BOOTER 개발 프로젝트

관리자매뉴얼 – 개요와 시스템 구성

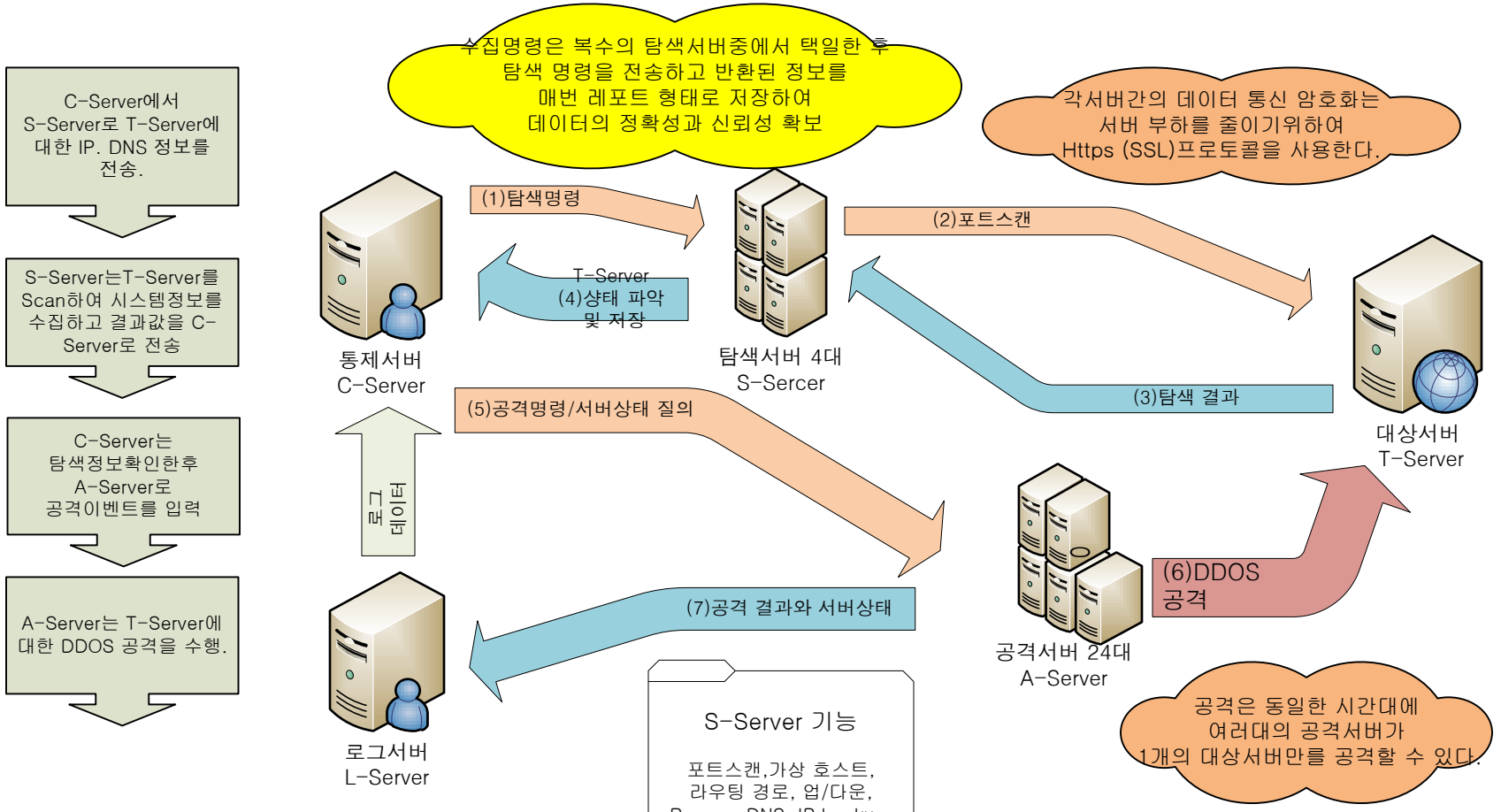
발주처 : ㈜제넷 시큐리티

시행처 : (주)심포니소프트

완료일자: 2016.12.09

Document History			
버젼	일자	작성내용	작성자
1.0	2016.9.20	초기작업 내용	김호익
1.1	2016.10.28	추가 작업 내용	김호익
1.3	2016.12.09	마무리 작업 내용 추가	김호익

시스템 개요와 구조	프로젝트 : Booter 개발		작성일 : 2017.12.9
기본 구조 기본 기능			연결용도 :



진행설명설명

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

(2) 탐색 프로세스

그림의 (1)~(4)까지의 진행을 통하여 대상 서버의 탐색과 상태을 파악한다.

