

네트워크 보안 과제3

Chapter 05 목록화

202246109

김기현

2025년 04월 05일

다양한 방법으로 스캔하기

Attacker: Vmware(Ubuntu 22.04.5 LTS)

Victim: : Vmware(Windows10)

배너 그래빙하기

Attacker: Vmware(Kali Linux)

Victim: Vmware(Ubuntu 22.04.5 LTS)

SNMP를 이용해 정보 수집하기

Attacker: Vmware(Kali Linux)

Victim: Vmware(Windows Server 2022)

실습 도구

스캐닝 도구:

fping: 네트워크 스위핑을 통한 활성 호스트 탐지

nmap: 포트 스캔 및 서비스 탐지

zenmap: nmap의 GUI 버전, 시각적 네트워크 매핑 제공

배너 그래빙 도구:

telnet: 원격 서비스 연결 및 배너 확인

SNMP 정보 수집 도구:

snmpwalk: SNMP를 통한 시스템 정보 수집

1. fping을 이용해 스캔하기

fping은 스캔 전에 네트워크의 시스템 목록을 확인할 때 사용한다.

fping은 ping과 달리 여러 호스트를 동시에 스캔할 수 있습니다.

-q 옵션은 ICMP Error Message를 숨기고 결과를 간단히 보여줍니다.

-a 옵션은 활성화된 시스템만 보여줍니다.

-s 옵션은 종료 시 누적 통계를 보여줍니다.

-g 옵션은 스캔범위를 설정합니다.

```
kgh@linux:~$ fping -qasg 192.168.40.0/24
192.168.40.2
192.168.40.128

    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

    0.043 ms (min round trip time)
    0.107 ms (avg round trip time)
    0.171 ms (max round trip time)
      9.093 sec (elapsed real time)
```

탐색 결과 192.168.40.0/24 네트워크에서 2개의 활성 호스트(192.168.40.2와 192.168.40.128)가 발견되었습니다. 총 254개의 타겟 중 252개는 도달할 수 없었습니다. 이 스캔은 약 9.093초가 소요되었습니다.

2. nmap을 이용해 스캔하기

nmap TCP SYN 스캔

-sS 옵션은 TCP SYN 스캔을 의미합니다. Half-Open 스캔이라고도 불리는데 TCP 연결을 완전히 성립시키지 않고 포트의 상태를 확인합니다.

```
kgh@linux:~$ sudo nmap -sS 192.168.40.128
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-05 15:02 KST
Nmap scan report for linux (192.168.40.128)
Host is up (0.0000050s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp   open  mysql
Nmap done: 1 IP address (1 host up) scanned in 0.08 seconds
```

스캔 결과 netbios-ssn(139), microsoft-ds(445), mysql(3306) 포트가 열려 있음을 확인했습니다.

nmap FIN 스캔

-sF 옵션은 FIN 스캔을 의미합니다. FIN 플래그가 설정된 패킷을 보내 포트 상태를 확인합니다.

```
kgh@linux:~$ sudo nmap -sF -p 80, 139 192.168.40.128
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-05 15:05 KST
Nmap scan report for linux (192.168.40.128)
Host is up (0.000027s latency).

PORT      STATE SERVICE
80/tcp    closed http
Nmap done: 2 IP addresses (1 host up) scanned in 3.09 seconds
```

스캔 결과 http(80) 포트는 닫혀 있음을 확인했습니다

```
kgh@linux:~$ sudo nmap -sF -p 3306 192.168.40.128
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-05 15:06 KST
Nmap scan report for linux (192.168.40.128)
Host is up.

PORT      STATE      SERVICE
3306/tcp  open|filtered mysql

Nmap done: 1 IP address (1 host up) scanned in 2.06 seconds
```

스캔 결과 mysql(3306)포트는 열려 있음을 확인했습니다.

