 추가 또는 변경 요청 시 사용가능한 Script Raw Data의 결과 값을 확보하여 점검 분석을 진행하는 것을 제안한다.

대다수의 숙련된 점검자들은 진단항목 외에 결과 값을 추가로 점검하여 진행하고 있지만 특정 결과 값이 없을 경우 참고용으로 사용되는 경우가 많다.

제한하는 점검 스크립트는 기존 방식에서 Script Raw Data의 결과 값을 최대한 활용할 수 있도록 구성되며, 이후 Vulnerability Management Program을 통해서 결과데이터를 활용이 가능하도록 구성한다. Script Data의 필요한 요소는[Table. 2]와 같다.

Table 2. Necessary elements of script data

Category	Contents
File result information	Result of the contents of the file that has the result value of the specific command
Setting information	Information related to security/ configuration files
Program information	Program information during installation /Setup
Version Information	OS, application, etc. Version information

1. 파일결과정보는 Shell 명령어를 통해 나온 결과 값으로 텍스트파일 형태로 저장되며, 저장 된 결과 값 정보에 대한 내용이다.
2. system/application 설정정보를 확인할 수 있는 데이터로 설정되어 있는 정책 또는 환경설정 정보에 대한 내용이다.
3. 설치되어 있는 프로그램의 종류와 상태에 대한 정보와 구동 프로세스 여부 정보에 대한 내용이다.
4. OS를 비롯하여 모든 프로그램에 대한 버전 및 업데이트 로그 정보 정보에 대한 내용이다.

Script Raw Data의 결과 값 활용의 경우 [Table. 3]와 같이 시스템에 설치 또는 구동되는 프로그램의 신규 또는 기존 취약점의 버전 정보 점검으로 취약점 여부를 확인 할 수 있다.

Table 3. Vulnerability

Category	Contents
CVE-2016-6309C VE-2016-7052	openssl Denial of Service Vulnerability (openssl version -a)
CVE-2017-6074	Linux kernel local privilege escalation vulnerability (cat /proc/version)
CVE-2016-6662	mysql Remote code execution, privilege escalation vulnerability (mysql -h 127.0.0.1 -u $dbid -p$dbpw -e "show variables like 'version';" -t)
CVE-2014-6271 CVE-2014-7169	Code injection vulnerability bash using environment variable (bash--version)

CVE(Common Vulnerabilities and Exposures)의 경우 시스템에 구동되는 프로그램 또는 취약한 버전 사용이 많을 경우 취약점 항목은 늘어날 수 있다.

그렇기 때문에 자동화 진단 방식에서 최대한 많은 정보를 추출하는 것이 중요하며, Script Data의 필요한 요소의 결과 데이터와 Vulnerability Management Program을 활용하여 시스템 취약점 점검의 효율성을 높일 수 있는 것이 중요하다.

제안하는 목표는 Shell Script를 통해 최대한 많은 데이터를 수집하고 담당자 인터뷰 등 수동진단항목을 제외하고 점검자가 효율적으로 진단하는 것이 목적이다.

3.2 Vulnerability Management Program

Vulnerability Management Program은 시스템 취약점 점검 시 시스템의 영향을 최소화 하는 Shell Script를 통해 결과 및 분석을 자동화한 프로그램이다.

즉, Shell Script를 통해 결과 데이터를 확인하고 결과 및 분석된 데이터를 활용하여 효율적으로 작업을 Shell Script를 이용 서버의 최소 리소스만 사용하여, 서버에

영향을 최소화하는 것이 특징이다. Vulnerability Management Program을 이용한 시스템 취약점 진단절차는 [Fig. 4]와 같다.

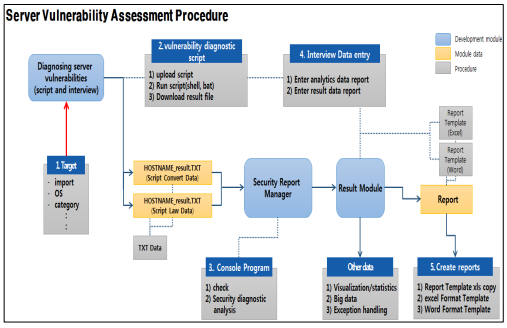

Fig. 4. System vulnerability diagnosis procedure

시스템 취약점 진단 절차는 기존 방식과 동일하게 진행되는 것이 특징이며, Vulnerability Management Program을 통해 점검자의 반복 작업 및 오탐 또는 결과 데이터 확인 등 불필요한 시간을 절약하여 효율적으로 진행할 수 있다.

