

클라우드 취약점 진단 서비스

팀 명 : NightOwl
지도 교수 : 양환석 교수님
팀 장 : 정명원
팀 원 : 이희우
조재환
이예림
한은섬

2022. 10.
중부대학교 정보보호학과

목 차

1. 서론

1.1 연구 배경	4
1.2 연구 필요성	4
1.3 연구 목적 및 주제 선정	4

2. 관련 연구

2.1 Liunx	5
2.2 ESXI	5
2.3 XenServer	5
2.4 Cubrid	5
2.5 MongoDB	5
2.6 MY-SQL	5
2.7 Postgres-SQL	5
2.8 Redis.....	6
2.9 Tomcat	6
2.10 Apache	6
2.11 NginX	6
2.11 Docker	6
2.11 Hadoop	6
2.11 Elasticsearch	6

3. 본론	
3.1 시스템 구성	7
3.2 프로그램 구성	7
3.2.1 진단 스크립트.....	7
3.2.2 웹서버 및 DB	8
4. 결론	
4.1 결론	9
4.2 기대 효과	9
5. 별첨	
5.1 소스 코드	10
5.2 발표 자료	15

1. 서론

1.1 연구 배경

현재 대한민국의 수많은 기업, 국가시설 또는 개인이 서버를 구축하고 사용하고 있다. 서버 및 프로그램의 종류도 엄청 많지만 제대로 관리되고 있는지는 여부는 알 수 없다. 공격자는 관리되지 않은 곳을 통해 취약점을 발견하고 그 취약점을 통해 정보시스템 파괴, 개인정보 유출, 홈페이지 위·변조 등의 피해를 발생시켜 정보시스템을 운영하는 기관과 개인이 운영하고 있는 서버까지 신뢰 하락과 많은 손실을 입고 있다. 이러한 문제점을 막기 위해 KISA(한국인터넷진흥원)에서 제공하는 취약점 진단 가이드를 참고하여 프로그램을 제작하였다.

1.2 연구 필요성

법에 명시된 것처럼 주요정보통신기반시설, 전자금융기반시설 또는 개인정보를 처리하는 기업들은 주기적인 보안 점검을 수행함으로써 주요 자산이 위협에 노출되는 것을 방지해야 할 의무가 있다. 또한 지속적으로 발생하는 공개 취약점, 진화하는 기술, 인프라 환경 변화에 의한 위협 노출 등에 대응하기 위해 주기적인 취약점 점검이 필요하다. 사고는 언제나 모르는 사이에 갑작스럽게 일어나는데 취약점도 똑같이 어느 순간 갑자기 일어나는데 우리는 그것을 막기 위해 항상 대비를 해야한다. 따라서 위협을 줄이기 위해서는 점검 주기가 짧을수록 좋지만, 기업의 환경과 각각의 시스템 특성을 고려하여, 수행 가능한 수준에서 가장 짧은 주기로 취약점을 점검하는 것이 필요하다.

1.3 연구 목적 및 주제 선정



[그림 1. 클라우드 보안 사고]

이번 연구는 클라우드 서비스의 수요가 증가함에 따라서, 각종 보안 위협에 대응하기 위해 각 항목에 관하여 공부 및 사용법을 숙지하고, 항목마다 취약점을 검사하여 취약점을 사용자 또는 서버에게 어떠한 점이 취약한지 확인하고, 또한 그 취약점을 가지고 모의

해킹 시뮬레이션을 통하여 어떤 방법으로 침입이 가능하고 어떠한 취약점이 있는지를 진단하고 알려주기 위하여 주제로 선정하였다.

2. 관련 연구

2.1 Linux

리눅스는 1991년 9월 17일 리누스 토르발스가 처음 출시한 운영 체제 커널인 리눅스 커널에 기반을 둔 오픈 소스 유닉스 계열 운영 체제 계열이다. 리눅스는 일반적으로 리눅스 배포판 안에 패키지 처리된다.

2.2 ESXI

VM웨어 ESXi는 가상 컴퓨터를 배치하고 서비스를 제공할 목적으로 VM웨어가 개발한 엔터프라이즈 계열 타입 1 하이퍼바이저이다. 타입 1 하이퍼바이저로서 ESXi는 운영 체제에 설치하는 응용 소프트웨어가 아니며, 대신 커널과 같은 중요한 운영 체제 구성 요소를 포함, 통합하고 있다.

2.3 XenServer

XenServer는 가상화 된 서버 인프라를 생성하고 관리 할 수있는 하이퍼 바이저 플랫폼이다. Citrix Systems가 개발했으며 Xen 가상 머신 하이퍼 바이저를 통해 구축되었다. XenServer는 서버 가상화 및 모니터링 서비스를 제공한다.

2.4 Cubrid

CUBRID는 관계형 데이터베이스 관리 시스템의 이름이며, 오픈 소스 소프트웨어이다. DBMS 엔진 부분은 아파치라이선스 2.0 라이선스가 적용되고 인터페이스 부분은 BSD 라이선스가 적용되었으며, 국제표준화기구의 표준 구조화 조회 언어를 지원한다

2.5 MongoDB

몽고DB는 크로스 플랫폼 도큐먼트 지향 데이터베이스 시스템이다. NoSQL 데이터베이스로 분류되는 몽고DB는 JSON과 같은 동적 스키마형 도큐먼트들을 선호함에 따라 전통적인 테이블 기반 관계형 데이터베이스 구조의 사용을 삼간다.