nmap fragmentation 스캔

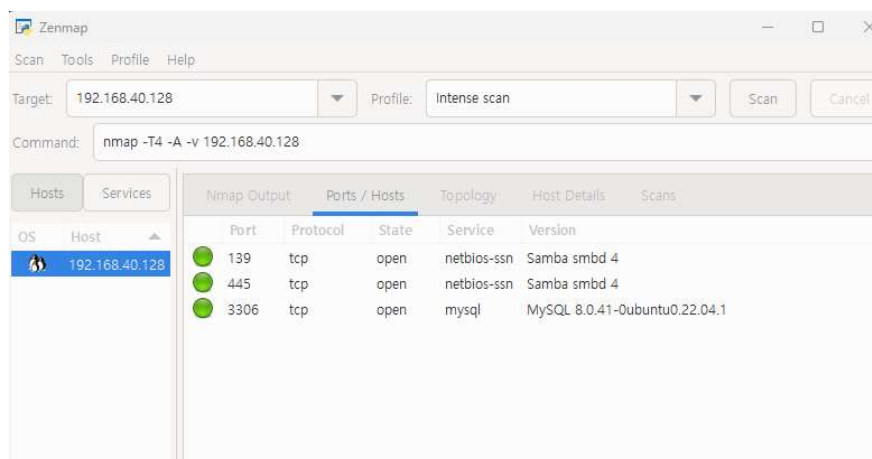
-f 옵션은 패킷 단편화(fragmentation)를 수행합니다. 이는 방화벽을 우회하기 위한 방법입니다.

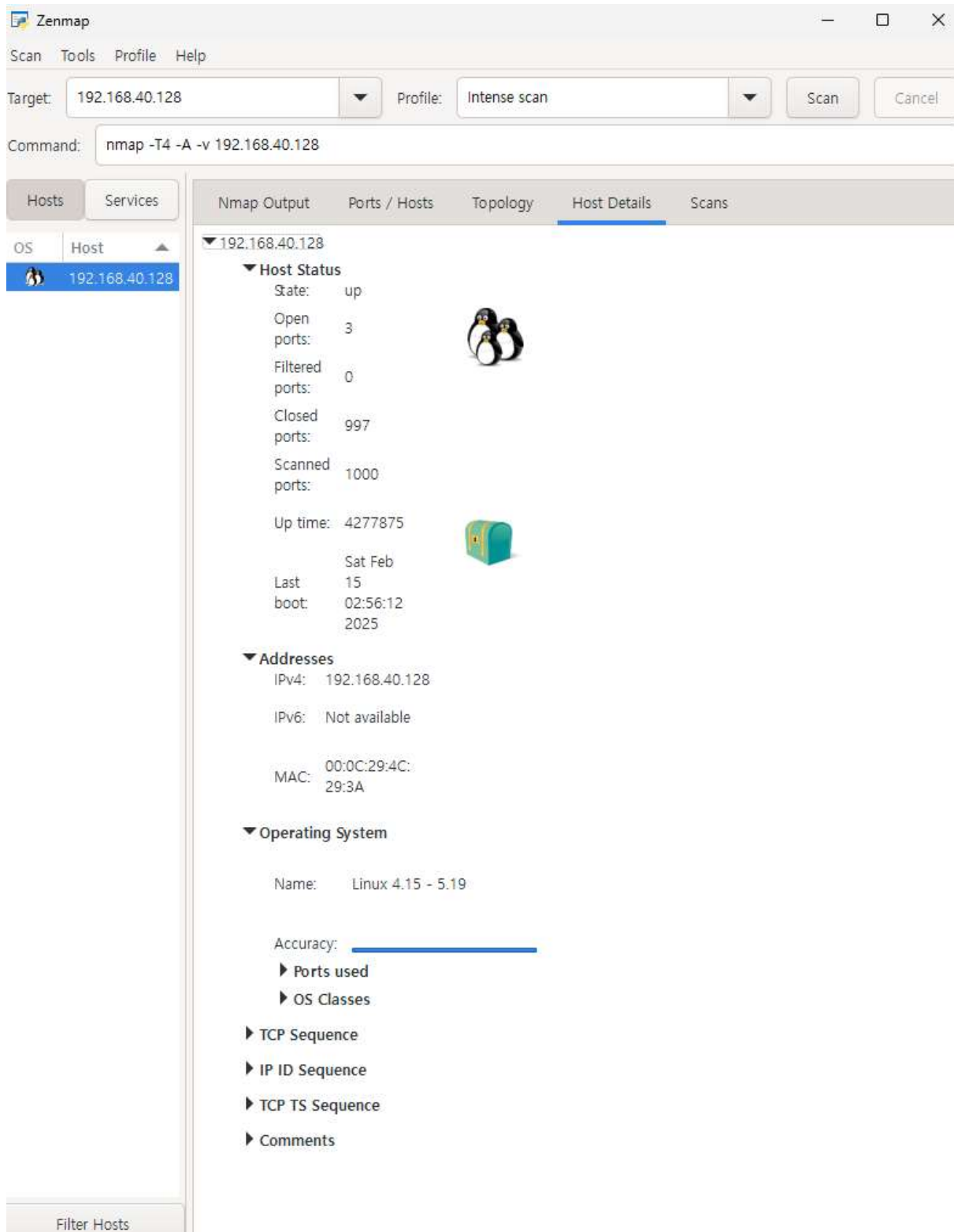
```
kgh@linux:~$ sudo nmap -f -sS 192.168.40.128
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-05 15:07 KST
Nmap scan report for linux (192.168.40.128)
Host is up (0.000016s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3306/tcp  open  mysql

Nmap done: 1 IP address (1 host up) scanned in 0.10 seconds
```

