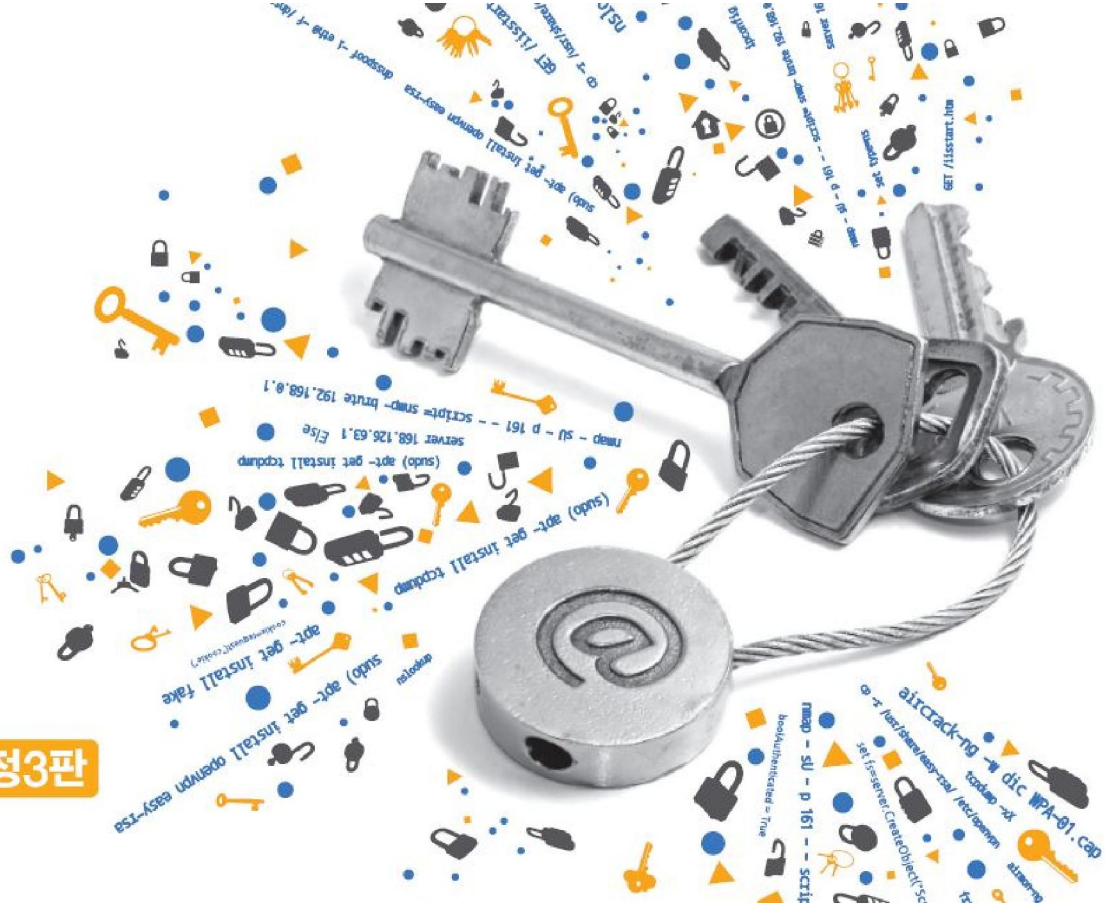
네트워크 해킹과 보안

개정3판

정보 보안 개론과 실습



Chapter 05 목록화

목차

IT COOKBOOK

학습목표

- 풋프린팅이 무엇인지 안다.
- 포트와 서비스의 관계를 이해한다.
- 다양한 포트 스캔 기술을 이해하고 실행할 수 있다.
- 운영체제, 방화벽, IDS를 탐지할 수 있다.
- 사용자, 공유 정보, 응용 프로그램 등에 대한 목록화를 이해한다.
- SNMP에 대해 이해하고 SNMP를 이용한 목록화를 수행할 수 있다.

1. 풋프린팅

1.1 풋프린팅에 대한 이해

■ 풋프린팅(Footprinting)

- 발자국을 살펴보는 일
- 공격 대상의 정보를 모으는 방법 중 하나

그림 5-1 풋프린팅의 개념

■ 사회 공학 기법(Social Engineering)

- 실제로 패스워드가 노출되는 사건의 대부분이 사회 공학에 의한 것
- 친구끼리 사용자 계정이나 패스워드 정보를 주고 받거나, 패스워드를 잊지 않으려고 수첩이나 컴퓨터 옆에 적어 놓은 것들을 이용하는 해킹

■ 해킹에 필요한 정보

- 침투하고자 하는 시스템의 사용자 계정
- 패스워드를 찾기 위한 계정을 사용하는 사람의 정보
- 게시판 이용
- 협력사나 계열사의 보안 조치 확인
- 주의사항 : 공격 대상 사이트를 직접 접속하는 것보다 유틸리티로 웹 사이트를 다운로드한 뒤 검색하는 것이 좋음.

그림 5-2 협력사의 보안 허점을 이용한 우회 침투

■ 스캔(Scan)

- 서비스를 제공하는 서버의 작동 여부와 서버가 제공하는 서비스를 확인하기 위한 작업
- 전화를 걸었을 때 한 쪽에서 '여보세요'라고 말하면 다른 쪽도 '여보세요'라고 말하며 서로를 확인하는 것과 같음.

그림 5-3 스캔의 기본 개념

2.2 ping

■ Ping(핑)

- 네트워크와 시스템이 정상적으로 작동하는지 확인하기 위한 간단한 유틸리티
- ICMP(Internet Control Message Protocol)를 사용하며, 기본적으로 TCP/IP 네트워크에서 사용

2.3 ICMP 스캔

■ ICMP를 이용해 공격 대상 시스템의 활성화 여부를 알아보는 방법

① Echo Request(Type 8)와 Echo Reply(Type 0) 이용하기

② Timestamp Request(Type 13)와 Timestamp Reply(Type 14) 이용하기

③ Information Request(Type 15)와 Information Reply(Type 16) 이용하기

④ ICMP Address Mask Request(Type 17)와 ICMP Address Mask Reply(Type 18) 이용하기

→ 가장 일반적인 방법은 Echo Request(Type 8)와 Echo Reply(Type 0)를 이용하는 것

■ 윈도우 실행 결과

① ICMP 패킷의 길이를 나타냄(윈도우는 32바이트, 유닉스나 리눅스는 56바이트)

② 공격 대상에서 보내온 ICMP Echo Reply 패킷의 크기

③ Echo Request 패킷을 보낸 후 Reply 패킷을 받기까지의 시간

④ TTL(Time To Live) 값

⑤ Request 패킷의 개수, Reply 패킷의 개수, 손실된 패킷의 개수

⑥ Request 패킷을 보낸 후 Reply 패킷이 오기까지의 시간 정보

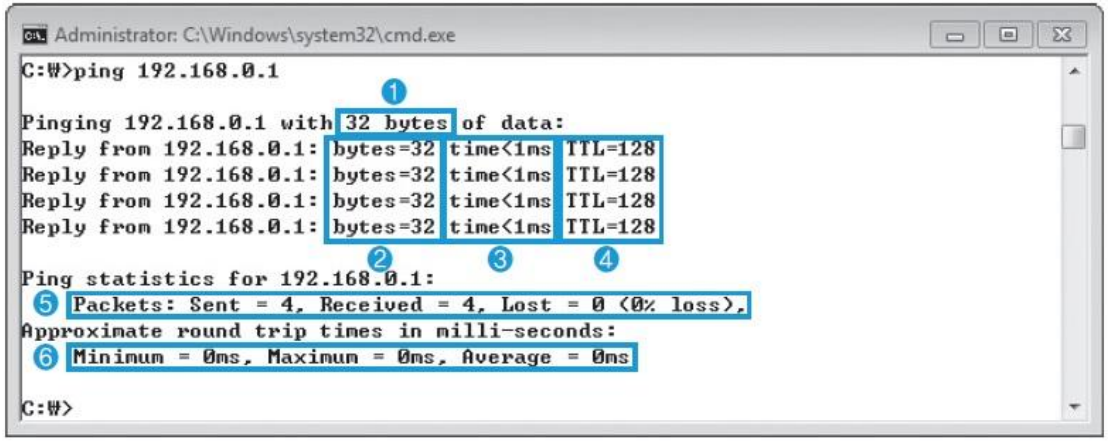


그림 5-4 윈도우 7 시스템에서 윈도우 2012 시스템으로 ping을 실행한 결과

■ 윈도우 실행 결과

표 5-1 운영체제별 TTL 값

운영체제	ICMP Request 패킷 TTL	ICMP Reply 패킷 TTL
리눅스 커널 2.6	64	64
리눅스 커널 2.2-2.4	255	64
리눅스 커널 2.0	64	64
우분투	128	128
FreeBSD	255	255
솔라리스	255	255
HP-UX	255	255
윈도우 95	32	32
윈도우 98	128	32
윈도우 NT	128	32
윈도우 서버 2003, 2008, 2012	128	128
윈도우 10	64	64

