Portfolio

정보보안 담당자 지원자
오석빈 포트폴리오

osb330@naver.com
https://github.com/hasihime/resume

오석빈

(Oh, SeokBin)

거주지 : 경기도 일산
이메일: osb330@naver.com
연락처: 010-9955-7170

학력

가천대학교 2013.03 – 2019. 02
컴퓨터공학전공(3.52/4.5)

자격증

CCNA : 2017.02.23
정보처리기사 : 2018.08.17

직무 관련 능력

Java : 중상
Linux : 중
Python : 중

교육 이력

삼성 청년 SW 아카데미 (2019.07~)

장점 / 강점

탐구정신

보안 전문성을 기르기 위해 개발부터 운영,
모니터링 공부 및 신기술을 익히기 위해
다양한 컨퍼런스 참석 및 프로젝트 진행

분석 및 정리

한번 배운 것은 잊지 않기 위해 작업의 문서화
및 Git 등 정리 습관화

직무 경험

네오위즈 : 보안팀 (2018.06 ~ 2018.12)

IDS(suricate), IPS(Tipping Point) 운용
모바일 게임 취약점 분석
ISMS 심사 준비 (클라우드,AWS 항목)

소만사 : RA팀(2019.02 ~ 2019.05)

보안 어플라이언스 생산
– 서버장비 및 솔루션 숙지

프로젝트 경험

Vue를 이용한 반응형 웹 프로젝트

기간 : 2020.01 ~ 2020.02(6주)
성과 : 반 우수 프로젝트 당선(2등)
팀 기여도 : 25%
나의 역할

AWS 서버 구축. Firebase와 AWS 연동.
AWS 서버에 올라간 Spring Controller https로 통신하게 함(사설키 인증)
Mixed content 에러 해결을 위한 cors 설정
Spring Boot를 이용한 Rest Controller 작성
Vue를 이용하여 반응형 웹 제작

IT 컨퍼런스 참석 경험

2019.11.14 Samsung SDS Techtonic – 빅데이터 및 AI
2019.05.21 Unite Souel 2019 – 유니티
2019.08.30 ISEC 2018 – 정보보안

목차

Table of Contents

Suricata 운용

프로젝트 기간

2018.06 – 2018.12

프로젝트 현황

완료

개요

IDS인 Suricata의 기능과 특징에 대해 설명을 한다. 그리고 설치와 사용법을 숙지할 수 있고, Suricata의 설정파일을 살펴봄으로써, 자신에게 필요한 항목을 설정할 수 있다.

담당 역할

Suricata를 중심으로 보안장비 운용 및 사용법 숙지

사용 Tool

IDS : Suricata

IPS : TrendMicro 사 TippingPoint

그 외 : SEIM OSSIM

내용

- Suricata를 이용한 IDS 패킷 분석.
- 매뉴얼 정리 및 일일 IDS 탐지 목록 정리

참고 링크

https://github.com/hasihime/resume/tree/master/project/00.SimpleProject/03_suricata