스캔 결과는 일반 SYN 스캔과 동일하게 나타났습니다.

- Zenmap으로 스캔하기





Zenmap은 nmap의 그래픽 사용자 인터페이스(GUI) 버전입니다.
스캔 결과 대상 시스템이 Linux 4.15-5.19 운영체제임을 확인했습니다.
열린 포트 및 서비스 정보도 확인할 수 있었습니다
netbios-ssn(139), microsoft-ds(445), mysql(3306)

배너 그래빙은 상대 시스템의 OS를 확인하는 가장 기본적인 방법입니다.

```
kgh@linux:~$ 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 0.0.0.0:445             0.0.0.0:*               LISTEN      1032/smbd
tcp        0      0 0.0.0.0:139             0.0.0.0:*               LISTEN      1032/smbd
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      6638/sshd: /usr/sbi
tcp        0      0 0.0.0.0:25              0.0.0.0:*               LISTEN      9197/sendmail: MTA:
tcp        0      0 0.0.0.0:587             0.0.0.0:*               LISTEN      9197/sendmail: MTA:
tcp        0      0 127.0.0.1:33060         0.0.0.0:*               LISTEN      1027/mysqld
tcp        0      0 0.0.0.0:3306            0.0.0.0:*               LISTEN      1027/mysqld
tcp        0      0 127.0.0.53:53          0.0.0.0:*               LISTEN      602/systemd-resolve
tcp        0      0 127.0.0.1:631          0.0.0.0:*               LISTEN      780/cupsd
tcp        0      0 127.0.0.1:25           127.0.0.1:47270        TIME_WAIT   -
tcp6       0      0 :::445                 :::*                   LISTEN      1032/smbd
tcp6       0      0 :::139                 :::*                   LISTEN      1032/smbd
tcp6       0      0 :::80                  :::*                   LISTEN      9673/apache2
tcp6       0      0 :::1:631               :::*                   LISTEN      780/cupsd
tcp6       0      0 :::22                  :::*                   LISTEN      6638/sshd: /usr/sbi
tcp6       0      0 :::23                  :::*                   LISTEN      7526/xinetd
tcp6       0      0 :::21                  :::*                   LISTEN      7125/vsftpd
```

Vimtim 환경구성

실습교재를 따라 모든 설정을 완료한 후 Victim 시스템에서 열린 포트 및 서비스를 확인했습니다.

