HVIDB를 이용한 해당 호스트의 오탐율 경고 발생 감소에 관한 연구

김태훈° 이금석
동국대학교 컴퓨터공학과
{xognsl°, kslee}@dongguk.edu

A Study on False Positive Alert reduction using HVIDB of Target Host

Taehoon Kim° Keumsuk Lee
Dept. of Computer Science, Dongguk University

요 약

NIDS(Network Intrusion Detection System)는 공격 탐지 과정에서 대량의 로그가 발생하게 되는데 일반적인 침입탐지 시스템에서 탐지되어 하루에 남는 로그만으로도 시스템에 막대한 양을 차지한다. 이러한 문제점은 관리자에게 많은 부담을 줄 뿐만 아니라 그렇게 남겨진 로그에는 오탐율(False Positive) 비율이 높기 때문에 관리자가 실제로 위협적인 침입을 식별하고, 침입 행위에 대한 빠른 대응을 어렵게 만든다. 그러므로 NIDS와 특정 호스트가 가지고 있는 보안상 취약한 부분을 비교하여 판단할 수 있는 침입탐지시스템을 선택, 운용하는 것은 관리측면이나 대응측면에서 매우 중요한 일이라고 할 수 있다. 본 논문에서는 NIDS와 해당 호스트 취약점 정보를 이용해 작성된 데이터베이스(HVIDB : Host Vulnerability Information Database)를 이용하여 호스트의 취약성에 관한 로그만을 최종 경고해줌으로써 오탐율의 양을 감소시키고 호스트 보안성의 향상과 관리자가 로그분석 등의 IDS 업무를 효과적으로 할 수 있는 모델을 제시한다.

1. 서 론

현재 NIDS(Network Intrusion Detection System)는 방화벽 앞이나 뒤에 설치하여 특정 내부 망을 보호할 수 있기 때문에 관리상의 비용이 저렴하고 시스템에 부하가 적어 많은 회사들이 NIDS를 이용하여 침입을 감시하고 있다[3][4]. 하지만 실제 공격이 아닌 정상행위인데도 불구하고 공격으로 판단하거나, 해당 호스트와 상관없는 공격 정보까지도 심각한 경고로 발생시키는 오탐지율이 높다는 근본적인 단점을 가지고 있고[7][10], 그러한 경보데이터가 다량으로 발생함에 따라서 탐지된 경보데이터 가운데 실제 침입 탐지에 사용되는 정보 데이터를 구분해내는데 다수의 시간이 걸린다는 단점 역시 가지고 있다. 따라서 관리자가 해당 호스트를 효율적으로 운용하기 위해서는 우선 IDS로부터 탐지된 경보데이터 가운데 실제 분석에 필요한 즉, 해당호스트가 가지고 있는 취약점과 관련된 정보를 이용하여 경보 데이터를 추출해 관련 정보만이 최종 관리자에게 보고 되어져야 한다.

본 논문에서는 이런 관점에서 네트워크에서 탐지되는 많은 경고 메시지 중 해당 호스트의 취약점 관련 정보만을 추출하여 DB로 구축한 후 그 정보를 이용하여 호스트에게 경고를 발생시킬 수 있는 시스템을 제안한다.

제안하는 시스템은 이런 HVIDB(Host Vulnerability Information Database)를 이용함으로써 기존 IDS에 큰 문제로 자리 잡고 있던 오탐지율을 줄이고, 결과적으로 관리자가 해당호스트의 취약한 부분에 대해서도 신속하게 대응 할 수 있고 그와 관련된 경고 데이터만을 분석함으로써 관리자의 빠른 대응효과 및 호스트의 보안성을 높일 수 있는 장점을 제공해 준다.

논문의 구성은 2장에서 개념 정의 및 관련연구를 설명하고 3장에서는 전체 시스템의 흐름과 제안하는 HVIDB의 구조에 대해 설명하고 마지막 4장에서는 결론과 향후 연구 방향을 제시한다.

