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)

Vicitim: Vmware(Ubuntu 22.04.5 LTS)

SNMP를 이용해 정보 수집하기

Attacker: Vmware(Kali Linux)

Vicitim: 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 네트위커의 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 이용새 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

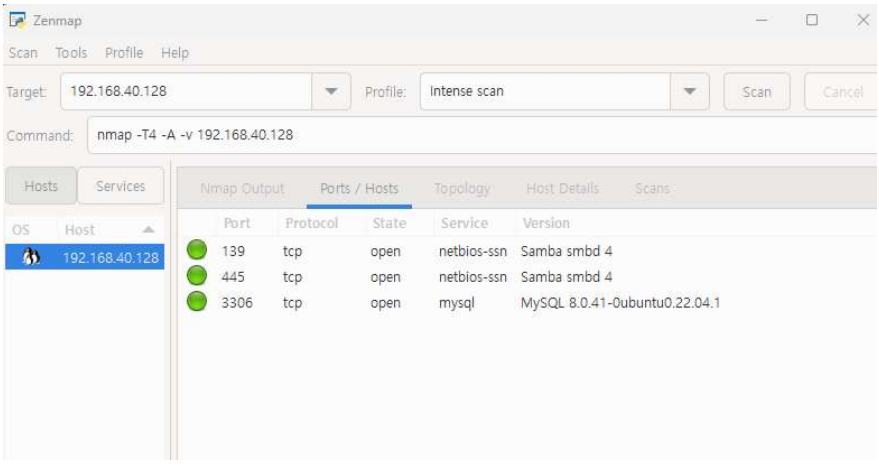
-f 옵션은 패킷 단편화(fragmentation)를 수행합니다. 이는 방화벽을 우회하기 위한 기법입니다.

