D'breed

실시간 취약점 관리체계 구현

연구 참여자 : 정현경 황선홍 배대식 조현욱 조수홍 표상영

2018.07.12

CCIT CULTURE CONTENTS & INFORMATION TECHNOLOGY

Dbreed

목차.

Dbreed

서론.

01 취약점 관리의 필요성

02 통합 보안관제의 실태

취약점 관리의 필요성.

D'breed

일년에 몇 번 하는 검사로는 충분하지 않다.

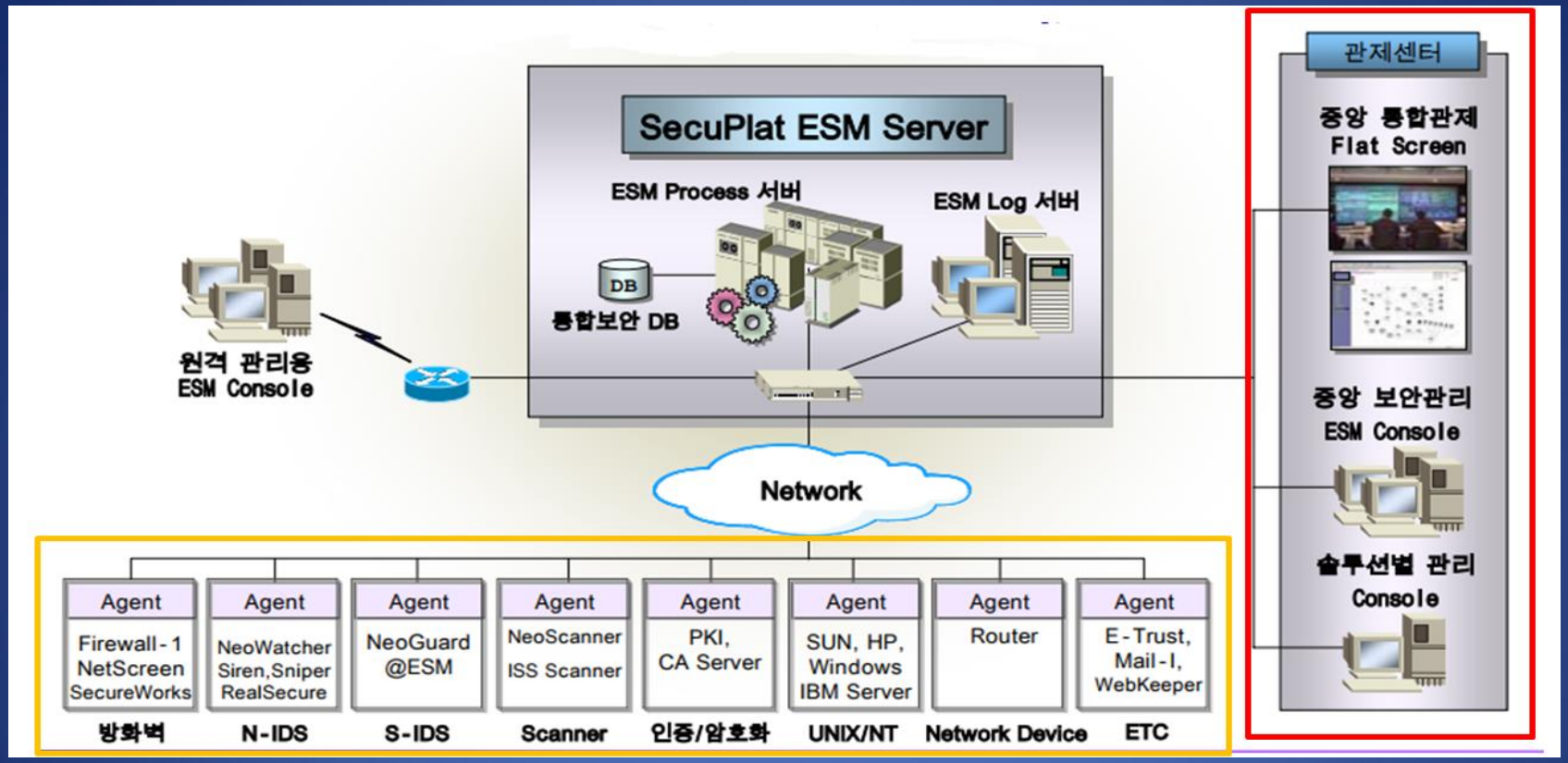
취약점은 매일 동적으로 변화하고 있다.

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

실시간 항시 운용체계 필요

통합 보안관제의 실태.

Dbreed



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

Dbreed

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

Splunk.

