



실시간 취약점 관리체계 구현

연구 참여자 : 정현경 황선홍 배대식 조현욱 조수홍 표상영
2018.07.12



목차.

- 01 서론
- 02 요소 기술
- 03 구현 설계
- 04 결과
- 05 향후 계획

서론.

- 01 취약점 관리의 필요성
- 02 통합 보안관제의 실태

취약점 관리의 필요성.

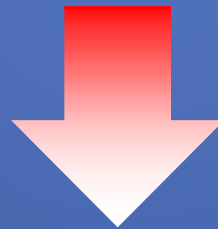
D'breed



일년에 몇 번 하는 검사로는 충분하지 않다.

취약점은 매일 동적으로 변화하고 있다.

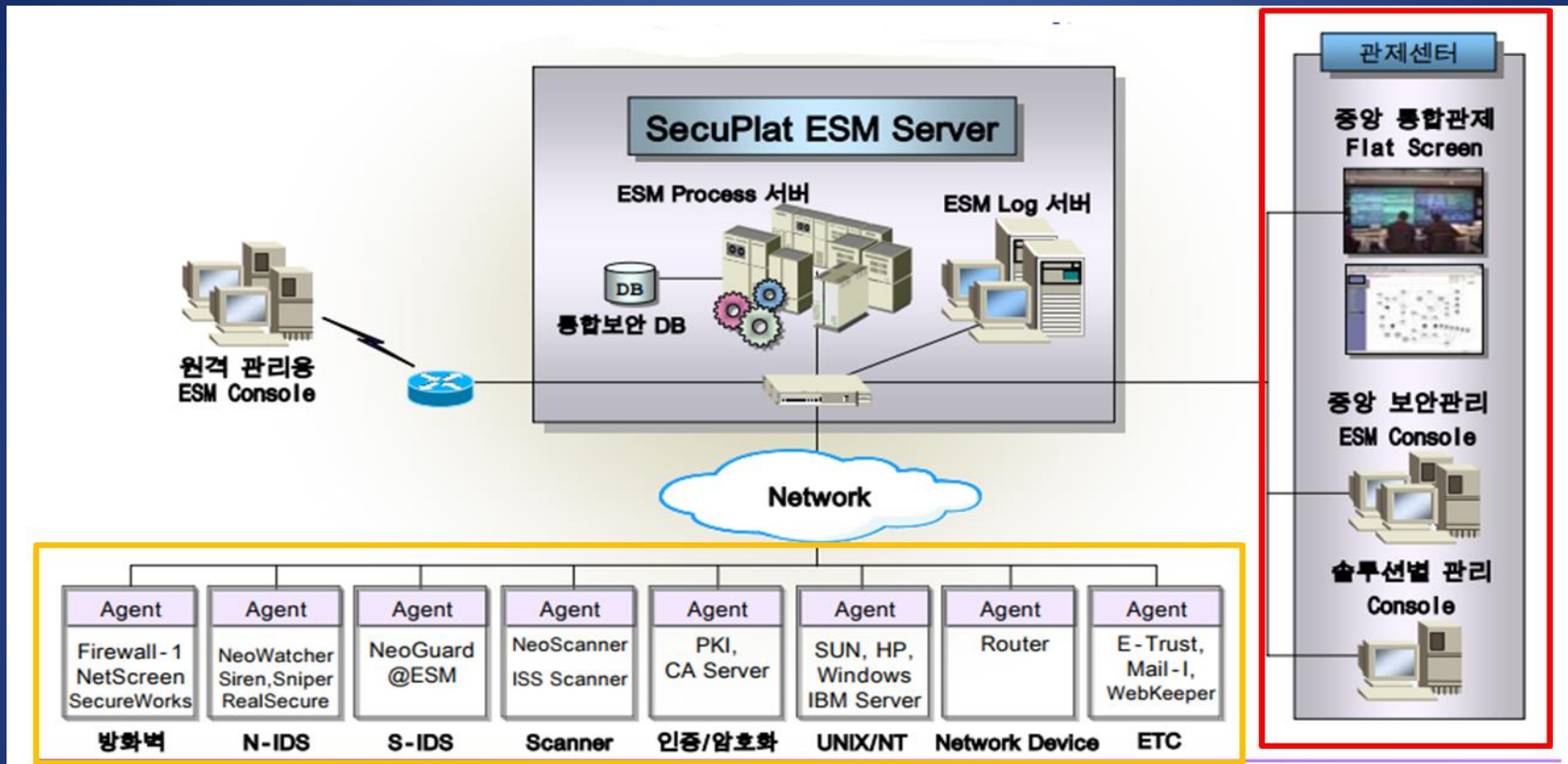
IT 인프라는 새로운 포트, 서비스, 호스트의 생성 등 동적으로 변화 중이다.