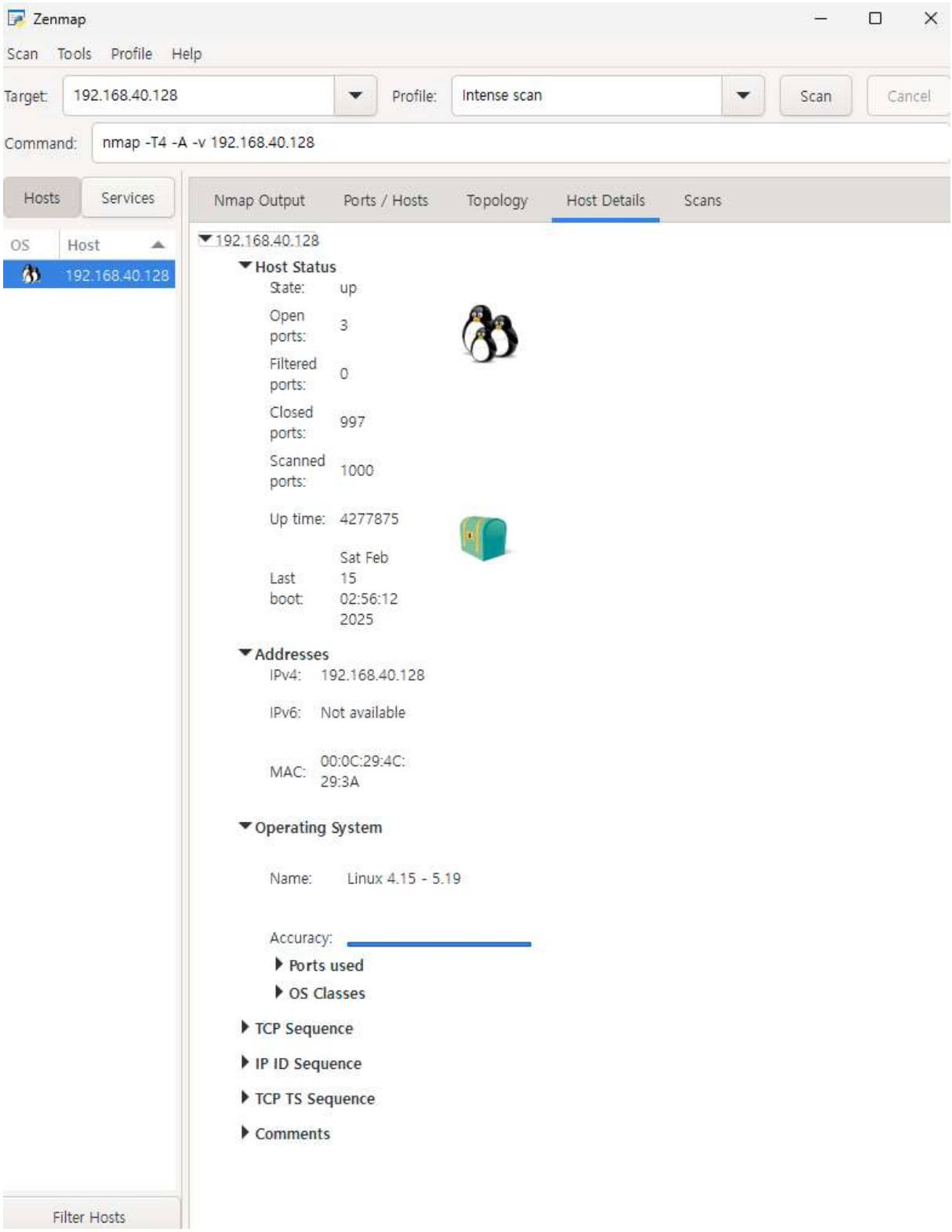
```
kgh@linux:~$ sudo nmap -f -sS 192.168.40.128
Starting Nmap 7.80 ( https://nmap.org ) at 2025-04-05 15:07 KST
Nmap scan report for linux (192.168.40.128)
Host is up (0.000016s latency).
Not shown: 997 closed ports
PORT     STATE SERVICE
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3306/tcp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

