Snort를 활용한 침입탐지 시스템 개발

최효현*, 김수지O
*인하공업전문대학 컴퓨터정보과,
O인하공업전문대학 컴퓨터정보과
e-mail: hchoi@inhatc.ac.kr*, suij20th@naver.comO

Development of intrusion detection System using Snort

Hyo Hyun Choi*, Su Ji KimO
*Dept. of Computer Science & Engineering, Inha Technical College,
ODept. of Computer Science & Engineering, Inha Technical College

● 요 약 ●

코로나 19에 따라 온라인 교육이나 재택근무 등 비대면 서비스에 대한 관심과 이용이 높아지면서, 비대면 서비스의 보안취약점으로 개인정보 유출과 해킹 등의 피해 우려도 제기되고 있는 상황이다. 본 논문에서는 오픈소스 IDS인 SNORT를 이용하여 침입탐지가 발생했을 경우 미리 설정해 놓은 priority에 따라 이메일 또는 문자메시지로 관리자에게 실시간 알림을 보내기 위한 방법을 제안한다. 제안한 시스템은 여러 개의 구성 요소로 이루어져 있다. Snort는 이벤트를 모니터하고 경계시키며(alert), 시스템 규칙을 사용하여 수신된 보안 이벤트로부터 경고를 생성한다. 경고를 파일에 LOG 형식으로 쌓게 되고 쉘 스크립트를 이용해 침입탐지를 분석하여 관리자에게 메일이나 SMS형태로 전송하게 된다.

키워드: 사이버 위협(Cyber threat), 침입탐지(Intrusion detection), 스노트(Snort)

I. Introduction

코로나 19에 따라 온라인 교육이나 재택근무 등 비대면 서비스에 대한 관심과 이용이 높아지면서, 비대면 서비스의 보안취약점으로 개인정보 유출과 해킹 등의 피해 우려도 제기되고 있는 상황이다. 때문에 정보보안의 역할이 그 어느 때보다 중요한 시점이며 급증하는 보안 위협에 얼마나 빠르고 정확한 대응이 필수적이다. 이에 본 논문에서는 오픈소스 IDS인 SNORT를 이용하여 침입탐지가 발생했을 경우 미리 설정해 놓은 priority에 따라 이메일 또는 문자메시지로 관리자에게 실시간 알림을 보내기 위한 방법을 제안한다.

II. Preliminaries

1. GNS

GNS3(Graphical Network Simulator-3)은 2008년에 처음 출시된 네트워크 소프트웨어 에뮬레이터이다. 가상 및 실제 기기의 결합을 허용하며 복잡한 네트워크를 시뮬레이션하는 목적으로 사용된다. Dynamips 에뮬레이션 소프트웨어를 사용하여 시스코 IOS를 시뮬레이션한다.

2. Snort

스노트(Snort)는 자유-오픈 소스 네트워크 침입 차단 시스템(NIPS: Network Intrusion Prevention System)이자, 네트워크 침입 탐지 시스템(NIDS: Network Intrusion Detection System)으로서, 마틴 로시가 1998년에 개발하였다. 스노트는 현재 로시가 창립자이자 개발자인 Sourcefire에 의해 개발되고 있으며, 2013년 이후로 시스코 시스템즈가 소유중이다.

III. The Proposed Scheme

GNS를 이용하여 칼리 리눅스 기반의 공격 PC, WEB 서버, IDS 서버가 서로 통신될 수 있는 네트워크 환경을 구축하고 칼리 리눅스의 여러 해킹툴을 이용하여 WEB서버에 공격을 시도한다 (그림 1). 이때 SNORT는 스위치의 포트 미러링을 통해 유입(sniffing) 되는 트래픽을 분석하여 작성한 탐지 규칙그림2에 맞춰 로그를 쌓는다(그림 3). 침입탐지 알리미(쉘스크립트)는 실시간으로 탐지된 로그를 AWK를 이용하여 분석해 탐지된 공격의 PK 값과 발생시각을 추출한다. 쉘스크립트는 공격 PK와 Priority가 맵핑되어있는 Attack_List.txt 파일에서 탐지된 PK의 Priority를 확인한다. 그림 4와 그림 5에서는

탐지 결과가 이메일과 문자로 전송되는 결과를 보였다.

