Telegram-bot 을 활용한 서버 취약점 진단

2조 : 일석이조

CONTENTS

01

주제 선정

01. 주제선정

서버 취약점 진단을 선정하는 이유

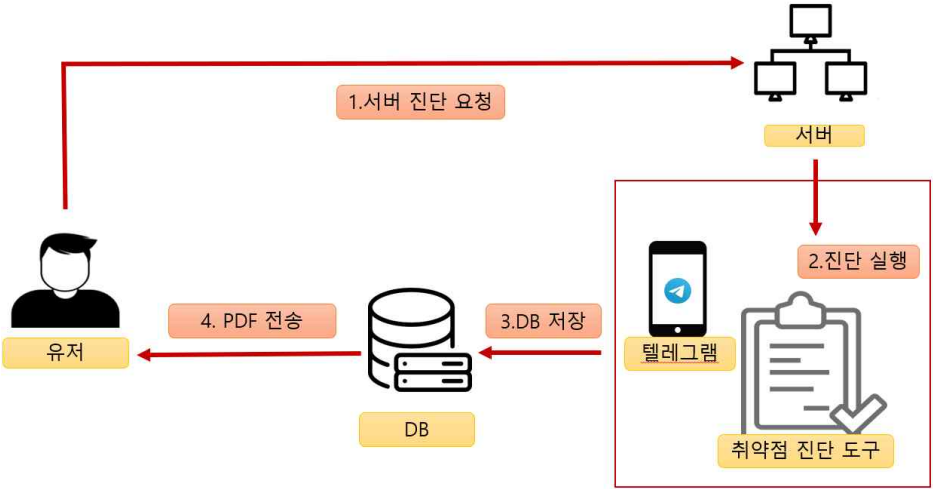
- [정보통신기반 보호법] 제 9조에 따라, 주요정보통신기반시설 관리기관은 매년 취약점 분석 평가를 실시하여야 한다.

- 사소해 보이는 취약점을 찾아서 위협 요소에 대한 조치 방안과 보호 대책을 제시하기 때문에 예방을 할 수 있다.

02

구상도

02. 구상도



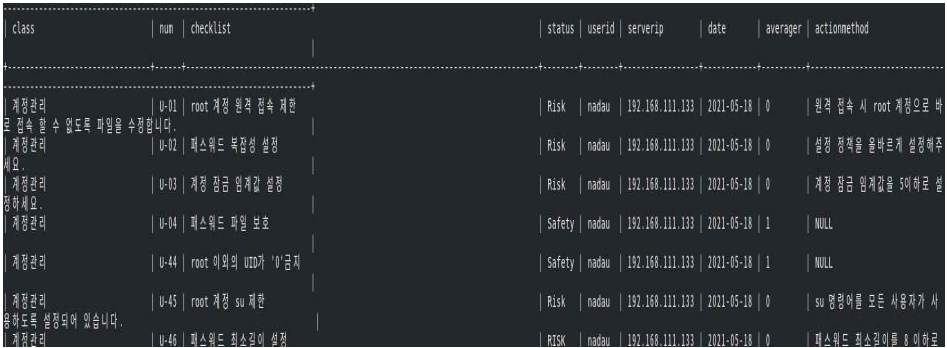
03

개발 일정 및 진행 사항

03. 개발 일정

추진기간 / 수행업무	3월	4월	5월	6월	7월	8월	9월	10월
기획 회의								
스크립트 개발								
DB연동 및 텔레그램 연동								
Main화면 만들기								

03. 개발내용



class	num	checklist	status	userid	serverip	date	averager	actionmethod
계정관리	U-01	root 계정 원격 접속 제한	Risk	nadau	192.168.111.133	2021-05-18	0	원격 접속 시 root 계정으로 바로 접속 할 수 없도록 파일을 수정합니다.
계정관리	U-02	패스워드 복잡성 설정	Risk	nadau	192.168.111.133	2021-05-18	0	설정 정책을 올바르게 설정해주세요.
계정관리	U-03	계정 잠금 임계값 설정	Risk	nadau	192.168.111.133	2021-05-18	0	계정 잠금 임계값을 5이하로 설정하세요.
계정관리	U-04	패스워드 파일 보호	Safety	nadau	192.168.111.133	2021-05-18	1	NULL
계정관리	U-44	root 이외의 UID가 '0'금지	Safety	nadau	192.168.111.133	2021-05-18	1	NULL
계정관리	U-45	root 계정 su 제한	Risk	nadau	192.168.111.133	2021-05-18	0	su 명령어를 모든 사용자가 사용하도록 설정되어 있습니다.
계정관리	U-46	패스워드 최소길이 설정	RISK	nadau	192.168.111.133	2021-05-18	0	패스워드 최소길이를 8 이하로