Suricata 운용

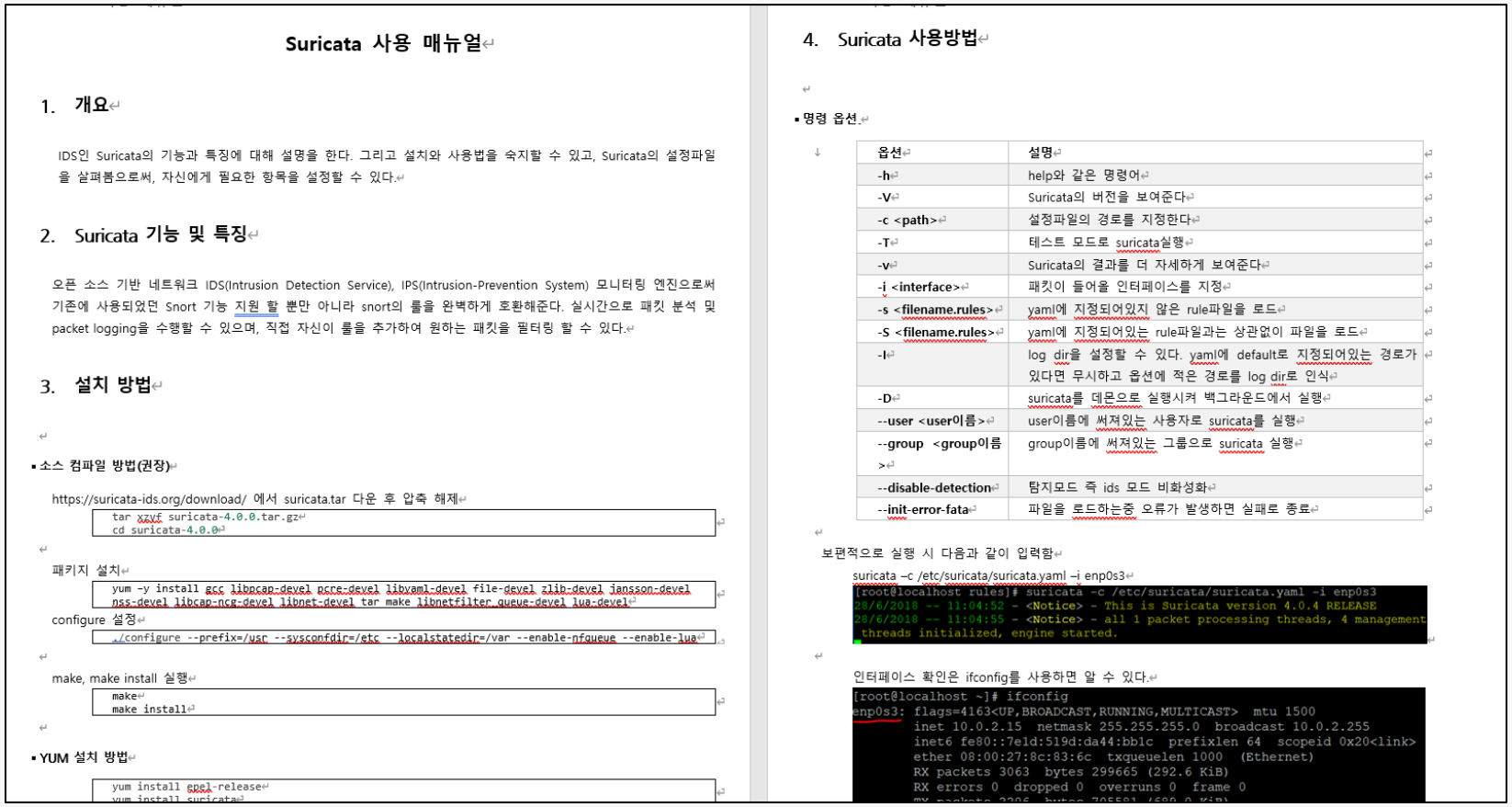
프로젝트 기간

2018.06 – 2018.12

프로젝트 현황

완료

프로젝트 이미지



Suricata 사용 매뉴얼

1. 개요

IDS인 Suricata의 기능과 특징에 대해 설명을 한다. 그리고 설치와 사용법을 숙지할 수 있고, Suricata의 설정파일을 살펴봄으로써, 자신에게 필요한 항목을 설정할 수 있다.

2. Suricata 기능 및 특징

오픈 소스 기반 네트워크 IDS(Intrusion Detection Service), IPS(Intrusion-Prevention System) 모니터링 엔진으로써 기존에 사용되었던 Snort 기능 지원 할 뿐만 아니라 snort의 룰을 완벽하게 호환해준다. 실시간으로 패킷 분석 및 packet logging을 수행할 수 있으며, 직접 자신이 룰을 추가하여 원하는 패킷을 필터링 할 수 있다.

3. 설치 방법

▪ 소스 컴파일 방법(권장)

https://suricata-ids.org/download/ 에서 suricata.tar 다운 후 압축 해제

```
tar xzvf suricata-4.0.0.tar.gz
cd suricata-4.0.0
```

패키지 설치

```
yum -y install gcc libpcap-devel pcre-devel libyaml-devel file-devel zlib-devel jansson-devel
nss-devel libcap-ng-devel libnet-devel tar make libnetfilter_queue-devel lua-devel
```

configure 설정

```
./configure --prefix=/usr --sysconfdir=/etc --localstatedir=/var --enable-nfqueue --enable-lua
```

make, make install 실행

```
make
make install
```

▪ YUM 설치 방법

```
yum install epel-release
yum install suricata
```

4. Suricata 사용방법

▪ 명령 옵션.