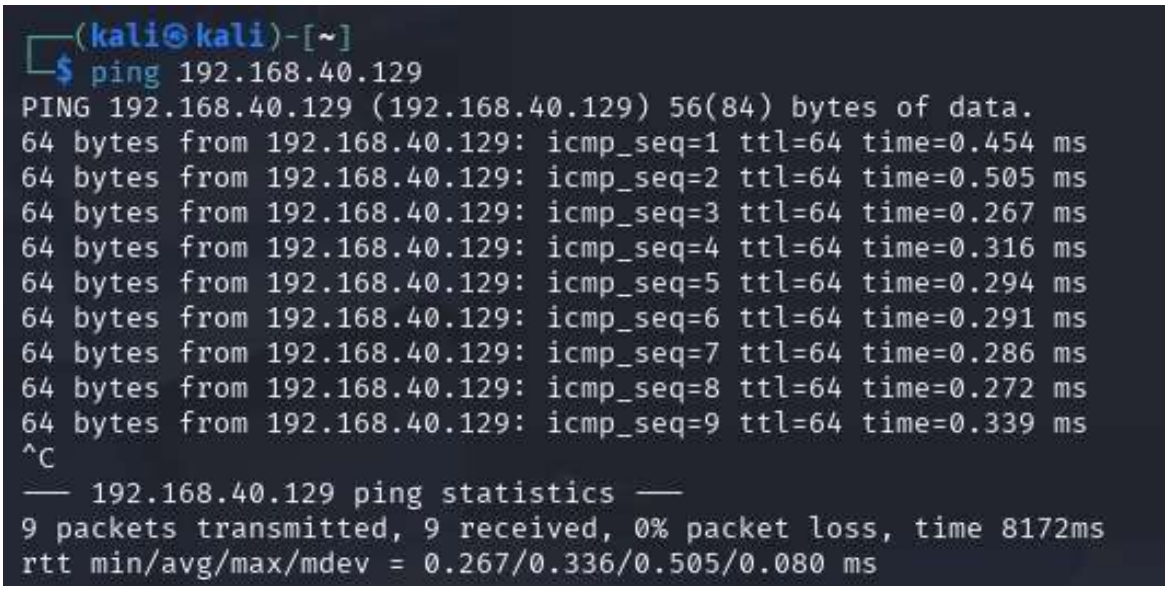
실습교재를 따라 모든 설정을 완료한 후 Victim 시스템에서 열린 포트 및 서비스를 확인했습다.

IPv4: 22(SSH), 25(SMTP) 포트 개방

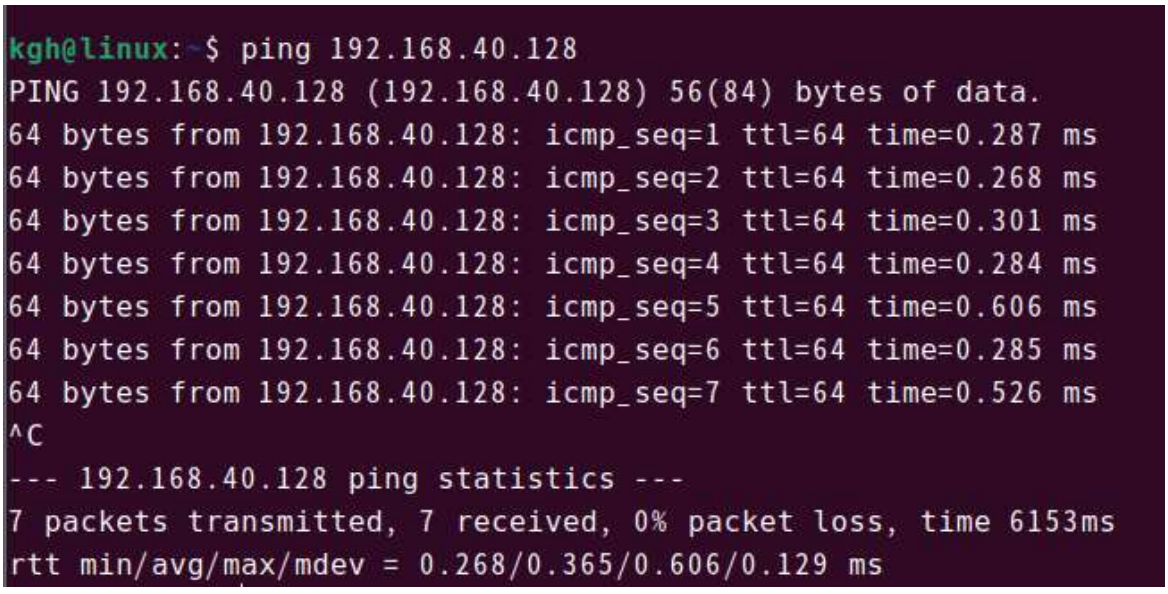
IPv6: 21(FTP), 22(SSH), 23(SSH), 80(HTTP) 포트 개방

Attacker <-> Victim 연결 확인

Attacker (Kali) 192.168.40.**128**



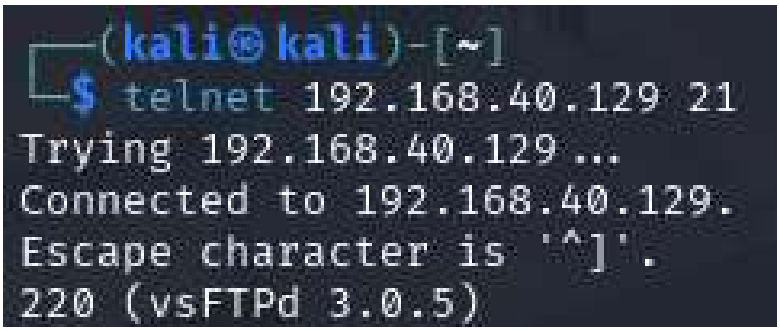
VIctim (Ubuntu) 192.168.40.**129**



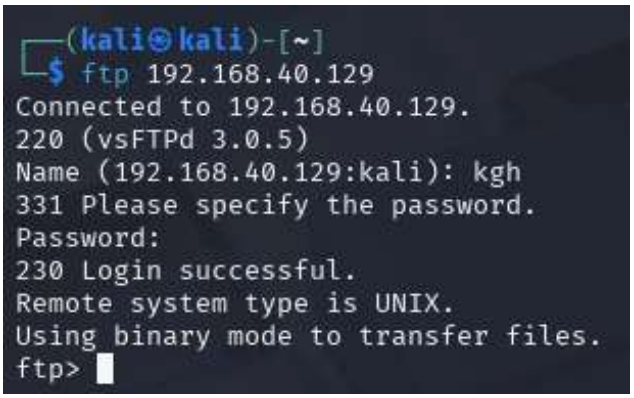