■ 우분투 실행 결과

- 리눅스는 중지 명령을 내리기 전까지 Request 패킷을 계속 보냄.

```
wishfree@ubuntu-14: ~
wishfree@ubuntu-14:~$ ping 192.168.0.100
PING 192.168.0.100 (192.168.0.100) 56(84) bytes of data.
64 bytes from 192.168.0.100: icmp_seq=1 ttl=128 time=0.311 ms
64 bytes from 192.168.0.100: icmp_seq=2 ttl=128 time=0.235 ms
64 bytes from 192.168.0.100: icmp_seq=3 ttl=128 time=0.186 ms
64 bytes from 192.168.0.100: icmp_seq=4 ttl=128 time=0.223 ms
^C
--- 192.168.0.100 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2998ms
rtt min/avg/max/mdev = 0.186/0.238/0.311/0.049 ms
wishfree@ubuntu-14:~$
```

그림 5-5 리눅스에서의 ping

■ ICMP Echo Request 패킷이 막혔을 때 이용할 수 있는 방법

① Timestamp Request 패킷 이용

② Information Request 패킷을 이용

③ ICMP Address Mask Request와 Reply 패킷을 이용

→ ICMP를 이용한 ping은 시스템 하나를 조사하기에 적절

표 5-2 운영체제별 Non Echo ICMP 패킷의 작동 여부

운영체제	Information	Timestamp	Address Mask
리눅스 커널 2.2-2.6	×	○	×
FreeBSD	×	○	×
솔라리스	×	○	○
HP-UX	○	○	×
AIX v4	○	○	×
윈도우 98	×	○	○
윈도우 NT sp4	×	×	×
윈도우 2000 이상	×	○	×

■ TCP Open 스캔

- TCP를 이용한 가장 기본적인 스캔

(a) 포트가 열린 경우 (b) 포트가 닫힌 경우

그림 5-6 TCP Open 스캔

■ TCP Open 스캔

- Reverse Ident : 세션을 성립한 상태에서 원격지 서버에서 데몬을 실행하고 있는 프로세스의 소유권자를 확인하기 위한 것
- 113번 포트는 사용자 인증을 위해 사용되지만, 이 서비스는 보통 중지되어 있음.

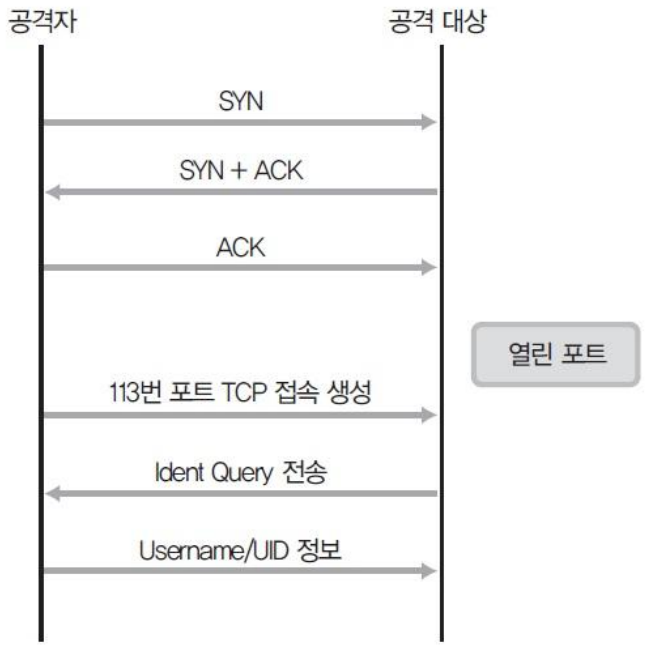
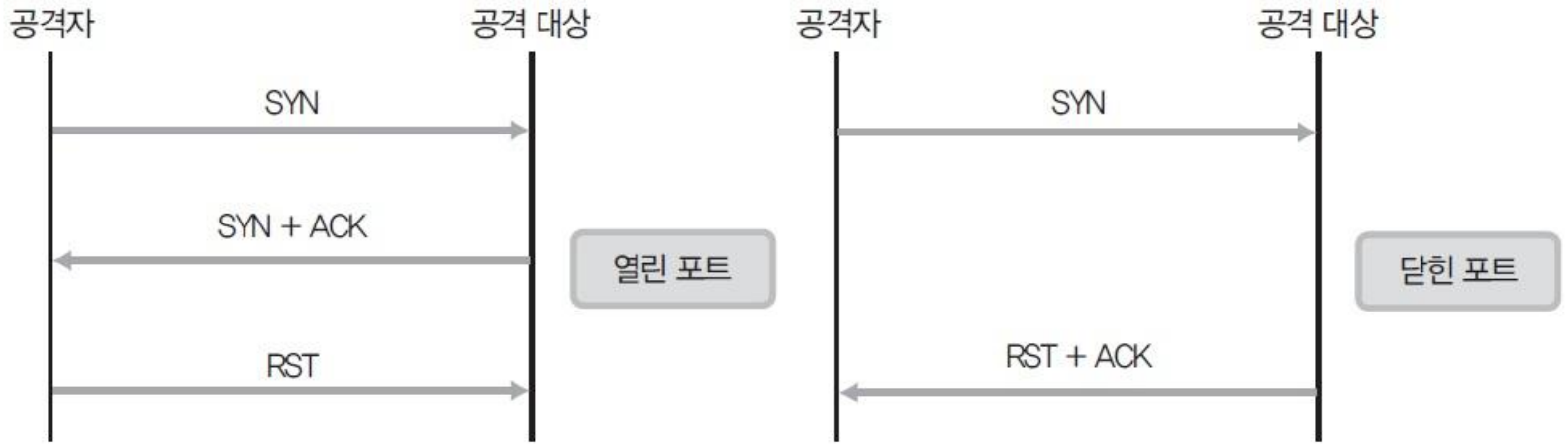


그림 5-7 TCP Open Ident 스캔

■ 스텔스(Stealth) 스캔

- 로그를 남기지 않는 것만이 아니라, 공격 대상을 속이고 자신의 위치를 숨기는 스캔 모두를 통칭
- 대표적인 경우로 TCP Half Open 스캔이 있음.



(a) 포트가 열린 경우 (b) 포트가 닫힌 경우

그림 5-8 TCP Half Open 스캔

■ 스텔스(Stealth) 스캔

- FIN(Finish) 스캔 : 포트가 열린 경우 응답이 없고, 닫힌 경우 RST 패킷이 돌아옴.
- NULL 스캔 : 플래그(Flag) 값을 설정하지 않고 보낸 패킷
- XMAS 스캔 : ACK, FIN, RST, SYN, URG 플래그 모두를 설정하여 보낸 패킷

(a) 포트가 열린 경우 (b) 포트가 닫힌 경우

그림 5-9 FIN, NULL, XMAS 스캔

■ ACK 패킷을 이용한 스캔

- 모든 포트에 ACK 패킷을 보낸 후 이에 대한 RST 패킷을 받아 분석
- 포트가 열린 경우 TTL 값이 64이하인 RST 패킷, 윈도우가 0이 아닌 임의의 값을 가진 RST 패킷이 돌아옴(닫힌 경우엔 TTL 값이 일정하게 큰 값이며, 윈도우 크기가 0인 RST 패킷).

■ TCP 패킷을 이용한 스캔

- 모든 시스템에 동일하게 적용되지 않으며, 많이 알려져서 거의 적용되지 않음.
- SYN 패킷을 이용한 스캔 방법은 세션을 성립하기 위한 정당한 패킷과 구별할 수 없기 때문에 아직도 유효하며 아주 효과적

■ TCP 단편화(Fragmentation)

- 크기가 20바이트인 TCP 헤더를 패킷 두 개로 나누어 보냄(첫 번째 패킷은 출발지와 도착지 IP주소, 두 번째 패킷에는 스캔하려는 포트 번호).
- 첫 번째 패킷은 TCP 포트에 대한 정보가 없어 방화벽을 통과하고, 두 번째 패킷은 출발지와 목적지 주소가 없어 방화벽을 지날 수 있음.

