

<https://gleaming.notion.site/Chapter-05-d7223dff200441a2bb0a95c826525db6>

<https://gleaming.notion.site/Chapter-04-IP-5cba3524e69c4537a41494c84855036b>

1. 실습환경 구성 : VMware WorkStation 16 Player
 - Attacker : Kali 가상머신
 - Victim : Windows Server(Ubuntu 22)
 - nmap (Zenmap)목표 : Attacker → Victim 으로 연결 확인 및 분석
2. 네트워크 스캔 도구 설치 및 사용
 - fping, nmap
 - fping 호스트 검색
 - nmap 으로 포트/서비스 스캔(-sS, -sU, -A , -p)
3. 배너 그래빙 실습
 - FTP(21) → telnet 을 이용한 로그인 시도 및 서버 확인
 - SMTP(25) → sendmail 설정 변경 후 배너 확인
 - SSH(22) → telnet 으로 접속하여 OpenSSH 배너확인
 - HTTP(80) → GET / 요청으로 HTML 응답 서버 정보 확인
4. SNMP 정보 수집
 - Windows Server SNMP 서비스 설치
 - Ubuntu 에서 nmap -su -p 161, --script=snmp-* 스크립트 사용

1.fping을 이용해 스캔하기

```
bm@bm-virtual-machine:~/Desktop$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.174.128 netmask 255.255.255.0 broadcast 192.168.174.255
    inet6 fe80::bc0b:dda7:fab1:7cae prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:42:e6:dd txqueuelen 1000 (Ethernet)
    RX packets 5949 bytes 8339913 (8.3 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 1601 bytes 135137 (135.1 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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 219 bytes 22777 (22.7 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 219 bytes 22777 (22.7 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

bm@bm-virtual-machine:~/Desktop$ fping -qasg 192.168.174.0/24
192.168.174.2
192.168.174.128

    254 targets
    2 alive
    252 unreachable
    0 unknown addresses

    1008 timeouts (waiting for response)
    1010 ICMP Echos sent
    2 ICMP Echo Replies received
    1000 other ICMP received

    0.109 ms (min round trip time)
    0.359 ms (avg round trip time)
    0.609 ms (max round trip time)
    10.262 sec (elapsed real time)
```

같은 대역 192.168.174.0/214 의 모든 IP에 대해 Ping을 보냄

실제 응답은 192.168.174.2 , 192.168.174.128 두 대 밖에 없는 것을 확인함

2.nmap을 이용해 스캔

```
bm@bm-virtual-machine:~/Desktop$ sudo nmap -sS 192.168.174.128
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-05 15:44 KST
Nmap scan report for bm-virtual-machine (192.168.174.128)
Host is up (0.0000040s latency).
All 1000 scanned ports on bm-virtual-machine (192.168.174.128) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.12 seconds
bm@bm-virtual-machine:~/Desktop$ sudo nmap -sF -p 80, 139 192.168.174.128
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-05 15:45 KST
Nmap scan report for bm-virtual-machine (192.168.174.128)
Host is up (0.000092s latency).

PORT      STATE SERVICE
80/tcp    closed http

Nmap done: 2 IP addresses (1 host up) scanned in 3.12 seconds
bm@bm-virtual-machine:~/Desktop$ sudo nmap -f -sS 192.168.174.128
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-05 15:45 KST
Nmap scan report for bm-virtual-machine (192.168.174.128)
Host is up (0.0000080s latency).
All 1000 scanned ports on bm-virtual-machine (192.168.174.128) are closed

Nmap done: 1 IP address (1 host up) scanned in 0.11 seconds
bm@bm-virtual-machine:~/Desktop$
```

-sS : SYN 스캔, 가장 일반적인 포트 스캔 방식 TCP 3-way 방식을 완전히 수행하지 않아 비교적 은밀하고 빠름

결과 : 모든 TCP 포트가 닫혀 있음, 연결을 시도했지만 SYN_ACK 응답을 받지 못하고 RST로 응답

-sF : FIN스캔, TCP 연결 없이 FIN플래그를 가진 패킷을 보내 포트 상태 유추, 일반적인 방화벽에 서는 탐지하기 어렵지만, 일부 시스템에서는 비표준으로 취급

