Docker 취약점 점검 상세 보고서

2023. 05. 20

HOSTNAME	Docker
OS	Linux ubuntu
IP	192.168.253.141

	점 검 항 목	취약도	점검결과	현재상태
D01	도커최신 패치 적용	상	양호	o Docker Client, Server의 버전이 23년도 최신버전 이기때문에 양호
D02	Docker daemon audit 설정	상	양호	o /etc/audit/rules.d/audit.rules에 /usr/bin/docker 감사 설정이 되어있으므로 양호
D03	/var/lib/docker audit 설정	상	취약	- /etc/audit/rules.d/audit.rules에 /var/lib/docker 감사 설정이 되어있지 않으므로 취약 - /etc/audit/rules.d/audit.rules에 '-w /etc/default/docker -k docker'추가 필요
D04	/etc/docker audit 설정	상	취약	o /etc/audit/rules.d/audit.rules에 /etc/docker 감사 설정이 되어있지 않으므로 취약 - /etc/audit/rules.d/audit.rules에 '-w /var/lib/docker -k docker'추가 필요
D05	docker.service audit 설정	상	취약	o /etc/audit/rules.d/audit.rules에 docker.service 감사 설정이 되어있지 않으므로 취약 - /etc/audit/rules.d/audit.rules에 '-w /lib/systemd/system/docker.service -k docker'추가
D06	docker.socker audit 설정	상	취약	o /etc/audit/rules.d/audit.rules에 docekr.socket 감사 설정이 되어있지 않으므로 취약 - /etc/audit/rules.d/audit.rules에 '-w /lib/systemd/system/docker.socket -k docker'추가 필요
D07	/etc/default/docker audit 설정	상	취약	o/etc/default/docker 파일의 감사 설정이 되어있지 않으므로 취약 1. /etc/default/docker audit
D08	default bridge를 통한 컨테이너 간 네트워크 트래픽 제한	상	취약	o docker.network.bridge.enable_icc:true로 제한이 설정이 되어있지 않으므로 취약 -docker.network.bridge.enable_icc:false로 제한 설정 필요
D09	docker.service 소유권 설정	상	양호	o docker.service 파일의 소유자 및 소유그룹이 root:root로 설정되어 있으므로 양호 1. docker.service file path
D10	docker.service 파일 접근권한 설정	상	양호	o docker.service 파일의 접근권한이 644 이하로 설정되어 있으므로 양호 1. docker.service file path
D11	docker.socket 소유권 설정	상	양호	o docker.socket 파일의 소유자 및 소유그룹이 root:root로 설정되어 있으므로 양호 1. docker.socket file path
D12	docker.socket 파일 접근권한 설정	상	양호	o docker.socket 파일의 접근권한이 644 이하임
D13	/etc/docker 디렉터리 소유권 설정	상	**양호**	o /etc/docker 디렉터리의 소유자 및 소유그룹이 root:root임
D14	/etc/docker 디렉터리 접근권한 설정	상	양호	o /etc/docker 디렉터리의 접근권한이 755 이하임
D15	/var/run/docker.sock 파일 소유권 설정	상	양호	o /var/rum/docker.sock 파일의 소유자 및 소유그룹이 root:root임 1. /var/run/docker.sock path /var/run/docker.sock 2. /var/run/docker.sock file ownership srw-rw---- 1 root docker 0 May 15 13:40 /var/run/docker.sock Result: Good
D16	/var/run/docker.sock 접근 권한 설정	상	양호	o /var/run/docker.sock 파일의 접근권한이 660 이하임
D17	daemon.json 파일 소유권 설정	상	양호	o /etc/docker/daemon.json 파일이 존재하지 않음
