다양한 패킷 캡처 프로그램 활용

오늘과내일 홍석범(antihong@tt.co.kr)

시스템이나 네트워크를 운영하다보면 보안상의 목적으로 또는 트라블슈팅을 위해 다양한 툴을 이용하여 패킷을 캡처하거나 모니터링 하여야 할 경우가 많다.
이러한 프로그램 중 가장 대표적인 몇 가지 툴의 사용방법에 대해 살펴보도록 하자.

1. tcpdump

tcpdump는 리눅스등 유닉스 계열에서 제공되는 가장 대표적인 패킷캡처 프로그램으로 표준이라 할만큼 매우 대중적으로 사용되는 유용한 도구이다. tcpdump는 대부분 시스템에 기본적으로 설치되어있지만 개별적으로 설치하려면 http://www.tcpdump.org/에서 소스를 다운로드 후 설치하거나 http://rpmfind.net/에서 tcpdump로 검색하여 설치해도 된다. 단, 이때 별도의 패킷캡처 라이브러리인 libpcap을 먼저 설치하여야 된다. 대부분 tcpdump 라는 용어 때문에 tcp만 dump할 수 있는 것이 아닐까 생각하지만 그렇지 않으며 udp,icmp등 프로토콜에 관계없이 캡처가 가능하다.
tcpdump에서 제공하는 옵션은 man tcpdump를 확인해 보거나 또는 간략히

# tcpdump -h를 실행하면 된다.

```
tcpdump version 3.6.3
libpcap version 0.6
```

이곳에서 제공하는 옵션은 BPF(Berkeley Packet Filter)라 하는데, 많은 패킷 캡처 프로그램에서 공통적으로 지원하는 경우가 많다. 이 중에서 몇 가지 중요한 옵션만 살펴보도록 하자.

```
# tcpdump -i eth1
```

별도의 옵션을 주지 않으면 tcpdump는 기본적으로 eth0 인터페이스의 트래픽을 모니터링 한다. 따라서 eth0이 아닌 별도의 인터페이스를 통과하는 트래픽을 모니터링하려면 -i eth1과 같은 옵션을 주어야 한다.

```
# tcpdump port 80
```

특정 포트에 대한 트래픽(소스 또는 목적지에 관계없이)을 모니터링 하고자 할 때 사용할 수 있다. 만약 소스 또는 목적지 포트로 한정하여 모니터링하려면
‘tcpdump dst port 80’또는 ‘tcpdump src port 80’과 같이 사용하면 되나 흔히 소스목적지에 관계없이 사용이 가능한 port를 많이 사용한다.

```
# tcpdump host 211.47.66.50
```

특정 ip에 대한 트래픽(소스 목적지 관계없이)을 모니터링 하고자 할 때 사용할 수 있다. 마찬가지로 만약 소스나 목적지 IP에 대한 정보만을 보고자 한다면
 tcpdump dst host 211.47.66.50' 또는 tcpdump src host 211.47.66.50 와 같이 사용하면 되나 흔히 소스 목적지에 관계없이 사용이 가능한 host를 많이 사용한다.

```
# tcpdump port 80 -X
```

80번에 대한 트래픽을 hex와 ascii로 함께 보여준다. 주로 패킷의 헤더정보 뿐만 아니라 상세한 내용을 보고자 할 때 사용한다.

```
# tcpdump host 211.47.66.50 and port 80
```

소스나 목적지 IP에 IP가 211.47.66.50이고, 소스나 목적지 포트가 80 즉 http인 트래픽을 모니터링 하고자 할 때 사용한다. 여러 가지의 패킷필터가 있을 경우 위와 같이 and 또는 or를 사용할 수 있다.

```
# tcpdump -i eth1 port 80
```

eth1을 통해 소스나 목적지 포트가 80번인 트래픽을 모니터링 하고자 할 때 사용한다.

```
# tcpdump port 80 and not host 1.1.1.1
```