실시간 항시 운용체계 필요

통합 보안관제의 실태.

D'breed



방화벽, N-IDS, S-IDS, Scanner, 인증/암호화 등 여러개의 Agent보안관리를 중앙 관제센터에서 통합적으로 관리 취약점영역은 미관리 영역임

➡ 상시 운용 SIEM체계에 실시간 관리 가능한 취약점 부분 통합운영 필요

요소 기술.

01 ESM & SIEM

02 Splunk

03 OWAS ZAP

04 NMAP

ESM & SIEM.

D'breed



ESM (Enterprise Security Management) 전사적보안관리시스템

- 기능별, 제품별로 모듈화된 보안관리 기능을 통합하여 일관되고, 직관적인 관리자 및 사용자 인터페이스를 제공
- 효율적이고 정책지향성의 체계적인 보안관리 시스템을 구축
- 표준 정책 기반하에서 모든 시스템의 통합 보안관리를 이용한 보안관제의 효율성을 제공하기 위한 체계

SIEM (Security Information and Event Management)

- 네트워크와 보안장비로부터 정보를 모으고 분석하여 제시하는 시스템으로 관리 프로그램의 식별과 접근, 취약점 관리와 협력적 정책, 운영체제, 데이터베이스와 프로그램 로그, 그리고 외부 위협을 포함하는 통합관리체계
- SIM와 SEM가 조합
- 네트워크, 하드웨어 및 응용 프로그램에 의해 생성된 보안 경고의 실시간 분석

ESM은 Event 위주의 단시간 위협분석과 DBMS기반
SIEM은 빅데이터 수준의 장기간(수개월) 심층분석과 Indexing 기반

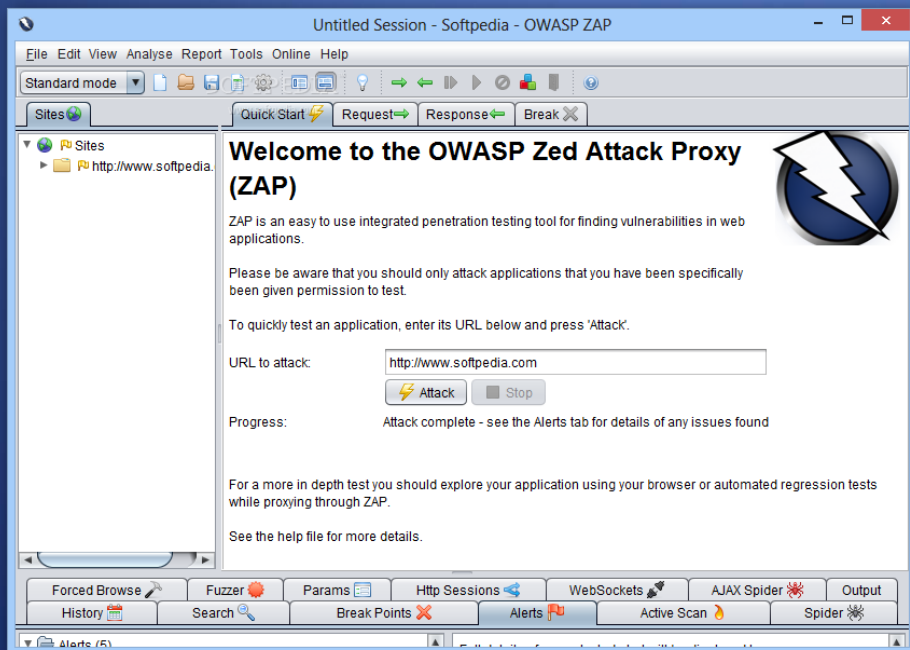
- 오픈소스 SIEM tool
- IT분야에서 발생하는 로그 데이터, 실시간 이벤트 데이터 및 다양한 장비 데이터를 수집하고 모니터링하며 검색, 분류, 분석할 수 있는 엔진을 제공
- 다양한 분석을 통해 사용자가 원하는 대쉬보드를 자유롭게 생성할 수 있음



OWASP ZAP.