결과 : 포트80은 closed상태, 즉 연결 시도가 있었지만 거부당함

-f : 패킷을 프래그먼트로 분할(일부 IDS/방화벽 우회를 위해 사용) -sS " SYN스캔

결과 : 모든 포트 닫혀있음

3. zenmap으로 스캔

Scan Tools Profile Help

Target: 192.168.174.128 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.174.128

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.174.128

| Port | Protocol | State | Service | Version |
|------|----------|-------|---------|---------------------------------------|
| 8000 | tcp | open | http | SimpleHTTPServer 0.6 (Python 3.10.12) |
| 8080 | tcp | open | http | SimpleHTTPServer 0.6 (Python 3.10.12) |
| 8888 | tcp | open | http | SimpleHTTPServer 0.6 (Python 3.10.12) |

Target: 192.168.174.128 Profile: Intense scan

Command: nmap -T4 -A -v 192.168.174.128

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

192.168.174.128

192.168.174.128

Host Status

State: up

Open ports: 3

Filtered ports: 0

Closed ports: 997

Scanned ports: 1000

Up time: 288897

Last boot: Wed Apr 2 08:05:56 2025

Addresses

IPv4: 192.168.174.128

IPv6: Not available

MAC: 00:0C:29:42:E6:DD

Operating System

Name: Linux 4.15 - 5.6

Accuracy: 96%

Ports used

OS Classes

TCP Sequence

IP ID Sequence

TCP TS Sequence

Comments

타겟 IP : 192.168.174.128

처음 zenmap을 실행해 스캔했을 때, 우분투 가상머신에는 열려 있는 포트가 하나도 없었음

기본적으로 우분투 환경에서 웹 서버나 SSH 등 외부 접근이 가능한 서비스가 실행되지 않았을 것으로 추측. 따라서 포트 스캔 결과가 전부 closed로 나왔으며 아무 정보도 표시 되지 않아서 수동으로 포트를 개방하였음.

파이썬이 제공하는 내장 HTTP 서버를 활용해 포트를 3개를 임의로 열어서 활용하였음

```
python3 -m http.server 8000
```

```
python3 -m http.server 8080
```

```
python3 -m http.server 8888
```

스캔 결과

- 전체 스캔 포트 : 1000
- 열린 포트 : 3
- 필터링 : 0
- 닫힌 포트 : 997

처음 실습을 통해 기본 우분투 환경에서는 외부에 개방된 포트가 없기 때문에 스캔시 탐지되는 포트가 없음을 확인함. 따라서 테스트를 위한 임의 포트 개방이 필요해 3개의 임의 포트를 열어 zenmap을 통해 위 포트들이 성공적으로 탐지 되는걸 확인하였음. 또한, MAC 주소도 정확하게 식별되어 네트워크 보안 확인에 유용한 도구임을 직접 알 수 있었음

```
bm-virtual-machine login: bm
Password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 6.8.0-57-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

Expanded Security Maintenance for Applications is not enabled.

220 updates can be applied immediately.
161 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.
```

배너 그래빙 전 환경설정

```
bm@bm-virtual-machine: ~  
GNU nano 6.2 /etc/vsftpd.conf  
listen=NO  
listen_ipv6=YES  
anonymous_enable=NO  
local_enable=YES  
write_enable=YES  
local_umask=022  
dirmessage_enable=YES  
use_localtime=YES  
xferlog_enable=YES  
connect_from_port_20=YES  
chroot_local_user=YES  
secure_chroot_dir=/var/run/vsftpd/empty  
pam_service_name=vsftpd  
rsa_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem  
rsa_private_key_file=/etc/ssl/private/ssl-cert-snakeoil.key  
ssl_enable=NO  
pasv_enable=Yes  
pasv_min_port=10000  
pasv_max_port=10100  
allow_writeable_chroot=YES
```