ping 테스트를 통해 양방향 연결이 정상적으로 수립되었음을 확인했습니다.

1. FTP(21)에 대해 배너 그래빙하기

telnet과 ftp 명령어를 통해 FTP서비스에 대한 정보를 수집했습니다.



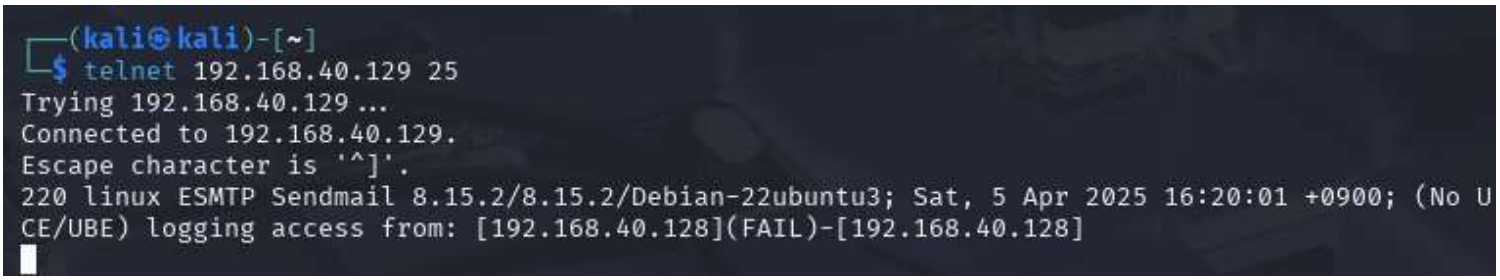
telnet 연결



ftp 연결

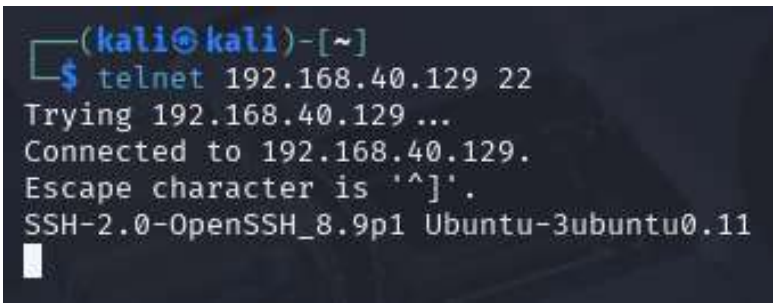
FTP 서버는 vsFTPd 3.0.5 버전을 사용중인걸 확인했습니다.

2. SMTP(25) 포트에 대해 배너 그래빙하기



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

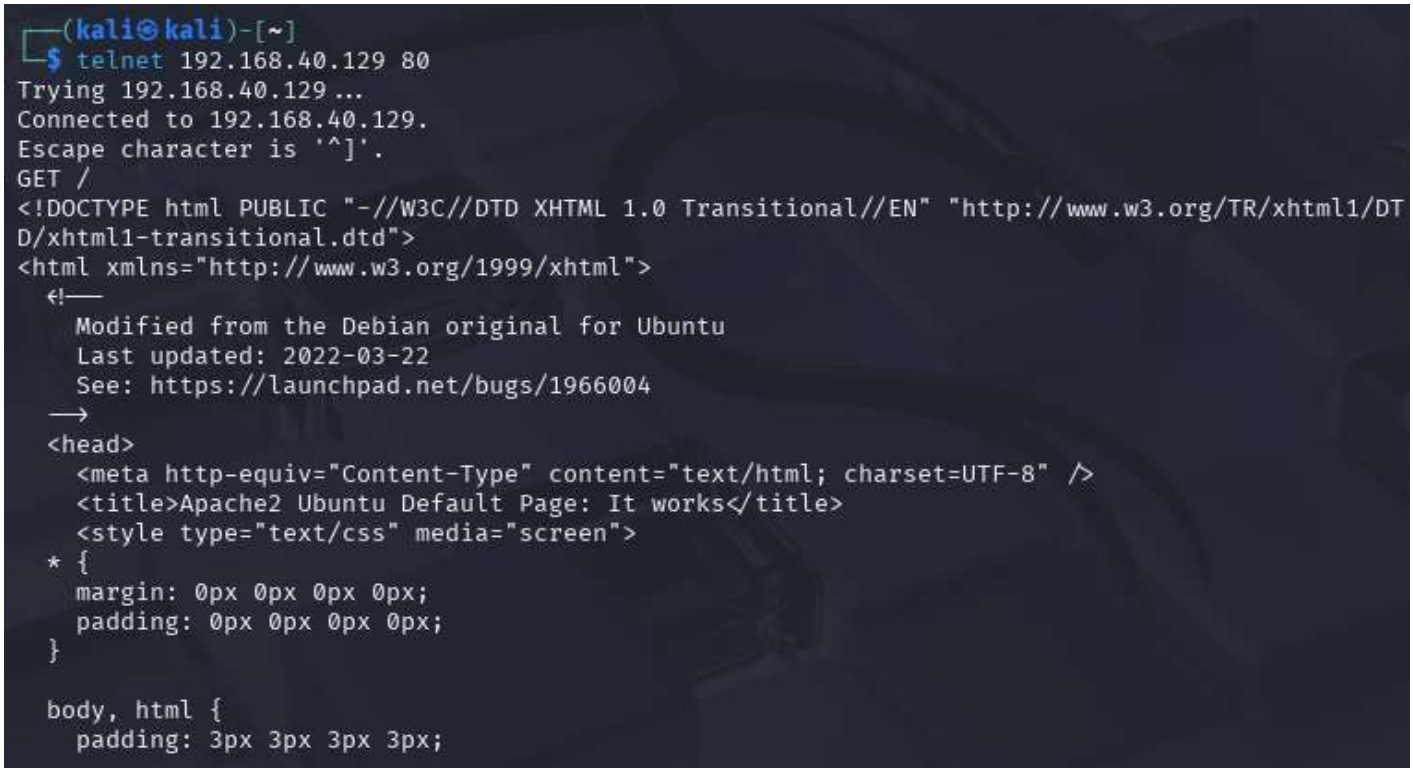
3. SSH(22) 포트에 대해 배너 그래빙하기