계정 관리 15개 항목

03. 개발내용 (script)

분류	항목	진행사항
계정 관리	Root 계정 원격 접속 제한	●
	패스워드 복잡성 설정	●
	계정 잠금 임계값 설정	●
	패스워드 파일 보호	●
	Root 이외의 UID가 0금지	●
	Root 계정 su 제한	●
	패스워드 최소 길이 설정	●
	패스워드 최대 사용기간 설정	●
	패스워드 최소 사용기간 설정	●
	불필요한 계정 제거	●
	관리자 그룹에 최소한의 계정포함	●
	계정이 존재하지 않는 GID금지	●
	동일한 UID금지	●
	사용자 shell 점검	▲
	Session Timeout 설정	●

파일 및 디렉터리 관리 20개 항목

03. 개발내용 (script)

분류	항목	진행사항	항목	진행사항
파일 및 디렉터리 관리	Root 홈, 패스 디렉터리 권한 및 패스 설정	●	World writable 파일 점검	●
	파일 및 디렉터리 소유자 설정	●	/dev에 존재하지 않는 device 파일 점검	●
	/etc/passwd 파일 소유자 및 권한 설정	●	$HOME/.rhosts, hosts.equiv 사용 금지	●
	/etc/shadow 파일 소유자 및 권한 설정	●	접속 IP 및 포트 제한	●
	/etc/hosts 파일 소유자 및 권한 설정	●	Hosts.lpd 파일 소유자 및 권한 설정	●
	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	●	NIS 서비스 비활성화	●
	/etc/syslog.conf 파일 소유자 및 권한 설정	●	UMASK 설정 관리	●
	/etc/services 파일 소유자 및 권한 설정	●	홈디렉터리 소유자 및 권한 설정	●
	SUID, SGID, Sticky bit 설정 파일 점검	●	홈디렉터리로 지정한 디렉터리의 존재 관리	●
	사용자, 시스템 시작 파일 및 환경파일 소유자 및 권한 설정	●	숨겨진 파일 및 디렉터리 검색 및 제거	●

서비스 관리 35개 항목

03. 개발내용 (script)

분류	항목	진행사항	항목	진행사항
서비스 관리	Finger 서비스 비활성화	●	Sendmail 버전 점검	●
	Anonymous FTP 비활성화	●	스팸 메일 릴레이 제한	●
	R 계열 서비스 비활성화	●	일반 사용자의 sendmail 실행방지	●
	Cron 파일 소유자 및 권한설정	●	DNS 보안 버전 패치	●
	Dos 공격에 취약한 서비스 비활성화	●	DNS Zone Transfer 설정	●
	NFS 서비스 비활성화	●	Apache 디렉터리 리스팅 제거	●
	NFS 접근 통제	●	Apache 웹 프로세스 권한 제한	●
	Automointd 제거	●	Apache 상위 디렉터리 접근 금지	●
	RPC 서비스 확인	●	Apache 불필요한 파일 제거	●
	NIS, NIS+ 점검	●	Apache 링크 사용 금지	●
	Tftp, talk 서비스 비활성화	●	Apache 파일 업로드 및 다운로드 제한	●

서비스 관리 35개 항목

03. 개발내용 (script)

분류	항목	진행사항	항목	진행사항
서비스 관리	Finger 서비스 비활성화	●	Sendmail 버전 점검	●
	Anonymous FTP 비활성화	●	스팸 메일 릴레이 제한	●
	R 계열 서비스 비활성화	●	일반 사용자의 sendmail 실행방지	●
	Cron 파일 소유자 및 권한설정	●	DNS 보안 버전 패치	●
	Dos 공격에 취약한 서비스 비활성화	●	DNS Zone Transfer 설정	●
	NFS 서비스 비활성화	●	Apache 디렉터리 리스팅 제거	●
	NFS 접근 통제	●	Apache 웹 프로세스 권한 제한	●
	Automointd 제거	●	Apache 상위 디렉터리 접근 금지	●
	RPC 서비스 확인	●	Apache 불필요한 파일 제거	●
	NIS, NIS+ 점검	●	Apache 링크 사용 금지	●
	Tftp, talk 서비스 비활성화	●	Apache 파일 업로드 및 다운로드 제한	●