FTP설정: 익명 로그인 불허, 기본 암호화 비활성, 방화벽 환경에서 FTP클라 연결 편리

```
bm@bm-virtual-machine:~$ sudo systemctl restart sendmail  
bm@bm-virtual-machine:~$ telnet localhost 25  
Trying 127.0.0.1...  
Connected to localhost.  
Escape character is '^]'.  
220 bm-virtual-machine ESMTP Sendmail 8.15.2/8.15.2/Debian-22ubuntu3; Sat, 5 Apr 2025 18:12:51 +0900; (No UCE/UBE) logging access from: localhost(OK)-localhost [127.0.0.1]
```

포트 25(SMTP)에서 sendmail이 정상적으로 작동중, 로컬에서 Telnet접속 성공, 로그 정상출력을 하고 localhost로부터 접근이 허용됨을 의미함

```
bm@bm-virtual-machine:~/Desktop$ sudo netstat -antp  
Active Internet connections (servers and established)  
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name  
tcp        0      0 127.0.0.1:53           0.0.0.0:*                 LISTEN      678/systemd-resolve  
tcp        0      0 0.0.0.0:22             0.0.0.0:*                 LISTEN      7423/sshd: /usr/sbi  
tcp        0      0 0.0.0.0:25             0.0.0.0:*                 LISTEN      44227/sendmail: MTA  
tcp        0      0 0.0.0.0:587            0.0.0.0:*                 LISTEN      44227/sendmail: MTA  
tcp        0      0 127.0.0.1:631          0.0.0.0:*                 LISTEN      30035/cupsd  
tcp6       0      0 :::80                  :::*                     LISTEN      44709/apache2  
tcp6       0      0 :::21                  :::*                     LISTEN      43068/vsftpd  
tcp6       0      0 :::23                  :::*                     LISTEN      42902/xinetd  
tcp6       0      0 :::22                  :::*                     LISTEN      7423/sshd: /usr/sbi  
tcp6       0      0 :::1:631               :::*                     LISTEN      30035/cupsd  
bm@bm-virtual-machine:~/Desktop$ s
```

설정 완료후 netstat 명령어를 통해 포트들이 활성화 됐는지 확인을 함.

SMTP, FTP, SSH, HTTP 서버가 각각 정상적으로 동작중임을 확인

4.. FTP 배너 그라빙

```
(kali㉿kali)-[~/Desktop]
$
(kali㉿kali)-[~/Desktop]
$ telnet 192.168.174.128 21
Trying 192.168.174.128 ...
Connected to 192.168.174.128.
Escape character is '^]'.
220 (vsFTPD 3.0.5)
```

attacker ↔ victim 연결 확인

```
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ ftp 192.168.174.128
Connected to 192.168.174.128.
220 (vsFTPD 3.0.5)
Name (192.168.174.128:kali): bm
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> █
```

ftp 연결 후 victim의 계정으로 로그인함, vsFTPD 3.0.5 & 원격 시스템의 타입인 UNIX임을 알 수 있음.

5.SMTP 배너 그라빙

```
(kali㉿kali)-[~/Desktop]
$ telnet 192.168.174.128 25
Trying 192.168.174.128 ...
Connected to 192.168.174.128.
Escape character is '^]'.
220 bm-virtual-machine ESMTP Sendmail 8.15.2/8.15.2/Debian-22ubuntu3; Sat, 5 Apr 2025 18:47:07 +0900; (No UCE/UBE) logging access from: [192.168.174.130](FAIL)-[192.168.174.130]
█
```

