윈도우 사용자를 위한
Snort + MySQL + HSC 연동 가이드

2005년 11월 16일

배상우 선임컨설턴트

STG Security, Inc.

1. 개요

본 문서는 Windows 2000/XP 환경에서 Snort, MySQL, Honeynet Security Console (이하 HSC 로 약칭함)를 연동하여 Snort 경고를 실시간 모니터링하는 것에 대해 다루고자 한다.
이 문서는 Honeynet Security Console의 라이센스 상의 제약으로 인해 단일 Snort 센서를 기준으로 작성하였다.

2. Snort 와 HSC

Snort 는 '실시간 트래픽 분석과 IP 네트워크 상에서 패킷 로깅이 가능한 경량 네트워크 침입 탐지 시스템'으로 패킷 수집 라이브러리인 libpcap 에 기반한 네트워크 스니핑 엔진과 손쉽게 편집 가능한 탐지 rule을 통해, 네트워크 트래픽을 감시하고 보안 위반 사항을 모니터링할 수 있는 도구이다.
Snort는 프로토콜 분석, 내용 검색/매칭, 버퍼오버플로우 공격, 포트스캐닝, CGI 공격, SMB 스캐닝, OS 정보 획득 시도 등의 다양한 공격과 스캐닝을 탐지할 수 있다. 또한 Snort의 탐지 rule은 손쉽게 편집 가능하여 보안 커뮤니티를 통해 지속적으로 업데이트되고, 본인이 자신의 환경에 맞게 수정, 추가할 수 있으므로 상용 제품에 비해 유연성이 뛰어나다.

Honeynet Security Console은 IDS, 방화벽 로그, Unix 시스템의 syslog, TCPDump 등 다양한 보안 도구의 로그 정보를 취합하여 실시간 모니터링을 수행할 수 있도록 설계된 시스템으로 일종의 ESM 시스템이다. Snort IDS와의 연동을 염두에 두고 다양한 통계 정보, 패킷 분석, nslookup, whois, ping 등 침입자 역추적에 필요한 네트워크 유틸리티 지원 기능을 포함하고 있으며, 상관 관계 분석 기능을 제공하여 발생된 이벤트에 대한 상세 분석을 지원한다. 기존에 Snort 연동에 즐겨 사용되던 ACID에 비해 미려하고 직관적인 사용자 인터페이스를 지원하여 상용 IDS에 못지 않는 편리함을 제공하는 것이 특징이다..

3. 도구 준비

가. WinPcap - http://www.winpcap.org/install/bin/WinPcap_3_1.exe
나. MySQL win32 - http://www.mysql.org/ : MySQL 4.1
다. Snort win32 - http://www.snort.org/dl/binaries/win32/Snort_243_Installer.exe
라. .NET Framework 1.1 - http://www.microsoft.com/
마. Honeynet Security Console - http://www.activeworx.org/downloads/hsc.v2.6.0.msi

4. 도구 설치

가. WinPcap 설치

먼저 윈도우에 WinPcap을 설치한다.

WinPcap 은 범용 패킷 캡쳐 라이브러리인 libpcap의 window 버전으로 Snort가 패킷 캡쳐를 수행하기 위해 반드시 필요하다.

WinPcap 은 '3. 도구 준비'에서 언급한 WinPcap 공식 사이트에서 최신버전을 다운받아 더블 클릭하면 자동으로 설치되며 별도의 설정 없이 간편하게 사용 가능하다.

나. MySQL Win32 설치

MySQL은 경량 DBMS로 Snort의 로그나 이벤트를 저장하기 위해 연동된다. '3. 도구 준비'에서 언급한 MySQL 공식 사이트에서 최신버전을 다운받아 설치한다. 이 때 MySQL 5 를 다운받지 않도록 주의하자. MySQL 5 는 최근까지 개발 버전이었으며 Snort 2.4.3 과의 연동에 일부 문제가 있다. MySQL 4.1.15 는 현재 시점에서 안정 버전 중 최신 버전이므로 이 버전을 사용하도록 하겠다.

다운받은 MySQL win32의 압축을 해제한 후 setup.exe를 실행한다.

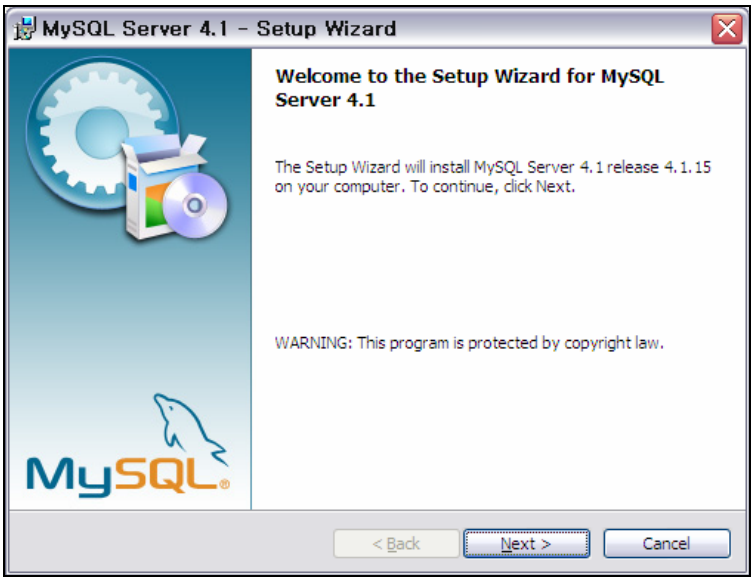

그림 1 MySQL 설치 초기 화면

설치 유형은 Typical 을 선택한다. MySQL에 대해 자세히 아는 사람이라면 다른 옵션을 선택해도 무방하나 본 문서에서는 Typical을 선택하도록 하겠다.

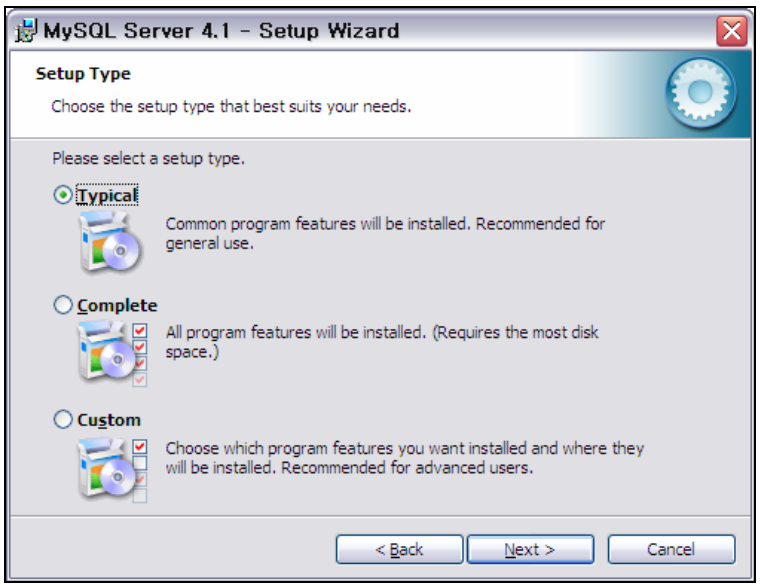

그림 2 MySQL 설치 유형

최종적으로 설치 의사를 묻는 화면이 나오면 [Install] 을 선택한다.

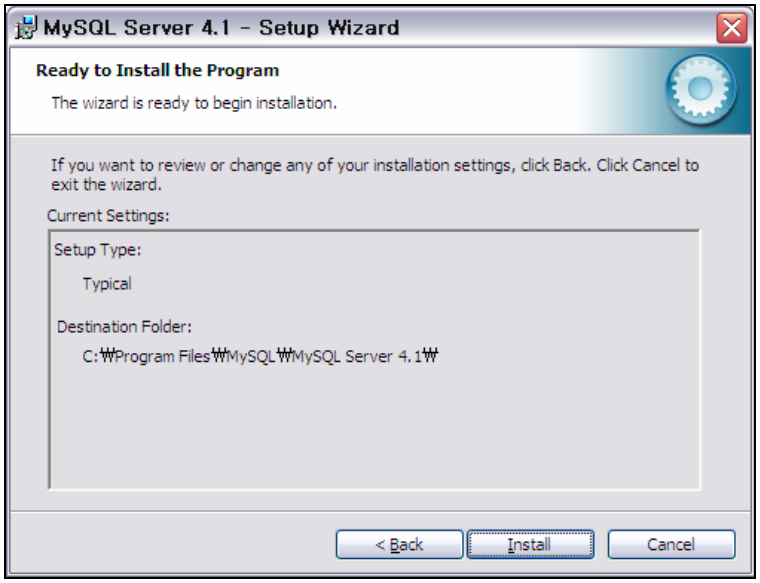

그림 3 설치 확인

설치 중 화면이 완료된 후에 아래와 같이 MySQL 사이트에 대한 등록 옵션이 뜨게 되는데 MySQL 사이트에 등록하고자 하는 사용자나 기존 등록 사용자라면 위의 2 개의 옵션을 선택하되, 본 문서에서는 등록을 하지 않을 예정이므로 3번째 옵션을 선택한다.

그림 4 사용자 등록 화면

설치 종료 시 아래와 같이 MySQL 설정을 시작할 지 묻게 되는데, 디폴트 상태로 해당 옵션을 체크한 상태로 [Finish]를 누른다.

그림 5 설치 종료 화면

MySQL 설정 화면에서 [next]를 선택하면 아래와 같이 설정 옵션을 묻는 화면이 나타난다. 디폴트 상태인 [Detailed Configuration]을 선택하여 세부 사항을 조정하도록 하자.