2.6 MY-SQL

MySQL은 세계에서 가장 많이 쓰이는 오픈 소스의 관계형 데이터베이스 관리 시스템이다. 다중 스레드, 다중 사용자 형식의 구조질의어 형식의 데이터베이스 관리 시스템으로서 오라클이 관리 및 지원하고 있으며, Qt처럼 이중 라이선스가 적용된다.

2.7 Postgres-SQL

PostgreSQL은 확장 가능성 및 표준 준수를 강조하는 객체-관계형 데이터베이스 관리

시스템의 하나이다. BSD 허가권으로 배포되며 오픈소스 개발자 및 관련 회사들이 개발에 참여하고 있다.

2.8 Redis

Redis는 Remote Dictionary Server의 약자로서, "키-값" 구조의 비정형 데이터를 저장하고 관리하기 위한 오픈 소스 기반의 비관계형 데이터베이스 관리 시스템이다. 2009년 살바토르 산필리포가 처음 개발했다. 2015년부터 Redis Labs가 지원하고 있다.

2.9 Tomcat

톰캣은 아파치 소프트웨어 재단에서 개발한 서블릿 컨테이너만 있는 웹 애플리케이션 서버이다. 톰캣은 웹 서버와 연동하여 실행할 수 있는 자바 환경을 제공하여 자바서버 페이지와 자바 서블릿이 실행할 수 있는 환경을 제공하고 있다.

2.10 Apache

아파치 HTTP 서버는 아파치 소프트웨어 재단에서 관리하는 오픈 소스, 크로스 플랫폼 HTTP 웹 서버 소프트웨어다. BSD, 리눅스 등 유닉스 계열 뿐 아니라 마이크로소프트 윈도우나 노벨 넷웨어 같은 기종에서도 무료로 운용할 수 있다.

2.11 NginX

Nginx는 웹 서버 소프트웨어로, 가벼움과 높은 성능을 목표로 한다. 웹 서버, 리버스 프록시 및 메일 프록시 기능을 가진다.

2.12 Docker

도커는 리눅스의 응용 프로그램들을 프로세스 격리 기술들을 사용해 컨테이너로 실행하고 관리하는 오픈 소스 프로젝트이다. 도커 웹 페이지의 기능을 인용하면 다음과 같다: 도커 컨테이너는 일종의 소프트웨어를 소프트웨어의 실행에 필요한 모든 것을 포함하는 완전한 파일 시스템 안에 감싼다.

2.13 Hadoop

하둡은 대량의 자료를 처리할 수 있는 큰 컴퓨터 클러스터에서 동작하는 분산 응용 프로그램을 지원하는 프리웨어 자바 소프트웨어 프레임워크이다. 원래 너치의 분산 처리를 지원하기 위해 개발된 것으로, 아파치 루씬의 하부 프로젝트이다.