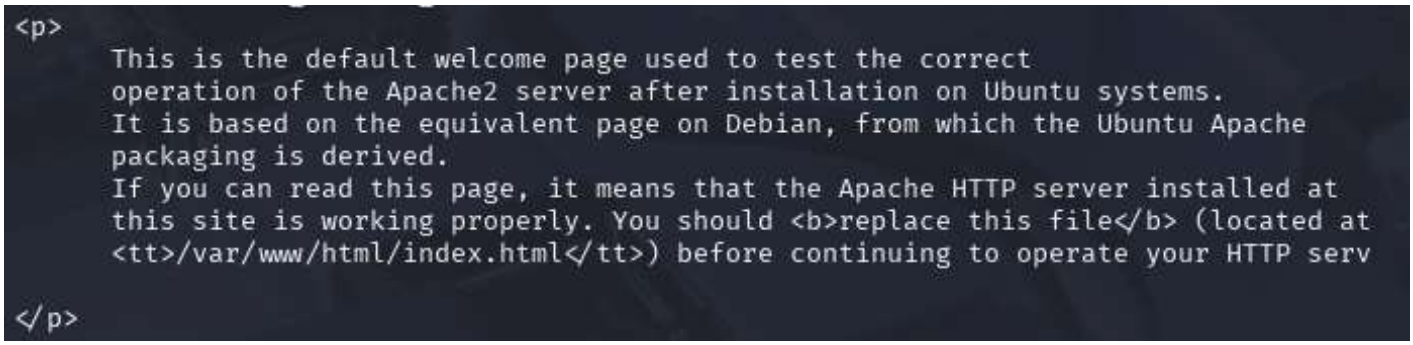


SSH-2.0-OpenSSH_8.9p1 Ubuntu-3ubuntu0.11 버전 사용 중이고 운영체제가 Ubuntu인걸 확인했습니다.

4. HTTP 포트에 대해 배너 그래빙하기

HTTP 배너 그래빙을 통해 다음 정보를 확인했습니다.





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

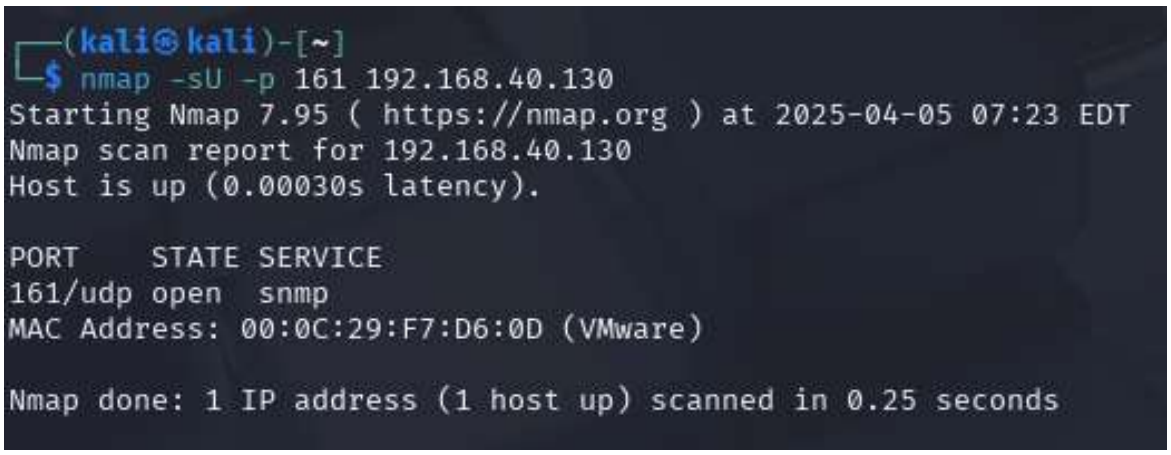
환경 구성

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

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