IPv4: 22(SSH), 25(SMTP) 포트 개방

IPv6: 21(FTP), 22(SSH), 23(SMTP), 80(HTTP) 포트 개방

Attacker <-> Victim 연결 확인

Attacker (Kali) 192.168.40.128

```
(kali@kali)-[~]  
$ ping 192.168.40.129  
PING 192.168.40.129 (192.168.40.129) 56(84) bytes of data.  
64 bytes from 192.168.40.129: icmp_seq=1 ttl=64 time=0.454 ms  
64 bytes from 192.168.40.129: icmp_seq=2 ttl=64 time=0.505 ms  
64 bytes from 192.168.40.129: icmp_seq=3 ttl=64 time=0.267 ms  
64 bytes from 192.168.40.129: icmp_seq=4 ttl=64 time=0.316 ms  
64 bytes from 192.168.40.129: icmp_seq=5 ttl=64 time=0.294 ms  
64 bytes from 192.168.40.129: icmp_seq=6 ttl=64 time=0.291 ms  
64 bytes from 192.168.40.129: icmp_seq=7 ttl=64 time=0.286 ms  
64 bytes from 192.168.40.129: icmp_seq=8 ttl=64 time=0.272 ms  
64 bytes from 192.168.40.129: icmp_seq=9 ttl=64 time=0.339 ms  
^C  
— 192.168.40.129 ping statistics —  
9 packets transmitted, 9 received, 0% packet loss, time 8172ms  
rtt min/avg/max/mdev = 0.267/0.336/0.505/0.080 ms
```

Victim (Ubuntu) 192.168.40.129

```
kgh@linux:~$ ping 192.168.40.128  
PING 192.168.40.128 (192.168.40.128) 56(84) bytes of data.  
64 bytes from 192.168.40.128: icmp_seq=1 ttl=64 time=0.287 ms  
64 bytes from 192.168.40.128: icmp_seq=2 ttl=64 time=0.268 ms  
64 bytes from 192.168.40.128: icmp_seq=3 ttl=64 time=0.301 ms  
64 bytes from 192.168.40.128: icmp_seq=4 ttl=64 time=0.284 ms  
64 bytes from 192.168.40.128: icmp_seq=5 ttl=64 time=0.606 ms  
64 bytes from 192.168.40.128: icmp_seq=6 ttl=64 time=0.285 ms  
64 bytes from 192.168.40.128: icmp_seq=7 ttl=64 time=0.526 ms  
^C  
--- 192.168.40.128 ping statistics ---  
7 packets transmitted, 7 received, 0% packet loss, time 6153ms  
rtt min/avg/max/mdev = 0.268/0.365/0.606/0.129 ms
```

ping 테스트를 통해 양방향 연결이 정상적으로 수립되었음을 확인했습니다.

1. FTP(21)에 대해 배너 그래빙하기

telnet과 ftp 명령어를 통해 FTP서비스에 대한 정보를 수집했습니다.

```
(kali@kali)-[~]
$ telnet 192.168.40.129 21
Trying 192.168.40.129 ...
Connected to 192.168.40.129.
Escape character is '^]'.
220 (vsFTPd 3.0.5)
```

telnet 연결

```
(kali@kali)-[~]
$ ftp 192.168.40.129
Connected to 192.168.40.129.
220 (vsFTPd 3.0.5)
Name (192.168.40.129:kali): kgh
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

ftp 연결

FTP 서버는 vsFTPd 3.0.5 버전을 사용중인걸 확인했습니다.

2. SMTP(25) 포트에 대해 배너 그래빙하기

```
(kali@kali)-[~]
$ telnet 192.168.40.129 25
Trying 192.168.40.129 ...
Connected to 192.168.40.129.
Escape character is '^]'.
220 linux ESMTP Sendmail 8.15.2/8.15.2/Debian-22ubuntu3; Sat, 5 Apr 2025 16:20:01 +0900; (No U
CE/UBE) logging access from: [192.168.40.128](FAIL)-[192.168.40.128]
```

SMTP 서버는 Sendmail 8.15.2 버전 사용 중이고 Debian 22ubuntu3 기반의 운영체제 사용 및 접속 시간 및 서버 로그 정보도 확인했습니다.

3. SSH(22) 포트에 대해 배너 그래빙하기

```
(kali@kali)-[~]
$ telnet 192.168.40.129 22
Trying 192.168.40.129 ...
Connected to 192.168.40.129.
Escape character is '^]'.
SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.11
```

SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.11 버전 사용 중이고 운영체제가 Ubuntu인걸 확인했습니다.

4. HTTP 포트에 대해 배너 그래빙하기

HTTP 배너 그래빙을 통해 다음 정보를 확인했습니다.

