Cloud 취약점 진단 서비스

7조 NightOwl

지도교수 : 양환석 교수님

팀장 : 정명원

이희우

조재환

한은섬

이예림

목차

서버 취약점 진단 서비스

소개

2.2. ESXi

계정 관리(4개 항목), 파일 시
24개 항목으로 구성된다.

구분	진단코드
가. 계정 관리	ES-01
	ES-02
	ES-03
	ES-04
나. 파일 시스템	ES-05
	ES-06
	ES-07
	ES-08
	ES-09
	ES-10
	ES-11
	ES-12
	ES-13
	ES-14
	ES-15
	ES-16
	ES-17
	ES-18
	ES-19
	ES-20
	ES-21
	ES-22
다. 패치 관리	ES-23
	ES-24

2.3. Linux

계정 관리(5개 항목), 파일 및
패치 및 로그 관리(2개 항목) 총 4

구분	진단코드	
가. 계정 관리	U-01	root
	U-02	패스워
	U-03	계정
	U-04	패스워
	U-05	패스워
나. 파일 및 디렉토리 관리	U-06	root
	U-07	파일
	U-08	/etc/pa
	U-09	/etc/sh
	U-10	/etc/ho
	U-11	/etc/(x
	U-12	/etc/sy
	U-13	/etc/se
	U-14	SUID,
	U-15	사용자
	U-16	world
	U-17	$HOM
	U-18	접속
	U-19	cron
다. 서비스 관리	U-20	Finger
	U-21	Anony
	U-22	r 계열
	U-23	DoS
	U-24	NFS
	U-25	NFS
	U-26	autom
	U-27	RPC
	U-28	NIS, N
	U-29	tftp, ta
	U-30	Sendm
	U-31	스팸
	U-32	일반사
	U-33	DNS
	U-34	DNS Z
라. 패치 및 로그관리	U-35	최신
	U-36	로그의

[표 3] Linux

2.16. Docker

Host 설정(8개 항목), 도커 데몬 설정(4개 항목), 도커 데몬 설정 파일(12개 항목), 컨테이너 이미지 및 빌드 파일(2개 항목) 컨테이너 런타임(6개 항목) 총 5개 영역에서 32개 항목으로 구성된다.

구분	진단코드	진단 항목	취약도
가. Host 설정	DO-01	도커 최신 패치 적용	상
	DO-02	도커 그룹에 불필요한 사용자 제거	중
	DO-03	Docker daemon audit 설정	상
	DO-04	/var/lib/docker audit 설정	상
	DO-05	/etc/docker audit 설정	상
	DO-06	docker.service audit 설정	상
	DO-07	docker.socket audit 설정	상
	DO-08	/etc/default/docker audit 설정	상
나. 도커 데몬 설정	DO-09	default bridge를 통한 컨테이너 간 네트워크 트래픽 제한	상
	DO-10	도커 클라이언트 인증 활성화	상
	DO-11	legacy registry (v1) 비활성화	하
	DO-12	추가 권한 획득으로부터 컨테이너 제한	중
다. 도커 데몬 설정 파일	DO-13	docker.service 소유권 설정	상
	DO-14	docker.service 파일 접근권한 설정	상
	DO-15	docker.socket 소유권 설정	상
	DO-16	docker.socket 파일 접근권한 설정	상
	DO-17	/etc/docker 디렉터리 소유권 설정	상
	DO-18	/etc/docker 디렉터리 접근권한 설정	상
	DO-19	/var/run/docker.sock 파일 소유권 설정	상
	DO-20	/var/run/docker.sock 접근권한 설정	상
	DO-21	daemon.json 파일 소유권 설정	중
	DO-22	daemon.json 파일 접근권한 설정	중
	DO-23	/etc/default/docker 파일 소유권 설정	상
	DO-24	/etc/default/docker 파일 접근권한 설정	상
라. 컨테이너 이미지 및 빌드 파일	DO-25	root가 아닌 user로 컨테이너 실행	중
	DO-26	도커를 위한 컨텐츠 신뢰성 활성화	중
마. 컨테이너 런타임	DO-27	컨테이너 SELinux 보안 옵션 설정	중
	DO-28	컨테이너에서 ssh 사용 금지	상
	DO-29	컨테이너에 privileged 포트 매핑 금지	중
	DO-30	PIDs cgroup 제한	상
	DO-31	도커의 default bridge docker0 사용 제한	하
	DO-32	호스트의 user namespaces 공유 제한	하

