**Open**

팀명 :

팀장 :

팀원 :

**개 정 이 력**

|  |  |  |  |
| --- | --- | --- | --- |
| 개정 번호 | 개정 내용 요약 | 추가/수정 항목 | 개정 일자 |
| 0.1 | 최종 제정 승인 | 원안 작성 | 2015.12.25 |
| 0.2 |  |  |  |
| 0.3 |  |  |  |
| 0.4 |  |  |  |
| 0.5 |  |  |  |
| 0.6 |  |  |  |
| 0.7 |  |  |  |
| 0.8 |  |  |  |
| 0.9 |  |  |  |
| 1.0 |  |  |  |

**문 서 규 칙**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Open Source를 이용한 IDS구축 및 네트워크 관리 프로그램 | | | ④ |
| Category | 첨부파일 버전 | 문서 최종 수정일 |
| ① | ② | ③ |

* 작성 및 확인은 Microsoft Word 2007으로 작성 되어 졌으며, Acrobat Reader로 읽는다.
* Category(①)에는 Manual, Utility, Tip, Analysis Report 로 구분하며, 기재된 정보가

Manual과 Utility가 혼합된 경우에는 "Manual + Utility" 라고 표기되며, 머리글의

Category에 해당 구분 정보를 표기된다.

* 본 문서의 주제가 되는 대상은 오른쪽 큰 여백에 기재된다. (④)
* 첨부 파일 버전(②)은 첨부 파일이 존재하는 경우에 기재되며, 첨부 파일의 버전이

표기된다. (유틸리티의 경우 최종 버전은 날짜 표기 대신 버전으로 대체한다)

* 문서 최종 수정일(③)에는 문서의 최종 수정날짜가 표기된다.

**목 차**

[1. 프로젝트 개요 7](#_Toc441080698)

[1.1 프로젝트 목표 7](#_Toc441080699)

[1.2 팀원 및 역할 7](#_Toc441080700)

[1.3 프로젝트 일정 8](#_Toc441080701)

[1.4 프로젝트 환경 9](#_Toc441080702)

[1.5 부분별 기대효과 10](#_Toc441080703)

[1.5.1 현황 (AS-IS) 10](#_Toc441080704)

[1.5.2 개선 및 기대효과 (TO-BE) 10](#_Toc441080705)

[1.6 Open Source를 이용한 IDS구축 11](#_Toc441080706)

[1.6.1 IDS 11](#_Toc441080707)

[1.6.2 Snort 12](#_Toc441080708)

[1.6.3 Splunk 13](#_Toc441080709)

[1.6.4 Yara / Cuckoo Sandbox 16](#_Toc441080710)

[2. 프로젝트 내용 19](#_Toc441080711)

[2.1 GNS3 구축환경 19](#_Toc441080714)

[2.2 Snort를 이용한 공격확인 20](#_Toc441080715)

[2.2.1 공격 List 20](#_Toc441080716)

[2.2.2 Ping of Death 21](#_Toc441080722)

[2.2.3 Land Attack 23](#_Toc441080723)

[2.2.4 Nmap 25](#_Toc441080724)

[2.2.5 Netcat 27](#_Toc441080725)

[2.2.6 Telnet 서버 접근 실패 시 패킷 검출 29](#_Toc441080726)

[2.3 Splunk로 Log기록 확인 31](#_Toc441080727)

[2.4 Yara / Cuckoo Sandbox 33](#_Toc441080728)

[2.4.1 Python, Yara 설치 33](#_Toc441080729)

[2.4.2 Cuckoo Sandbox 설정 33](#_Toc441080737)

[2.4.3 Cuckoo Sandbox 실행 34](#_Toc441080738)

[2.4.4 Cuckoo Sandbox 관리자 페이지 35](#_Toc441080739)

[2.5 IP, Port 관리 프로그램 36](#_Toc441080740)

[2.5.1 개요 36](#_Toc441080741)

[2.5.2 Python 코딩 36](#_Toc441080750)

[2.5.3 실행화면 및 사용방법 37](#_Toc441080751)