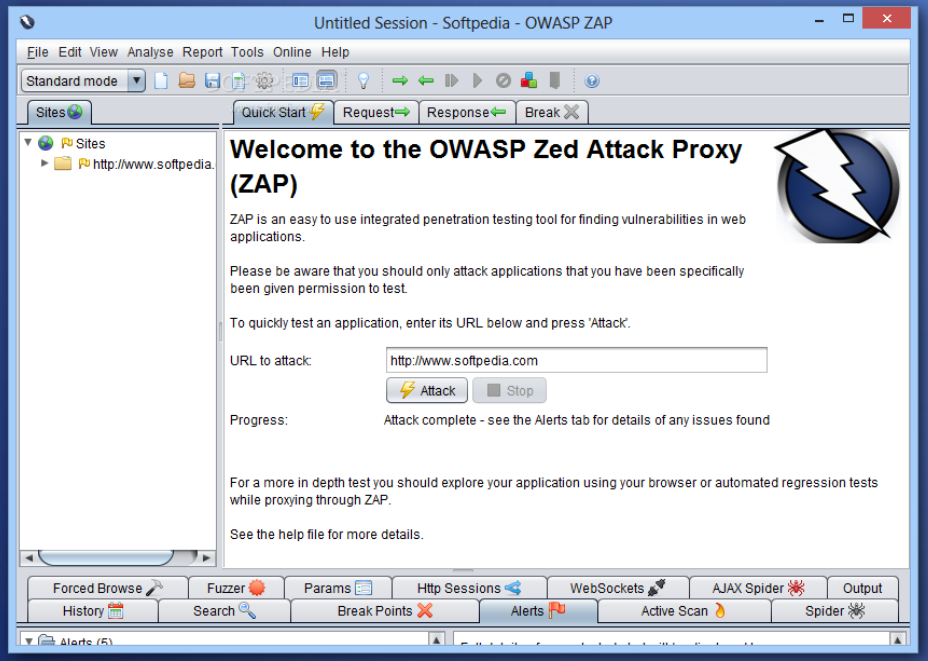
D'breed

- 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



NMAP.

Dbreed

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.

Dbreed

구현 설계.