2. 관련 연구

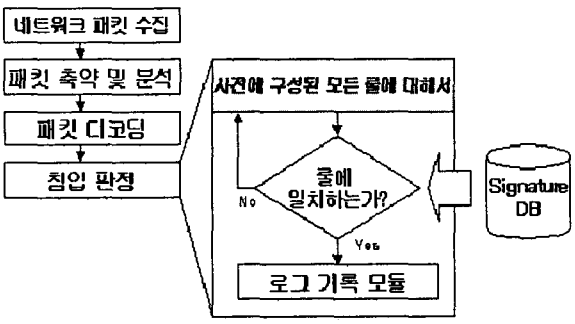
IDS에서 탐지되어 최종적으로 관리자에게 보고 되어지는 경고들 중에는 오탐지 정보들을 많이 포함하고 있다. 이런 오탐지 율이 너무 높으면 IDS의 탐지결과를 신뢰할 수 없으며, 경고간의 상관관계 분석이나 고수준의 의미분석을 할 수 없기 때문에 분석된 결과의 신뢰성이나 효율성 또한 저하된다. 그래서 최근 들어 IDS 연구도 이런 오탐지를 줄이고자 하는 연구 방향으로 많이 진행되어지고 있다[2][3][4].

대표적인 연구로써는 비정상적 탐지 모델 (Anomalous Intrusion Detection)접근 법으로써 통계적인 방법, 특징 추출 방법, Anomaly measures의 결합 방법, 예측 가능

패턴 생성 방법, 신경망을 이용한 방법 등이 있고[7][8] 오용 탐지 모델 (Misuse Intrusion Detection)의 접근 방법에는 조건부 확률 방법, 전문가 시스템 방법, 상태 전이 분석 방법, 키 입력 관찰 방법, 모델 기반 침입탐지 방법, 패턴 매칭 등의 대표적인 방법들이 있다[9][10]. 하지만 이런 연구들의 문제점은 네트워크에서 유입되는 악성패킷을 기준으로 탐지하기 때문에 실질적으로 호스트에 영향을 미치지 않는 공격까지도 심각한 공격으로 보고를 함으로써 관리자나 시스템에게 부담을 주는 단점을 가지고 있다[5][6].

2.1 IDS (Intrusion Detection System) 동작 과정

기존 IDS를 이용한 경보 데이터 처리 구조는 [그림1]과 같다.



[그림 1 기존 IDS의 침입탐지 과정]

침입 탐지 과정을 살펴보면, 먼저 패킷 수집 모듈이 네트워크 상의 데이터를 수집하고 수집된 패킷에 대해 축약 과정과 디코딩 과정을 거치게 된다. 이렇게 패킷 수집 및 분석과정을 거친 데이터는 공격과 연관된 침입 판정 모듈로 이동하게 되는데, 이 과정에서 공격 Signature DB에 있는 침입탐지를 식별할 수 있는 데이터들과 비교 과정을 거쳐 침입 가능성이 있는 데이터에 대한 경보를 발생시킨다. 이로 인해 발생된 경보에 대한 정보를 담고 있는 데이터를 "Alert"라고 한다. 이렇게 발생된 경보 데이터는 로그 기록 모듈로 이동하여 기록되어진다[4].

경보 데이터들을 기록하는 로그에는 방대한 양의 경보 데이터가 기록되며, 이 로그들은 출력 모듈을 통해 관리자에게 보고 되어진다. 그러나 기존의 IDS에서는 이 과정에서 실제 침입과 관련 없는 경보데이터까지 다량으로 관리자에게 제공되므로 IDS 관리자가 침입을 정확하게 분석하고 발생한 침입에 대응하는 것을 어렵게 한다.

2.2 Snort

본 논문에서 사용하는 Snort 툴은 NIDS로 대표적인 오용탐지 기반의 시스템이다[11][12]. Snort의 큰 장점으로는 비교적 구체적인 룰을 사용자가 생성 가능하다는 것과 로그를 사용자가 원하는 여러 가지 형태로 남길 수 있다는 장점 등을 가지고 있다. 하지만 큰 단점으로는 이미 작성되어진 단순한 룰 기반의 패턴 매칭으로 인하여 높은 오탐지의 위험성을 가지고 있다는 단점을 가지고 있다[11].