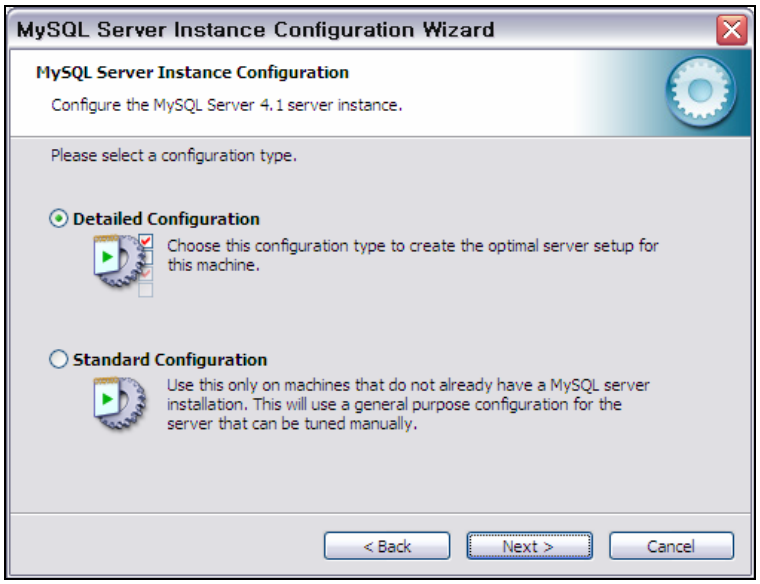

그림 6 설정 옵션 선택 화면

MySQL 서버 사용 유형에서 디폴트 값은 [Developer Machine]으로 메모리를 최소화하여 사용하게 된다. Snort 가 모니터링 할 네트워크 대역의 트래픽이 높지 않다면 디폴트 값으로도 큰 문제가 없으므로 디폴트 값을 선택하도록 한다.

그림 7 MySQL 사용 유형

MySQL 내부 DB 엔진에 대해 선택하는 아래와 같은 화면이 나오면 역시 디폴트 값인 [Multifunctional Database]를 선택한다.

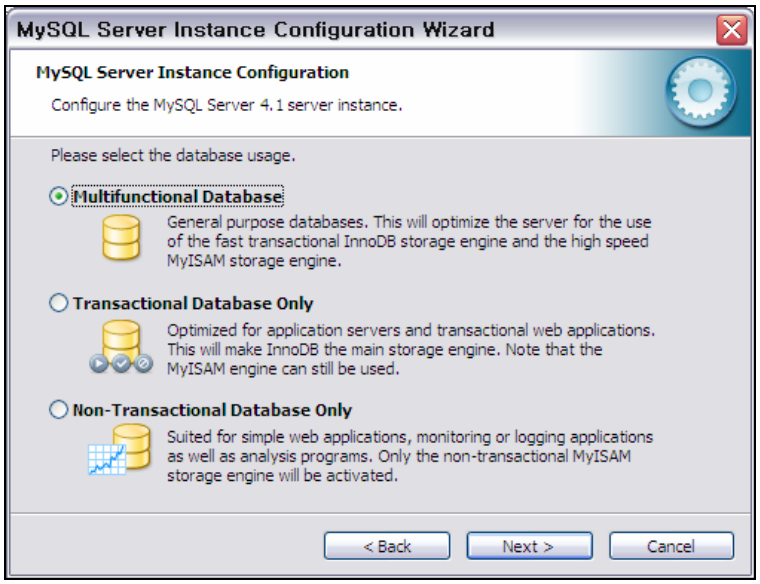

그림 8 DBMS 유형

MySQL이 내부적으로 사용하는 파일이 설치될 위치를 묻는데, 적절한 드라이브와 디렉터리를 지정한다. 별도의 드라이브가 있다면 해당 드라이브(예: D:₩MySQL)로 지정해주면 하드 디스크 접근 속도 상에서 약간 이득을 볼 수 있다.

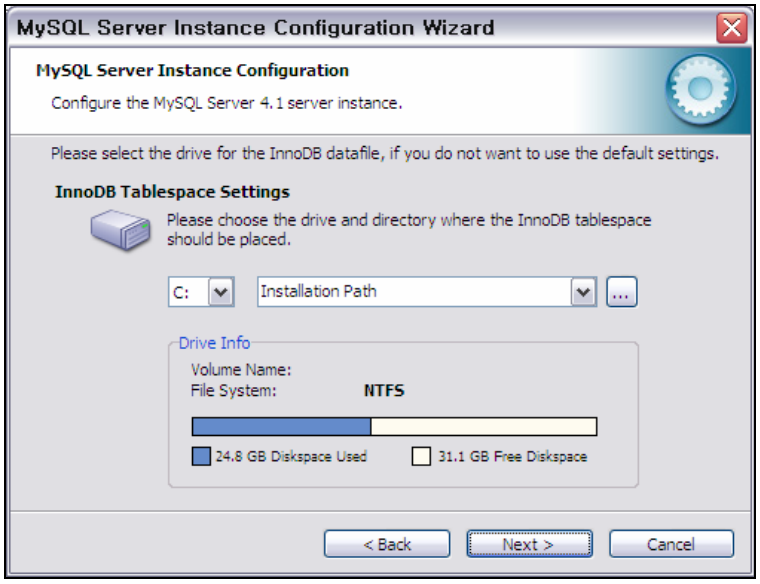

그림 9 설치 위치 지정 화면

MySQL에 대한 동시 접속 수를 설정하는 부분에서 디폴트 값을 사용해도 무방하나 본 문서에서는 [Manual Setting]을 선택하여 동시 접속 15 개로 지정하였다.

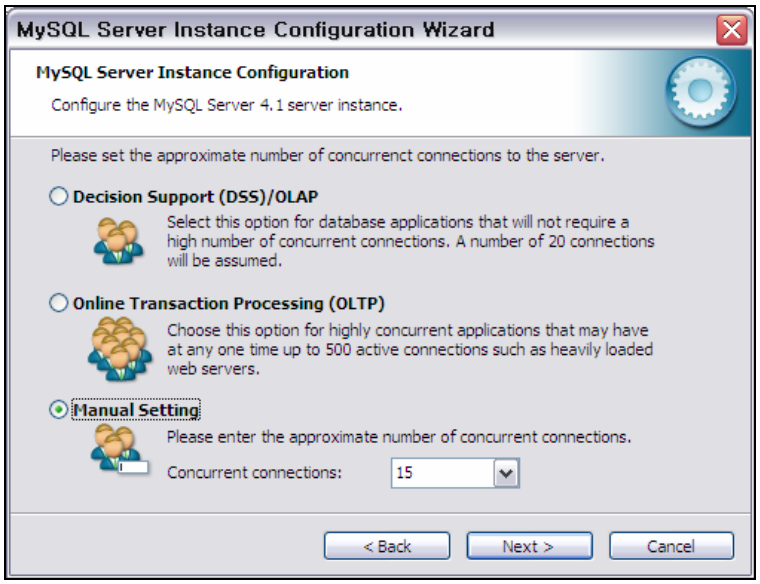

그림 10 동시 접속 수 설정 화면

MySQL을 윈도우의 named pipe가 아닌 네트워크를 통해 접속할 수 있도록 포트를 지정해주는 화면인데, 해당 옵션을 해제해주는 것이 보안 상 보다 바람직하나 Snort 로그를 원격지에서도 모니터링 할 수 있도록 해당 옵션을 선택해준다.

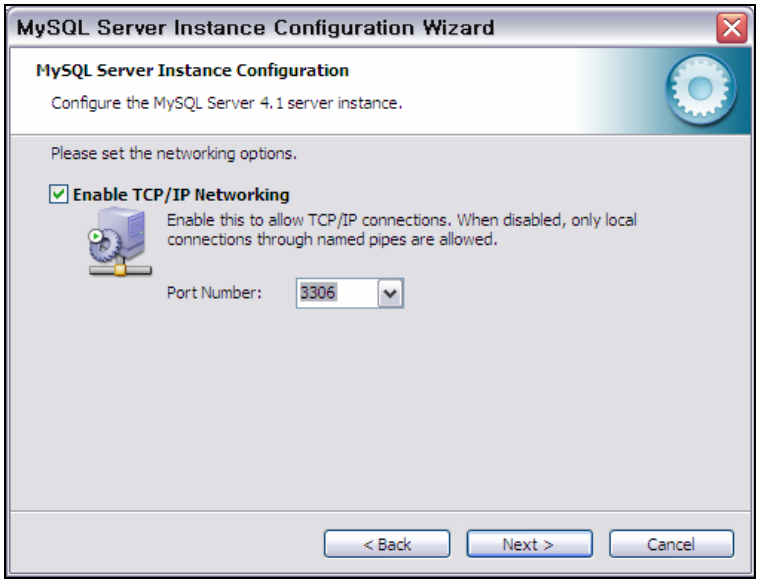

그림 11 MySQL 네트워크 지원 포트 설정

MySQL의 사용 문자셋은 임의의 값으로 설정해도 무방하나 한글 지원 등을 고려하여 2번째 옵션을 선택한다.

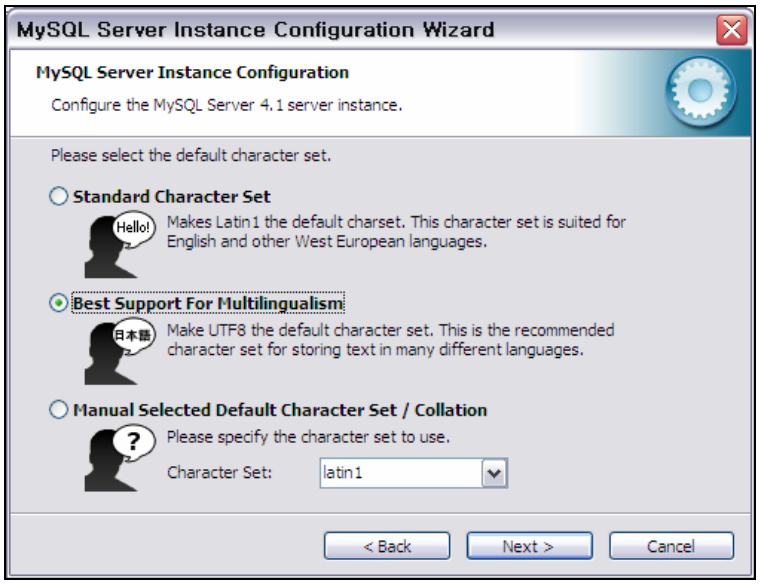

그림 12 문자셋 설정 화면

윈도우가 켜질 때마다 MySQL 서버를 자동으로 시작하기 위해서는 디폴트 값인 [Install As Windows Service]를 그대로 둔다. 향후 mysql 설정 작업을 보다 원활히 하기 위해서 [Include Bin Directory in Windows PATH] 옵션도 선택한다.