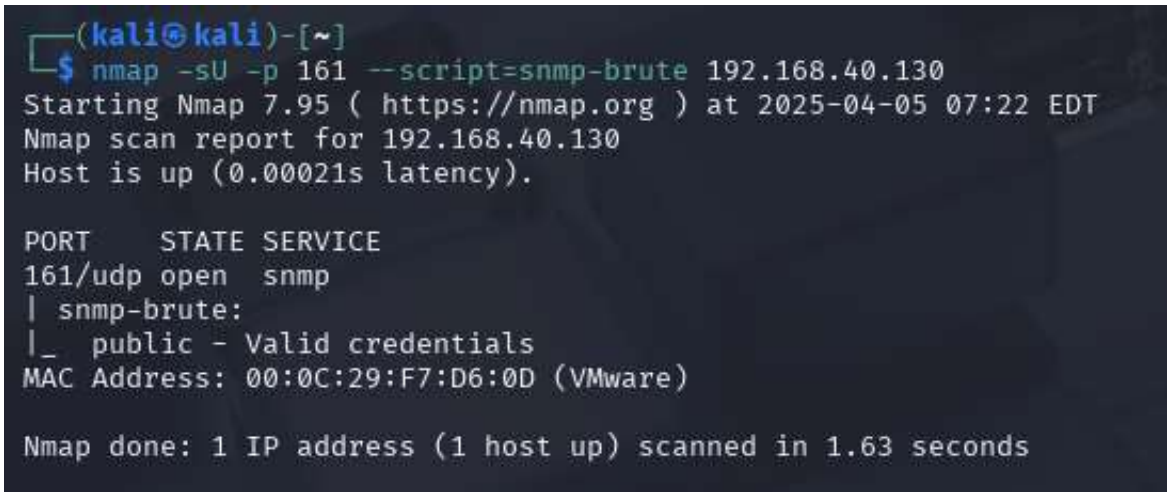
실습교재의 SNMP 세팅과 snmpwalk 설치에 대한 내용은 생략했습니다.

nmap을 이용해 SNMP 포트(161/udp) 스캔을 수행했습니다



Victim의 161/udp 포트가 열려있는걸 확인하였고 MAC주소도 확인했습니다.

nmap의 스크립트를 이용하여 SNMP 취약점을 스캔했습니다.



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 (Bu
ild 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-T0RCD7015GD"
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
```