01 구현 환경

02 시연 영상

구현환경

Dbreed

KALI

splunk>

C++

Simple_Console.cpp

콘솔 환경
SIEM 서비스

KALI

OWASP ZAP

NMAP

C++

Simple_Agent.cpp

에이전트 환경
취약점 스캐닝

Linux

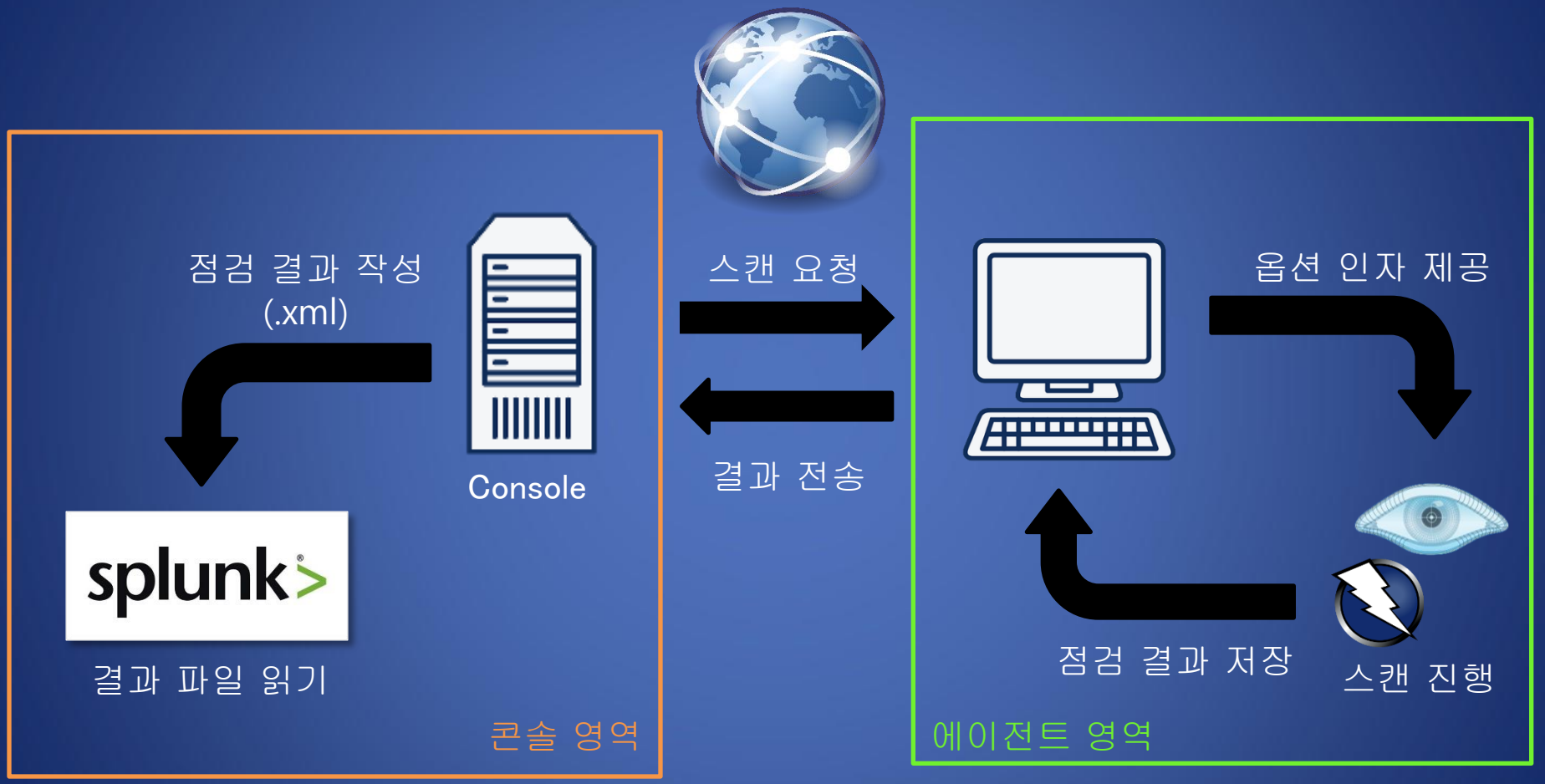
웹서버

DB

점검 대상 환경

프로세스

Dbreed


점검 결과 작성
(.xml)
Console
스캔 요청
결과 전송
옵션 인자 제공
splunk>
결과 파일 읽기
콘솔 영역
점검 결과 저장
스캔 진행
에이전트 영역

결과.

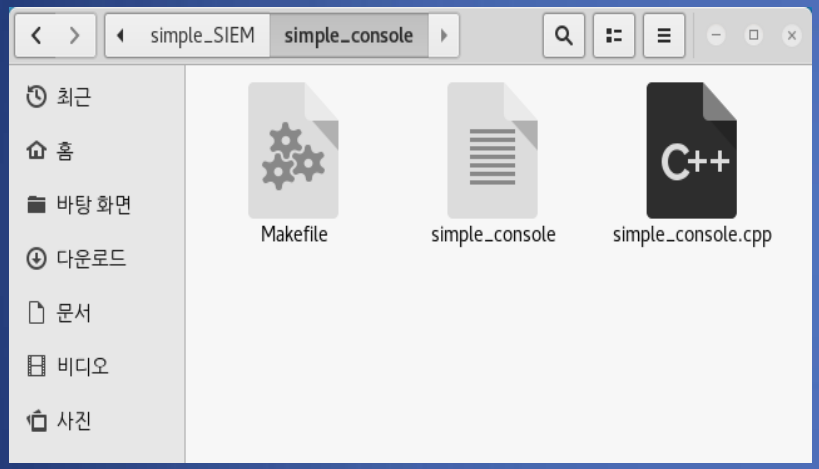
01 View

02 시연 영상

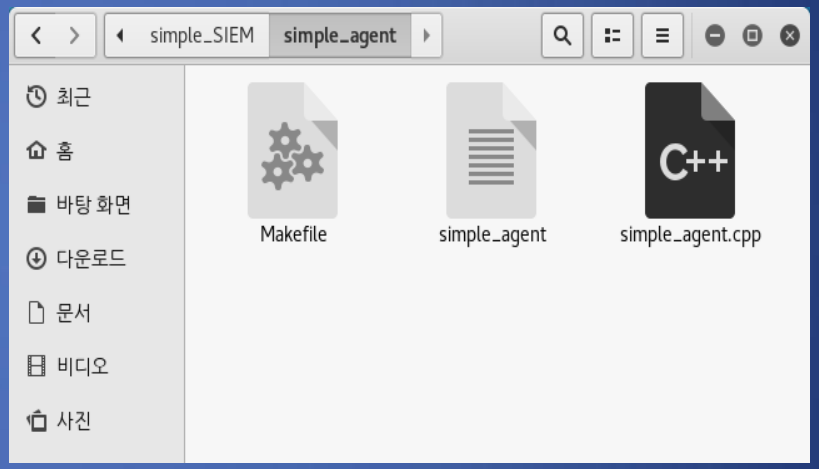
View.