소스나 목적지 포트가 80번인 트래픽중에서 소스나 목적지 ip가 1.1.1.1이 아닌 트래픽을 모니터링 하고자 할 때 사용할 수 있다.

```
# tcpdump -i eth1 arp
```

eth1 인터페이스를 통과하는 arp 패킷을 보여준다.

```
# tcpdump -i eth1 -e
```

eth1 인터페이스를 통과하는 패킷에 대해 mac 정보도 함께 보여준다.

```
# tcpdump -i eth1 net 10.64.4.0 mask 255.255.255.0
```

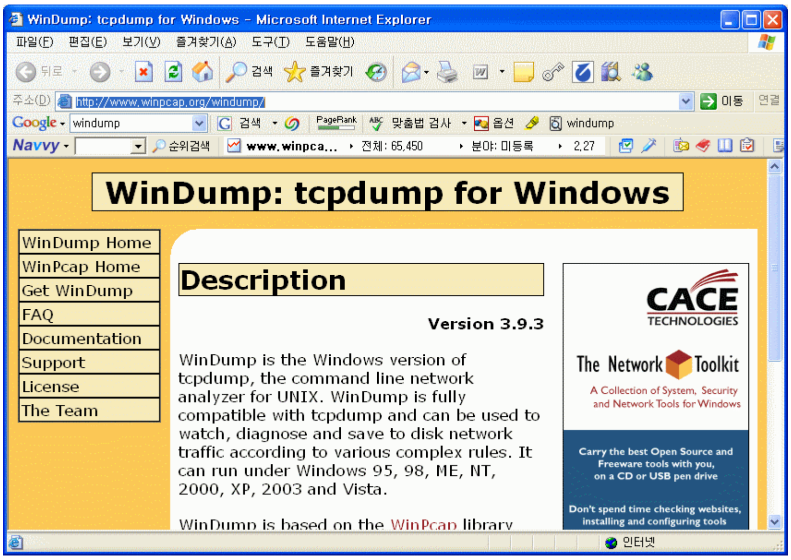
eth1 인터페이스를 통과하는 패킷 중 소스나 목적지 ip 대역이 10.64.4.0/24 대역에 속하는 패킷을 보여준다.

```
# tcpdump -n
```

dump하는 패킷에 대해 ip나 포트번호 등에 대한 역질의(reverse lookup)를 하지 않는다.

2. windump

리눅스 등 유닉스 계열에 tcpdump가 있다면 windows에는 windump라는 프로그램이 있다. windump는 http://www.winpcap.org/windump/에서 다운로드 가능하며 홈페이지에서 명시한 바와 같이 tcpdump의 windows 버전이라고 생각해도 될 만큼 tcpdump와 매우 유사하다. 앞에서 tcpdump를 설치하려면 libpcap 패킷 캡처 라이브러리가 있어야 한다고 했던 것처럼 windump를 설치하려면 winpcap을 먼저 설치하여야 한다. 홈페이지에서 관련 프로그램을 제공하므로 함께 설치해서 사용하면 된다.


WinDump: tcpdump for Windows - Microsoft Internet Explorer
파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도구(T) 도움말(H)
뒤로
검색
즐겨찾기
주소(D) http://www.winpcap.org/windump/
이동
연결
Google windump
검색
PageRank
맞춤법 검사
옵션
windump
Navvy
순위검색
www.winpca...
전체: 65,450
분야: 미등록
2.27
인터넷

WinDump: tcpdump for Windows

WinDump Home
WinPcap Home
Get WinDump
FAQ
Documentation
Support
License
The Team

Description

Version 3.9.3

WinDump is the Windows version of tcpdump, the command line network analyzer for UNIX. WinDump is fully compatible with tcpdump and can be used to watch, diagnose and save to disk network traffic according to various complex rules. It can run under Windows 95, 98, ME, NT, 2000, XP, 2003 and Vista.

WinDump is based on the WinPcap library

CACE TECHNOLOGIES
The Network Toolkit
A Collection of System, Security and Network Tools for Windows
Carry the best Open Source and Freeware tools with you, on a CD or USB pen drive
Don't spend time checking websites, installing and configuring tools

[그림] windump 홈페이지

최근에는 Windows기반에서는 GUI 기반인 ethereal(http://www.ethereal.com/) 등과 같은 패킷 캡처 프로그램이 널리 사용되고 있는 추세이다. 역시 동일하게 BPF 기능을 제공한다.

