https://doi.org/10.5392/JKCA.2021.21.01.284

다중 검색엔진을 활용한 보안관제 모델 개선방안

Improvement Mechanism of Security Monitoring and Control Model Using Multiple Search Engines

이제국, 조인준
배재대학교대학원 사이버보안학과

Je-Kook Lee(jekook.lee@igloosec.com), In-June Jo(injune@pcu.ac.kr)

요약

현재 보안관제 시스템은 공격자의 공격 후 대응만을 위한 수동적인 시스템으로 운용됨에 따라 공격 발생 이후 침해사고 대응이 일반적이다. 특히, 신규 자산 추가 및 실제 서비스가 이루어지는 경우 실제 해커의 관점에서 취약점 테스트 및 사전 방어에 한계가 있다. 본 논문에서는 해킹 관련 다중 검색엔진을 활용하여 보호 자산의 사전 취약점 대응 기능을 추가한 보안관제 모델을 새롭게 제안하였다. 즉, 범용 또는 특수한 목적을 지닌 다중의 검색엔진을 이용하여 보호 대상 자산의 특수한 취약점을 사전에 점검하고, 점검결과로 나타난 자산의 취약점을 사전에 제거하도록 하였다. 그리고 실제 해커의 입장에서 인지되는 보호 자산의 객관적인 공격 취약점을 미리 점검하는 기능, IP 대역에 위치한 광범위한 시스템 관련 취약점을 사전에 발굴하여 제거하는 기능 등을 추가로 제시하였다.

■ 중심어 : | 보안관제 | 취약점분석 | 웹 취약점 | 쇼단 | 구글해킹 |

Abstract

As the current security monitoring system is operated as a passive system only for response after an attacker's attack, it is common to respond to intrusion incidents after an attack occurs. In particular, when new assets are added and actual services are performed, there is a limit to vulnerability testing and pre-defense from the point of view of an actual hacker. In this paper, a new security monitoring model has been proposed that uses multiple hacking-related search engines to add proactive vulnerability response functions of protected assets. In other words, using multiple search engines with general purpose or special purpose, special vulnerabilities of the assets to be protected are checked in advance, and the vulnerabilities of the assets that have appeared as a result of the check are removed in advance. In addition, the function of pre-checking the objective attack vulnerabilities of the protected assets recognized from the point of view of the actual hacker, and the function of discovering and removing a wide range of system-related vulnerabilities located in the IP band in advance were additionally presented.

■ keyword : | Security Monitoring | Vulnerability Analysis | Web Vulnerability | SHODAN | GHDB |

접수일자 : 2020년 09월 25일
수정일자 : 2020년 10월 20일
심사완료일 : 2020년 10월 20일
교신저자 : 조인준, e-mail : injune@pcu.ac.kr

I. 서 론

정부 부처와 기업을 대상으로 이루어지는 해킹 공격은 하루가 다르게 지능적이고 기술적으로 발전되고 있다. 이로 인한 피해를 언론을 통해서 자주 접할 수 있다. '2019년 정보보호 실태조사'에 따르면 국내 기업체의 2.8%가 침해사고를 겪었다. 이는 전 년 대비 0.5%가 증가한 수치이며 이는 매년 기업체를 겨냥한 공격이 증가하고 있음을 나타낸다. 침해 유형을 살펴보면, 랜섬웨어, 악성코드(컴퓨터 바이러스, 웜, 트로이잔, APT공격 등), DoS/DDoS, 해킹 등의 공격이다[1]. 기업체는 이러한 침해사고를 예방하고 포괄적인 정보보호를 위해 정보보호 정책 수립, 정보보호 조직 운영, 정보보호 교육 등의 관리적 보호조치를 취함과 동시에 보안관제, 인증서비스, 보안컨설팅 등의 보안서비스를 도입하고 있다. 이 중에서도 사이버 공격을 예방, 실시간 탐지 및 침해사고에 즉시 대응하는 보안관제가 그 중요성을 더해가고 있다[2].

기존의 국내 보안관제에서 이루어지는 전산 자산 취약점 진단은 대부분 사전규정된 '취약점 진단 항목'을 중심으로 이루어진다. 이는 국가 기관의 모든 전산시스템이 최소한의 보안 수준을 만족시킬 수 있도록 표준화된 취약점 진단 항목을 국가에서 지정한 것이다. 하지만 표준화된 최소 진단 항목만으로 동일 항목의 반복적인 취약점 점검과 제거를 하는 것은 커다란 잠재적 보안 위협이 될 수 있다. 전산시스템을 공격하는 실제 해커들의 공격은 점차 고도화되어 표준화된 취약점의 허점을 이용하는 비중이 작아졌기 때문이다[0]. 따라서 필수 진단 항목 외 다양한 취약점들은 그대로 공격자에게 노출될 수밖에 없다. 특히 하루에도 수많은 전산시스템 신규 취약점이 개발되고, 보안 피해 규모와 심각성이 점차 확대되고 있어 다음과 같은 요소를 지닌 대책이 필요하다.