Dbreed

프로그램



콘솔 프로그램 화면

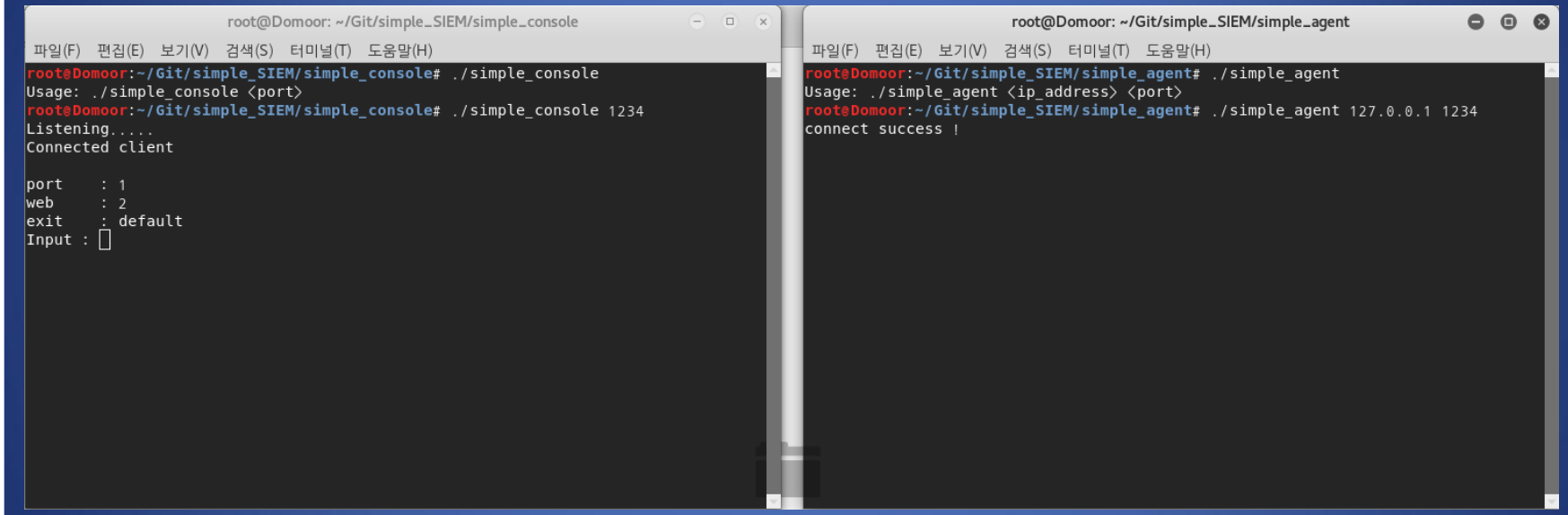


에이전트 프로그램 화면

View.

