Ecoarium DB 서버(Linux CentOS7) 보안점검리스트

1. 시스템 구성

점검 항목	점검 내용	조치사항
적절한 보안패치가 이루어지고 있는가?	서버 제작사에서 배포되고 있는 최신의 보안패치가 적용되는지 확인한다.	yum check-update, yum update 명령어 통한 최신버전 패치완료
원격(Remote)에서root로 로그인 하는 것이 금지되어 있는가?	원격지에서 텔넷(Telnet)등의 서비스를 이용하여 root로 접근하는 것이 금지되어 있는지 확인한다.	원격지 접속 시 root로의 최초접근 불가, 원격접속 용 계정 키값으로 접근 후 su - 명령어 사용필요
root계정이 사용하는 경로(Path)의 설정은 적절한가?	root계정이 사용하는 경로의 맨 앞에“.”이 존재하지 않는지 확인한다.	root 계정 환경변수 변경 /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
관리자용 명령어의 권한 설정은 적절한가?	관리자만이 사용할 수 있는 명령어에 대해 일반사용자가 접근할 수 없도록 권한이 설정되어 있는지 확인한다.	각 파일 중요도에 따른 권한 설정 완료 777 등의 과도한 권한 없음
시스템 환경 파일에 대한 접근 권한은 적절한가?	시스템 환경 구성에 이용되는 파일의 접근 권한이 적절하게 설정되어 있는지 확인한다.	/etc/ssh/sshd_config 등 중요 파일 및 디렉토리 접근 권한 확인, 이상 없음
root계정의umask값의 설정은 적절한가?	root계정의umask값이027로 설정되어 있는지 확인한다.	umask 명령어 통한 0027 값 확인
불필요한setUID, setGID를 가지는 파일이 존재하는가?	특수한 파일 이외에 root권한으로 된setUID, setGID가 설정된 파일이 존재하는지 확인한다.	이상 없음
원격호출(Remote Call)이 이루어질 수 있는 계정이 존재하는가?	각 계정중에서 .rhosts, .netrc파일을 가지고 있는 계정이 있는지 확인한다.	존재하지만 원격접속 콘솔pc 로컬환경에서 private key가 존재해야함
불필요한 서비스는 존재하지 않는가?	/etc/inetd.conf안에 불필요한 서비스가 설정되어 있는지 확인한다.	불필요 서비스 미존재

2. 계정 정책 및 제한

점검 항목	점검 내용	조치사항
shadow패스워드 시스템을 사용하고 있는가?	/etc/passwd파일과의 연계되어 사용되어지는 shadow패스워드 시스템을 사용하고 있는지 확인한다.	이상 없음
패스워드 시스템 관련 파일의 퍼미션은 적절한가?	/etc/passwd, /etc/shadow파일은 root만이 접근할 수 있는지 확인한다.	파일 권한 각각 /etc/passwd(644), /etc/shadow(000) 확인
최대 암호 사용기간을30일로 지정하고 있는가?	사용자의 암호가30일 마다 변경되게 설정되어 있는지와 사용기간이 지난 암호는 자동으로 사용불가 되게 설정되어 있는지 확인한다.	이상 없음
최소 암호 사용기간을1일로 지정하고 있는가?	암호의 즉시 변경을 방지하기 위하여 최소 암호 사용기간이1일로 설정되어 있는지 확인한다.	이상 없음
최소 암호 길이를6자리 이상으로 지정하고 있는가?	암호의 최소 길이가6자리 이상으로 설정되어 있는지 확인한다.	이상 없음
3회 로그온 실패 시 계정 잠금을 잠그는가?	로그온 실패 횟수가3회 되었을 때 계정 잠금이 설정되어 있는지 확인한다.	작품 시연 중 편의 위해 해당 정책 적용하지 않음 (혹시 잠기면 큰일)
임시로 발급한 계정에 대해서는 파기 날짜 지정하는가?	계약직이나 임시직 사용자 계정에 대해서는 계정 만료 날짜를 지정하여 지정된 날짜 이후에는 계정을 사용할 수 없도록 설정되어 있는지 확인한다.	임시 계정 없음
사용하지 않는 계정은 삭제하는가?	전배,퇴사 등으로 사용하지 않는 계정이 삭제되어 있는지 확인한다.	이상 없음
중복된UID가 존재하는가?	계정중에서 특히UID가0인 계정이 중복되어 있는지 확인한다.	이상 없음
그룹과 사용자ID가 일치하는가?	그룹과 사용자ID가 서로 일치하는지 확인한다.	이상 없음
홈 디렉토리는 소유자만이 접근할 수 있는가?	홈 디렉토리가 소유자 이외의 다른 사용자가 쓰기 할 수 있는지 확인한다.	관리 편의 위해 소유자 이외 root가 읽기만 가능
각 계정 소유의 기본 파일에 소유자만이 접근할 수 있는가?	각 계정의.profile파일을 다른 사용자가 쓰기할 수 있는지 확인한다.	관리 편의 위해 소유자 이외 root가 읽기만 가능
홈 디렉토리가 없는 계정이 존재하는가?	등록된 계정 중에서 홈 디렉토리를 가지고 있지 않은 계정이 존재하는지 확인한다	이상 없음
쉘이 없는 계정이 존재하는가?	등록된 계정 중에서 쉘을 가지고 있지 않은 계정이 존재하는지 확인한다.	이상 없음
그룹과 사용자ID가 일치하는가?	그룹과 사용자ID가 서로 일치하는지 확인한다.	이상 없음

