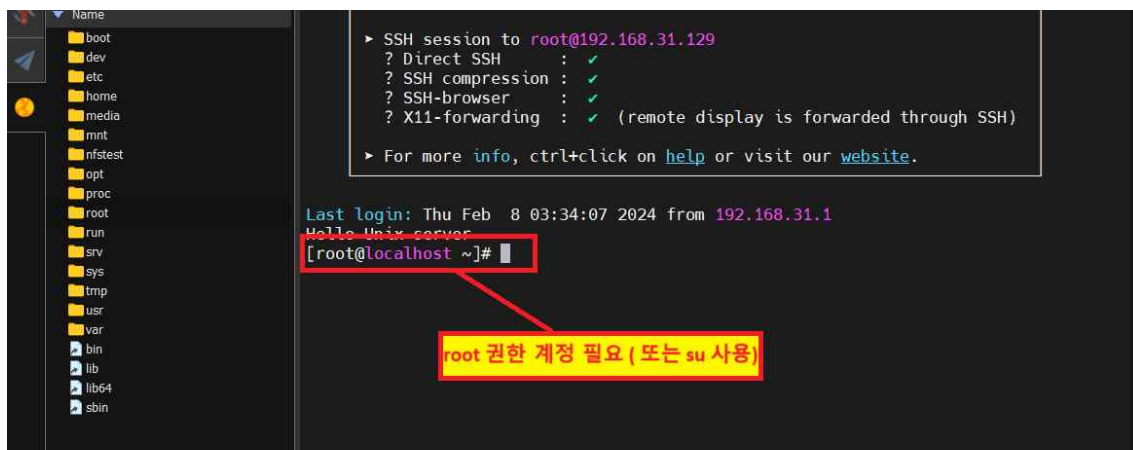
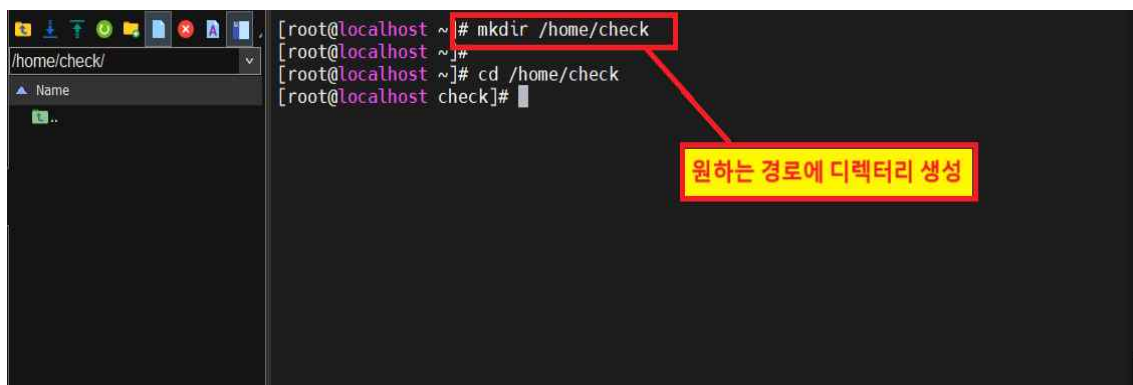


Linux_Script_by_psh 사용 예시

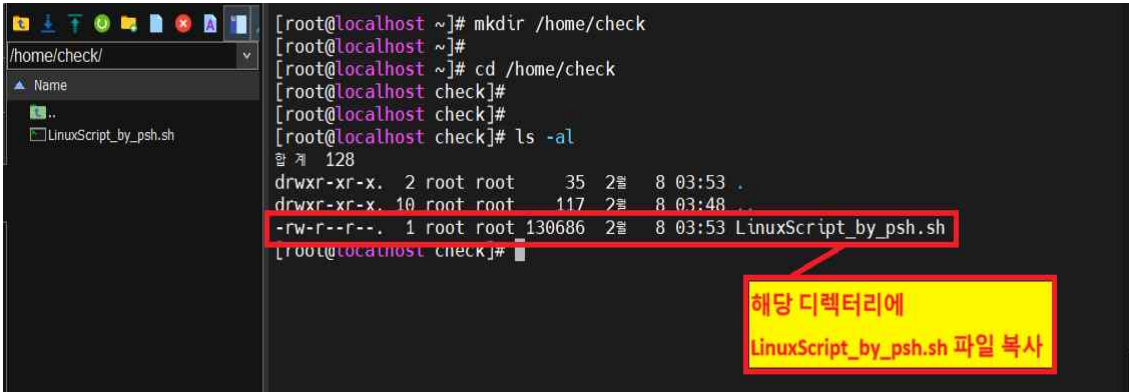
1. 점검할 서버에 접속. root권한의 계정으로 로그인 (또는 su사용)



