

# BOOTER 개발 프로젝트

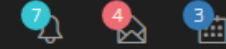
## 사용자 인터페이스

발주처 : ㈜제넷 시큐리티

시행처 : (주)심포니소프트

완료일자: 2016.12.20





진행설명설명

- 1. Booter 서버 상황과 탐색 공격 진행 사항을 전체를 보여준다.
- 2. 탐색보고서를 미리보기하면 탐색했던 상화의 상세 내용을 보여준다.

서버수 합계

사용자수 합계

탐색 보고서 개수

이벤트 개수

(1)상세 보고서보기

새 서버

등록시간	서버아이디	카테고리	서버명	IP
년월일시	s01	탐색	탐색-1	125.209.222.141
년월일시	a02	공격	공격-2	125.209.222.142

새 보고서

등록시간	보고서아이디	대상서버	보기	IP
년월일시	1234	s01	<a href="#">미리보기</a>	125.209.222.141
년월일시	1235	a01	<a href="#">미리보기</a>	125.209.222.142

통제서버 네트워크 상황

통제서버 CPU 상황

통제서버 Memory 상황

통제서버 Process 상황

통제서버 Volumn 상황

통제서버 DB 상황

특이사항

UI는 AWS 관리자 화면의 기준으로 벤치마킹하여 제작함.



진행설명설명

1. 작성된 탐색보고서를 확인하고 필요시 다운로드 한다.

보고서 추가

실행 ▼

검색창

검색하기

<input type="checkbox"/>	이벤트아이디	대상서버-id	탐색서버-id	보기	상태	시작 시간	종료 시간	다운로드
<input type="checkbox"/>	es-161023-01	s-161003-01	s-161003-01	미리보기	대기중	년월일시	년월일시	다운로드
<input type="checkbox"/>	ea-161023-01	홍길동	홍길동	미리보기	공격중	년월일시	년월일시	다운로드

(1)선택하고

(2)우측마우스로  
클릭하면

레코드 수정  
-----  
레코드 삭제

(3)클릭하면

보고서  
미리보기

(4)클릭하면

보고서  
다운로드

특이사항

UI는 AWS 관리자 화면의 기준으로 벤치마킹하여 제작함.



탐색보고서아이디\*

대상 서버\*

탐색 서버\*

**탐색 시작**

최종 상태\*

시작 시간\*

종료 시간\*

(1)아이디  
입력,  
대상서버  
지정,  
탐색서버  
지정 후

(2) 탐색시작 버튼 클릭하면  
-----  
탐색서버가 대상서버를 탐색하여  
정보를 가져와서 보고서를 만듦

목록으로    휴지통    **업데이트**

서버 지정\*

버지니아-1

캘리포니아-2

캘리포니아-2

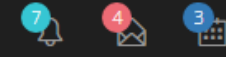
**탐색 보고서 내용**    **보고서 미리보기**

(3)보고서 내용을  
읽어옴

(4)클릭하면  
보고서  
미리보기

(1) 탐색보고서 아이디는 임의로 지정한다.  
(2) 탐색시  
1. NMAP scan 통하여 대상서버가 running 되고 있는지 여부를 확인한다.

미는 뒷장에 첨부된 서버등록 참조 이미지를 참조한다..



진행설명설명

이벤트 추가

실행

검색창

검색하기

필터링 OFF

필터링 ON

필터링할 카테고리를 선택해 주세요.

검색창

검색하기

<input type="checkbox"/>	이벤트아이디	이벤트명	이벤트카테고리	공격종류	pps	실행서버	대상서버-id	서버상태	이벤트상태	시작종료
<input type="checkbox"/>	es-161023-01	dasfdsaf	탐색	ICMP	10000	Hd-a01외 23	s-1613-01	On	대기중	~
<input type="checkbox"/>	ea-161023-01	sdfaaf	공격	TCP_SYN	500000	Hd-a01외 23	홍길동	Off	대기중	~

(1)선택하고

(2)우측마우스로 클릭하면

탐색중지

공격중지

탐색 재시작

공격 재시작

레코드 수정

레코드 삭제

Network 비교

CPU 비교

Memory 비교

Process 비교

Volumn 비교

DB Access 비교

대상 서버 상태

\*\*\*\*  
(1) 선택이전에 서버의 카테고리를 필터할 수 있다.

\*\*\*\*  
(1) 선택이전에 검색으로 표시 서버를 필터할 수 있다.

1. 모니터링 시작과 중지 명령은 해당화면에서 수행된다.