첫째, 적은 시간 안에 많은 시스템 점검이 가능해야 한다. 국내 여건상 소수의 인원이 많은 시스템을 관리하는 경우가 대부분이기 때문이다. 둘째, 취약점 점검 방법이 최대한 간단하고 규격화할 수 있어야 한다. 표준화된 취약점 진단 항목의 불완전함을 보완하기 위해 보안관제요원의 비정기 수시진단이 가능해야 하기 때문이다. 본 논문에서는 이러한 문제점을 개선하기 위한 방안을 제시하였다. 보안관제요원이 실제 해커들이 이용하는 범용 또는 특수한 목적을 지닌 다중의 검색엔진을 이용하여, 보호가 필요한 IT 자산을 대상으로 사전 취약점을 진단한다. 그리고 그 자산의 취약점을 사전에 제거하는 방안이다. 즉, 공격자의 관점에서 취약점 진단을 시도하고 규정되어 있지 않은 취약점을 탐지·대응·예방조치 한다. 이러한 방식으로 개선된 사이버 공격 대응체계를 수립할 수 있는 보안관제 모델을 제안하였다.

II. 기존 탐지체계 및 취약점 분석 문제점 요약

1. 기존 탐지체계의 문제점

정부나 기업에서 보안관제 행위가 이루어질 때 일반적으로 보안 위협 식별, 사용자 인식강화 및 대응체계 점검 등의 예방 활동과 보안시스템에서 발생하는 이벤트 수집, 상관분석을 통한 정확한 대응을 최우선 목표로 두고 탐지를 하고 있다[2]. 즉, 공격자의 침입이 탐지된 이후 관제대상의 로그를 분석하고 해당 IP를 차단하는 등의 수동적인 보안관제 행위를 한다. 기존 프로세스의 보안관제에서 공격자의 방법으로 보호 대상 IT 자산을 객관적·능동적 분석을 하는 것은 구조적으로 쉽지 않다. 또한, 이러한 수동적 보안관제 행위는 점차 고도화·다변화되는 해커의 악의적 공격에 매우 취약하다.

2. 사후 대처식 보안관제의 문제점

기존 보안관제 프로세스의 경우, 출처가 불분명하거나 식별할 수 없는 사용자의 공격, 침입 시 다음과 같이 대응한다. 먼저 침해시도에 대한 초동 분석·대응으로 일차적인 침해대응을 시행한다. 그 후 모의 해킹 등으로 사전에 보안 위협을 식별하고, 대응체계 점검, 정기적인 관제요원 훈련 등으로 새로운 공격에 대비한 예방(Protect)을 한다. 결국, 기존 보안관제 프로세스는 수많은 새로운 공격들의 사후 대처는 가능하다. 그러나 신규 취약점(Zero day Attack)으로 공격하거나, 사전 규정된 취약점 이외의 공격을 효과적으로 대응하는 것은 현실적으로 불가능하다.

3. 공개된 취약점으로 제한되는 문제점

각각의 보안관제 전문 기업이나 정부 기관에서는 “표준 웹 취약점 진단 항목”을 사전 규정하여 공개하고 있다. 또한, 이러한 진단 항목 점검을 위해 매년 취약점 점검과 모의 해킹을 법적으로 의무화하여 실시하고 있다. [표 1]은 행정안전부 “표준 웹 취약점 진단 항목”[5]을 나타낸 것이다. 물론 이러한 제도적 취약점 점검 의무화는 평균적으로 IT 자산의 보안성을 향상시킬 수 있는 장점이 있다. 반면, 공격자는 해당 점검항목을 미리 학습하여 취약점 우회 또는 역이용 등으로 공격할 수 있는 맹점이 존재한다. 또는 지정된 취약점 점검항목을 제외한 보안 사각지대 집중공격을 유발할 수 있다. 따라서 이러한 기존의 문제점들을 보완하기 위한 노력이 차세대 보안관제 프로세스 구성에 필요하다.