Talnet을 통해 SMTP 접속 연결 .. 서버 종류 : 우분투 sendmail 버전 : 8.15.2


```
bm@bm-virtual-machine: ~/Desktop
tcp6      0      0 ::::631          :::*              LISTEN          -
bm@bm-virtual-machine: ~/Desktop$ sudo netstat -antp
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State           PID/Program name
tcp        0      0 127.0.0.53:53        0.0.0.0:*            LISTEN          678/systemd-resol
tcp        0      0 0.0.0.0:22           0.0.0.0:*            LISTEN          7423/sshd: /usr/s
tcp        0      0 0.0.0.0:25           0.0.0.0:*            LISTEN          44227/sendmail: M
tcp        0      0 0.0.0.0:587          0.0.0.0:*            LISTEN          44227/sendmail: M
tcp        0      0 127.0.0.1:631        0.0.0.0:*            LISTEN          30035/cupsd
tcp6       0      0 :::80              :::*              LISTEN          44709/apache2
tcp6       0      0 :::21              :::*              LISTEN          43068/vsftpd
tcp6       0      0 :::23              :::*              LISTEN          42902/xinetd
tcp6       0      0 :::22              :::*              LISTEN          7423/sshd: /usr/s
tcp6       0      0 ::::631          :::*              LISTEN          30035/cupsd
bm@bm-virtual-machine: ~/Desktop$ cleaer
Command 'cleaer' not found, did you mean:
  command 'clear' from deb ncurses-bin (6.3-2ubuntu0.1)
Try: sudo apt install <deb name>
bm@bm-virtual-machine: ~/Desktop$ ping 192.168.174.130
PING 192.168.174.130 (192.168.174.130) 56(84) bytes of data.
64 bytes from 192.168.174.130: icmp_seq=1 ttl=64 time=1.97 ms
64 bytes from 192.168.174.130: icmp_seq=2 ttl=64 time=0.684 ms
64 bytes from 192.168.174.130: icmp_seq=3 ttl=64 time=0.964 ms
64 bytes from 192.168.174.130: icmp_seq=4 ttl=64 time=0.239 ms
64 bytes from 192.168.174.130: icmp_seq=5 ttl=64 time=1.30 ms
64 bytes from 192.168.174.130: icmp_seq=6 ttl=64 time=0.218 ms
64 bytes from 192.168.174.130: icmp_seq=7 ttl=64 time=0.745 ms
64 bytes from 192.168.174.130: icmp_seq=8 ttl=64 time=1.01 ms
64 bytes from 192.168.174.130: icmp_seq=9 ttl=64 time=0.964 ms
64 bytes from 192.168.174.130: icmp_seq=10 ttl=64 time=1.17 ms
64 bytes from 192.168.174.130: icmp_seq=11 ttl=64 time=0.216 ms
^C
--- 192.168.174.130 ping statistics ---
11 packets transmitted, 11 received, 0% packet loss, time 1013ms
rtt min/avg/max/ndev = 0.216/0.862/1.973/0.507 ms
bm@bm-virtual-machine: ~/Desktop$
```

```
kali@kali: ~/Desktop
File Actions Edit View Help
