**SetUID를 이용한 local Backdoor 생성과 탐지**

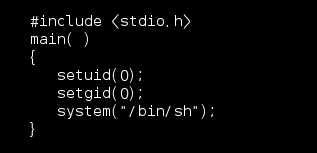
\* 로컬 백도어 : 일반 계정으로 로그인하여 특정 프로그램을 실행시켜 관리자 권한 탈취

**1. Backdoor 생성**

**1) Backdoor 생성.**

단계 1. Backdoor 파일 생성

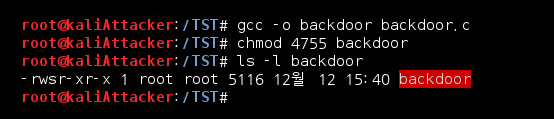
#vi backdoor.c

****

단계 2. 컴파일 후 SetUID 권한 설정

#gcc –o backdoor backdoor.c //컴파일

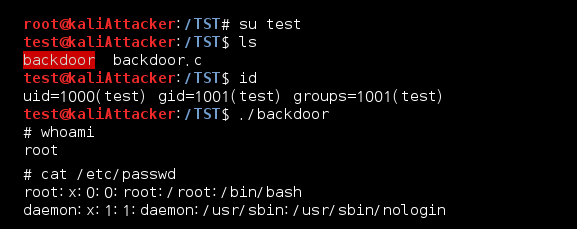
#chmod 4755 backdoor //SetUID 권한 설정

****

단계 3. 백도어를 이용하여 root 권한 탈취

#su test

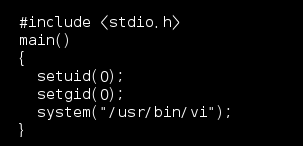
#./backdoor

****

**2) Backdoor 생성**

단계 1. Backdoor 파일 생성

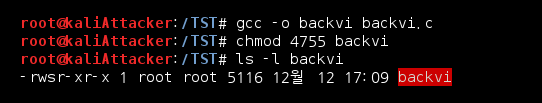
#vi backvi.c

****

단계 2. 컴파일 후 SetUID 권한 설정

#gcc –o backvi backvi.c //컴파일

#chmod 4755 backvi //SetUID 권한 설정

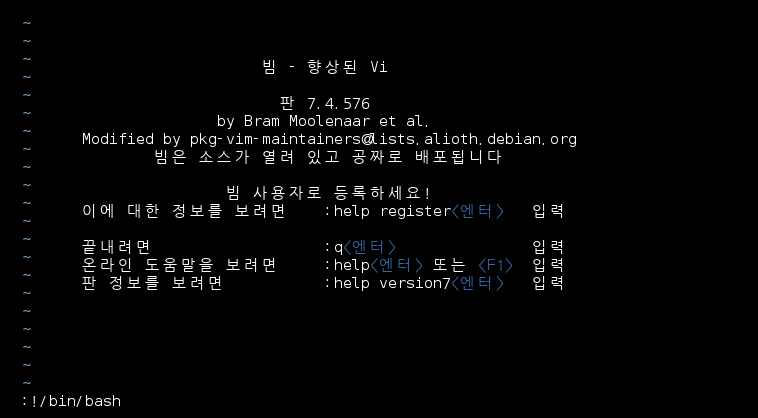
****

단계 3. 백도어를 이용하여 root 권한 탈취

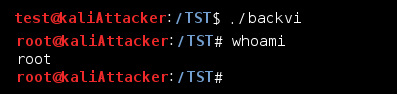
#su test

#./backvi

**:!/bin/bash**



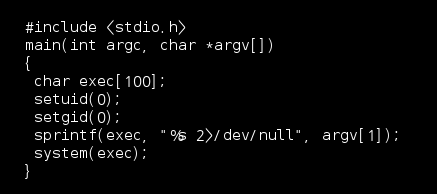
단계 4. root 권한 탈취