2. 원하는 경로에 디렉터리 생성 (경로나 디렉터리 이름은 상관없음)



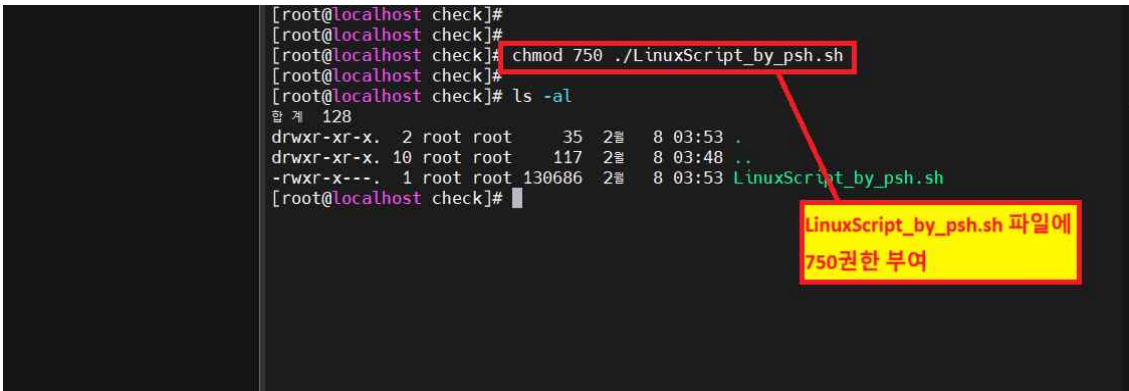
3. 생성한 디렉터리에 LinuxScript_by_psh.sh 파일 복사



```
[root@localhost ~]# mkdir /home/check
[root@localhost ~]#
[root@localhost ~]# cd /home/check
[root@localhost check]#
[root@localhost check]#
[root@localhost check]# ls -al
합계 128
drwxr-xr-x. 2 root root   35 2월  8 03:53 .
drwxr-xr-x. 10 root root  117 2월  8 03:48 ..
-rw-r--r--. 1 root root 130686 2월  8 03:53 LinuxScript_by_psh.sh
[root@localhost check]#
```

해당 디렉터리에
LinuxScript_by_psh.sh 파일 복사

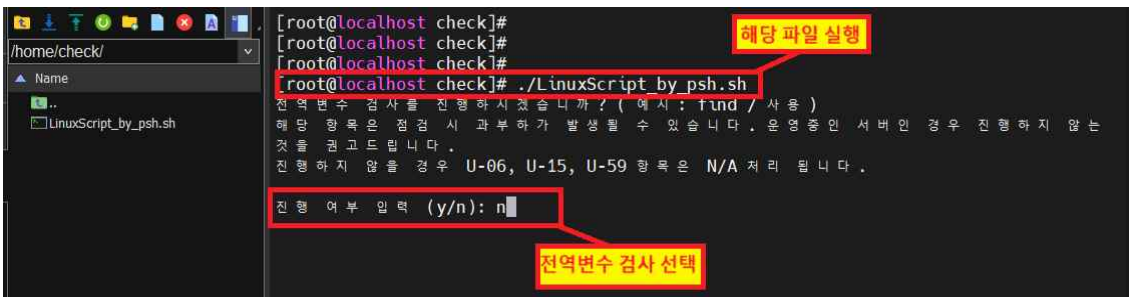
4. 복사한 LinuxScript_by_psh.sh 파일에 750 권한 부여



```
[root@localhost check]#
[root@localhost check]#
[root@localhost check]# chmod 750 ./LinuxScript_by_psh.sh
[root@localhost check]#
[root@localhost check]# ls -al
합계 128
drwxr-xr-x. 2 root root   35 2월  8 03:53 .
drwxr-xr-x. 10 root root  117 2월  8 03:48 ..
-rwxr-x---. 1 root root 130686 2월  8 03:53 LinuxScript_by_psh.sh
[root@localhost check]#
```