■ 시간차를 이용한 스캔

- 아주 짧은 시간 동안 많은 패킷을 보내는 방법 : 방화벽과 IDS 처리 용량의 한계를 넘기는 방법
- 아주 긴 시간 동안 패킷을 보내는 방법

■ 시간차에 의한 공격의 구분

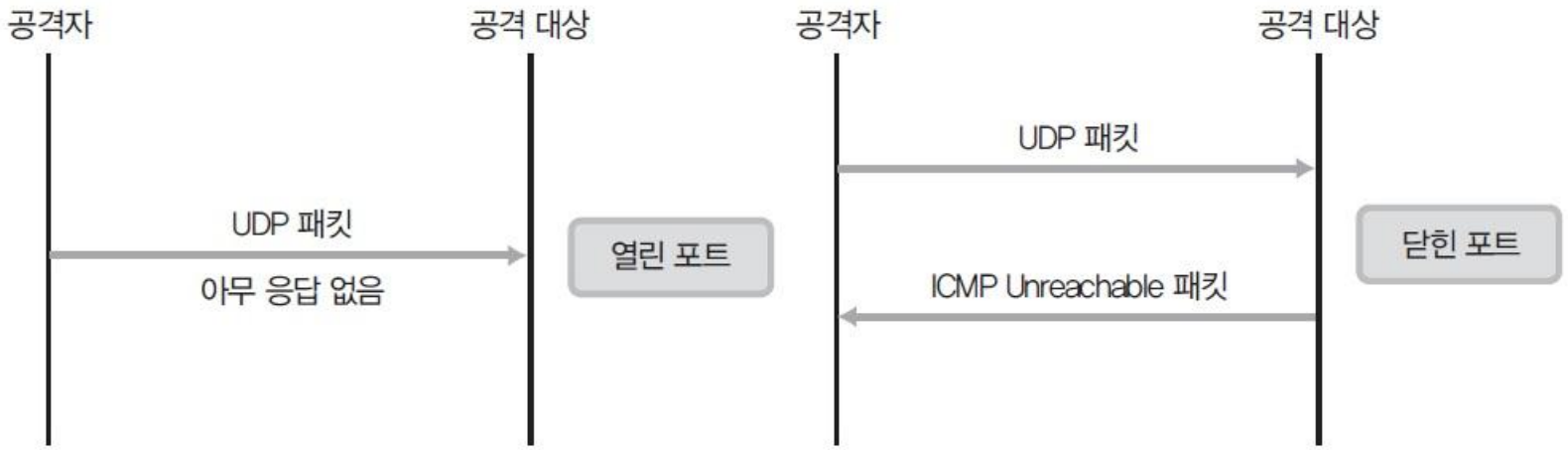
- Paranoid : 5분이나 10분 간격으로 패킷을 하나씩 보냄.
- Sneaky : WAN에서는 15초 단위로, LAN에서는 5초 단위로 패킷을 보냄.
- Polite : 패킷을 0.4초 단위로 보냄.
- Normal : 정상적인 경우
- Aggressive : 호스트에 대한 최대 타임아웃은 5분, 패킷당 1.25초까지 응답을 기다림.
- Insane : 호스트에 대한 최대 타임아웃은 75초, 패킷당 0.3초까지 응답을 기다림. 방화벽과 IDS의 네트워크 카드가 100Mbps 이상이 아니면 탐지하지 못함.

■ FTP 바운스(Bounce) 스캔

- 취약한 FTP 서버에서 PORT 명령어를 통해 다른 시스템의 포트 활성화 여부를 확인

■ UDP 스캔

- 포트가 닫힌 경우 공격 대상이 ICMP Unreachable 패킷을 보내지만, 열린 경우에는 보내지 않음(신뢰성이 떨어짐).



(a) 포트가 열린 경우 (b) 포트가 닫힌 경우

그림 5-10 UDP 포트 스캔

2. 스캔

실습 5-1 다양한 방법으로 스캔하기

실습환경
- 공격자 시스템 : 윈도우 7과 우분투 데스크탑 14
- 공격 대상 시스템 : 윈도우 서버 2012
- 필요 프로그램 : fping, hping3, sing, nmap

① 관련 툴 설치하고 사용법 익히기

- 우분투에서 제공하는 패키지 설치 툴인 'apt-get'을 이용해 설치
- apt-get은 기본적으로 root 권한으로 실행
- 일반 사용자 계정 권한의 쉘에서 실행할 때에는 apt-get 명령 앞에 sudo를 붙임.

2. 스캔

실습 **5-1** 다양한 방법으로 스캔하기

① 관련 툴 설치하고 사용법 익히기

- apt-get 사용법

실행 명령	내용
# apt-get update	패키지 캐시 갱신
# apt-cache search 〈패키지명〉	원하는 패키지 찾기
# apt-cache show 〈패키지명〉	원하는 패키지를 찾은 다음 정보 출력
# apt-get install 〈패키지명〉	개별 패키지 설치
# apt-get --reinstall install 〈패키지명〉	설치한 패키지에 이상이 있을 경우 재설치
# apt-get remove 〈패키지명〉	패키지 삭제
# apt-get --purge remove 〈패키지명〉	설정 파일까지 모두 삭제
# dpkg -l	설치된 패키지 확인

① 관련 툴 설치하고 사용법 익히기

- fping 패키지 검색

sudo apt-cache search fping*

```
wishfree@ubuntu-14: ~
wishfree@ubuntu-14:~$ sudo apt-cache search fping*
nagios-plugins-standard - Plugins for nagios compatible monitoring systems
fping - sends ICMP ECHO_REQUEST packets to network hosts
hobbit-plugins - plugins for the Xymon network monitor
oping - sends ICMP_ECHO requests to network hosts
wishfree@ubuntu-14:~$
```

그림 5-11 fping 패키지 찾기

① 관련 툴 설치하고 사용법 익히기

- fping 확인

sudo apt- cache show fping

```
wishfree@ubuntu-14: ~
wishfree@ubuntu-14:~$ sudo apt-cache show fping
[sudo] password for wishfree:
Package: fping
Priority: optional
Section: universe/net
Installed-Size: 117
Maintainer: Ubuntu Developers <ubuntu-devel-discuss@lists.ubuntu.com>
Original-Maintainer: Anibal Monsalve Salazar <anibal@debian.org>
Architecture: amd64
Version: 3.8-1
Depends: libc6 (>= 2.15)
Filename: pool/universe/f/fping/fping_3.8-1_amd64.deb
Size: 30722
MD5sum: 85adb4d1a41d84416a2b790132dc0901
SHA1: dc221440cc8e80be385022a3d941a555b6a9ca6a
SHA256: 8f28e9900659f4e17113e09c9a1ea46815bc07933ee9d406621c8a227f63562b
Description-en: sends ICMP ECHO_REQUEST packets to network hosts
 fping is a ping like program which uses the Internet Control Message Protocol
 (ICMP) echo request to determine if a target host is responding.  fping
 differs from ping in that you can specify any number of targets on the command
 line, or specify a file containing the lists of targets to ping.  Instead of
 sending to one target until it times out or replies, fping will send out a
 ping packet and move on to the next target in a round-robin fashion.
Description-md5: 39b9ab73fb3b3bedff57b40efd2819fd
Homepage: http://www.fping.org/
Bugs: https://bugs.launchpad.net/ubuntu/+filebug
Origin: Ubuntu

wishfree@ubuntu-14:~$
```

그림 5-12 fping 내용 확인

① 관련 툴 설치하고 사용법 익히기

- fping 설치

sudo apt-get install fping

```
wishfree@ubuntu-14: ~
wishfree@ubuntu-14:~$ sudo apt-get install fping
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libntdb1 linux-headers-4.2.0-27 linux-headers-4.2.0-27-generic
  linux-image-4.2.0-27-generic linux-image-extra-4.2.0-27-generic python-ntdb
Use 'apt-get autoremove' to remove them.
The following NEW packages will be installed:
  fping
0 upgraded, 1 newly installed, 0 to remove and 3 not upgraded.
Need to get 0 B/30.7 kB of archives.
After this operation, 120 kB of additional disk space will be used.
Selecting previously unselected package fping.
(Reading database ... 246047 files and directories currently installed.)
Preparing to unpack .../archives/fping_3.8-1_amd64.deb ...
Unpacking fping (3.8-1) ...
Processing triggers for man-db (2.6.7.1-1ubuntu1) ...
Setting up fping (3.8-1) ...
wishfree@ubuntu-14:~$
```

그림 5-13 fping 설치

② fping을 이용해 스캔하기

- 스캔 전에 네트워크 시스템 목록을 확인할 때 사용
- -q : ICMP Request와 Reply를 숨김.
- -a : 활성화되어 있는 시스템을 보여줌.
- -s : 스캔이 끝난 후 결과를 정리해서 보여줌.

② fping을 이용해 스캔하기

- fping 실행

fping -q -a -s -g 192.168.0.0/24

```
root@ubuntu-14: /
root@ubuntu-14:/# fping -q -a -s -g 192.168.0.0/24
192.168.0.1
192.168.0.100
192.168.0.200

     254 targets
       3 alive
     251 unreachable
       0 unknown addresses

     251 timeouts (waiting for response)
    1007 ICMP Echos sent
       3 ICMP Echo Replies received
     952 other ICMP received

 0.02 ms (min round trip time)
 0.19 ms (avg round trip time)
 0.30 ms (max round trip time)
       26.963 sec (elapsed real time)

root@ubuntu-14:/#
```

그림 5-14 fping 실행

③ nmap을 이용해 스캔하기

- 포트 스캔을 위해 흔하게 사용하는 가장 강력한 툴
- -sT 옵션 : TCP Open 스캔

nmap - sT 192.168.0.1

```
root@ubuntu-14: /
root@ubuntu-14:/# nmap -sT 192.168.0.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-07-09 14:28 KST
Nmap scan report for 192.168.0.1
Host is up (0.00012s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49160/tcp open  unknown
MAC Address: 00:16:D3:CA:85:67 (Wistron)

Nmap done: 1 IP address (1 host up) scanned in 2.37 seconds
root@ubuntu-14:/#
```

그림 5-15 nmap Open 스캔

③ nmap을 이용해 스캔하기

- -sS 옵션 : SYN 스텔스 스캔

nmap - sS 192.168.0.1

```
root@ubuntu-14: /
root@ubuntu-14:/# nmap -sS 192.168.0.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-07-09 14:28 KST
Nmap scan report for 192.168.0.1
Host is up (0.00023s latency).
Not shown: 987 closed ports
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown
49158/tcp open  unknown
49160/tcp open  unknown
MAC Address: 00:16:D3:CA:85:67 (Wistron)

Nmap done: 1 IP address (1 host up) scanned in 47.25 seconds
root@ubuntu-14:/#
```