****

**3) Backdoor 생성**

단계 1. Backdoor 파일 생성

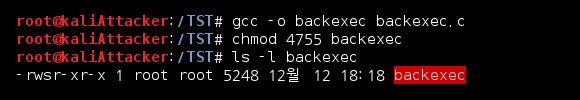
#vi backexec.c

****

단계 2. 컴파일 후 SetUID 권한 설정

#gcc –o backexec backexec.c //컴파일

#chmod 4755 backexec //SetUID 권한 설정

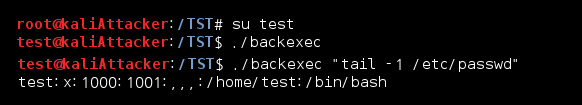
****

단계 3. 백도어를 이용하여 root 권한 탈취

#su test

#./backexec

#./backexec “tail –l /etc/passwd” // 실행 명령어 뒤에 큰 따옴표 안에 명령어를 입력



단계 4. root 권한 탈취 확인

****

**2. Backdoor 숨기기**

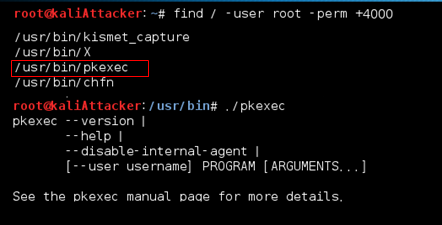
* 백도어가 마치 시스템 상의 중요한 setuid 파일인 것처럼 위장

단계 1. 위장할 파일 조회하기

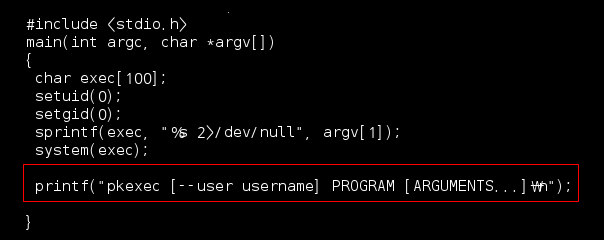
#find / -user root –perm +4000

#cd /usr/bin

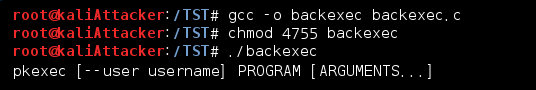
#./pkexec

****

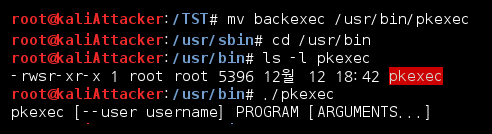
단계 2. 백도어 파일 내용 수정



단계 3. 컴파일 후 권한 재설정



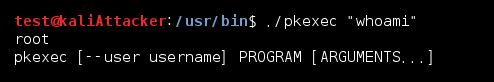
단계 4. 파일 pkexec에 파일 backexec를 덮어 씌움 후 파일 실행



단계 5. Backdoor 실행하기

$ cd /usr/bin

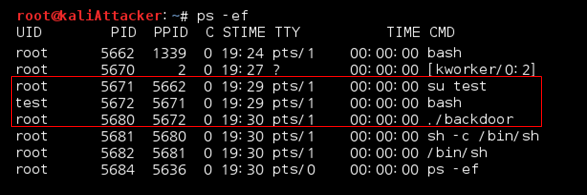
$./pkexec “whoami”