표 1. 행정안전부 웹 취약점 표준 점검항목(21개)

	점검항목 (코드명)	설명	조치영역
1	운영체제 명령 실행(OC)	■웹 서버에 존재하는 명령어 실행 가능 함수 인자를 조작하여 특정 명령어 실행이 가능한 취약점	소스코드
2	디렉터리 인덱싱(DI)	■본 페이지의 파일 미존재 시 자동으로 디렉터리 리스트를 출력하는 취약점	서버
3	정보누출(IL)	■개발자의 부주의, 디폴트로 설정된 에러 페이지 등 웹 애플리케이션에서 민감한 정보가 노출되는 취약점	소스코드
4	악성콘텐츠 (CS)	■정상적인 콘텐츠 대신에 악성 콘텐츠를 주입하여 사용자에게 악의적인 영향을 미치는 취약점	소스코드
5	크로스 사이트 스크립트(XS)	■웹 사이트를 통해 다른 최종 사용자의 클라이언트에서 임의의 스크립트가 실행되는 취약점	소스코드
6	약한 문자열 강도(BF)	■비밀번호 조합규칙(영문, 숫자, 특수문자 등)이 불충분하여 추측 가능한 취약점	소스코드
7	불충분한 인증 및 인가(IN)	■사용자 인증 및 접근제한 미흡으로 불법 접근 및 조작이 가능한 취약점	소스코드
8	취약한 패스워드 복구(PR)	■취약한 패스워드 복구로직을 통해 다른 사용자의 패스워드를 획득, 변경할 수 있는 취약점	소스코드
9	불충분한 세션 관리(SM)	■단순 숫자 증가 방법 등의 취약한 특정 세션의 ID를 예측하여 세션을 가로채거나 중복 접속을 허용하는 경우 타 사용자의 세션을 획득하여 권한 획득 할 수 있는 취약점	소스코드
10	크로스사이트 리퀘스트 변조 (CF)	■로그온 한 사용자 브라우저로 하여금 사용자의 세션 쿠키와 기타 인증 정보를 포함하는 위조된 HTTP 요청을 취약한 웹 애플리케이션에 전송하는 취약점	소스코드
11	파일업로드 (FU)	■파일 업로드 기능을 이용하여 시스템 명령어를 실행할 수 있는 파일을 업로드 하는 취약점	소스코드
12	경로추적 및 파일다운로드 (FD)	■다운로드 함수 인자를 조작하여 서버에 존재하는 파일 다운로드 가능한 취약점	소스코드
13	관리자페이지 노출(AE)	■단순한 관리자 페이지 이름, 설정, 설계상 오류 등 관리자 메뉴에 직접 접근할 수 있는 취약점	서버
14	데이터 평문전송(SN)	■서버와 클라이언트 통신 시 비암호화 전송으로 중요 정보 등이 노출되는 취약점	서버 소스코드
15	쿠키 변조(CC)	■보호되지 않는 쿠키를 사용하여 값 변조를 통한 사용자 위장 및 권한 상승 등이 가능한 취약점	소스코드
16	웹 서비스 메소드 설정 공격(MS)	■PUT, DELETE 등의 메소드를 악용하여 악성 파일(웹쉘) 업로드가 가능한 취약점	서버
17	URL/파라미터 변조(UP)	■URL, 파라미터의 값을 검증하지 않아 특정 사용자의 권한 획득이 가능한 취약점	소스코드
18	SQL인젝션 (SI)	■입력폼에 악의적 쿼리문 삽입으로 DB정보, 타 사용자 권한획득 가능 취약점	소스코드
19	XPath 인젝션(XI)	■Xpath 쿼리문 구조 임의 변경으로 DB정보, 타 사용자 권한획득 가능 취약점	소스코드
20	자동화공격 (AU)	■정해진 프로세스에 자동화된 공격 수행으로 수많은 프로세스 진행 가능 취약점	소스코드
21	위치공개(PL)	■임시파일, 백업파일등에 접근 가능하여 핵심정보가 노출될 수 있는 취약점	서버

Ⅲ. 본 논문에서 활용한 다중 검색엔진 특성 요약

1. 다중 검색엔진의 정의

본 논문에서 다중 검색엔진의 정의는 “인터넷에 연결되어있는 모든 구성요소(웹, 웹캠, 의료장비, PC, 키오스크, TV, 청소기 등)의 인덱싱(Indexing)된 서비스 정보를 검색할 수 있는 검색엔진”이다. 일반적인 검색엔진(네이버, 구글 등)의 경우 웹 콘텐츠를 인덱싱한다. 그러나 일부 특수한 검색엔진의 경우 인터넷에 연결된 모든 장치의 서비스 배너(Banner) 정보를 인덱싱한다. 다중 검색엔진을 이용한 취약점 점검의 경우 각 검색엔진의 특성에 맞는 질의를 사용, 대상 시스템 취약점 정보를 열람한다. 본 논문에서 활용된 검색엔진 항목은 다음과 같다.

2. SHODAN

SHODAN은 전 세계 해커들이 이용하는 웹 페이지이다. 등의 취약점을 온라인 검색을 통해 쉽게 찾을 수 있게 해주는 해커 중심의 검색엔진이다. SHODAN은

TCP SYN 스캔을 통해 해당 IP주소 포트의 개방 여부를 확인한다. 그리고 해당 포트를 대상으로 배너 그랩을 수행하여 정보를 획득한다[4]. 사용법은 검색 창에 여러 가지 필터를 사용하여 특정 시스템의 취약점을 검색하는 것이다. 이러한 필터를 이용한 검색 외에도 다양한 서비스를 제공한다[3].