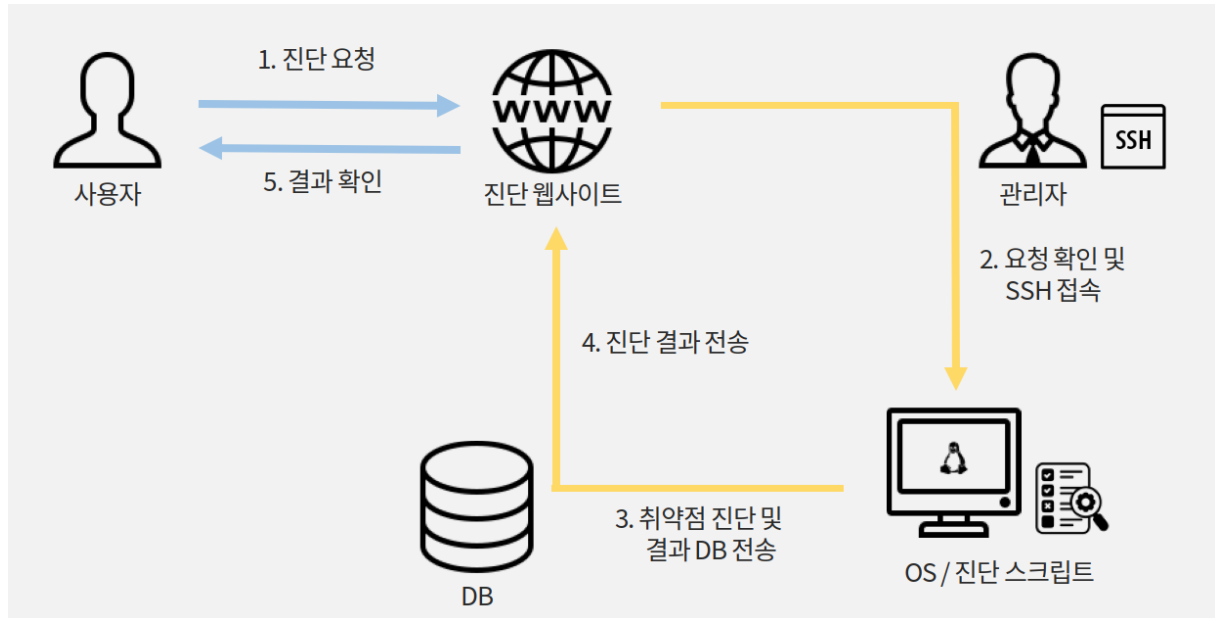
2.14 Elasticsearch

Elasticsearch 루씬 기반의 검색 엔진이다. HTTP 웹 인터페이스와 스키마에서 자유로운 JSON 문서와 함께 분산 멀티테넌트 지원 전문 검색 엔진을 제공한다. 일래스틱서치는 자바로 개발되어 있으며 아파치 라이선스 조항에 의거하여 오픈 소스로 출시되어 있다.

3. 본론

3.1 시스템 구성

진단 요청받은 서버를 관리자가 진단서버에 원격 접속하여 취약점 진단후, 진단 결과 데이터를 DB에 전송하여 웹으로 출력 해 사용자가 결과를 확인할 수 있는 구성이다.



3.2 프로그램 구성

3.2.1 진단 스크립트

클라우드 서비스 기반의 시스템은 기존의 물리적 인프라 기반의 서비스에 비해 전사관점의 투자 리스크를 줄이고 보다 효율적인 시스템의 구축과 운영을 가능하게 한다. 그러나 이러한 장점을 제공하기 위한 클라우드 서비스의 서비스모델과 기술적 관점의 특징으로 인해 기존보다 더 많은 보안 취약점에 노출될 수 있다. 이러한 보안 취약점에 효과적인 대응을 하기 위해서는 이러한 클라우드 서비스의 특징을 이해하고 이를 기반으로 한 기술적/관리적 보안 대응책을 정의하고 실행하는 것이 필요하다. 그리하여 KISA의 클라우드 웹 취약점 진단 가이드를 활용하여 15가지 항목을 가지고 취약점 진단 스크립트를 작성했다.

3.2.2 웹서버 및 DB *

SSH 프로토콜을 이용하여 해당 서버에 원격 접속 후, 진단 스크립트를 실행.

진단 결과를 관리자 PC에 가져와 DB에 저장을 하게 된다. DB에 저장되는 데이터는 진단 구분, 진단 코드, 진단 항목, 취약 또는 양호, 항목 DB에 저장된 값을 웹으로 가져와 취약한 것과 양호한 것을 출력해 주고 취약하면 어떤 부분이 뭐 때문에 취약한지 보여준

다.

개발내용

진단 항목	취약 항목	양호 항목	수동 항목	요청 항목
24	10	7	7	ESXi

분류	진단 코드	중요도	진단 항목	위험도	진단 결과	조치 방법
계정관리	ES-01	상	root 계정 원격 접속 제한	위약	PermitRootLogin 설정이 yes로 설정되어 있음	PermitRootLogin 설정을 no로 변경
계정관리	ES-02	상	취약한 패스워드 사용제한	수동	패스워드 크레딧 톨업 존 디폴트 (John the Ripper)를 이용하여 취약한 패스워드 확인	지역별 부서별 담당자-성명-대표 업무명 root-admin 등과 같은 패스워드는 피해야함.
계정관리	ES-03	상	계정 잠금 임계값 설정	위약	계정 잠금 임계값이 5회 초과로 현재 계정 임계값이 8회이므로 수정 설정되어 있음	
계정관리	ES-04	상	사용자 계정 관리	수동	es) esxi system permission list 사용자 계정 관련 확인	권한 설정 esxi system permission set --uid test1 -- ReadOnly
보안관리	ES-05	중	사용자 계정 관리	양호	ESXi Shell이 비활성화 되어있음	-
보안관리	ES-06	중	ESXi Shell 자동 종료	양호	ESXi Shell 시간 초과 설정이 86400초로 설정되어 있음	-
보안관리	ES-07	중	ESXi Shell 및 SSH 세션 타임아웃 설정	양호	유효 세션에 대한 시간 초과 설정이 86400초로 설정되어 있음	-
보안관리	ES-08	상	가상 스위치 MAC 주소 변경 정책 설정	양호	가상 스위치의 MAC 주소 변경 정책이 거부로 설정되어 있음	-
보안관리	ES-09	상	가상 스위치 Promiscuous 모드 정책 설정	위약	가상 스위치의 Promiscuous 모드 정책 허용으로 설정되어 있음	es) esxi network vswitch standard policy security set -v "[가상 스위치 이름]" -p false 입력
보안관리	ES-10	상	가상 스위치 Forged Transmits 모드 정책 설정	위약	가상 스위치의 Forged Transmits 정책이 허용으로 설정되어 있음	es) esxi network vswitch standard policy security set -v "[가상 스위치 이름]" -f false 입력
보안관리	ES-11	상	SSH 기본 비밀번호 사용 인증 허용 제한	양호	PermitEmptyPasswords 설정이 있거나 no로 설정되어 있음	

