(2) shadow 파일

(가) 개념

① /etc/shadow 파일에 각 사용자 계정에 대한 패스워드가 암호화 되어 있다.

(나) /etc/shadow 파일 예

```
testuser : $1$E2loH9Yc$01Cc52Zml6mcrOhF : 12818 : 0 : 99999 : 5 : 7 : 0 : 12842
   ①                    ②                    ③    ④     ⑤    ⑥  ⑦   ⑧    ⑨
```

표 228 /etc/shadow 파일 예

① 사용자 계정 : login ID (etc/passwd 파일과 사용자 정보를 서로 연계한다.)
② 암호(패스워드) : 실제 비밀번호가 암호화되어 저장된다.
- $1: 적용된 일방향 해시 알고리즘(1: MD5, 5: SHA-256, 6: SHA-512 등)
- $E2loH9Yc: salt값 즉 패스워드 암호화 강도를 높이기 위한 값으로 공격자의 사전공격에 대응하기 위해 랜덤한 값으로 생성한다.
- $01Cc52ZhmlgLAtwxUen7tTY...(중략): 사용자가 지정한 패스워드에 salt 값을 추가해서 암호화된 패스워드(해시값)값.

③ LAST DAY(**12818**) : 암호가 마지막으로 변경된 날짜를 지정, (1970년 1월 1일을 기준으로 며칠이 지났는지 그 일 수로 표기한다.)

(다) vi 또는 more로 열어본 /etc/shadow 파일

```
# more /etc/shadow
root:$h$M2FIW$/nrp4rc:11485::::::
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:*:6445::::::
jslim:NP:6445::::::
hskim: :11611::::::
```

그림 26 more로 열어본 /etc/shadow 파일

① /etc/shadow 의 패스워드 필드는 암호화된 패스워드로 기록되며 패스워드가 없는 경우 빈 필드로 남는다.
② shadow 파일에서 hskim 사용자는 암호화 부분이 빈칸으로 되어 있으므로 비밀번호 없이 시스템에 로그인이 가능하다.
③ NP(no password)는 패스워드가 없는 어카운트(계정)를 의미한다.
④ " !! " : 비밀번호가 설정되어 있지 않음
⑤ " *, ! " : 계정 잠금 - 사용되는 계정의 패스워드가 무효화되어 로그인 불가능

setUID/setGID p.574

2019년 14회

179. 아래의 명령어 수행 후 test.out 의 속성에 관한 설명으로 옳은 것은?

```
chmod 4755 test.out
```

① 파일 실행시 읽기 실행 가능
② 파일 실행시 staff권한으로 실행되어 읽기 / 실행 가능
③ 실행하는 사용자 권한에 상관 없이 test.out은 user권한으로 실행
④ 실행하는 사용자 권한에 상관 없이 test.out은 staff권한으로 실행

정답	3

SetUID(4)비트가 설정되어 있다.

2018년 12회

180. 다음 지문의 설명에서 옳지 않은 것은?

① 접근 권한이 rwxr-xr-x인 경우 고유한 숫자로 표기하면 755가 된다.
② UNIX시스템에서 SetUID 비트는 2이다.
③ 디렉토리의 권한은 파일 소유자 권한, 그룹 권한, 일반(Others) 권한으로 구분된다.
④ 유닉스/리눅스 시스템에서는 사용자 계정 목록을 /etc/passwd 파일에 저장하고 있다.

정답	2

UNIX시스템에서 SetUID 비트는 4이다. (4000)

2015년 05회

181. 다음의 리눅스 파일 시스템에서 SetUID, SetGID, Sticky bit 설명으로 옳은 것은?

① 파일에 SetUID가 걸려 있어도 겉으로는 알 수 없다.
② 파일에 대한 접근 권한이 7777'이면 문자로는 'rwsrwgrwt'로 표시된다.
③ SetUID 비트가 세트된 파일을 실행하면 파일 소유자 권한으로 수행된다.
④ SetUID 비트가 세트되어 있어도 루트 권한으로 실행되는 경우는 없다.