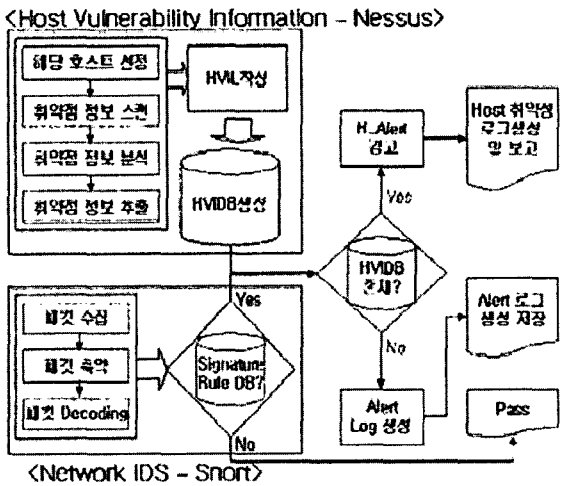
2.3 Nessus

Nessus는 하나의 호스트뿐만 아니라 네트워크 전체를 검사할 수 있어 시스템에 존재하는 취약점을 찾는데 유용한 오픈 소스 툴이다. Nessus는 Plug-in 형식으로 취약점 정보를 추가하여 최신 취약점 존재 여부도 쉽게 검사할 수 있고, GUI 인터페이스를 제공해주기 때문에 매우 편하고 쉽게 해당 호스트의 보안 취약점을 검사할 수 있다[13]. 일반적으로 네트워크 공격 절차는 가장 먼저 공격대상에 대한 정보 수집 단계와 취약점 탐색과정을 거친다. 그 후 수집한 정보를 바탕으로 시스템 침입 단계를 거치게 된다. 이런 네트워크 공격의 절차에서도 볼 수 있듯이 해당 호스트의 취약점을 제공해주는 툴을 이용해 누구보다도 호스트 관리자가 먼저 취약점을 정확히 파악하는 것이 중요하다.

3. 제안 모델

3.1 전체 시스템 흐름

본 논문에서 제안하고자 하고자 하는 시스템의 전체적인 시스템 구조도는 아래 [그림 2]와 같다.



[그림 2 HVIDB를 이용한 침입탐지시스템 구성도]

전제적인 시스템은 크게 주 탐지 시스템으로 오용탐지 기반, NIDS인 Snort 부분과 호스트 기반에서 취약성 분석 자료 생성을 위한 스캔툴인 Nessus의 자료생성 부분으로 나누어 구성된다.

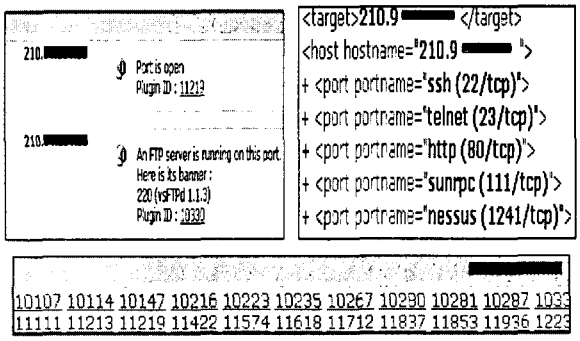
네트워크로부터 유입되는 악성 패킷은 Snort가 가지고 있는 Signature Rule DB와 비교를 하여 일차 탐지가 되고, Nessus를 통해 생성되어진 해당 시스템이 가지고 있는 취약점 리스트(HVIL : Host Vulnerability Information List)를 바탕으로 HVIDB를 구축해 네트워크 기반에서 걸러진 공격 패킷과 호스트 취약점 정보 분석 자료와 비교 과정을 거치게 된다. 이렇게 함으로써 네트워크로부터

들어오는 악성 패킷 중 해당 호스트가 가지고 있는 취약성 정보와 최종 비교 하여 취약성에 관련된 경고만을 관리자에게 보고하게 된다. 그 외에 Snort에서는 탐지가 되었지만 해당 호스트의 취약점 자료에 존재하지 않는 경고는 Alert로그만을 생성하고 저장하게 된다.