[3. 결론 38](#_Toc441080752)

[4. 추후과제 및 후기 39](#_Toc441080753)

[5. 참고자료 40](#_Toc441080754)

**표 목 차**

[[표 1‑1] 팀원 및 역할 7](#_Toc441060694)

[[표 1‑2] 프로젝트 일정 8](#_Toc441060695)

[[표 1‑3] 프로젝트 환경 9](#_Toc441060696)

[[표 2‑1] 공격을 알려 주는 기능 List 20](#_Toc441060697)

**그 림 목 차**

[[그림 1‑1] NIDS와 HIDS 11](#_Toc441072461)

[[그림 1‑2] Splunk의 주요기능 13](#_Toc441072462)

[[그림 1‑3] Splunk 그래프와 통계 15](#_Toc441072463)

[[그림 1‑4] Cuckoo Sandbox 실행화면 16](#_Toc441072464)

[[그림 1‑5] Cuckoo Sandbox 파일 분석결과 창 18](#_Toc441072465)

[[그림 2‑1] GNS3 구축 환경 19](#_Toc441072466)

[[그림 2‑2] Show ip route 명령어 실행 결과 20](#_Toc441072467)

[[그림 2‑3] hping3를 이용한 Ping of Death 21](#_Toc441072468)

[[그림 2‑4] 공격 후 패킷 분석 21](#_Toc441072469)

[[그림 2‑5] Snort에서 Local Rules 생성 22](#_Toc441072470)

[[그림 2‑6] Ping of Death에 대한 Snort 알림 화면 22](#_Toc441072471)

[[그림 2‑7] hping3를 이용한 Land Attack 23](#_Toc441072472)

[[그림 2‑8] Land Attack 후 패킷분석 결과 23](#_Toc441072473)

[[그림 2‑9] sameip 옵션 추가 24](#_Toc441072474)

[[그림 2‑10] Land Attack Log기록 24](#_Toc441072475)

[[그림 2‑11] Nmap SYN Scan 25](#_Toc441072476)

[[그림 2‑12] 열린 포트 확인 25](#_Toc441072477)

[[그림 2‑13] SYN, ACK, NULL Rule 정책 추가 26](#_Toc441072478)

[[그림 2‑14] Port Scan 시 알림 26](#_Toc441072479)

[[그림 2‑15] 공격자 Netcat 명령어 27](#_Toc441072480)

[[그림 2‑16] Reverse Shell 연결 27](#_Toc441072481)

[[그림 2‑17] 접속 성공 27](#_Toc441072482)

[[그림 2‑18] Netcat Rule 정책 추가 28](#_Toc441072483)

[[그림 2‑19] Netcat Log기록 확인 28](#_Toc441072484)

[[그림 2‑20] Telnet 접속 실패 29](#_Toc441072485)

[[그림 2‑21] Login 실패 시 정책 29](#_Toc441072486)

[[그림 2‑22] Alert의 Log기록 30](#_Toc441072487)

[[그림 2‑23] Splunk Log Table 31](#_Toc441072488)

[[그림 2‑24] Dashboard 32](#_Toc441072489)

[[그림 2‑25] Python 설치 및 버전 확인 33](#_Toc441072490)

[[그림 2‑26] Yara 설치 및 버전 확인 33](#_Toc441072491)

[[그림 2‑27] cuckoo.conf 33](#_Toc441072492)

[[그림 2‑28] cuckoo.py 실행 34](#_Toc441072493)

[[그림 2‑29] Cuckoo Sandbox 파일분석페이지 35](#_Toc441072494)

[[그림 2‑30] Python 코딩 36](#_Toc441072495)

[[그림 2‑31] Python Overload 실행화면 37](file:///C:\Users\Project\Open%20Source를%20이용한%20IDS구축%20및%20네트워크%20관리%20프로그램_v1.0_0120.docx#_Toc441072496)

[[그림 2‑32] VIEW 실행 화면 37](#_Toc441072497)