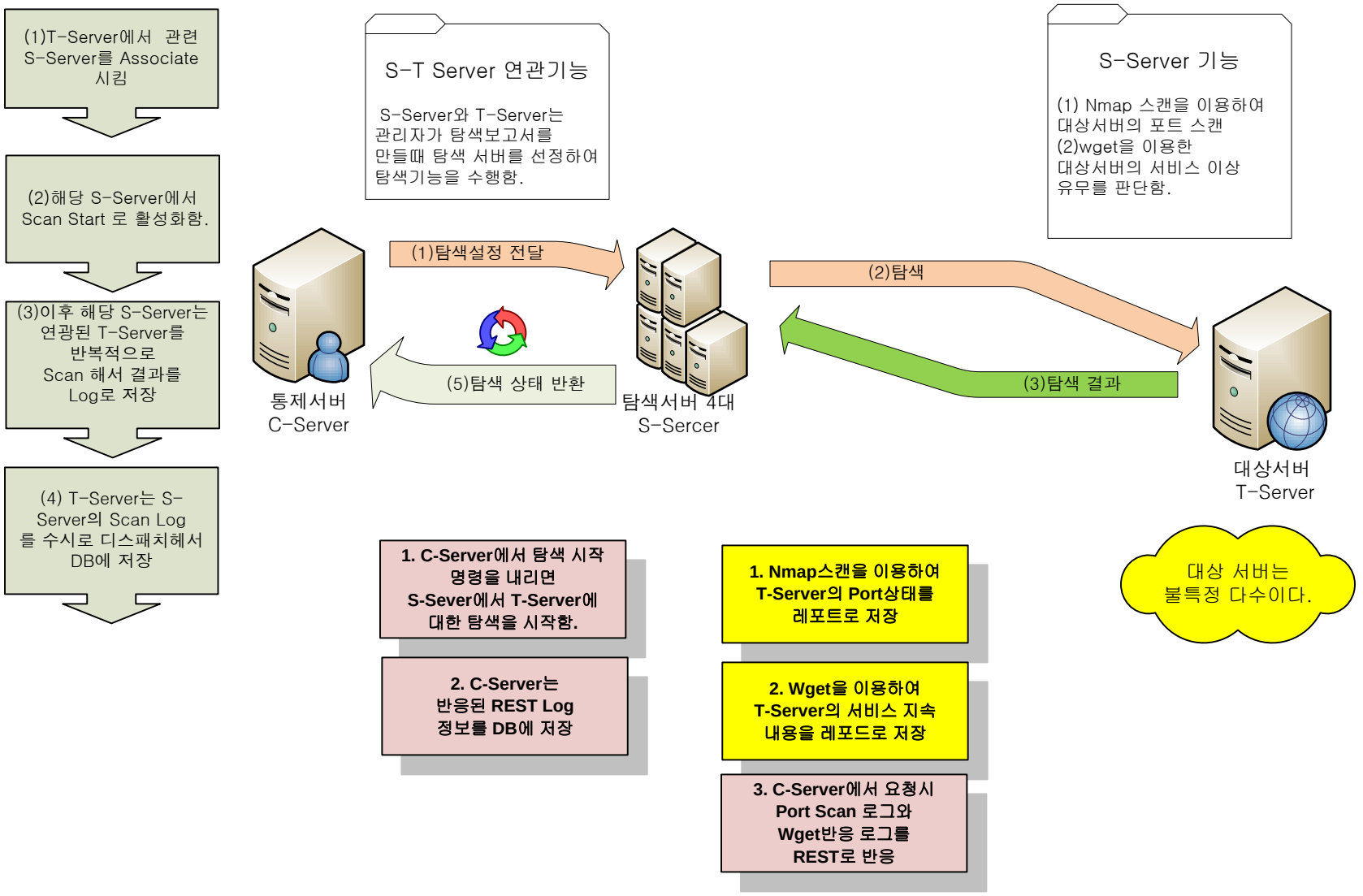
(3) 공격 프로세스

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.

(4) 공격이 진행 중이거나 끝난 경우 (1)~(4)까지를 다시 진행하여 대상 서버의 상태를 파악할 수 있다.