그림 5-16 nmap TCP SYN 스캔

③ nmap을 이용해 스캔하기

- -p 옵션 : 특정 포트 스캔

nmap - sF - p 80,139 192.168.0.1

```
root@ubuntu-14: /
root@ubuntu-14:/# nmap -sF -p 80,139 192.168.0.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-07-09 14:31 KST
Nmap scan report for 192.168.0.1
Host is up (0.00026s latency).
PORT    STATE         SERVICE
80/tcp  open|filtered http
139/tcp open|filtered netbios-ssn
MAC Address: 00:16:D3:CA:85:67 (Wistron)

Nmap done: 1 IP address (1 host up) scanned in 1.45 seconds
root@ubuntu-14:/#
```

그림 5-17 nmap FIN 스캔

③ nmap을 이용해 스캔하기

- -f 옵션 : 스캔하고자 하는 목적지 포트를 숨겨서 방화벽을 통과하기 위한 패킷
- 처음 패킷이 16바이트, 뒤의 패킷이 4바이트로 나뉨
- 윈도우 서버 2012를 대상으로 수행할 경우 해당 패킷은 필터됨.

nmap -f - sS 192.168.0.100

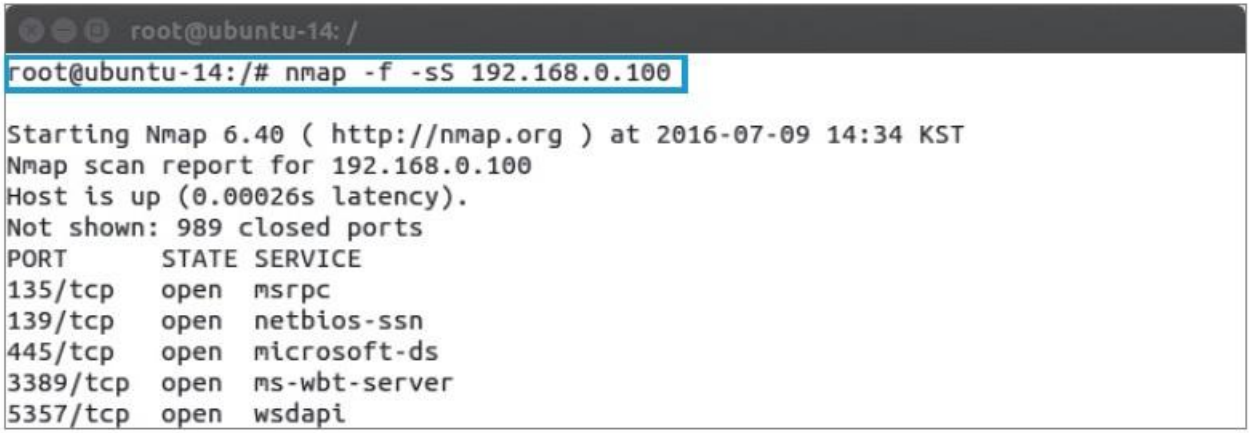


그림 5-18 nmap fragmentation 스캔

③ nmap을 이용해 스캔하기

표 5-3 nmap 스캔 옵션

옵션 종류	내용
-sT	connect( ) 함수를 이용한 Open 스캔
-sS	세션을 성립시키지 않는 SYN 스캔
-sF	FIN 패킷을 이용한 스캔
-sN	NULL 패킷을 이용한 스캔
-sX	XMAS 패킷을 이용한 스캔
-sP	ping을 이용한 호스트 활성화 여부 확인
-sU	UDP 포트 스캔
-sR	RPC 포트 스캔
-sA	ACK 패킷에 대한 TTL 값의 분석
-sW	ACK 패킷에 대한 윈도우 크기 분석
-b	FTP 바운스 스캔

③ nmap을 이용해 스캔하기

표 5-4 nmap 실행 옵션

옵션 종류	내용
-f	스캔할 때 방화벽을 통과할 수 있도록 패킷을 조각냄
-v	스캔의 세부 사항 표시
-P0	스캔 전 ping을 하지 않고 ICMP Echo Request를 허용하지 않는 호스트에 대한 스캔을 할 때 설정
-PT	ping의 대용으로 ICMP 패킷을 이용하지 않고, TCP 패킷을 이용하여 해당 시스템이 작동 중인지 검사
-PS	TCP의 SYN 패킷만을 보내 시스템 활성화 여부를 검사
-PI	시스템 활성화 여부를 ICMP로 검사
-PB	TCP와 ICMP 둘 다 사용해서 호스트 활성화 여부를 검사
-O	시스템 운영체제를 추정
-I	Ident 프로토콜(RFC 1413)을 사용해 열려 있는 프로세스가 어떤 사용자에 의한 것인지 검사
-n	DNS 룩업(lookup)을 하지 않음
-R	DNS 룩업(lookup)을 함
-T	시간차를 이용한 스캔을 하기 위한 것으로 Paranoid, Sneaky, Polite, Normal, Aggressive, Insane이 각각 0부터 5까지의 숫자를 가짐

③ nmap을 이용해 스캔하기

- 윈도우 nmap은 운영체제의 종류, 상대방 시스템의 MAC 주소 등 네트워크 상황에 따라 수집 가능한 다량의 정보를 얻을 수 있음.

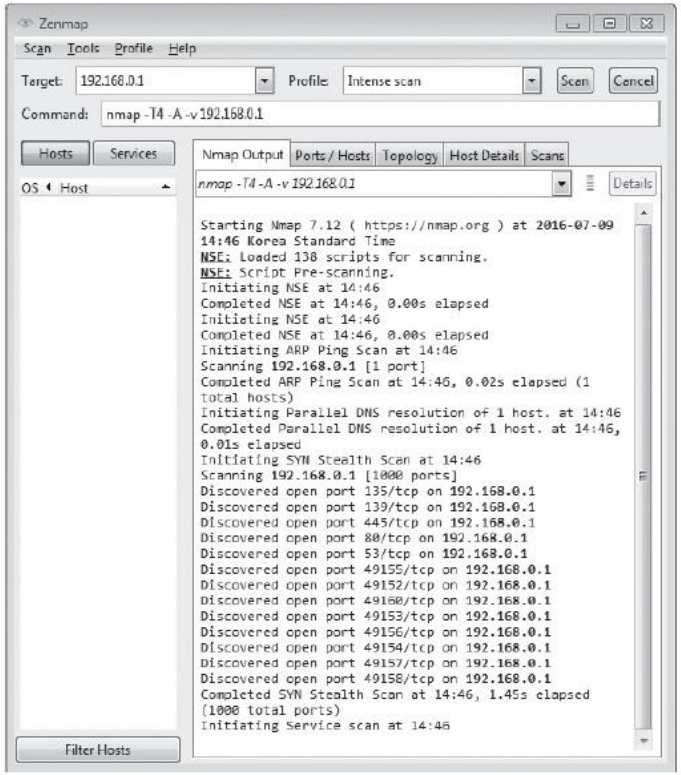


그림 5-19 윈도우용 nmap 실행 결과

■ 배너 그래빙(Banner Grabbing)