서비스 관리 35개 항목

03. 개발내용 (script)

분류	항목	진행사항	항목	진행사항
서비스 관리	Finger 서비스 비활성화	●	Sendmail 버전 점검	●
	Anonymous FTP 비활성화	●	스팸 메일 릴레이 제한	●
	R 계열 서비스 비활성화	●	일반 사용자의 sendmail 실행방지	●
	Cron 파일 소유자 및 권한설정	●	DNS 보안 버전 패치	●
	Dos 공격에 취약한 서비스 비활성화	●	DNS Zone Transfer 설정	●
	NFS 서비스 비활성화	●	Apache 디렉터리 리스팅 제거	●
	NFS 접근 통제	●	Apache 웹 프로세스 권한 제한	●
	Automointd 제거	●	Apache 상위 디렉터리 접근 금지	●
	RPC 서비스 확인	●	Apache 불필요한 파일 제거	●
	NIS, NIS+ 점검	●	Apache 링크 사용 금지	●
	Tftp, talk 서비스 비활성화	●	Apache 파일 업로드 및 다운로드 제한	●

서비스 관리 35개 항목

03. 개발내용 (script)

분류	항목	진행사항
서비스 관리	Apache 웹 서비스 영역의 분리	●
	Ssh 원격접속 허용	●
	ftp 서비스 확인	●
	ftp 계정 shell 확인	●
	Ftpusers 파일 소유자 및 권한 설정	▲
	Ftpusers 파일 설정	●
	At 파일 소유자 및 권한 설정	●
	SNMP 서비스 구동 점검	●
	SNMP 서비스 커뮤니티 스트링의 복잡성 설정	●
	로그온 시 경고 메시지 제공	●
	NFS 설정 파일 접근 제한	●
	Expn, vrfy 명령어 제한	●
	Apache 웹 서비스 정보 숨김	●

03. 개발내용 (window script)

분류	항목	진행사항	분류	항목	진행사항
계정 관리	Administrator 계정 이름 변경 또는 보안성 강화	●	계정 관리	패스워드 최소 암호 길이	●
	Guest 계정 비활성화	●		패스워드 최대 사용 기간	●
	불필요한 계정 제거	●		패스워드 최소 사용 기간	●
	계정 잠금 임계값 설정	●		마지막 사용자 이름 표시 안 함	●
	해독 가능한 암호화를 사용하여 암호 저장 해제	●		로컬 로그온 허용	●
	관리자 그룹에 최소한의 사용자 포함	●		익명 SID/이름 변환 허용 해제	●
	Everyone 사용권한을 익명 사용자에 적용 해제	●		최근 암호 기억	●
	계정 잠금 기간 설정	●		콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한	●
	패스워드 복잡성 설정	●		원격터미널 접속 가능한 사용자 그룹 제한	●

03. 개발내용 (window script)

분류	항목	진행 사항
서비스 관리	공유 권한 및 사용자 그룹 설정	●
	하드디스크 기본 공유 제거	●
	불필요한 서비스 제거	●
	IIS 서비스 구동 점검	●
	IIS 디렉토리 리스팅 제거	●
	IIS CGI 실행 제한	●
	IIS 상위 디렉토리 접근 금지	●
	IIS 불필요한 파일 제거	●
	IIS 웹프로세스 권한 제한	●
	IIS 링크 사용 금지	●
	IIS 파일 업로드 및 다운로드 제한	●
	IIS DB 연결 취약점 점검	●

항목	진행 사항
IIS 가상 디렉토리 삭제	●
IIS 데이터파일 ACL 적용	●
IIS 미사용 스크립트 매핑 제거	●
IISExec 명령어 쉘호출 진단	●
IIS WebDAV 비활성화	●
NetBIOS 바인딩 서비스 구동 점검	●
FTP 서비스 구동 점검	●
FTP 디렉토리 접근권한 설정	●
Anonymous FTP 금지	●
FTP 접근 제어 설정	●
DNS Zone Transfer 설정	●
RDS 제거	●

항목	진행 사항
최신 서비스팩 적용	●
터미널 서비스 암호화 수준 설정	●
IIS 웹 서비스 정보 숨김	●
SNMP 서비스 구동 점검	●
SNMP 서비스 커뮤니티스트링의 복잡성 설정	●
SNMP Access control 설정	●
DNS 서비스 구동 점검	●
HTTP/FTP/SMTP 배너 차단	●
Telnet 보안 설정	●
불필요한 ODBC/OLE-DB 데이터소스와 드라이브 제거	●
원격터미널 접속 타임아웃 설정	●
예약된 작업에 의심스러운 명령이 등록되어 있는지 점검 중	●

