사이버 침입 탐지 시뮬레이션을 위한 SSFNet 기반 IDS의 확장

유관종°, 이은영, 김도환, 최경희
*아주대학교 정보통신전문대학원, **국가보안기술연구소
kjyou@ajou.ac.kr°, eylee@etri.re.kr, dkim@etri.re.kr khchoi@ajou.ac.kr

Extending of IDS for Network Intrusion simulations based on SSFNet

Kwan jong Yoo°, Eun young Lee, Do hwan Kim, Kyung hee Choi
*Graduate School Information and Communication, Ajou University
**National Security Research Institute

요 약

사이버침입을 수행하고 이에 따른 네트워크의 행동변화를 시뮬레이션 하기 위해서는 실제 네트워크 구조를 반영하는 네트워크를 모델링한 후 각 서브시스템의 특성을 네트워크 모델에 반영하여야 한다. 본 논문에서는 프로세스 기반 사건 중심 시뮬레이션 시스템인 SSFNet을 기반으로 사이버 침입 시뮬레이션에서 핵심 요소인 침입 탐지 시스템(IDS)을 구현하였다. 구현된 IDS는 룰 기반 오용 행위 탐지 방식의 네트워크 침입탐지 시스템이며, 다양한 시뮬레이션을 통해 구현된 모듈의 성능 및 실세계 반영 모습을 제시하였다.

1. 서 론

최근 인터넷을 통한 네트워크 침입의 증가와 점점 더 정교해지고 복잡해지는 네트워크 침입의 구조들로 인해 네트워크의 운용을 관장하는 시스템 관리자들은 더욱 높은 수준의 침입탐지와 사이버 테러에 대한 효율적인 방어를 위한 노력을 필요로 한다. 사이버 테러의 분석과 방어를 위해서는 실제 네트워크 환경에서 발생되었거나 발생 가능한 침입에 대한 방어를 수행해보고, 그에 대한 행동 특성을 분석해 보는 것이 가장 좋은 방법이다. 하지만, 실제 대규모 네트워크 환경에서 이러한 실험을 하는 것은 현실적으로 불가능 하거나, 많은 비용이 든다. 그러므로 실제 네트워크 환경과 유사한 동작을 하는 시뮬레이션을 통한 연구가 가장 적합한 방법이며, 이 기법은 모델링을 통한 실험이므로 실제 시스템에 대한 위험 부담이 없고, 모델에 대한 실험이므로 적응이 용이하고 비용이 저렴하며, 기존의 침입 기법뿐만 아니라 이들의 다양한 조합을 통한 향후 발생 가능한 침입유형에 대한 분석이 가능하다는 이점을 갖는다.

본 논문에서는 SSFNet 환경에서 여러 사이버침입을 방어하는 시뮬레이션의 핵심 요소인 침입 탐지 시스템(IDS)을 구현하였다. IDS는 네트워크 상에서 이루어지는 침입을 탐지하기 위한 소프트웨어 · 하드웨어적 도구로서, 크게 호스트 기반의 침입탐지 시스템과 네트워크 기반의 침입탐지 시스템으로 나누어질 수 있다.

본 논문에서 구현된 IDS는 다양한 네트워크 침입을 유형을 탐지해 낼 수 있는 Snort System을 기반으로 한 규칙 기반 오용 행위 탐지 방식의 네트워크 침입탐지 시스템(NIDS)이다.

본 논문의 개요는 다음과 같다. 2장 에서는 IDS 구현에 관련된 기존의 연구에 대해 알아보고, 3,4장 에서는 본 논문에서 제안하는 IDS의 구조를 설명한다. 그리고 마지막 5장 에서는 결론과 함께 향후 과제에 대해 기술한다.

2. 관련연구

2.1 SSFNet [1]

NS-II[2] 와 함께 대표적인 네트워크 시뮬레이터인 Scalable Simulation Framework Network Models (SSFNet)은 Domain Modeling Language(DML)을 이용하여 10만개 이상의 시스템이 존재하는 대규모 네트워크를 호스트 단위로 디자인 할 수 있다. 또한 SSFNet이 지원하는 현실 세계를 반영하는 호스트 모델링과 라우팅 프로토콜, 네트워크의 속도 등 각 네트워크가 갖는 특성을 바탕으로 네트워크를 구성하기 때문에 사이버 침입과 관련한 현실 세계와 유사하게 동작하는 네트워크 환경의 모습을 관찰할 수 있다.