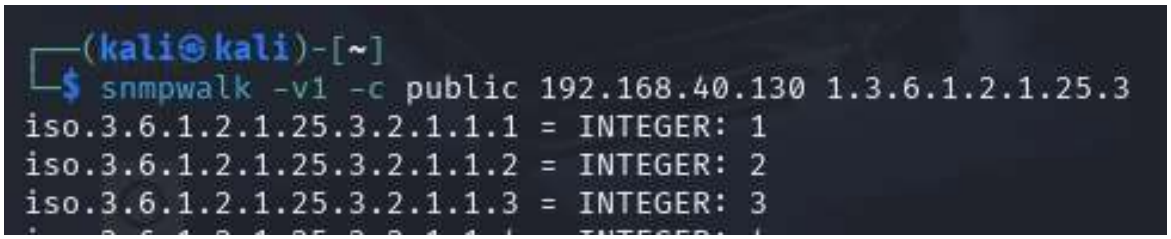
HEX to ASCII로 디코딩 한 결과

ETX ACK SOH STX SOH STX STX SOH STX SOH SO Software Loopback Interface 1 NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX STX SOH STX SO WAN Miniport (GRE) NUL ETX ACK SOH STX SOH STX STX SOH STX ETX SO Microsoft 6to4 Adapter NUL ETX ACK SOH STX SOH STX STX SOH STX EOT SO Microsoft IP-HTTPS Platform Adapter NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX ENQ SO WAN Miniport (IP) NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX ACK SO Microsoft Kernel Debug Network Adapter NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX STX SOH STX BEL SO WAN Miniport (SSTP) NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX STX SOH STX BS SO Microsoft Teredo Tunneling Adapter NUL ETX ACK SOH STX SOH STX STX SOH STX SO Intel(R) 82574L Gigabit Network Connection NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX STX SOH STX DLE SO WAN Miniport (PPTP) NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX DC1 SO WAN Miniport (PPOE) NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX DC2 SO WAN Miniport (IPv6) NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX DC3 SO WAN Miniport (IKEv2) NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX DC4 SO WAN Miniport (L2TP) NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX NAK SO WAN Miniport (Network Monitor) NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX SYN SO Intel(R) 82574L Gigabit Network Connection-WFP Native MAC Layer LightWeight Filter-0000 NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX ETB SO Intel(R) 82574L Gigabit Network Connection-QoS Packet Scheduler-0000 NUL ETX ACK SOH STX SOH STX STX SOH STX SOH STX CAN SO Intel(R) 82574L Gigabit Network Connection-WFP 802.3 MAC Layer LightWeight Filter-0000 NUL ETX ACK SOH STX SOH STX STX SOH STX EM SO WAN Miniport (IP)-WFP Native MAC Layer LightWeight Filter-0000 NUL ETX ACK SOH STX SOH STX STX SOH STX SO WAN Miniport (IP)-QoS Packet Scheduler-0000 NUL ETX ACK SOH STX SOH STX STX SOH STX ! SO WAN Miniport (IPv6)-WFP Native MAC Layer LightWeight Filter-0000 NUL ETX ACK SOH STX SOH STX STX SOH STX " SO WAN Miniport (IPv6)-QoS Packet Scheduler-0000 NUL ETX ACK SOH STX SOH STX STX SOH STX # SO WAN Miniport (Network Monitor)-WFP Native MAC Layer LightWeight Filter-0000 NUL ETX ACK SOH STX SOH STX STX SOH STX $ SO WAN Miniport (Network Monitor)-QoS Packet Scheduler-0000 NUL

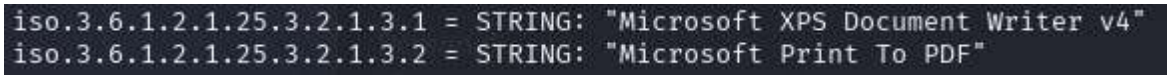
총 24개의 네트워크 인터페이스가 있으며 각각에 대한 정보를 확인할 수 있었습니다.

3. Shared Printers

OID 1.3.6.1.2.1.25.3 영역에서 시스템의 하드웨어 장치 정보를 확인해보겠습니다.