03. 개발내용 (window script)

분류	항목	진행사항
패치 관리	최신 HOT FIX 적용	●
	백신 프로그램 업데이트	●
	정책에 따른 시스템 로깅설정	●
로그 관리	로그의 정기적 검토 및 보고	●
	원격으로 액세스 할 수 있는 레지스트리 경로	●
	이벤트 로그 관리 설정	●
	원격에서 이벤트 로그파일 접근 차단	●

03. 개발내용 (window script)

분류	항목	진행사항	항목	진행사항
서비스 관리	백신 프로그램 설치	●	Dos 공격 방어 레지스트리 설정	●
	SAM 파일 접근 통제 설정	●	사용자가 프린터 드라이버를 설치할 수 없게 함	●
	화면보호기 설정	●	세션 연결을 중단하기 전에 필요한 유휴시간	●
	로그온 하지 않고 시스템 종료 허용 해제	●	경고 메시지 설정	●
	원격 시스템에서 강제로 시스템 종료	●	사용자별 홈 디렉토리 권한 설정	●
	보안감사를 로그할 수 없는 경우 즉시 시스템 종료 해제	●	LAN Manager 인증 수준	●
	SAM 계정과 공유의 익명 열거 허용 안함	●	보안 채널 데이터 디지털 암호화 또는 서명	●
	Autologon 기능 제어	●	파일 및 디렉토리 보호	●
	이동식 미디어 포맷 및 꺼내기 허용	●	컴퓨터 계정 암호 최대 사용 기간	●
	디스크 볼륨 암호화 설정	●	시작 프로그램 목록 분석	●

03. 개발내용 (script)

Main 코드

```
#!/bin/bash

clear

while [ True ]
do
        echo -e "\n********************취약점 진단 프로그램********************₩n"
        echo -e "                                                만든이 : 2조(이게뭐조)₩n"
       echo -en "1.진단하기₩n\n2.진단결과 확인하기₩n\n3.만든이 보기₩n\n4.나가기₩n\n입력:"
       read check


    if [ $check -eq 1 ]; then


        while [ True ]
        do

            echo -n "회원ID 입력:"
            read TMPID

            mysql -h localhost -usebin -p1234 -e "select id from user where id like '$TMPID';" joongbu_db > /joongbu_script/UID.txt

            if [ -z "`cat /joongbu_script/UID.txt`" ]; then
                clear
                echo "존재하지 않는 아이디 입니다."
                continue
            else
                clear
                echo "아이디가 존재 합니다."
                uid=`cat /joongbu_script/UID.txt | tail -1`
                #rm -rf /joongbu_script/UID.txt
                break
            fi
        done
```

03. 개발내용 (script)

Main 코드

```
〈 중부대학교 고양캠퍼스 소속 〉
91613703 남승택                    91812335 박세빈
91812608 신자연                    91812701 왕나원
91812672 양재희
〈 주요 프로젝트 내용 〉
리눅스 서버 구축 및 취약점 진단 스크립트 작성
윈도우 서버 구축 및 취약점 진단 스크립트 작성
진단 결과 pdf 파일로 확인
DB 연동 및 텔레그램 연동
메뉴로 돌아가시겠습니까? (y):
```

```
********************취약점 진단 프로그램********************
                                        만든이 : 2조(이게뭐조)
1. 진단하기
2. 진단결과 확인하기
3. 만든이 보기
4. 나가기
입력:
```

03. 개발내용 (script)

Main 코드

```
총 합 : 73
전체 양 호 : 46
전체 취 약 : 22
자체 검 사 : 2
전체 검사 불가 : 3
Connection to 192.168.111.100 closed.
 [3: J

**********취약점 진단 프로그램**********

                                    만든이 : 2조(이게뭐조)

1. 진단하기

2. 진단결과 확인하기

3. 만든이 보기

4. 나가기

입력:
```

```
원격지 ID입력 :root
원격지 IP 입력 :192.168.111.100

  아이디가 존재 합니다.

  OS 종류를 선택 하세요. (1. linux(centos) 2. windows server 2012) :

〈 U-53 사용자 shell 점검 〉

상태 : 취약
로그인이 필요하지 않은 계정에 /bin/false(/sbin/nologin)쉘이 부여되지 않았습니다.

================================================================================

〈 U-54 Session Timeout 설정 〉

상태 : 취약
TMOUT이 설정되어 있지 않습니다

================================================================================

                                    계정관리 총 합 : 15
                                    계정관리 양 호 : 5
                                    계정관리 취 약 : 10
                                    계정관리 검사 불가 : 0
```