- 상대 시스템의 운영체제를 확인하는 가장 기본적인 방법
- 텔넷처럼 원격지 시스템에 로그인을 하면 뜨는 안내문과 비슷한 배너를 확인하는 기술

그림 5-20 텔넷 배너 그래빙

실습 5-2 배너 그래빙하기

실습환경 • 공격자 시스템 : 우분투 데스크탑 14
• 스캔 대상 시스템 : 우분투 서버 16

① FTP에 대해 배너 그래빙하기

telnet 192.168.0.2 21

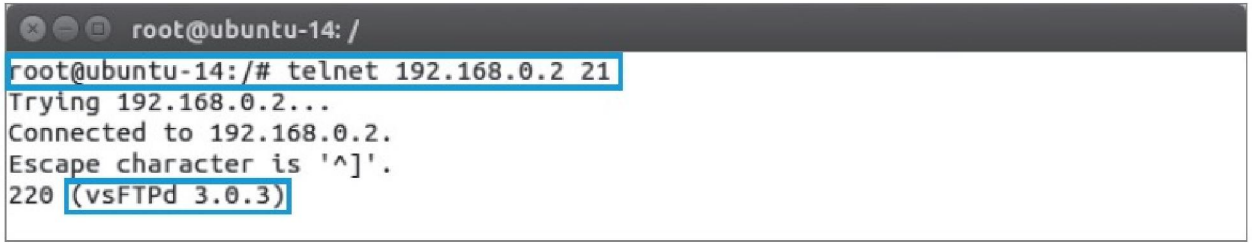


그림 5-21 FTP 포트에 대한 텔넷

ftp 192.168.0.2

그림 5-22 FTP 포트 접속

② SMTP 포트에 대해 배너 그래빙하기

telnet 192.168.0.2 25

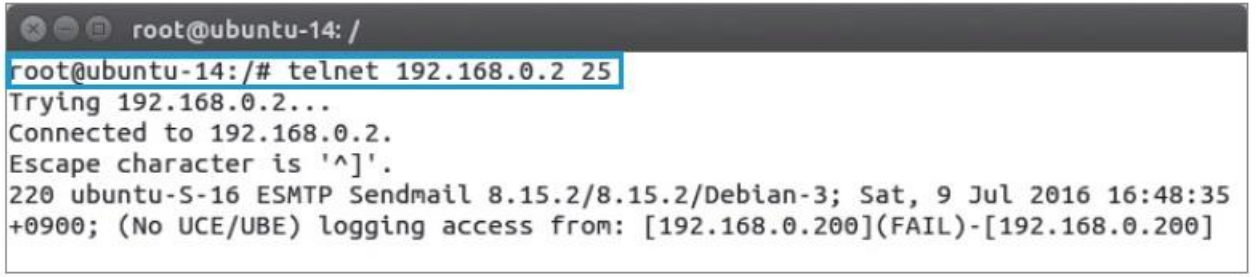


그림 5-23 SMTP 포트에 대한 텔넷

telnet 127.0.0.1 22

telnet 127.0.0.1 110

telnet 127.0.0.1 143

② SMTP 포트에 대해 배너 그래빙하기

telnet 192.168.0.1 80

GET /iisstart.htm

```
root@ubuntu-14: /
root@ubuntu-14:/# telnet 192.168.0.1 80
Trying 192.168.0.1...
Connected to 192.168.0.1.
Escape character is '^]'.

GET /iisstart.htm
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Strict//EN" "http://www.w3.org/TR/x
html1/DTD/xhtml1-strict.dtd">
<html xmlns="http://www.w3.org/1999/xhtml">
<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<title>IIS Windows Server</title>
<style type="text/css">
<!--
body {
        color:#000000;
```

그림 5-24 HTTP 동작 확인

■ TCP/IP 반응 살펴보기

- FIN 스캔 이용 : 적용되는 운영체제는 윈도우, BSD, Cisco, IRIS 등
- 세션 연결 시 TCP 패킷의 시퀀스 넘버 생성을 관찰
  - 윈도우 : 시간에 따른 시퀀스 넘버 생성
  - 리눅스 : 완전한 랜덤
  - FreeBSD, Digital-Unix, IRIX, 솔라리스 : 시간에 따른 랜덤한 증분

■ Netcraft 이용하기

- 공격 대상의 운영체제에 대한 다양한 정보를 보여줌.

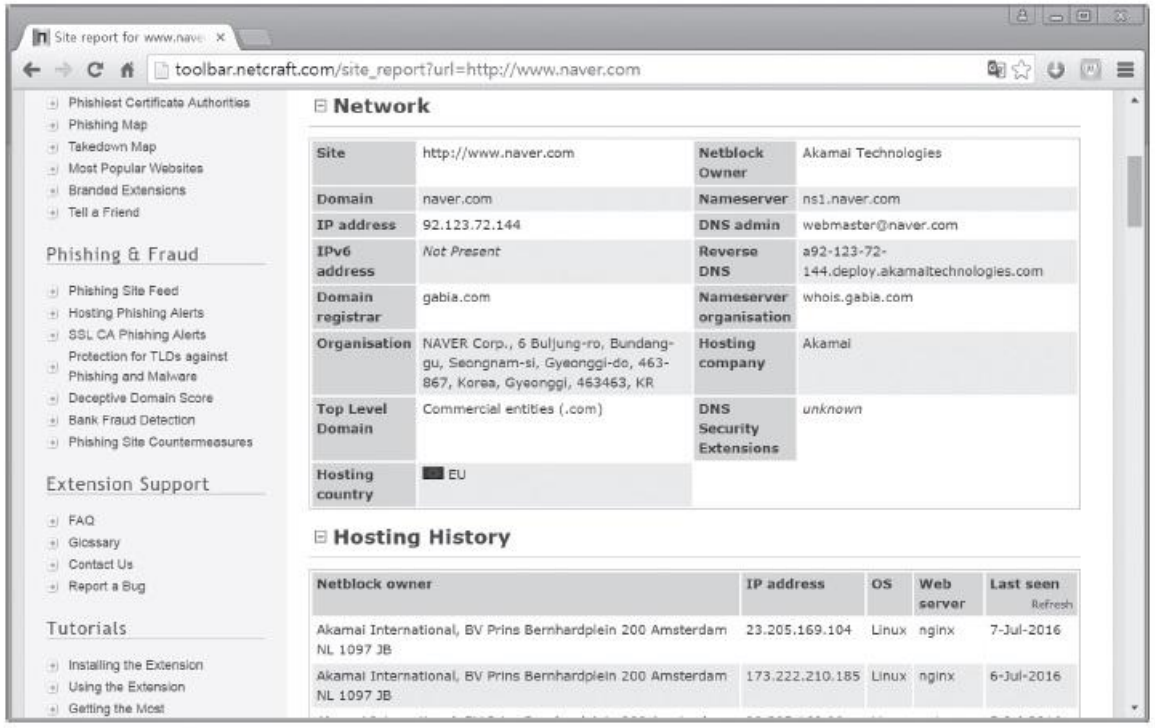


그림 5-26 Netcraft 사이트에 결과 확인

■ 방화벽

- 침입자를 차단하는 1차 방어선
- 접속에 대한 허용과 차단을 결정
- 침입 탐지 시스템(Intrusion Detection System, IDS) : 방화벽이 막을 수 없거나 차단에 실패한 공격을 탐지하여 관리자에게 알려주는 역할

■ 방화벽 탐지

- 방화벽 설치 여부를 알 수 있는 가장 손쉬운 방법은 traceroute
- Traceroute를 실행했을 때 *만으로 표시되는 곳이 라우팅에서 필터링 해주고 있거나 방화벽이 존재하는 것

```
root@ubuntu-14: /
root@ubuntu-14:/# traceroute www.google.com
traceroute to www.google.com (59.18.46.251), 30 hops max, 60 byte packets
 1  192.168.0.1 (192.168.0.1)  0.199 ms * *
 2  * * *
 3  192.168.137.1 (192.168.137.1)  0.573 ms * *
 4  210.108.84.1 (210.108.84.1)  1.239 ms  1.558 ms  1.980 ms
 5  210.108.84.254 (210.108.84.254)  3.619 ms  3.600 ms  3.586 ms
 6  211.51.39.17 (211.51.39.17)  3.574 ms  3.952 ms  3.853 ms
 7  121.162.167.53 (121.162.167.53)  3.843 ms  3.831 ms  3.822 ms
 8  * * *
 9  112.188.53.193 (112.188.53.193)  4.234 ms  2.992 ms  2.982 ms
10  112.174.59.53 (112.174.59.53)  4.408 ms  4.397 ms  4.390 ms
11  112.174.7.126 (112.174.7.126)  3.200 ms  2.871 ms  2.839 ms
12  * * *
13  * * *
14  * * *
15  * * *
```

그림 5-27 방화벽이 있는 경우의 traceroute 결과

■ firewalk(파이어워크)

- 방화벽의 ACL(Access Control List)을 알아내는 방법

■ firewalk 원리

- 방화벽이 탐지되면 방화벽까지의 TTL보다 1만큼 더 큰 TTL 값을 생성하여 보냄.
- 방화벽이 패킷을 차단할 경우, 아무 패킷도 돌아오지 않음
- 방화벽이 패킷을 그대로 보내면 패킷은 다음 라우터에서 사라지고 라우터는 traceroute 과정처럼 ICMP Time Exceeded 메시지(Type 11)를 보냄.
- 공격자는 ICMP Time Exceeded 메시지 여부를 받은 포트에 대해 열린 포트임을 추측할 수 있음.

■ 방화벽이 닫힌 포트에 패킷을 보낸 경우

- 응답 패킷이 돌아오지 않음.

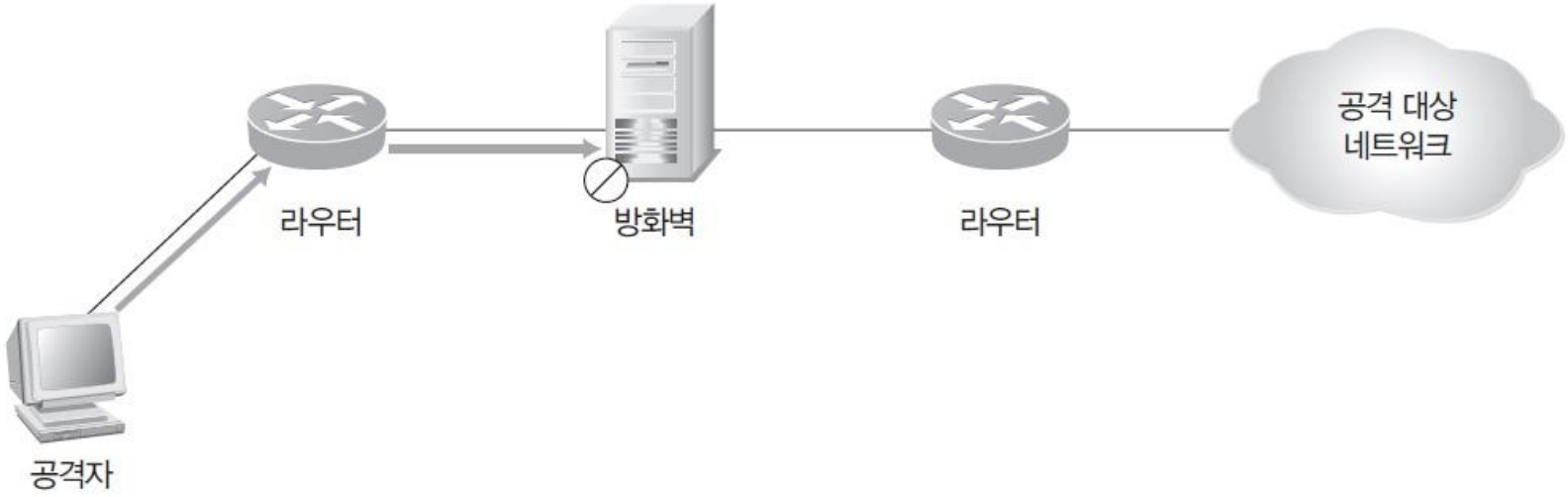


그림 5-28 방화벽의 포트가 닫힌 경우 firewalk의 동작

■ 방화벽이 열린 포트에 패킷을 보낸 경우

- 다음 라우터까지 전달된 후 ICMP Time Exceeded 메시지가 돌아옴.