LinuxScript_by_psh.sh 파일에
750권한 부여

5. Linux_Script_by_psh.sh 파일 실행 및 전역변수 검사 선택



```
[root@localhost check]#
[root@localhost check]#
[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
```

해당 파일 실행

전역변수 검사 선택

6. 스크립트 진단 완료 후 생성된 결과파일을 PC로 이동

```
진행 여부 입력 (y/n): n
전역 변수 검사를 수행하지 않습니다.

=====
2021 KISA 주요 정보통신기반시설 기술적 취약점 분석/평가 가이드 기준
=====

< Linux 진단 스크립트 >

Made by 박수현
feedback email : qkrtngus211@naver.com
Version : 1.0v

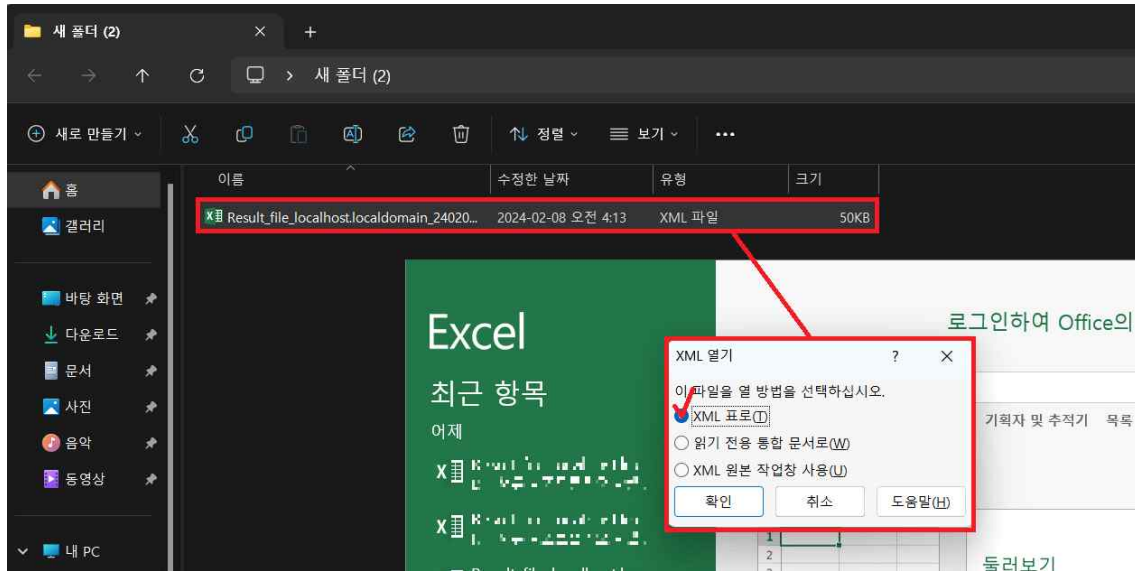
=====
START
[U-01] root 계정 원격접속 제한
[U-02] 패스워드 복잡성 설정
[U-03] 계정 잠금 임계값 설정
[U-04] 패스워드 파일 보호
[U-05] Rootkit, 패스 디렉터리 권한 및 패스 설정
[U-06] 파일 및 디렉터리 소유자 설정 [ N/A ]
[U-07] /etc/passwd 파일 소유자 및 권한 설정
[U-08] /etc/shadow 파일 소유자 및 권한 설정
[U-09] /etc/hosts 파일 소유자 및 권한 설정
[U-10] /etc/(x)inetd.conf 파일 소유자 및 권한 설정
[U-11] /etc/syslog.conf 파일 소유자 및 권한 설정
[U-12] /etc/services 파일 소유자 및 권한 설정
[U-13] SUID, SGID 설정 파일 점검
[U-14] 사용자, 시스템 시작 파일 및 환경파일 소유자 및 권한 설정
[U-15] world writable 파일 점검 [ N/A ]
[U-16] /dev에 존재하지 않는 device 파일 점검
[U-17] $HOME/.rhosts, hosts.equiv 사용 금지
[U-18] 접속 IP 및 포트 제한
[U-19] Finger 서비스 비활성화
[U-20] Anonymous FTP 비활성화
[U-21] r 계열 서비스 비활성화
[U-22] crond 파일 소유자 및 권한 설정

=====
[U-44] root 이외의 UID가 '0' 금지
[U-45] root 계정 su 제한
[U-46] 패스워드 최소 길이 설정
[U-47] 패스워드 최대 사용기간 설정
[U-48] 패스워드 최소 사용기간 설정
[U-49] 불필요한 계정 제거
[U-50] 관리자 그룹에 최소한의 계정 포함
[U-51] 계정이 존재하지 않는 GID 금지
[U-52] 동일한 UID 금지
[U-53] 사용자 shell 점검
[U-54] Session Timeout 설정
[U-55] hosts.lpd 파일 소유자 및 권한 설정
[U-56] UMASK 설정 관리
[U-57] 홈 디렉터리 소유자 및 권한 설정
[U-58] 홈 디렉터리로 지정한 디렉터리의 존재 관리
[U-59] 숨겨진 파일 및 디렉터리 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 접근제한)
[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 접근권한
[U-70] expn, vrfy 명령어 제한
[U-72] 정책에 따른 시스템 로깅 설정

=====
[ E N D ]

(결과파일) Result_file_localhost.localdomain_240208.xml 파일을 확인해주세요.
감사합니다.
[root@localhost check]#
[root@localhost check]# ls
LinuxScript_by_psh.sh Result file localhost.localdomain_240208.xml
[root@localhost check]#
```