3. 감사 및 로그

점검 항목	점검 내용	조치사항
시스템 기본 로그는3개월간 보관되는가?	시스템 기본 로그는 3개월 동안 보관하고 있는지 확인한다.	시스템 기본 로그 1개월 보관 → 3개월 보관으로 변경완료
로그온 정보에 대한 감사가 수행되고 있는가?	시스템 로그인 및 로그아웃 정보에 대한 감사가 수행되고 있는지 확인한다.	/etc/audit/audit.rules 파일 내 -w /var/log/auth.log -p wa -k login_logout_audit -w /var/log/secure -p wa -k login_logout_audit 추가하여 로그인 관련 이벤트 감사 수행하도록 변경완료
감사 및 보안 로그의 관리를 하는가?	root만이 시스템 로그에 대한 접근 권한을 가지고 있는지 확인한다.	/var/log 내 audit(700), messages(600), secure(600) 등 로그 파일 권한 확인

Ecoarium DBMS(Linux CentOS7 내 MySQL) 보안점검리스트

1. 시스템 구성

점검 항목	점검 내용	조치사항
최신의 보안패치가 적용되어 있는가?	설치된DBMS에 최신의 보안패치가 적용되어 있는지 확인한다.	SELECT VERSION(); 확인 시 8.0.36으로 보안 안정성 있는 버전 확인
사용자는 응용시스템을 통해서만DB에 접근할 수 있는가?	사용자가 응용시스템을 통하지 않고 직접DB에 접근할 수 있는지 확인한다.	DB 포트 3306으로만 통신하도록, 사용자는 웹서버 node.js 시퀄라이즈로 통신
패스워드 파일을 이용하는가?	OS로그인과 별도로DB에 접속하기 위한 별도의 패스워드 시스템을 이용하는지 확인한다.	별도 패스워드 시스템 사용 확인 및 패스워드 암호화 저장 확인
DBMS시스템 파일 접근 권한 설정은 적절한가?	DBMS시스템 파일에DBA그룹이 아닌 사람에게 권한 밖의 접근 권한이 설정되어 있는지 확인한다.	/var/lib 디렉토리 내 chmod 750 /var/lib/mysql/mysql.sock /var/lib/mysql/mysql.sock.lock 조치하여 DBA 그룹 외 사용자 접근 제한 조치, /etc/my.cnf 권한 644 설정
Data Dictionary에 대한 보호는 적절히 이루어지고 있는가?	DBA권한으로 접속한 사용자만이 Data Dictionary상의 ANY시스템 권한을 사용할 수 있는지 확인한다.	시스템 메타데이터 확인(SELECT * FROM information_schema.tables WHERE table_schema = 'mysql';) 및 DBMS 사용자 권한 확인
사용자의table space가 정의되어 있는가?	user생성시default tablespace와 temporary tablespace가 설정되어 있는지 확인한다.	MySQL에서는 사용자별로 테이블스페이스를 지정하는 기능이 없음
사용자별로table space의 제한이 되어 있는가?	user생성시table space의 한계를 설정해 놓았는지 확인한다.	MySQL에서는 사용자별로 테이블스페이스를 지정하는 기능이 없음
Sqlplus '/as sysdba'의 사용제한은 적절한가?	Sqlplus '/as sysdba'로 DB에 접속할 수 있는 계정의 설정이 적절한지 확인한다.	MySQL계정 root로 원격접속(웹에서의 접속)이 불가하여 root와 똑같은 oracle12 계정 만들어 관리
사용자 리소스 사용제한은 설정되어 있는가?	한 사용자의 리소스 과점유를 방지하기 위하여 시스템 프로파일의 사용자별로 할당되어 있으며 프로파일 내의 보안관련 파라메터가 세팅되어 있는지 확인한다.	/etc/my.cnf 사용자 리소스 제한 max_connections=100 max_user_connections=10 max_questions=10000 max_updates=1000 설정