```
(kali㉿kali)-[~]
$ telnet 192.168.40.129 80
Trying 192.168.40.129 ...
Connected to 192.168.40.129.
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;
      }

    </style>
  </head>
  <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 replace this file (located at
    <tt>/var/www/html/index.html</tt>) before continuing to operate your HTTP serv
  </p>
```

- 해당 서버의 OS 정보 : Ubuntu
- 실행중인 Web Server 정보 : Apache2 server
- 수정하길 권고하고 있는 기본 페이지 경로 : /var/www/html/index.html

환경 구성

Attacker (Kali Linux): 192.168.40.**128**

Victim (Windows server) 192.168.40.**130**

실습교재의 SNMP 세팅과 snmpwalk 설치에 대한 내용은 생략했습니다.

nmap을 이용해 SNMP 포트(161/udp) 스캔을 수행했습니다

```
(kali㉿kali)-[~]  
$ nmap -sU -p 161 192.168.40.130  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-05 07:23 EDT  
Nmap scan report for 192.168.40.130  
Host is up (0.00030s latency).  
  
PORT      STATE SERVICE  
161/udp   open  snmp  
MAC Address: 00:0C:29:F7:D6:0D (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

Victim의 161/udp 포트가 열려있는걸 확인하였고 MAC주소도 확인했습니다.

nmap의 스크립트를 이용하여 SNMP 취약점을 스캔했습니다.

```
(kali㉿kali)-[~]  
$ nmap -sU -p 161 --script=snmp-brute 192.168.40.130  
Starting Nmap 7.95 ( https://nmap.org ) at 2025-04-05 07:22 EDT  
Nmap scan report for 192.168.40.130  
Host is up (0.00021s latency).  
  
PORT      STATE SERVICE  
161/udp   open  snmp  
| snmp-brute:  
|_ public - Valid credentials  
MAC Address: 00:0C:29:F7:D6:0D (VMware)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
```

커뮤니티 스트링 public이 유효한 것으로 확인했으며

이를 통해 SNMP 정보도 접근 가능했습니다.

snmpwalk 명령을 이용해 Victim(Windows Server)의 상세 정보를 수집했습니다

1. System MIB

```
(kali@kali)-[~]
$ snmpwalk -v1 -c public 192.168.40.130 1.3.6.1.2.1.1
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 151 Stepping 2 AT/AT COMPATIBLE - Software: Windows Version 6.3 (Build 20348 Multiprocessor Free)"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.311.1.1.3.1.2
iso.3.6.1.2.1.1.3.0 = Timeticks: (1149947) 3:11:39.47
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "WIN-T0RCD701SGD"
iso.3.6.1.2.1.1.6.0 = ""
```

시스템 하드웨어: Intel 64 Family 6 Model 151 (AT/AT COMPATIBLE)

운영체제: Windows Version 6.3 (Build 20348 Multiprocessor Free)

OID: iso.3.6.1.4.1.311.1.1.3.1.2

부팅 시간: 3일 11시간 29분 47초

호스트명: WIN-T0RCD701SGD

2. Interfaces

```
(kali@kali)-[~]
$ snmpwalk -v1 -c public 192.168.40.130 1.3.6.1.2.1.2
iso.3.6.1.2.1.2.1.0 = INTEGER: 24
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.2 = INTEGER: 2
iso.3.6.1.2.1.2.2.1.2.2 = Hex-STRING: 57 41 4E 20 4D 69 6E 69 70 6F 72 74 20 28 47 52 45 29 00
iso.3.6.1.2.1.2.2.1.2.3 = Hex-STRING: 4D 69 63 72 6F 73 6F 66 74 20 36 74 6F 34 20 41 64 61 70 74 65 72 00
iso.3.6.1.2.1.2.2.1.2.4 = Hex-STRING: 4D 69 63 72 6F 73 6F 66 74 20 49 50 2D 48 54 54 50 53 20 50 6C 61 74 66 6F 72 6D 20 41 64 61 70 74 65 72 00
```