D18	daemon.json 접근 권한 설정	상	양호	o daemon.json 파일의 접근 권한이 644 이하임
D19	/etc/default/docker 파일 소유권 설정	상	양호	o daemon.json 파일의 소유권이 root:root임
D20	/etc/default/docker 접근 권한 설정	상	양호	o /etc/default/docker 파일의 소유권이 root:root임
D21	컨테이너에서 ssh 사용 금지	상	취약	o 컨테이너 SSH 활성화
D22	호스트 OS 주요 자원 접근 제어	상	취약	o 주요 시스템 디렉터리 마운트 금지 필요, /lib 디렉터리 마운트 상태로 취약
D23	인증-권한 제어	상	검토	o docker group 내 사용자 확인, 신뢰하지 않은 사용자 검토 후 불필요 사용자 삭제 필요
D24	SSL/TLS 적용	상	취약	o SSL/TLS 적용 미흡, --tlsverify --tlscacert --tlscert --tlskey 사용 확인 불가
D25	컨테이너 권한 제어	상	취약	o --no-new-privileges 값 설정 미흡
D26	인증제어	상	양호	o swarm mode 불필요하게 활성화 금지, swarm mode 동작하지 않음
D27	SSL/TLS 적용	상	취약	o SSL/TLS 적용 미흡, --tlsverify --tlscacert --tlscert --tlskey 사용 확인 불가
D28	도커 그룹에 불필요한 사용자 제거 (kisa(DO-02))	중	검토	o docker group 내 사용자 확인, 신뢰하지 않은 사용자 검토 후 불필요 사용자 삭제 필요
D29	legacy registry (v1) 비활성화 (kisa(DO-11), sk(3.3))	하	양호	o --disable-legacy-registry 옵션 적용되어 있음
D30	추가 권한 획득으로부터 컨테이너 제한 (kisa(DO-12), sk(1.8))	중	취약	o 컨테이너 추가 권한 획득 제한 설정이 적용되어 있지 않음
D31	root가 아닌 user로 컨테이너 실행(kisa(DO-25), sk(1.4))	중	취약	o 컨테이너가 root 권한으로 실행됨 1. 7e29df341bfef1860a648ddb8642bcy82d7030df5e36e61314d509237d589655cdd: User=
D32	도커를 위한 컨텐츠 신뢰성 활성화 (kisa(DO-26), sk(3.3))	중	취약	o Docker 컨텐츠 신뢰성 설정이 비활성화 1. DOCKER_CONTENT_TRUST
D33	컨테이너 SELinux 보안 옵션 설정 (kisa(DO-27), sk(1.8))	중	취약	o 도커 컨텐츠 신뢰성 설정이 비활성화 1. # DOCKER_OPTS="DOCKER_OPTS="--selinux-enabled" 주석처리 됨 Result : Vulnerable
D34	컨테이너에서 privileged 포트 매핑 금지 (kisa(DO-29), sk(1.5))	중	양호	o 컨테이너 포트가 privileged 포트에 매핑되어 있지 않음 1. docker inspect c192484c4895 | grep -A 50 NetworkSettings | grep Ports
D35	도커의 default bridge docker() 사용 제한 (kisa(DO-31), sk(1.5))	하	취약	o Default bridge docker () 를 사용 1. docker0: flags=4136<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
D36	호스트의 user namespaces 공유제한 (kisa, sk) (kisa(DO-32), sk(1.4))	하	양호	o 호스트의 user namespace를 컨테이너와 공유하고 있지 않음 1.
D37	컨테이너 보안 정책 (sk(1.8))	중	취약	oSELinux 설정이 되어 있지 않으므로 취약 -docker daemon --selinux-enabled 설정 필요
D38	로그 관리 (sk(1.9))	하	취약	o --log-level 파라미터 값이 존재하지 않으며 중앙 집중식 원격 로깅 구성이 되어있지 않으므로 취약
D39	Dockerfile Config (sk(3.1))	중	취약	o dockerfile 내 ADD 명령어 사용 IMAGE CREATED CREATED BY
D40	이미지 취약점 및 무결성 점검 (sk(3.2))	중	양호	o 컨테이너 내 존재하는 패키지는 모두 신뢰할 수 있는 패키지이므로 양호 Name Version Architecture Description
D41	네트워크 제어 (sk(4.3))	중	양호	o docker swarm 네트워크 인터페이스가 존재하지 않음