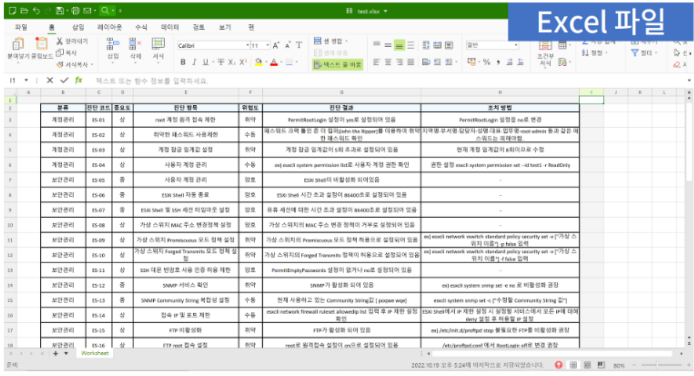
진단 결과 페이지

점검표 확인

개발내용

사용자 이름	IP 주소	사용자 계정	root 비밀번호	요청 항목	결과	진단 결과	Excel	요청 시간
정명권	192.168.100.128	root	ouddhjs@5134	ESXi	완료	확인하기	다운로드	2022-10-19 16:44:35

Excel 파일



사용자 페이지

클라이언트 진단 결과 확인

4. 결론

4.1 결론

클라우드 취약점 진단 스크립트 항목에 대한 이해도를 높였으며 리눅스의 명령어 사용 방법과 항목에 대한 설정을 알게 되었고 설정 파일, 권한 설정, 비밀번호 설정이 취약하게 설정되어있을 경우 어떤 문제가 발생 되는지 알게 되었다. 각 항목에 대해서 클라우드 취약점 진단 스크립트를 사용했을 경우 취약점을 확인하고 보안이 가능하다.

4.2 기대효과

현재 클라우드 서비스는 단순 저장 기능뿐만 아닌 IT분야의 전체를 아우르고 있다. 이러한 클라우드 서비스의 보안이 취약할 경우 기업, 회사의 경제적, 비경제적 손실이 막대할 것으로 예상된다. 이런 이유로 서버에 대한 취약점 진단이 중요하다. 클라우드 취약점 진단 스크립트를 사용할 경우 수많은 서버를 취약점 진단 검사가 가능하다. 그리고 원격으로 진단하기에 장소의 구애를 받지 않고, 원격으로 하지만 통신은 SSH로 통신을 하여 전송할 때는 암호화된 데이터를 전송하기에 네트워크 공격으로부터 보호를 받을 수 있다. 또 한 웹으로 진단요청 및 확인과 재검사도 가능하며 이전에 진단했던 기록도 확인할 수 있다. 위와 같은 취약점 분석 스크립트를 이용한다면 피해 상황을 미리 방지하고 대응 및 사전 준비가 용이할 것으로 예상된다.

5. 별첨

5.1 발표 자료

클라우드 취약점 점검 가이드
- 보안설정(CCE)
| 2020. 12. 1

KISA 한국인터넷진흥원

소개

2.2. ESX

계정 관리(사제 항목), 파일 시스템 및 로그 관리(사제 항목) 중 4

구분	항목번호	항목명
기. 계정 관리	ES-01	root 권한
	ES-02	접근권
	ES-03	계정
	ES-04	접근권
	ES-05	접근권
	ES-06	접근권
	ES-07	접근권
	ES-08	접근권
	ES-09	접근권
	ES-10	접근권
	ES-11	접근권
	ES-12	접근권
	ES-13	접근권
	ES-14	접근권
	ES-15	접근권
	ES-16	접근권
	ES-17	접근권
	ES-18	접근권
	ES-19	접근권
	ES-20	접근권
	ES-21	접근권
	ES-22	접근권
	ES-23	접근권
	ES-24	접근권
	ES-25	접근권
	ES-26	접근권
	ES-27	접근권
	ES-28	접근권

2.3. Linux

계정 관리(사제 항목), 파일 시스템 및 로그 관리(사제 항목) 중 4

구분	항목번호	항목명
기. 계정 관리	LI-01	root 권한
	LI-02	접근권
	LI-03	계정
	LI-04	접근권
	LI-05	접근권
	LI-06	접근권
	LI-07	접근권
	LI-08	접근권
	LI-09	접근권
	LI-10	접근권
	LI-11	접근권
	LI-12	접근권
	LI-13	접근권
	LI-14	접근권
	LI-15	접근권
	LI-16	접근권
	LI-17	접근권
	LI-18	접근권
	LI-19	접근권
	LI-20	접근권
	LI-21	접근권
	LI-22	접근권
	LI-23	접근권
	LI-24	접근권
	LI-25	접근권
	LI-26	접근권
	LI-27	접근권
	LI-28	접근권
	LI-29	접근권
	LI-30	접근권
	LI-31	접근권
	LI-32	접근권
	LI-33	접근권
	LI-34	접근권
	LI-35	접근권
	LI-36	접근권
	LI-37	접근권
	LI-38	접근권
	LI-39	접근권
	LI-40	접근권
	LI-41	접근권
	LI-42	접근권
	LI-43	접근권
	LI-44	접근권
	LI-45	접근권
	LI-46	접근권
	LI-47	접근권
	LI-48	접근권
	LI-49	접근권
	LI-50	접근권

2.16. Docker

Host 설정(사제 항목), 도커 엔진 설정(사제 항목), 도커 엔진 설정(사제 항목), 컨테이너 이미지 및 빌드(사제 항목), 컨테이너 관리(사제 항목) 중 8개 항목(사제 항목)으로 구성된다.