# 프로젝트 개요

* 1. 프로젝트 목표

기존

* 1. 팀원 및 역할

아래

|  |  |
| --- | --- |
| 이름 | 역할 |
|  | - 총 |
| ) | - 네트워크 구 |
|  | - 보고서 작 |

[표 ‑] 팀원 및 역할

* 1. 프로젝트 일정

아래 [표 1-2]와

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | 1주차 | | 2주차 | | 3주차 | | 4주차 | | 5주차 | |
| 자료조사 |  |  |  |  |  |  |  |  |  |  |
| 환경 |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

[표 ‑] 프로젝트 일정

* 1. 프로젝트 환경

아래 [표 1-3]의 프로그램들을 이용하여 프로젝트를 진행하였다.

|  |  |  |
| --- | --- | --- |
| 운영 체제  (Snort, Splunk) |  | CentOS 6.7 |
| 운영 체제  (Yara, Cuckoo Sandbox) | C:\Users\kitri\Downloads\Files for web\PNG\canonical-friends_orange_hex.png | Ubuntu 15.04 |
| 가상 환경 |  | VMware 11 |
| 개발 언어 |  | Python 2.7.9 |
| 네트워크 구축 |  | GNS3 1.3.4 |
| 공격 시도 |  | Kali Linux 2.3.0.5 |

[표 ‑] 프로젝트 환경

* 1. 부분별 기대효과
     1. 현황 (AS-IS)
* 비정상적인 공격이 있을 경우 차단 방법 없다.
* .  
  + 1. 개선 및 기대효과 (TO-BE)
* Rule 정책으로 인한 패턴 적용으로 비정상적인 공격 인식 가능하다.
  1. Ope
     1. ID