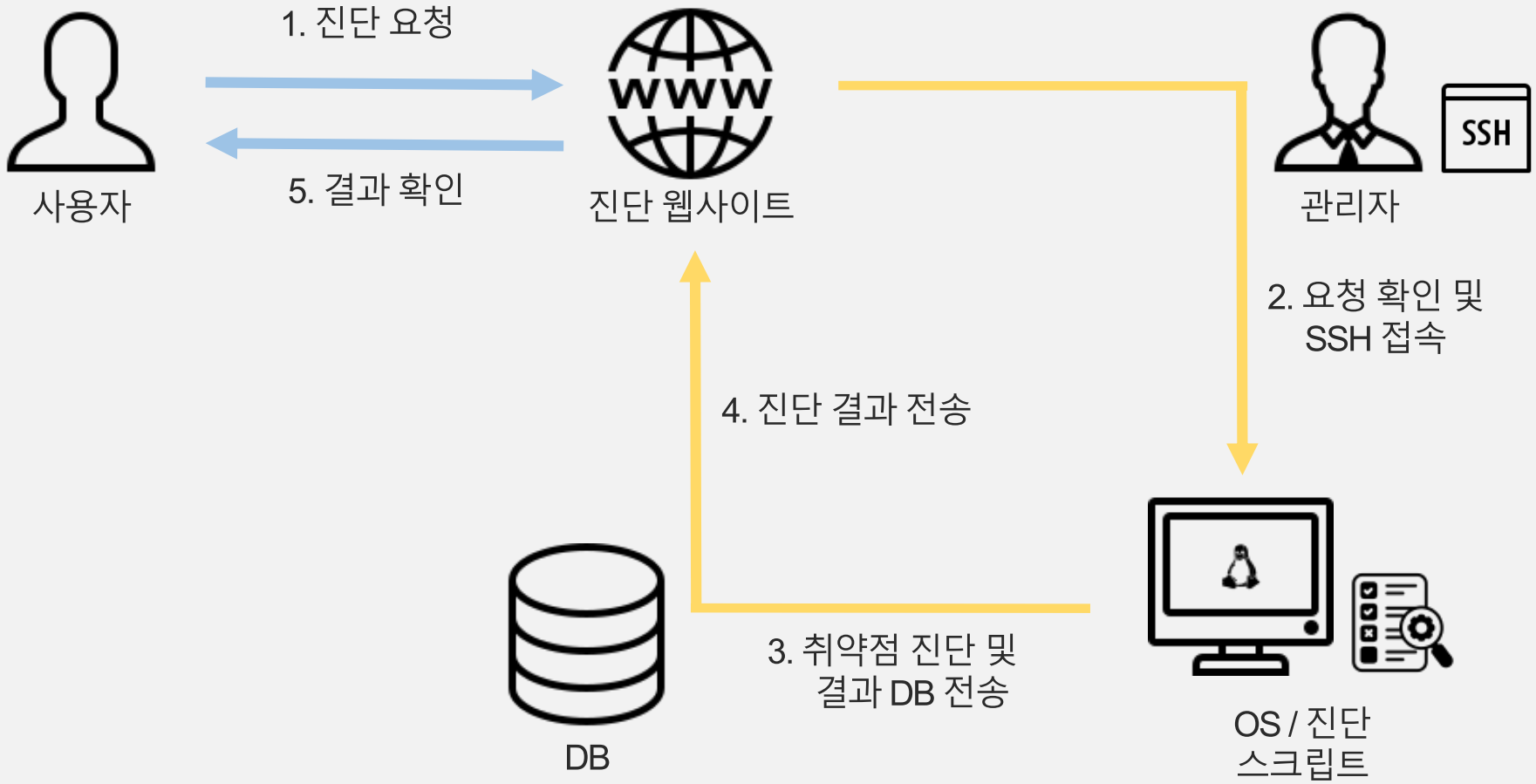
[표 16] Docker 점검 체크리스트

주요정보통신기반시설 클라우드 취약점 점검 가이드2020 기반

주제 선정 이유

클라우드 도입 시 보안 위협의 심각성

구상도


1. 진단 요청
5. 결과 확인
사용자
www
진단 웹사이트
SSH
관리자
2. 요청 확인 및
SSH 접속
4. 진단 결과 전송
3. 취약점 진단 및
결과 DB 전송
DB
OS / 진단
스크립트