구분	항목번호	항목명	항목 상세	항목 상세
기. Host 설정	DO-01	도커 엔진 설치 여부		항목
	DO-02	도커 그룹에 불일치한 사용자 계정		항목
	DO-03	Docker daemon audit 모듈		항목
	DO-04	AvahiDocker audit 설정		항목
	DO-05	AtDocker audit 설정		항목
	DO-06	docker-secure audit 설정		항목
	DO-07	docker-secure audit 설정		항목
	DO-08	AtDocker audit 설정		항목
기. 도커 엔진	DO-09	default bridge 모듈 컨테이너 간 네트워크 브리징		항목
	DO-10	도커 클러스터링 모듈 설정		항목
	DO-11	legacy registry v1 지원 여부		항목
	DO-12	도커 엔진 컨테이너 이미지나 레인		항목
	DO-13	docker-secure 모듈 설정		항목
	DO-14	docker-secure 모듈 설정		항목
	DO-15	docker-secure 모듈 설정		항목
	DO-16	docker-secure 모듈 설정		항목
	DO-17	AtDocker audit 모듈 설정		항목
	DO-18	AtDocker audit 모듈 설정		항목
	DO-19	AtDocker audit 모듈 설정		항목
	DO-20	AtDocker audit 모듈 설정		항목
	DO-21	AtDocker audit 모듈 설정		항목
	DO-22	AtDocker audit 모듈 설정		항목
	DO-23	AtDocker audit 모듈 설정		항목
	DO-24	AtDocker audit 모듈 설정		항목
	DO-25	AtDocker audit 모듈 설정		항목
	DO-26	AtDocker audit 모듈 설정		항목
	DO-27	AtDocker audit 모듈 설정		항목
	DO-28	AtDocker audit 모듈 설정		항목
	DO-29	AtDocker audit 모듈 설정		항목
	DO-30	AtDocker audit 모듈 설정		항목
	DO-31	AtDocker audit 모듈 설정		항목
	DO-32	AtDocker audit 모듈 설정		항목
	DO-33	AtDocker audit 모듈 설정		항목
	DO-34	AtDocker audit 모듈 설정		항목
	DO-35	AtDocker audit 모듈 설정		항목
	DO-36	AtDocker audit 모듈 설정		항목
	DO-37	AtDocker audit 모듈 설정		항목
	DO-38	AtDocker audit 모듈 설정		항목
	DO-39	AtDocker audit 모듈 설정		항목
	DO-40	AtDocker audit 모듈 설정		항목
	DO-41	AtDocker audit 모듈 설정		항목
	DO-42	AtDocker audit 모듈 설정		항목
	DO-43	AtDocker audit 모듈 설정		항목
	DO-44	AtDocker audit 모듈 설정		항목
	DO-45	AtDocker audit 모듈 설정		항목
	DO-46	AtDocker audit 모듈 설정		항목
	DO-47	AtDocker audit 모듈 설정		항목
	DO-48	AtDocker audit 모듈 설정		항목
	DO-49	AtDocker audit 모듈 설정		항목
	DO-50	AtDocker audit 모듈 설정		항목

주요정보통신기반시설 클라우드 취약점 점검 가이드 2020 기반

주제 선정 이유

날짜	보안사고 원인(내부 관리 실수)	내용
2019년 09월	클라우드서비스제공기업(CSP) 실수	A/S 내부 직원 중 장애 발생 (인명피해, 데이터면허 등 서비스 중단)
2017년 03월	클라우드서비스제공기업(CSP) 실수	A/S 내부 관리 실수 (데이터면허, 클라우드 등 서비스 중단)
2018년 11월	클라우드서비스제공기업(CSP) 실수	A/S 사용자인 DNS 서버 설정 오류 (URL, 메일, 무명 등 서비스 중단)
09월	고객사 실수	인도 클라우드 서비스 제공 (개인정보 무단인용)
07월	고객사 실수	중국어 서버, 직원 실수 (고객사 데이터 유출)
2019년 01월	고객사 실수	클라우드 계정 관리 실수 (개인정보 240만건 유출)
	고객사 실수	A/S 관리자서버서 서버 설정 오류 (고객정보 대량 유출)