03. 개발내용 (script)

Main 코드

```
********************취약점 진단 프로그램 *********************

                                        만든이 : 2조(이게뭐조)

1. 진단하기

2. 진단결과 확인하기

3. 만든이 보기

4. 나가기

입력 : 2
```

```
*************** 계정관리 부분 ***************
                계정 관리 양 호 : 5
                계정 관리 취 약 : 10
                계정 관리 검사 불가 : 0
                계정 관리 총 합 : 15

*************** 파일 및 디렉터리 관리 ***************
                파일 및 디렉터리 관리 양 호 : 12
                파일 및 디렉터리 관리 취 약 : 5
                파일 및 디렉터리 관리 검사 불가 : 2
                파일 및 디렉터리 관리 자체 검사(U-60) : 1
                파일 및 디렉터리 관리 총 합 : 20

*************** 서비스 관리 ***************
                서비스 관리 양 호 : 28
                서비스 관리 취 약 : 6
                서비스 관리 검사 불가 : 1
                서비스 관리 총 합 : 35

*************** 패치 및 로그 관리 ***************
                패치 및 로그 관리 양 호 : 1
                패치 및 로그 관리 취 약 : 1
                패치 및 로그 관리 검사 불가 : 0
                패치 및 로그 관리 자체 검사(U-43) : 1
                패치 및 로그 관리 총 합 : 3

총 합 : 73
전체 양 호 : 46
전체 취 약 : 22
자체 검 사 : 2
전체 검사 불가 : 3

메뉴로 돌아가시겠습니까? (y):
```

03. 개발내용 (script)

계정 관리 U-03

```
< U-03 계정 잠금 임계값  설정 >

상태 : 취약
계정 잠금 임계값이 설정되어 있지 않거나, 5 이하의 값으로 설정되어 있지 않습니다.

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

```
#!/bin/bash

echo ""
echo "< U-03 계정 잠금 임계값  설정 >"
echo ""

if [ -f "/etc/pam.d/system-auth" ];
then
        grep pam_tally.so /etc/pam.d/system-auth > /dev/null
        if [ $? -eq 0 ];
        then
                echo -e "상태 : \e[1;36m양호\e[0m"
                echo "계정관리,U-03,계정 잠금 임계값 설정,Safety,$userid,$serverip,$DATE,1 " >> /jb/result.txt
                AccountSafety=`expr $AccountSafety + 1`

        else
                echo -e "상태 : \e[1;31m취약\e[0m"
                echo "계정 잠금 임계값이 설정되어 있지 않거나, 5 이하의 값으로 설정되어 있지 않습니다."
                echo "계정관리,U-03,계정 잠금 임계값 설정,Risk,$userid,$serverip,$DATE,0,계정 잠금 임계값을 5이하로 설정하세요." >> /jb/result.txt
                AccountRisk=`expr $AccountRisk + 1`
        fi
else
        echo -e "상태 : \e[1;33m검사 불가\e[0m"
        echo "/etc/pam.d/system-auth 파일이 존재하지 않습니다."
        echo "계정관리,U-03,계정 잠금 임계값 설정,Risk,$userid,$serverip,$DATE,0,파일이 없습니다." >> /jb/result.txt
        AccountError=`expr $AccountError + 1`
fi
echo""
echo ================================================================================
```

03. 개발내용 (script)

계정 관리 U-46

```
< U-46 패스워드 최소 길이 설정 >

상태 : 취약
패스워드 최소 길이가 8자 미만으로 설정되어 있습니다.