3. snort

다음으로 소개할 프로그램은 snort이다. snort는 공개 IDS(침입탐지시스템)로 유명한데, 자체적으로 훌륭한 패킷 캡처 기능을 제공하고 있다. 특히 패킷의 헤더뿐만 아니라 데이터(payload)를 분석하고자 할 때 아주 유용하다. 물론 tcpdump에도 -X 옵션을 제공하기는 하지만 snort는 더욱 깔끔한 인터페이스를 제공해 준다. snort는 홈페이지(http://www.snort.org/)에서 소스를 다운로드 및 압축 해제 후 ./configure ; make; make install로 설치하면 되며 물론 libpcap이 사전에 설치되어 있어야 한다.

snort에서도 tcpdump와 같은 다양한 BPF를 제공하는데, 특히 다음과 같이 -vde 옵션을 함께 사용하면 아주 좋다.

-v : 상세한(verbose) 정보를 제공한다.
-d : 응용프로그램 수준(Application Layer)의 데이터를 hex나 ascii 모드로 보여준다.
-e : MAC 주소 등 데이터링크(Layer 2) 수준의 데이터까지 보여준다.

아래는 ‘snort -vde”를 실행하였을 때 보이는 정보로서 첫줄에는 MAC 정보가, 두 번째 줄에는 IP 정보가 보인다. ***AP***는 tcp flag중 ACK와 PSH 비트가 설정되었다는 의미이다. 그리고 우측에는 ascii가 디코딩된 정보가 출력되며 이를 통해 mail.server.com에 pop3 접속에 대한 응답인 것을 알 수 있다.

```
02/19-16:17:56.790278 0:2:FC:8:C4:A0 -> 0:50:8B:9A:1B:1B type:0x800 len:0x3C
```

```
10.2.3.4:110 -> 10.2.4.39:1763 TCP TTL:121 TOS:0x0 ID:22164 IpLen:20
DgmLen:40
***AP*** Seq: 0x2B9D2415  Ack: 0x6405A45C  Win: 0x16D0  TcpLen: 20

2B 4F 4B 20 50 4F 50 33 20 73 74 61 66 66 73 2E   +OK POP3 mail.
74 74 2E 63 6F 2E 6B 72 20 76 32 30 30 31 2E 37   server.com v2001.7
38 72 68 20 73 65 72 76 65 72 20 72 65 61 64 79   8rh server ready
0D 0A
```

4. ngrep

마지막으로 살펴볼 프로그램은 ngrep이라는 프로그램이다.

ngrep은 network grep의 의미로서, 홈페이지 (http://www.packetfactory.net/projects/ngrep/) 또는 http://rpmfind.net/에서 rpm 버전으로 다운로드 가능하다. ngrep은 앞에서 언급한 tcpdump나 snort와 비슷한 기능을 제공하지만 snort와 같이 설치과정이 복잡하지도 않고 바이너리 파일만 복사해서 바로 사용할 수 있을만큼 가벼워서 모니터링시 유용하게 사용 가능하다.

사실, 개인적으로는 tcpdump나 snort보다 이 프로그램을 더욱 많이 사용하고 있는데, 역시 기본적으로 BPF도 제공한다. 몇 가지 유용한 기능을 예와 함께 살펴보도록 하자.

```
# ngrep -qi -c 80 port 80
T 221.xxx.68.251:3414 -> 211.47.xx.xx:80 [AP]
  GET /tt/site/skin/member/CONNECT_LIST/SITE_CONNECT_LIST/images/title_all.gi
  f HTTP/1.1..Accept: */*..Referer: http://test.tt.co.kr/tt/site/ttmember.c
  gi?act=connect_list..Accept-Language: ko..Accept-Encoding: gzip, deflate..I
  f-Modified-Since: Tue, 21 Feb 2006 06:19:41 GMT..If-None-Match: "2a4043-77-
  43fab0fd"..User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; M
  axthon; i-NavFourF; InfoPath.1; .NET CLR 1.1.4322)..Host: test.tt.co.kr..
  Connection: Keep-Alive..Cookie: WRITE=store_user_info=0&; X2VID=Z4402067
  F93; oldserver=done; _home_test_public_html_tt_site_
  SESSION_ID=ee641d3190188207f3320f075f1c2b10....
```