3. CENSYS

CENSYS는 인터넷 전반에 걸친 스캔을 하여 모은 데이터를 기반으로 하는 공개 검색엔진이다. 기존 정보 조회 도구보다 검색에 요구되는 시간을 상당 부분 줄였으며 응답 장치, 암호화 여부, 구성 방식 등 세부 정보 확인이 가능하다. CENSYS는 ZMap의 SYN 스캔을 통해 포트 개방 여부를 확인하고, ZGrab을 사용해 핸드셰이크를 완료하여 해당 포트의 애플리케이션에 대한 배너 그랩을 수행한다.

4. Google Hacking DataBase

Google Hacking Database(이하 GHDB)는 구글(Google) 검색을 통해 취약점 분석, 관리자페이지 접근 등을 할 수 있다. GHDB는 가장 많은 데이터를 가진 구글 검색엔진을 활용하여 공격을 시도하는 만큼 위험성이 제일 높다. 또한, 서버에 직접 접속하지 않고 구글에 저장된 페이지로 접근하여 취약한 시스템 정보 수집이 가능하다.

5. IVRE

IVRE는 Bro, Argus, NFDUMP, ZMap과 같은 도구를 사용하여 인터넷에 연결된 장치에 대한 데이터를 표시한다. 또한, Nmap 및 Masscan에서 XML 데이터를 가져오는 기능도 지원함과 동시에 키워드를 사용하여 정렬할 수 있는 Nmap 스캔 결과를 제공한다.

Ⅳ. 다중 검색엔진을 활용한 보안관제 모델 제안

1. 제안 프로세스 구성

제안한 기본 아이디어는 관제대상이 되는 IP, PORT 등에 대해 정보 수집에 필요한 점검 질의목록을 사전에 작성한 후 다중 검색엔진을 활용한 점검과 더불어 기존의 취약점 점검과 병행한다.

기존의 보안관제 시스템은 예방 프로세스가 정형적인 취약점 점검항목에 의존하여 자산을 보호하였다. 이는 수동적인 관제행위로 정형적인 취약점 분석 항목에 포함되지 않은 취약점에 대해서는 예방하지 못하는 단점을 지닌다. 이를 해결하고자 본 논문에서는 다중 검색엔진을 활용한 취약점 진단을 추가하여 기존 취약점 진단이 가지는 문제점을 능동적으로 보완하려 한다. 즉, 보안관제 요원의 개선된 취약점 예방행위를 추가하여 자산의 취약점을 사전에 제거하고, 앞으로의 공격 가능성도 미리 방지하도록 보다 강화된 점검 프로세스를 제안하였다.

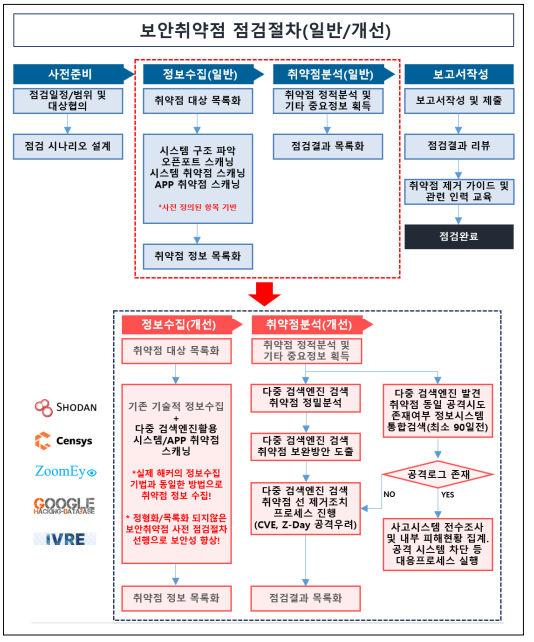

그림 1. 기존 점검 프로세스에 추가된 제안 프로세스 구성도

[그림 1]의 제안 프로세스 구성도를 기준으로 보안취약점 점검 및 분석 절차를 간략히 설명하면 다음과 같다. 첫째, 진단대상 IP 주소영역 범위를 되도록 전체로 설정한 다음 다중 검색엔진을 이용하여 취약점 정보를 취합한다. 둘째, 수집한 배너 정보 정밀 분석 후 대상별

취약점을 목록화한다. 셋째, IT 자산 중요도에 따라 취약점 제거 우선순위 대상을 선정하고 위험도가 높은 취약점부터 보완한다. 넷째, 취약점 보완과 동시에 다중 검색엔진으로 탐지된 위험도가 높은 취약점(CVE 등)의 보안장비 탐지정책을 신속히 추가한다. 다섯째, 정리된 IT 자산 취약점이 검색엔진에 캐싱(Cashing)된 경우 다중 검색엔진 별 직접 요청을 통해 삭제 요청한다.

