
Linux 진단 스크립트 개발

Made by 박수현

Email : qkrtnigus211@naver.com

A Table of Contents.

1 개요

2 평가 기준 및 항목

3 사용 예시

Linux 시스템의 설정 값을 진단하기 위한 자동화 스크립트입니다.

진단 기준 : 2021 KISA 주요정보통신기반시설 기술적 취약점 분석/평가 가이드

작성 언어 : Shell Script

개발 목적 : 운영중인 서버 시스템의 취약점을 제거하고 서비스의 안정성 및 신뢰성 향상을 목표로 함

세부적인 코드 내용과 스크립트 파일은 아래 Github URL을 통해 확인하실 수 있습니다.

Github URL : https://github.com/zjsl3784/Linux_script_v1



Part 2, 평가 기준 및 항목

평가 기준

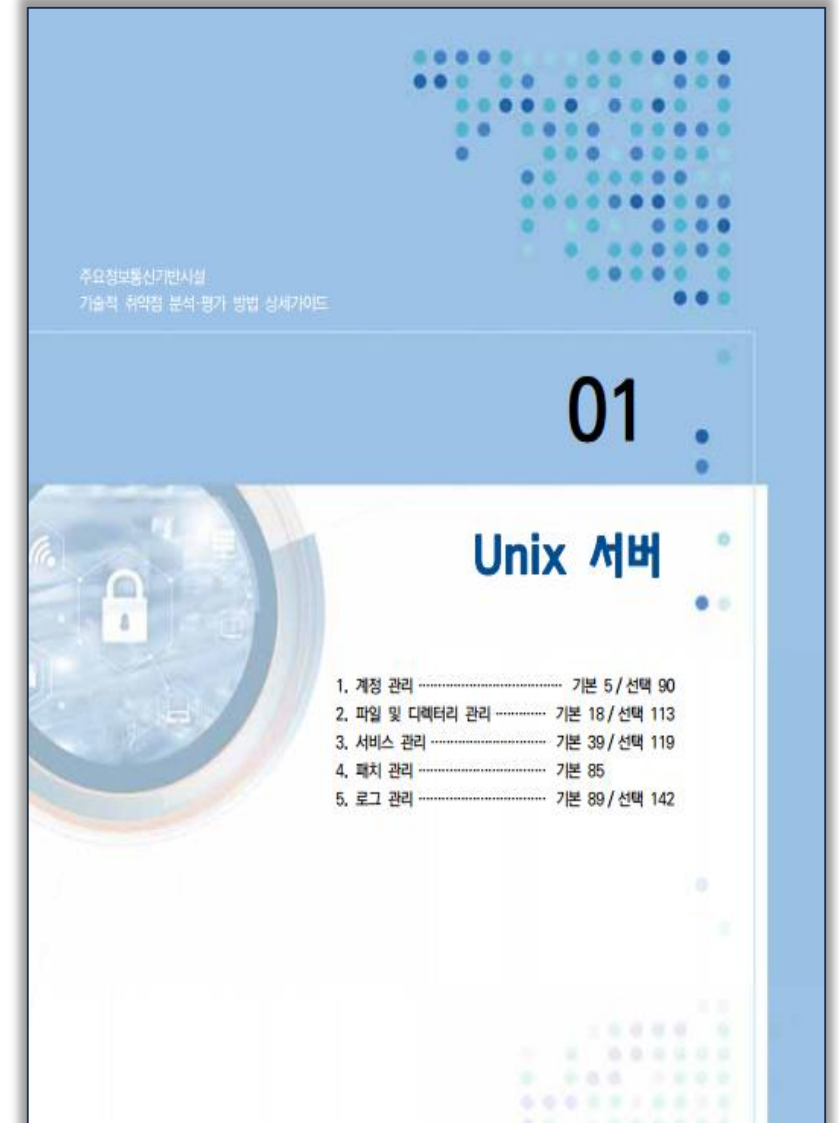
2021 KISA 주요정보통신기반시설 기술적 취약점 분석/평가 가이드의 “Unix 서버” 평가 항목을 기준으로 해당 가이드의 U-01 ~ U-72 코드 순서대로 진단을 수행 합니다.