위의 경우 port 80번에 대한 패킷을 캡처한 것으로 패킷의 상세한 내용까지 보여주고 있는 것을 알 수 있다. 여기에서 -c 80은 출력되는 컬럼의 폭을 80자로 제한하여 가동성을 높이기 위한 설정이다.

```
# ngrep -qwi 'user|pass' port 110
T 211.47.xx.xx:2502 -> 211.47.xx.xx:110 [AP]
  USER antihong..
T 211.47.xx.xx:110 -> 211.47.xx.xx:2502 [AP]
  +OK User name accepted, password please..
```

```
T 211.47.xx.xx:4567 -> 211.47.xx.xx:110 [AP]
  PASS sdlkjlfsdf.
```

이는 port 110번에 대한 패킷 중 대소문자에 관계없이(-i) ‘user’ 또는 ‘pass’ 라는 문자열이 보이는 패킷만을 보여주는 것으로, 특정한 문자열만을 캡처해서 보고자 할 때 유용하게 사용할 수 있다.

```
# ngrep -tW byline port 80
#
T 2006/03/13 17:30:16.416882 222.xxx.xx.254:4767 -> 211.47.xx.xx:80 [AP]
GET /tt/site/skin/member/CONNECT_LIST/SITE_CONNECT_LIST/images/bt_profile.gif
HTTP/1.1.
Accept: */*.
Referer: http://test.tt.co.kr/tt/site/ttmember.cgi?act=connect_list.
Accept-Language: ko.
Accept-Encoding: gzip, deflate.
If-Modified-Since: Tue, 21 Feb 2006 06:19:41 GMT.
If-None-Match: "2a403f-1eb-43fab0fd".
User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; i-NavFourF).
Host: custom.tt.co.kr.
Connection: Keep-Alive.
Cookie:         WRITE=store_user_info=0&;         main_ttnews_276_no_popup=20060116;
X2VID=Z43D56FAC3AF43;                             main_ttnews_281_no_popup=20060208;
Recruit200603=done;                                                  oldserver=done;
_home_test_public_html_tt_site_SESSION_ID=9796a3f30d4473ca6c7382e8a7ab42b6.
.
##
T 2006/03/13 17:30:16.418319 211.47.xx.xx:80 -> 222.235.xx.xxx:4767 [AP]
HTTP/1.1 304 Not Modified.
Date: Mon, 13 Mar 2006 08:30:16 GMT.
Server: Microsoft-IIS/5.0.
Connection: Keep-Alive, Keep-Alive.
Keep-Alive: timeout=15, max=99.
ETag: "2a403f-1eb-43fab0fd".
```

위와 같이 -t 옵션을 추가하면 패킷이 캡처되는 시간이 함께 보이고, -W byline을 추가하면 앞에서와 달리 캡처되는 내용들이 한 줄에 나열되지 않고 항목에 따라 여러 줄에 나누어 보여주므로 패킷을 분석하는데 편리하게 사용가능하다.

추가적으로, ngrep에 대한 자세한 내용은 ngrep --help를 참고하기 바라며 패킷 캡처와 관련하여 생각해 볼만한 이슈가 두 가지가 있는데, 만약 패킷 캡처된 내용을 별도의 파일에

저장하고자 할 경우에는 어떻게 하여야 할까?

이러한 경우 각 프로그램에서 자체적으로 제공하는 별도의 저장 옵션을 이용해도 되고 간단히 ngrep > cap.txt 와 같이 실행하여도 된다.

아울러, 패킷 캡처시 시스템에 부하를 유발하지는 않지만 패킷 캡처를 장기간 지속적으로 실행할 경우 패킷 캡처 자체가 부하를 유발할 수도 있으므로 주의하기 바란다.