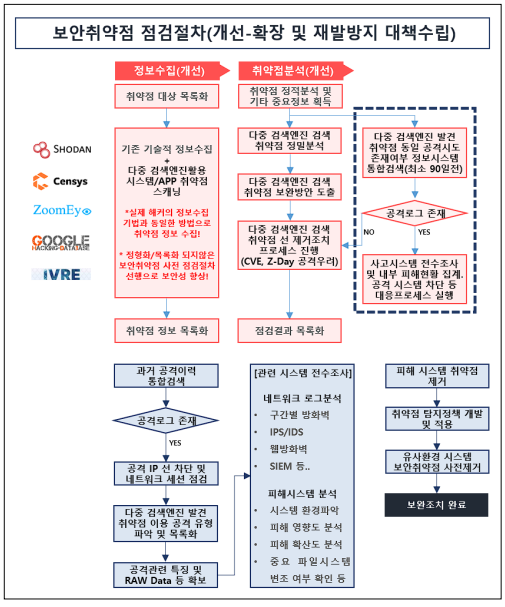

그림 2. 개선된 보안취약점 점검절차-재발방지 대책수립

또한, 제안 프로세스는 [그림 2]에서 보듯이 정형화되지 않은 취약점의 위협 예방은 물론, 특수한 유형의 지능화된 공격의 탐지에도 효과적이다. 다중 검색엔진을 이용한 보안취약점 점검 분석결과 하나의 시스템에 다수의 취약점이 발견되는 경우 특히 유효하다. 이러한 시스템이 다중 검색엔진 취약점 점검에서 탐지되는 경우, 약 90일 이전 과거 시점의 피해 시스템 로그를 순차 정밀분석한다. 이때 피해 시스템의 네트워크 로그, 보안시스템 로그를 포함 시켜 일괄 검사한다. 또한, 보안취약점에 대한 특징 및 패킷 샘플링, 시스템 위협분석, 시스템 피해 확산 및 영향도 분석 등의 프로세스를 동시에 진행한다. 이후 신속하게 순차적 취약점 제거를 수행하여 보안성을 크게 강화할 수 있다. 해당 프로세스는 취약점 점검 팀과 보안관제 팀의 긴밀한 협조를 통해 이루어진다. 이렇듯 개선된 보안관제 모델을 적용하여 예방 측면의 정보보안 활동을 수행한다면 다음과 같은 이점이 있다. 먼저, 향후 발생 가능한 특수하고 민감한 취약점을 이용한 다양한 공격으로부터 전산 인프라를 신속하고 안전하게 보호할 수 있다. 그리고 더 나아가 공격자가 특정 대상을 집요하게 공격하는 APT 공격 등 특수한 공격에 대해 공격 전 또는 공격 도중 차단, 더 나아가 앞으로의 보안 위협을 효과적으로 예방할 수 있다.

2. 제안 프로세스 적용 결과 예시

2.1 기존 보안관제모델에서 취약점 진단

제안한 보안관제 모델이 기존 모델과 비교하여 제안 모델의 타당성을 점검하기 위해 비교실험을 진행하였다. 비교실험에서는 현재 널리 알려진 OWASP(Open Web Application Security Project)에서 발표한 '10 대 웹 취약점'[6] 기준 웹 취약점 진단 항목을 정하고 특정 URL에 대해 모의 취약점 진단을 시행하였다.

표 2. 웹 취약점 진단 항목(OWASP 기준)

웹 취약점 진단 항목		
대상 URL	* 보안 문제로 미기재(실 운영 웹서비스)	
점검 항목	점검 방법	점검결과 (O, X)
부적절한 쿠키/세션 관리	- 쿠키/세션 정보 암호화 점검 - 서버 측 쿠키 유효화 검사 여부 점검 - 복잡한 세션 ID 사용 여부 점검	O
취약한 공개 소프트웨어 사용	- 공개 소프트웨어 취약점 점검 - 안전한 버전 사용 점검	O
XSS(Cross Site Scripting) 취약점	- 입력 값 필터링 점검	O
URL 접속제한 실패	- 중요 URL에 비인가 접근방지 여부 점검	O
부적절한 오류처리	- 프로그램 에러정보 노출 여부 점검	O
*취약점 점검에서 취약점이 발견된 항목은 〈 O 〉 발견되지 않은 항목은 〈 X 〉		

기존관제 모델을 적용한 취약점 점검에서는 [표 2]에서 본 바와 같다. 즉, 시험에서 사용한 점검 URL에 대해서 취약점 진단을 진행하였을 때 10개의 진단 항목

중 5개의 항목에서 취약점이 발견되었다.