예외 항목

일부 항목 (U-35 ~ U-41, U-71)은 Unix 서버 시스템과는 조금 무관한 웹 서버 Apache의 점검 내용이기예 제외 하였습니다. 해당 웹 서버 항목은 차후에 “웹 서버-Apache” 진단 스크립트를 별도로 제작할 때 추가하여 제작할 예정입니다.

예외 사유

Unix 시스템에서 웹 서버를 사용하지 않을 수 있으며, 또한 웹 서버를 Apache만 사용하는 것이 아니기에 별도로 분리하여 진단하는 것이 혼란을 최소화 하고, 여러 관점(컨설턴트 및 고객사)에서 보다 합리적이라 생각합니다.



Part 2, 평가 기준 및 항목

평가 항목

예외 항목을 제외한 점검 리스트 입니다.

2021 KISA 주요정보통신기반시설 기술적 취약점 분석/평가 가이드의 3p, 4p 참조

점검 시 과부하가 발생할 수 있는 항목에 대해

진단 여부 선택 가능

(진단 예시 : find / 명령어 사용)

운영중인 서버인 경우 진행하지 않는 것을 권고

분류	점검항목	항목 중요도	항목코드
1. 계정 관리	root 계정 원격 접속 제한	상	U-01
	패스워드 복잡성 설정	상	U-02
	계정 잠금 임계값 설정	상	U-03
	패스워드 파일 보호	상	U-04
	root 이외의 UID가 '0'금지	중	U-44
	root 계정 su 제한	하	U-45
	패스워드 최소 길이 설정	중	U-46
	패스워드 최대 사용기간 설정	중	U-47
	패스워드 최소 사용기간 설정	중	U-48
	불필요한 계정 제거	하	U-49
	관리자 그룹에 최소한의 계정 포함	하	U-50
	계정이 존재하지 않는 GID 금지	하	U-51
	동일한 UID 금지	중	U-52
	사용자 shell 점검	하	U-53
	Session Timeout 설정	하	U-54
2. 파일 및 디렉터리 관리	root 홈, 패스 디렉터리 권한 및 패스 설정	상	U-05
	파일 및 디렉터리 소유자 설정	상	U-06
	/etc/passwd 파일 소유자 및 권한 설정	상	U-07
	/etc/shadow 파일 소유자 및 권한 설정	상	U-08
	/etc/hosts 파일 소유자 및 권한 설정	상	U-09
	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상	U-10
	/etc/syslog.conf 파일 소유자 및 권한 설정	상	U-11
	/etc/services 파일 소유자 및 권한 설정	상	U-12
	SUID, SGID, Sticky bit 설정 파일 점검	상	U-13
	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상	U-14
	world writable 파일 점검	상	U-15
	/dev에 존재하지 않는 device 파일 점검	상	U-16
	\$HOME/.rhosts, hosts.equiv 사용 금지	상	U-17
	접속 IP 및 포트 제한	상	U-18
	hosts.lpd 파일 소유자 및 권한 설정	하	U-55
	UMASK 설정 관리	중	U-56
	홈디렉토리 소유자 및 권한 설정	중	U-57
	홈디렉토리로 지정한 디렉토리의 존재 관리	중	U-58
	숨겨진 파일 및 디렉터리 검색 및 제거	하	U-59