HEX to ASCII로 디코딩 한 결과

```
Software Loopback Interface 1 WAN
Miniport (GRE) Microsoft 6to4 Adapter WAN Miniport (IP)
Microsoft IP-HTTPS Platform Adapter WAN Miniport (IP)
Microsoft Kernel Debug Network Adapter WAN
Miniport (SSTP) Microsoft Teredo Tunneling Adapter WAN
Intel(R) 82574L Gigabit Network Connection WAN
Miniport (PPPOE) WAN Miniport (PPPOE)
WAN Miniport (IPv6) WAN Miniport (IKEv2)
WAN Miniport (L2TP) WAN Miniport (Network Monitor)
Intel(R) 82574L Gigabit Network Connection-WFP Native MAC Layer
LightWeight Filter-0000 Intel(R) 82574L Gigabit Network
Connection-QoS Packet Scheduler-0000 Intel(R) 82574L
Gigabit Network Connection-WFP 802.3 MAC Layer LightWeight Filter-0000
WAN Miniport (IP)-WFP Native MAC Layer LightWeight Filter-0000
WAN Miniport (IP)-QoS Packet Scheduler-0000
WAN Miniport (IPv6)-WFP Native MAC Layer LightWeight Filter-0000
WAN Miniport (IPv6)-QoS Packet Scheduler-0000
Miniport (Network Monitor)-WFP Native MAC Layer LightWeight Filter-0000
WAN Miniport (Network Monitor)-QoS Packet Scheduler-0000
```

총 24개의 네트워크 인터페이스가 있으며 각각에 대한 정보를 확인할 수 있었습니다.

3. Shared Printers

OID 1.3.6.1.2.1.25.3 영역에서 시스템의 하드웨어 장치 정보를 확인해보겠습니다.

```
(kali@kali)-[~]  
$ snmpwalk -v1 -c public 192.168.40.130 1.3.6.1.2.1.25.3  
iso.3.6.1.2.1.25.3.2.1.1.1 = INTEGER: 1  
iso.3.6.1.2.1.25.3.2.1.1.2 = INTEGER: 2  
iso.3.6.1.2.1.25.3.2.1.1.3 = INTEGER: 3  
iso.3.6.1.2.1.25.3.2.1.1.4 = INTEGER: 4
```

시스템에 설치된 프린터 2대 확인했습니다.

```
iso.3.6.1.2.1.25.3.2.1.3.1 = STRING: "Microsoft XPS Document Writer v4"  
iso.3.6.1.2.1.25.3.2.1.3.2 = STRING: "Microsoft Print To PDF"
```

프린터 #1: "Microsoft XPS Document Writer v4" (가상 프린터)

프린터 #2: "Microsoft Print To PDF" (가상 프린터)

4. Services

```
(kali@kali)-[~]  
$ snmpwalk -v1 -c public 192.168.40.130 1.3.6.1.4.1.77.1.2.3  
iso.3.6.1.4.1.77.1.2.3.1.1.5.80.111.119.101.114 = STRING: "Power"  
iso.3.6.1.4.1.77.1.2.3.1.1.6.83.101.114.118.101.114 = STRING: "Server"  
iso.3.6.1.4.1.77.1.2.3.1.1.6.84.104.101.109.101.115 = STRING: "Themes"  
iso.3.6.1.4.1.77.1.2.3.1.1.7.83.121.115.77.97.105.110 = STRING: "SysMain"  
iso.3.6.1.4.1.77.1.2.3.1.1.9.73.80.32.72.101.108.112.101.114 = STRING: "IP Helper"  
iso.3.6.1.4.1.77.1.2.3.1.1.10.68.78.83.32.67.108.105.101.110.116 = STRING: "DNS Client"  
iso.3.6.1.4.1.77.1.2.3.1.1.10.68.78.83.32.83.101.114.118.101.114 = STRING: "DNS Server"  
iso.3.6.1.4.1.77.1.2.3.1.1.11.68.72.67.80.32.67.108.105.101.110.116 = STRING: "DHCP Client"  
iso.3.6.1.4.1.77.1.2.3.1.1.11.84.105.109.101.32.66.114.111.107.101.114 = STRING: "Time Broker"  
iso.3.6.1.4.1.77.1.2.3.1.1.11.87.111.114.107.115.116.97.116.105.111.110 = STRING: "Workstation"  
iso.3.6.1.4.1.77.1.2.3.1.1.12.83.78.77.80.32.83.101.114.118.105.99.101 = STRING: "SNMP Service"  
iso.3.6.1.4.1.77.1.2.3.1.1.12.85.115.101.114.32.77.97.110.97.103.101.114 = STRING: "User Manager"  
iso.3.6.1.4.1.77.1.2.3.1.1.12.86.77.119.97.114.101.32.84.111.111.108.115 = STRING: "VMware Tools"
```