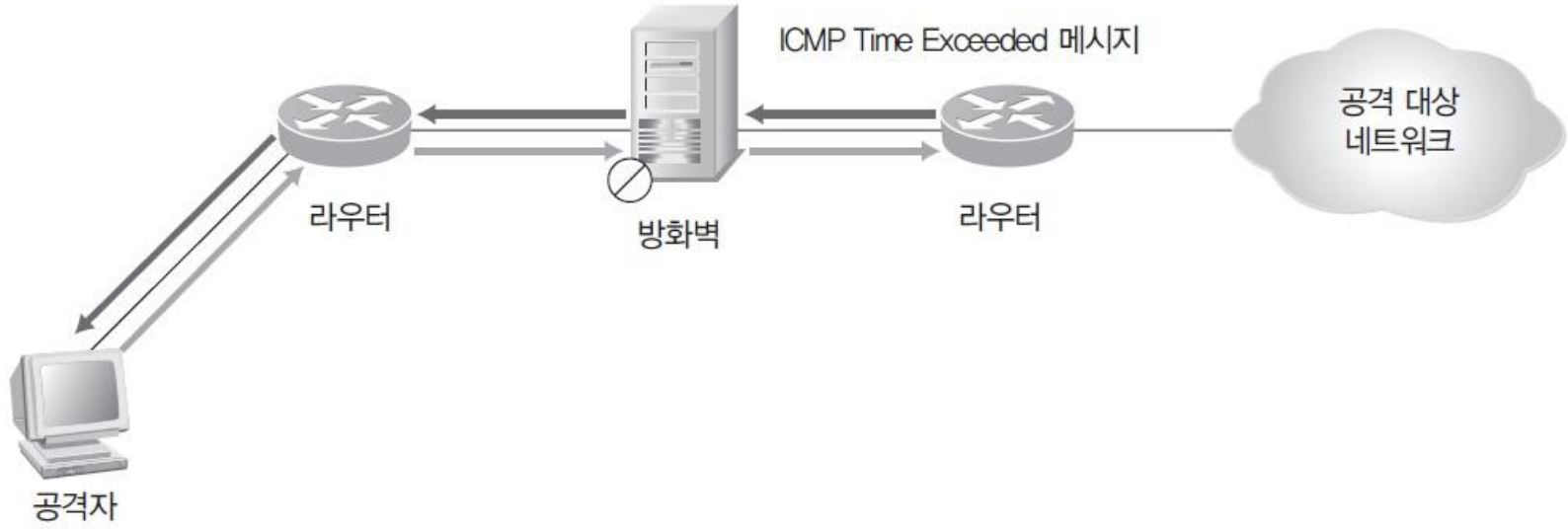


그림 5-29 방화벽 포트가 열린 경우 firewalk의 동작

■ SNMP(Simple Network Management Protocol)

- 중앙 집중적인 관리 툴의 표준 프로토콜

■ SNMP 소개

- SNMP 버전 1
  - 1988년 IAB에서 표준화 작업을 거쳐 SGMP(Simple Gateway Monitoring Protocol)를 발전시켜 만든 것
  - 보안 기능이 없어 해당 네트워크 장비의 모든 정보를 얻어낼 수 있음.
- SNMP 버전 2
  - 1993년 PDU(Protocol Data Unit) 타입을 정의할 수 있고, DES와 MD5를 이용한 보안 기능을 추가하여 만듦.
- SNMP 버전 3
  - 1999년 SNMP 버전 2에 인증 기능을 더함.

■ SNMP 구성 요소

- 관리 시스템과 관리 대상(Agent)으로 나뉨.
- 에이전트의 구성
  - SNMP(Simple Network Management Protocol) : 전송 프로토콜
  - MIB(Management Information Base) : 관리할 개체의 집합
  - SMI(Structure of Management Information) : 관리 방법
- 관리 시스템과 에이전트 통신의 최소 일치 사항
  - 버전, 커뮤니티, PDU 타입

표 5-5 SNMP의 PDU 타입에 대한 함수

PDU 타입	함수
0	Get Request
1	Get Next Request
2	Set Request
3	Get Response
4	Trap

■ 관리 시스템과 에이전트 통신

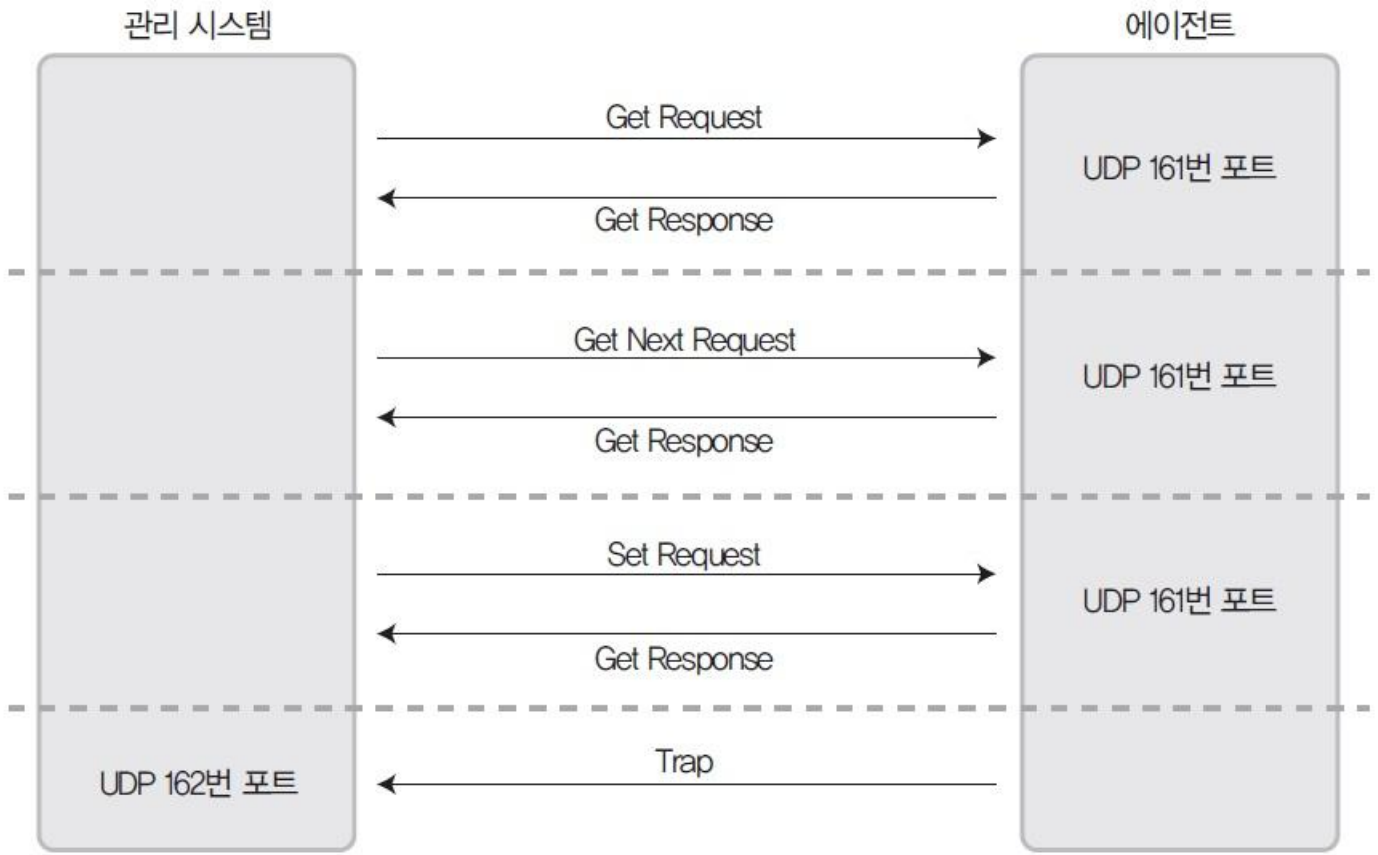


그림 5-30 SNMP 함수의 동작

■ 관리 시스템과 에이전트 통신

- Get Request : 관리 시스템이 특정 변수 값을 읽음.
- Get Next Request : 관리 시스템이 이미 요청한 변수 다음의 변수 값을 요청
- Set Request : 관리 시스템이 특정 변수 값의 변경을 요청
- Get Response : 에이전트가 관리 시스템에 해당 변수 값을 전송
- Trap : 에이전트의 특정 상황을 관리 시스템에 알림.