2.2 Snort[3]

Snort는 Martin Roesch에 의해 초기 개발되어지고 현재는 많은 수의 개발자에 의해 연구되고 있는 packet sniffer, packet logger, 네트워크 기반 IDS등의 기능을 가진 보안 어플리케이션이다. Snort에는 core snort suite 뿐만 아니라 snort 로그 파일들을 기록 · 유지하고, 최근의 Snort Rule Set들을 패치 · 보존하며, 잠재적인 유해 트래

픽 발생시 시스템 관리자에 경고해주는 여러가지 부가 프로그램이 개발되어 있다. 게다가 기본적으로 제공하는 TCP/IP 네트워크 프로토콜뿐만 아니라 부가적인 사용자 정의 확장 프로그램을 사용하면 노벨사의 IPX등의 통신 프로토콜에 대한 지원도 가능하다. 그러므로 Snort는 네트워크 관리자들이 사이버 침입에 대응하는 보안 정책을 설계할 때 유용하다.

2.3 일반적인 침입 탐지 시스템의 구조[4]

침입 탐지 시스템은 크게 패킷을 캡처하는 부분과, 캡처한 패킷을 침입 탐지 룰에 매칭하기 용이하도록 디코딩하는 패킷 디코더(Packet Decoder)부분, 사용자가 지정한 룰 셋을 이용하여 룰 테이블을 관리하는 룰 테이블(Rule Table), 디코딩된 패킷을 룰 테이블과 비교하는 탐지 엔진(Detection Engine), 그리고 탐지된 룰을 기록하는 로그 부분으로 그 역할을 구분할 수 있으며, 본 논문에서 구현된 IDS도 이 구조를 따른다.

3. IDS 룰 셋

룰 셋은 IDS에서 가장 중요한 부분으로, 캡처한 패킷을 사용자가 지정한 룰 셋과 비교하여 일치하면 유해한 패킷으로 검출 할 수 있도록 한다.

각각의 룰 셋은 프로토콜(Protocol)별로 구분되어 저장되어 있으며, 또 각각의 프로토콜별로 저장된 룰들은 다시 TCP와 UDP는 목적 포트별로, ICMP는 ICMP타입별로 구분되어 저장된다.

룰 셋은 룰 헤더 부분과 룰 옵션 부분으로 구분되며, 룰 헤더는 패킷을 구분할 때 의미가 있는 중요한 특성을 표현하고, 룰 옵션부분은 해당 패킷을 구분하기 위한 부가적인 정보를 담고 있다.

Rule Header	
이름	설 명
action	룰에 매치 되었을 시에 할 행동의 지정. ALERT(경고 메시지), LOG(로그 메시지), IGNORE(무시)의 세 종류가 있다.
protocol	TCP/UDP/ICMP 세 가지 프로토콜 타입의 프로토콜이 고려되었다. 캡처한 패킷의 프로토콜 타입을 구분한다.
scrAddr	패킷의 Source 주소
srcPort	패킷의 Source Port 번호
dstAddr	패킷의 Destination 주소
dstPort	패킷의 Destination Port 번호

[표 1] IDS Rule Set Header

Rule Option	
이름	설명
ttl	IP 헤더의 Time To Live
tos	IP 헤더의 Type Of Service
icmp_type	ICMP message type
icmp_code	ICMP message code
icmp_id	ICMP message ID
icmp_seq	ICMP message sequence
tcp_flags	TCP의 SYN, FIN, ACK등의 필드를 지정
tcp_seq	TCP의 sequence number를 지정
tcp_ack	TCP의 Acknowledge number를 지정
payload	각 서비스의 데이터 payload에 대한 정보. 캡처한 패킷의 payload 부분에 일치하는 패턴이 발견되면 룰에 해당 되는 공격으로 인식
rate	해당 룰 셋이 매치되는 횟수를 지정하여, 1초 동안 이 횟수 이상으로 매치 되면 침입으로 인식
msg	룰 셋의 정보를 표시

[표 2] IDS Rule Set Option

룰 매칭 프로세스를 살펴보면 다음과 같다.

