

BOOTER 개발 프로젝트

관리자매뉴얼 - 개요와 시스템 구성

발주처 : ㈜제넷 시큐리티

시행처 : (주)심포니소프트

완료일자: 2016.12.09

<p>시스템 개요와 구조</p>	<p>프로젝트 : Booter 개발</p>	<p>작성일 : 2017.12.9</p>
<p>기본 구조 기본 기능</p>	<p>연결용도 :</p> <p>진행설명설명</p> <p>(1) 서버의 기본구성 통제서버 : 1대 탐색서버 : 4대 공격서버 : 24대 로그서버 : 1대 대상서버 : 불특정 다수개</p> <p>(2) 탐색 프로세스 그림의 (1)~(4)까지의 진행을 통하여 대상 서버의 탐색과 상태를 파악한다.</p> <p>(3) 공격 프로세스 그림의 (5)~(7)까지의 진행을 통하여 대상 서버에 대한 DDOS 공격을 진행한다. 이때 공격서버에 대한 헬스 체크 정보를 통제 서버에서 확인할 수 있으며 만약 대상 서버를 실험용으로 구성하여 대상서버에 헬스체크 모듈을 설치한 경우 대상서버에 대한 헬스체크도 가능하다.</p> <p>(4) 공격이 진행 중이거나 끝난 경우 (1)~(4)까지를 다시 진행하여 대상 서버의 상태를 파악할 수 있다.</p>	<p>특이사항</p>

C-Server에서 S-Server로 T-Server에 대한 IP, DNS 정보를 전송.

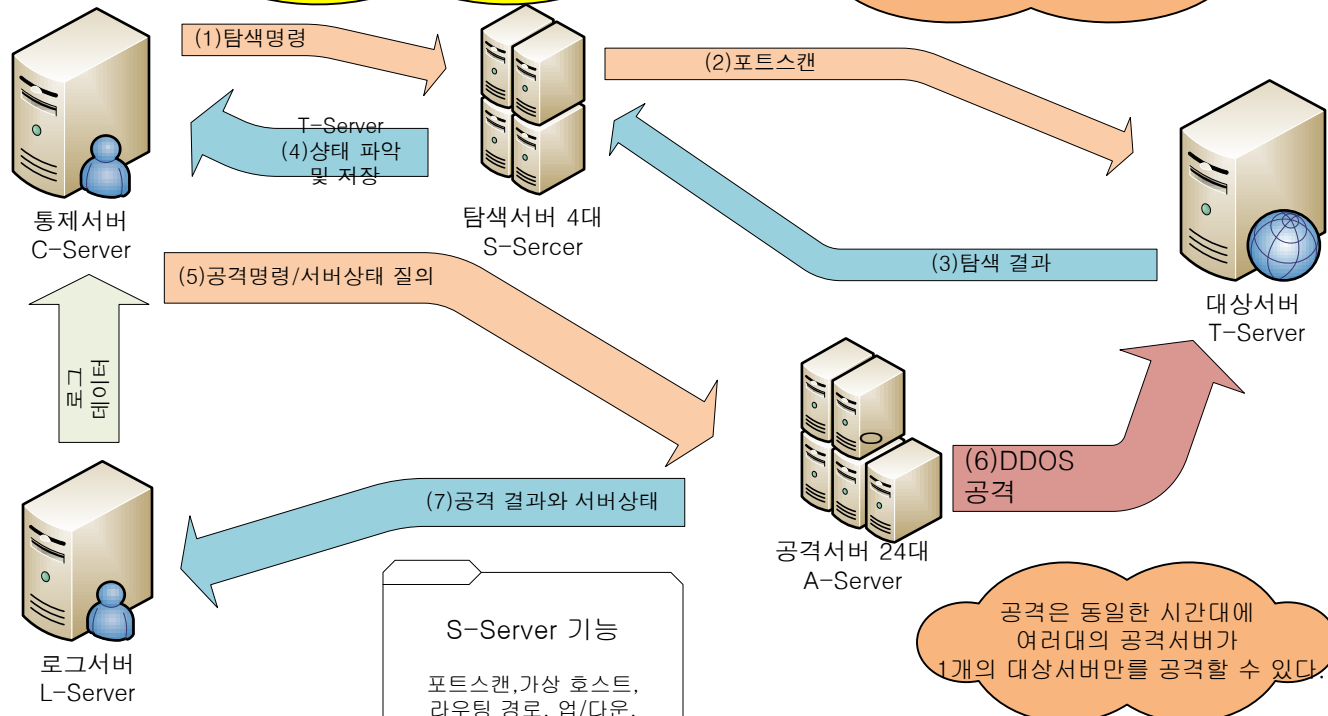
S-Server는 T-Server를 Scan하여 시스템정보를 수집하고 결과값을 C-Server로 전송

C-Server는 탐색정보확인후 A-Server로 공격이벤트를 입력

A-Server는 T-Server에 대한 DDOS 공격을 수행.