3.3 데이터 처리

Vulnerability Management Program은 Shell Script에 의한 텍스트 파일형태의 결과 데이터를 불러와서 원하는 데이터를 처리하도록 구현되었다.

텍스트파일 형태의 진단 데이터를 한 번에 확인 가능하여 효율적으로 진행 가능하며 결과는 [Fig. 5]와 같다.

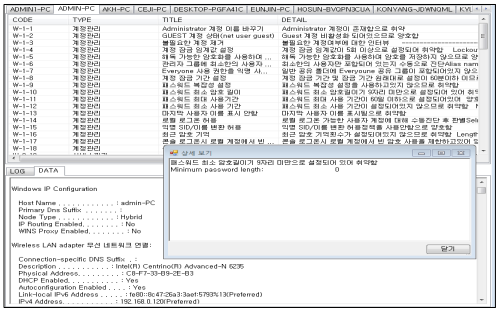

Fig. 5. Result of diagnostic data processing

기존 텍스트 결과 데이터에 비해 좀 더 가독성이 높으며 상단 탭으로 여러 시스템의 정보를 간편하게 점검 확인이 가능하다.

3.4 자동화 처리

자동화 처리는 점검자의 반복적인 작업들을 자동화 처리를 통해 효율적인 작업이 가능하도록 텍스트 파일 형태의 점검결과 데이터를 보고서 파일 형태로 결과를 저장하여 점검자의 수작업을 줄이고 효율적인 작업이 될 수 있도록 처리하였다. 자동화 처리된 결과는 [Fig. 6]와 같다.

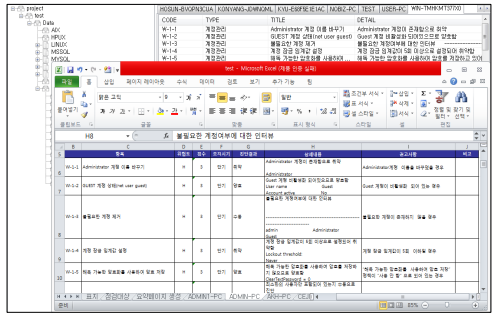

Fig. 6. Result of diagnostic data processing

텍스트 파일 형태의 결과데이터의 내용을 parsing하여 보고서 형태로 변환된다. 점검자는 인터뷰 등 수동점검 항목에 대해서 수정작업을 진행하면 되기 때문에 기존 대비 점검의 효율성을 높일 수 있다.

4. 제안 시스템 취약점 점검

4.1 시간당 처리량 평가

기존 점검방식보다 텍스트 파일 형태의 결과데이터를 직접 확인하지 않고 Vulnerability Management Program을 통해 정리된 결과 값을 가지고 점검을 진행하기 때문에 짧은 시간에 많은 내용을 확인 가능하다. 또한 반복적인 작업시간을 줄이기 때문에 작업을 효율적으로 진행할 수 있다. 효율성 분석을 위한 시간당 처리량 평가 내용은 [Table. 4]와 같다.

Table 4. Time throughput evaluation contents

Division	Contents
Inspection rate	Whether to check the quantity of 100 units of inspection system
Unchecked rate	Whether to check the quantity of 100 units of the inspection system
Working time	Work time for time throughput check Limited to 60 minutes
Remarks	Conventional method: 4 people, proposed method: progress of one person

테스트 진행시 시간당 처리량 분석을 위해 제안 방식은 Vulnerability Management Program을 활용하기 때문에 1명의 점검자, 기존 방식은 4명의 점검자가 테스트를 진행한 결과 제안 방식은 1명의 점검자가 100대의 대상에 대한 시스템 취약점 점검을 완료하였다. 이에 따라 제안방식의 경우 짧은 점검시간동안 높은 점검률을 확인할 수 있었으며 비교한 결과를 [Fig. 7]에서 확인할 수 있다.