1. 개요

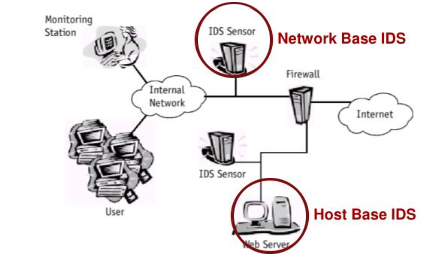
* Intrusion Detecti

1. NIDS (Network 기반)

* 네트워크에서

1. HIDS (Host 기반)

* 전체적인



[그림 ‑] NIDS와 HIDS

* + 1. Snort

1. 개요

* 패킷 수집

1. 기능

* 침입탐지 Rule에 일치되는 네트워크 트래픽을 감시하고 기록 및 경고
* 프로토콜 분석,

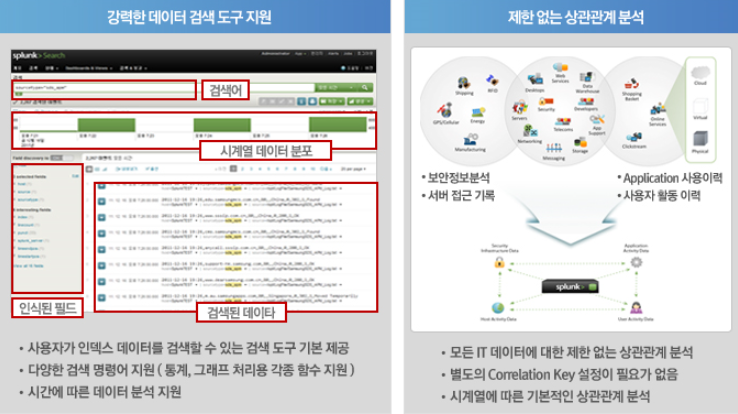
1. 구조

* Sniffer :
  + 1. Splunk

1. 개요

* IT분야에서

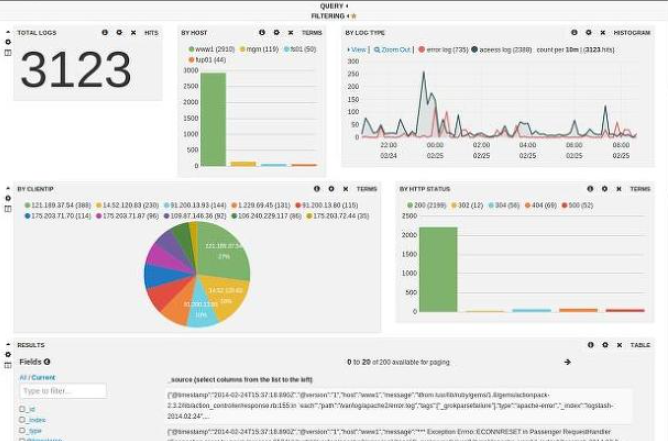
1. 기능



[그림 ‑] Splunk의 주요기능

1. 데이터 수집 및 인덱싱

* Log, 네트워크 트래픽, 웹 서버, 클라우드 서비스 등 형식이나 위치에 관계없이 데이터를 인덱싱
* 구조 및 스키마가 검색 시에만 적용되기 때문에 데이터를 제한 없이 분석가능

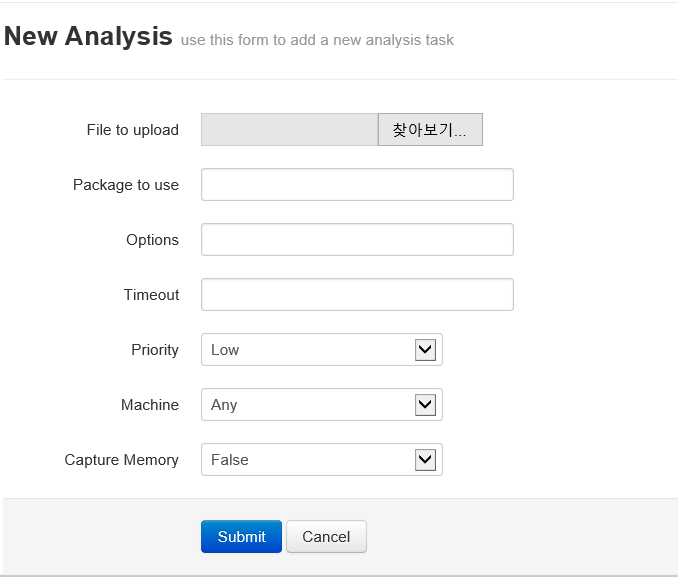


[그림 ‑] Splunk 그래프와 통계

1. 시각화 및 보고

* 운영 또는 보안 요구 사항에 따라 조정된 사용자 지정 대시보드 및 보고서에서 동향 및 특징을 초보자도 보기 간편하게 시각화
  + 1. Yara / Cuckoo S