수집 명령은 복수의 탐색서버중에서 택일한 후 탐색 명령을 전송하고 반환된 정보를 매번 레포트 형태로 저장하여 데이터의 정확성과 신뢰성 확보

각서버간의 데이터 통신 암호화는 서버 부하를 줄이기위하여 Htps (SSL)프로토콜을 사용한다.



수집데이터와 분석 리포트

- S-Server에서 보내진 Scan 정보는 정형화하여 DB에 저장되고 보고서로 출력된다.
- 수집데이터는 대상에 따라 기간 지정/관리자 옵션으로 레포트/통계 기능을 제공 한다.

S-Server 기능

포트스캔, 가상 호스트, 라우팅 경로, 업/다운, Reverse DNS, IP Lookup, Who is, Nmap vulscan

DDoS 공격

메소드 필요요소 7종

- (1)SYN flood
- (2)UDP flood
- (3)TCP Null flood
- (4)LAND
- (5)DNS Amplification
- (6)NTP Amplification
- (7)HTTP Get flood

공격은 동일한 시간대에 여러대의 공격서버가 1개의 대상서버만을 공격할 수 있다.

진행설명설명

(1) T-Server에서 관련 S-Server를 Associate 시킴

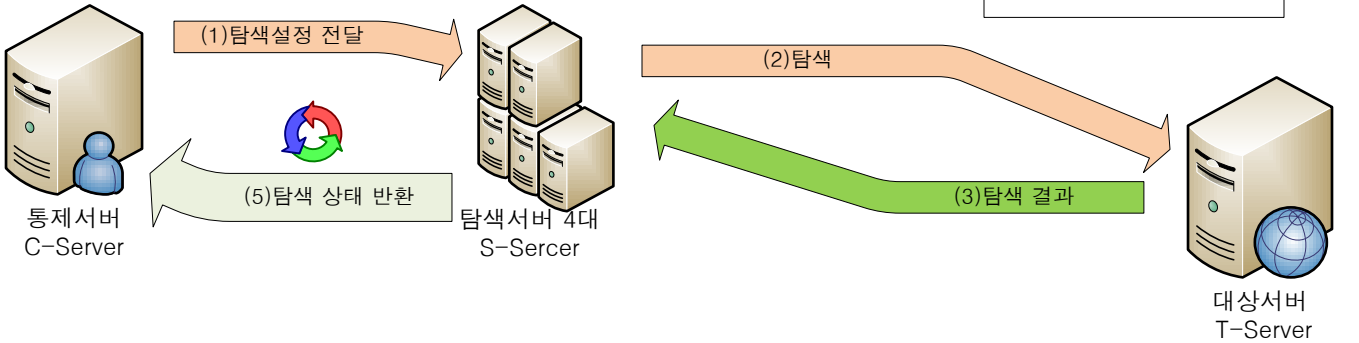
(2) 해당 S-Server에서 Scan Start 로 활성화함.

(3) 이후 해당 S-Server는 연관된 T-Server를 반복적으로 Scan 해서 결과를 Log로 저장

(4) T-Server는 S-Server의 Scan Log를 수시로 디스패치해서 DB에 저장

S-T Server 연관기능
S-Server와 T-Server는 관리자가 탐색보고서를 만들때 탐색 서버를 선정하여 탐색기능을 수행함.

S-Server 기능
(1) Nmap 스캔을 이용하여 대상서버의 포트 스캔
(2) wget을 이용한 대상서버의 서비스 이상 유무를 판단함.



1. C-Server에서 탐색 시작 명령을 내리면 S-Server에서 T-Server에 대한 탐색을 시작함.

2. C-Server는 반응된 REST Log 정보를 DB에 저장

1. Nmap스캔을 이용하여 T-Server의 Port상태를 레포트로 저장

2. Wget을 이용하여 T-Server의 서비스 지속 내용을 레포트로 저장

3. C-Server에서 요청시 Port Scan 로그와 Wget반응 로그를 REST로 반응

대상 서버는 불특정 다수이다.