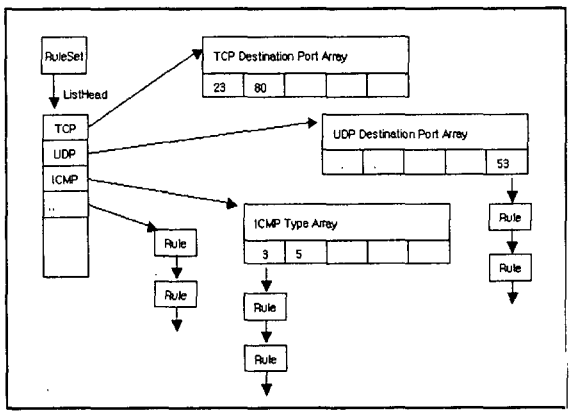
① 캡처한 패킷의 프로토콜 종류를 파악한 후, 지정된 프로토콜의 룰 셋 리스트를 찾아간다.

② TCP 또는 UDP 패킷 이라면 룰 셋 리스트에서 Destination Port를 기준으로 검색을 하고, ICMP패킷인 경우 ICMP Type을 기준으로 검색을 한다.

③ 검색된 룰 셋에 Payload 정보가 있다면, 룰 셋에서 검출 하고자 하는 스트링이 패킷의 Payload 부분에 존재하는지 검색한다.

④ 검색된 룰 셋에 Rate 정보가 있다면, 1초 동안 해당 룰 셋이 지정된 횟수 이상 일치했는지 검사하고 그렇다면 룰 셋 매칭이 된다.

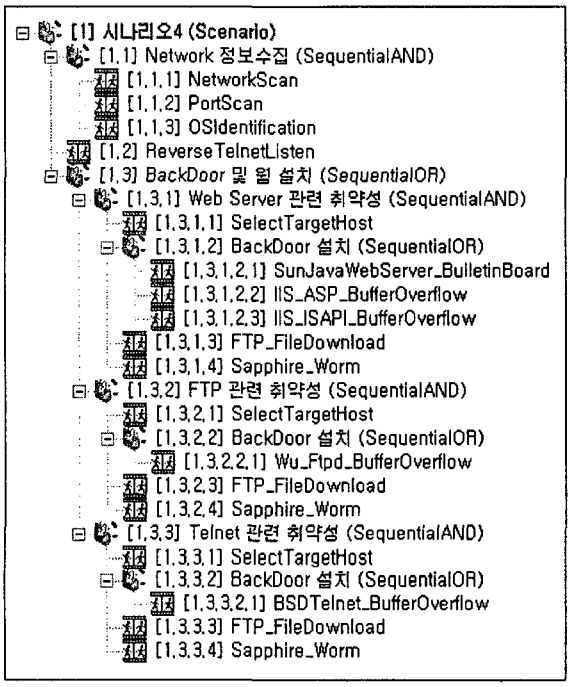
⑤ 매치된 룰 셋 과 패킷 정보를 LOG 에 기록한다.



[그림 1] Rule Set Matching Flow

4. 시뮬레이션

본 논문에서는 구현된 IDS를 테스트 하기위해 SSFNet 기반의 시뮬레이터에서 각종 공격 시나리오를 작성하였다.



[그림 2] 각종 공격 시나리오

이 시나리오는 우선 ①네트워크 스캔을 통해 대상을 선정하고, 선정된 호스트들에게 ②웹 서버 / FTP / Telnet 취약성을 이용한 공격을 시도하게 되며, 취약성 공격이 성공하면 ③Sapphire Worm 전파를 시도한다.

각 공격을 위해서 각각 특징적인 트래픽 패턴이 발생하게 되는데, 네트워크 스캔 시에는 짧은 시간동안 비정상적으로 다량의 ICMP패킷이 검출되며, 취약성 공격 시에는 payload 부분에 Buffer overflow가 확인되고, Sapphire worm이 전파될 때에는 특정 포트(TCP 1434)를 사용한 트래픽이 검출 된다. 이러한 특징을 기반으로 IDS 룰 셋이 작성되었다.