표 5-6 Trap 메시지 목록

번호	메시지	내용
0	Cold Start	에이전트를 초기화
1	Warm Start	에이전트를 설정의 변화 없이 초기화
2	Link Down	에이전트 통신 연결의 링크 하나가 끊어짐
3	Link Up	에이전트 통신 연결의 링크 하나가 연결됨
4	Authentication Failure	관리 시스템으로부터의 커뮤니티가 일치하지 않음
5	Egp Neighbor Loss	EGP(Exterior Gateway Protocol)의 상태가 변함
6	Enterprise Specific	벤더별 특정한 코드 값의 Trap

■ MIB

- 관리자가 조회하거나 설정할 수 있는 개체들의 데이터베이스
- 개체별로 트리 형식 구조를 이룸.

표 5-7 SNMP의 MIB 목록

목록	내용
SNMP	SNMP에 대한 정보 그룹
System	시스템의 상태에 대한 정보 그룹으로, 마지막으로 부팅한 시각, 시스템 위치 등이 해당됨
Interface	인터페이스 그룹은 모든 시스템에서 필수 사항으로, 시스템의 인터페이스 개수, 상태 등이 해당됨
AT	Address Translation 그룹으로, 각 인터페이스별 네트워크 주소 해석에 대한 정보 등이 해당됨
IP	IP 패킷의 fragmentation, 패킷의 재조합 상태 등이 해당됨
ICMP	ICMP 오류 패킷의 수, 전송 불가 패킷 수 등이 해당됨
TCP	TCP 접속에 대한 상태 정보로, 이 상태 정보는 접속이 끝남과 동시에 소멸됨
UDP	전송된 UDP 패킷 수, 수신된 UDP 패킷 개수, 열린 포트 등의 정보가 해당됨
EGP	EGP를 유지 관리하기 위한 정보 그룹
Transmission	각 인터페이스별 전송에 대한 정보

■ SMI

- 표준에 적합한 MIB를 생성하고 관리하는 기준(관리 정보 구조)

■ OID

- MIB를 생성하려면 OID를 지정받아야 함(IP 주소와 유사한 표기법 사용)
- 각 제조업체나 기관은 특정 번호를 할당받고 이 번호를 생산한 장비에 부여

■ OID

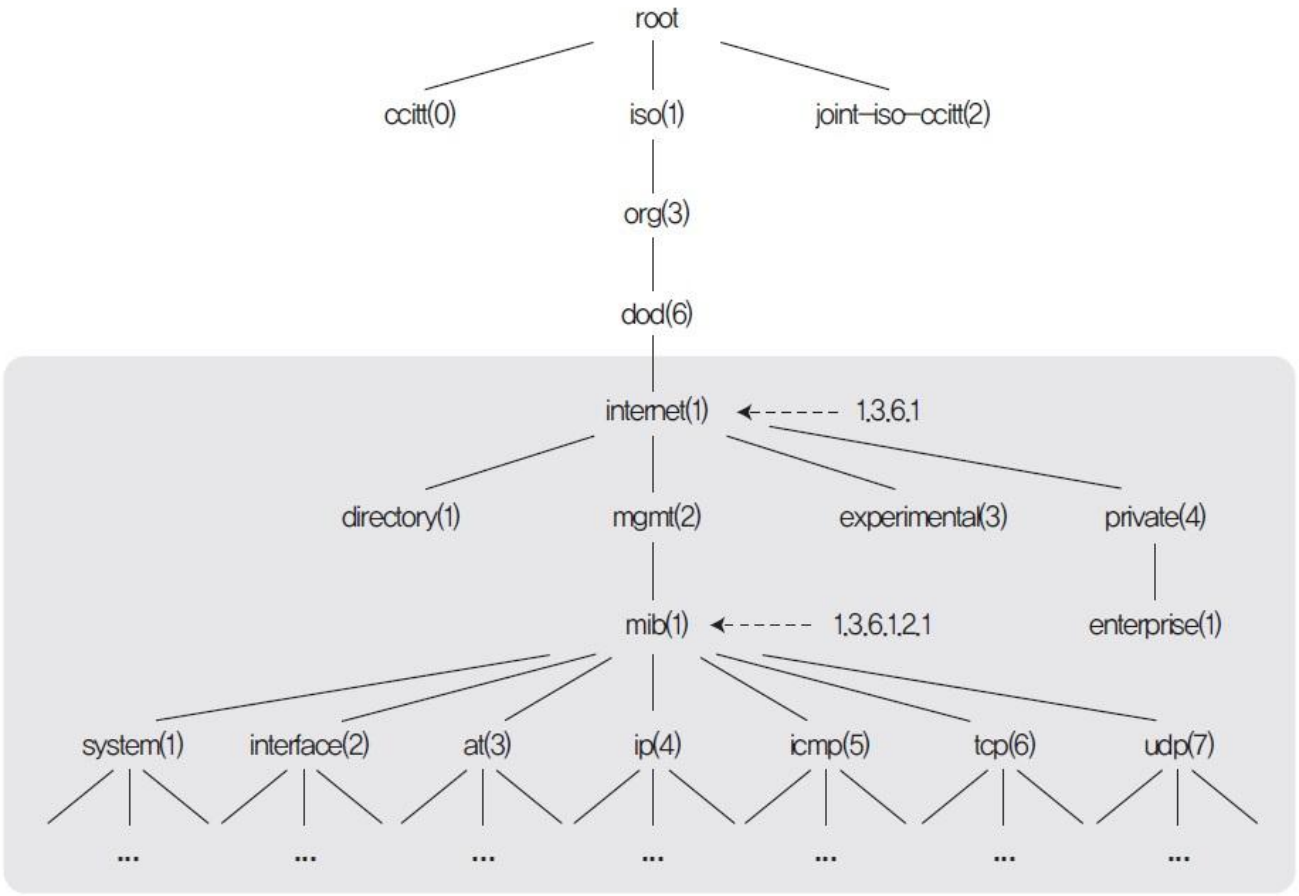


그림 5-31 OID 계층

■ SNMP의 취약점

- 기본적으로 누구라도 SNMP의 MIB정보를 볼 수 있음.
- 패킷이 UDP로 전송되어 연결의 신뢰도가 낮음.
- 데이터가 암호화되지 않은 평문으로 전송되어 스니핑 가능

실습 5-3 SNMP를 이용해 정보 수집하기

실습환경
- 공격자 시스템 : 우분투 데스크탑 14
- 공격 대상 시스템 : 윈도우 서버 2012
- 필요 프로그램 : snmpwalk

① SNMP 설치하기

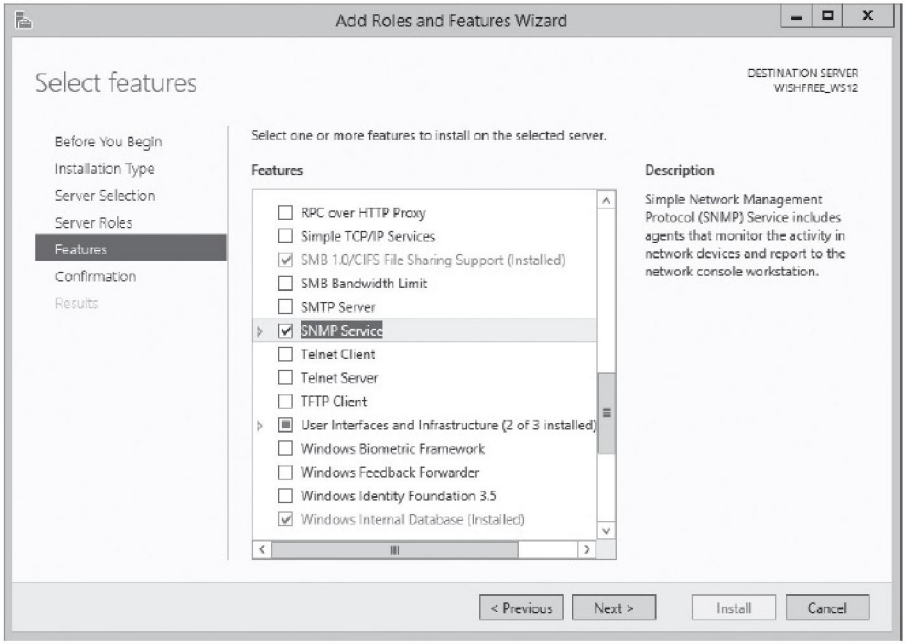


그림 5-32 SNMP 설치

② SNMP Community String 설정하기

- [Properties] 메뉴에서 [Security] 탭의 <Add>버튼을 클릭
- 권한은 'READ ONLY', 커뮤니티 이름은 'public'으로 입력