분류	점검항목	항목 중요도	항목코드
3. 서비스 관리	finger 서비스 비활성화	상	U-19
	Anonymous FTP 비활성화	상	U-20
	r 계열 서비스 비활성화	상	U-21
	cron 파일 소유자 및 권한설정	상	U-22
	Dos 공격에 취약한 서비스 비활성화	상	U-23
	NFS 서비스 비활성화	상	U-24
	NFS 접근 통제	상	U-25
	automountd 제거	상	U-26
	RPC 서비스 확인	상	U-27
	NIS, NIS+ 점검	상	U-28
	tftp, talk 서비스 비활성화	상	U-29
	Sendmail 버전 점검	상	U-30
	스팸 메일 릴레이 제한	상	U-31
	일반사용자의 Sendmail 실행 방지	상	U-32
	DNS 보안 버전 패치	상	U-33
	DNS Zone Transfer 설정	상	U-34
	웹서비스 타겟도리 리스킹 제거	상	U-35
	웹서비스 웹 프로세스 권한 제한	상	U-36
	웹서비스 상위 타겟도리 접근 금지	상	U-37
	웹서비스 불필요한 파일 제거	상	U-38
	웹서비스 쿼크 사용 금지	상	U-39
	웹서비스 파일 업로드 및 다운로드 제한	상	U-40
	웹서비스 영역의 분리	상	U-41
	ssh 원격접속 허용	중	U-60
	ftp 서비스 확인	하	U-61
	ftp 계정 shell 제한	중	U-62
	Ftpusers 파일 소유자 및 권한 설정	하	U-63
	Ftpusers 파일 설정	중	U-64
	at 파일 소유자 및 권한 설정	중	U-65
	SNMP 서비스 구동 점검	중	U-66
	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	U-67
	로그온 시 경고 메시지 제공	하	U-68
	NFS 설정파일 접근 제한	중	U-69
	expn, vrfy 명령어 제한	중	U-70
	Apache 웹 서비스 정보 숨김	중	U-71
4. 패치 관리	최신 보안패치 및 벤더 권고사항 적용	상	U-42
5. 로그 관리	로그의 정기적 검토 및 보고	상	U-43
	정책에 따른 시스템 로깅 설정	하	U-72