2. 탐색/공격과 같은

3. 실행 내용

탐색중지: 탐색진행중 내용 중지

공격중지: 공격진행중 내용 중지

탐색재시작: 중지 내용 재개

공격재시작: 중지내용 재개

레코드 수정: 해당 레코드 수정

레코드 삭제: 해당 레코드 삭제

(공격에 가담한 각 서버에 대한)

Network 비교:

CPU 비교:

Memory 비교:

Process 비교:

Volumn 비교:

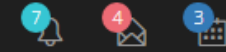
DB Access 비교:

(공격대상 서버의 각 항목별)

대상 서버 상태:

특이사항

UI는 AWS 관리자 화면의 기준으로 벤치마킹하여 제작함.



진행설명설명

(1) 이벤트는 공격만 들어갈 수 있도록 변경한다.

\*\* 탐색은 탐색 보고서에서 진행하는 것으로 변경한다.

목록으로 휴지통 업데이트

서버 지정\*

<input type="checkbox"/>	버지니아-1	▼
<input type="checkbox"/>	캘리포니아-2	
<input type="checkbox"/>	캘리포니아-2	

(7) 공격 서버 지정  
해당 공격에  
가담할 서버를  
지정

이벤트 아이디\*

이벤트 명\*

이벤트 설명\*

(1)아이디  
입력,  
이벤트명,  
이벤트 설명  
지정 후

현재 UTC 시간

(2) UTC 시간을 확인한 후  
-----  
공격 시작 시간과 종료 시간을  
UTC 시간에 맞추어 지정한다.

시작 시간

종료 시간

Source IP 설정

(3) Source IP 설정  
Real IP / Static IP / Randon IP /  
Random Last IP  
로 지정 가능함.

대상 서버\*

(4) 대상 서버 지정  
해당 서버는 "새 서버"로 이미  
등록되어 있어야 함.

이벤트 카테고리\*

(5) 이벤트 카테고리  
공격으로 지정되어 있어야 함.

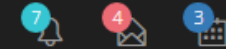
공격 방법\*

공격 주기(pps)\*

- (7) 공격 주기
- 1
  - 100
  - 10,000
  - 500,000
  - 1,000,000
  - 1,500,000
  - MAX
- (6) 공격 방법
- UDP
  - ICPM
  - ICMP-E/R
  - ARP-REQ
  - TCP/SYN
  - TCP/ACK
  - TCP/RST
  - TCP\_FIN
  - TCP\_RDM
  - AMP/DNS
  - AMP/DNS-A
  - AMP/NTP
  - HTTP FLOODING

특이사항

UI는 뒷장에 첨부된 서버등록  
참조 이미지를 참조한다..



진행설명설명

카테고리명\*

부모\*

우선순위\*

필수\*

설명\*

등록

취소

(2) 수정  
-----  
삭제

(1) 이벤트  
카테고리  
내용입력  
-----

검색창

검색하기

<input type="checkbox"/>	카테고리명	설명	카운트	우선순위	필수
<input type="checkbox"/>	공격서버	공격한다.	25	25	<input type="checkbox"/>

(3)우측마우스로  
클릭하면  
수정  
-----  
삭제

(1) 카테고리 추가는 간단하며므로 리스트 화면과 수정화면을 동시에 구성한다.

(2)원편의 입력란에 입력하고 작성버튼을 클릭하면 수정한 내용을 기록함 후 오른쪽의 리스트 화면에서 리프레쉬하여 보여준다.

(3)이벤트 카테고리는 공격만 있으면 되므로 더 이상 내용에 대한 추가를 하지 않도록 한다.

(4) 이벤트 카테고리는 부모를 입력할 필요가 없다. 필수는 지정하고 설명도 입력하지 않는다.

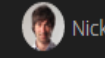
특이사항

UI는 AWS 관리자 화면의 기준으로 벤치마킹하여 제작함.





TRONIC



진행설명설명

1. 서버 현황과 헬스 상태를 점검한다.

서버 추가

실행

비교

필터링 OFF

필터링 ON

필터링할 카테고리를 선택해 주세요.

검색창

검색하기

<input type="checkbox"/>	서버아이디	서버명	카테고리	Public IP	Network	액션 상태	헬스 상태	가동 상태
<input type="checkbox"/>	s161023-01	버지니아-1	A/B/C	121.33.343.39	eth1	대기중	대기중	On
<input type="checkbox"/>	a161023-01	캘리포니아-2	탐색	121.33.343.39	eth2	대기중	대기중	On

(1)선택하고

(2)우측마우스로 클릭하면

- 
- 헬스 상태
- 
- 헬스 상태 중지
- 
- 레코드 수정
- 
- 레코드 삭제
- 
- 서버 모니터링
- 
- 서버 중지
- 
- 서버 재시동
- 
- 일괄 업데이트
- 
- 서버 데이터 삭제

(3)우측마우스로 클릭하면

- 
- Network
- 
- CPUs
- 
- Memory
- 
- Process
- 
- Volumn
- 
- DB Access

\*\*\*\*  
(1) 선택이전에 서버의 카테고리를 필터할 수 있다.

\*\*\*\*  
(1) 선택이전에 검색으로 표시 서버를 필터할 수 있다.