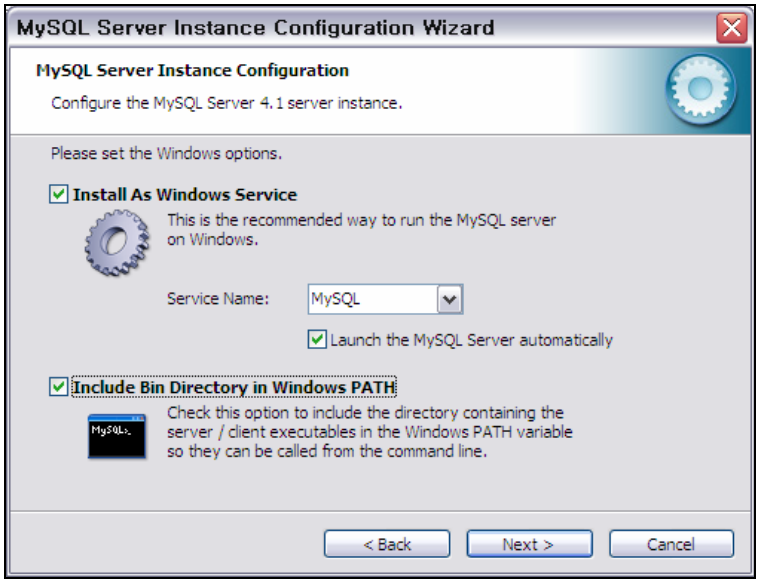

그림 13 MySQL 서비스 설정

이제 MySQL 관리자 패스워드를 설정할 차례다. MySQL이 보안을 의식하기 시작하고 있음을 보여주는 부분이다. 과거에 디폴트로 익명 사용자가 설치되던 것과 달리 익명 사용자는 의도적으로 선택하기 전에는 생성되지 않는다. MySQL 관리자 계정인 root 의 패스워드를 추측하기 어려운 암호로 설정하자.

그림 14 관리자 계정 암호 설정

최종 설정이 완료되기 직전 단계이다. 이제까지의 설정에 문제가 없었으면 [Execute]를 선택하고, 일부 수정할 사항이 있다고 생각되면 다른 버튼을 클릭한다.

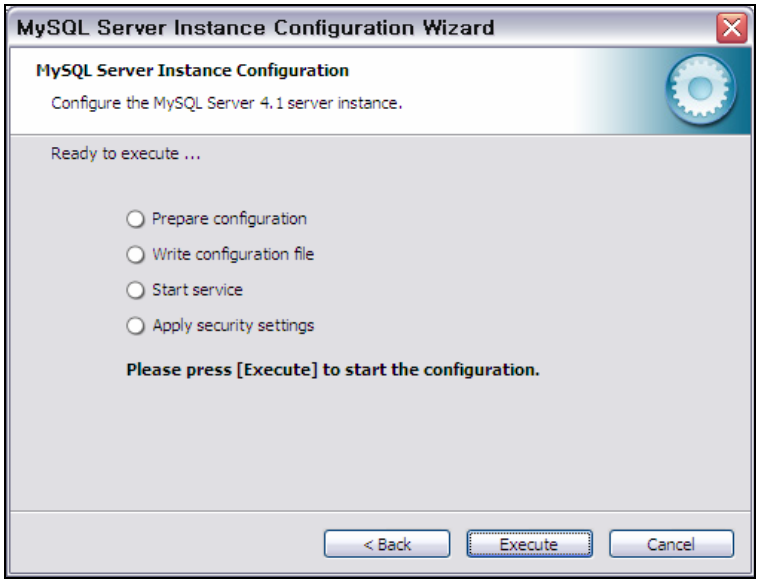

그림 15 최종 설정 완료 직전 화면

이제 최종 설정이 완료되었다.

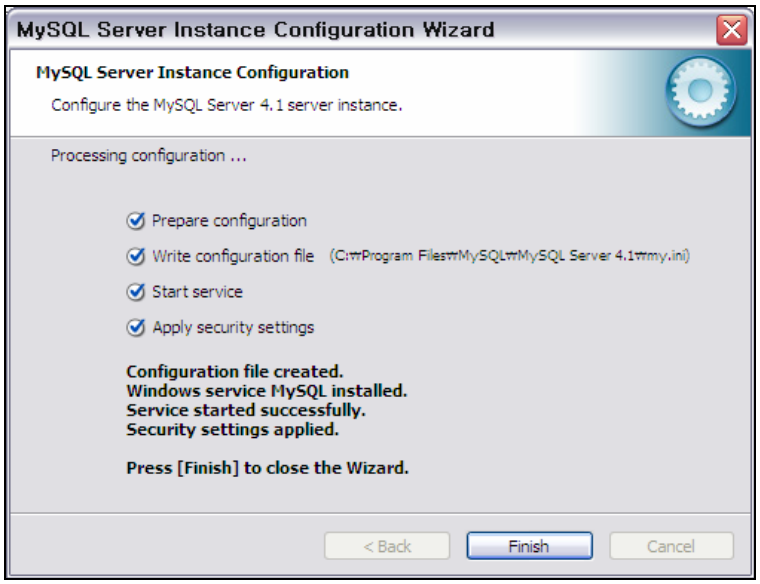

그림 16 최종 설정 완료 화면

설치가 성공적으로 되었는지 확인하기 위해서는 [시작]->[실행]을 선택하여 'cmd' 로 윈도우 명령행 창을 열고 아래와 같이 mysql에 접속해보면 된다.

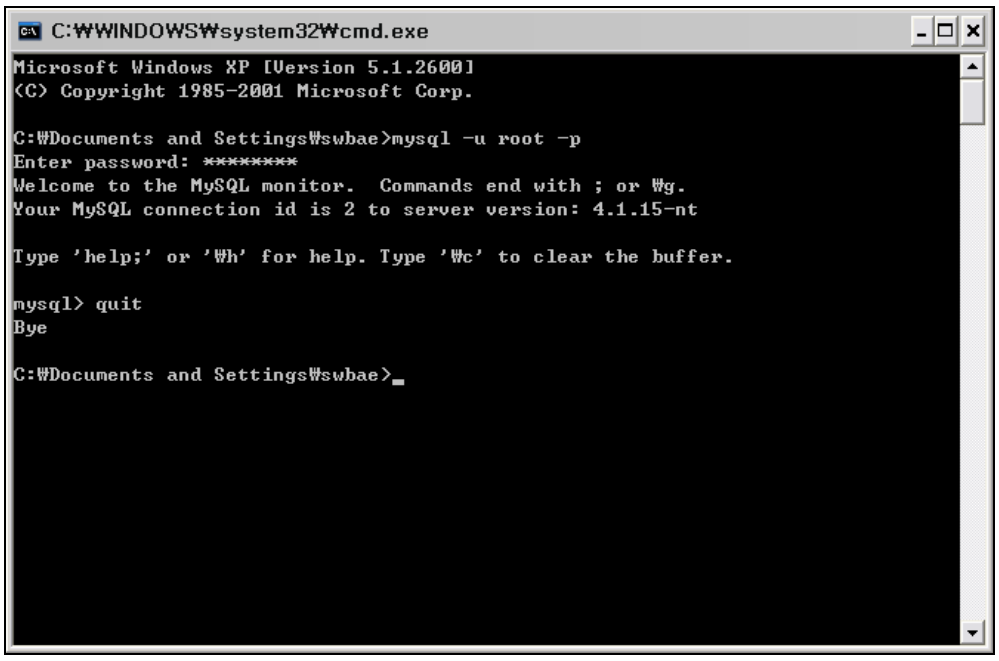

그림 17 설치 확인 완료

다. Snort Win32 설치

'3. 도구 준비'에서 언급한 Snort 공식 사이트에서 최신버전을 다운받아 설치한다. 설치 프로그램의 GPL 라이센스 확인에 동의하고 나면 아래와 같이 DB 연동 설정에 대해 묻는 화면이 나오는데, 본 문서에서는 MySQL과 연동할 예정이므로 디폴트 값을 그대로 선택하고 다

음으로 넘어간다.