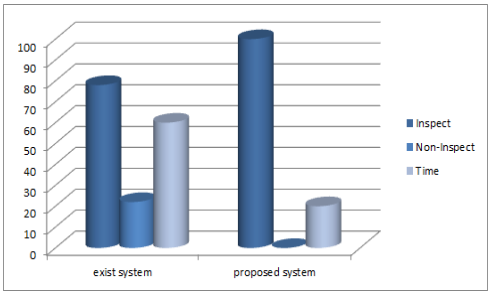

Fig. 7. Throughput per Hour

기존방식의 경우 78% 점검률, 22%의 미점검률 결과를 확인할 수 있다. 제안된 방식에서는 점검인원 대비 100%의 점검률, 0%의 미점검율을 보였으며, 특히 시간당 처리량에 속해있는 점검시간의 경우 20분 소요로 기존방식보다 70%의 성능 차이를 볼 수 있었다. 이에 따라 제안방식이 기존방식 대비 효율적으로 진단이 가능한지 확인할 수 있다.

4.2 취약점 분석 항목 평가

취약점 분석 항목 평가의 경우 기존 방식의 주요정보통신기반시설 취약점 점검항목 중 자동화된 점검 Script 기반 기준항목으로 평가를 진행하였다. 자동화된 점검 스크립트 방식은 [Table. 5]와 같이 199개의 항목에 대하여 점검을 진행한다. 이는 수동진단 인터뷰 점검항목을 포함한다.

Table 5. Vulnerability check item for automatable diagnosis

Division	High	Middle·Low	Total
WINDOWS	45	37	82
UNIX	43	30	73
DBMS	11	13	24
PC	14	6	20
Total	113	86	199

기존 방식의 경우 '주요정보통신기반시설 취약 점 점검항목'을 기반으로 점검스크립트를 통하여 점검을 진행한다. 제안하는 점검스크립트의 경우 기존 항목 외에 취약점 분석 항목을 추가 분석 할 수 있으며, 시스템에 구동되는 프로그램 또는 취약한 버전 사용이 많을 경우 취약점 항목은 늘어날 수 있다. [Table. 6]는 특정 버전에서 발생 가능성 있는 취약점을 나타내며, [Fig. 8]과 같이 기존 방식에 비해 제안하는 방식은 신규 취약점 분석 항목에서 많은 차이를 나타내고 있다.

Table 6. Common Vulnerabilities and Exposures

Division	CVE
Openssl	CVE-2016-6304, CVE-2016-6305, CVE-2016-2183 CVE-2016-6303, CVE-2016-6302, CVE-2016-2182 CVE-2016-2180, CVE-2016-2177, CVE-2016-2178 CVE-2016-2179, CVE-2016-2181, CVE-2016-6306 CVE-2016-6307, CVE-2016-6308
bash	CVE-2014-6271, CVE-2014-7169, CVE-2014-6277 CVE-2014-6278, CVE-2014-7186, CVE-2014-7187

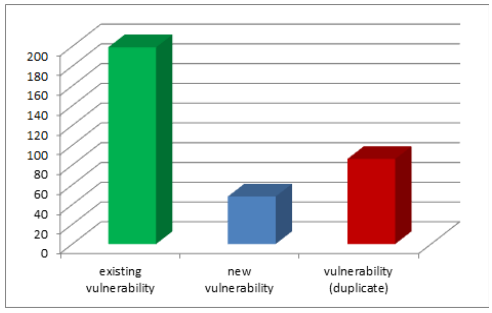

Fig. 8. Test analysis

신규 취약점 항목분석을 통해 취약점 보안 조치가 완료하게 되면 중복된 취약점 항목들에 대한 조치가 동시에 진행 가능하기 때문에 기존방식 대비 65%의 취약점 항목 조치가 향상될 수 있는 것을 알 수 있다.

5. 결론

본 논문에서는 시스템 취약점 개선의 필요성에 따른 효율적인 점검 방법에 관하여 연구하였다. 제안방법은 통해 효율적인 점검방식으로 인하여 점검 소요시간을 줄일 수 있으며 Script Raw Data의 결과를 이용하여 기존 항목 외에 추가적으로 점검항목을 점검할 수 있는 시간을 확보할 수 있도록 설계하였으며, 이를 기반으로 신규

취약점에 대응하여 새로운 점검항목 반영 등 기존 점검 방법에서 국내 설정에 맞게 시스템 취약점 점검 방식에 적합하게 수행할 수 있는 효율적인 점검 방식이라는 것을 확인 할 수 있었다.