D'breed

- 오픈 소스 웹 응용 프로그램 보안 스캐너
- 전문 보안 침투 테스터뿐 아니라 애플리케이션 보안에 익숙하지 않은 사람도 사용 가능 (GUI 제어판 제공)
- 프록시 서버 차단, AJAX 웹 크롤러, 자동 스캐너, 수동 스캐너, 강제 찾아보기, Fuzzer, WebSocket 지원, 스크립팅 언어 및 Plug-n-Hack 지원
- 플러그인 기반 아키텍처와 새로운 또는 업데이트 된 기능을 추가 할 수 있는 온라인 '마켓 플레이스'를 가지고 있음



고든 라이온(Gordon Lyon)이 작성한 보안 스캐너

Nmap은 원격 컴퓨터들의 자세한 정보를 알아내고 네트워크 “지도”를 생성
운영 체제, 장치 종류, 운영 시간, 서비스에 쓰이는 소프트웨어 제품, 그 제품의
정확한 버전, 방화벽 기술의 존재와 심지어 근거리 네트워크에서 네트워크 카드의
공급자도 포함

기능

호스트 탐지 - 네트워크상의 컴퓨터들을 확인한다. 예를 들어 ping 응답이나 특정 포트가 열린 컴퓨터들을 나열한다.

포트 스캔 - 하나 혹은 그 이상의 대상 컴퓨터들에 열린 포트들을 나열한다.

버전 탐지 - 응용 프로그램의 이름과 버전 번호를 확인하기 위해 원격 컴퓨터의 네트워크 서비스에 주의를 기울인다.

운영 체제 탐지 - 원격으로 운영 체제와 네트워크 장치의 하드웨어 특성을 확인한다.

```
Starting Nmap 6.00 ( http://nmap.org ) at 2012-05-17 12
Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.00031s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh         OpenSSH_5.3p1 Debian 3ubuntu7
|_ ssh-hostkey: 1024 1a:0a:d6:67:54:9d:0a:00:00:00:00:00:00:00:00:00
|_ 2048 79:f8:5b:4a:34:11:2c:63:bb:1f:02:4c:6c:90:82:85:ec
80/tcp    open  http        Apache/2.2.3 ((Ubuntu))
|_ http-titles:
9929/tcp  open
Device type: general purpose
Running: Linux 2.6.X|3.X
OS CPE: cpe:/o:linux:kernel:2.6 cpe:/o:linux:kernel:3
OS details: Linux 2.6.32 - 2.6.39, Linux 2.6.38 - 3.0
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel
```



구현 설계.