3.2. HVIDB 구성

제안 하는 시스템에서 사용하는 HVIDB는 취약점 분석 툴인 Nessus를 이용해서 나온 결과 자료를 바탕으로 취약점 분석에 이용할 정보를 추출한다. 사용하게 될 정보는 해당 호스트의 IP Address, 현재 열려있는 Port정보, 서비스 되고 있는 Protocol, 마지막으로 취약점 분석 툴을 통해 얻은 호스트의 취약성 정보이다. 생성된 취약점 정보는 취약성 이름을 표준화 시키는 CVE(Common Vulnerabilities and Exposure)형식에 맞게 작성되어져서 보고 되어진다.[14].

[그림 3]은 Nessus를 이용하여 얻을 수 있는 해당 호스트의 취약점 정보를 나타낸 그림이다.



[그림 3 Nessus를 이용한 취약점 정보 추출 결과]

그림에서 보듯이 Nessus를 이용하여 취약점을 검사하면 해당 호스트의 IP Address와 현재 열려있는 Port에 관한 정보, 제공되어지고 있는 서비스 프로토콜에 대한 정보를 얻을 수 있다. 이런 정보를 이용하여 [그림 4]와 같이 Snort 규칙에 맞게 DB를 구축하여 전체 시스템에 적용시킬 수 있다.

```
Create Table HVIDB (
        Host IP Address
        Open Port
        Service Protocol
        Host Vulnerability )
```

< 그림 4 호스트 취약점 정보를 이용한 DB 구축>

4. 결론 및 향후 연구과제

NIDS의 경우 일정한 규칙 패턴이나 시스템에 존재하고 있는 시그너쳐 데이터베이스를 두어 탐지하는 형태로 많은 오탐율이 발생하게 된다. 그로 인해서 시스템에 많은 부하를 줄 뿐만 아니라 탐지된 경고 데이터 가운데 실제 침입과 관련된 데이터를 구분해내는 작업에 많은 시간을 소비해 IDS 운용에 있어 비효율적인 면이 많이 생기게 된다.

이에 본 논문에서는 NIDS가 가지고 있는 문제점 중 오탐지율을 감소시키고 관리자의 업무 효율을 향상시키고자 취약점 분석 툴을 이용하여 해당 호스트의 취약점 정보를 수집 분석하고 하나의 데이터베이스 즉, 해당 호스트의 취약점 정보 데이터베이스(HVIDB)를 구축하고, 그 자료를 이용해 네트워크 기반에서 탐지된 공격 패킷이 최종 공격 여부를 판단 받을 때 한 번 더 검사 받게 함으로써 최종적으로 호스트가 가지고 있는 취약점과 관련된 정보만을 관리자에게 보고해주는 시스템을 제안하였다. 특히, 해당 호스트에 남는 오탐율을 감소시키는데 초점을 맞추었다.

향후 연구과제로는 본 논문에서 제시한 기법을 실험을 통하여 검증하는 과정과, 테스트 과정 중에 쓰일 호스트 취약성 조사와 분석과정을 세분화 및 자동화시켜 좀더 호스트에 위험성 있는 패킷을 구분해 내는 시스템에 관한 연구가 필요하다.

5. 참고 문헌

[1]심철준 "침입탐지 시스템에서 Alert의 패턴 학습을 이용한 Flase Positive 감소에 대한 연구", 건국대학교 컴퓨터공학과 2004

[2] PAUL E. PROCTOR, "THE PRACTICAL Intrusion Detection HANDBOOK", pp6~7, 2001

[3]R.G. Bace, Intrusion Detection, Macmillan Technical Pulishing, 2000

[4]B.Mukherjee, T.L. Heberlein and K.L. Levitt, Network Intrusion Detection, IEEE Network, May/June, 1994

[5]Klaus Julisch, "dealing with False Positive in Intrusion Detection"

[6]Yan Qiao, Xie Weixin "A Network IDS with low false positive rate" IEEE,Volume:2,2002

[7]R.Seker, A High-Performance NIDS, ACM 1999

[8]ICSA IDS and Assessment." ICSA Labs, 1999.12

[9]S.Kumar and E.Spafford, "A Pattern Matching Model for Misuse Intrusion Detection," 1994

[10]R.Seker, A High-Performance NIDS, ACM 1999

[11]Martin Roesch,"Snort-Lightweight Intrusion Detection for Network," Proceedings of LISA '99

[12]www.snort.org

[13]www.Nessus.org

[14]http://cve.mitre.org