1. 개요
2. Yara
   * 악성코드
3. Cuckoo Sandbox
   * 악성코드를 진단하는데
4. 기능



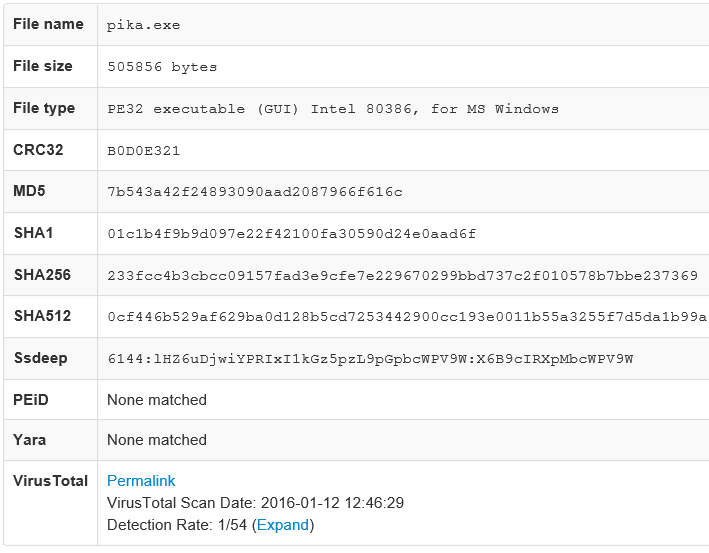
[그림 ‑] Cuckoo Sandbox 실행화면

1. 특징

* 공개 소스코드
* CUI /
* 분석
  + 기본 윈도우 실행 파일, DLL 파일

1. 출력으로 나오는 결과물

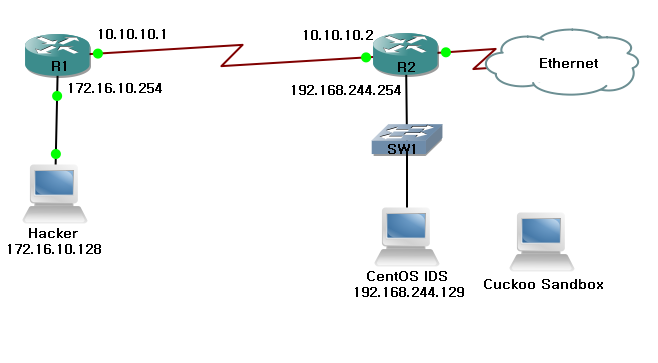
* 악성코드에 의해
* 악성코드에 의해 생성
* 있는)가상머신의 풀 메모리 덤프(Full memory dump) 파일



[그림 ‑] Cuckoo

# 프로젝트 내용

2. 1. GN



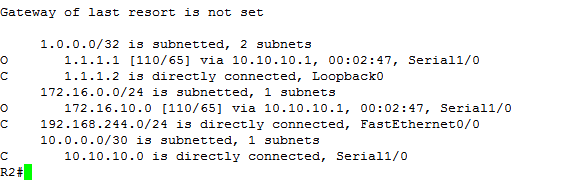
[그림 ‑] GNS3 구축 환경

위 [그림 2-4]

위 [그림 2-4]와

아래[그림 2-2]

악성코드를 분석



[그림 ‑] Show i

Router설정은 OSPF.

* 1. Snort를
     1. 공격

|  |  |
| --- | --- |
| 항목 | 설명 |
| Ping of Death | ICMP패킷을 이용하는 |
| Land Attack | 출발지와 목적지의 |
| Nmap | 공격대상의 |
| NetCat | TCP / UDP로 피해자에 |
| Telnet 접속 실패 시  Log 알림 | 내외부에서 |