2. 계정 관리

점검 항목	점검 내용	조치사항
사용자 계정의 패스워드는 변경되어 있는가?	사용자 계정의 패스워드는 변경되어 있는지 확인한다.	root / oracle12 계정 pw 변경 완료
계정의 권한은 적절히 설정되어 있는가?	User에게 부여된 권한에 필요이상의 권한이 부여되어 있지 않은가 확인한다.	root / oracle12 계정 모두 최고 권한이지만, 관리자 원격 접속, 웹서버 시퀄라이즈 사용 시 테이블 생성 및 변경 등에 사용되어야 하므로 불가피
3번 이상 패스워드를 잘못 입력한 경우 로그인이 통제되는가?	로그인 과정에서 3번이상 패스워드를 잘못 입력했을 경우 계정이 LOCK되도록 설정되어 있는지 확인한다.	작품 시연 중 편의 위해 해당 정책 적용하지 않음 (혹시 잠기면 큰일)
최대 암호 사용기간이 30일로 설정되어 있는가?	사용자의 암호가30일 마다 변경되게 설정되어 있는지와 사용기간이 지난 암호는 자동으로expire되게 설정되어 있는지 확인한다.	ALTER USER 'root'@'localhost' PASSWORD EXPIRE INTERVAL 30DAY; ('oracle12'@'%'도 똑같이 수정)
패스워드 재사용 횟수가 지정되어 있는가?	한번 사용되었던 패스워드에 대하여 재사용할 수 있기 까지의 횟수 설정이 되어 있는지 확인한다.	MySQL은 패스워드 재사용 횟수 지원하지 않음
단순 패스워드 사용이 금지되어 있는가?	유추하기 쉬운 구조의 패스워드의 사용을 금지시켰는지 확인한다.	암호 정책 설정 위해 SET GLOBAL validate_password.policy = 'MEDIUM'; STRONG부터는 원격접속 불가
DBA만이LOCK된 계정을 해제시킬 수 있는가?	Expire등의 이유로LOCK된 계정이 DBA가Reset시킬 경우에만 재 사용 가능하도록 설정되어 있는지 확인한다.	작품 시연 중 편의 위해 해당 정책 적용하지 않음 (혹시 잠기면 큰일)

3. 권한 및 역할 관리

점검 항목	점검 내용	조치사항
OS Role관리는 적절하게 이루어 지고 있는가?	DBMS설치 시 부여되는 OS Role은 DBA에게만 할당되었는지 확인한다.	DB서버 -Web(AP)서버 물리적 분리에 따른 계정 분리
각 응용시스템별로Role이 정의되어 있는가?	각 응용시스템별로 적절한 Role이 정의되어 있는지 확인한다.	DB서버 -Web(AP)서버 물리적 분리에 따른 응용시스템 분리
사용자 유형에 대한Role이 정의되어 있는가?	manager 등 같은 사용자 유형에 대한 Role이 정의되어 있는지 확인한다.	root(local)계정, oracle12(원격접속) 계정 분리

4. 로깅 정책

점검 항목	점검 내용	조치사항

DB의 모든 데이터의 갱신에 관련한 모든 사항이 로그로 기록되는가?	CREATE TABLE과 CREATE INDEX 시 NOLOGGING 키워드가 사용된 table이나index가 있는지 확인한다.	MySQL에서 NOLOGGING 키워드 없음, /etc/my.cnf 내 로깅 활성화 추가
		general_log = 1
		# 일반 쿼리 로깅 활성화
		general_log_file
		= /var/log/mysql.log
		# 일반 쿼리 로그 파일 경로
		log_error
		= /var/log/mysqld.log
		# MySQL 서버 오류를 기록하는 오류 로그 파일 경로
		slow_query_log = 1
		# 느린 쿼리 로깅 활성화
		slow_query_log_file
		= /var/log/slow_query.log
		# 느린 쿼리 로그 파일 경로
		long_query_time = 1
		# 느린 쿼리로 간주되는 시간 (초)
		log_bin
		= /var/log/mysql/mysql-bin.log
		# 이진 로그 활성화 및 파일 경로