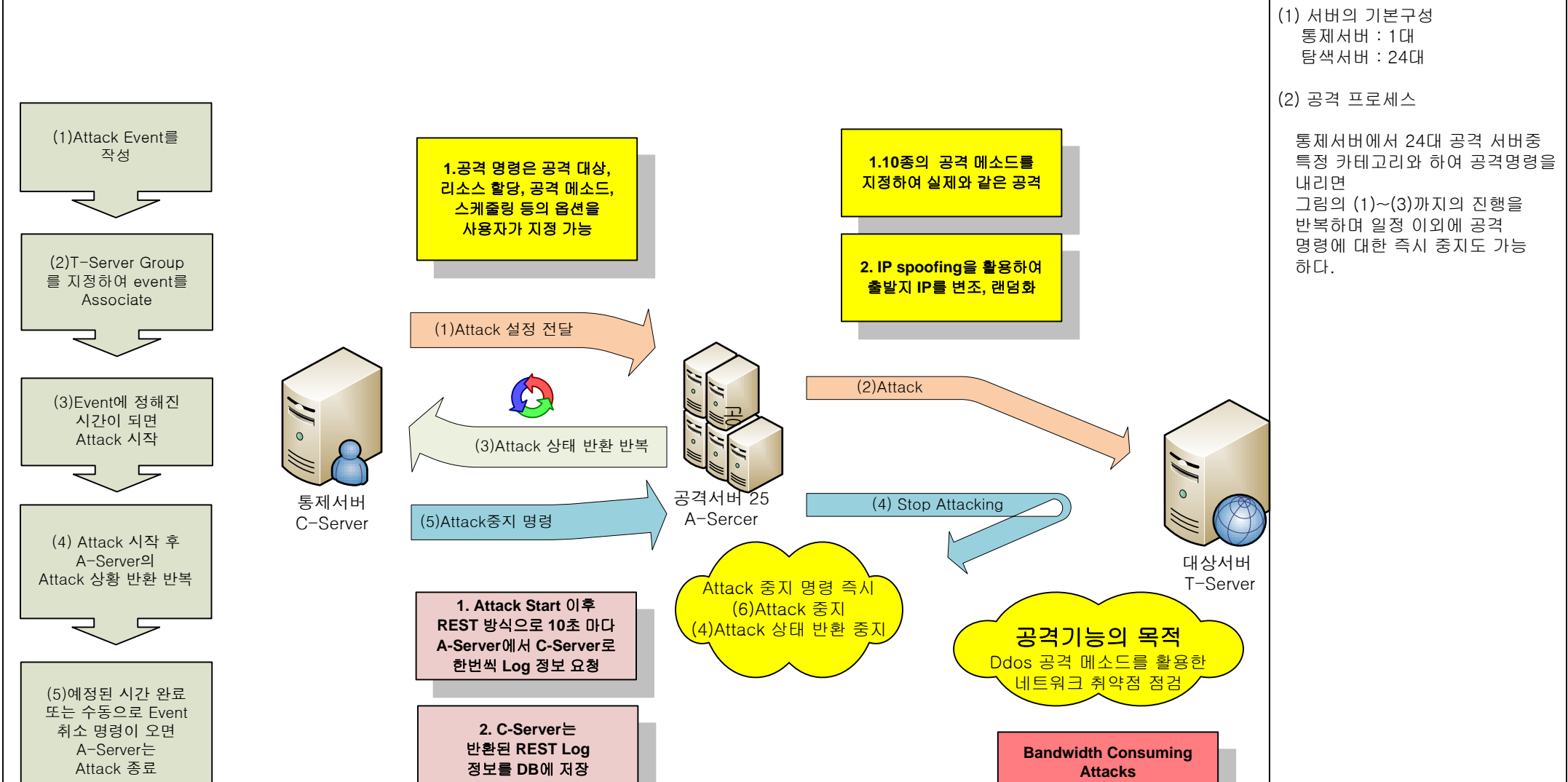
(1) 서버의 기본구성
통제서버 : 1대
탐색서버 : 4대

(2) 탐색 프로세스

통제서버에서 4대의 탐색서버중 1대를 선정하여 탐색명령을 내리면 그림의 (1)~(5)까지의 진행을 통하여 대상 서버의 탐색과 상태를 파악한다.

특이사항

	진행설명설명
--	--------



(1) 서버의 기본구성
 통제서버 : 1대
 탐색서버 : 24대

(2) 공격 프로세스

통제서버에서 24대 공격 서버중 특정 카테고리화 하여 공격명령을 내리면 그림의 (1)~(3)까지의 진행을 반복하며 일정 이외에 공격 명령에 대한 즉시 중지도 가능하다.