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

```
#!/bin/bash

echo ""
echo "< U-60 숨겨진 파일 및 디렉터리 검색 및 제거>"
echo ""


#c_time=`ls -l --time-style full-iso /root/anaconda-ks.cfg | awk '{print $6}'`
#find /home -type f -name ".*" -newermt '2020-12-21'

#find /home -name ".*" -type f -newer /root/anaconda-ks.cfg

scan_dir=("/boot" "/usr" "/bin" "/sbin" "/etc/" "/tmp" "/home" "/var")

for i in ${scan_dir[@]}
do
        echo ------$i 숨김파일들--------- >> /jb/tmp.txt
        find $i -name ".*" -type f -newer /root/anaconda-ks.cfg >> /jb/tmp.txt
        echo "" >> /jb/tmp.txt
done


echo "상태 : N/A"
echo ""
cat /jb/tmp.txt
echo "파일 및 디렉터리 관리,U-60,숨겨진 파일 및 디렉터리 검색 및 제거,N/A,$userid,$serverip,$DATE,1" >> /jb/result.txt

echo ""
echo ================================================================================
rm -rf /jb/tmp.txt
```

03. 개발내용 (script)

서비스 관리 U-32

```
< U-32 일반사용자의 Sendmail 실행 방지 >

상태 : 양호

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

```
#!/bin/bash
echo ""
echo "< U-32 일반사용자의 Sendmail 실행 방지 >"
echo ""

ps -ef | grep sendmail | grep -v grep > /jb/ee.txt

if [ -s "/jb/ee.txt" ]; then
        grep -v '^ *#' /etc/mail/sendmail.cf | grep PrivacyOptions | grep restrictqrun  > /jb/ff.txt
        if [ -s "/jb/ff.txt" ]; then
                echo -e "상태 : \e[1;36m양호\e[0m"
                echo "서비스관리,U-32,일반사용자의 Sendmail 실행 방지,Safety,$userid,$serverip,$DATE,1" >> /jb/result.txt
                ServiceSafety=`expr $ServiceSafety + 1`

        else
                echo -e "상태 : \e[1;31m취약\e[0m"
                echo "SMTP서비스를 사용하는데 일반사용자의 Sendmail 실행 방지가 설정되어 있지 않습니다."
                echo "서비스관리,U-32,일반사용자의 Sendmail 실행 방지,Risk,$userid,$serverip,$DATE,0,/etc/mail/sendmail.cf파일에서 restrictqrun옵션을 추가하세요." >> /jb/result.txt
                ServiceRisk=`expr $ServiceRisk + 1`

        fi
else
        echo -e "상태 : \e[1;36m양호\e[0m"
        echo "서비스관리,U-31,스팸 메일 릴레이 제한,Safety,$userid,$serverip,$DATE,1" >> /jb/result.txt
        ServiceSafety=`expr $ServiceSafety + 1`

fi

echo ""
echo ================================================================================

rm -rf /jb/ee.txt
rm -rf /jb/ff.txt
```

03. 개발내용 (script)

파일 및 디렉터리 관리 U-60

```
#!/bin/bash

echo ""
echo "< U-60 숨겨진 파일 및 디렉터리 검색 및 제거>"
echo ""


#c_time=`ls -l --time-style full-iso /root/anaconda-k
#find /home -type f -name ".*" -newermt '2020-12-21'

#find /home -name ".*" -type f -newer /root/anaconda-

scan_dir=("/boot" "/usr" "/bin" "/sbin" "/etc/" "/tmp

for i in ${scan_dir[@]}
do
        echo ------$i 숨김파일들--------- >> /jb/tmp.
        find $i -name ".*" -type f -newer /root/anaco
        echo "" >> /jb/tmp.txt
done


echo "상태 : N/A"
echo ""
cat /jb/tmp.txt
echo "파일 및 디렉터리 관리,U-60,숨겨진 파일 및 디렉터

echo ""
echo ==========
rm -rf /jb/tmp.txt
```

```
< U-60 숨겨진 파일 및 디렉터리 검색 및 제거>

상태 : N/A

------/boot 숨김파일들----------

------/usr 숨김파일들----------
/usr/lib64/firefox/fonts/.uuid

------/bin 숨김파일들----------

------/sbin 숨김파일들----------

------/etc/ 숨김파일들----------

------/tmp 숨김파일들----------
/tmp/.X0-lock
/tmp/.X1024-lock

------/home 숨김파일들----------
/home/hdfs/.esd_auth
/home/hdfs/.bash_history
/home/hdfs/.vim/.netrwhist
/home/hdfs/.viminfo
/home/yarn/.esd_auth
/home/yarn/.bash_history

------/var 숨김파일들----------
/var/lib/sss/secrets/.secrets.mkey
/var/lib/gdm/.ICEauthority


