

\* 가상머신 리눅스에서 Visual Studio Code를 사용하여 간단한 C 프로그램을 작성합니다.

[1] 가상머신 리눅스에서 VS Code를 설치하고, 실행 화면을 캡처한 내용입니다.

#### VS code 설치

```
(kali㉿kali)-[~]  
$ vscode  
Command 'vscode' not found, but can be installed with:  
sudo apt install code-oss  
Do you want to install it? (N/y)y  
sudo apt install code-oss  
Reading package lists... Done
```

#### VS code 실행

```
(kali㉿kali)-[~]  
$ code-oss &  
[1] 2802
```

[2] rand 함수를 사용하여 무작위로 생성된 0~99사이의 정수(0과 99 포함)를 5번 printf("%d\n"); 하도록 out.c 프로그램을 작성했습니다. 프로그램을 실행하면, 실행 결과가 터미널에 출력됩니다. 소스코드를 수정하지 않고 실행 결과를 data.txt 파일에 저장하게 하려면, > 명령어를 이용해야 합니다.

```
(kali㉿kali)-[~]  
$ vi out.c  
  
(kali㉿kali)-[~]  
$ gcc out.c  
  
(kali㉿kali)-[~]  
$ mv a.out outrun.exe  
  
(kali㉿kali)-[~]  
$ ./outrun.exe > data.txt  
  
(kali㉿kali)-[~]  
$ cat data.txt  
83  
86  
77  
15  
93
```

[3] 다섯 번 `scanf`를 실행하여 `int`형 정수 5개를 읽고 총합을 출력하도록 `in.c` 프로그램을 작성했습니다. 프로그램을 실행하면, 터미널에서 5개의 숫자를 입력해야 합니다. 소스코드를 수정하지 않고, `data.txt` 파일의 내용을 `scanf`의 입력으로 전달하려면, `>` 명령어를 이용해야 합니다.

```
(kali㉿kali)-[~]
$ vi in.c

(kali㉿kali)-[~]
$ gcc in.c

(kali㉿kali)-[~]
$ mv a.out inrun.exe

(kali㉿kali)-[~]
$ ./inrun.exe < data.txt
SUM: 354
```

\* 가상머신 리눅스에서 동일한 네트워크에 연결된 장비를 검색하고, 포트를 스캔합니다.

[1] VBox 가상머신의 네트워크 어댑터를 [어댑터에 브릿지]로 설정합니다. 가상머신에 할당된 IP 주소는 `ifconfig` 실행결과 화면을 통해 확인할 수 있습니다.

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet [redacted] netmask [redacted] broadcast [redacted]
    inet6 [redacted] prefixlen 64 scopeid 0x20<link>
    ether [redacted] txqueuelen 1000 (Ethernet)
    RX packets 67 bytes 6362 (6.2 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 28 bytes 4208 (4.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet [redacted] netmask [redacted]
    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
```

[redacted] 부분에 나와있는 주소가 가상머신에 할당된 IP주소입니다.

[2] 가상머신 IP가 속한 C 클래스 주소 전체를 대상으로 네트워크에 연결된 기기를 탐색하는 명령을 실행하고, 그 결과를 캡처한 화면입니다.

## 명령

```
(kali㉿kali)-[~]  
$ sudo netdiscover -r [redacted]/24  
[sudo] password for kali: [redacted]
```

## 결과

```
Currently scanning: Finished! | Screen View: Unique Hosts  
114 Captured ARP Req/Rep packets, from 3 hosts. Total size: 6840  


| IP         | At MAC Address | Count | Len  | MAC Vendor / Hostname           |
|------------|----------------|-------|------|---------------------------------|
| [redacted] | [redacted]     | 81    | 4860 | TP-Link Corporation Limited     |
| [redacted] | [redacted]     | 31    | 1860 | Intel Corporate                 |
| [redacted] | [redacted]     | 2     | 120  | Arcadyan Technology Corporation |


```

[3] 탐색된 기기 중 한 대를 골라(없으면 가상머신의 IP를 사용), 해당 IP를 대상으로 1-1000번까지 포트 스캐닝을 수행하고, 그 결과를 캡처한 화면입니다.