01 구현 환경

02 시연 영상



Simple_Console.cpp

콘솔 환경
SIEM 서비스



Simple_Agent.cpp

에이전트 환경
취약점 스캐닝

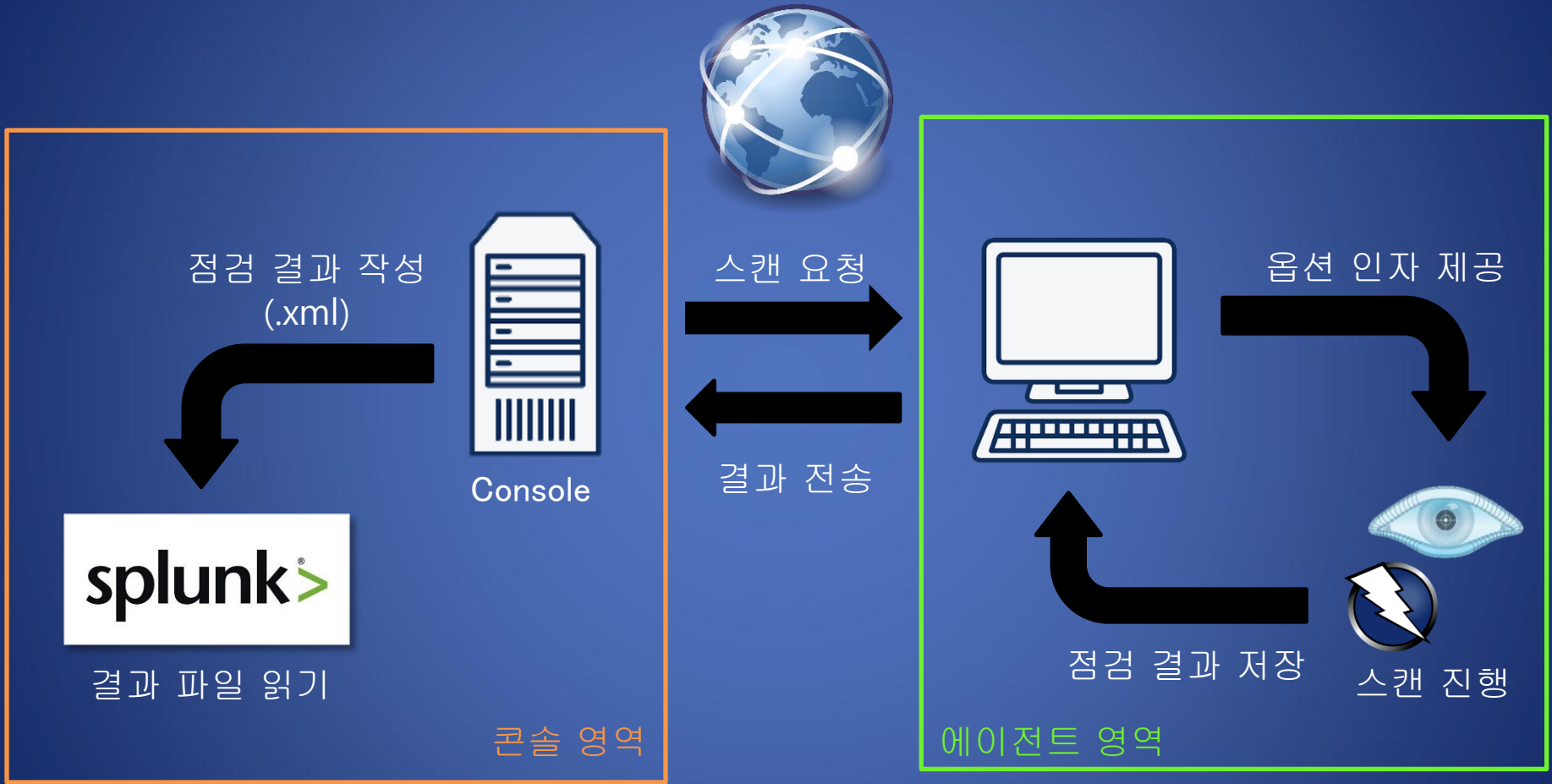


웹서버



DB

점검 대상 환경



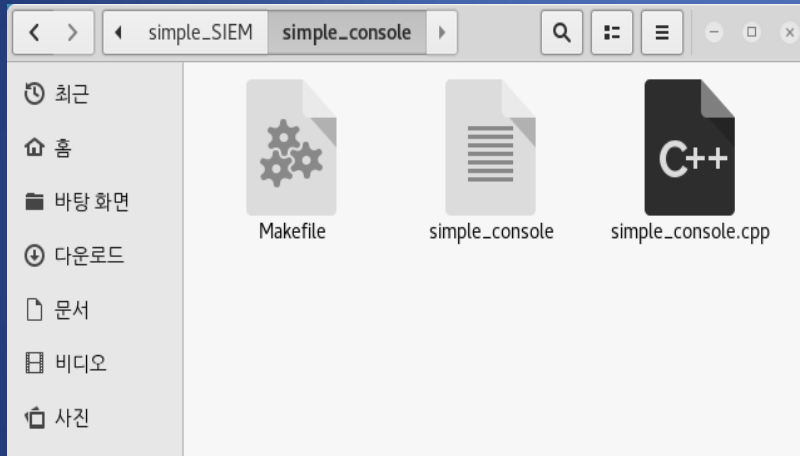
결과.