구분	항목번호	항목명
기. 계정 관리	ES-01	root 권한
	ES-02	접근권
	ES-03	계정
	ES-04	접근권
	ES-05	접근권
	ES-06	접근권
	ES-07	접근권
	ES-08	접근권
	ES-09	접근권
	ES-10	접근권
	ES-11	접근권
	ES-12	접근권
	ES-13	접근권
	ES-14	접근권
	ES-15	접근권
	ES-16	접근권
	ES-17	접근권
	ES-18	접근권
	ES-19	접근권
	ES-20	접근권
	ES-21	접근권
	ES-22	접근권
	ES-23	접근권
	ES-24	접근권
	ES-25	접근권
	ES-26	접근권
	ES-27	접근권
	ES-28	접근권

구분	항목번호	항목명	항목 상세	항목 상세
기. Host 설정	DO-01	도커 엔진 설치 여부		항목
	DO-02	도커 그룹에 불일치한 사용자 계정		항목
	DO-03	Docker daemon audit 모듈		항목
	DO-04	AvahiDocker audit 설정		항목
	DO-05	AtDocker audit 설정		항목
	DO-06	docker-secure audit 설정		항목
	DO-07	docker-secure audit 설정		항목
	DO-08	AtDocker audit 설정		항목
기. 도커 엔진	DO-09	default bridge 모듈 컨테이너 간 네트워크 브리징		항목
	DO-10	도커 클러스터링 모듈 설정		항목
	DO-11	legacy registry v1 지원 여부		항목
	DO-12	도커 엔진 컨테이너 이미지나 레인		항목
	DO-13	docker-secure 모듈 설정		항목
	DO-14	docker-secure 모듈 설정		항목
	DO-15	docker-secure 모듈 설정		항목
	DO-16	docker-secure 모듈 설정		항목
	DO-17	AtDocker audit 모듈 설정		항목
	DO-18	AtDocker audit 모듈 설정		항목
	DO-19	AtDocker audit 모듈 설정		항목
	DO-20	AtDocker audit 모듈 설정		항목
	DO-21	AtDocker audit 모듈 설정		항목
	DO-22	AtDocker audit 모듈 설정		항목
	DO-23	AtDocker audit 모듈 설정		항목
	DO-24	AtDocker audit 모듈 설정		항목
	DO-25	AtDocker audit 모듈 설정		항목
	DO-26	AtDocker audit 모듈 설정		항목
	DO-27	AtDocker audit 모듈 설정		항목
	DO-28	AtDocker audit 모듈 설정		항목
	DO-29	AtDocker audit 모듈 설정		항목
	DO-30	AtDocker audit 모듈 설정		항목
	DO-31	AtDocker audit 모듈 설정		항목
	DO-32	AtDocker audit 모듈 설정		항목
	DO-33	AtDocker audit 모듈 설정		항목
	DO-34	AtDocker audit 모듈 설정		항목
	DO-35	AtDocker audit 모듈 설정		항목
	DO-36	AtDocker audit 모듈 설정		항목
	DO-37	AtDocker audit 모듈 설정		항목
	DO-38	AtDocker audit 모듈 설정		항목
	DO-39	AtDocker audit 모듈 설정		항목
	DO-40	AtDocker audit 모듈 설정		항목
	DO-41	AtDocker audit 모듈 설정		항목
	DO-42	AtDocker audit 모듈 설정		항목
	DO-43	AtDocker audit 모듈 설정		항목
	DO-44	AtDocker audit 모듈 설정		항목
	DO-45	AtDocker audit 모듈 설정		항목
	DO-46	AtDocker audit 모듈 설정		항목
	DO-47	AtDocker audit 모듈 설정		항목
	DO-48	AtDocker audit 모듈 설정		항목
	DO-49	AtDocker audit 모듈 설정		항목
	DO-50	AtDocker audit 모듈 설정		항목

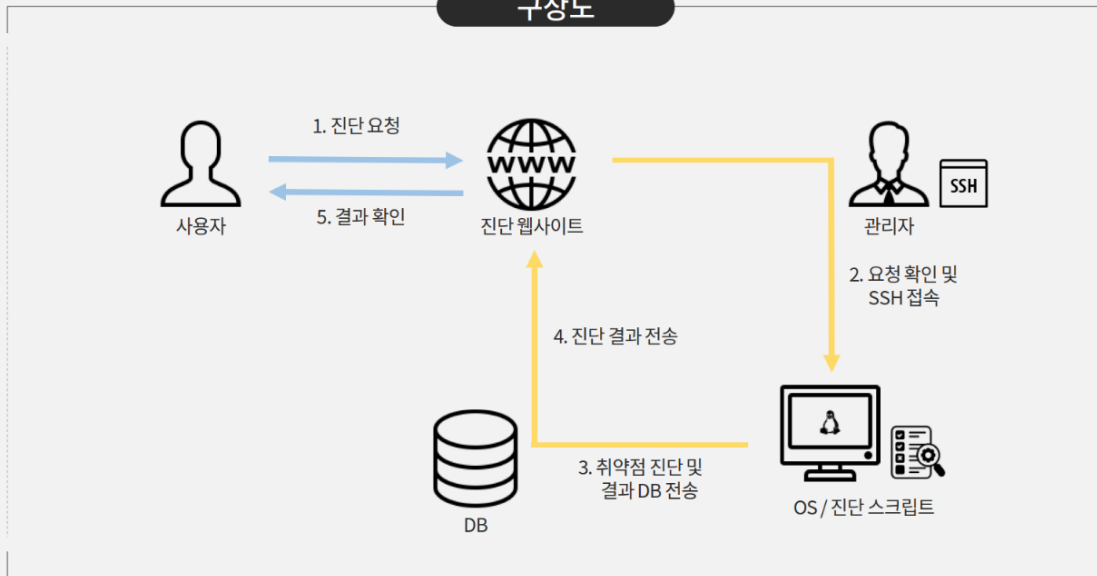
클라우드 도입 시 느낀 어려움 (단위: %)

