IDS/IPS 개발 계획서

2020. 07. 20.

이 얼마나 아름다운 청춘인가!

오선식, 김청준, 이안나, 백송선, 전은영

1. 개요

1) 목적: IDS/IPS 구현

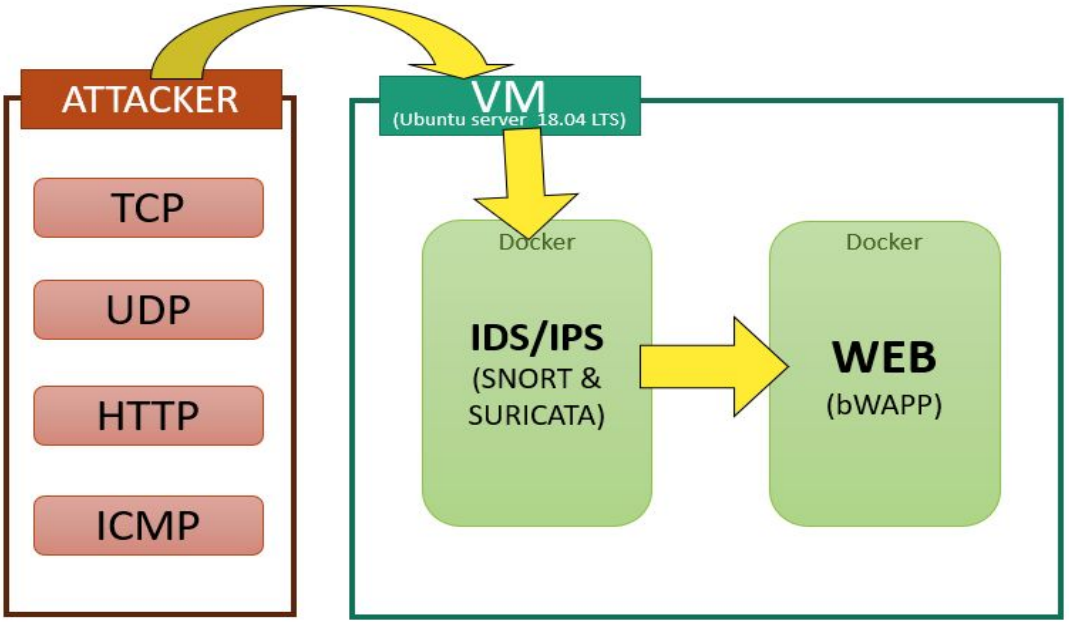
2) 개발환경

- Linux(Ubuntu Server 18.04 LTS)
- Virtual Machine(VMware / Virtual Box)
- Docker
- Snort 3.0.2
- Suricata 5.0.3

3) 네트워크 환경 : NAT, Bridge

4) 구성 : VM ~ IDS/IPS(Docker) ~ bWAPP(Docker)

2. 구조



1) Network architecture

- Expected Network Flow : VM ~ IDS ~ IPS ~ bWAPP
- Docker network conf. : Undefined
- Port forwarding : Undefined

2) IDS

- 공격자가 접속을 하게되면 패킷을 분석하여 공격 탐지
- 넓은 범위의 룰을 적용하여, alert와 로그 기록
- Rule Set Level : Strict

3) IPS

- 공격자의 패킷 탐지 및 차단
- IDS Log를 분석하여, Black List 방식의 Drop 룰 작성
- 룰적용을 반복하여 False positive와 False Negative의 정도를 판단
- Rule Set Level : Rough

3. 공격 목록

1) TCP

- TCP SYN Flooding
- SYN_FIN flag 변형 비정상 패킷
- FIN flag만 설정된 비정상 패킷
- flag가 설정되지 않은 비정상 TCP패킷(NULL 패킷)

2) UDP

- UDP port scanning
- UDP Flooding

3) HTTP

- HTTP GET Flooding
- HTTP POST Flodding
- Slow HTTP POST Dos
- Slow HTTP Header Dos
- Slow HTTP Read Dos
- XSS
- SQL Injection
- File Upload
- CSRF

4) ICMP

- ICMP Redirection(Type 5)
- ICMP Flooding

4. 명령어 사용 예제

1) Snort

- alert tcp any any -> any 80 (content:"?Action="; nocase; pcre:"/\?Action\=(MainMenu|Show|Course|getTerminalInfo|ServerInfo|Cmd1?Shell|EditFile|Servu|sql|Search|UpFile|DbManager|proxy|toMdb)/i";)
- bWAPP를 통해 공격 시그니처 파악 후, BODY부분에 적용

2) Suricata

- drop tcp $SOURCE_NET any -> $DESTINATION_NET any (msg:"Message with semicolon\;" +옵션 ;)
- 참조 (https://suricata.readthedocs.io/en/suricata-4.1.4/rules/intro.html)

5. 일정

프로젝트명 : IDS/IPS
프로젝트팀명 : 나는 왕자가 될 상인가?(오선식, 김정준, 이안나, 백송삼, 전은영)

"무쭉권! 명확하고 간결하게"

주요 Task				산출물	담당자	7월			8월			
대분류	중분류	소분류	상세 Task			11-17	18-24	25-31	1-7	8-14	15-21	22-28
착수	개발준비	개발사전준비	마음의 준비 및 텐 션 업	S2 의지 S2	공통							
	계획서 수립	프로젝트 계획서 작성	프로젝트 범위 설정 및 일정 계획	WBS	공통							
		개발 계획서 작성	기능 요구사항 분석	개발 계획서	공통							
	사전 학습	개발 관련 내용 사전 학습	- 방화벽 원리 및 이해 (IDS/IPS) - snort 및 suricata 학습 - Protocol 학습 (TCP / UDP / ICMP / HTTP)	지식	공통							
	요구사항 분석	snort 룰	shell-strom, apache exploit, Exploit-db.com 등의 자료 참고 공격 패킷 특징(payload) 분석 -> 그에 따른 방화벽의 동작	요구사항정의서	공통							
구축 및 구현	구축	구현 및 테스트 하기 위한 환경 구성	Ubuntu 18.04 LTS server - dorker - snort, suricata, BWAFF		공통							
			Nework 환경 : NAT(Port 포워딩 호스트 한 번, NAT Setting으로 한 번)		공통							
	구현	Rule set 구현	여러 공격을 막기 위한 방화벽에 쓰일 기반 Rule 구현		공통							
		단위 테스트	단위테스트 진행 및 수정사항 도출	단위테스트 결과	공통							
테스트	검증	동작 검증	wfuzzer & 4조에서 만드는 퍼저로 테스트		공통							
결과	보고서 작성	결과보고서 작성	- 구현된 프로그램 설명 - 프로그램 사용 방법 작성 - 기타 등등	결과보고서	공통							
Mile Stone	기초단계 마감	프로젝트 계획 및 개발 환경구성	개발 계획서 작성 및 개발 환경 구성 완료	-	공통							
	중간 보고	기능 구현 중간 검토	기능 단위테스트 및 보고서 중간 검토	중민 멘토님의 관심과 사랑	공통							
	완료 보고	프로젝트 마무리	결과물 산출 및 개발 보고서 완료, 최종 검토		공통							