64 bytes from 192.168.174.128: icmp_seq=3 ttl=64 time=0.279 ms
64 bytes from 192.168.174.128: icmp_seq=4 ttl=64 time=1.28 ms
64 bytes from 192.168.174.128: icmp_seq=5 ttl=64 time=1.13 ms
64 bytes from 192.168.174.128: icmp_seq=6 ttl=64 time=1.09 ms
64 bytes from 192.168.174.128: icmp_seq=7 ttl=64 time=0.570 ms
64 bytes from 192.168.174.128: icmp_seq=8 ttl=64 time=1.15 ms
64 bytes from 192.168.174.128: icmp_seq=9 ttl=64 time=1.20 ms
64 bytes from 192.168.174.128: icmp_seq=10 ttl=64 time=0.351 ms
64 bytes from 192.168.174.128: icmp_seq=11 ttl=64 time=0.670 ms
64 bytes from 192.168.174.128: icmp_seq=12 ttl=64 time=0.351 ms
64 bytes from 192.168.174.128: icmp_seq=13 ttl=64 time=0.277 ms
64 bytes from 192.168.174.128: icmp_seq=14 ttl=64 time=0.252 ms
64 bytes from 192.168.174.128: icmp_seq=15 ttl=64 time=0.479 ms
64 bytes from 192.168.174.128: icmp_seq=16 ttl=64 time=1.20 ms
64 bytes from 192.168.174.128: icmp_seq=17 ttl=64 time=1.46 ms
64 bytes from 192.168.174.128: icmp_seq=18 ttl=64 time=1.12 ms
64 bytes from 192.168.174.128: icmp_seq=19 ttl=64 time=0.341 ms
64 bytes from 192.168.174.128: icmp_seq=20 ttl=64 time=1.49 ms
64 bytes from 192.168.174.128: icmp_seq=21 ttl=64 time=0.275 ms
64 bytes from 192.168.174.128: icmp_seq=22 ttl=64 time=0.907 ms
64 bytes from 192.168.174.128: icmp_seq=23 ttl=64 time=1.23 ms
64 bytes from 192.168.174.128: icmp_seq=24 ttl=64 time=1.04 ms
64 bytes from 192.168.174.128: icmp_seq=25 ttl=64 time=1.02 ms
64 bytes from 192.168.174.128: icmp_seq=26 ttl=64 time=1.15 ms
64 bytes from 192.168.174.128: icmp_seq=27 ttl=64 time=1.22 ms
64 bytes from 192.168.174.128: icmp_seq=28 ttl=64 time=0.778 ms
64 bytes from 192.168.174.128: icmp_seq=29 ttl=64 time=0.536 ms
64 bytes from 192.168.174.128: icmp_seq=30 ttl=64 time=0.456 ms
64 bytes from 192.168.174.128: icmp_seq=31 ttl=64 time=0.931 ms
64 bytes from 192.168.174.128: icmp_seq=32 ttl=64 time=0.284 ms
64 bytes from 192.168.174.128: icmp_seq=33 ttl=64 time=0.340 ms
64 bytes from 192.168.174.128: icmp_seq=34 ttl=64 time=0.353 ms
64 bytes from 192.168.174.128: icmp_seq=35 ttl=64 time=0.567 ms
64 bytes from 192.168.174.128: icmp_seq=36 ttl=64 time=1.27 ms
64 bytes from 192.168.174.128: icmp_seq=37 ttl=64 time=0.969 ms
64 bytes from 192.168.174.128: icmp_seq=38 ttl=64 time=1.72 ms
^C
--- 192.168.174.128 ping statistics ---
38 packets transmitted, 38 received, 0% packet loss, time 37378ms
rtt min/avg/max/ndev = 0.252/0.830/1.724/0.413 ms
kali@kali: ~/Desktop
```