Part 2, 평가 기준 및 항목

코드 내용 일부

가이드 5p

U-01 (상)		1. 계정관리 > 1.1 root 계정 원격접속 제한
		취약점 개요
점검내용	■ 시스템 정책에 root 계정의 원격터미널 접속차단 설정이 적용되어 있는지 점검	
점검목적	■ 관리자계정 탈취로 인한 시스템 장애를 방지하기 위해 외부 비인가자의 root 계정 접근 시도를 원천적으로 차단하기 위함	
보안위험	■ root 계정은 운영체제의 모든기능을 설정 및 변경이 가능하여(프로세스, 커널변경 등) root 계정을 탈취하여 외부에서 원격을 이용한 시스템 장애 및 각종 공격으로(무작위 대입 공격) 인한 root 계정 사용 불가 위험	
참고	※ root 계정: 여러 사용자가 사용하는 컴퓨터에서 모든 기능을 관리할 수 있는 총괄권한을 가진 유일한 특별 계정. 유닉스 시스템의 루트(root)는 시스템 관리자인 운용 관리자(Super User)로서 윈도우의 Administrator 보다 높은 System 계정에 해당하며, 사용자 계정을 생성하거나 소프트웨어를 설치하고, 환경 및 설정을 변경하거나 시스템의 동작을 감시 및 제어할 수 있음 ※ 무작위 대입 공격(Brute Force Attack): 특정한 암호를 풀기 위해 가능한 모든 값을 대입하는 공격 방법 ※ 사전 대입 공격(Dictionary Attack): 사전에 있는 단어를 입력하여 암호를 알아내거나 암호를 해독하는 데 사용되는 컴퓨터 공격 방법	
		점검대상 및 판단기준
대상	■ SOLARIS, LINUX, AIX, HP-UX 등	
판단기준	양호 : 원격 터미널 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우	
	취약 : 원격 터미널 서비스 사용 시 root 직접 접속을 허용한 경우	
조치방법	원격 접속 시 root 계정으로 바로 접속 할 수 없도록 설정파일 수정	

```
85 echo "==" [U-01] root 계정 원격접속 제한 ====="
86 echo " <row>" >> $Mk 2>&1
87 echo " <분류>계정관리</분류>" >> $Mk 2>&1
88 echo " <점검항목>root 계정 원격 접속 제한</점검항목>" >> $Mk 2>&1
89 echo " <주요코드>U-01</주요코드>" >> $Mk 2>&1
90 echo " <위험도>상</위험도>" >> $Mk 2>&1
91 echo " <점검내용>" >> $Mk 2>&1
92 echo "※ 기준 : 원격 터미널 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우 양호." >> $Mk 2>&1
93 echo " " >> $Mk 2>&1
94 echo "※ 현황 :" >> $Mk 2>&1
95 if [ `systemctl status telnet.socket 2>/dev/null | wc -l` -gt 0 ]; then
96 echo "[ telnet 서비스 실행 중 ]" >> $Mk 2>&1
97 echo "ps -ef | grep "telnetd" | grep -v "grep" >> $Mk 2>&1
98 if [ `cat /etc/securetty | grep "pts" | grep -v "#" | wc -l` -gt 0 ]; then chk 1
99 echo "/etc/securetty 파일에 pts 설정이 존재함 (취약)" >> $Mk 2>&1
100 echo "cat /etc/securetty | grep "pts" >> $Mk 2>&1
101 fi
102 if [ `cat /etc/pam.d/login | grep "pam_securetty.so" | grep "#" | wc -l` -gt 0 ]; then chk 1
103 echo "/etc/pam.d/login 파일 확인필요" >> $Mk 2>&1
104 echo "cat /etc/pam.d/login | grep "pam_securetty.so" >> $Mk 2>&1
105 fi
106 else echo "[ telnet 서비스 미사용 ]" >> $Mk 2>&1
107 fi
108 echo "" >> $Mk 2>&1
109
110 if [ `ps -ef | grep "sshd" | grep -v "grep" | wc -l` -gt 0 ]; then
111 echo "[ SSH 서비스 실행 중 ]" >> $Mk 2>&1
112 echo "ps -ef | grep "sshd" | grep -v "grep" >> $Mk 2>&1
113 if [ `cat /etc/ssh/sshd_config | grep "PermitRootLogin" | grep "yes" | grep "#" | wc -l` -gt 0 ]; then chk 1
114 echo " " >> $Mk 2>&1
115 echo "[ /etc/ssh/sshd_config 설정 값 ]" >> $Mk 2>&1
116 echo "cat /etc/ssh/sshd_config | grep "PermitRootLogin" | grep "yes" | grep "#" >> $Mk 2>&1
117 echo " " >> $Mk 2>&1
118 echo "PermitRootLogin 설정이 주석처리된 경우 root 원격 로그인 허용됨(취약)" >> $Mk 2>&1
119 fi
120 if [ `cat /etc/ssh/sshd_config | grep "PermitRootLogin" | grep "yes" | grep -v "#" | wc -l` -gt 0 ]; then ch
121 echo " " >> $Mk 2>&1
122 echo "[ /etc/ssh/sshd_config 설정 값 ]" >> $Mk 2>&1
123 echo "cat /etc/ssh/sshd_config | grep "PermitRootLogin" | grep "yes" | grep -v "#" >> $Mk 2>&1
124 echo " " >> $Mk 2>&1
125 echo "PermitRootLogin 설정이 허용됨 (취약)" >> $Mk 2>&1
126 else echo "SSH 서비스가 실행중이나 Root 로그인이 차단됨 (양호)" >> $Mk 2>&1
127 fi
128 else echo "[ ssh 서비스 미사용 ]" >> $Mk 2>&1
129 fi
```

Part 3, 사용 예시

사용 예시

Step1) 점검할 서버에 접속. Root권한의 계정 필요 (또는 su 사용)

```
▶ SSH session to root@192.168.31.129
? Direct SSH      : ✓
? SSH compression : ✓
? SSH-browser     : ✓
? X11-forwarding  : ✓ (remote display is forwarded through SSH)

▶ For more info, ctrl+click on help or visit our website.

Last failed login: Mon Feb 26 05:12:10 KST 2024 from gateway on ssh:notty
There were 4 failed login attempts since the last successful login.
Last login: Mon Feb 26 05:00:02 2024 from gateway
Hello Unix server
[root@localhost ~]#
```