5. 무결성 체크

점검 항목	점검 내용	조치사항
각 데이터 블록의 무결성이 훼손되지 않았는가?	DB의 인덱스를 검증함으로써,각 데이터 블록의 무결성을 검증하고,블록이 훼손되었는지 확인한다.	이상 없음
테이블이 훼손되지 않았는가?	테이블의 인덱스 구조를 검증하고, 테이블과 인텍스 간에 교차 참조를 확인한다.	이상 없음
클러스터가 훼손되지 않았는가?	클러스터 인덱스를 포함하여 클러스터 테이블의 모든 인덱스 구조를 검증 및 확인한다.	이상 없음
테이블에 제약조건이 설정되어 있는가?	테이블의 행들에 대해 제약조건이 설정되어 있는지 확인한다.	이상 없음

취약점 진단 https://github.com/antonio-kim-1994/bash.git 리포지토리 내 KISA(한국인터넷진흥원) 기준의 CSAP_클라우드_취약점_점검_가이드-Linux에 맞춘 linux-vulnerability-scan/kisa/centos7.8 스크립트 실행 결과

```
**********************************************************************
*                                리눅스 스크립트                                *
**********************************************************************
항목에 따라 시간이 다른 항목에 비하여 다소 오래 걸릴수 있습니다.
스캔 보고서는 hostname_scan_result_시간.txt 파일로 /root에 저장 됩니다.
기준은 [CSAP 클라우드 취약점 점검 가이드] 문서입니다.
**********************************************************************

############################## 시작 시간 ##############################
Mon May 27 06:47:56 UTC 2024

============================  시스템  정보 ============================
1. 시스템 기본 정보
운영체제: CentOS Linux release 7.9.2009 (Core)
호스트 이름: ip-172-31-xx-xx.ap-northeast-2.compute.internal // ip노출 블러
커널 버전: 3.10.0-1160.114.2.el7.x86_64

2. 네트워크 정보
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 9001
inet 172.31.xx.xx  netmask 255.255.xx.xx  broadcast 172.31.xx.xx // ip노출 블러
inet6 fe80::8c1:62ff:xxxx:xxxx  prefixlen 64  scopeid 0x20<link> // ip노출 블러
ether 0a:c1:62:xx:xx:xx  txqueuelen 1000  (Ethernet) // mac노출 블러
RX packets 482861  bytes 130383810 (124.3 MiB)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 435285  bytes 128652896 (122.6 MiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
inet 127.0.0.1  netmask 255.0.0.0
inet6 ::1  prefixlen 128  scopeid 0x10<host>
loop  txqueuelen 1000  (Local Loopback)
RX packets 721  bytes 222557 (217.3 KiB)
RX errors 0  dropped 0  overruns 0  frame 0
TX packets 721  bytes 222557 (217.3 KiB)
TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

************************* 취약점 체크 시작 *************************

==
[36m[U-01] root 계정 원격 접속 제한[0m
양호 : 원격 터미널 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우
취약 : 원격 터미널 서비스 사용 시 root 직접 접속을 허용한 경우
==
[32m[양호] : /etc/securetty 파일 안에 pts/#이 존재하지 않습니다.[0m
[32m[양호] : PermitRootLogin이 차단되어 있습니다.[0m

==
[36m[U-02] 패스워드 복잡성 설정[0m
양호 : 영문, 숫자, 특수문자를 조합하여 2종류 조합 시 10자리 이상, 3종류 이상 조합 시 8자리 이상의 패스워드가 설정된 경우
취약 : 영문, 숫자, 특수문자를 조합하지 않거나 2종류 조합 시 10자리 미만, 3종류 이상 조합 시 8자리 미만의 패스워드가 설정된 경우
==
[32m[양호] : /etc/security/pwquality.conf의 minlen 옵션이 올바르게 설정되어 있습니다. minlen=8[0m
[32m[양호] : /etc/security/pwquality.conf의 dcredit 옵션이 올바르게 설정되어 있습니다. dcredit=-1[0m
[32m[양호] : /etc/security/pwquality.conf의 ucredit 옵션이 올바르게 설정되어 있습니다. ucredit=-1[0m
[32m[양호] : /etc/security/pwquality.conf의 lcredit 옵션이 올바르게 설정되어 있습니다. lcredit=-1[0m
[32m[양호] : /etc/security/pwquality.conf의 ocredit 옵션이 올바르게 설정되어 있습니다. ocredit=-1[0m