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

03. 개발내용 (telegram)

```
#Telegram Bot API token
botToken = '[redacted]'

#Bot
botP

#Def
sshU
sshP
sshH
sshH

#Roo
root

#Log
logging = True
logFile = '/joongbu_script/telegram/t
```

```
@bot.message_handler(func=lambda message: True, commands=['on'])
def activate_user(message):
    if knownUsers.get(message.chat.id) == None:
        newUser = User(message.chat.id)
        newUser.userName = ''
```


```
        knownUsers.get(message.chat.id).userName = message.chat.first_name

        bot.send_message(message.chat.id, "접속을 환영합니다!")
    else:
        password = bot.send_message(message.chat.id, "패스워드가 틀렸습니다. 다시 입력해주세요 :")
```

03. 개발내용 (telegram)

```
@bot.message_handler(func=lambda message: \
                     knownUsers.get(message.chat.id).userStep == 2, commands=['clientid'])
def request_client_id(message):
    knownUsers.get(message.chat.id).userStep = 1
    clientid = bot.send_message(message.chat.id, "점검을 신청한 회원 id 입력 :")
    bo

def ac
    f
    kn
    kn
    so                                                                    tf8')
    cu
    cu
    re

    if

    el
        bot.send_message(message.chat.id, "아이디가 존재합니다.")
        re = ''.join(filter(str.isalnum, result))
        f.write(re)
        f.close()
        bot.send_message(message.chat.id, "/remoteuser")
```

03. 개발내용 (telegram)

03. 개발내용 (telegram)

```
@bot.message_handler(func=lambda message: \
                     knownUsers.get(message.chat.id).userStep == 2, commands=['remotehost'])
def request_ssh_host(message):
    kn
    se
    bo

def ad
    f =
    kn
    kn
    f.write('\n')
    f.write(knownUsers.get(message.chat.id).remoteHost)
    f.close()
    bot.send_message(message.chat.id, "/sendfile")
```

03. 개발내용 (telegram)

03. 개발내용 (telegram)

03. 개발내용 (Windows)

계정 관리 W-5

```
@ECHO OFF
ECHO.
ECHO ^< W-5 해독 가능한 암호화를 사용하여 암호 저장 기준 ^>
ECHO.

secedit /export /cfg C:₩jb₩LocalSecurityPolicy.txt | find /v "작업을" | find /v "자세한"

TYPE C:₩jb₩LocalSecurityPolicy.txt | find /i "ClearTextPassword" | find "0" > NUL

if not errorlevel 1 echo "결과 : 양호"
if not errorlevel 1 echo "계정 관리,W-05,해독 가능한 암호화를 사용하여 암호 저장기준,Safety,%userid%,%serverip%,%date%,1" >> C:₩Users₩%name%₩jb₩result.txt
if not errorlevel 1 set /a AccountSafety=%AccountSafety%+1

if errorlevel 1 echo "결과 : 취약"&echo,"해독 가능한 암호화를 사용하여 암호 저장 정책이 사용으로 되어 있습니다."
if errorlevel 1 echo "계정 관리,W-05,해독 가능한 암호화를 사용하여 암호 저장기준,Risk,%userid%,%serverip%,%date%,0,해독 가능한 암호화를 사용하여 암호 저장 정책을 사용 안 함으로 설정하세요." >> C:₩Users₩%name%₩jb₩result.txt
if errorlevel 1 set /a AccountRisk=%AccountRisk%+1

ECHO.
ECHO.==========================================================================
```

```
< W-5 해독 가능한 암호화를 사용하여 암호 저장 기준 >


"결과 : 양호"
지정된 경로를 찾을 수 없습니다.

==========================================================================
계속하려면 아무 키나 누르십시오 . . .
```

03. 개발내용 (Windows)

서비스 관리 W-15

```
@ECHO OFF

ECHO.
ECHO ^< W-17 IIS 파일 업로드 및 다운로드 제한 ^>
ECHO.

dir | find "web.config" || dir | find "applicationHost.config" > C:₩w17.txt
IF %errorlevel% EQU 0 (echo "상태 : 양호"
        echo "서비스 관리,W-17,IIS 파일 업로드 및 다운로드 제한,Safety,%userid%,%serverip%,%date%,1" >> C:₩Users₩%name%₩jb₩result.txt
        set /a ServiceSafety=%ServiceSafety%+1
) ELSE (echo "상태 : 취약"&echo."웹 프로세스의 서버 자원 관리가 되어있지 않습니다."
echo "서비스 관리,W-17,IIS 파일 업로드 및 다운로드 제한,Risk,%userid%,%serverip%,%date%,0,웹 프로세스의 서버 자원 관리를 설정하세요." >> C:₩Users₩%name%₩jb₩result.txt
set /a ServiceRisk=%ServiceRisk%+1
)

del C:₩w17.txt
ECHO.
ECHO.==========================================================================
```

```
< W-17 IIS 파일 업로드 및 다운로드 제한 >

"상태 : 취약"
"웹 프로세스의 서버 자원 관리가 되어있지 않습니다."
지정된 경로를 찾을 수 없습니다.

==========================================================================
계속하려면 아무 키나 누르십시오 . . .
```