옵션	설명
-h	help와 같은 명령어
-V	Suricata의 버전을 보여준다
-c <path>	설정파일의 경로를 지정한다
-T	테스트 모드로 suricata실행
-v	Suricata의 결과를 더 자세하게 보여준다
-i <interface>	패킷이 들어올 인터페이스를 지정
-s <filename.rules>	yaml에 지정되어있지 않은 rule파일을 로드
-S <filename.rules>	yaml에 지정되어있는 rule파일과는 상관없이 파일을 로드
-l	log dir을 설정할 수 있다. yaml에 default로 지정되어있는 경로가 있다면 무시하고 옵션에 적은 경로를 log dir로 인식
-D	suricata를 데몬으로 실행시켜 백그라운드에서 실행
--user <user이름>	user이름에 써져있는 사용자로 suricata를 실행
--group <group이름>	group이름에 써져있는 그룹으로 suricata 실행
--disable-detection	탐지모드 즉 ids 모드 비화성화
--init-error-fata	파일을 로드하는중 오류가 발생하면 실패로 종료

보편적으로 실행 시 다음과 같이 입력함

suricata –c /etc/suricata/suricata.yaml –i enp0s3

```
[root@localhost rules]# suricata -c /etc/suricata/suricata.yaml -i enp0s3
28/6/2018 -- 11:04:52 - <Notice> - This is Suricata version 4.0.4 RELEASE
28/6/2018 -- 11:04:55 - <Notice> - all 1 packet processing threads, 4 management
threads initialized, engine started.
```

인터페이스 확인은 ifconfig를 사용하면 알 수 있다.

```
[root@localhost ~]# ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::7e1d:519d:da44:bb1c  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:8c:83:6c  txqueuelen 1000  (Ethernet)
        RX packets 3063  bytes 299665 (292.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
```

Suricata에 대한 설명 및 기능, 사용법 매뉴얼 작성 이미지

모바일 게임 취약점 분석

프로젝트 기간

2018.07 (2주)

프로젝트 현황

완료

개요

모바일 App 취약점 점검의 목적은 모바일 App 취약점 점검을 실시하여 외부로부터의 공격에 대한 위험 요소를 파악하고 이에 대한 개선 방안을 제시함으로써 정보 시스템들의 보안성과 안전성을 확보하는데 있다.

담당 역할

서비스 중인 모바일 어플리케이션 취약점 점검

사용 Tool

APK Easy Tool , Game Guardian, Unity

수행 내역

메모리변조 및 적용 여부 확인

루팅권한으로 실행 여부 확인

어플리케이션 위변조 여부 확인

모바일 게임 취약점 분석

프로젝트 기간

2018.07 (2주)

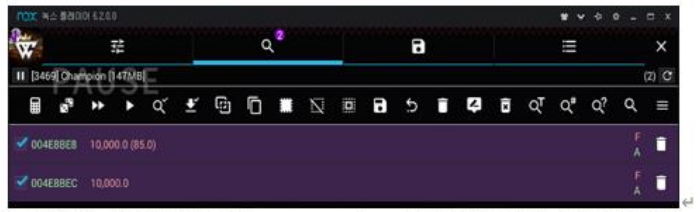
프로젝트 현황

완료

프로젝트 이미지

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
메모리 변조 도구 점검 실행	●		●	●	●		●		●	●	●	●	●		●	●	●
메모리 변조 확인			●				●		●	●	●						●
디바이스의 루팅 상태 점검	●		●	●	●		●		●	●	●	●	●		●	●	●
어플리케이션 위/변조					●						●				●		●
가상 머신 내 실행	●		●	●	●	●	●	●	●	●	●	●	●		●	●	●
Unity 라이브러리 난독화 적용				●		●	●			●	●	●	●	●			

모바일 게임 점검 항목 List

점검 항목	메모리 변조	메모리 변조 도구 점검 실행 및 변조확인
점검 결과 상세	  게임 실행 전 메모리 변조 도구(GameGuardian) 설치/실행 상태를 점검하고 있지 않으며, 라이프 수치가 변조 가능하여 게임 플레이 시 Miss가 발생해도 Game Over 되지 않음 ⇨ 메모리 변조 도구(GameGuardian) 탐지 기능 추가를 권고 드립니다. ⇨ 중요 변수 값은 인코딩 하여 메모리 상에서 다른 형태로 존재하도록 적용 ⇨ 단말기의 루팅 상태를 파악하여, 게임 앱이 설치 또는 실행되지 않도록 적용

각 게임 별 점검 결과 정리 및 보고서 작성

AWS 와 보안

프로젝트 기간

2018.09 – 2018.12

프로젝트 현황

완료

개요

ISMS 심사를 대비하여 사내 운용중인 AWS 실태 파악 및 클라우드 보안 대책 강구를 위한 서버 환경 구성 및 보안 서비스를 알아보고 직접 사용해 봄

담당 역할

AWS 운용 상태 파악 및 보안 서비스 조사

개발 환경

AWS

개발 내용

- ISMS 심사에 대비한 AWS의 보안 서비스 및 모니터링 서비스 확인
- 사내 AWS 구상도를 통해 개인 AWS 환경 구축을 하고 각종 보안 서비스 적용