**3. Backdoor 탐지 방법**

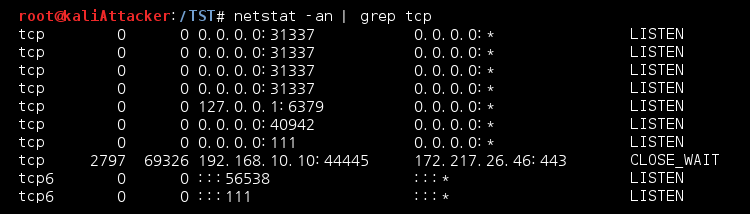
**∙현재 동작중인 프로세스 및 열린 포트 확인**

#ps –ef

****

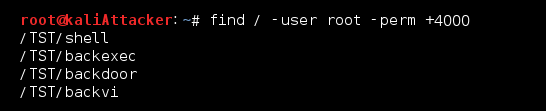
**∙** **열려 있는 포트 확인**

#netstat –an | grep tcp



**∙** **SetUID 파일 검색**

#find / -user root –perm +4000 //backdoor 찾기

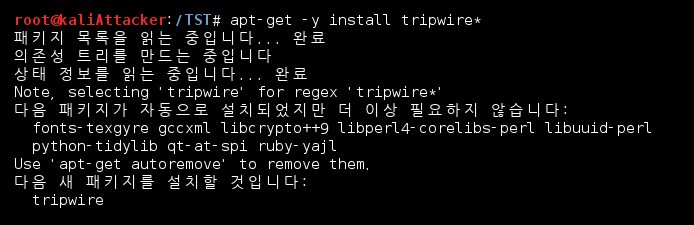
****

#find / -user root –perm +4000 –exec rm {} \; //backdoor 삭제

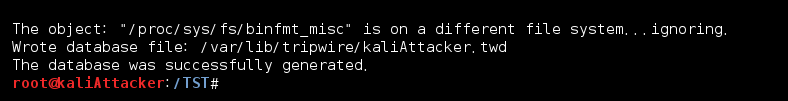
**∙** **무결성 확인**

* 침입자에 의해 변경된 파일 있는지 검사
* Tripwire 툴을 이용한 무결성 검사 가능

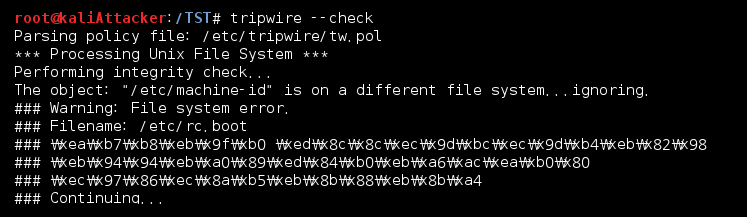
#apt-get –y install tripwire\*

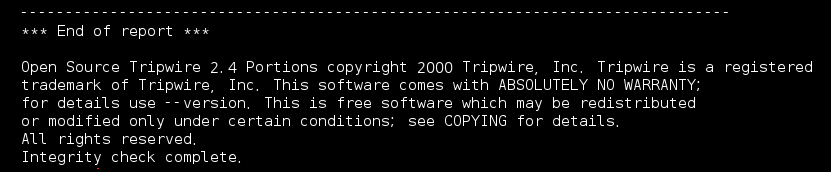


#tripwire --init // 데이터베이스 초기화

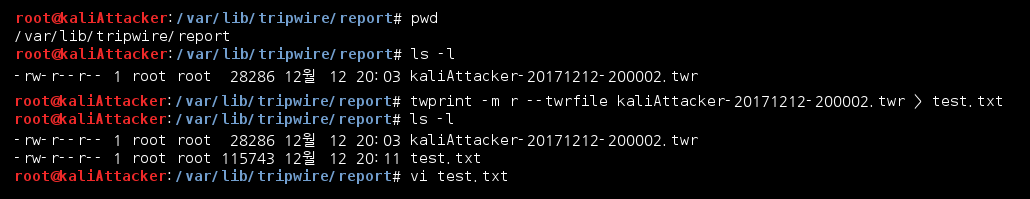


#tripwire --check // 무결성 검사 시작

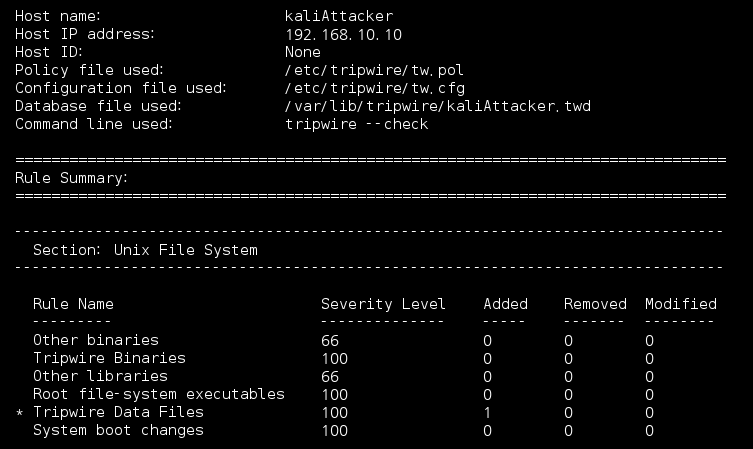




#cd /var/lib/tripwire/report // 무결성 검사 결과 파일 확인

#twprint –m r –twrfile 레포트이름 > test.txt // 레포트를 텍스트 파일로 저장 

#vi test.txt // 검사파일 확인



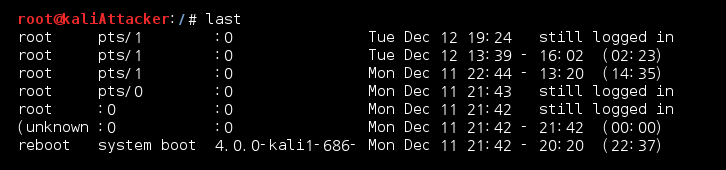
**∙** **로그 분석**

* 침입자의 기록을 분석

wtmp

➀ 로그인, 로그아웃 히스토리를 모두 저장하며 shutdown, booting기록까지 저장

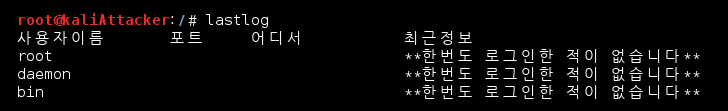
➁ 명령어 : last



lastlog

➀ 최근 사용자의 이름, 터미널, 마지막 로그인 시간으로 출력

➁ 명령어 : lastlog



**∙** **백신 프로그램의 탐지 방법**

* 백신은 파일의 기계어 로그를 분석하여 특정한 동작을 하는 코드가 있으면

악성 코드로 인식

* 알려진 악성코드는 탐지 할 수 있지만 변종들은 탐지 못함