정답	3

- SetUID는 유닉스 시스템에서 타인의 권한으로 작업하는 것을 허용하는 메커니즘이다.
- SetGID 비트가 파일에 설정되어 있으면 새로 설정된 파일은 사용자가 속한 그룹의 권한이 아닌 소유주의 그룹권한을 갖게 된다.

2013년 02회

182. 패스워드 관리에 대한 설명으로 올바르지 않은 것은?

① /etc/passwd 퍼미션은 600으로 변경하는 것이 좋다.

② 일반 권한보다 특수 권한인 setuid, setgid를 최대한 활용해주어야 한다.

③ 암호화된 패스워드는 /etc/shadow 파일에 저장이 된다.

④ 패스워드 없이 로그인할 수 있는 계정이 있는지 살펴본다.

정답	2

1. 권한상승(SetUID, SetGID)

1) SetUID

- SetUID란 파일이 실행되는 동안 해당 파일 소유자의 권한을 획득하는 것을 말한다.
- 즉 SetUID 비트를 실행 파일에 적용하면 실 사용자(프로그램을 실제 실행 중인 사용자)에서 프로그램 소유자의 ID로 유효사용자가 변경된다.
- UNIX, 리눅스 시스템에서 관리자(root) 권한이 필요 없는 프로그램에 소유자가 관리자로 되어 있으면서 SetUID가 설정된 경우에는 시스템의 보안에 허점을 초래할 수 있다. 실제로 이것이 설정 된 파일은 백도어 및 버퍼 오버플로우 등 여러 공격에 이용된다.
- SetUID 비트는 4이다. (4000)

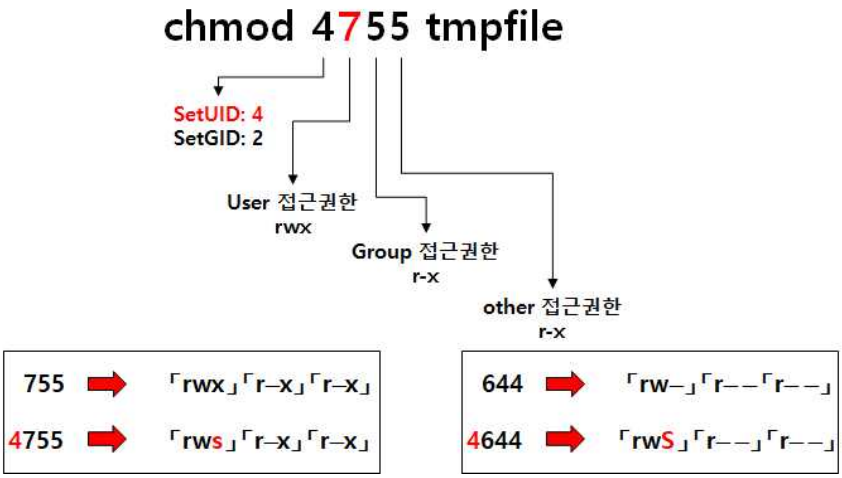

그림 27 SetUID 비트설정

2. SetUID 비트가 설정된 파일의 위험성

- UNIX시스템에서 SetUID를 적용하는 것이 시스템 운영 면에서 효율적이라 적용되었다.
- 예를 들어 유닉스에서 일반 유저가 자신의 패스워드를 변경할 때 SetUID를 활용하면 손쉽게 변경할 수 있다.
- 즉 SetUID가 설정된 파일을 실행 되는 동안에 잠깐 관리자 권한을 빌려오고, 작업을 마친후엔 다시 권한을 돌려주는 것이다.