① 네트워크 스캔을 검출하는 룰 셋

- Action=ALERT useProtocol=icmp srcAdd=* srcPort=* destAdd=* destPort=* (icmp_code=0 icmp_type=8 rate=10 msg=[ICMP Ping Flood])

② 취약성 공격을 검출하는 룰 셋(FTP인 경우)

- Action=ALERT useProtocol=tcp srcAdd=* srcPort=* destAdd=* destPort=21 (payload={BUFFEROVERFLOW} msg=[FTP Buffer overflow])

③ Sapphire Worm을 검출하는 룰 셋

- Action=ALERT useProtocol=tcp srcAdd=* srcPort=* destAdd=* destPort=1434 (msg=[Sapphire Worm])|

위의 시나리오를 이용하여 시뮬레이션 했을 때, IDS가 출력한 로그파일을 살펴보면 다음과 같다.

```
[IDS-Log] 1.01 [IDS=1:0] 7:3:1(0) 1:10(0) ICMP Ping Flood Atteck Detected
[IDS-Log] 1.02 [IDS=1:0] 7:3:1(0) 1:11(0) ICMP Ping Flood Atteck Detected
[IDS-Log] 1.03 [IDS=1:0] 7:3:1(0) 1:12(0) ICMP Ping Flood Atteck Detected
                                .
                                .
[IDS-Log] 221 [IDS=1:0] 7:3:1(0) 1:10(0) FTP Buffer Overflow Atteck Detected
[IDS-Log] 222 [IDS=1:0] 7:3:1(0) 1:11(0) FTP Buffer Overflow Atteck Detected
[IDS-Log] 223 [IDS=1:0] 7:3:1(0) 1:12(0) FTP Buffer Overflow Atteck Detected
                                .
                                .
[IDS-Log] 521 [IDS=1:0] 7:3:1(0) 1:10(0) Sapphire Worm Atteck Detected
[IDS-Log] 522 [IDS=1:0] 7:3:1(0) 1:11(0) Sapphire Worm Atteck Detected
[IDS-Log] 523 [IDS=1:0] 7:3:1(0) 1:12(0) Sapphire Worm Atteck Detected
```

5. 결론 및 향후과제

본 논문에서는 SSFNet에서 방화벽과 더불어 네트워크 관리의 핵심 요소라고 할 수 있는 침입 탐지 시스템을 확장하였다. 제안된 시스템은 침입 탐지 시스템 중 가장 대표적으로 잘 알려진 Snort 시스템의 기본 개념을 바탕으로 유입되는 패킷의 프로토콜 분석, 내용 검색/매칭을 통하여, 침입 탐지 시스템의 규칙에 따른 침입 탐지 기능을 수행할 수 있다.

향후 과제로는 고도로 복잡화 된 네트워크 침입에 대한 유형 분석을 통하여 좀 더 현실 세계와 유사한 네트워크 침입 탐지 결과를 표현할 수 있고, 좀 더 다양한 사용자의 규칙 적용을 통해 네트워크 트래픽을 감시하고 경고할 수 있는 시스템을 구현해야 할 것이다.

[참고문헌]

[1] SSFNet, http://www.ssfnet.org
[2] NS2, http://www.isi.edu/nsnam/ns/
[3] Snort System, http://www.snort.org/
[4] Anderson, D., Frivold, T. and Valdes A.: Next Generation Intrusion Detection Expert-System (NIDES) - A Summary, Technical Report SRI-CSL-95-07, SRI International, 1995
[5] Donald Welch, Greg Conti, "A Framework for an Information Warfare Simulation", Proceedings of the 2001 IEEE Workshop on Information Assurance and Security, United States Military Academy, West Point, NY, 5-6 June, 2001.
[6] Information Warfare and Security, Addison-Wesley, 1999
[7] Jea-hyuk Lee, Eul-guy Im, Joo-beom Yoon, Seung-kyu Park, "Network Intrusion and Defense Simulation Framwork based on SSFNet", The 6th international conference on advanced communication technology, 2004
[8] Jin-hyuk Kim, Eul-gyu Im, Joo-beom Yoon, Seung-koo Park, "Network Intrusion Model for analyzing intrusion patterns", The 6th international conference on advanced communication technology, 2004