==
[36m[U-03] 계정 잠금 임계값 설정[0m
양호 : 계정 잠금 임계값이 5 이하의 값으로 설정되어 있는 경우
취약 : 계정 잠금 임계값이 설정되어 있지 않거나, 5 이하의 값으로 설정되어 있지 않은 경우
==
[32m[양호] : /etc/pam.d/system-auth 내 pam_tally2 설정이 정상입니다.[0m
[32m[양호] : /etc/pam.d/password-auth 내 pam_tally2 설정이 정상입니다.[0m

==
[36m[U-04] 패스워드 최대 사용 기간 설정[0m
양호 : 패스워드의 최대 사용기간이 90일 이내로 설정되어 있는 경우
취약 : 패스워드의 최대 사용기간이 없거나, 90일 이내로 설정되어 있지 않은 경우

==========
[32m[양호] : /etc/login.defs 내 PASS_MAX_DAYS가 90일로 설정되어 있습니다.[0m

==========
[36m[U-05] 패스워드 파일 보호[0m
양호 : 쉐도우 패스워드를 사용하거나, 패스워드를 암호화하여 저장하는 경우
취약 : 쉐도우 패스워드를 사용하지 않고, 패스워드를 암호화하여 저장하지 않는 경우
==========
[32m[양호] : /etc/passwd 내 패스워드가 암호화되어 있습니다.[0m

==========
[36m[U-06] root 홈, 패스 디렉터리 권한 및 패스 설정[0m
양호 : PATH 환경변수에 '.' 이 맨 앞이나 중간에 포함되지 않은 경우
취약 : PATH 환경변수에 '.' 이 맨 앞이나 중간에 포함된 경우
==========
[32m[양호] : /root/.bash_profile 내 PATH 경로에 '.' 이 포함되어 있지 않습니다.[0m

==========
[36m[U-07] 파일 및 디렉터리 소유자 설정[0m
양호 : 소유자나 그룹이 존재하지 않는 파일 및 디렉터리가 없는 경우
취약 : 소유자나 그룹이 존재하지 않는 파일 및 데릭터리가 있는 경우
==========
[32m[양호] : 소유자나 그룹이 확인되지 않는 파일 및 데릭터리가 없습니다.[0m

==========
[36m[U-08] /etc/passwd 파일 소유자 및 권한 설정[0m
양호 : /etc/passwd 파일의 소유자가 root이고, 권한이 644 이하인 경우
취약 : /etc/passwd 파일의 소유자가 root가 아니거나, 권한이 644 초과인 경우
==========
[32m[양호] : /etc/passwd의 권한 수준이 정상입니다.[0m
[32m[양호] : /etc/passwd의 소유자가 root입니다.[0m

==========
[36m[U-09] /etc/shadow 파일 소유자 및 권한 설정[0m
양호 : /etc/shadow 파일의 소유자가 root이고, 권한이 400 이하인 경우
취약 : /etc/shadow 파일의 소유자가 root가 아니거나, 권한이 400 초과인 경우
==========
[32m[양호] : /etc/shadow의 권한 수준이 정상입니다.[0m
[32m[양호] : /etc/shadow의 소유자가 root입니다.[0m

==========
[36m[U-10] /etc/hosts 파일 소유자 및 권한 설정[0m
양호 : /etc/hosts 파일의 소유자가 root이고, 권한이 644 이하인 경우
취약 : /etc/hosts 파일의 소유자가 root가 아니거나, 권한이 644 초과인 경우
==========
[32m[양호] : /etc/hosts의 권한 수준이 정상입니다.[0m
[32m[양호] : /etc/hosts의 소유자가 root입니다.[0m

==========
[36m[U-11] /etc/(x)inetd.conf 파일 소유자 및 권한 설정[0m
양호 : /etc/(x)inetd.conf 파일의 소유자가 root이고, 권한이 644 이하인 경우
취약 : /etc/(x)inetd.conf 파일의 소유자가 root가 아니거나, 권한이 644 초과인 경우
==========
[31m[양호] : /etc/xinetd.conf의 권한 수준이 644입니다.[0m
[32m[양호] : /etc/xinetd.conf의 소유자가 root입니다.[0m

==========
[36m[U-12] /etc/sysconfig/rsyslog 파일 소유자 및 권한 설정[0m
양호 : /etc/sysconfig/rsyslog 파일의 소유자가 root이고, 권한이 644 이하인 경우
취약 : /etc/sysconfig/rsyslog 파일의 소유자가 root가 아니거나, 권한이 644 초과인 경우
==========
[32m[양호] : /etc/sysconfig/rsyslog의 권한 수준이 정상입니다.[0m
[32m[양호] : /etc/sysconfig/rsyslog의 소유자가 root입니다.[0m

==========
[36m[U-13] /etc/services 파일 소유자 및 권한 설정[0m
양호 : /etc/services 파일의 소유자가 root이고, 권한이 644 이하인 경우
취약 : /etc/services 파일의 소유자가 root가 아니거나, 권한이 644 초과인 경우
==========
[32m[양호] : /etc/services의 권한 수준이 정상입니다.[0m
[32m[양호] : /etc/services의 소유자가 root입니다.[0m

==========
[36m[U-14] SUID, SGID, sticky bit 설정 파일 점검[0m
양호 : 주요 실행파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있지 않은 경우
취약 : 주요 실행파일의 권한에 SUID와 SGID에 대한 설정이 부여되어 있는 경우
==========
[31m[취약] : SUID와 SGID 설정이 부여되어 있는 실행파일이 존재합니다.[0m

조치사항