참고 링크

https://github.com/hasihime/resume/blob/master/project/00.SimpleProject/01_aws/aws.md

AWS 와 보안

프로젝트 기간

2018.09 – 2018.12

프로젝트 현황

완료

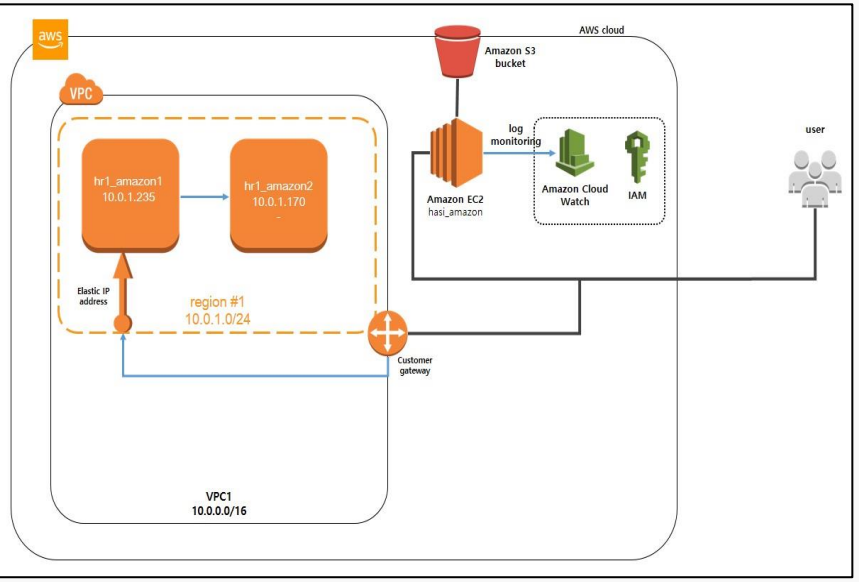
프로젝트 이미지

AWS 에서 **보안 서비스는 IAM, VPC 설정** 등이 있으며, **모니터링과 관련된 서비스는 CloudWatch, CloudTrail, Trusted Advisor**가 있음

- 현재 사내에서 사용중인 AWS 보안대책은 다음과 같음 .
  - 정책에 따라 보안 설정이 되어있으며, 시스템 팀에서 운영 중

구분	서비스명		내용
네트워크 보안	VPC	Security Group	OS 기반 가상 서버의 보안 서비스
		ACL 설정	각 VPC 영역간 네트워크 접근 통제 정책 적용
		VPN	Private IP 로 설정된 인스턴스의 통신이 가능하게 해준다.
	EC2	Security Group	AWS 리소스의 보안 서비스
계정 보안	IAM		계정, 그룹, 정책, 역할 관리 및 권한 부여
모니터링 및 로그 관리	Cloud Watch Logs		AWS 리소스 및 AWS기반 어플리케이션 모니터링 및 알람 설정
	Cloud Trail		AWS API 요청에 대한 로그 기록
	Trusted Advisor		비용, 가용성, 보안 측면의 취약점 검사 및 개선사항 제시 및 이를 응용한 키 유출 시 알려줌

AWS의 보안 서비스와 모니터링 서비스 정리 문서



사내 AWS 현황으로 구성한 개인 AWS 구상도

Vue를 이용한 반응형 웹 프로젝트

프로젝트 기간

2020.01 – 2020.02

프로젝트 현황

완료

개요

창작자를 위한 작품 투고 반응형 웹페이지를 제작하면서 서버환경 설정 및 통신 관련 이슈를 해결한 프로젝트.

담당 역할

서버 환경 구축, HTTPS 환경 세팅, BackEnd 컨트롤러 개발

개발 환경

Frontend : Vue

Backend : SpringBoot, Mysql

Server : firebase AWS

개발 내용

- AWS 서버 구축. Firebase와 AWS 연동.
- Mixed content 에러 해결을 위한 cors 설정
- 웹페이지 테스트 시나리오 작성 후 수행

참고 링크

https://github.com/hasihime/resume/blob/master/project/02.VueProject/VueProjectDoc.md