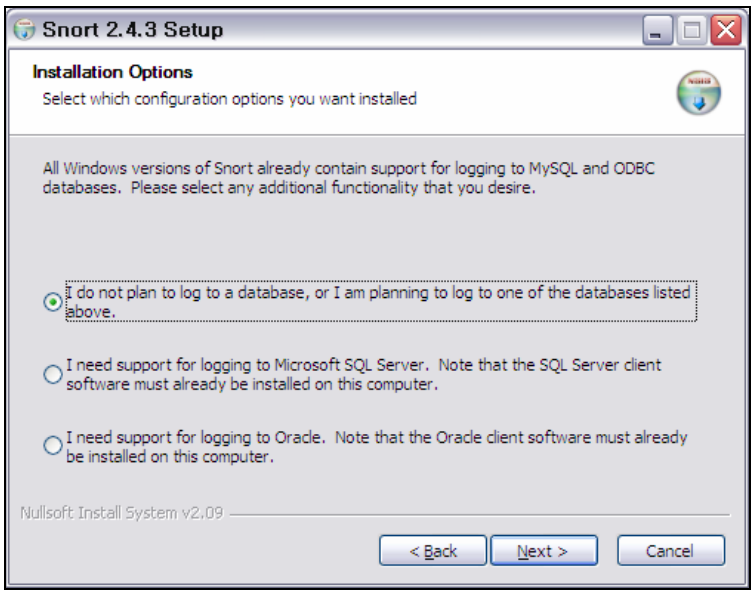

그림 18 Snort DB 연동 선택 화면

설치할 패키지도 역시 디폴트로 선택하고 다음으로 넘어가면, Snort 설치 디렉터리를 묻는 화면이 나온다. 디폴트 값도 무방하나 자신이 원하는 다른 디렉터리를 선택해주어도 좋다. 그러나 Snort 설정 파일에서 해당 디렉터리의 절대 경로를 참조하기 때문에, Snort 설정을 편하게 하기 위해서는 'C:₩Program Files' 처럼 디렉터리명이 길고 복잡한 곳에 설치하지 않는 것이 좋다. 본 문서에서는 디폴트 값인 C:₩Snort를 선택하였다.

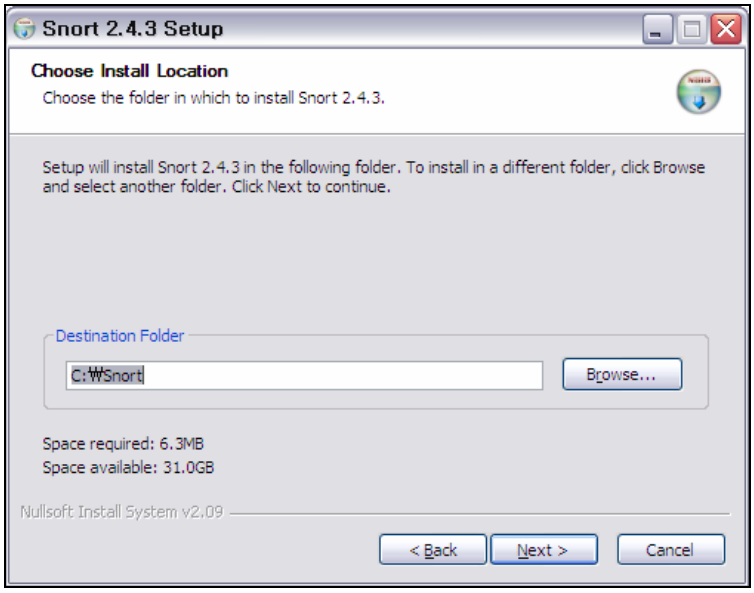

그림 19 설치 디렉터리 지정

이제 Snort 설치가 완료되었다. 설치 완료 후 나오는 길다란 설명 문서는 WinPcap 을 설치해야 한다는 안내 문구로 우리는 이미 설치하였으므로 상관이 없다.

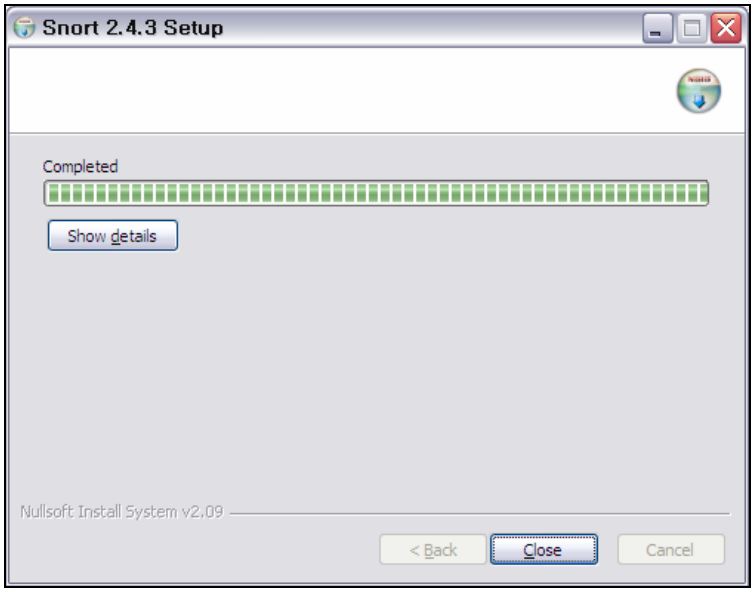

그림 20 Snort 설치 완료 화면

라. HSC 설치

컴퓨터에 이미 .NET Framework 가 깔려있다면 아무 문제가 없으나 깔려있지 않다면 마이크로소프트 사이트에서 .NET Framework 1.1 재배포 가능 버전을 다운받아 설치하고, 필히 윈도우 업데이트를 수행하여 .NET Framework 1.1 서비스팩(SP 1)을 설치한다.

HSC가 내부적으로 .NET Framework에 의존하기 때문이다.

이제 activeworx 사 홈페이지에서 Honeynet Security Console을 다운받아 설치하자.

라이센스 문구에서 동의를 선택하고 다음으로 넘어가서, 사용자명과 소속 기관 부분에 대해 적절한 값을 선택하여 다음으로 넘어간다. 설치 디렉터리를 묻는 화면이 나오는데, 적절한 디렉터리로 변경해주거나 디폴트 상태에서 다음을 선택한다.

그림 21 설치 디렉터리 선택

이후에 나오는 화면에서 [install]을 선택하면 아래와 같이 최종 설치가 완료된다. 만약 아래와 같은 화면이 나타나지 않고 Chart FX 관련 에러 메시지가 나타나면 .NET Framework 가 설치되지 않은 것이니 마이크로소프트 사이트에서 다운받아 설치하도록 한다.

그림 22 설치 완료 화면

이제 기본적인 설치는 완료되었고 Snort, MySQL, HSC를 상호 연동할 차례다.

5. 설정 및 연동

가. Snort 설정

Snort 설치 디렉터리(본 문서에서는 C:₩Snort) 아래의 etc 디렉터리에 보면 snort 설정 파일인 snort.conf 파일이 있다.
해당 설정 파일에서 var HOME_NET 부분에 모니터링할 네트워크 대역을 설정한다. 예를 들면 디폴트값인 var HOME_NET any 를 var HOME_NET 10.1.2.0/24 과 같이 수정하면 된다.
운영 환경이 윈도우 환경이므로 설정 파일에서 var RULE_PATH 부분에 snort 탐지룰 디렉터리를 절대 경로로 설정한다(예: var RULE_PATH c:₩snort₩rules).
classification.conf 도 snort 절대 경로를 포함하도록 수정한다(예: include c:₩snort₩etc₩classification.config).
reference.conf 도 snort 절대 경로를 포함하도록 수정한다(예: include c:₩snort₩etc₩reference.config).
추가로 해당 설정 파일에서 snort 탐지룰 디렉터리를 참조하는 '/' 문자를 찾아서 윈도우 디렉터리 구분자인 '₩' 로 대체해준다. 예를 들면 'include $RULE_PATH/local.rules'를 'include $RULE_PATH₩local.rules' 로 변경한다.

나. Snort 룰 설치

Snort 탐지 룰을 설치할 차례이다. Snort 공식 사이트(http://www.snort.org/pub-bin/downloads.cgi)에서 Snort 탐지 룰을 다운받아 압축을 해제한다. 압축이 해제되면 doc 디렉터리와 rules 디렉터리가 생성되는데, rules 디렉터리 이하의 파일은 Snort 설치 디렉터리의 rules 디렉터리(c:₩snort₩rules)에 복사하고, doc₩signature 디렉터리 이하의 파일은 Snort 설치 디렉터리의 signature 디렉터리(c:₩snort₩doc₩signature)에 복사한다.

다. Snort 와 MySQL 연동

Snort 와 MySQL를 연동할 차례이다.
먼저 snort 로그와 이벤트를 저장할 MySQL db와 table을 만들어야 하므로 [시작]->[실행]에서 'cmd' 로 윈도우 명령행 창을 열고 아래와 같이 snort 가 사용할 db 를 생성한다. DB 명은 구분을 쉽게 하기 위해 snort로 설정하였으며, 사용자가 원하는 임의의 이름을 사용하여도 좋다.

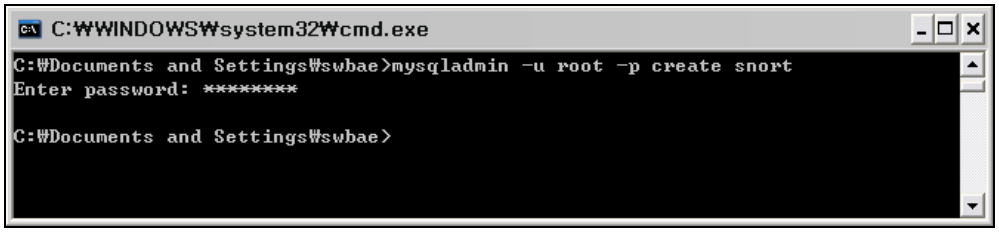

그림 23 Snort DB 생성

이제 아래와 같이 Snort 가 내부적으로 사용하는 DB 테이블 등의 스키마를 생성한다.

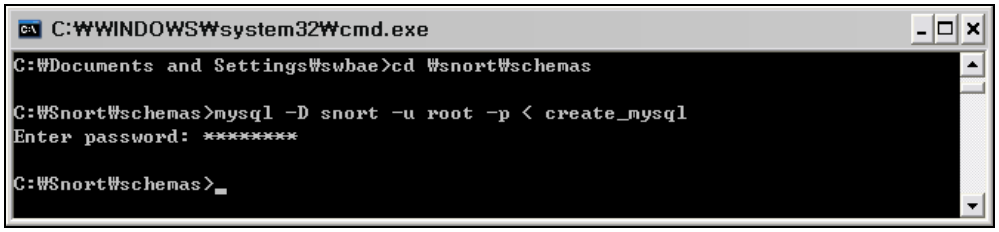

그림 24 Snort DB 스키마 생성

snort.conf 파일에서 'output database: log, mysql, user=root password=test dbname=db host=localhost' 과 같이 되어 있는 부분을 찾아 주석(#)을 제거하고, 패스워드 부분에 이전에 설정한 MySQL 패스워드를 삽입한다. dbname 에는 DB 생성 시 사용한 DB명을 사용한다. 예제에서는 다음과 같다.

output database: log, mysql, user=root password=[password] dbname=snort host=localhost

이제 Snort와 MySQL의 연동 작업이 완료되었다.