01 View

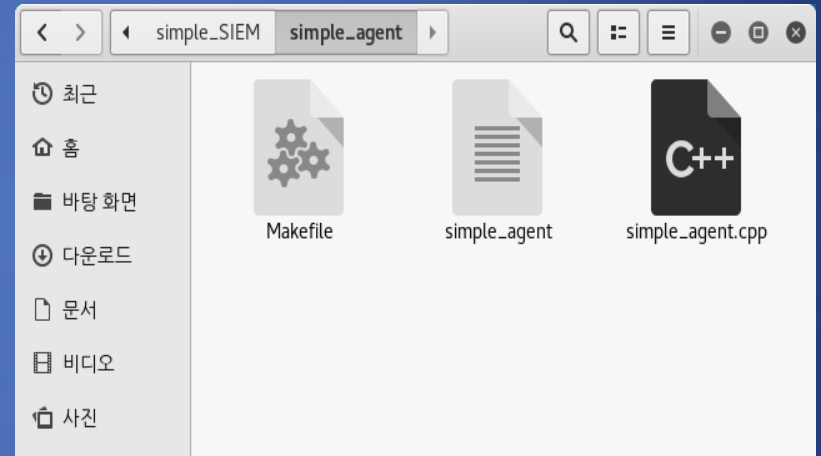
02 시연 영상



프로그램

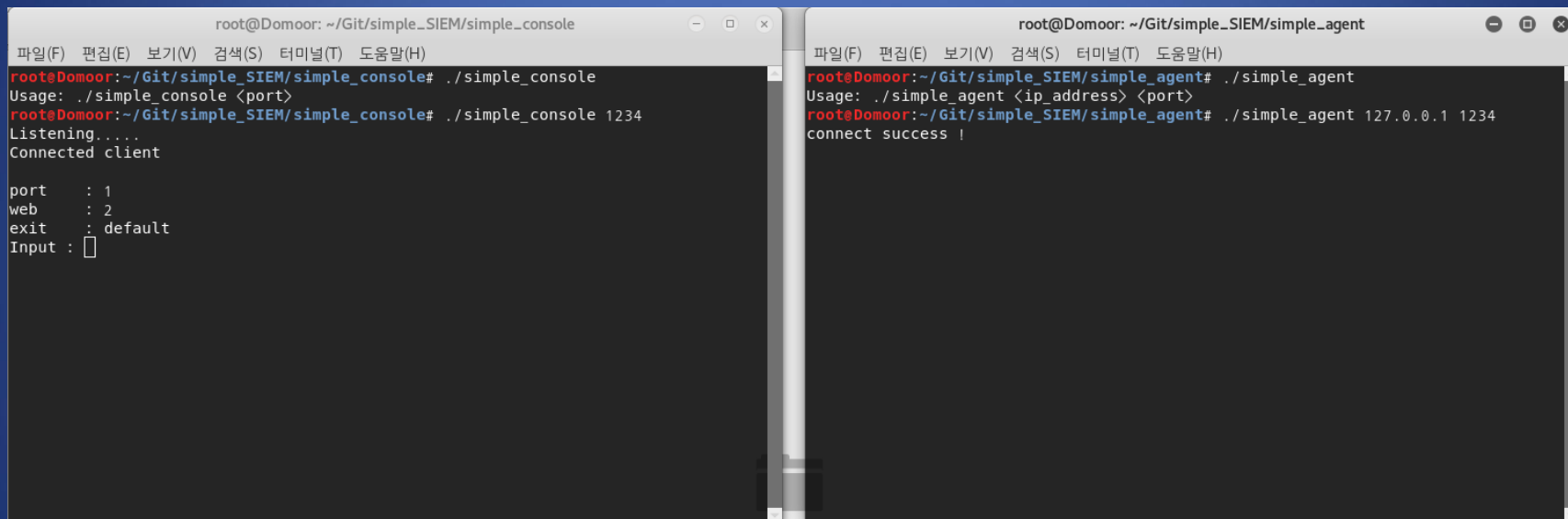


콘솔 프로그램 화면



에이전트 프로그램 화면

초기 화면

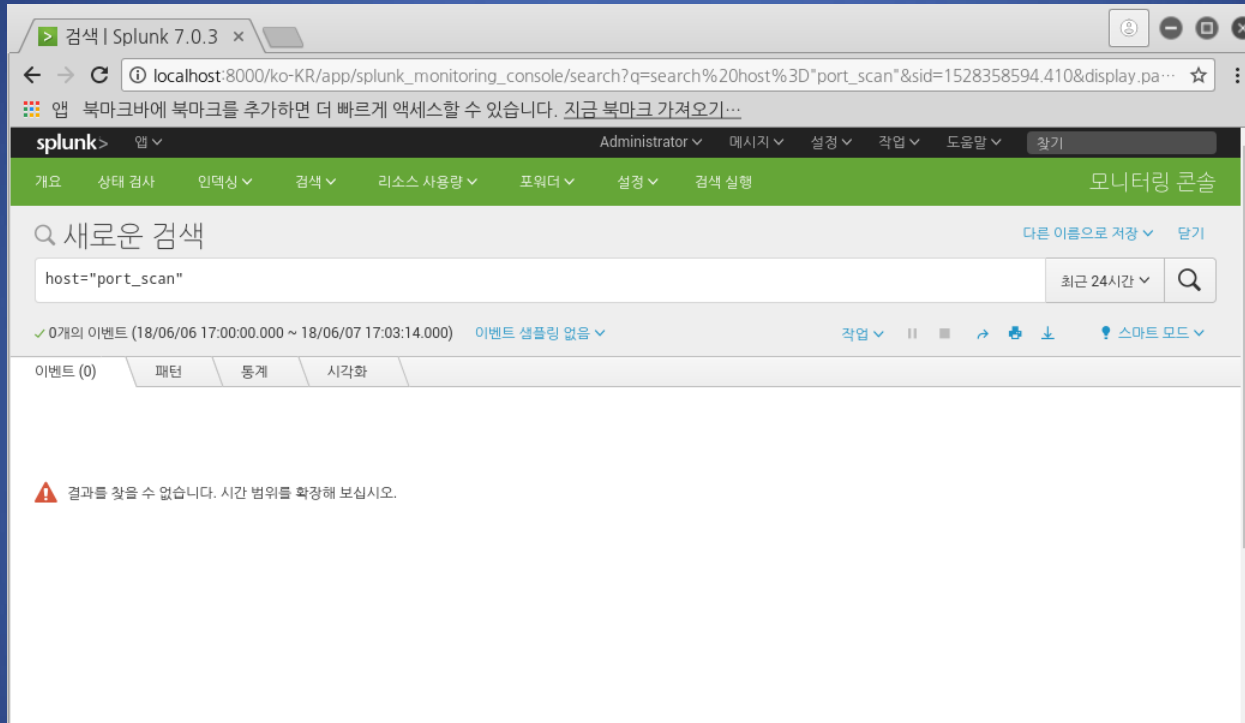


```
root@Domoor: ~/Git/simple_SIEM/simple_console
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
root@Domoor:~/Git/simple_SIEM/simple_console# ./simple_console
Usage: ./simple_console <port>
root@Domoor:~/Git/simple_SIEM/simple_console# ./simple_console 1234
Listening.....
Connected client

port   : 1
web    : 2
exit   : default
Input : 
```

```
root@Domoor: ~/Git/simple_SIEM/simple_agent
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
root@Domoor:~/Git/simple_SIEM/simple_agent# ./simple_agent
Usage: ./simple_agent <ip_address> <port>
root@Domoor:~/Git/simple_SIEM/simple_agent# ./simple_agent 127.0.0.1 1234
connect success !
```

콘솔 및 에이전트 프로그램 실행 화면



포트 스캔 전 Splunk 로그 확인

포트 스캔

```
root@Domoor: ~/Git/simple_SIEM/simple_console
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