47.0	44.0	40.3	34.3	32.8	29.9	20.9
보안 우려	IT기술 전문성 부족 (내부 부족)	클라우드 비용관리	클라우드/하이브리드 클라우드 구축	클라우드 도입 관리 우려	클라우드/하이브리드 클라우드 통합 관리의 복잡성	단일 클라우드 활용에 클라우드 관리 어려움 및 중복

클라우드 보안 위협의 심각성과 대응의 중요성

- 10 -

구상도



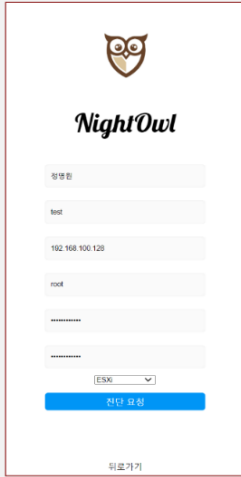
개발내용

The screenshot shows the main page and a login modal for the NightOwl service:

- Main Page (메인 페이지)**:
 - Header: NightOwl 클라우드 취약점 진단 서비스
 - Section: 본 서비스는
 - Text: 클라우드 보안 인증 담당자 및 클라우드 담당자의 책임관리를 위해 CCE 취약점에 대한 기술적 보안 서비스를 제공합니다. IS영역의 진단 서비스를 제공하여 진단목록, 진단개요, 진단결과, 조치방법으로 구성되어 있습니다.
 - Image: A cloud with a padlock icon.
- Login Modal (회원가입)**:
 - Fields: 비밀번호 (Password), text, ...
 - Buttons: 회원가입 (Join), 뒤로가기 (Back)

메인 페이지 & 회원가입

개발내용



NightOwl

아이디: test
 비밀번호: 192.168.100.128
 사용자명: root
 이메일: *****
 비밀번호: *****
 ESKM (선택)
 [전단 요청] 버튼
 [뒤로가기] 링크

사용자 이름	IP 주소	사용자 계정	root 비밀번호	요청 항목	결과	진단 결과	Excel	요청 시간
정영원	192.168.100.128	root	ouddrj@5134	ESXI	대기중	진단하기	다운로드	2022-10-19 16:44:35

localhost의 메시지

요청 처리중

[확인] 버튼

사용자 페이지

클라이언트진단 요청

개발내용



요청목록
 회원리스트
 로그아웃

사용자 이름	사용자 아이디	IP 주소	사용자 계정	root 비밀번호	요청 항목	상태	요청 시간	완료 메시지	결과 전송
정영원	test	192.168.100.128	root	ouddrj@5134	ESXI	대기중	2022-10-19 16:44:35	전송	업로드

OpenSSH SSH client

```

C:\WINDOWS\system32>scp C:\owl.tar root@192.168.100.128:/CLOUD
Password:
owl.tar 100% 55KB 10.8MB/s 00:00
C:\WINDOWS\system32>ssh root@192.168.100.128 -p 22
Password:
The time and date of this login have been sent to the system logs.
WARNING:
All commands run on the ESXi shell are logged and may be included in
support bundles. Do not provide passwords directly on the command line.
Most tools can prompt for secrets or accept them from standard input.
VMware offers supported, powerful system administration tools. Please
see www.vmware.com/go/sysadmintools for details.
The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@localhost:~] cd /CLOUD
[root@localhost:~] ls
owl.tar
[root@localhost:~]
    
```

관리자 페이지

요청 정보를 토대로 진단 파일 전송 & 원격 접속

개발내용

```

OpenSSH SSH client
[root@localhost:/CLOUD] tar xvf owl.tar
ESXi.tar
main.sh
[root@localhost:/CLOUD] sh main.sh
main.sh: line 6: figlet: not found

진단일시 : 2022년 05월 21일 17시 32분

1) 부분진단
2) 전체진단
3) 종료하기
1)
1) XenServer
2) ESXi
3) Linux
4) Cubrid
5) MongoDB
6) MY-SQL
7) Postgres-SQL
8) Redis
9) Tomcat
10) Apache
11) Nginx
12) Docker
13) OpenStack
14) Hadoop
15) Elasticearch
3) 종료하기
2
ESXi 진단이 완료되었습니다.
q
Thank you
[root@localhost:/CLOUD]
    
```

```

관리자: NightOwl
C:\WINDOWS\system32\cmd.exe /c scp root@192.168.100.128:/Nightowl/DB.txt C:\WDB.txt
Password:
DB.txt

C:\WINDOWS\system32\cmd.exe /c scp root@192.168.100.128:/Nightowl/Score.txt C:\WScore.txt
Password:
Score.txt

C:\WINDOWS\system32>
    
```