적절히 설정되었는지 확인하기 위해서는 snort 명령어 프로그램을 사용하여 검사해야 한다. 먼저 현재 컴퓨터에 설치된 네트워크 카드를 알아보자.

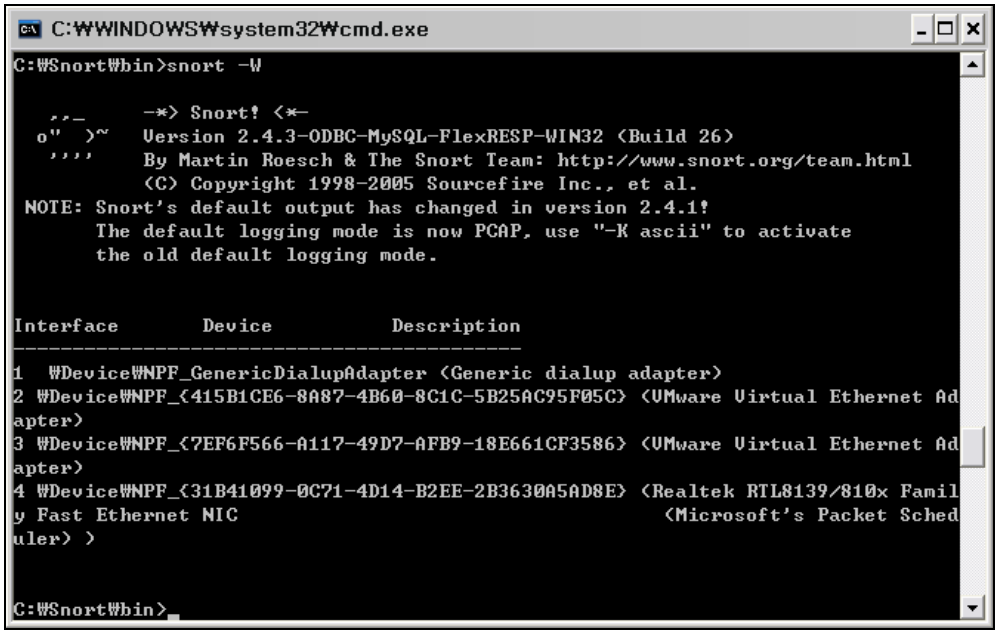

그림 25 네트워크 카드 확인

4개의 네트워크 카드가 검색되었으며, 이 중 1개는 모뎀, 2개는 가상 네트워크 카드, 마지막 1개는 리얼텍 랜카드인 것을 알 수 있다. 우리가 모니터링할 네트워크는 리얼텍 랜카드의 네트워크 대역이므로 아래와 같은 명령어를 수행하여 Snort 설정 파일의 정상 여부를 점

검할 수 있다.

그림 26 Snort 설정 파일 검사

각 옵션의 의미는 다음과 같다.

- T 옵션 : Snort 설정 파일 정상 여부 테스트
- l 옵션 : 로그 파일 저장 위치, MySQL을 사용하므로 무조건 snort 설치 디렉터리 이하의 log 디렉터리로 지정.
- c 옵션 : Snort 설정 파일 위치, 일반적으로 c:₩snort₩etc₩snort.conf.
- i 옵션 : 모니터링할 네트워크 카드의 번호, -W 옵션 결과를 통해 지정하면 쉬움.

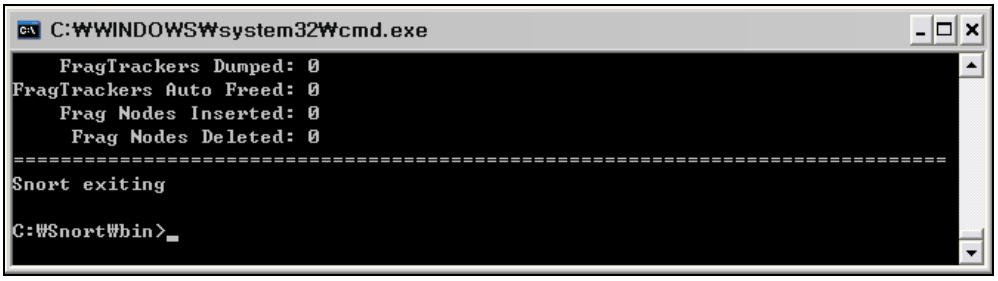

그림 27 점검 결과

별다른 에러 메시지 없이 Snort exiting 메시지가 나타나면 설정 파일에 아무 문제가 없다는 의미이다. 만약 에러 메시지가 나타난다면 Snort 설정 파일을 다시 살펴보도록 한다.

라. HSC 와 MySQL 연동

HSC와 MySQL을 연동할 차례이다.

HSC는 내부적으로 별도의 DB를 사용하므로 아래와 같이 HSC가 사용할 DB를 생성한다. HSC가 이용하는 DB의 디폴트명은 aw_hsc 이다.

그림 28 HSC 용 DB 생성

이제 아래와 같이 HSC 가 내부적으로 사용하는 DB 테이블 등의 스키마를 생성한다.

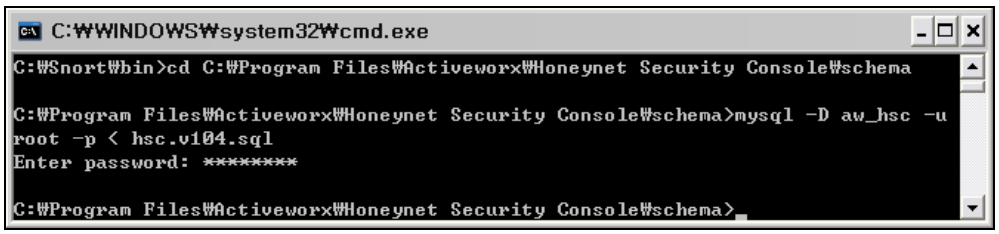

그림 29 HSC 용 DB 스키마 생성

바탕화면의 HSC 아이콘을 클릭하여 프로그램을 실행하면 아래와 같이 로그인 화면이 나타난다. Username에는 MySQL 관리자명인 root를, Password에는 이전에 설정한 MySQL 관리자 패스워드를 넣는다. IP Address는 본 문서에서는 자신의 컴퓨터인 127.0.0.1 로 지정한다.

그림 30 로그인 화면

맨 처음 로그인 하면 에러 창이 뜨게 되는데 정상이므로 놀라지 말고, 아래와 같이 Snort가 사용하는 MySQL DB를 등록한다. 프로그램 화면 왼쪽의 [Resources]를 선택하면 창이 열리면서 [Databases]가 나타난다.

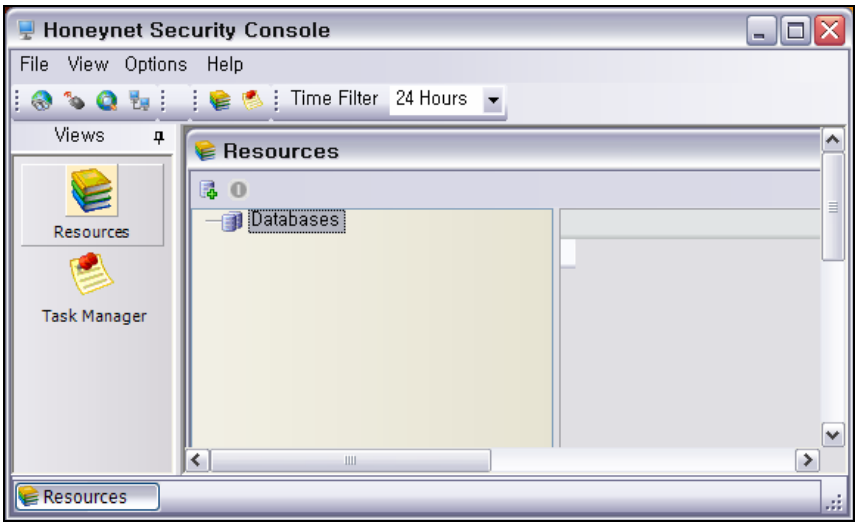

그림 31 MySQL DB 등록 절차 1

[Databases]를 선택한 후 마우스 오른쪽 버튼을 누르면 아래와 같이 Add database 가 나타난다.

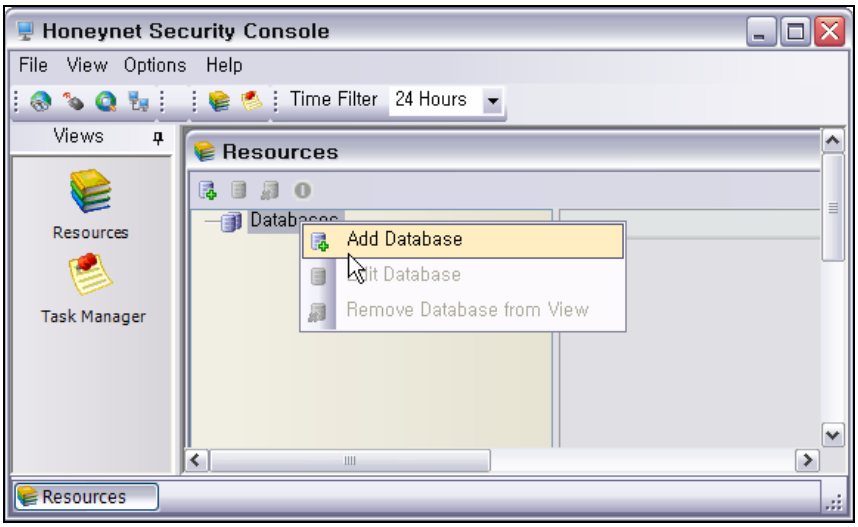

그림 32 MySQL DB 등록 절차 2

이어서 나타나는 화면에서 아래 화면과 같이 해당 부분을 다 기입한 후 OK 버튼을 누른다. 이 때 Database Name 부분은 먼저 [Fill Databases] 버튼을 클릭하고 나면 나오는 리스트 중 Snort 가 사용하는 DB명(예:snort)을 선택하도록 주의한다.