개발환경

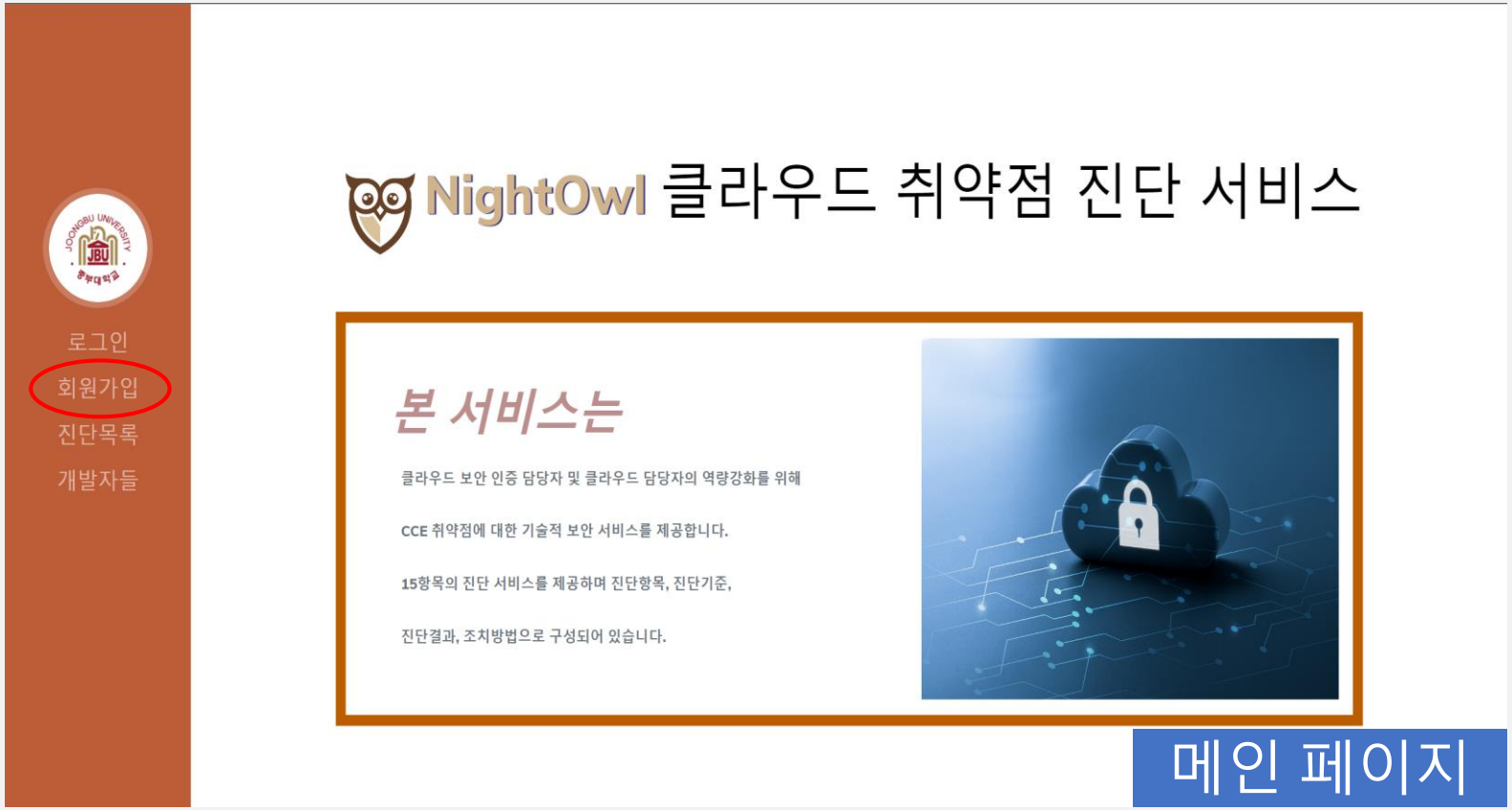
진단 스크립트

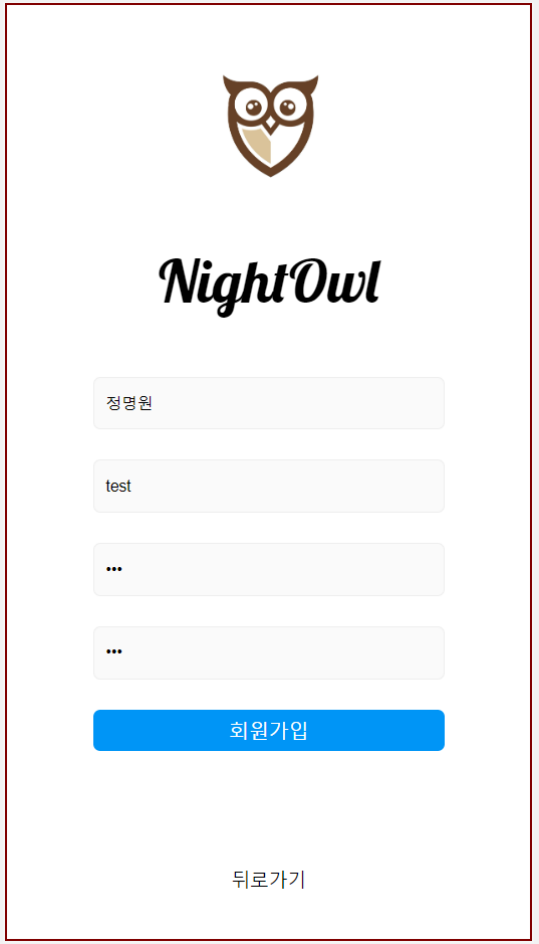
진단 환경

WEB

DB

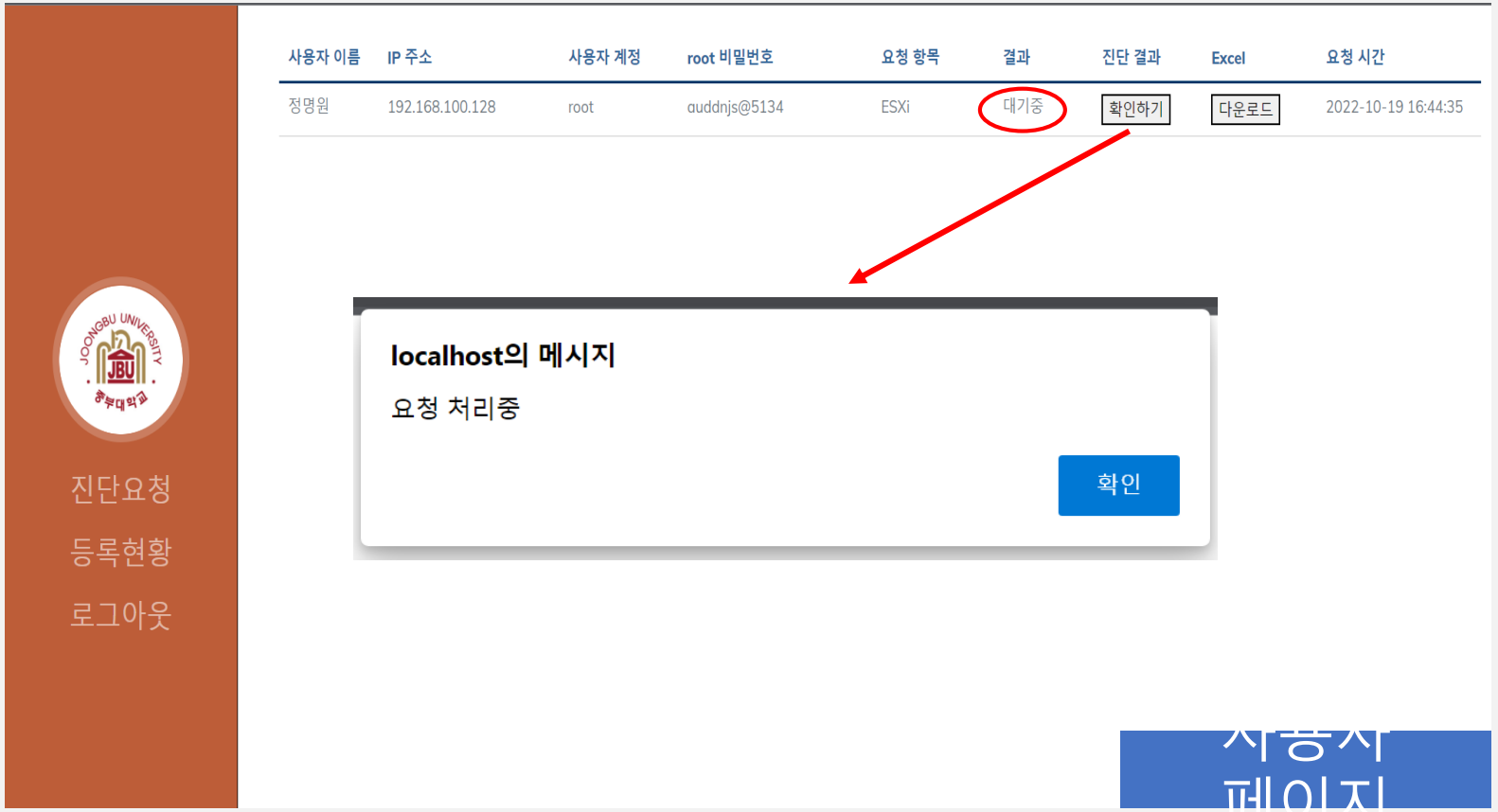
개발내용





메인 페이지 & 회원가입

개발내용



클라이언트진단 요청

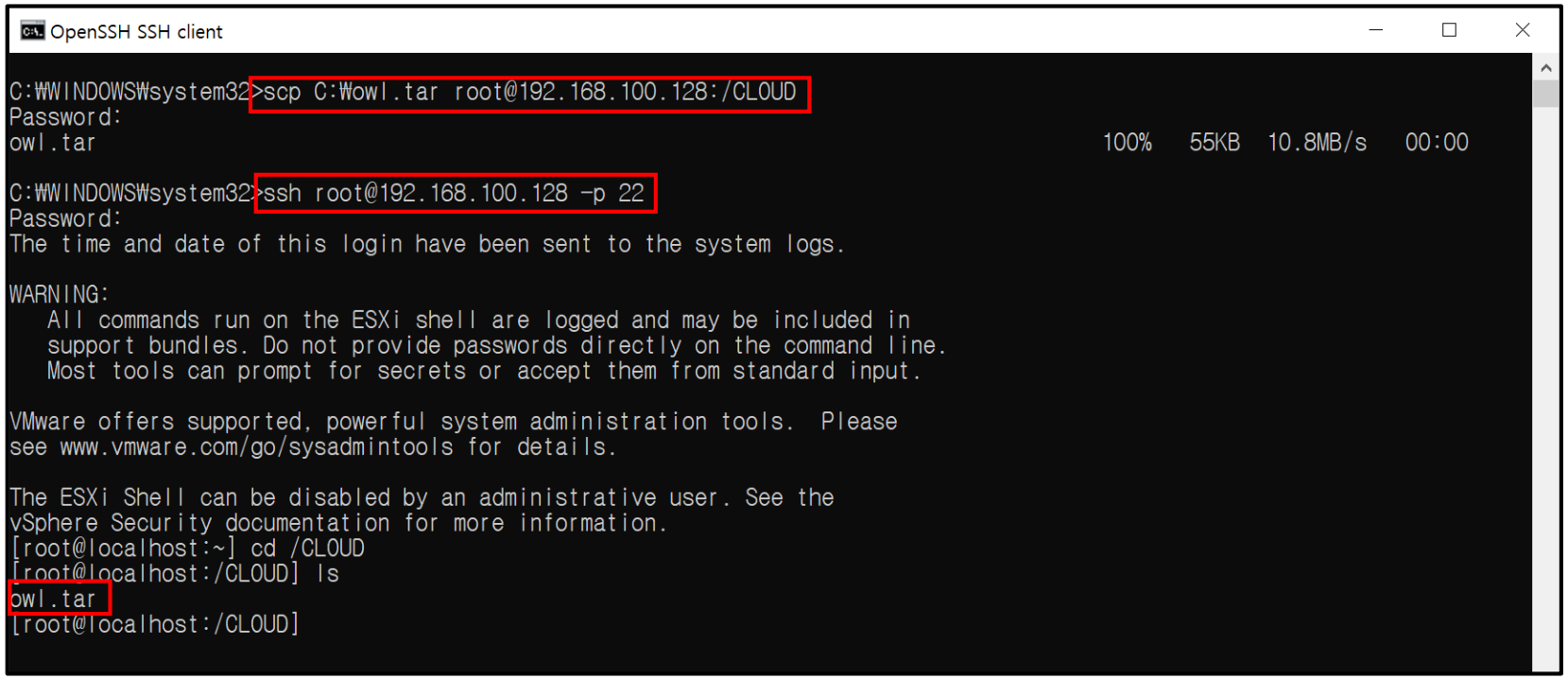
개발내용

요청목록

회원리스트

로그아웃

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



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
q) 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) Elasticseatch
q) 종료하기
2
ESXi 진단이 완료되었습니다.
q
Thank you
[root@localhost:/CLOUD]
```

관리자: NightOwl

```
C:₩WINDOWS₩system32>scp root@192.168.100.128:/Nightowl/DB.txt C:₩DB.txt
Password:
DB.txt

C:₩WINDOWS₩system32>scp root@192.168.100.128:/Nightowl/Score.txt C:₩Score.txt
Password:
Score.txt