Root권한 계정 필요 (또는 su 사용)

Step2) 원하는 경로에 디렉터리 생성 (경로나 디렉터리 이름은 상관 없음. 파일이 섞이는 것을 방지하기 위함)

```
▶ SSH session to root@192.168.31.129
? Direct SSH      : ✓
? SSH compression : ✓
? SSH-browser     : ✓
? X11-forwarding  : ✓ (remote display is forwarded through SSH)

▶ For more info, ctrl+click on help or visit our website.

Last failed login: Mon Feb 26 05:12:10 KST 2024 from gateway on ssh:notty
There were 4 failed login attempts since the last successful login.
Last login: Mon Feb 26 05:00:02 2024 from gateway
Hello Unix server
[root@localhost ~]#
[root@localhost ~]# mkdir /home/check
[root@localhost ~]#
[root@localhost ~]# cd /home/check
[root@localhost check]#
[root@localhost check]#
```

원하는 경로에 디렉터리 생성

사용 예시

Step3) 생성한 디렉터리에 스크립트 파일 복사

```
▶ SSH session to root@192.168.31.129
? Direct SSH      : ✓
? SSH compression : ✓
? SSH-browser     : ✓
? X11-forwarding  : ✓ (remote display is forwarded through SSH)

▶ For more info, ctrl+click on help or visit our website.

Last failed login: Mon Feb 26 05:12:10 KST 2024 from gateway on ssh:notty
There were 4 failed login attempts since the last successful login.
Last login: Mon Feb 26 05:00:02 2024 from gateway
Hello Unix server
[root@localhost ~]#
[root@localhost ~]# mkdir /home/check
[root@localhost ~]#
[root@localhost ~]# cd /home/check
[root@localhost check]#
[root@localhost check]# ls -al
합 계 128
drwxr-xr-x. 2 root root   35 2월 26 05:41 .
drwxr-xr-x. 10 root root  117 2월 26 05:37 ..
-rw-r--r--. 1 root root 130686 2월 26 05:41 LinuxScript_by_psh.sh
you have new mail in /var/spool/mail/root
[root@localhost check]#
[root@localhost check]#
```

해당 디렉터리에 스크립트 파일 복사

Step4) 복사한 스크립트 파일에 750 권한 부여

```
[root@localhost check]# ls -al
합 계 128
drwxr-xr-x. 2 root root   35 2월 26 05:41 .
drwxr-xr-x. 10 root root  117 2월 26 05:37 ..
-rw-r--r--. 1 root root 130686 2월 26 05:41 LinuxScript_by_psh.sh
[root@localhost check]#
[root@localhost check]# chmod 750 ./LinuxScript_by_psh.sh
[root@localhost check]#
[root@localhost check]#
```

스크립트 파일에 750 권한 부여

사용 예시

Step5) 스크립트 실행 및 전역변수 검사 선택

```
[root@localhost check]# ls -al
합계 128
drwxr-xr-x. 2 root root   35 2월 26 05:41 .
drwxr-xr-x. 10 root root  117 2월 26 05:37 ..
-rw-r--r--. 1 root root 130686 2월 26 05:41 LinuxScript_by_psh.sh
[root@localhost check]#
[root@localhost check]# chmod 750 ./LinuxScript_by_psh.sh
[root@localhost check]#
[root@localhost check]# ./LinuxScript_by_psh.sh
전역변수 검사를 진행하시겠습니까? ( 예시 : find / 사용 )
해당 항목은 점검 시 과부하가 발생할 수 있습니다 . 운영중인 서버인 경우 진행하지 않는
것을 권고드립니다 .
진행하지 않을 경우 U-06, U-15, U-59 항목은 N/A 처리 됩니다 .
```