root@Domoor:~/Git/simple_SIEM/simple_console# ./simple_console
Usage: ./simple_console <port>
root@Domoor:~/Git/simple_SIEM/simple_console# ./simple_console 1234
Listening.....
Connected client

port      : 1
web       : 2
exit      : default
Input    : 1

열려있는 포트에 대해 검사를 시작합니다.
취약점 검사 대상을 입력해 주세요.
ex) 127.0.0.1
: 192.168.40.18

검사가 완료 되었습니다.

port      : 1
web       : 2
exit      : default
Input    :

root@Domoor: ~/Git/simple_SIEM/simple_agent
파일(F) 편집(E) 보기(V) 검색(S) 터미널(T) 도움말(H)
25/tcp    open  smtp
53/tcp    open  domain
80/tcp    open  http
111/tcp   open  rpcbind
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
512/tcp   open  exec
513/tcp   open  login
514/tcp   open  shell
1099/tcp  open  rmiregistry
1524/tcp  open  ingreslock
2049/tcp  open  nfs
2121/tcp  open  ccproxy-ftp
3306/tcp  open  mysql
5432/tcp  open  postgresql
5900/tcp  open  vnc
6000/tcp  open  X11
6667/tcp  open  irc
MAC Address: 00:0C:29:82:81:39 (VMware)
Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds
설2초간 대기합니다.
점검 내역이 서버로 전송되었습니다.
```