C:₩WINDOWS₩system32>
```

진단 완료 후 관리자 PC로 파일 전달

개발내용

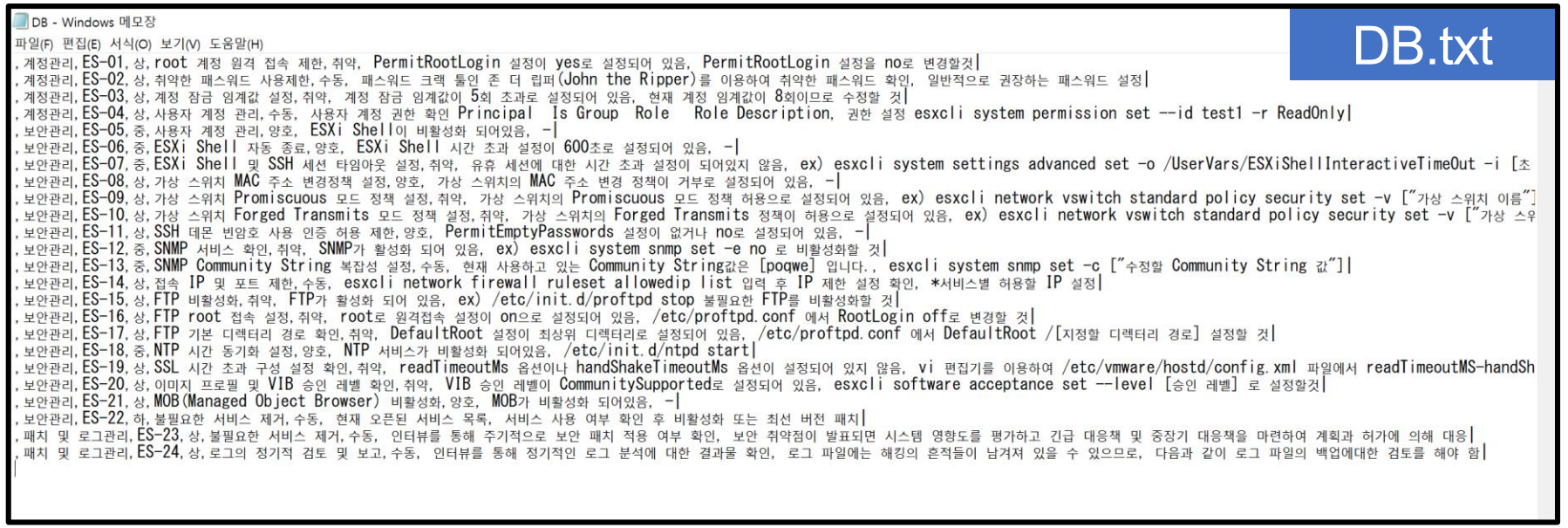
요청목록

회원리스트

로그아웃

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

DB.txt



DB - Windows 메모장

파일(F) 편집(E) 서식(O) 보기(V) 도움말(H)

,계정관리,ES-01,상,root 계정 원격 접속 제한,취약, PermitRootLogin 설정이 yes로 설정되어 있음, PermitRootLogin 설정을 no로 변경할것|
,계정관리,ES-02,상,취약한 패스워드 사용제한,수동, 패스워드 크랙 툴인 존 더 립퍼(John the Ripper)를 이용하여 취약한 패스워드 확인, 일반적으로 권장하는 패스워드 설정|
,계정관리,ES-03,상,계정 잠금 임계값 설정,취약, 계정 잠금 임계값이 5회 초과로 설정되어 있음, 현재 계정 임계값이 8회이므로 수정할 것|
,계정관리,ES-04,상,사용자 계정 관리,수동, 사용자 계정 권한 확인 Principal Is Group Role Role Description, 권한 설정 esxcli system permission set --id test1 -r 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 600초로 설정되어 있음, -|
,보안관리,ES-07,중,ESXi Shell 및 SSH 세션 타임아웃 설정,취약, 유휴 세션에 대한 시간 초과 설정이 되어있지 않음, ex) esxcli system settings advanced set -o /UserVars/ESXiShellInteractiveTimeOut -i [초
,보안관리,ES-08,상,가상 스위치 MAC 주소 변경정책 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) esxcli network vswitch standard policy security set -v ["가상 스위치 이름"]
,보안관리,ES-10,상,가상 스위치 Forged Transmits 모드 정책 설정,취약, 가상 스위치의 Forged Transmits 정책이 허용으로 설정되어 있음, ex) esxcli network vswitch standard policy security set -v ["가상 스위
,보안관리,ES-11,상,SSH 데몬 빈암호 사용 인증 허용 제한,양호, PermitEmptyPasswords 설정이 없거나 no로 설정되어 있음, -|
,보안관리,ES-12,중,SNMP 서비스 확인,취약, SNMP가 활성화 되어 있음, ex) esxcli system snmp set -e no 로 비활성화할 것|
,보안관리,ES-13,중,SNMP Community String 복잡성 설정,수동, 현재 사용하고 있는 Community String값은 [poqwe] 입니다., esxcli system snmp set -c ["수정할 Community String 값"]|
,보안관리,ES-14,상,접속 IP 및 포트 제한,수동, esxcli network firewall ruleset allowedip list 입력 후 IP 제한 설정 확인, *서비스별 허용할 IP 설정|
,보안관리,ES-15,상,FTP 비활성화,취약, FTP가 활성화 되어 있음, ex) /etc/init.d/proftpd stop 불필요한 FTP를 비활성화할 것|