Victim(Windows Server)에서 실행중인 서비스 목록을 확인했습니다.

5. Accounts

```
(kali@kali)-[~]  
$ snmpwalk -v1 -c public 192.168.40.130 1.3.6.1.4.1.77.1.2.25  
iso.3.6.1.4.1.77.1.2.25.1.1.5.71.117.101.115.116 = STRING: "Guest"  
iso.3.6.1.4.1.77.1.2.25.1.1.13.65.100.109.105.110.105.115.116.114.97.116.111.114 = STRING: "Administrator"  
iso.3.6.1.4.1.77.1.2.25.1.1.14.68.101.102.97.117.108.116.65.99.99.111.117.110.116 = STRING: "DefaultAccount"  
iso.3.6.1.4.1.77.1.2.25.1.1.18.87.68.65.71.85.116.105.108.105.116.121.65.99.99.111.117.110.116 = STRING: "WDAGUtilityAccount"
```

Windows 시스템의 사용자 계정을 4개 확인했습니다.

6. TCP/IP Networks

```
(kali㉿kali)-[~]  
$ snmpwalk -v1 -c public 192.168.40.130 1.3.6.1.2.1.4.20  
iso.3.6.1.2.1.4.20.1.1.127.0.0.1 = IPAddress: 127.0.0.1  
iso.3.6.1.2.1.4.20.1.1.192.168.40.130 = IPAddress: 192.168.40.130  
iso.3.6.1.2.1.4.20.1.2.127.0.0.1 = INTEGER: 1  
iso.3.6.1.2.1.4.20.1.2.192.168.40.130 = INTEGER: 9  
iso.3.6.1.2.1.4.20.1.3.127.0.0.1 = IPAddress: 255.0.0.0  
iso.3.6.1.2.1.4.20.1.3.192.168.40.130 = IPAddress: 255.255.255.0  
iso.3.6.1.2.1.4.20.1.4.127.0.0.1 = INTEGER: 1  
iso.3.6.1.2.1.4.20.1.4.192.168.40.130 = INTEGER: 1  
iso.3.6.1.2.1.4.20.1.5.127.0.0.1 = INTEGER: 65535  
iso.3.6.1.2.1.4.20.1.5.192.168.40.130 = INTEGER: 65535
```

Victim 시스템의 네트워크 구성과 서브넷 마스크를 확인했습니다.

어려웠던 점 및 해결방법

nmap -sU -p 명령을 이용한 스캔에서 교재에서는 MAC 주소가 출력되었으나, 실습 중에는 확인되지 않는 문제가 있었습니다. 원인을 분석해보니 attacker IP가 192.168.**220**.130이고 victim IP가 192.168.**40**.128로 서로 다른 네트워크에 있었기 때문이었습니다.

해결책으로 Attacker의 네트워크 주소를 192.168.**40**.130으로 변경하여 동일한 네트워크 대역에 위치시켰더니 정상적으로 MAC 주소 정보가 확인되었습니다. 이는 Nmap이 MAC 주소를 표시하려면 ARP 패킷으로 해당 호스트의 MAC 주소를 직접 알아야 하는데 같은 로컬 네트워크에 없기 때문에 발생한 문제였습니다.