https://blog.naver.com/bestheroz/95858524 [출처:리눅스 서버 보안관리 실무(저. 홍석범)]에 따라 다음과 같이 조치

 # chmod u-s /usr/bin/chage
 # chmod u-s /usr/bin/gpasswd
 # chmod g-s /usr/bin/wall
 # chmod u-s /usr/bin/chfn
 # chmod u-s /usr/bin/chsh
 # chmod u-s /usr/bin/newgrp
 # chmod g-s /usr/bin/write
 # chmod u-s /usr/bin/at
chmod: cannot access '/usr/bin/at': No such file or directory
 # chmod u-s /usr/sbin/usernetctl
 # chmod u-s /usr/sbin/userhelper
chmod: cannot access '/usr/sbin/userhelper': No such file or directory
 # chmod u-s /bin/mount
 # chmod u-s /bin/umount

출처에 나와있듯 다음 파일들에 대해서는 각각 SUID/SGID 권한을 해제하지 않음
/usr/sbin/lockdev (sgid)
- devices를 잠글 때 필요하며 lock이라는 그룹 권한으로 설정되어 있는데, 그대로 두는 것이 좋다.

/bin/ping (suid)
- icmp echo request 패킷을 발송하는 것으로 일반 유저에게 ping을 허용하려면 suid를 그대로 유지하고 일반유저에게 ping을 금지하려면 suid를 해제하면 된다. 만약 4755 대신 0755로 설정한 상태에서 일반 유저가 ping을 실행하면 아래와 같은 에러가 나게 된다. - ping: icmp open socket: Operation not permitted

/usr/sbin/traceroute (suid)
- traceroute는 네트워크 경로를 추적하는 명령어로서 일반 유저에게 traceroute를 허용하려면 suid를 그대로 유지하고, 금지하려면 suid를 해제하면 된다.

/usr/bin/passwd (suid)
- suid가 설정된 파일 중 가장 많이 사용되는 명령어일 것이다. 일반 유저가 자신의 암호를 변경하려면 /etc/shadow 파일을 읽고 쓸 수 있는 권한이 있어야 하는데, 이는 root 권한만이 가능하므로 passwd 파일은 root 소유의 suid가 설정되어 있어야 한다. 따라서 이 파일의 퍼미션을 755등으로 변경하면 오직 root만이 암호를 변경할 수 있게 된다.

/usr/bin/crontab (suid)
- 일반 유저가 cron을 설정하여 사용하도록 허용할 경우에는 suid가 필요하지만 일반 유저가 cron을 사용할 수 없도록 제한할 경우에는 불필요하다.

==========

[36m[U-15] 사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정[0m
양호 : 사용자, 시스템 시작파일 및 환경 파일 소유자가 root 또는 해당 계정이고 권한이 644로 설정되어 있는 경우
취약 : 사용자, 시스템 시작파일 및 환경 파일 소유자가 root 또는 해당 계정이 아니거나 권한이 644로 설정되어 있지 않은 경우
==========
[31m[취약] : /home/centos의 접근권한이 올바르지 않습니다.[0m
[32m[양호] : /home/centos의 소유권한이 centos에게 할당되어 있습니다.[0m
[31m[취약] : /home/test의 접근권한이 올바르지 않습니다.[0m
[32m[양호] : /home/test의 소유권한이 test에게 할당되어 있습니다.[0m

조치사항
aws 홈페이지 https://repost.aws/knowledge-center/ec2-server-refused-our-key 참조 시
Linux home directory, /home, for example, should be (0755/drwxr-xr-x).
User's home directory, /home/ec2-user/, for example, should be (0700/drwx------).
.ssh directory permission, /home/ec2-user/.ssh, for example, should be (0700/drwx------).
authorized_keys file permission, /home/ec2-user/.ssh/authorized_keys, for example, should be (0600/-rw-------).
Amazon Linux 기준이지만 이에 맞추어 권한 설정하였으므로 644가 아닌 700으로 설정됨

==========
[36m[U-16] world writable 파일 점검[0m
양호 : world writable 파일이 존재하지 않거나, 존재 시 설정 이유를 확인하고 있는 경우
취약 : world writable 파일이 존재하나 해당 설정 이유를 확인하고 있지 않는 경우
==========
[31m[취약] : world writable 파일이 존재합니다.[0m

조치사항
 # find / -xdev -type f -perm 777 실행 결과 아무 파일도 검색되지 않음.
 # find / -type f -perm 777 -exec ls -l {} \; 실행 결과
find: '/proc/26575/task/26575/fdinfo/5': No such file or directory
find: '/proc/26575/fdinfo/6': No such file or directory
해당 파일 없음 확인
 # find / -type f -perm -2 -exec ls -l {} \; 실행 결과
권한이 666 또는 222로 설정되어 있는 파일은 확인했지만 777로 설정되어 있는 파일 없음 확인

==========
[36m[U-17] world writable 파일 점검[0m