진단 완료 후 관리자 PC로 파일 전달

개발내용

사용자 이름	사용자 아이디	IP 주소	사용자 계정	root 비밀번호	요청 항목	상태	요청 시간	완료 메시지	결과 전송
정영필	test	192.168.100.128	root	audrnp@5134	ESX	완료	2022-10-19 16:44:35	전송	성공

요청목록
회원리스트
로그아웃


```

DB.txt
#vimdb - Windows 메모장
권한이 없습니다. 서식(아 보기)이 적용되어
계정관리: ES-01 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-02 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-03 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-04 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-05 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-06 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-07 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-08 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-09 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-10 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-11 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-12 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-13 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-14 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-15 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-16 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-17 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-18 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-19 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-20 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-21 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-22 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-23 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
계정관리: ES-24 사용자, root 계정 관리 가능. 계정, PermitRootLogin 설정이 yes로 설정되어 있음. PermitRootLogin 설정을 no로 변경함
    
```

관리자 페이지

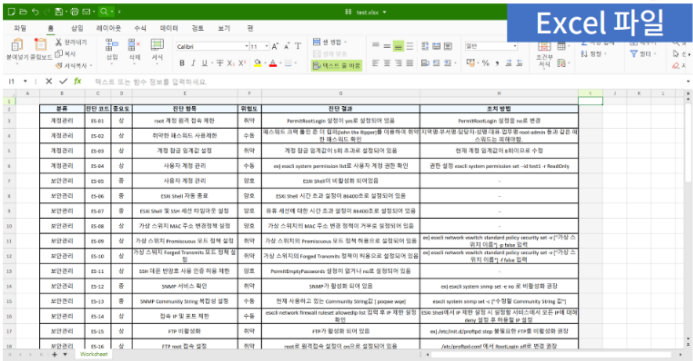
사용자에게 완료 메시지 & 결과물 전송

개발내용



진단요청
등록현황
로그아웃

사용자 이름	IP 주소	사용자 계정	root 비밀번호	요청 항목	결과	진단 결과	Excel	요청 시간
정명원	192.168.100.128	root	ouddhjs@5134	ESXI	완료	확인하기	다운로드	2022-10-19 16:44:35



Excel 파일

사용자 페이지

클라이언트 진단 결과 확인

개발내용

NightOwl		종목/진행				
진단 항목	취약 항목	알고 항목	수동 항목	요청 항목		
24	10	7	7	ESXI		
분류	진단 코드	중요도	진단 항목	위험도	진단 결과	조치 방법
계정관리	ES-01	상	root 계정 원격 접속 제한	취약	PermitRootLogin 설정이 yes로 설정되어 있음	PermitRootLogin 설정을 no로 변경
계정관리	ES-02	상	취약한 패스워드 사용제한	수동	패스워드 규칙 설정 중 디 톨바 시퀀스 포함 검사 및 Light the Ripper를 이용하여 취약한 패스워드 확인	시퀀스 포함 검사 설정 해제, 일부 root/admin 등과 같은 패스워드는 약한 패스워드 확인
계정관리	ES-03	상	계정 잠금 임계값 설정	취약	계정 잠금 임계값이 5회 초과로 설정되어 있음	현재 계정 임계값이 5회이므로 수정 설정되어 있음
계정관리	ES-04	상	사용자 계정 관리	수동	ex) esxi system permission list 로 사용자 계정 관련 확인	권한 설정 esxi system permission set --id test1 - ReadOnly
보안관리	ES-05	중	사용자 계정 관리	양호	ESXI Shell이 비활성화 되어있음	-
보안관리	ES-06	중	ESXI Shell 자동 종료	양호	ESXI Shell 시간 초과 설정이 86400초로 설정되어 있음	-
보안관리	ES-07	중	ESXI Shell 및 SSH 세션 타임 아웃 설정	양호	유용 세션에 대한 시간 초과 설정이 86400초로 설정되어 있음	-
보안관리	ES-08	상	가상 스위치 MAC 주소 변경 정책 설정	양호	가상 스위치의 MAC 주소 변경 정책이 거부로 설정되어 있음	-
보안관리	ES-09	상	가상 스위치 Promiscuous 모드 정책 설정	취약	가상 스위치의 Promiscuous 모드 정책 허용으로 설정되어 있음	ex) esxi network vswitch standard policy security set -v "[가상 스위치 이름]" -p false 입력
보안관리	ES-10	상	가상 스위치 Forged Transmits 모드 정책 설정	취약	가상 스위치의 Forged Transmits 정책이 허용으로 설정되어 있음	ex) esxi network vswitch standard policy security set -v "[가상 스위치 이름]" -f false 입력
보안관리	ES-11	상	SSH 데몬 비밀번호 사용 인증 허용 제한	양호	PermitEmptyPasswords 설정이 없거나 no로 설정되어 있음	-

점검표 확인

5.2 소스코드 *

<https://github.com/pingmem/Nightowl>