2.2 제안 보안관제모델 적용 후 취약점 진단

앞절에서 동일한 시험 환경에서 개선된 보안관제 모델을 적용한 시험을 하였다. 즉, 수동적 보안관제 체계를 능동적인 보안관제 체계로 전환하여 공격자 관점에서 취약점 진단을 시행하였다. 특히, 침투 벡터를 다양화하기 위해 대상 범위를 목표 URL 하나로 국한하지 않았다. 즉, 목표 URL IP의 C 클래스 주소영역으로 확장하여 공격 벡터를 다양화하였다.

앞서 소개한 다중 검색 엔진들을 이용해서 취약점을 수집한 결과는 [표 3]과 같다.

표 3. 웹 취약점 진단 항목(다중 검색엔진 활용)

다중 검색엔진 활용 웹 취약점 진단 항목		
대상 URL	* 보안 문제로 미기재(실 운영 웹서비스)	
취약점 검색엔진	취약점 발견 항목	비고
Shodan Censys Zoomeye IVRE GHDB	- 디렉토리 리스팅	19건
	- 로그인페이지 노출	8건
	- 불필요한 중요정보 노출 • WEB/WAS 애플리케이션 정보 노출 • NTP서버 접속정보 노출 • NTP서버 설정정보 노출 • 웹 프로그래밍 언어 버전정보 노출 • 취약한 쿠키설정정보 노출 • 웹서버 Portmap 설정정보 노출 • SMB 버전정보 노출	21건
	- 웹서버 내부 문서파일 노출	3건
	- 불필요한 포트 노출	31건
	- Github 정보노출	5건
	- 중요 보안시스템 로그인페이지 접근	2건
	- 네트워크 시스템 로그인페이지 접근	1건
	- 불필요 웹 메소드 허용 취약점	3건
	- WAS 기본 설치페이지 노출	6건
	- 기타 CVE 취약점 노출 • CVE-2012-2531, CVE-2018-17199 • CVE-2019-0196, CVE-2018-1312 • CVE-2010-1899, CVE-2018-1333 • CVE-2010-2730, CVE-2010-1256 • CVE-2019-0220, CVE-2012-2532 • CVE-2019-0211, CVE-2017-15715 • CVE-2017-15710, CVE-2010-3972 • CVE-2018-11763, CVE-2018-1283	16건

시험에서 행해진 점검결과는 [표 3]에서와 같이 다양한 치명적 취약점이 추가로 도출되었다. 개선된 보안관제 모델 적용 전후의 보안취약점 진단결과 비교는 [표 4]와 같다.

표 4. 보안취약점 진단시험 결과 비교

	OWASP Top 10 진단기준	제안 모델 진단기준
점검 항목	10개 • 인젝션 • 취약한 인증 • 민감한 데이터 노출 • XML 외부개체 참조 • 취약한 접근 통제 • 잘못된 보안구성 • XSS • 불안한 역직렬화 • 알려진 취약점이 있는 구성요소 사용 • 불충분한 로깅 및 모니터링	**Limitless(제한 없음)** 단 OWASP TOP 10 중 7개 기준도 포함됨 • 취약한 인증 • 민감한 데이터 노출 • XML 외부개체 참조 • 취약한 접근 통제 • 잘못된 보안구성 • 불안한 역직렬화 • 알려진 취약점이 있는 구성요소 사용
진단 대상	1개 URL	진단대상 IP C클래스 주소영역의 모든 애플리케이션 및 전산 인프라(웹, 서버, 네트워크, DB 등)
진단 결과	1개 URL 5개 취약점 발견	8개 URL, 17개 IP 약 115개 취약점 발견
점검 시간	1개 웹, 40페이지 기준 4시간	8개 웹, 17개 IP 기준 1시간
점검 방법	도구이용 자동점검 30% 수동점검 70%	다중검색엔진 활용 100% 자동 점검

진단결과는 다음과 같다. 우선 점검항목 및 도출 취약점 비교결과 제안모델은 115개 취약점 도출로 기존 취약점 진단결과와 현격한 차이를 보였다. 이는 자동 수집되는 다양한 장치 메타데이터에서 분석 가능한 취약점의 종류가 수동 진단에 비해 많기 때문이다.

또한, 취약점 점검시간과 효율성 측면에서 제안방안이 기존 모델대비 월등한 장점을 보였다. 기존 보안관제 모델 취약점 점검의 경우 1개 URL, 10개의 점검항목, 5개 취약점 발견 기준으로 약 4시간의 점검시간을 필요로 하였다. 반면에 제안방안은 17개 IP, 8개 URL, 115개 취약점 발견 및 무제한 점검항목 기준으로 1시간의 점검시간을 보여 투입시간 대비 상당한 효율성의 장점이 있음을 볼 수 있다.