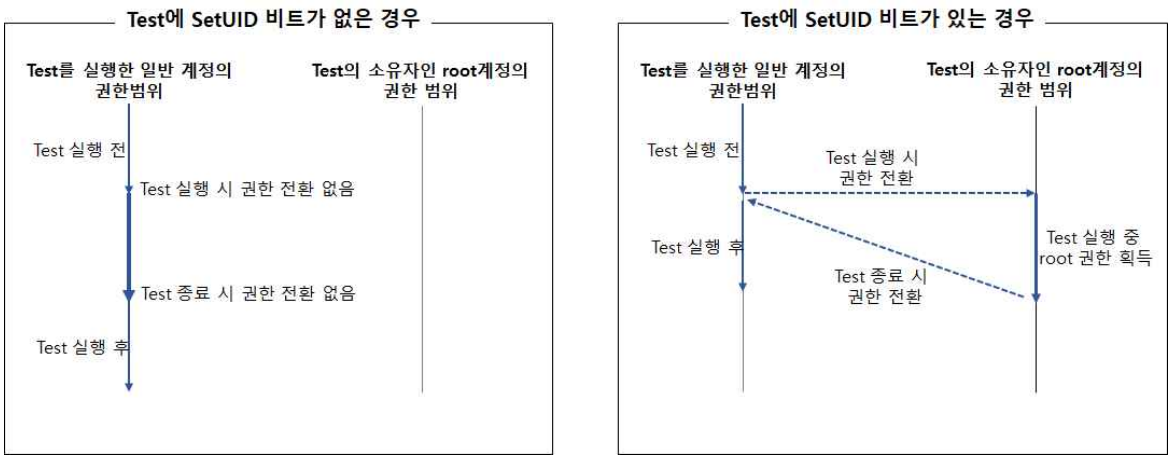

그림 28 SetUID 미 설정 시 프로세스 권한과 SetUID 설정 시 프로세스 권한 변경

2018년 11회

183. SetUID와 SetGID가 설정된 모든 파일을 찾으려는 명령어가 바르게 기술된 것은?

① find / -type f ₩(-perm -1000 -0 perm -2000 ₩) -print

② find / -type f ₩(-perm -2000 -0 perm -4000 ₩) -print

③ find / -type f ₩(-perm -100 -0 perm -200 ₩) -print

④ find / -type f ₩(-perm -200 -0 perm -400 ₩) -print

정답	2

2017년 10회

184. 크래커들이 자주 사용하는 방법 중에는 한번 들어온 서버에 다시 쉽게 침입할 수 있도록 suid가 설정된 root 소유의 프로그램을 백도어로 설치하여 다음에는 손쉽게 root 권한을 획득 할 수 있도록 하는 방법이 있다. 아래의 명령어를 사용하여 시스템관리자는 주기적으로 suid로 설정된 파일을 모니터링 하여 시스템을 안전하게 보호할 필요가 있다. 괄호 ( ) 안에 들어갈 옵션을 순서대로 바르게 나타낸 것은 어느 것인가?

#find / -( ) root -( ) 4000 -( ) ls -l { } ,

① user, exec, perm ② exec, user, perm

③ perm, user, exec ④ user, perm, exec

정답	4

#find / - user root - exec 4000 - perm ls -l { }

2016년 08회

185. 다음은 크래커 A가 남긴 C소스 코드와 바이너리 파일이다. 이에 대한 설명으로 적합한 것은?

```
$ls -l
total 20
-rwsr-wr-x 1 root root 1435 Oct 7 21:13 test
-rw-rw-r-- 1 root root 88 Oct 7 21:12 test.c

$ cat test.c
#include
void main() {
   setuid(0);
   setgid(0);
   system("/bin/bash");
}
```

① setgid 시스템 콜의 인자를 0으로 준 것으로 보아 Race Condition 기법의 공격이다.
② /bin/sh를 실행시키는 거승로 보아 Sniffing 기법이다.
③ setuid 시스템 콜의 인자가 0이고 컴파일된 바이너리 파일의 퍼미션이 4755인 것으로 보아 루트 권한을 탈취하는 백도어이다.
④ main 함수의 리턴형태가 void 이므로 Format String Attack으로 보인다.

정답	3

가) 백도어(Backdoor) = 트랩도어(Trapdoor)

(1) 개념

① **백도어는 프로그램이나 손상된 시스템에 허가되지 않는 접근을 할 수 있도록 정상적인 보안 절차를 우회하는 악성 소프트웨어이다.**
② 로그인과 같은 정상적인 사용자 인증 과정을 거치지 않고 프로그램에 접근하는 일종의 통로이다.
③ 정보의 갈취 뿐 아니라, 시스템을 조작할 수도 있다.