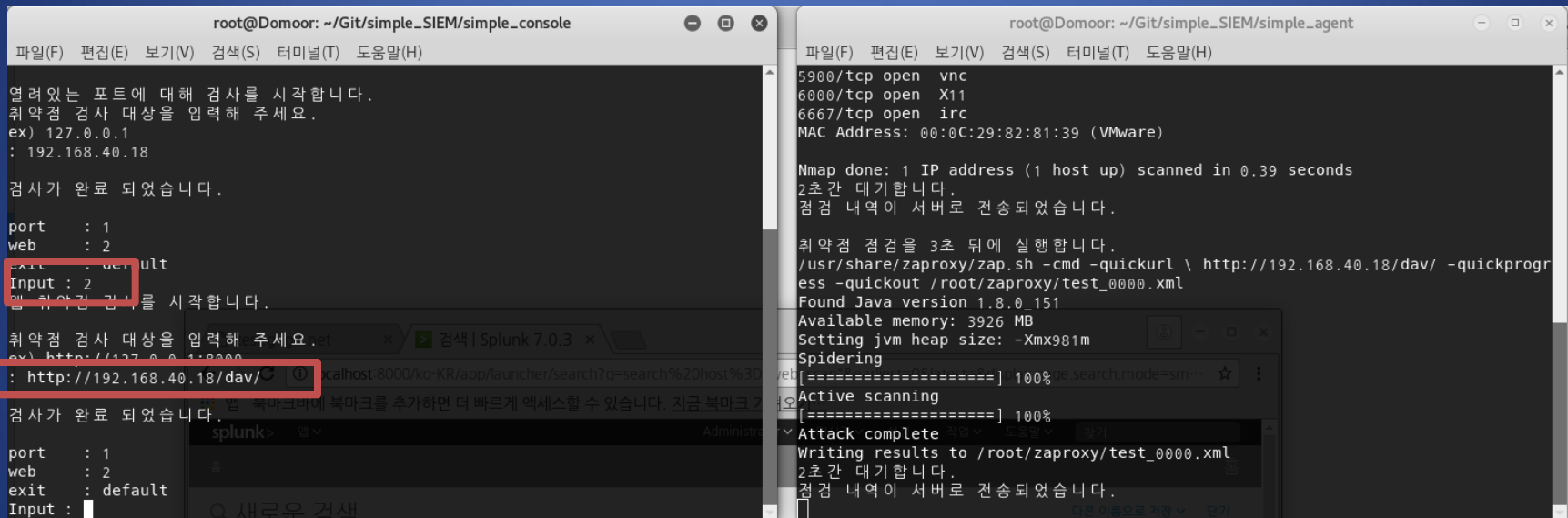
포트 스캔 선택 및 스캔 대상 입력

The screenshot shows the Splunk 7.0.3 monitoring console interface. The search bar contains the query `host="port_scan"`. Below the search bar, it indicates 3 events were found between 18/06/06 17:00:00.000 and 18/06/07 17:10:20.000. The results are displayed in a table with columns for index (i), time (시간), and event (이벤트).

i	시간	이벤트
> 1	18/06/07 17:04:46.000	<?xml version="1.0" encoding="UTF-8"?> <!DOCTYPE nmaprun> <?xml-stylesheet href="file:///usr/bin/..share/nmap/nmap.xsl" type="text/xsl"?> host = port_scan source = /opt/splunk/test/port/result_0000.xml sourcetype = xml-too_small
> 2	18/06/07 17:04:43.000	<host starttime="1528358683" endtime="1528358683"><status state="up" reason="arp-res ponse" reason_ttl="0"/> <address addr="192.168.40.18" addrttype="ipv4"/>