V. 고찰

이 장에서는 제안한 다중 검색엔진을 활용한 보안관제 개선모델이 기존 방식의 웹 애플리케이션 보안 취약

점 점검모델과 비교하여 어떤 특징을 지닌 것인지를 [표 5]에 요약하였다.

표 5. 웹 취약점 점검모델 비교

	기존 취약점 점검모델	제안모델
점검 목록	알려진 취약점 위주의 목록화/규격화된 점검	목록화되지 않거나 다소 알려지지 않은 취약점 점검
점검 도구	자동/수동 점검 도구 (Nmap, Kali Linux 등)	다중 검색엔진 Shodan, Google 등
점검 대상	URL, IP (넓은 범위의 IP 점검은 다소 불편함)	URL, IP (넓은 범위의 IP 점검 용이)
필요 숙련도	취약점 점검 경험이 풍부한 숙련된 인력 필요	검색 템플릿을 사전 작성하면 낮은 숙련도의 인력도 가능
투입 비용	인력, 점검도구 비용 등 상당 비용 발생	이미 구축된 시스템을 이용, 별도비용 없음
소요 시간	웹페이지 규모에 따라 많은 변수 발생	쿼리 입력에 따라 즉시 결과 도출 가능
이행 빈도	낮음(연간 1~2회)	높음 (간단한 점검 프로세스로 정기/수시 설정 가능)
장점	규격화된 명확한 점검 기준을 바탕으로 평균적인 전산인프라 보안성 향상	공격자(해커) 관점에서 규격화되지 않은 공격포인트 사전 점검, 취약점 제거를 통한 보안성향상
단점	규격화된 목록 이외의 점검 어려움, 투입 시간 및 인력 비용 등 상당한 리소스 소모	취약점 유형의 다양성으로 완전한 취약점 제거 조치에 상당한 노력 및 숙련된 인력 필요

검색엔진을 활용한 보안관제 개선모델의 장점을 주요 비교 요소별 항목에 따라 정리하면 다음과 같다.

첫째, 제안모델은 점검항목의 다양성과 점검대상의 확장에 용이하다. 기존 보안관제모델의 취약점 점검의 경우 점검항목 및 진단대상의 확장이 제한적이다. 반면에 제안방안은 취약점 검색엔진의 'Crawler Bot'을 이용한 신규 취약점 자동화 수집이 가능하여 점검항목 확장의 제한이 없다. 또한 IoT(Internet of Things) 검색엔진 기반의 취약점 다중검색 방식으로 점검대상 범위 내 모든 디바이스의 동시 취약점 검색이 가능하다.

둘째, 다중 검색엔진 활용 시 비교적 간단한 선수지식으로 적은 시간을 할애하여 점검이 이루어진다. 따라서 편의성 측면에서도 우수함을 알 수 있다. 이는 검색엔진이 가지는 검색결과의 즉시 노출 특성 때문이다. 이러한 자동화, 간편화된 특성을 이용하여 점검자는 적은 지식과 시간을 들여 최대의 결과를 얻을 수 있다.

셋째, 다중 검색엔진 활용 취약점 점검 진행 시, 일반적인 애플리케이션 취약점 점검에서 발견되지 않는 다양한 치명적 취약점 진단이 가능하다. 이는 기존의 수동 보안 진단의 한계를 보완할 수 있는 장점으로 볼 수 있다.

상기와 같이 요약된 비교내용에서 보듯이 제안 보안관제 모델은 기존 취약점 점검의 불완전한 부분을 보완하였다. 특히 관제센터 요원 또는 보안관리자가 사전에 제안 프로세스[그림 1][그림 2]를 통해 정기적으로 보안관제 대상의 취약점을 발굴/인지할 수 있는 특징을 들 수 있다. 이를 통해서 보다 강화된 보안취약점을 제거할 수 있고, 유사 유형 공격에 대해 사전에 대비할 수 있도록 보안시스템 탐지규칙을 제작 및 우선 적용할 수 있다. 결과적으로 제안모델은 내부 전산 인프라의 보안성 및 안전성 제고에 상당히 긍정적 영향을 미칠 수 있다. 이와 동시에 기존의 보안관제 인력의 역할이 더욱 더 중요해짐에 따라 보안관제 인력의 위치가 견고해지고 기존의 보안관제 프로세스를 획기적으로 개선할 수 있음을 보였다.