(2) 특징

① **백도어 종류도 트로이목마의 일종이다.**
② **유틸리티 프로그램 내에 악의적인 코드를 내장하거나, 그 자체를 유틸리티 프로그램으로 위장한다.**
③ **특정 환경/조건이나 배포자의 의도에 따라 사용자의 정보 유출 또는 자료 파괴 같은 피해를 입힌다.**

(3) 백도어와 트로이목마와의 차이점

① 백도어는 Administrative hook이나 트랩 도어(Trapdoor)라고도 부르며, 이러한 경우는 개발자의 장난이나 악의에 의해 만들어진 것도 있지만 특별히 해킹을 위한 것은 아니다.

(4) 백도어(BackDoor) 공격 종류 (트로이 목마 S/W와 유사)

① 넷버스(Netbus)
② 백오리피스(Back Orifice)
③ 루트킷(RootKit)

(5) 백도어 탐지 방법

(가) 현재 동작 중인 프로세스 확인

① 현재 동작 중인 프로세스를 확인해 정상 프로세스가 아닌 프로세스를 확인한다.
② 웜/바이러스나 **백도어가 가장 애용하는 것은 csrss와 svchost 프로세스**이다.
③ csrss.exe(Client Server Runtime Subsystem: 클라이언트 서버 런타임 하위 시스템)는 윈도우 콘솔을 관장하고, 스레드를 생성·삭제하며 32비트 가상 MS-DOS 모드를 지원한다.

그림 29 cpu점유율을 99%잡아먹은 csrss.exe

④ svchost.exe(Service Host Process) : DLL(Dynamic Link Libraries)에 의해 실행되는 프로세스의 기본 프로세스이다. 따라서 한 시스템에서 여러 개의 svchost 프로세스를 볼 수 있다.
⑤ 따라서 svchost.exe가 여러 개라 해서 무조건 바이러스라고 볼 수 없다. 백신 프로그램으로 바이러스여부를 확인해야 한다.

umask p.579

나) 파일접근권한(umask)

(1) 개념

① umask는 기존 **디렉터리나 파일의 제거할 접근 권한을 명시**할 때 사용하는 쉘 내부 명령어이다.

② 시스템 관리자는 umask를 설정하여 전체 사용자에게 획일적인 umask 값을 적용할 수 있다.

③ rwx를 숫자로 표시하면 r : 4, w : 2, x : 1 이다.

(3) umask 연산

(가) default permission

① 리눅스에서 폴더를 처음 생성하면 기본적으로 777의 권한이 설정되어 있고, **파일을 처음 생성하면 666(rw-rw-rw-)의 권한**이 설정되어 있다.

② 디렉터리의 경우 기본 접근권한으로 777(rwxrwxrwx)이 설정되어 있다.ㅋ

```
파      일: 666 (rw-rw-rw-)
디렉터리: 777 (rwxrwxrwx)
```

(나) umask로 제거할 권한 명시

① umask 명령어를 통해 현재 설정된 권한을 제거할 수 있다.

② umask 022

```
[root@localhost ex1]# umask 022
```

```
파      일: 644 (rw-r--r--)
디렉터리: 755 (rwxr-xr-x)
```

2018년 11회

186. 유닉스 시스템 명령어는?

시스템의 파일 또는 디레터리가 만들어질 때의 허가권의 기본값을 지정하기 위해서 사용한다. 해당 설정은 모든 계정 사용자들에게 존재하는 값으로서 각 계정 사용자들이 생성하는 파일 또는 디렉터리의 허가권을 결정하기 위한 값이다.

① chmod ② umask

③ chown ④ touch

정답	2

2016년 08회

187. 사용자가 자신의 홈 디렉터리 내에서 새롭게 생성되는 서브파일에 디폴트 파일 허가권을 파일 소유자에게는 읽기와 쓰기, 그룹과 other에게는 읽기만 가능하도록 부여하고 싶다. 로그인 셸에 정의해야 하는 umask의 설정갑은 어느 것인가?