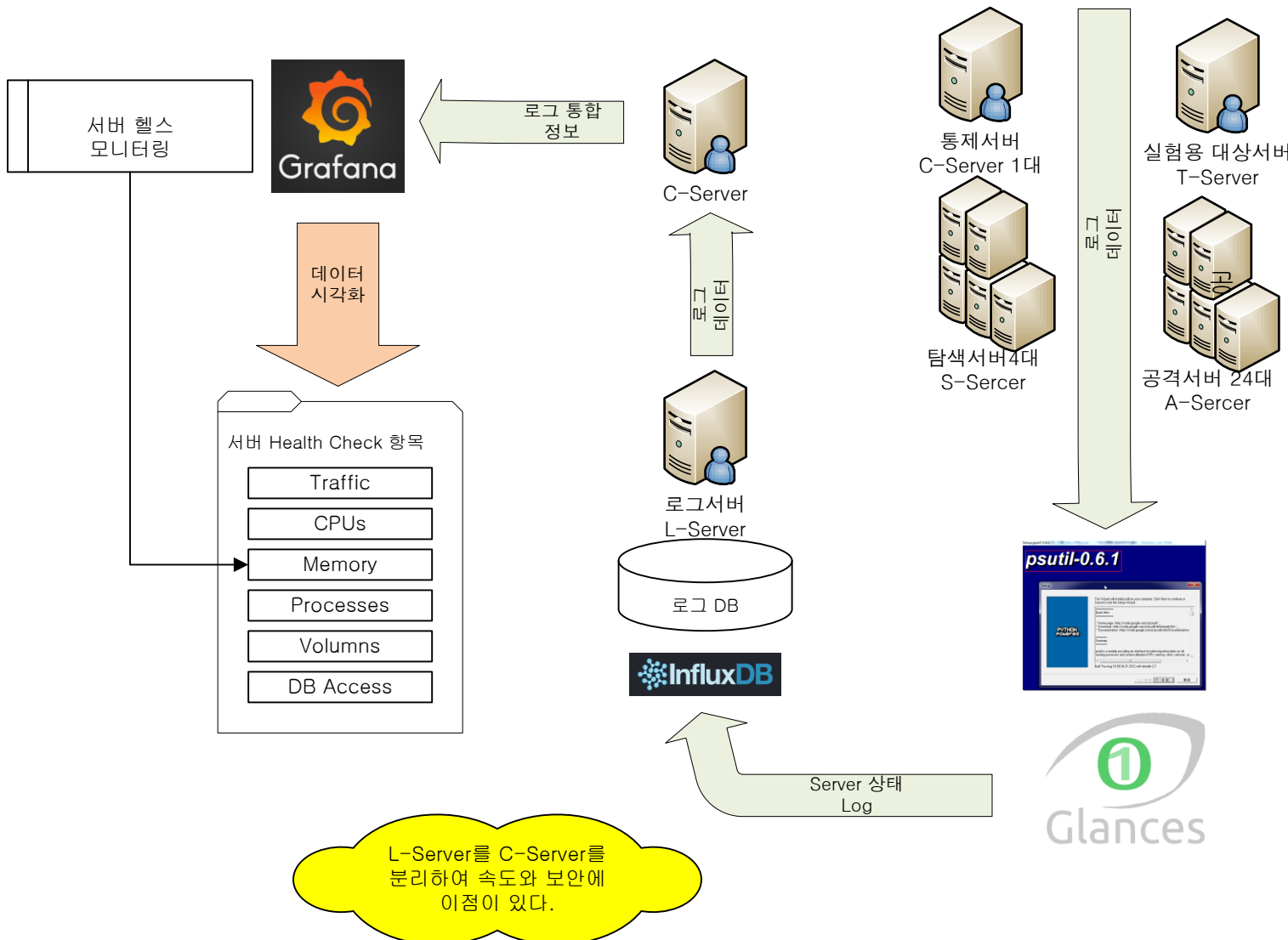
	특이사항
--	------

--	--

진행설명설명

- (1) 서버의 기본구성
- 통제서버 : 1대
 - 탐색서버 : 4대
 - 공격서버 : 24대
 - 로그서버 : 1대
 - 대상서버 : 불특정 다수(실험용)

- (2) 로그 발생 활용 프로세스
- 30개의 서버에서 10초에 1번씩 서버의 헬스 체크 정보를 REST API 로 받음.
 - Django ORM과 REST API에서 발생할 부하 예상으로 인하여 Log 정보 데이터를 Grances에서 로그서버로 기록하고 인터페이스를 통하여 로그정보를 직접 쿼리하는 것으로 변경함.
 - 해당 내용 적용시 통제서버의 부하가 대폭 감소하며 30개이상의 서버가 로그정보를 보내오는 경우라도 문제없이 처리가 가능함.



특이사항