Ⅵ. 결론 및 향후 연구

본 논문에서는 기존 보안관제 프로세스에서의 수동적인 대응과 취약점 분석을 진행하는 과정에서 발생하는 한계를 해결하는 방안을 제시하였다. 물론 다중 검색엔진에서 검색된 배너 데이터를 분석하는 능력에 따라 인지 가능한 취약점 영역이 다소 편차가 있다는 점. 그리고 취약점 검색을 위해 검색엔진을 각각 이용해야 한다는 점은 앞으로 개선해야 할 부분이다. 하지만 제안모델은 기존 방식과 달리, 다양한 유형의 취약점 항목에 대해 기구축된 다중 검색엔진을 통해 신속하게 점검할 수 있다. 또한, 점검대상 범위의 확장성이 좋고 동시 점검 수행이 가능하며, 누구에게나 익숙한 방식의 검색형 취약점 점검 수행이 가능하다. 따라서 보안관제 보안취약점 점검업무 수행 시 공격자의 관점에서 점검대상 분석을 쉽게 하고 효율적인 대응을 할 수 있도록 한다. 특히, 취약점이 많은 시스템에 대한 비정상 행위 추적 프로세스 적용으로 최소한의 보안 위협을 목표로

하였다. 따라서 특수한 유형의 공격에 대한 대비도 사전에 할 수 있는 장점이 있다. 즉, 경제성과 신속성, 효율성, 활용도, 예방적 보안 측면에서 기존의 방식보다 장점이 있다. 따라서 제안모델은 보안관제 취약점 진단 업무 수행 시 기존 취약점 진단의 불완전한 요소들을 효과적으로 보완할 수 있는 대안으로 활용 가능할 것으로 사료된다.

향후 연구 방향으로 본 논문에서 언급한 다중 검색엔진 활용 취약점 점검을 하나의 플랫폼에서 자동화할 방안을 연구해야 할 것이다.

참 고 문 헌

[1] 과학기술정보통신부, 한국정보보호산업협회, 2019 정보보호 실태조사, pp.33-34, 2020.

[2] 김영진, 이수연, 권헌영, 임종인, “국가 전산망 보안관제업무의 효율적 수행방안에 관한 연구,” 한국정보보호학회 논문지, 제19권, 제1호, pp.103-111, 2009.

[3] 조이든, 박수진, 강남희, “사물인터넷의 경량 IP 카메라 취약점을 이용한 해킹 공격 및 대응 방안,” 한국디지털콘텐츠학회 논문지, 제20권, 제5호, pp.1069-1077, 2019.

[4] R. Bodenheim, J. Butts, S. Dunlap, and B. Mullins, “Evaluation of the ability of the Shodan search engine to identify Internet-facing industrial control devices,” International Journal of Critical Infrastructure Protection, Vol.7, No.2, pp.114-123, 2014.

[5] 행정안전부, 웹 취약점 표준 점검 항목, p.1, 2019.

[6] OWASP Top Ten Web Application Security Risks | OWASP. (2017). Retrieved from https://owasp.org/www-project-top-ten/

[7] 한규석, 김태규, 심신우, 전성구, 윤지원, “기계학습을 이용한 네트워크 전장정보 수집,” 한국정보과학회 논문지, 제45권, 제10호, pp.1096-1103, 2018.

[8] 김민준, 김귀남, “데이터 마이닝 기반 보안관제 시스템,” 한국융합보안학회 논문지, 제11권, 제6호, pp.3-8, 2011.

[9] 조창섭, 신용태, “보안관제 조직을 위한 사이버보안 프레임워크 개선에 관한 연구,” 한국융합보안학회 논문지, 제19권, 제1호, pp.111-120, 2019.

[10] 이재헌, 이상진. “웹 서비스 특성 기반 효율적인 보안관제 모델 연구,” 한국정보보호학회 논문지, 제29권, 제1호, pp.175-185, 2019.

저 자 소 개

이 제 국(Je-Kook Lee) 준회원

- 2003년 2월 : 충북도립대학교 정보통신학과(전문학사)
- 2015년 8월 : 국가평생교육진흥원 학점은행제 정보통신학과(공학사)
- 2017년 3월 ~ 현재 : 배재대학교 사이버보안학과 석사과정
- 2010년 7월 ~ 현재 : ㈜이글루시큐리티 인프라사업본부 파견관제팀 보안관제 PM

〈관심분야〉 : 보안관제 고도화, 데이터 Visualization, Open Source Security

조 인 준(In-June Jo) 정회원

- 1982년 2월 : 전남대학교 계산통계학과 학사
- 1985년 2월 : 전남대학교 전자계산학과 석사
- 1999년 2월 : 아주대학교 컴퓨터공학과 박사
- 1983년 ~ 1993년 : 한국전자통신연구원 선임연구원
- 1991년 ~ 현재 : 컴퓨터시스템응용기술사
- 2006년 ~ 현재 : 정보시스템수석감리원
- 1994년 ~ 현재 : 배재대학교 사이버보안학과 교수

〈관심분야〉 : 정보보호, 컴퓨터네트워크보안, 컴퓨터시스템응용, 정보시스템감리