양호 : login, shell, exec 서비스를 사용하지 않거나, 사용 시 아래와 같은 설정이 적용된 경우
- /etc/hosts.equiv 및 ${HOME}/.rhosts 파일 소유자가 root 또는, 해당 계정인 경우

- /etc/hosts.equiv 및 ${HOME}/.rhosts 파일 권한이 600 이하인 경우
- /etc/hosts.equiv 및 ${HOME}/.rhosts 설정에 '+' 설정이 없는 경우
- /etc/hosts.equiv 파일 또는 .rhosts 파일이 존재하지 않을 경우
취약 : Anonymous FTP (익명 ftp) 접속을 차단하지 않은 경우
- /etc/hosts.equiv 및 ${HOME}/.rhosts 파일 소유자가 root 또는 해당 계정이 아닌 경우
- /etc/hosts.equiv 및 ${HOME}/.rhosts 파일 권한이 600 초과인 경우
- /etc/hosts.equiv 및 ${HOME}/.rhosts 설정에 '+' 설정이 있는 경우
- /etc/hosts.equiv 파일 또는 .rhosts 파일이 존재하는 경우
==========
[32m[양호] : /etc/hosts.equiv 파일이 존재하지 않습니다.[0m
[32m[양호] : /root/.rhosts 파일이 존재하지 않습니다.[0m

==========
[36m[U-19] cron 파일 소유자 및 권한 설정[0m
양호 : /etc/crontab 파일의 소유자가 root이고, 권한이 640 이하인 경우
취약 : /etc/crontab 파일의 소유자가 root가 아니거나, 권한이 640 초과인 경우
==========
[32m[양호] : /etc/crontab 파일의 소유자와 권한이 정상입니다.[0m

==========
[36m[U-20] Finger 서비스 비활성화[0m
양호 : finger 서비스가 비활성화 되어 있는 경우
취약 : finger 서비스가 활성화 되어 있는 경우
==========
[32m[양호] : Finger 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

==========
[36m[U-21] ANONYMOUS FTP 비활성[0m
양호 : Anonymous FTP (익명 ftp) 접속을 차단한 경우
취약 : Anonymous FTP (익명 ftp) 접속을 차단하지 않은 경우
==========
[31m[취약] : Default FTP 서비스가 활성화 상태입니다.[0m
[32m[양호] : ProFTP 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m
[32m[양호] : vsFTP 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

조치사항

개발 편의 위해 WinSCP 프로그램 사용하여 로컬과 디비 간 파일 이동 및 수정하여 Default FTP 서비스 활성화 시켜 놓아야만 함

==========

[36m[U-22] r 계열 서비스 비활성화[0m
양호 : r 계열 서비스(rlogin, rsh, rexec)가 비활성화 되어 있는 경우
취약 : r 계열 서비스(rlogin, rsh, rexec)가 활성화 되어 있는 경우
==========
[32m[양호] : rsh 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m
[32m[양호] : rlogin 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m
[32m[양호] : rexec 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

==========
[36m[U-23] DoS 공격에 취약한 서비스 비활성화[0m
양호 : DoS 공격에 취약한 echo, discard, daytime, chargen 서비스가 비활성화 되어 있는 경우
취약 : DoS 공격에 취약한 echo, discard, daytime, chargen 서비스가 활성화 되어 있는 경우
==========
[32m[양호] : echo 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m
[32m[양호] : discard 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m
[32m[양호] : daytime 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m
[32m[양호] : chargen 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

==========
[36m[U-24] NFS 서비스 비활성화[0m
양호 : NFS 서비스 관련 데몬이 비활성화 되어 있는 경우
취약 : NFS 서비스 관련 데몬이 활성화 되어 있는 경우
==========
[32m[양호] : NFS 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

==========
[36m[U-25] NFS 접근통제[0m
양호 : NFS 서비스 사용 시 everyone 공유를 제한한 경우
취약 : NFS 서비스 사용 시 everyone 공유를 제한하지 않은 경우
==========
[32m[양호] : NFS 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

==========
[36m[U-26] automountd[0m
양호 : automount 서비스가 비활성화 되어 있는 경우
취약 : automount 서비스가 활성화 되어 있는 경우
==========
[32m[양호] : automount 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