Dbreed

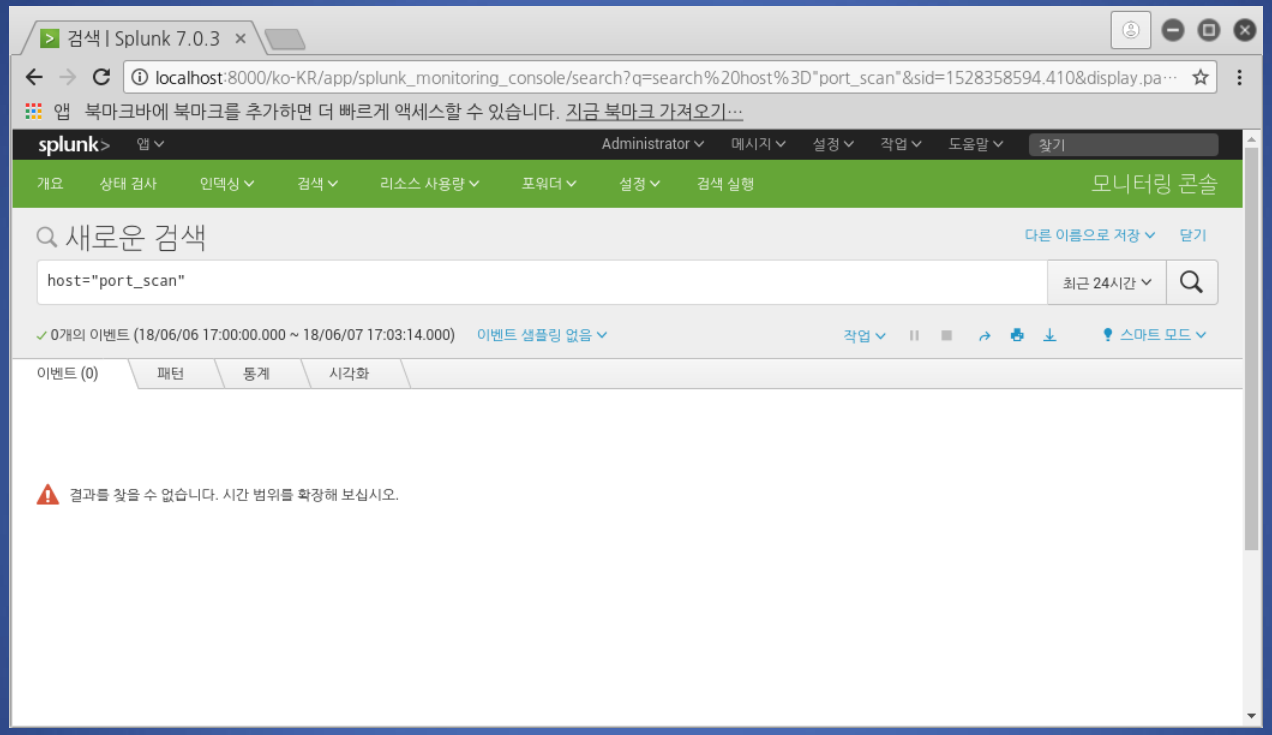
초기 화면



콘솔 및 에이전트 프로그램 실행 화면

View.

Dbreed

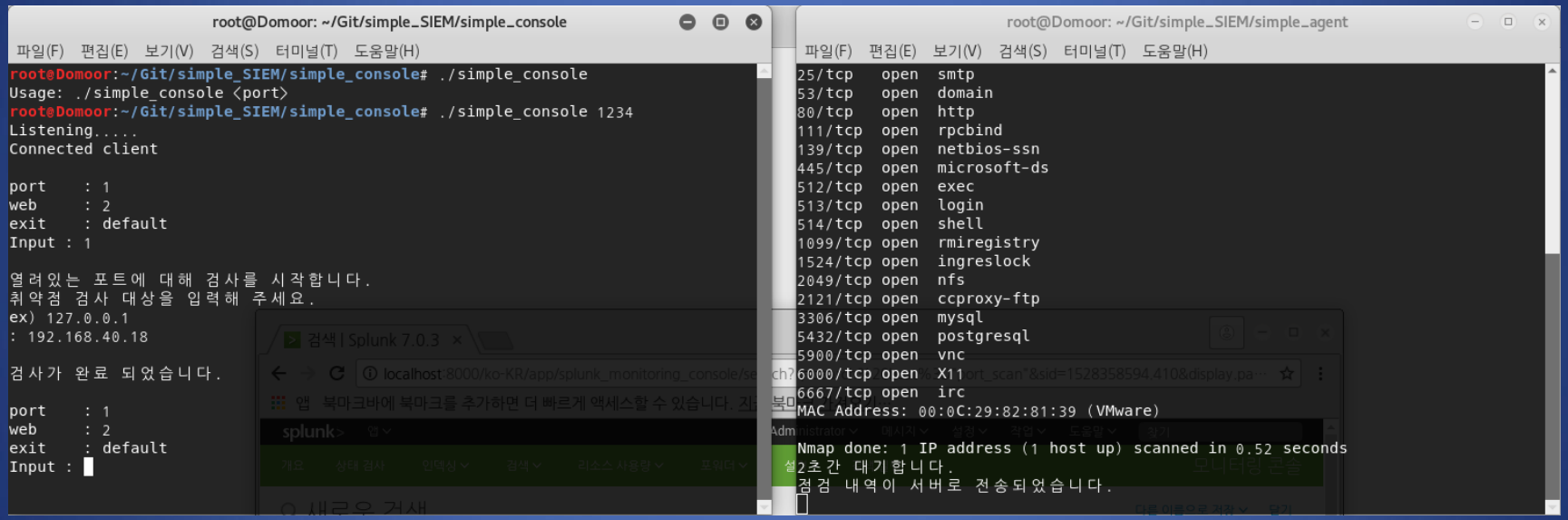


포트 스캔 전 Splunk 로그 확인

View.