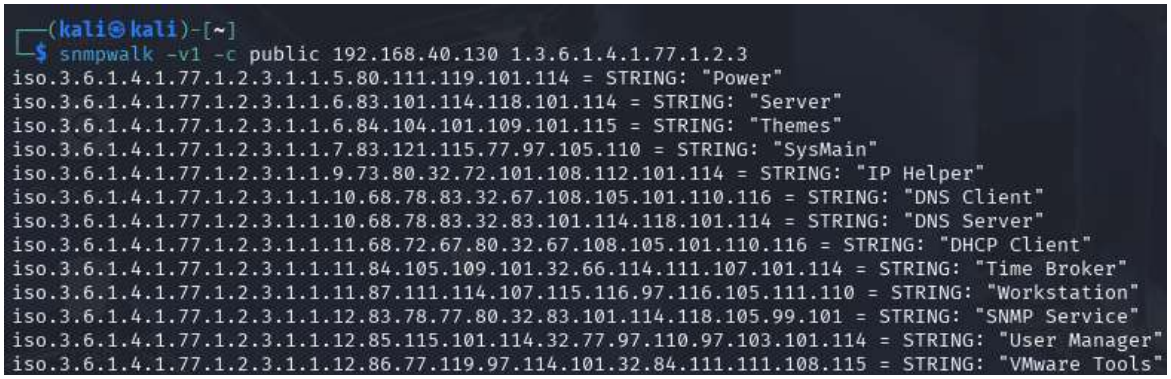
시스템에 설치된 프린터 2대 확인했습니다.



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

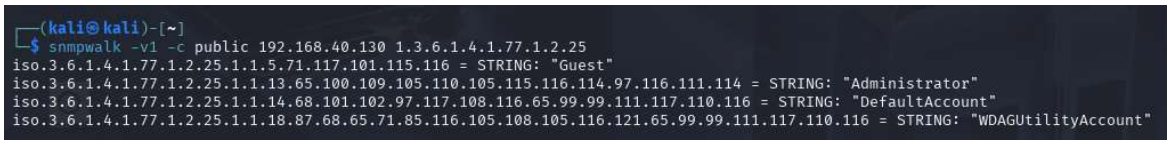
프린터 #2: "Microsoft Print To PDF" (가상 프린터)

4. Services



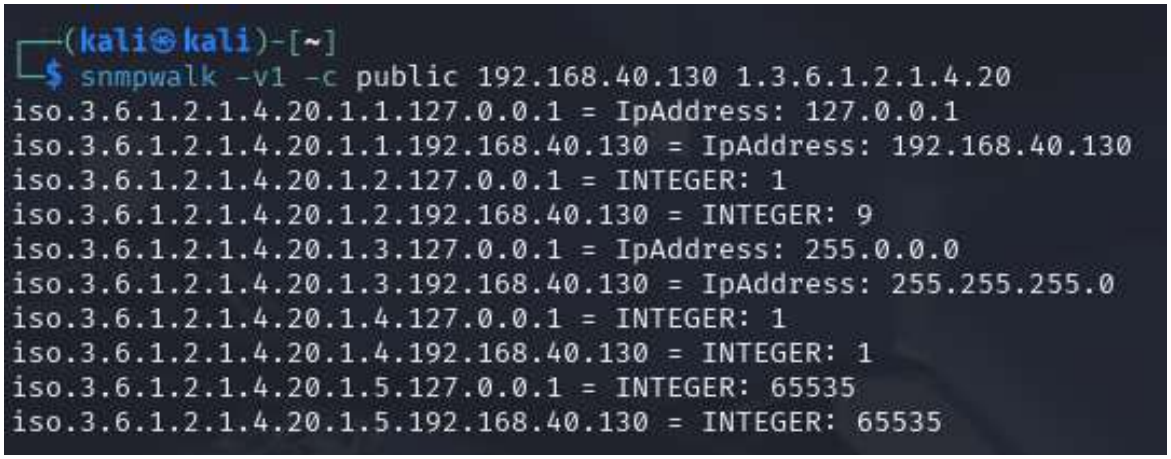
Victim(Windows Server)에서 실행중인 서비스 목록을 확인했습니다.

5. Accounts



Windows 시스템의 사용자 계정을 4개 확인했습니다.

6. TCP/IP Networks



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 패키스로 해당 호스트의MAC 주소를 직접 알아야 하는데 같은 로컬네트워크에 없기 때문에 발생한 문제였습니다.