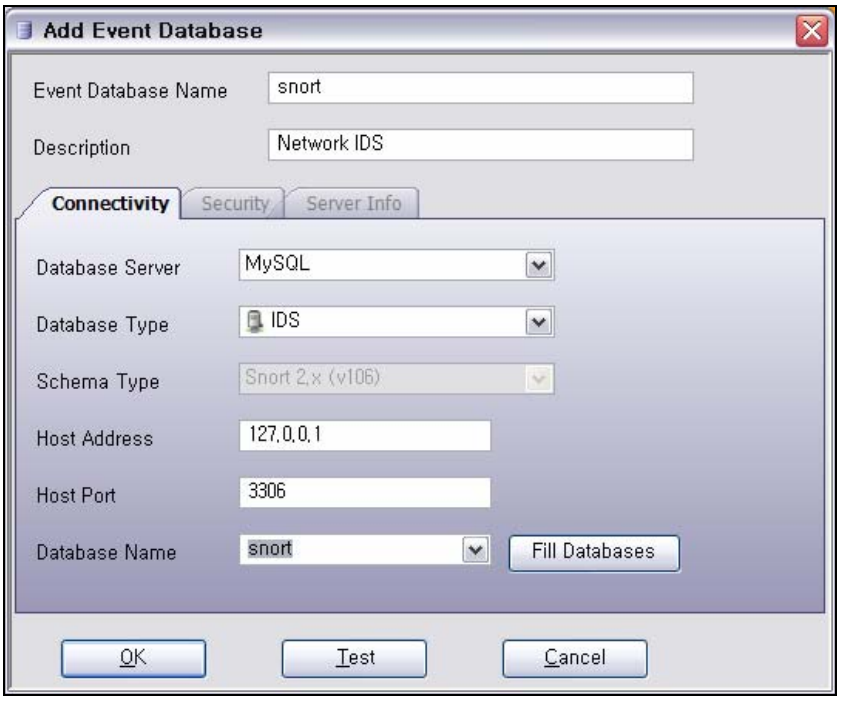

그림 33 MySQL 연동 정보 기입

HSC가 MySQL 접속에 성공하면 아래와 같이 IDS Sensors 라는 항목이 나타나면서 왼쪽 메뉴에 IDS 메뉴가 추가된다.

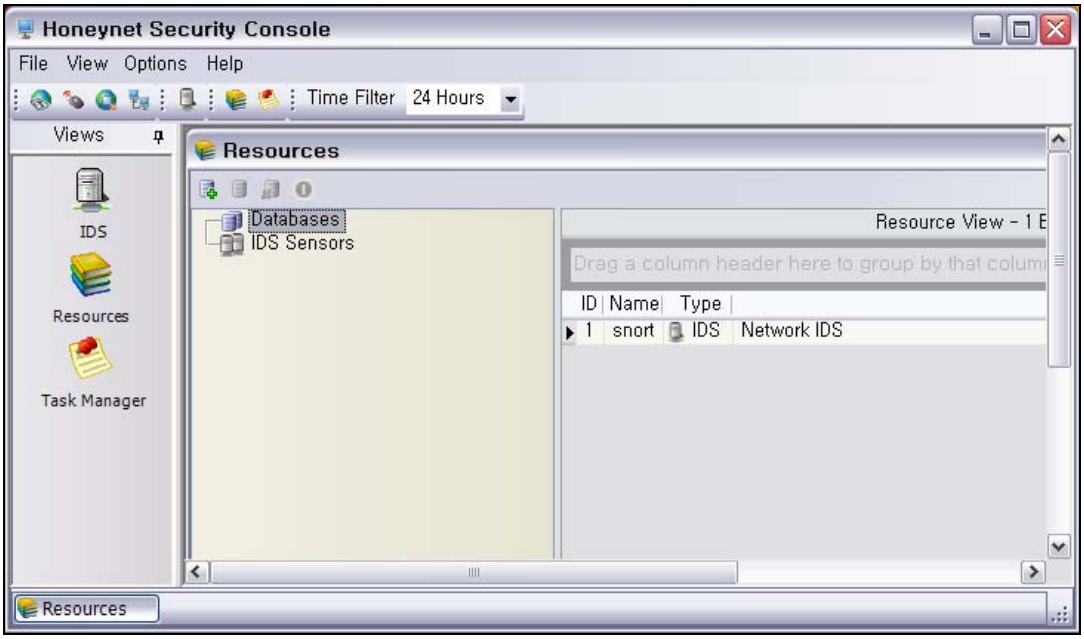

그림 34 Snort 사용 MySQL DB 연동 성공

왼쪽에 추가된 IDS 메뉴를 누르면 아래와 같이 IDS 이벤트 모니터링 창이 뜨게 된다.

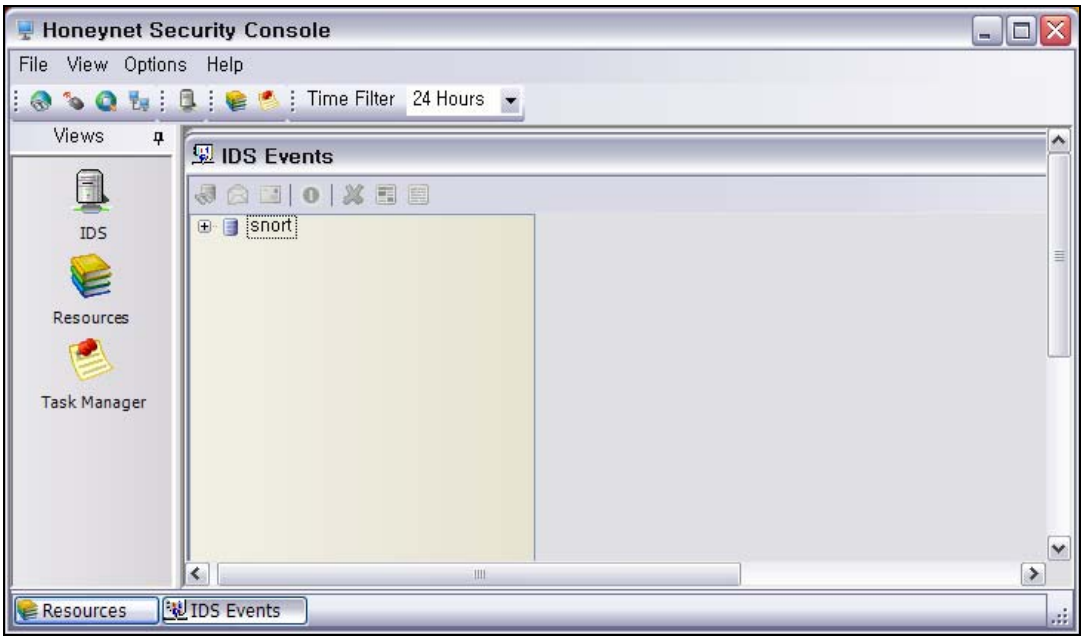

그림 35 IDS 모니터링 준비

해당 창에서 + 버튼을 누르면 아래와 같이 다양한 하위 메뉴가 열리며, IDS 모니터링을 위한 준비가 완료된다.

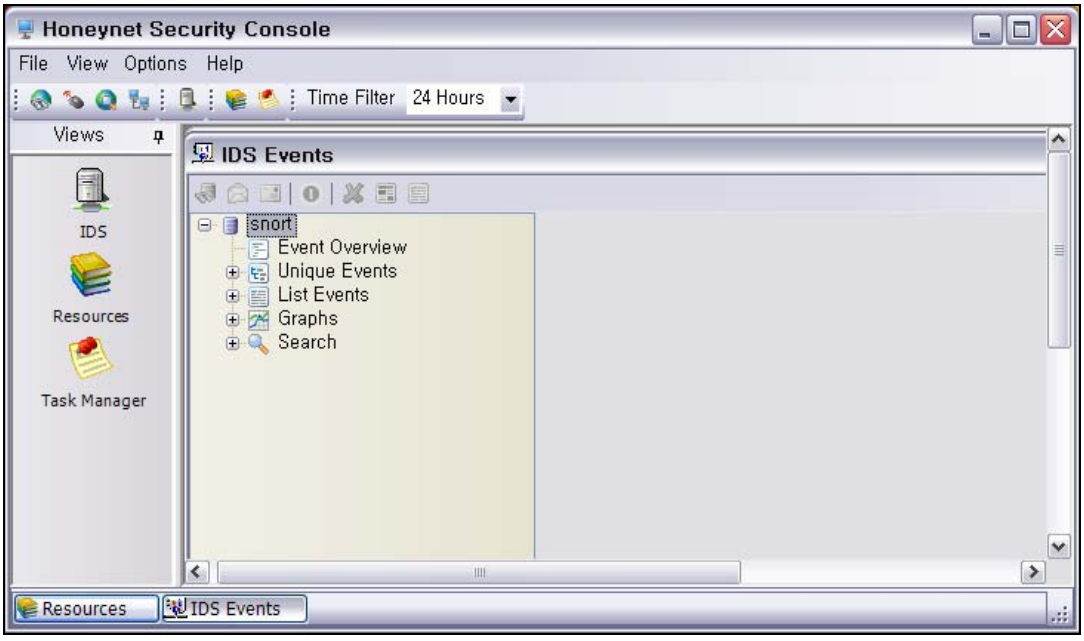

그림 36 IDS 모니터링 준비 완료

마. Snort 실행 및 모니터링

이제 본격적으로 Snort를 사용할 차례이다.
지금까지의 설명을 충실히 따른 사용자라면 설정에 문제가 없을 것으로 본다.
아래와 같이 Snort를 실행한다.