진행 여부 입력 (y/n): n

전역변수 검사 선택

Step6) 진단 완료 후 생성된 결과 파일을 PC로 이동

```
== [U-55] hosts.lpd 파일 소유자 및 권한 설정 ==
== [U-56] UMASK 설정 관리 ==
== [U-57] 홈 디렉토리 소유자 및 권한 설정 ==
== [U-58] 홈 디렉토리로 지정한 디렉토리의 존재 관리 ==
== [U-59] 숨겨진 파일 및 디렉토리 검색 및 제거 == [ N/A ] ==
== [U-60] ssh 원격접속 허용 ==
== [U-61] ftp 서비스 확인 ==
== [U-62] ftp 계정 shell 제한 ==
== [U-63] ftpusers 파일 소유자 및 권한 설정 ==
== [U-64] ftpusers 파일 설정 (FTP 서비스 root 계정 접근 제한) ==
== [U-65] at 서비스 권한 설정 ==
== [U-66] SNMP 서비스 구동 점검 ==
== [U-67] SNMP 서비스 Community String의 복잡성 설정 ==
== [U-68] 로그인 시 경고 메시지 제공 ==
== [U-69] NFS 설정파일 접근 권한 ==
== [U-70] expn, vrfy 명령어 제한 ==
== [U-72] 정책에 따른 시스템 로깅 설정 ==
```

=====[E N D]=====

(결과 파일) Result_file_localhost.localdomain_240226.xml 파일을 확인해주세요.
감사합니다.

```
[root@localhost check]#
[root@localhost check]#
[root@localhost check]# ls
LinuxScript_by_psh.sh Result_file_localhost.localdomain_240226.xml
[root@localhost check]#
[root@localhost check]#
```