시스템 취약점 점검의 고도화의 필요성이 높아짐에 따라 국내의 현실에 맞는 취약점 데이터베이스를 구축하여 국내의 취약점 점검의 효율성을 높일 수 있어야 한다. 향후, 제안방법을 강화하여 취약점 데이터베이스와 연동함으로써, 국내·외 취약점 점검항목을 포함하고 취약점 점검이 효율적으로 점검이 가능하게 하여 국내의 시스템 취약점 점검에 대한 필요성과 효율성을 증가할 예정이다.

References

[1] KISA, "IT Security Evaluation and Certification Guide", 2009.

[2] KISA, "Establishment of information technology management system for new technology", 2010.

[3] K. H. Han, I. S. Kim, “A Study on Threat Analysis of PC Security and Countermeasures in Financial Sector”, The Journal of The Institute of Internet, Broadcasting and Communication(IIBC), vol. 15, no. 6, pp. 283-290, Dec. 2015.
DOI: http://dx.doi.org/10.7236/JIIBC.2015.15.6.283

[4] M. K. Yi, H. J. Hwang, “A Study on Security Weakness and Threats in Personal Health Record Services”, The Journal of The Institute of Internet, Broadcasting and Communication (IIBC), vol. 15, no. 6, pp. 163-171, Dec. 2015.
DOI: http://dx.doi.org/10.7236/JIIBC.2015.15.6.163

[5] Moon-sung Hwang, Yong-Hee Lee, Jung-Ah Shim, Keun-Heiu Kim, “Study on Countermeasures and Security Vulnerability of Fintech Services”, Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, vol. 6, no. 3, pp. 71-79, Mar. 2016.
DOI: http://dx.doi.org/10.14257/AJMAHS.2016.03.24

[6] Hee-Hoon Cho, Dal-Soo Weon, Jong-Bae Kim, “A Study on the Security Vulnerability of Android”, Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, vol. 5, no. 6, pp. 1-8, Mar. 2015.

[7] S. H. Kim, "(The)critical information and communication infrastructure technical field vulnerability assessment improvements research", 2016.

[8] Security Trends, "Need to upgrade system vulnerability check", 2016.

[9] J. B. Kim, “A Study on the Successful Implementation about Vulnerability Supplmention and Effective Recovery from Damage related with web Application”, Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, vol. 6, no. 1, pp. 53-60, Jan. 2016.
DOI: http://dx.doi.org/10.14257/AJMAHS.2016.02.22

[10] J. T. Kim, “Analyses of Requirement of Security based on Gateway Architecture for Secure Internet of Thing”, Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, vol. 6, no. 3, pp. 461-470, Mar. 2016.
DOI: http://dx.doi.org/10.14257/AJMAHS.2016.03.02

[11] C. H. Cho, J. K. Bae, “An Exploratory Study on the Key Components of Financial Information Technology Compliance Systems: Focusing on the In-depth Interviews with Experts”, Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, vol. 7, no. 6, pp. 785-795, Jun. 2017.
DOI: http://dx.doi.org/10.14257/ajmahs.2017.06.48

[12] Ministry of Future Creation and Science, "Vulnerability Analysis and Evaluation Criteria for Information and Communication Infrastructure Facilities", Ministry of Future Creation and Science, 2013-37, 2013.

[13] S. T. Park, et al., "Vulnerability Analysis and Evaluation Management for the Protection of Major IT Infrastructure", Journal of Information Security 19th volume no. 6, 2009.

[14] B. G. Joo,N. W. Min, M. S. Chang, C. K. Ahn, D. H. Yang, Development of Vulnerability Scanner using Search Engine, The Journal of The Institute of Webcasting, Internet Television and Telecommunication vol. 9 no. 1, pp. 19-24, 2009.