특이사항

시스템 개요와 구조	프로젝트 : Booter 개발		작성일 : 2017.12.9
통제-탐색-대상서버 상세구조와 기능			연결용도 :



진행설명설명

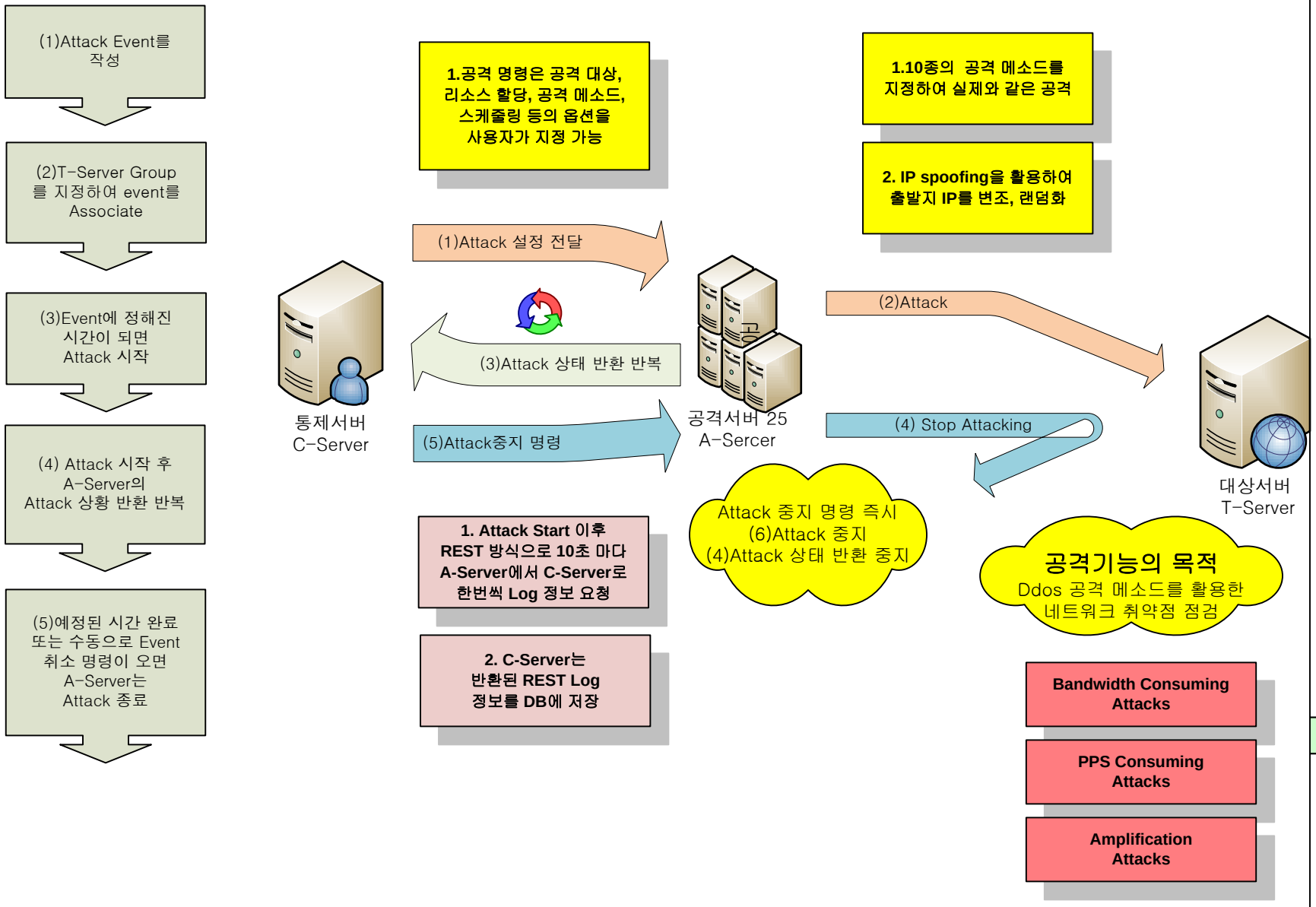
(1) 서버의 기본구성
통제서버 : 1대
탐색서버 : 4대

(2) 탐색 프로세스

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

특이사항

시스템 개요와 구조	프로젝트 : Booter 개발		작성일 : 2017.12.9
통제-공격-대상서버 상세구조와 기능			연결용도 :