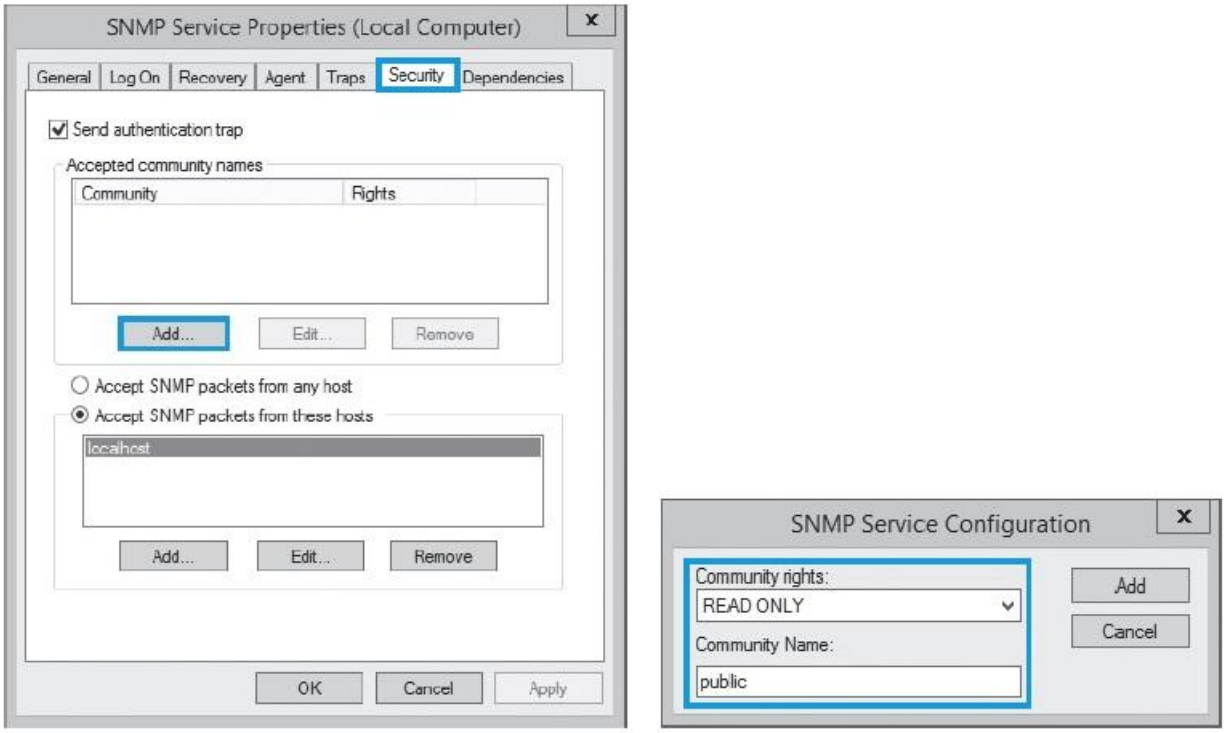


그림 5-34 SNMP 서비스의 [Security] 탭에서 커뮤니티 등록

② SNMP Community String 설정하기

- 'Accept SNMP packets from any host'를 체크하여 커뮤니티 등록

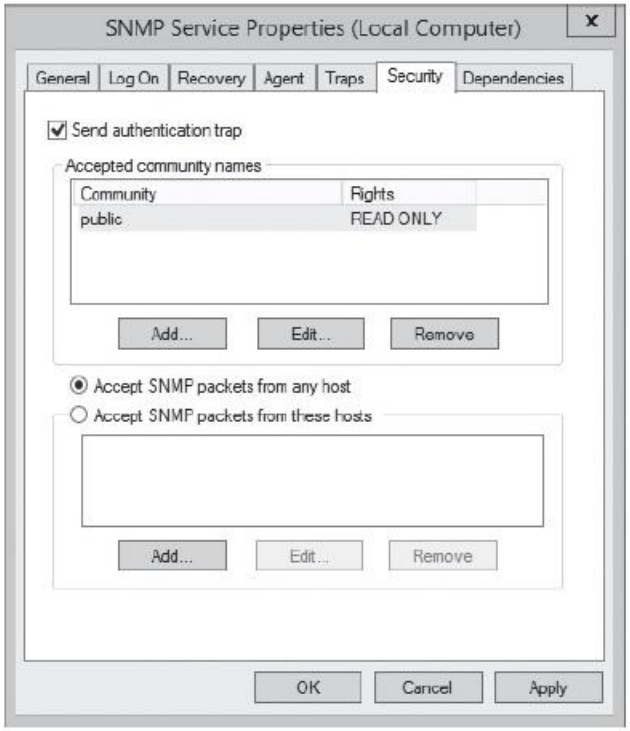


그림 5-35 커뮤니티 등록 후의 SNMP 속성 창

③ snmpwalk 설치하기

(sudo) apt- get install snmp

④ SNMP 스캐닝하기

- SNMP 서비스 포트 161가 열려 있는지 확인

nmap - sU - p 161 192.168.0.1

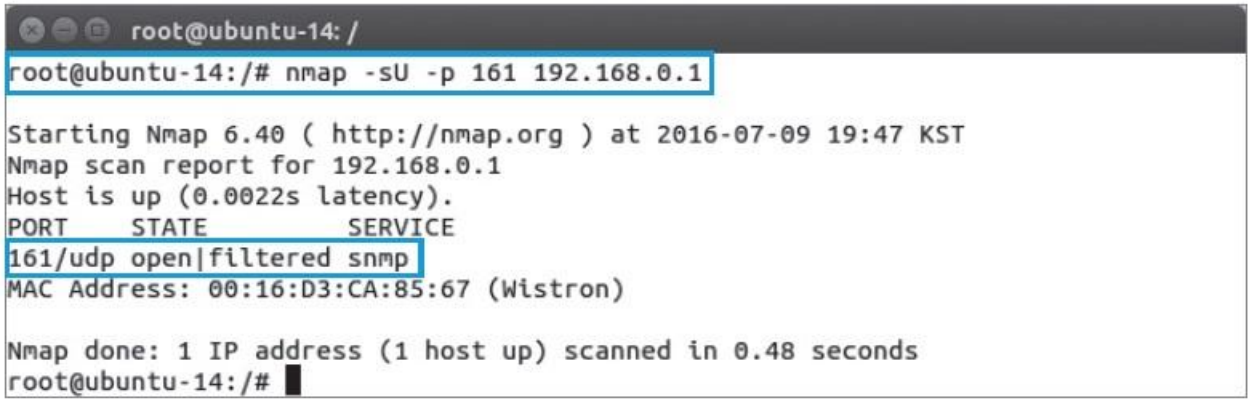


그림 5-36 NMAP을 통해 SNMP 서비스 포트의 Open 여부 확인

③ SNMP 스캐닝하기

- nmap로 Community String 크랙

nmap - sU - p 161 - - script= snmp- brute 192.168.0.1

```
root@ubuntu-14: /
root@ubuntu-14:/# nmap -sU -p 161 --script=snmp-brute 192.168.0.1

Starting Nmap 6.40 ( http://nmap.org ) at 2016-07-09 19:49 KST
Nmap scan report for 192.168.0.1
Host is up (0.00027s latency).
PORT    STATE         SERVICE
161/udp open|filtered snmp
| snmp-brute:
|_  public - Valid credentials
MAC Address: 00:16:D3:CA:85:67 (Wistron)

Nmap done: 1 IP address (1 host up) scanned in 1.28 seconds
root@ubuntu-14:/#
```

그림 5-37 NMAP을 통해 SNMP Community String 크랙

③ SNMP 스캐닝하기

snmpwalk - v 1 - c public 192.168.0.1 1.3.6.1.2.1.1

```
root@ubuntu-14: /home/wishfree/TEST
root@ubuntu-14:/home/wishfree/TEST# snmpwalk -v 1 -c public 192.168.0.1 1.3.6.1.
2.1.1
iso.3.6.1.2.1.1.1.0 = STRING: "Hardware: Intel64 Family 6 Model 58 Stepping 9 AT
/AT COMPATIBLE - Software: Windows Version 6.3 (Build 9600 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: (476129) 1:19:21.29
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "WISHFREE_WS12"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 76
root@ubuntu-14:/home/wishfree/TEST#
```

그림 5-38 snmpwalk 스캔

③ SNMP 스캐닝하기

- SNMP로 얻을 수 있는 정보(윈도우 시스템)
  - System MIB : 호스트 이름, 설치된 운영체제 버전, 마지막 부팅 시각 등
  - Interfaces : 논리적인 인터페이스인 루프백(Loopback)과 실제 인터페이스 스위치의 경우 다수의 인터페이스에 대한 사항을 하나씩 모두 확인할 수 있음.
  - Shared Printers : 공유된 프린터 확인
  - Services : 스캔한 시스템에서 운용하고 있는 서비스 목록 확인
  - Accounts : 사용 계정을 확인
  - Shares : 공유 자원 확인
  - TCP/IP Networks : 연결된 네트워크 목록 확인
  - Routes : 시스템의 라우팅 테이블 확인
  - UDP Services : 제공하고 있는 UDP 서비스 확인
  - TCP Connections : 스캔한 시스템의 현재 TCP 세션과 열린 포트를 확인

■ SNMP의 보안 대책

- SNMP가 불필요하다면 SNMP 사용을 막음.
- SNMP를 사용해야 한다면 커뮤니티를 패스워드처럼 복잡하게 설정하여 쉽게 노출되지 않도록 관리
- 패킷을 주고받을 호스트를 설정하여 SNMP를 사용할 시스템의 IP를 등록

감사합니다.

네트워크 해킹과 보안 개정3판

정보 보안 개론과 실습