victim → attacker

attacker → victim

6. SSH 배너 그래빙 하기

```
Applications
File Actions Edit View Help

(kali@kali)-[~/Desktop]
$ telnet 192.168.174.128 22
Trying 192.168.174.128 ...
Connected to 192.168.174.128.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.11
```

포트 22를 통해 SSH 서비스가 외부에 열려있는 것을 확인. Telnet를 이용하여 포트 22번에 접속
결과 서버에서 OpenSSH8.9p1 Ubuntu 버전이 실행중임을 확인할 수 있음

7. HTTP 포트에 대해 배너 그래빙

```
File Actions Edit View Help
(kali㉿kali)-[~/Desktop]
$ telnet 192.168.174.128 80
Trying 192.168.174.128 ...
Connected to 192.168.174.128.
Escape character is '^]'.
GET /
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2022-03-22
    See: https://launchpad.net/bugs/1966004
  -->
  <head>
    <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
    <title>Apache2 Ubuntu Default Page: It works</title>
    <style type="text/css" media="screen">
      * {
        margin: 0px 0px 0px 0px;
        padding: 0px 0px 0px 0px;
      }

      body, html {
        padding: 3px 3px 3px 3px;
```

7-1. OS 정보 : Ubuntu

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//E
d">
<html xmlns="http://www.w3.org/1999/xhtml">
  <!--
    Modified from the Debian original for Ubuntu
    Last updated: 2022-03-22
    See: https://launchpad.net/bugs/1966004
  -->
```

주석 부분에 OS정보가 나와있는걸 볼 수 있음

7-2.Web Server 정보 : Apach2

```
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8" />
  <title>Apache2 Ubuntu Default Page: It works</title>
  <style type="text/css" media="screen">
* {
  margin: 0px 0px 0px 0px;
  padding: 0px 0px 0px 0px;
}
```

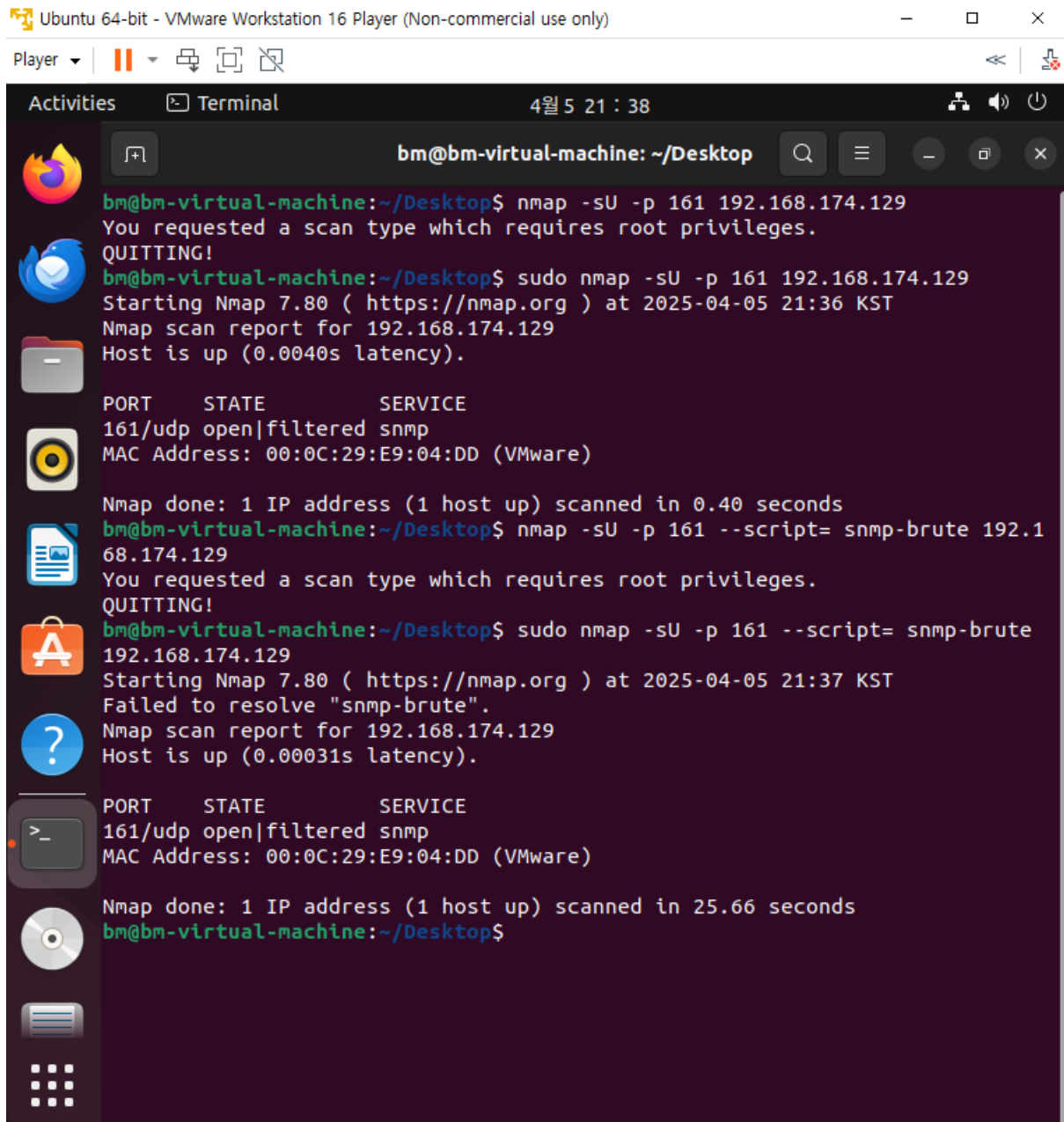
title부분에 웹 서버 정보가 나타나 있는 걸 볼 수 있음

7-3. 수정하길 권고하는 경로