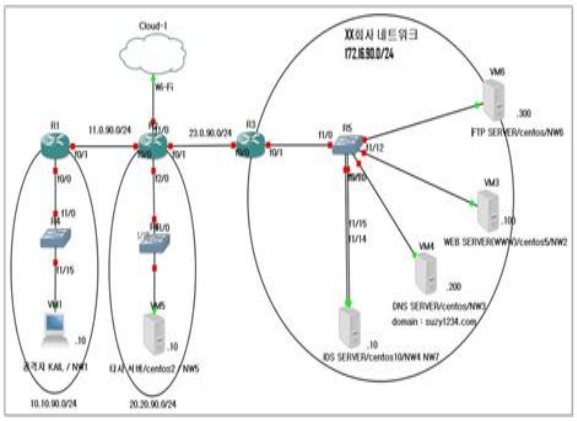

Fig. 1. Network Topology using GNS3

```
#XSS 공격
alert tcp any any -> 172.16.90.100 any (sid:1000006; msg: "XSS_Detected";\
content:"|25 33 43|script"; nocase;)

#SYN Flooding 공격
alert tcp any any -> 172.16.90.100 80 (sid:1000008; msg: "TCP_Syn_Flooding_
flags:S; threshold: type both, track by_dst, count 100, seconds 1;)
```

Fig. 2. The Example of Snort Policy

```
[**] [1:1000006:0] XSS Detected [**]
[Priority: 0]
12/02-01:28:10.368579 10.10.90.10:58736 ->
TCP TTL:61 TOS:0x0 ID:28058 IpLen:20 DgmLen
***AP*** Seq: 0x24DC229C Ack: 0x4CF7A798
TCP Options (3) => NOP NOP TS: 33181544 125

[**] [1:1000008:0] TCP Syn Flooding Attack
[Priority: 0]
12/02-01:31:15.110801 53.53.147.184:2632 ->
TCP TTL:61 TOS:0x0 ID:45071 IpLen:20 DgmLen
******S* Seq: 0x70B3F60B Ack: 0x19DF8823
```

Fig. 3. The example of Logging

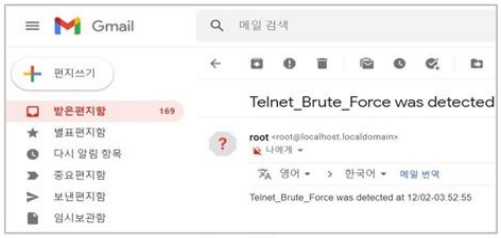

Fig. 4. Email alerting the Intrusion Detection

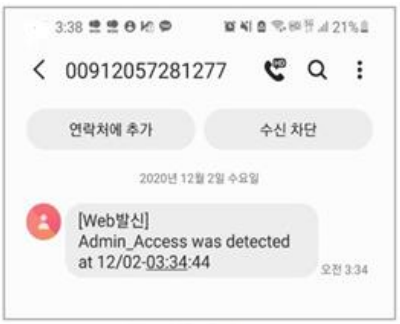

Fig. 5. SMS alerting the Intrusion Detection

IV. Conclusions

본 논문에서는 정보보안의 역할이 그 어느 때보다 중요한 시점이며 급증하는 보안 위협에 얼마나 빠르고 정확한 대응이 필요한지 알아보고 오픈소스 IDS인 SNORT를 이용하여 침입탐지가 발생했을 경우 미리 설정해 놓은 priority에 따라 이메일 또는 문자메시지로 관리자에게 실시간 알림을 보내기 위한 시스템을 개발 결과를 보였다. 추후에는 실제로 동작하는 네트워크 시스템에서의 개발 및 테스트를 수행할 계획이다.

REFERENCES

[1] GNS3 https://www.gns3.com/software/download
[2] SNORT https://www.snort.org/downloads