,보안관리,ES-16,상,FTP root 접속 설정,취약, root로 원격접속 설정이 on으로 설정되어 있음, /etc/proftpd.conf 에서 RootLogin off로 변경할 것|
,보안관리,ES-17,상,FTP 기본 디렉터리 경로 확인,취약, DefaultRoot 설정이 최상위 디렉터리로 설정되어 있음, /etc/proftpd.conf 에서 DefaultRoot /[지정할 디렉터리 경로] 설정할 것|
,보안관리,ES-18,중,NTP 시간 동기화 설정,양호, NTP 서비스가 비활성화 되어있음, /etc/init.d/ntpd start|
,보안관리,ES-19,상,SSL 시간 초과 구성 설정 확인,취약, readTimeoutMs 옵션이나 handShakeTimeoutMs 옵션이 설정되어 있지 않음, vi 편집기를 이용하여 /etc/vmware/hostd/config.xml 파일에서 readTimeoutMS-handSh
,보안관리,ES-20,상,이미지 프로필 및 VIB 승인 레벨 확인,취약, VIB 승인 레벨이 CommunitySupported로 설정되어 있음, esxcli software acceptance set --level [승인 레벨] 로 설정할것|
,보안관리,ES-21,상,MOB(Managed Object Browser) 비활성화,양호, MOB가 비활성화 되어있음, -|
,보안관리,ES-22,하,불필요한 서비스 제거,수동, 현재 오픈된 서비스 목록, 서비스 사용 여부 확인 후 비활성화 또는 최선 버전 패치|
,패치 및 로그관리,ES-23,상,불필요한 서비스 제거,수동, 인터뷰를 통해 주기적으로 보안 패치 적용 여부 확인, 보안 취약점이 발표되면 시스템 영향도를 평가하고 긴급 대응책 및 중장기 대응책을 마련하여 계획과 허가에 의해 대응|
,패치 및 로그관리,ES-24,상,로그의 정기적 검토 및 보고,수동, 인터뷰를 통해 정기적인 로그 분석에 대한 결과물 확인, 로그 파일에는 해킹의 흔적들이 남겨져 있을 수 있으므로, 다음과 같이 로그 파일의 백업에대한 검토를 해야 함|

관리자 페이지

사용자에게 완료 메시지 & 결과물 전송

개발내용

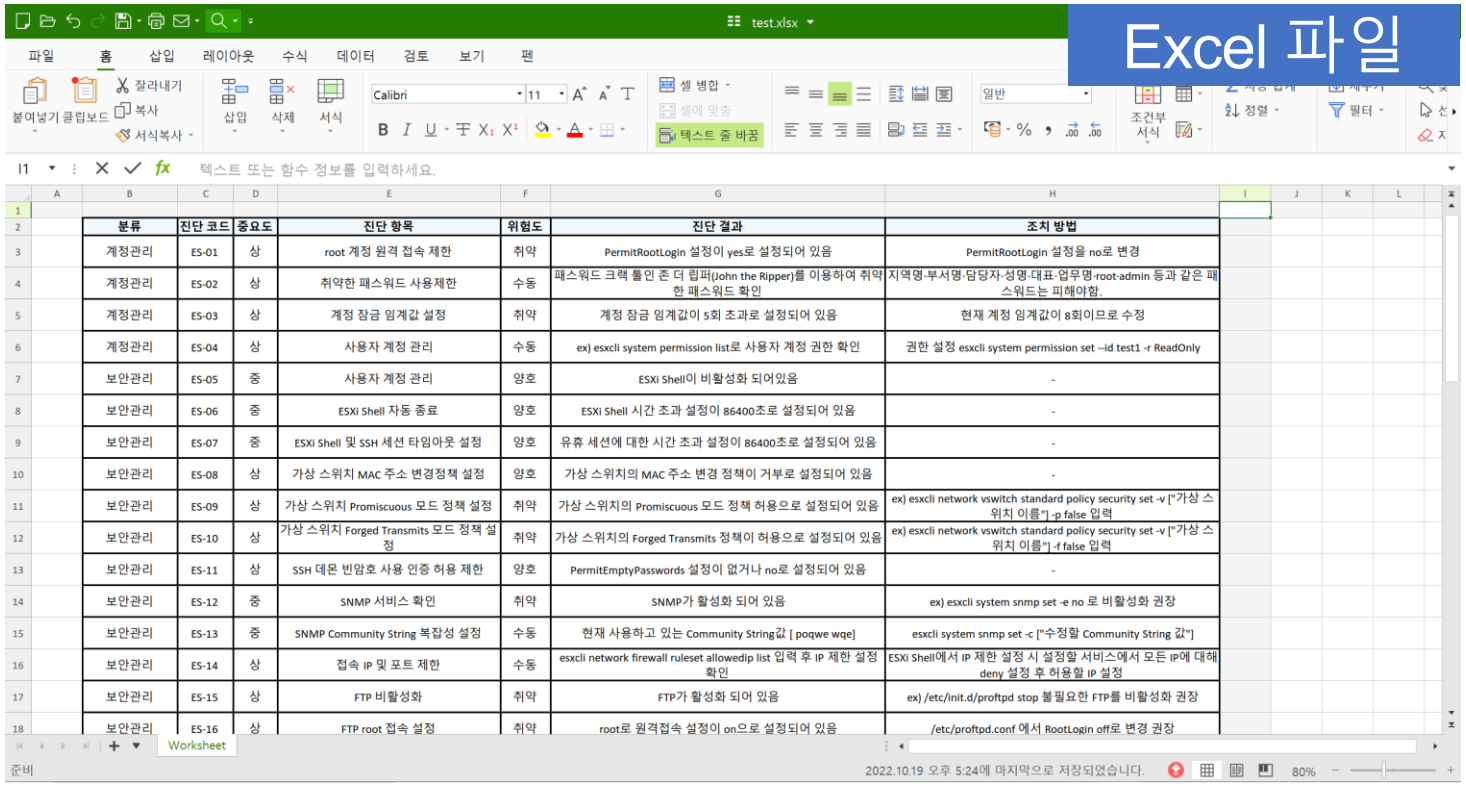
진단요청

등록현황

로그아웃

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

Excel 파일



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 크랙 툴인 존 더 립퍼(John the Ripper)를 이용하여 취약한 패스워드 확인	지역명·부서명·담당자·성명·대표·업무명·root·admin 등과 같은 패스워드는 피해야함.
계정관리	ES-03	상	계정 잠금 임계값 설정	취약	계정 잠금 임계값이 5회 초과로 설정되어 있음	현재 계정 임계값이 8회이므로 수정
계정관리	ES-04	상	사용자 계정 관리	수동	ex) esxcli system permission list로 사용자 계정 권한 확인	권한 설정 esxcli system permission set --id test1 -r 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	유휴 세션에 대한 시간 초과 설정이 86400초로 설정되어 있음	-
보안관리	ES-08	상	가상 스위치 MAC 주소 변경정책 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) esxcli 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) esxcli network vswitch standard policy security set -v ["가상 스위치 이름"] -f false 입력