```
</div>
<div class="content_section floating_element">
  <div class="content_section_text">
    <p>
      This is the default welcome page used to test the correct
      operation of the Apache2 server after installation on Ubuntu systems.
      It is based on the equivalent page on Debian, from which the Ubuntu Apache
      packaging is derived.
      If you can read this page, it means that the Apache HTTP server installed at
      this site is working properly. You should <b>replace this file</b> (located at
      <tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP server.
    </p>
    <p>
      If you are a normal user of this web site and don't know what this page is
      about, this probably means that the site is currently unavailable due to
      maintenance.
      If the problem persists, please contact the site's administrator.
    </p>
  </div>
</div>
```

Telnet을 통해 victim 서버의 80번 포트 HTTP요청을 보내 Apache2의 기본 HTML출력됨
응답 확인 후 서버가 Ubuntu 운영체제에서 구동되고 있으며, Apache2의 웹서버를 사용중인 것을
확인함. 웹 페이지 파일 경로가 /var/www/html/index.html임을 확인할 수 있고 설정 페이지 변조
로 사용될 수 있는 단서임

8. SNMP를 이용해 정보수집



```
bm@bm-virtual-machine: ~/Desktop
bm@bm-virtual-machine:~/Desktop$ nmap -sU -p 161 192.168.174.129
You requested a scan type which requires root privileges.
QUITTING!
bm@bm-virtual-machine:~/Desktop$ sudo nmap -sU -p 161 192.168.174.129
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-05 21:36 KST
Nmap scan report for 192.168.174.129
Host is up (0.0040s latency).

PORT      STATE      SERVICE
161/udp   open|filtered snmp
MAC Address: 00:0C:29:E9:04:DD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 0.40 seconds
bm@bm-virtual-machine:~/Desktop$ nmap -sU -p 161 --script= snmp-brute 192.1
68.174.129
You requested a scan type which requires root privileges.
QUITTING!
bm@bm-virtual-machine:~/Desktop$ sudo nmap -sU -p 161 --script= snmp-brute
192.168.174.129
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-05 21:37 KST
Failed to resolve "snmp-brute".
Nmap scan report for 192.168.174.129
Host is up (0.00031s latency).

PORT      STATE      SERVICE
161/udp   open|filtered snmp
MAC Address: 00:0C:29:E9:04:DD (VMware)

Nmap done: 1 IP address (1 host up) scanned in 25.66 seconds
bm@bm-virtual-machine:~/Desktop$
```

nmap -sU -p 161 : UDP 스캔 SNMP 포트가 열려 있는지 확인하는 것임 161번이 열려있거나 필터링 된걸로 볼 수 있음

--script=snmp-brute : SNMP의 커뮤니티 문자열(Public)을 무작위로 대입

그 외 옵션 스캔)

```
bm@bm-virtual-machine: ~/Desktop
bm@bm-virtual-machine:~/Desktop$ snmpwalk -v 1 -c public 192.168.174.129 1.3.6.1.2.1.1
Timeout: No Response from 192.168.174.129
```

SNMP 장비의 정보를 수집하는 것인데 현재 응답이 없어 실패로 나온걸 볼 수 있음

<https://gleaming.notion.site/Chapter-05-d7223dff200441a2bb0a95c826525db6>

<https://gleaming.notion.site/Chapter-04-IP-5cba3524e69c4537a41494c84855036b>