포트 스캔 후 Splunk 로그 확인

웹 스캔



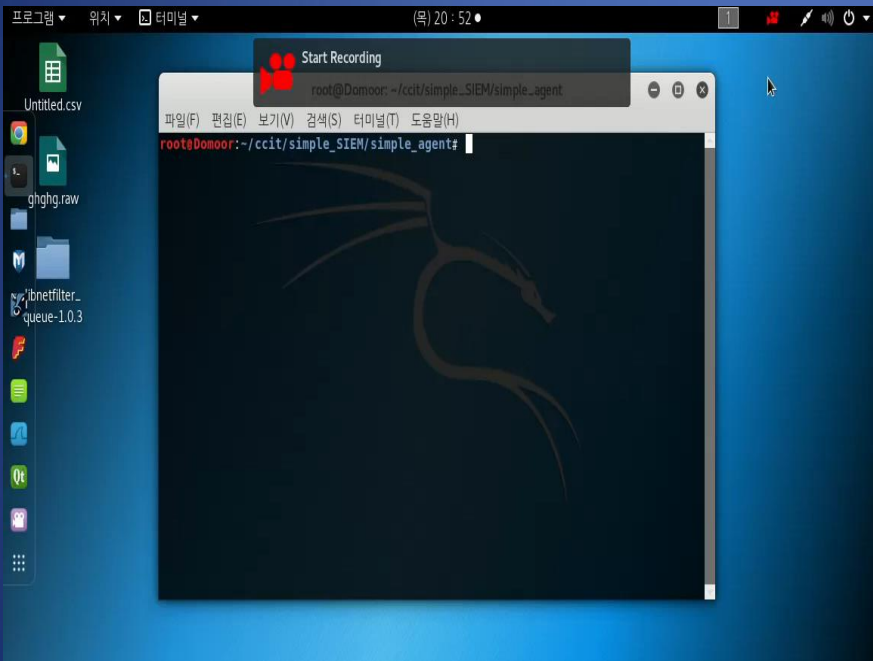
웹 스캔 선택 및 스캔 대상 입력

The screenshot shows the Splunk search interface. The search query is `host="web_scan"`. The results show one event from 18/06/07 18:01:17.000. The event details are as follows:

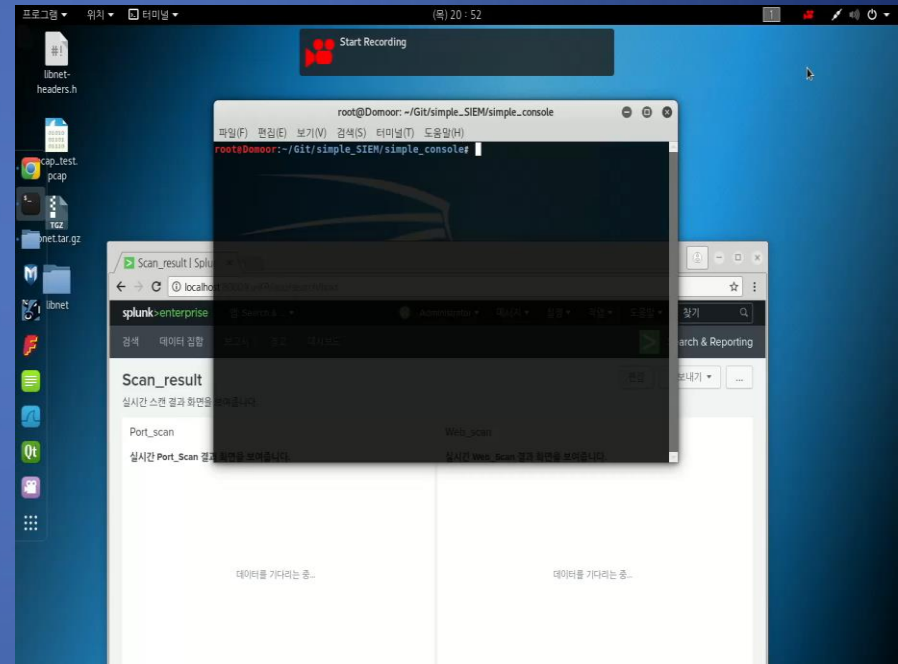
시간	이벤트
18/06/07 18:00:51.000	<pre><?xml version="1.0"?><OWASPZAPReport version="2.7.0" generated="목, 7 6월 2018 18:00:47" "> <site name="http://192.168.40.18" host="192.168.40.18" port="80" ssl="false"><alerts><al ertitem> <pluginid>10016</pluginid> <alert>Web Browser XSS Protection Not Enabled</alert> <name>Web Browser XSS Protection Not Enabled</name></pre>

웹 스캔 후 Splunk 로그 확인

Agent



Console



향후 계획.



1. 네트워크 및 시스템 영역 추가 진행예정
2. U및 보고서 영역에 대한 연구 진행
3. 관련학회 및 세미나 시 발표 및 기고 예정



기대 효과

- * SIEM+SCANNER연동구조는 국내 최초 개념으로 기존의 ESM구조와 연동시 보안 대비 비용효과 측면에서 신개념의 정보보안 로드맵
- * 취약점분석 공개S/W를 이용하는 구조는 정보보안 운용자에 의한 손쉬운 운용과 기존 보안서비스와의 통합운용으로 침해대응체계 고도화



END