Dbreed

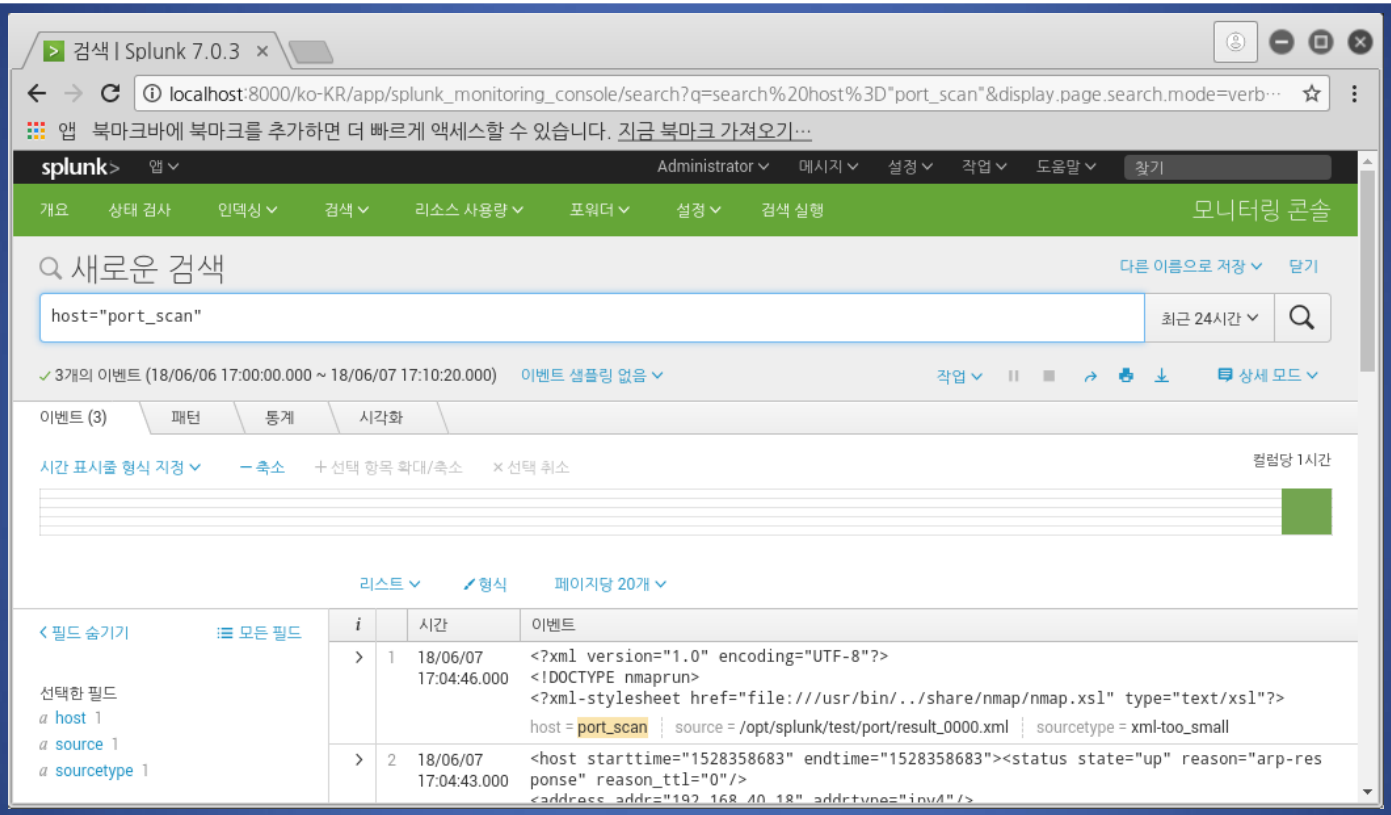
포트 스캔



포트 스캔 선택 및 스캔 대상 입력

View.