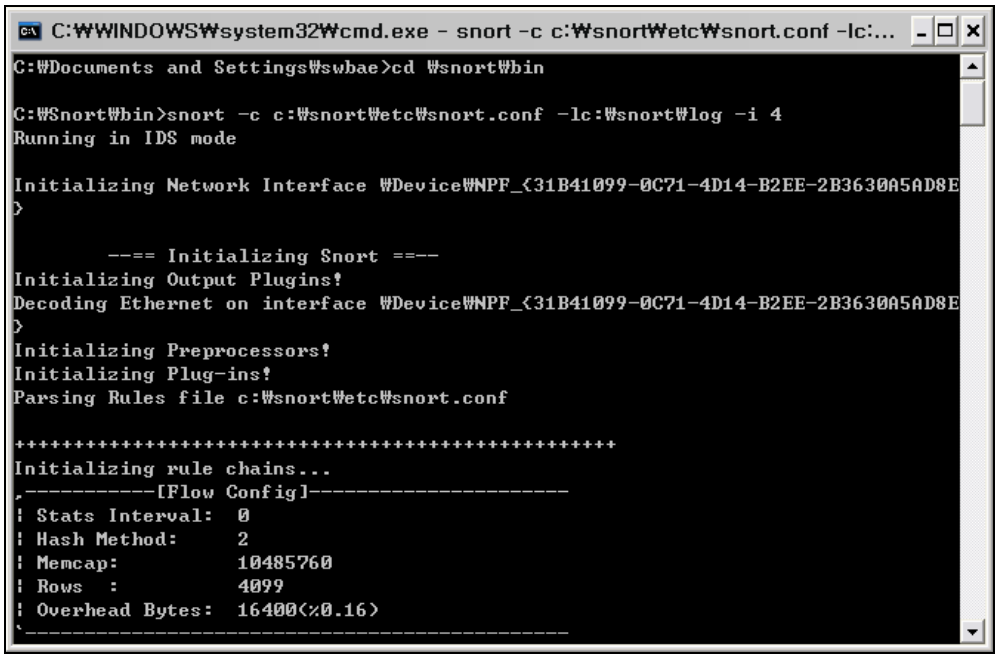

그림 37 Snort 실행

유심히 본 사용자라면 Snort 설정 파일이 정상적인지 점검하는 명령어에서 -T 옵션만 제거한 명령어라는 것을 알 수 있을 것이다.

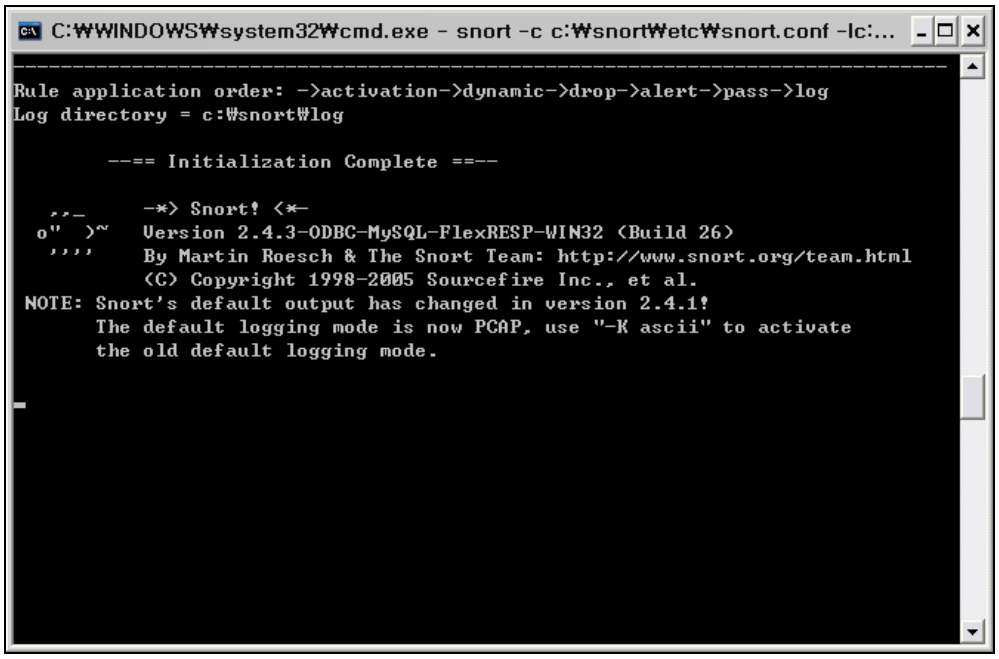

그림 38 Snort 실행 결과 화면

각 도구가 적절히 연동되어 실시간 모니터링이 가능한지 살펴보기 위해, 취약점 스캐너를 이용해 스캐닝을 해보도록 한다.

Snort와 MySQL의 연동에 문제가 없으면 스캐닝 수행 중에 아래와 같이 화면에 변화가 없어야 한다. 만약 해당 화면에 insert 등의 문자열이 뿌려지면서 화면이 스크롤되면 Snort와 MySQL 연동에 문제가 있는 것이니, MySQL 설정, Snort 설정 파일 등을 점검해보도록 한다.

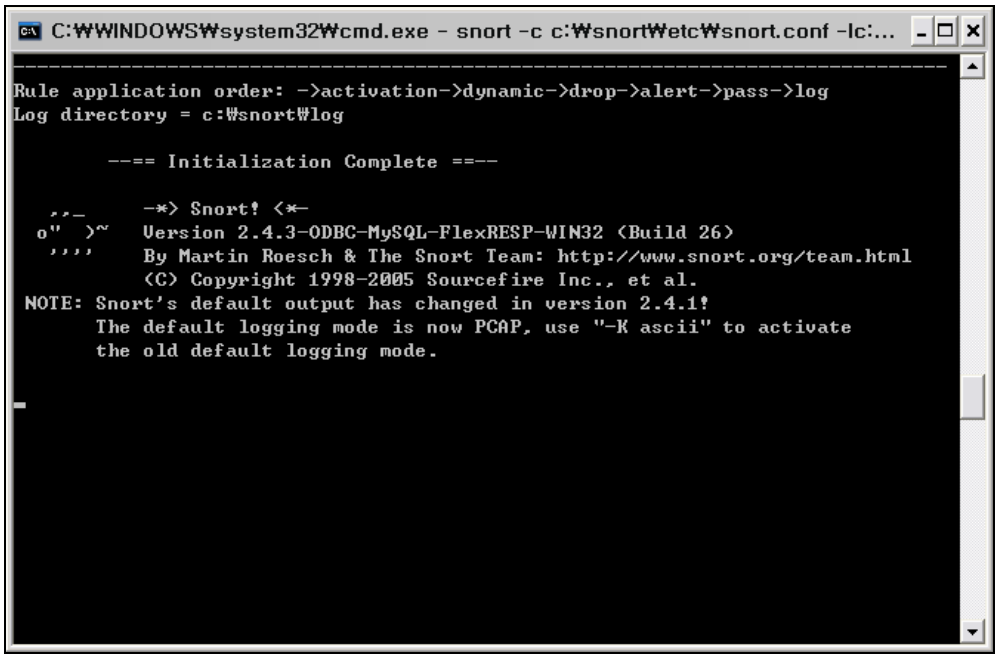

그림 39 스캐닝 수행 중 Snort 화면

HSC를 사용하여 Snort의 이벤트 및 로그를 실시간으로 모니터링하는 화면은 다음과 같다.

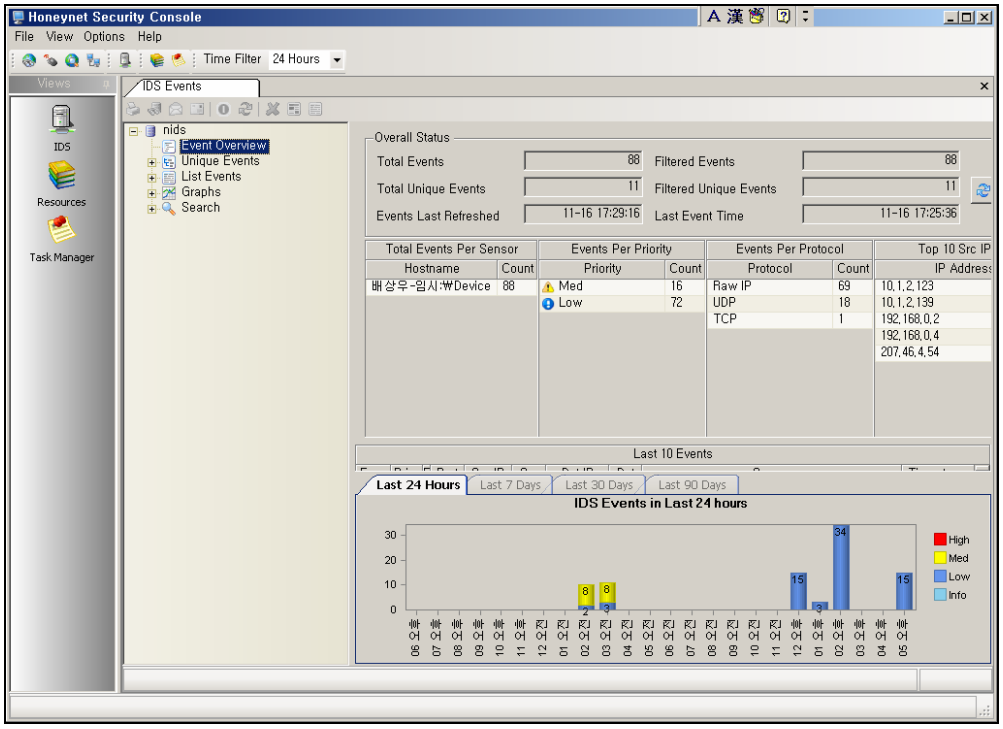

그림 40 HSC 실시간 모니터링 화면

6. HSC 사용

HSC의 사용법은 직관적이어서 별도의 설명이 필요 없으나, 기본적인 사용법을 설명하면 다음과 같다.