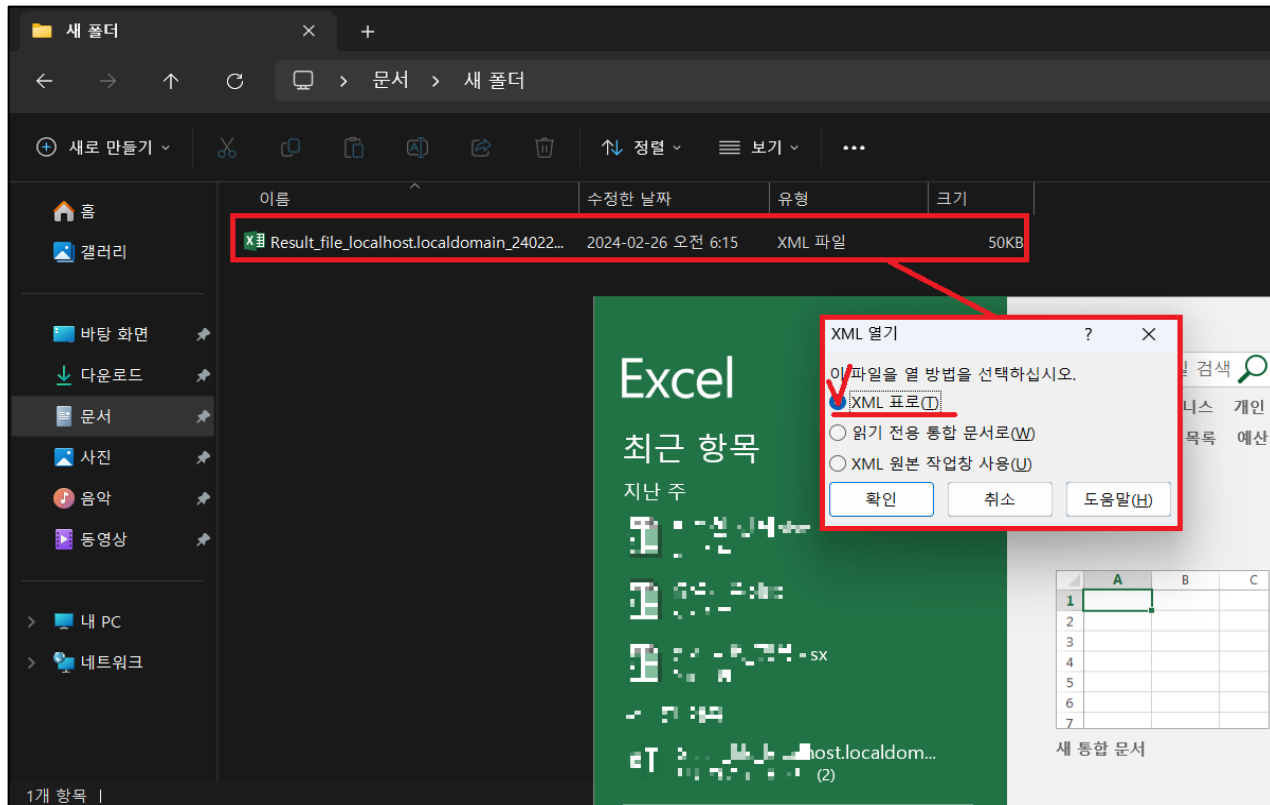
생성된 결과파일을 PC로 복사

Result file localhost.localdomain 240226.xml

Part 3, 사용 예시

사용 예시

Step7) PC로 복사한 결과 파일을 엑셀 -> XML 표를 선택하여 열기



사용 예시

Step8) 결과 확인

1	A	B	C	D	E	F
	분류	점검항목	주요코드	위험도	점검내용	결과
	Info	점검 기준 : KISA 2021 주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세가이드	점검 대상 : 호스트 IP : localhost 192.168.3. caldomain 1.129	OS정보 : CentOS Linux release 7.9.2009 (Core) NAME="CentOS Linux" VERSION="7" (Core) ID="centos" ID_LIKE="rhel fedora" VERSION_ID="7" PRETTY_NAME="CentOS Linux 7 (Core)" CPE_NAME="cpe:/o:centos:centos:7" CENTOS_MANTISBT_PROJECT="CentOS-7" CENTOS_MANTISBT_PROJECT_VERSION="7" REDHAT_SUPPORT_PRODUCT="centos" REDHAT_SUPPORT_PRODUCT_VERSION="7" CentOS Linux release 7.9.2009 (Core) CentOS Linux release 7.9.2009 (Core)	점검일자 : 2024. 02. 26. (월) 06:13:11 KST	
2	계정관리	root 계정 원격 접속 제한	U-01	상	※ 기준 : 원격 터미널 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우 양호. 현황 : [telnet 서비스 미사용] [SSH 서비스 실행 중] root 1207 1 0 04:54 ? 00:00:00 /usr/sbin/sshd -D root 2820 1207 0 04:57 ? 00:00:00 sshd: root@pts/1 root 6051 1207 0 05:17 ? 00:00:00 sshd: root@pts/2 root 6055 1207 0 05:17 ? 00:00:00 sshd: root@notty [/etc/ssh/sshd_config 설정 값] PermitRootLogin yes PermitRootLogin 설정이 허용됨 (취약)	취약
3						

4	분류	점검항목	주요코드	위험도	점검내용	결과
	계정관리	패스워드 복잡성 설정	U-02	상	※ 기준 : 패스워드 최소길이 8자리 이상, 영문 숫자 특수문자 최소 입력 기능이 설정된 경우 양호. 현황 : [/etc/security/pwquality.conf 설정 값] lcredit = -1 ucrcedit = -1 dcredit = -1 ocredit = -1 # minlen = 8 설정값이 주석처리 되어 있거나 부적절한 설정입니다. (취약) KISA 권장값 : lcredit -1, ucrcedit -1, dcredit -1, ocredit -1, minlen 8이상	취약
4	계정관리	계정 잠금 임계값 설정	U-03	상	※ 기준 : 계정 잠금 임계값이 10회 이하의 값으로 설정되어 있는 경우 양호. 현황 : [/etc/pam.d/system-auth 설정 값] auth required pam_env.so auth required pam_faildelay.so delay=2000000 auth required pam_deny.so account required pam_unix.so account required pam_permit.so 계정 잠금 임계값 설정이 존재하지 않음. (취약)	취약
5						

감사합니다.

Made by 박수현

Email : qkrtnigus211@naver.com

URL : https://github.com/zjsl3784/Linux_script_v1