Dbreed

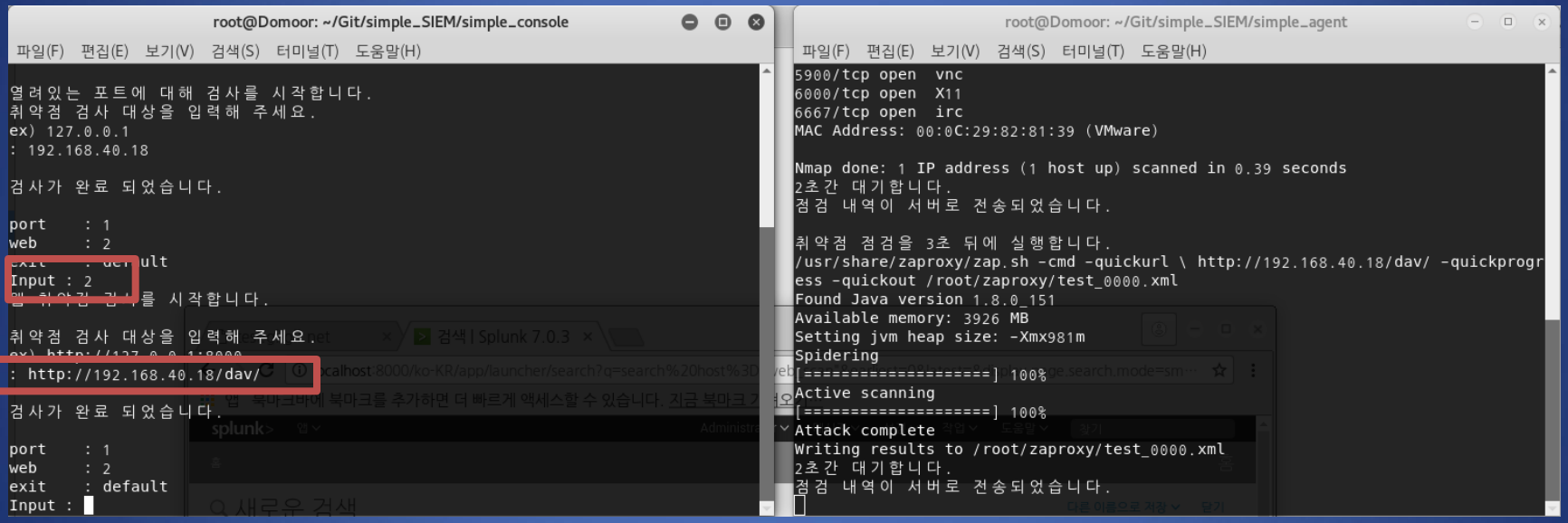


포트 스캔 후 Splunk 로그 확인

View.

Dbreed

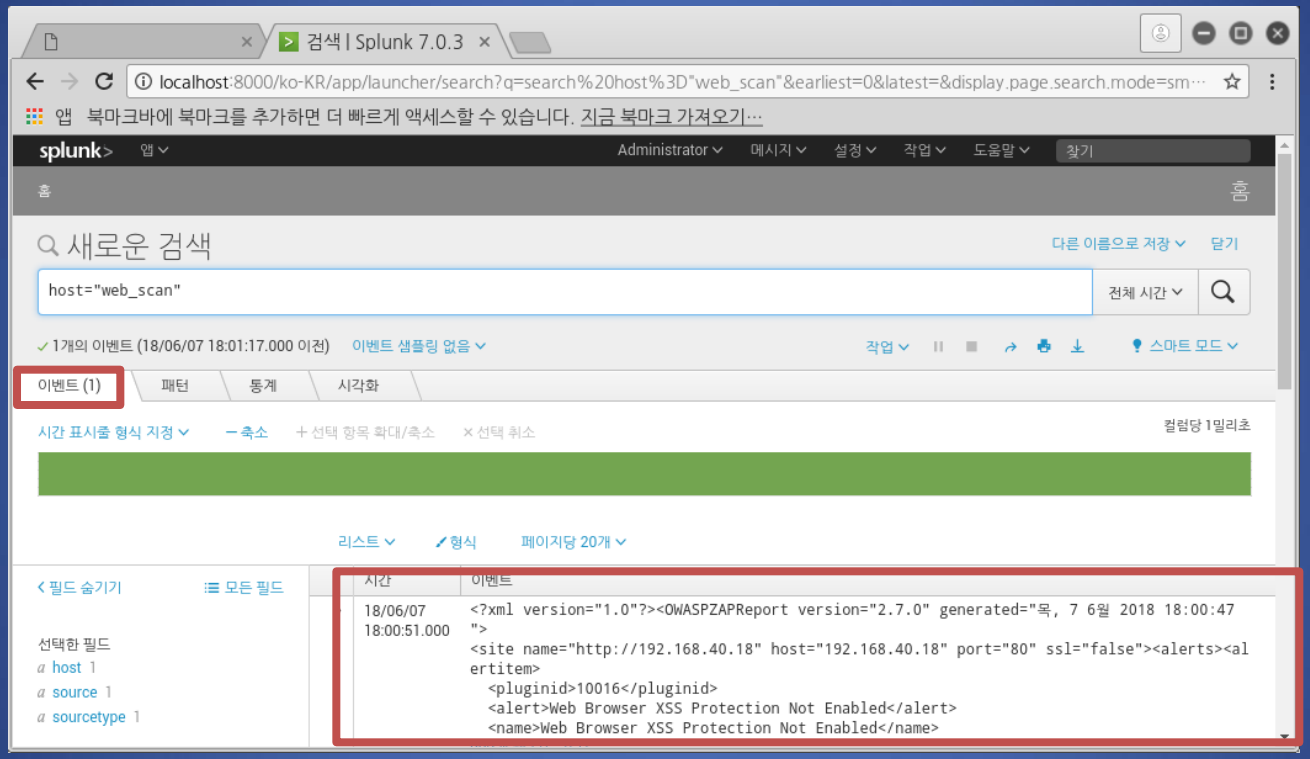
웹 스캔



웹 스캔 선택 및 스캔 대상 입력

View.