```
==========================================================================
[36m[U-27] RPC 서비스 확인[0m
양호 : 불필요한 RPC 서비스가 비활성화 되어 있는 경우
취약 : 불필요한 RPC 서비스가 활성화 되어 있는 경우
==========================================================================
[32m[ 양호 ] : RPC 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

==========================================================================
[36m[U-28] NIS, NIS+ 점검[0m
양호 : NIS, NIS+ 서비스가 구동 중이지 않을 경우
취약 : NIS, NIS+ 서비스가 구동 중일 경우
==========================================================================
[32m[ 양호 ] : NIS 또는 NIS+ 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

==========================================================================
[36m[U-29] tftp, talk 서비스 비활성화[0m
양호 : tftp, talk 서비스가 비활성화 되어 있는 경우
취약 : tftp, talk 서비스가 활성화 되어 있는 경우
==========================================================================
[32m[ 양호 ] : tftp 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m
[32m[ 양호 ] : talk 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m
[32m[ 양호 ] : ntalk 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

==========================================================================
[36m[U-30] Sendmail 버전 점검[0m
양호 : Sendmail 버전을 정기적으로 점검하고, 최신 버전 패치를 했을 경우
취약 : Sendmail 버전을 정기적으로 점검하지 않거나, 최신 버전 패치가 되어 있지 않은 경
우
==========================================================================
[32m[ 양호 ] : Sendmail 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

==========================================================================
[36m[U-31] 스팸 메일 릴레이 제한[0m
양호 : SMTP 서비스를 사용하지 않거나 릴레이 제한이 설정되어 있는 경우
취약 : SMTP 서비스를 사용하며 릴레이 제한이 설정되어 있지 않은 경우
==========================================================================
[32m[ 양호 ] : Sendmail 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

==========================================================================
```

[36m[U-32] 일반사용자의 Sendmail 실행 방지[0m
양호 : SMTP 서비스 미사용 또는, 일반 사용자의 Sendmail 실행 방지가 설정된 경우
취약 : SMTP 서비스 사용 또는, 일반 사용자의 Sendmail 실행 방지가 설정되지 않은 경우
==
[32m[양호] : Sendmail 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

==
[36m[U-33] DNS 보안 버전 패치[0m
양호 : DNS 서비스를 사용하지 않거나 주기적으로 패치를 관리하고 있는 경우
취약 : DNS 서비스를 사용하며, 주기적으로 패치를 관리하고 있지 않은 경우
==
[32m[양호] : Bind(named) 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m

==
[36m[U-34] DNS ZoneTransfer 설정[0m
양호 : DNS 서비스 미사용 또는, Zone Transfer를 허가된 사용자에게만 허용한 경우
취약 : DNS 서비스 사용하며 Zone Transfer를 모든 사용자에게 허용한 경우
==
[32m[양호] : Bind(named) 서비스가 설치되어 있지 않거나 실행 중이지 않습니다.[0m