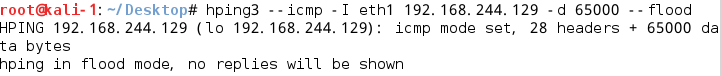
[표 ‑] 공격

위 [표 2-1]의

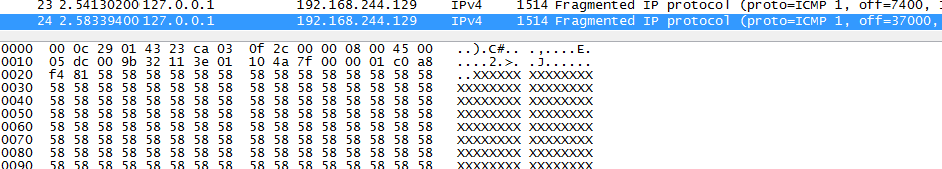
2. 2. 2. Ping of Death
3. Ping of

* Ping패킷에

1. 공격 후



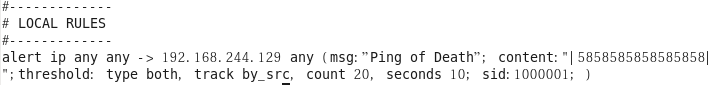
[그림 ‑] hping3를



[그림 ‑] 공격

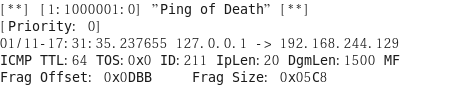
* 위 [그림 2-3], [그림
* ICMP 데이터가

1. Rule 정책 추가 및



[그림 ‑] Snort에서

* 192.168.244.129 생성
* Rule 정책



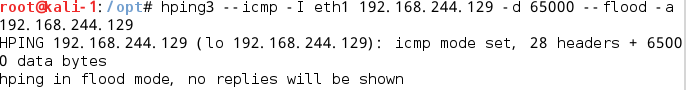
[그림 ‑] Ping of Death에

* 위 [그림 2-6]과 같이 다시
  + 1. Land Attack

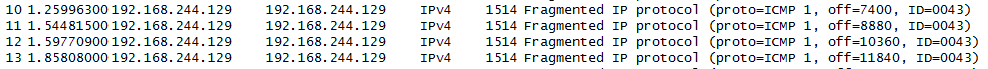
1. Land Attack

* LAN Denial Attack의 약자로 IP Spoofing을 이용한 SYN 공격
* 공격자는
* 이 과정이 반복 시 시스템 버퍼가 범람하게 되어 결과적으로 서비스거부 상태가 된다.

1. 공격 후



[그림 ‑] hping3를



[그림 ‑] Land

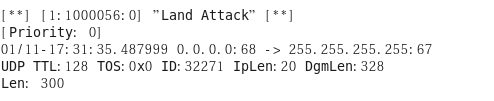
* 위 [그림 2-8]과 같

1. Rule 정책 추가



[그림 ‑]