7. PC로 복사한 결과파일을 엑셀 -> XML 표를 선택하여 열기



통합 문서1 - Excel									
파일	홈	삽입	페이지 레이아웃	수식	데이터	검토	보기	수행할 작업을 알려 주세요.	
잘라내기 붙여넣기 서식 복사	말은 고딕 가 가 가 가 가 가	11 가 가	가 가	가 가	가 가	가 가	가 가	가 가	가 가
글리드	글리드	글리드	글리드	글리드	글리드	글리드	글리드	글리드	글리드
K2									
1	분류	점검항목	주요코드	위험도	점검내용				
2	Info	<p>점검 기준 : KISA 2021 주요정보통신기반시설 기술적 취약점 분석 평가 방법 상세가이드</p>		<p>점검 대상 : localhost caldomain</p>	<p>호스트 IP 192.168.3 1.129</p> <p>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)</p>		<p>점검일자 : 2024. 02. 08. (목) 04:07:39 KST</p>		
3	계정관리	root 계정 원격 접속 제한	U-01	상	<p>※ 기준 : 원격 터미널 서비스를 사용하지 않거나, 사용 시 root 직접 접속을 차단한 경우 양호.</p> <p>현황 : [telnet 서비스 미사용]</p> <p>[SSH 서비스 실행 중]</p> <pre>root 1197 1 0 2월07 ? 00:00:00 /usr/sbin/sshd -D root 36778 1197 0 03:35 ? 00:00:00 sshd: root@pts/1 root 36794 1197 0 03:35 ? 00:00:00 sshd: root@notty</pre> <p>[/etc/ssh/sshd_config 설정 값]</p> <pre>PermitRootLogin yes</pre> <p>PermitRootLogin 설정이 허용됨 (취약)</p>		취약		
4	계정관리	패스워드 복잡성 설정	U-02	상	<p>※ 기준 : 패스워드 최소길이 8자리 이상, 영문 숫자 특수문자 최소 입력 기능이 설정 된 경우 양호.</p> <p>현황 : [/etc/security/pwquality.conf 설정 값]</p> <pre>lcredit = -1 ucredit = -1 dcredit = -1 ocredit = -1 # minlen = 8</pre> <p>설정값이 주석처리 되어 있거나 부적절한 설정입니다. (취약) KISA 권장값 : lcredit -1, ucredit -1, dcredit -1, ocredit -1, minlen 8이상</p>		취약		
5	계정관리	계정 잠금 임계값 설정	U-03	상	<p>※ 기준 : 계정 잠금 임계값이 10회 이하의 값으로 설정되어 있는 경우 양호.</p> <p>현황 : [/etc/pam.d/system-auth 설정 값]</p> <pre>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</pre> <p>계정 잠금 임계값 설정이 존재하지 않음. (취약)</p>		취약		