진행설명설명

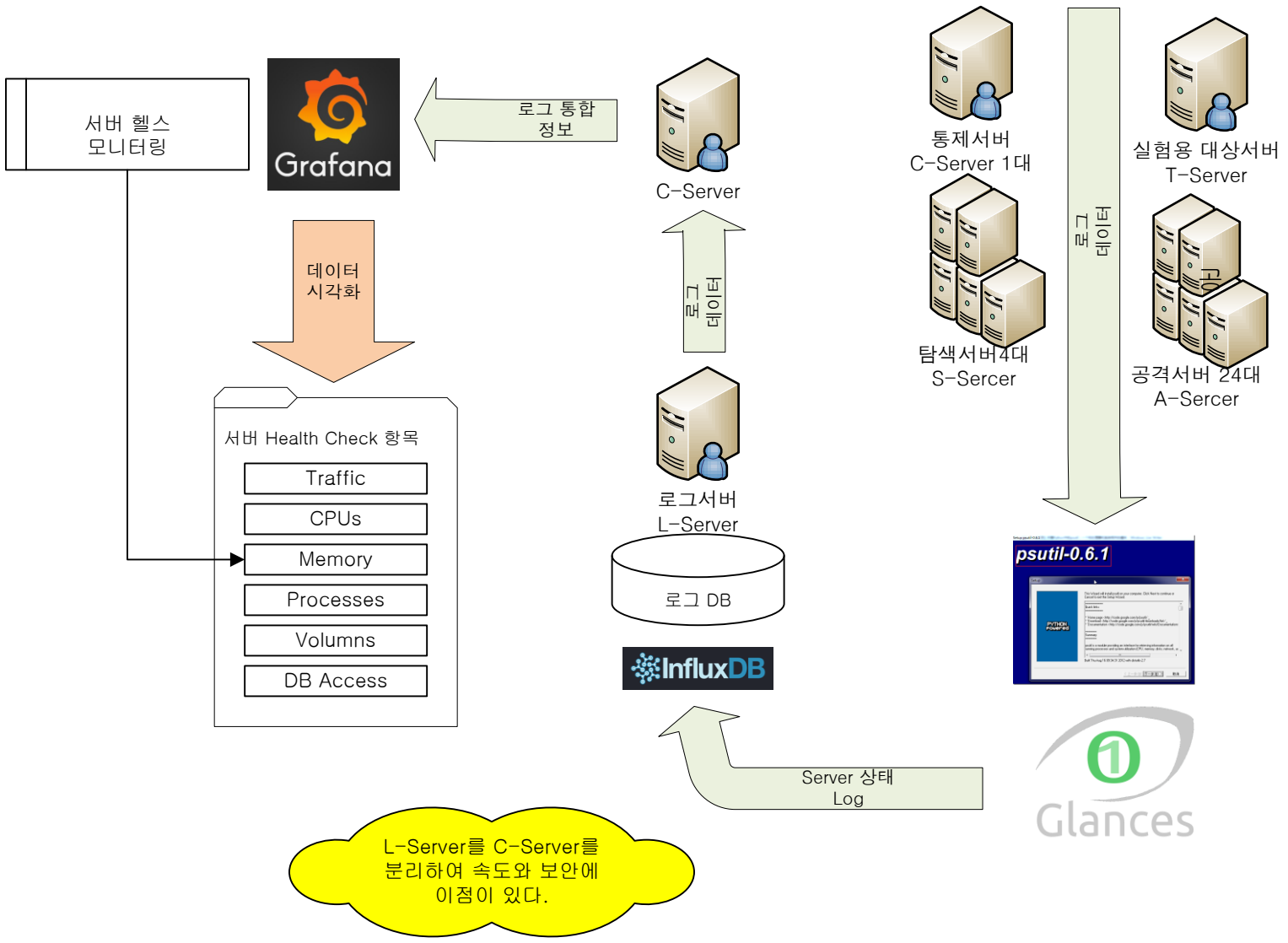
(1) 서버의 기본구성
통제서버 : 1대
탐색서버 : 24대

(2) 공격 프로세스

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

특이사항

시스템 개요와 구조	프로젝트 : Booter 개발		작성일 : 2017.12.9
통제-로그서버 상세구조와 기능			연결용도 :



진행설명설명

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

(2) 로그 발생 활용 프로세스

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

특이사항