```
(kali㉿kali)-[~]  
$ nmap -p 1-1000 [redacted]  
Starting Nmap 7.94 ( https://nmap.org ) at 2023-09-25 05:49 EDT  
Nmap scan report for 192.168.0.1  
Host is up (0.024s latency).  
Not shown: 997 closed tcp ports (conn-refused)  
PORT      STATE SERVICE  
53/tcp    open  domain  
80/tcp    open  http  
443/tcp   open  https  
  
Nmap done: 1 IP address (1 host up) scanned in 0.26 seconds
```

\* [2]번에 표시된 [redacted] 부분을 동일하게 [3]에 입력하면 됩니다.

\* 포트 포워딩을 통해 호스트 PC에서 가상머신으로 연결하는 실습입니다.

[1] 가상머신의 네트워크 어댑터를 [NAT]로 설정합니다. 가상머신에서 `ipconfig` 명령으로 IP 주소를 확인하고, 호스트 머신에서 `ifconfig` 또는 `ipconfig` 명령으로 IP 주소를 확인한 결과입니다.

가상머신의 IP 주소는? [redacted]

호스트 머신의 IP 주소는? [blueacted]

```
Connection-specific DNS Suffix . : 
Link-local IPv6 Address . . . . . : 
IPv4 Address. . . . . : 
Subnet Mask . . . . . : 
Default Gateway . . . . . :
```

```
(kali@kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet netmask broadcast
    inet6 prefixlen 64 scopeid 0x20<link>
    ether txqueuelen 1000 (Ethernet)
    RX packets 3 bytes 1770 (1.7 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 23 bytes 3638 (3.5 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet netmask
    inet6 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
```

\* 각 부분에 대한 정보는 각각 같은 색으로 표시된 부분에서 확인할 수 있습니다.

[2] 가상머신에서 ssh 서비스를 실행합니다. \$ systemctl 명령으로 ssh 서비스의 status를 조회하고, 그 결과를 캡처한 화면입니다.

```
(kali@kali)-[~]
$ systemctl start ssh.service

(kali@kali)-[~]
$ systemctl status ssh
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; disabled; preset: disabled)
   Active: active (running) since EDT; 7s ago
     Docs: man
           man
   Process: ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
  Main PID: (sshd)
    Tasks: 1 (limit:)
   Memory: 
      CPU: 
         /system.slice/ssh.service
        2379 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Sep 25 05:53:42 kali systemd[1]: Starting ssh.service - OpenBSD Secure Shell server ..
Sep 25 05:53:42 kali sshd[2379]: Server listening on 0.0.0.0 port 22.
Sep 25 05:53:42 kali sshd[2379]: Server listening on :: port 22.
Sep 25 05:53:42 kali systemd[1]: Started ssh.service - OpenBSD Secure Shell server.
```

[3] 호스트 머신에서 가상머신으로 ssh 접속을 시도하고, 그 결과를 캡처한 화면입니다. 지금은 접속이 되지 않고, timeout 오류가 발생하는 것을 볼 수 있습니다.

```
C:\Users\user> ping [redacted]

Pinging [redacted] with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for [redacted]:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

\* [redacted] 부분은 가상머신의 IP 주소이고, 해당 부분에 같은 내용이 들어가 있음을 확인할 수 있습니다.

[4] VBox에서 포트 포워딩 규칙을 설정합니다. 포트 포워딩 규칙 입력을 위한 윈도우에 규칙을 입력한 후, 캡처한 화면입니다.

이름	프로토콜	호스트 IP	호스트 포트	게스트 IP	게스트 포트
Rule 1	TCP	[redacted]	222	[redacted]	22

\* [redacted] 는 가상머신의 IP주소이고, [redacted] 는 호스트머신의 IP주소입니다.

[5] 호스트 머신에서 가상머신으로 ssh 접속을 시도하고, 그 결과를 캡처한 화면입니다. 이제, 가상 머신으로 ssh 접속이 되는 것을 확인할 수 있습니다.

```
C:\Users\user>ssh kali@[REDACTED] -p 222
The authenticity of host '[REDACTED]:222 ([REDACTED]:222)' can't be established.
[REDACTED] key fingerprint is [REDACTED]
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[REDACTED]:222' to the list of known hosts.
kali@[REDACTED]'s password:
Linux kali 6.3.0-kali1-amd64 #1 SMP PREEMPT_DYNAMIC Debian 6.3.7-1kali1 (2023-06-29) x86_64

The programs included with the Kali GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Kali GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
(kali@kali)-[~]
└─$
```

\* [REDACTED] 는 호스트머신의 IP주소 입니다.