보안관리	ES-11	상	SSH 데몬 빈암호 사용 인증 허용 제한	양호	PermitEmptyPasswords 설정이 없거나 no로 설정되어 있음	-
보안관리	ES-12	중	SNMP 서비스 확인	취약	SNMP가 활성화 되어 있음	ex) esxcli system snmp set -e no 로 비활성화 권장
보안관리	ES-13	중	SNMP Community String 복잡성 설정	수동	현재 사용하고 있는 Community String값 [poqwe wqe]	esxcli system snmp set -c ["수정할 Community String 값"]
보안관리	ES-14	상	접속 IP 및 포트 제한	수동	esxcli network firewall ruleset allowedip list 입력 후 IP 제한 설정 확인	ESXi Shell에서 IP 제한 설정 시 설정할 서비스에서 모든 IP에 대해 deny 설정 후 허용할 IP 설정
보안관리	ES-15	상	FTP 비활성화	취약	FTP가 활성화 되어 있음	ex) /etc/init.d/proftpd stop 불필요한 FTP를 비활성화 권장
보안관리	ES-16	상	FTP root 접속 설정	취약	root로 원격접속 설정이 on으로 설정되어 있음	/etc/proftpd.conf 에서 RootLogin off로 변경 권장

사용자 페이지

클라이언트 진단 결과 확인

개발내용

NightOwl 등록/현황

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	취약	PermitRootLogin 설정이 yes로 설정되어 있음	PermitRootLogin 설정을 no로 변경
계정관리	ES-02	상	취약한 패스워드 사용제한	수동	패스워드 크랙 툴인 존 더 립퍼(John the Ripper)를 이용하여 취약한 패스워드 확인	지역명·부서명·담당자·성명·대표·업무명·root·admin 등과 같은 패스워드는 피해야함.
계정관리	ES-03	상	계정 잠금 임계값 설정	취약	계정 잠금 임계값이 5회 초과로 설정되어 있음	현재 계정 임계값이 8회이므로 수정
계정관리	ES-04	상	사용자 계정 관리	수동	ex) esxcli system permission list 로 사용자 계정 권한 확인	권한 설정 esxcli system permission set --id test1 -r 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	유휴 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) esxcli 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) esxcli network vswitch standard policy security set -v ["가상 스위치 이름"] -f false 입력
보안관리	ES-11	상	SSH 데몬 빈암호 사용 인증 허용 제한	양호	PermitEmptyPasswords 설정이 없거나 no로 설정되어 있음	

진단 결과 페이지

진단 점검표 확인

결론 & 기대효과

결론

· 클라우드 취약점 진단 스크립트 항목에 대한 이해도를 높였으며 운용되고 있는 서버에 취약점 진단을 수행하고 점검 결과를 토대로 위협에 대한 보호대책 제시를 통해 보안 사고 발생 위험 감소

기대효과

· 취약점 진단 자동화 시스템을 개발함으로써 효율적인 업무가 가능해질 것으로 예상되며, 보고서에 기재된 상세한 조치 방안으로 빠른 조치 가능