03. 개발내용 (Windows)

계정 관리 W-49

```
@ECHO OFF
ECHO.
ECHO ^< W-49 패스워드 최소 암호 길이 ^>
ECHO.

secedit /export /cfg C:₩LocalSecurityPolicy.txt

TYPE C:₩LocalSecurityPolicy.txt | find /i "MinimumPasswordLength = " > C:₩passwd.txt

FOR /f "tokens=3" %%a IN (C:₩passwd.txt) DO SET pass_length=%%a

IF %pass_length% GEQ 8 ECHO "상태 : 양호"
IF %pass_length% GEQ 8 ECHO "계정 관리,W-49, 패스워드 최소 암호 길이,Safety,%userid%,%serverip%,%date%,1" >> C:₩Users₩%name%₩jb₩result.txt
IF %pass_length% GEQ 8 set /a AccountSafety=%AccountSafety%+1

IF NOT %pass_length% GEQ 8 ECHO "상태 : 취약"&ECHO."최소 암호 길이가 설정되지 않았거나 8문자 미만으로 설정되어 있는 경우입니다."
IF NOT %pass_length% GEQ 8 ECHO "계정 관리,W-49,패스워드 최소 암호 길이,Risk,%userid%,%serverip%,%date%,0,최소 암호 길이를 8문자 이상으로 설정해주세요." >> C:₩Users₩%name%₩jb₩result.txt
IF NOT %pass_length% GEQ 8 set /a AccountRisk=%AccountRisk%+1

ECHO.
ECHO.============================================================================

del C:₩LocalSecurityPolicy.txt
DEL C:₩passwd.txt
```

```
< W-49 패스워드 최소 암호 길이 >


작업을 성공적으로 완료했습니다.
자세한 정보는 %windir%₩security₩logs₩scesrv.log를 참조하십시오.
"상태 : 취약"
"최소 암호 길이가 설정되지 않았거나 8문자 미만으로 설정되어 있는 경우입니다."
지정된 경로를 찾을 수 없습니다.

============================================================================
계속하려면 아무 키나 누르십시오 . . .
```

03. 개발내용 (Windows)

보안 관리 W-76

```
@ECHO OFF
ECHO.
ECHO ^< W-76 사용자별 홈 디렉토리 권한 설정 ^>
ECHO.


dir %systemroot%₩..₩Users | find /v "." | find /v "Public" | find "<DIR>" > c:₩user.txt
TYPE c:₩user.txt | find /i "Everyone" > nul

IF %ERRORLEVEL%==0 (
        ECHO "결과 : 취약"
        ECHO "홈 디렉토리에 Everyone 권한이 있습니다."
        ECHO "보안 관리,W-76,사용자별 홈 디렉토리 권한 설정,Risk,%userid%,%serverip%,%date%,0,홈 디렉토리에 Everyone 권한이 있습니다." >> c:₩Users₩%name%₩jb₩result.txt
        set /a SecurityRisk=%SecurityRisk%+1
) ELSE (
        ECHO "결과 : 양호"
        ECHO "보안 관리,W-76,사용자별 홈 디렉토리 권한 설정,Safety,%userid%,%serverip%,%date%,1" >> c:₩Users₩%name%₩jb₩result.txt
        set /a SecuritySafety=%SecuritySafety%+1
)


ECHO.
ECHO.============================================================


DEL c:₩user.txt
```

```
< W-76 사용자별 홈 디렉토리 권한 설정 >

"결과 : 양호"
지정된 경로를 찾을 수 없습니다.

================================================================================
계속하려면 아무 키나 누르십시오 . . .
```

04. 결론 및 기대효과

결론

- 리눅스 서버 진단 쉘 스크립트 작성
- 윈도우 서버 진단 배치파일 작성
  -> 스크립트를 이용한 빠른진단 및 서버의 취약한 부분 확인 가능

기대효과

- 취약점 진단 도구를 이용해 빠르게 보안 상태를 점검가능
- 스마트폰으로 빠른 진단 가능

Thank you