① umask 644 ② umask 022

③ umask 330 ④ umask 033

정답	2

666

- 022

644

2018년 12회

188. UNIX에서 업무상/보안상 불필요한 telnet, ftp, ssh 등의 서비스를 제거하려고 한다.이때 시스템 Administrator가 수정하는 파일은 무엇인가?

① /var/adm/sulog

② /etc/passwd

③ /etc/crontab

④ /etc/inetd.conf

정답	4

inetd 데몬은 n개의 개별별서버를 하나로 통합하여 클라이언트로부터 서비스 요청이 올 때마다 해당 서비스와 관련된 실행 모듈(FTP, Telnet, TFTP, SSH 등)을 실행해준다.
inetd.conf 설정 파일을 열어 보면 ftp, telnet 등의 서비스 설정에 대한 내용이 있다.
예를 들어 ftp 서비스를 하지 않으려면 inetd.conf 파일을 열어 ftp 관련 내용 앞에 #을 붙여 주석처리한 후 /etc/inetd restart 로 inetd 데몬을 다시 읽어 설정한 내용을 적용시킨다.

2016년 08회
189. 다음 xinetd에 대한 설정으로 틀린 설명은?

```
#cat telnet
service telnet
{
   disable = no
   flags = REUSE
   socket_type = stream
   wait = no
   user = root
   server = /usr/sbin/in.telnetd
   log_on_failure += USERID
}
```

① 현재 telnet 서비스는 동작 중에 있다.
② wait 값이 no인 것으로 보아 단일 클라이언트만 처리할 수 있다.
③ 소켓 형태는 스트림 기반의 서비스이다.
④ user 옵션을 통해 실행중인 서비스의 소유자인 사용자를 고르는게 가능하다.

정답 2

xinetd는 네트워크에 들어오는 요청을 듣고, 거기에 맞는 적절한 서비스를 실행시킨다.
요청들은 식별자로서 포트 번호를 사용하여 만들어지며, 보통 요청을 다루는 다른 데몬을 실행시킨다.

wait가 yes라면 xinetd는 연결이 된 경우에 서비스를 위한 요청을 받지 않는다.
그래서 연결의 숫자는 하나가 된다.
이것은 우리가 한번에 단지 한 연결만 설정하길 원할 때 유용하다.
wait : no면 여러 클라이언트를 처리할 수 있다.

TCP_WRAPPER p.581
2015년 05회
190. 다음의 보기에서 빈칸에 알맞은 용어는 무엇인가?

( )는 /etc/hosts.deny와 /etc/hosts.allow 파일을 통하여 접근 통제를 구현한다.

① tcp_wrapper ② tripwire
③ SARA ④ NESSUS

정답 1

■ TCP 래퍼(TCP Wrapper)
- 유닉스 계열의 운영체제에서 네트워크 연결에 대한 접근제어 도구이다.
- TCP Wrapper는 네트워크 접근제어 환경설정을 구성하는 프로그램으로, 설정해야 할 설정환경 파일은 /etc/hosts.allow, /etc/hosts.deny 이다.

2014년 03회

191. TCP_WRAPPER 활용시에 로그파일은 일반적으로 ( )과 ( )파일에 기록된다. 괄호안에 순서대로 알맞은 내용은?

① dmessage, secure ② message, secure

③ btmp, message ④ wtmp, secure

정답 2

TCP Wrapper가 기록하는 로그 내용은 운영체제별로 다음 장소에 기록

- aix: /var/admin/messages
- hpux10: /usr/spool/mqueue/syslog
- irix: /var/admin/syslog
- solaris: /var/log/syslog
- linux: /var/log/messages, /var/log/secure

2019년 14회

192. 다음 중 리눅스 시스템의 TCP Wrapper에서 제공하는 기능이 아닌 것은?2

① 로깅

② 포트 접근통제

③ IP기반 접근통제

④ 네트워크 서비스 기반 통제

정답 2

TCP Wrapper는 유닉스/리눅스 계열의 운영체제에서 네트워크 연결에 대한 접근제어 및 방화벽 도구이다.

2014년 03회

193. 다음에서 설명하고 있는 스캔탐지도구는 무엇인가?

포트스캔을 실시간으로 탐지하고 tcp_wrapper와 결합하여 hosts.deny 파일에 자동으로 ip를 등록하여 방어해주는 스캔 탐지형 도구이다.

① SARA ② NESSUS

③ PORTSENTRY ④ NIKTO2

정답 3

PortSentry : 자주들어오는 패킷(공격) 이라고 판단하면 Tcp_Wrapper로 설정해버린다.