* 위 [그림 2-9]의



[그림 ‑] Land A

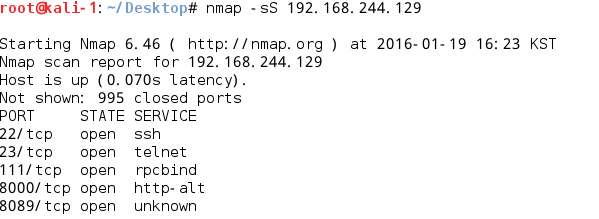
* 위 [그림 2-10]과 같이
  + 1. Nma

1. Nmap

* 고든 라이온이
* 활용성이 높아 악의적으로

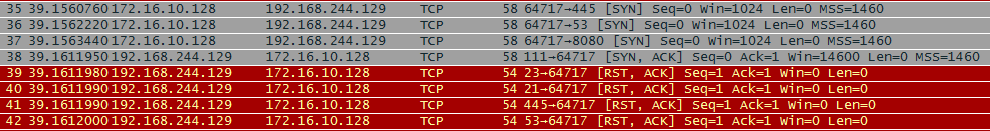
1. 공격

* 아래 [그림 2-11]은 S

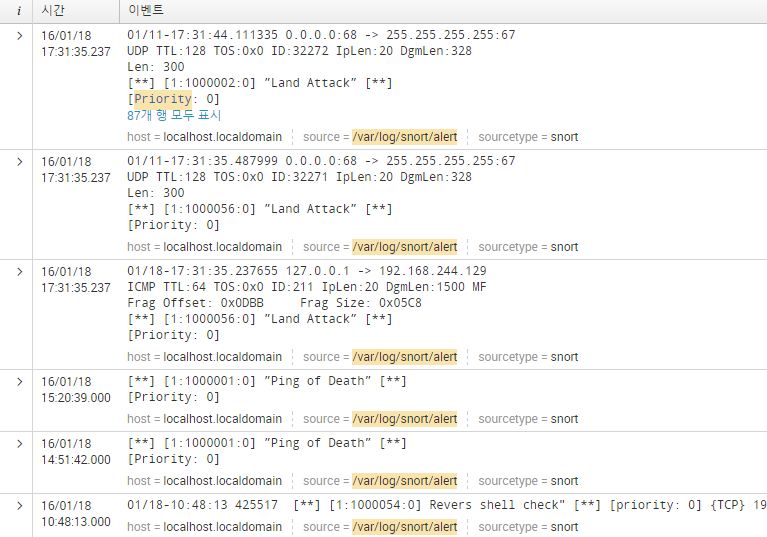


[그림 ‑] Nmap

* 아래 [그림 2-12]과



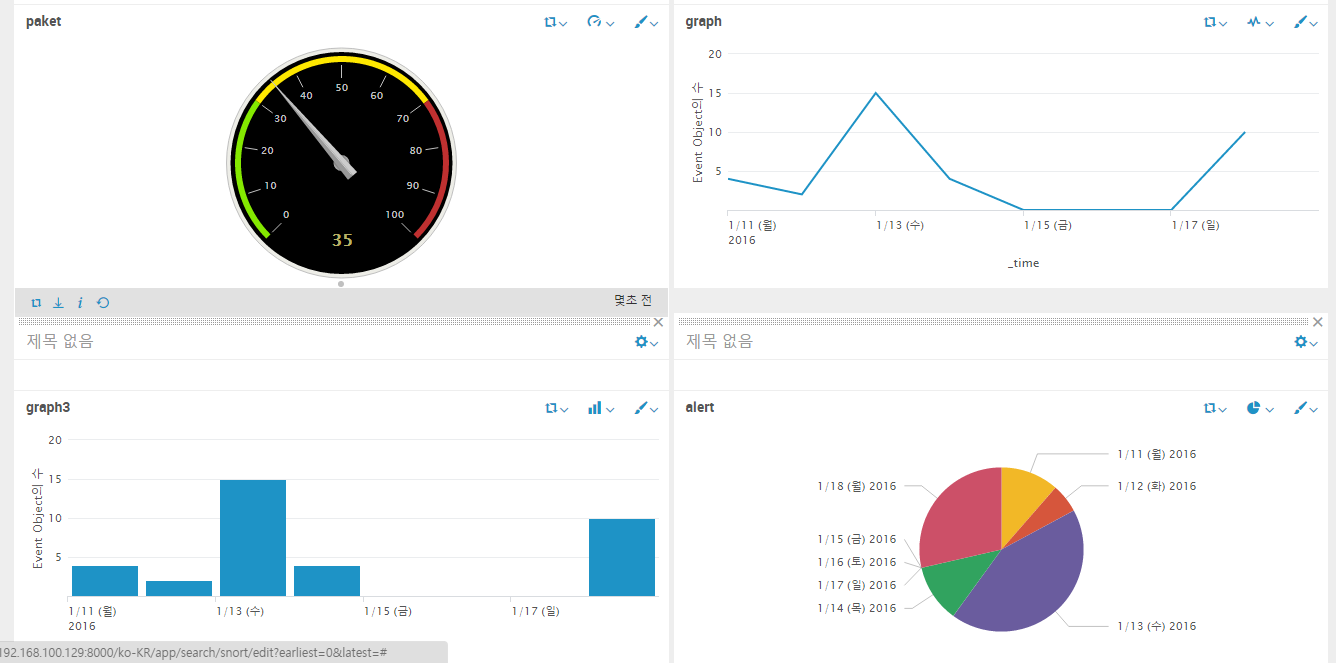
[그림 ‑] 열린 포트 확인

* 1. Splunk로 

[그림 ‑] Splunk

위 [그림 2-23]과 같이 Snort의

프로젝트에서는



[그림 ‑] Dashboard

위 [그림 2-24]와 같이 연동시킨 Snort

.

* 1. Yara /
     1. Python

EMB000022d8023d

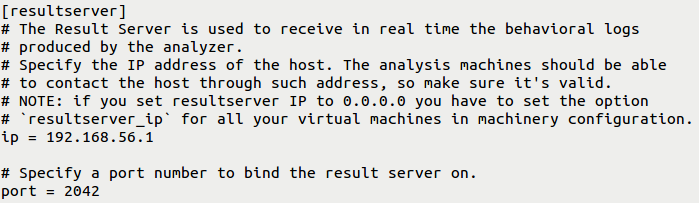
[그림 ‑] Python

EMB000022d80240

[그림 ‑] Yara

* 위 [그림2-25], [그림2-25]와 같이 Cuckoo Sandbox 실행을 위한 파일을 설치한다.
* 못하지만 패턴기반으로 악성 파일이나 프로세스를 탐지한다.

2. 4. 2. Cuckoo



[그림 ‑] cuckoo.conf

* vi /opt/cuckoo/conf/.

# 결론

IDS 시스템은 다양한

람이 있다.

# 추후과제 및 후기

이번 IDS서버 구축

# 참고자료

[1] Snort