특이사항

UI는 AWS 관리자 화면의 기준으로 벤치마킹하여 제작함.



서버 아이디\*

서버명\*

서버 IP\*

Network \*

(1) 서버 정보 입력

- (2) Network 지정
- - Eth0
  - 
  - Eth2
  - 
  - Eth3
  - 
  - Eth4
  -

등록

취소

(3) 등록

-----

취소

목록으로   휴지통   업데이트

<input type="checkbox"/>	카테고리명	설명	필수
<input type="checkbox"/>	공격서버	공격한다.	<input type="checkbox"/>
<input type="checkbox"/>	탐색서버	탐색한다	<input type="checkbox"/>
<input type="checkbox"/>	공격서버	공격한다.	<input type="checkbox"/>
<input type="checkbox"/>	--공격서버-A 그룹	공격한다.	<input type="checkbox"/>

(4)우측마우스로 클릭하면

수정

-----

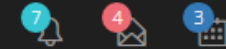
삭제

(1) 서버 카테고리는 다중 선택이 가능하도록 구성한다.

(2) 서버 카테고리는 다중으로 지정이 가능해야 하며 서버는 그룹핑을 통하여 특정 공격 세션 그룹으로 동시에 실행되게 된다.

특이사항

UI는 뒷장에 첨부된 서버등록 참조 이미지를 참조한다..



진행설명설명

카테고리명\*

부모\*

우선순위\*

필수\*

설명\*

등록

취소

실행 ▼

(2) 수정  
-----  
삭제

<input type="checkbox"/>	카테고리명	설명	카운트	우선순위	필수
<input type="checkbox"/>	탐색서버	탐색한다	4	4	<input type="checkbox"/>
<input type="checkbox"/>	공격서버	공격한다.	25	25	<input type="checkbox"/>
<input type="checkbox"/>	-- 공격서버-A 그룹	공격한다.	25	25	<input type="checkbox"/>

(3)우측마우스로  
클릭하면  
수정  
-----  
삭제

(1) 카테고리  
정보  
입력  
-----

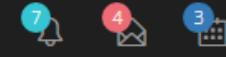
(1) 카테고리 추가는 간단하며므로 리스트 화면과 수정화면을 동시에 구성한다.

(2)원편의 입력란에 입력하고 작성버튼을 클릭하면 수정한 내용을 기록함 후 오른쪽의 리스트 화면에서 리프래쉬하여 보여준다.

(3)탐색서버와 공격서버 카테고리는 반드시 있어야하며 지워서는 안된다. 이경우 반드시 카테고리명을"탐색서버", "공격서버"로 철자가 틀리지 않게 입력하여야 한다. 필수란에는 Checked가 되어 있어야 한다..

특이사항

UI는 AWS 관리자 화면의 기준으로 벤치마킹하여 제작함.



진행설명설명

그래파나 주기(초)

10

업데이트

서버 헬스 체크  
정보를 가져오는  
주기

(1)서버의 헬스 체크 정보를 가져오는 주기가 짧을수록 서버의 실시간 정보를 확인할 수 있는 반면 그만큼 로그서버에 부하를주게 되므로 심할 경우 로그 서버가 다운된 것처럼 보이는 경우가 있으므로 적절한 주기를 설정하여야 한다.

(2) 현재 10초 주기를 주었을 경우 로그서버에 무리를 주지 않으면서도 원하는 정보를 실시간에 가깝게 볼 수 있었다.

특이사항

UI는 AWS 관리자 화면의 기준으로 벤치마킹하여 제작함.



진행설명설명

(1)전체 서버의 일괄적인 변경이 발생할 경우 해당 페이지에서 작업을 수행한다.

검색할 유저

업데이트

정보 검색에 연관될 유저 선택

서버 업데이트

전체 서버 업데이트

전체 서버 업데이트

서버의 이동이나 IP 변경이 일어날때

로그 서버 선택

로그 서버 업데이트

로그 서버의 IP를 변경하였을 때

Bash 명령어 실행

Bash 명령어 실행

전체 서버에 일괄적인 명령어를 수행할때 예) 전체서버의 전체 시스템 삭제

특이사항

UI는 AWS 관리자 화면의 기준으로 벤치마킹하여 제작함.



진행설명설명

- (1) 이메일은 한자리 입력 시 유효성 체크를 한다.
- (2) 비밀번호는 8자리 이상과 1자리 이상의 특수문자로 구성한다.
- (3) 작성을 클릭하면 입력한 내용으로 사용자가 만들어지거나 수정된다.

개인정보 작성

이름

Email

비밀번호 입력 (8자리 이상, 특수문자 혼합 필수)

비밀번호

비밀번호 확인

메일 인증번호 전송

새로운 사용자를 추가할 경우

특이사항

UI는 AWS 관리자 화면의 기준으로 벤치마킹하여 제작함.