Dbreed

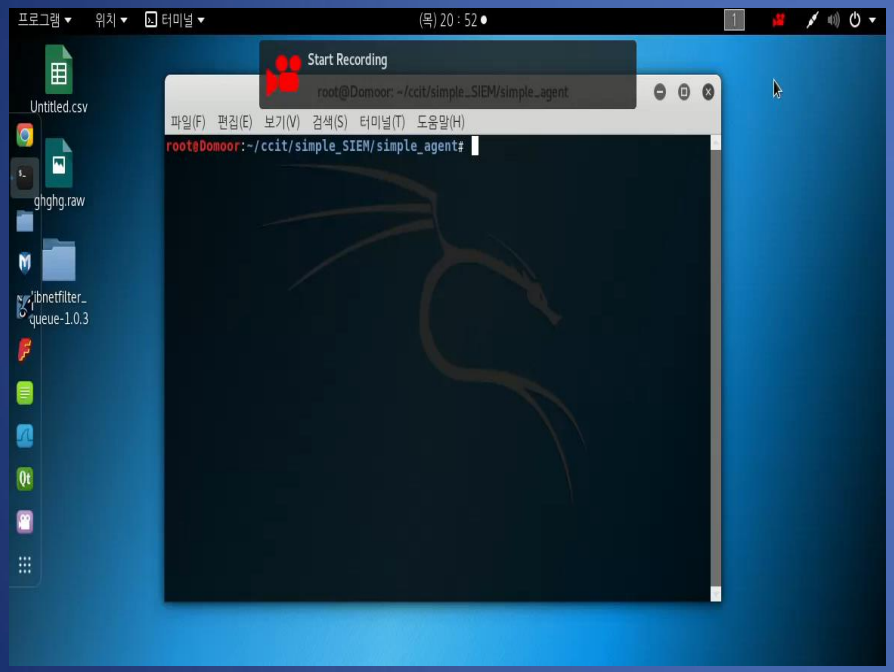


웹 스캔 후 Splunk 로그 확인

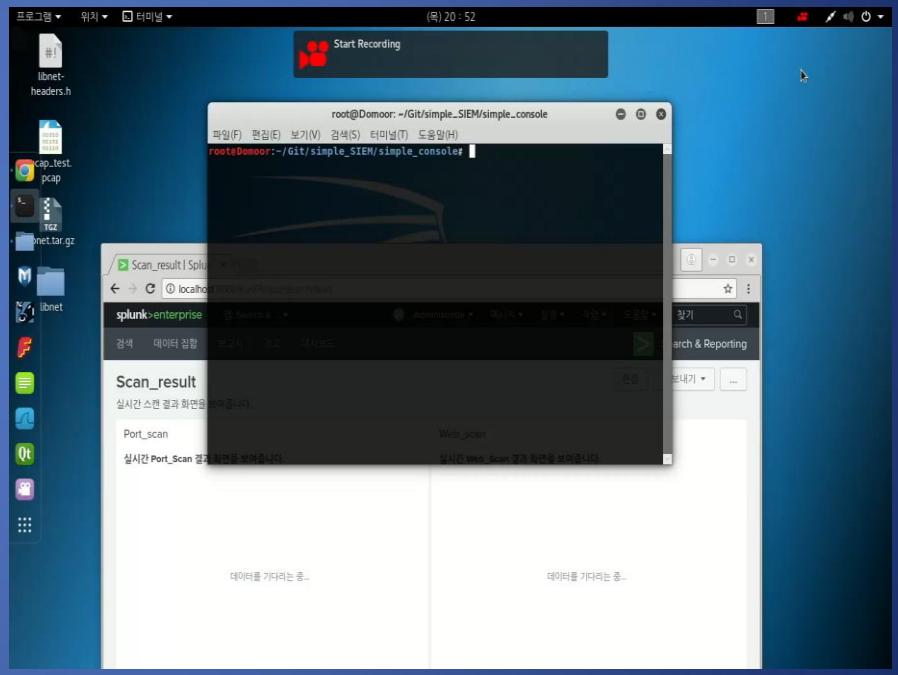
시연 영상.

D'breed

Agent



Console



향후 계획.

향후 계획.

D'breed

1. 네트워크 및 시스템 영역 추가 진행예정

2. UI및 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

Dbreed

END