[15] H. K. Yang, A Study of Security Weaknesses of QR Codes and Its Countermeasures, The Journal of The Institute of Webcasting, Internet and Telecommunication vol. 12 no. 1, pp. 83-89, 2012.
DOI: http://dx.doi.org/10.7236/JIWIT.2012.12.1.83

[16] B. W. Jin, J. O. Park, M. S. Jun, A Study on Authentication Management and Communication Method using AKI Based Verification System in Smart Home Environment, The Journal of The Institute of Internet, Broadcasting and Communication (IIBC), vol. 16, no. 6, pp. 25-31, Dec. 31, 2016.
DOI: https://doi.org/10.7236/JIIBC.2016.16.6.25

[17] H. W. Noh, "A Study on the effective management of Critical Information Infrastructure Protection ", Soongsil University Information and Communications University, Master Thesis, 2012.

[18] S. H. Jang, "A Study on Improvement of Evaluation Criteria for Information Security in Information Infrastructure", Dongguk University Graduate School of International Information Studies, Master Thesis, 2015.

[19] H. S. Lee, "Implementation of Shell Script to Improve Security Vulnerabilities of Linux Server", Kyungpook National University Graduate School of Industry, Master Thesis, 2012.

[20] N. K. Baik, Y. H. Lee, Design and caomparision of DDoS Attack and Defence Mechanism Classification system, Asia-pacific Journal of Multimedia Services Convergent with Art, Humanities, and Sociology, vol. 6, no. 12, pp. 595-604, Dec. 2016.
DOI: http://dx.doi.org/10.14257/AJMAHS.2016.12.59

[21] KISA, "Strategies for the improvement of the protections of the major information and communications infrastructures", 2013.

민 소 연(So-Yeon Min) **[종신회원]**

- 1994년 2월 : 숭실대학교 전자공학과 (공학사)
- 1996년 2월 : 숭실대학교 일반대학원 전자공학과 (공학석사)
- 2003년 2월 : 숭실대학교 일반대학원 전자공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 정보통신과 부교수

<관심분야>
통신 및 신호처리, 임베디드 시스템

정 찬 석(Chan-Suk Jung) **[정회원]**

- 1997년 2월 : 인천대학교 전자공학과 (공학사)
- 2002년 2월 : 숭실대학교 정보통신 (공학석사)
- 2016년 2월 : 숭실대학교 컴퓨터 (공학박사)
- 2011년 4월 ~ 현재 : (주)엔오비즈 대표이사

<관심분야>
정보보안, 보안관리, 머신러닝, 클라우드 서비스

이 광 형(Kwang-Hyong Lee) **[종신회원]**

- 1998년 2월 : 광주대학교 컴퓨터공학과 (공학사)
- 2002년 2월 : 숭실대학교 컴퓨터학과 (공학석사)
- 2005년 2월 : 숭실대학교 컴퓨터공학과 (공학박사)
- 2005년 3월 ~ 현재 : 서일대학교 소프트웨어공학과 부교수

<관심분야>
멀티미디어 보안, 사물인터넷, 학습콘텐츠, 영상처리

조 은 숙(Eun-Sook Cho) **[정회원]**

- 1993년 2월 : 동의대학교 전산통계학과 (이학사)
- 1996년 2월 : 숭실대학교 대학원 컴퓨터학과(공학석사)
- 2000년 2월 : 숭실대학교 대학원 컴퓨터학과(공학박사)
- 2000년 3월 ~ 2005년 2월 : 동덕여자대학교 정보학부 강의전임교수
- 2005년 3월 ~ 현재 : 서일대학교 소프트웨어공학과 부교수

<관심분야>
소프트웨어공학, 임베디드 소프트웨어, 모바일 컴퓨팅

유 승 호(Seung-Ho You) **[정회원]**

- 2014년 2월 : 국가평생교육진흥원 학점은행제 (정보처리)
- 2015년 6월 ~ 현재 : (주)엔오비즈 취약성 분석팀 팀장

<관심분야>
정보보안, 보안 데이터 시각화, 취약성 분석

윤 태 복(Tae-Bok Yoon) **[종신회원]**

- 2001년 2월 : 공주대학교 전자계산학과 이학사
- 2005년 2월 : 성균관대학교 컴퓨터공학과 공학석사
- 2010년 2월 : 성균관대학교 컴퓨터공학과 공학박사
- 2011년 3월 ~ 현재 : 서일대학교 소프트웨어공학과 조교수

<관심분야>
지능시스템, 게임 인공지능, 사용자 모델링