Vue를 이용한 반응형 웹 프로젝트

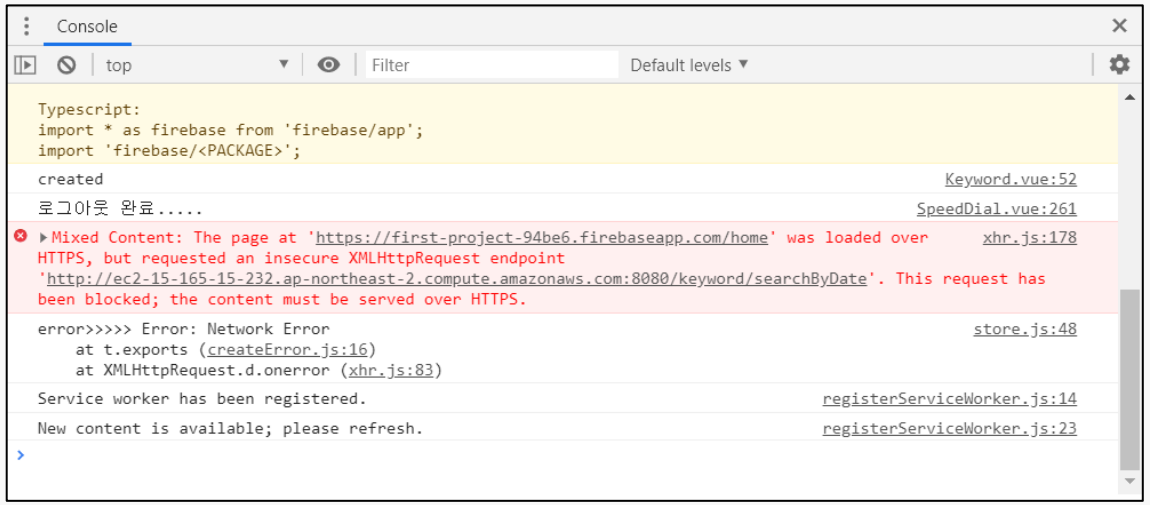
프로젝트 기간

2020.01 – 2020.02

프로젝트 현황

완료

프로젝트 이미지




```
21
22
23 @CrossOrigin(origins ="*", maxAge = 6000)
```

```
server.port=8443
http.port=8080
server.ssl.enabled=true
server.ssl.key-store-type= PKCS12
server.ssl.key-store= classpath:ssafy.p12
server.ssl.key-store-password= otoxmaho330
server.ssl.key-alias= tomcat
```

firebase에 올라간 Vue Frontend와 AWS에 SpringBoot BackEnd의 서로 맞지 않은 통신(HTTPS-HTTP)으로 문제 발생

-> Tomcat의 SSL 환경 세팅 및 BackEnd의 컨트롤러에 Cors 적용으로 해결한 코드

맛집 빅데이터 분석 및 추천 프로젝트

프로젝트 기간

2020.02 – 2020.03

프로젝트 현황

진행중

개요

맛집 빅데이터를 통해 사용자에게 음식점을 분석 후 제공해주고 나아가 추천해주는 서비스를 제공해준다.

담당 역할

Python Django RestController 및 추천 알고리즘 구현

개발 환경

BackEnd : Python Django

데이터 분석 : Pandas

개발 내용

- BackEnd 컨트롤러를 Python Django로 구현
- 데이터 분석을 위해 Pandas로 전처리 후 가공
- TF-IDF를 통해 리뷰별 사용자 추천 알고리즘 구현 중

맛집 빅데이터 분석 및 추천 프로젝트

프로젝트 기간

2020.02 – 2020.03

프로젝트 현황

진행중

프로젝트 이미지

```python
from parse import load_dataframes
import pandas as pd
import shutil


def sort_stores_by_score(dataframes, n=20, min_reviews=30):
    """
    Req. 1-2-1 각 음식점의 평균 평점을 계산하여 높은 평점의 음식점 순으로 `n`개의 음식점을 정렬하여 리턴합니다

    """
    stores_reviews = pd.merge(
        dataframes["stores"], dataframes["reviews"], left_on="id", right_on="store"
    )
    # print(stores_reviews)
    scores_group = stores_reviews.groupby(["store", "store_name"])
    scores = scores_group.mean().sort_values(by=['score'],axis=0,ascending=False)
    """
```

```
[최고 평점 음식점]
----------------------------------------------------------------------------------------------------------------------------------

1위: 더아리엘(4.82점)
2위: 농민백암순대(4.61점)
3위: 다운타우너(4.61점)
4위: 정돈(4.43점)
5위: 미분당(4.37점)
6위: 소이연남(4.30점)
7위: 을밀대(4.29점)
8위: 사모님돈가스(4.25점)
9위: 고기리 막국수(4.24점)
10위: 종암해장(4.21점)
11위: 명진전복(4.18점)
12위: 명동교자(4.16점)
13위: 브루클린더버거조인트(4.13점)
```

Pandas를 이용하여 DataFrame을 생성 후
원하는 필터로 구현 코드 및 결과

감사합니다