가. Event Overview

Event Overview 는 자동으로 refresh 되는 실시간 모니터링 화면으로, 발생되는 이벤트에 대한 종합적인 관점을 제공한다.

주요 공격자 IP, 시간별 공격 동향 그래프, 발생 이벤트의 위험도 현황, 주요 공격 이벤트 등 종합적인 통계를 제공하여 공격 동향 모니터링에 유용하다.

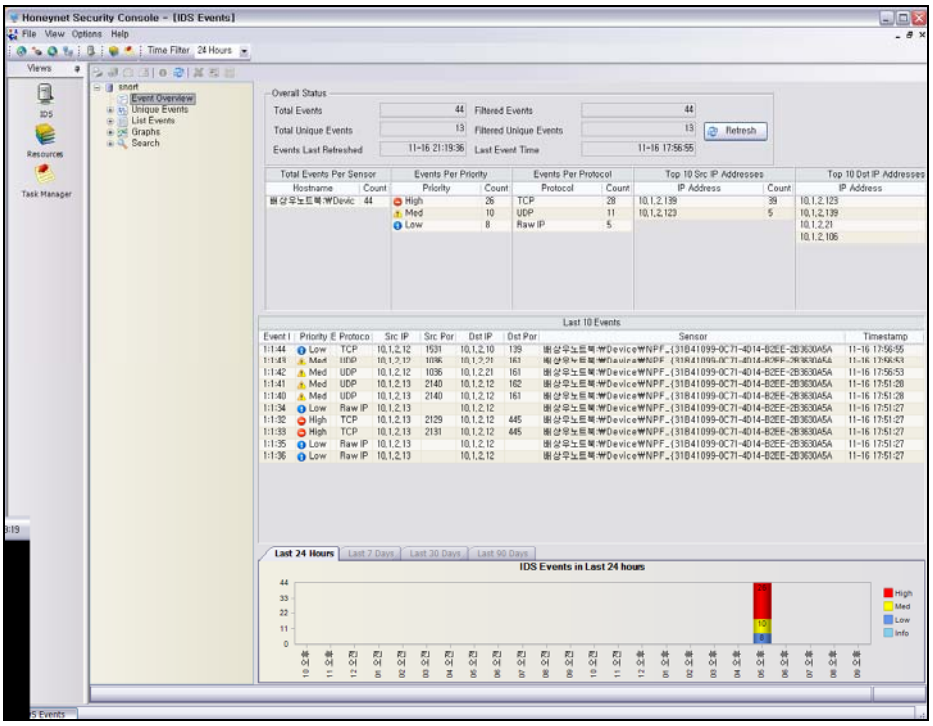

그림 41 Event Overview 화면

나. Uniq Events

Uniq Events는 최근에 발생한 이벤트를 카테고리화하여 보여주는 화면으로, 최근에 발생한 공격 유형을 파악하는데 유용하다. 동일한 이벤트가 여러 건 발생하여도 Uniq Events 화면에서는 동일 카테고리로 분류되므로, 현재 환경에서 어떤 공격 유형이 주로 발생하는지 파악하는데 유용하다.

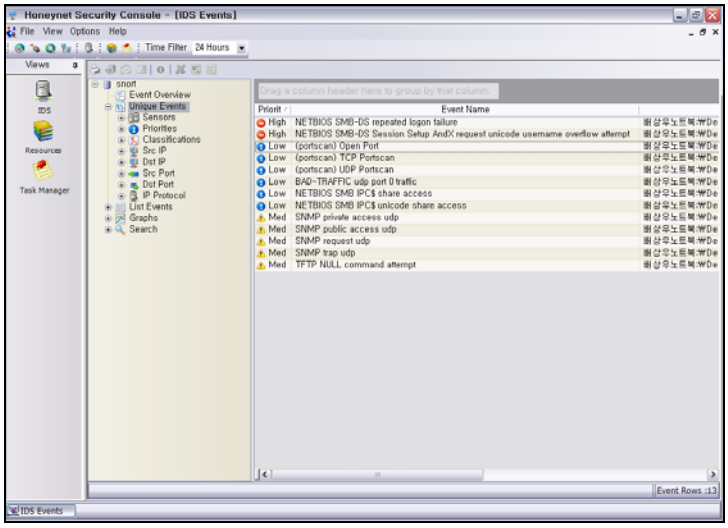

그림 42 Uniq Events 화면

다. Lists Events

List Events는 최근에 발생한 이벤트를 시간 순서로 보여주는 화면으로 최근에 어떤 공격이 발생했는지 파악하는데 유용하다. 동일한 이벤트가 여러 건 발생하는 경우 스캐닝 등 공격이 이루어지고 있는 징후이므로 공격자 IP 정보를 파악하여 신속히 대응할 필요가 있다.

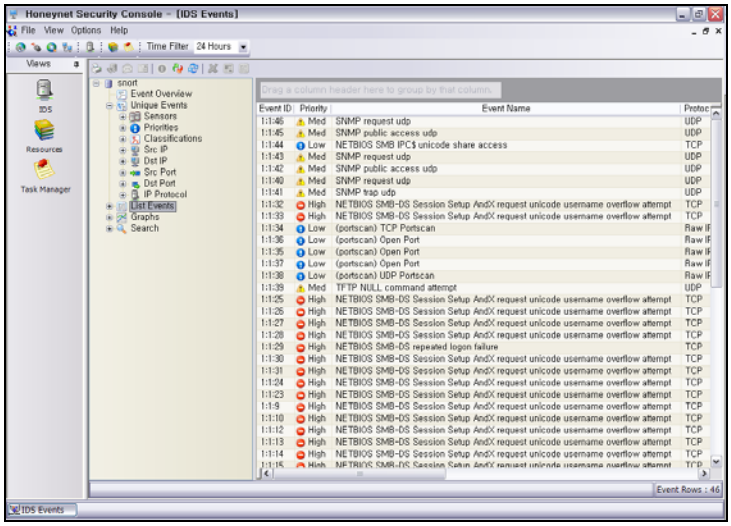

그림 43 List Events 화면

위험도별 통계를 통해 공격의 위험도 분포를 파악 가능하다.

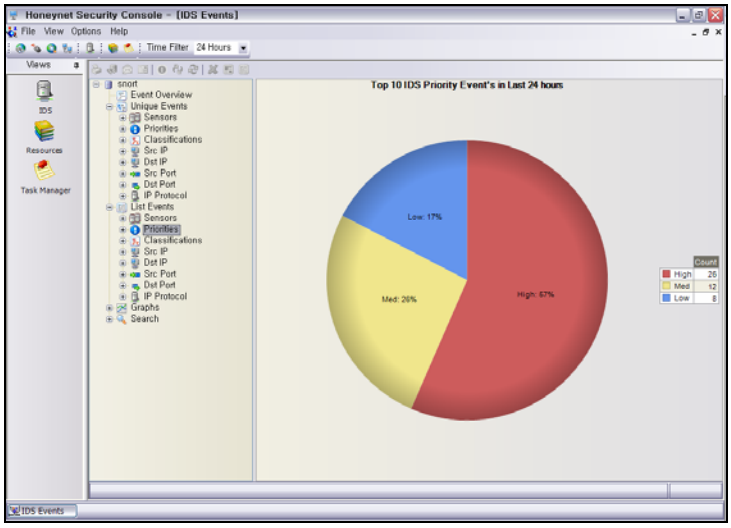

그림 44 위험도별 통계

공격 유형별 통계는 Snort 탐지 룰 상의 공격 유형(classification)에 대응하는 통계 정보를 제공하여 주로 어떤 유형의 공격이 발생하는지 파악하는데 유용하다.

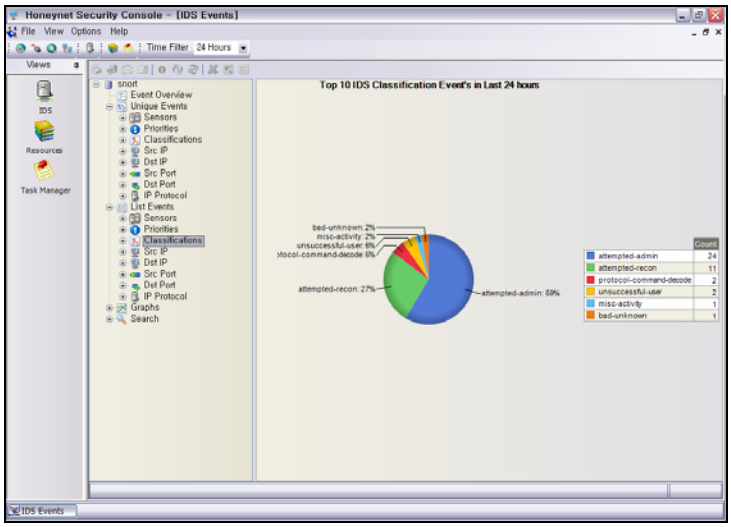

그림 45 공격 유형별 통계

기타 공격자 IP, 피해 IP, 공격 포트, 피해 포트 등 다양한 통계 정보를 제공하며, 해당 정보를 하루, 주간, 월간 단위로 파악할 수 있어 내부 네트워크 상황 모니터링 및 공격 동향 파악에 유용하다.