안전한 포트 스캔 탐지 시스템의 설계 및 구현

강진석[0]· 윤종철[00]· 강흥식[000]
인제대학교 정보컴퓨터 공학부
comdol12@netian.com
pcman95@hanmail.net
hskang@nice.inje.ac.kr

Design and Implementation of Safe Port Scan Detection System

Jin-Suck Kang[0] · Jong Chul Yun[00] · Heung-Seek Kang[000]
Dept of Computer Engineering, Inje University

요 약

오늘날 포트 스캔과 같은 취약점 분석 도구들의 보급 확대로 인해 공공의 호스트나 개인 호스트들의 침입 사례가 증폭되고 있는 실정이다. 더욱이, 포트 스캔의 공격 형태 또한 나날이 그 기법이 지능화와 더불어 서비스 거부 공격을 이용한 시스템 무력화라는 형태로 발전하고 있어 기존의 시스템으로는 탐지와 대응에 어려움이 가중되고 있다. 따라서 본 논문에서는 이러한 지능적이면서 공격적인 포트 스캔에 대응하여 호스트를 효율적으로 유지할 수 있는 안전한 포트 스캔 탐지 시스템을 제안한다. 본 시스템은 기존의 NIDS 탐지 기법과는 달리 IP와 TCP 소켓 정보를 동시에 활용하여 포트 스캔을 이용한 서비스 거부 공격 시에 적절한 대응책으로 동일 IP 주소에 따른 선택적 로그 파일 저장 기법과 해시 알고리즘을 이용한 데이터 저장 기법이라는 제반 사항들을 구현함으로써 현재 대부분의 탐지 시스템들이 간과하고 있는 포트 스캔을 통한 서비스 거부 공격에 대한 일정 수준의 보호를 가능하게 하였다.

1. 서론

최근 인터넷을 통해 공개된 다양한 형태의 포트 스캔 도구들은 해커들에 의해 공격 시스템의 보안 취약점 정보 및 공격 대상을 찾는데 널리 활용되고 있다. 공격자는 이러한 포트 스캔을 통해 실질적인 공격에 앞서 해당 시스템의 취약점을 분석할 수 있고, 동시에 공격이 가장 용이한 부분을 선택적으로 판별할 수 있는 사전 정보를 가질 수 있게 된다. 따라서 현재까지도 포트 스캔이란 해킹이 성공하기 위한 가장 기본적인 필수 과정으로 인식되고 있다. 더구나, 과거에는 포트 스캔이 보안 관리를 목적으로 개발되던 것이 오늘날에는 공격 가능한 취약점을 자동으로 찾아주기 위한 침입을 목적으로 개발되기 때문에 그 위험성이 날로 심각해지고 있는 실정이다. 뿐만 아니라 오늘날의 포트 스캔 도구들은 기본적인 기능을 확장하여 경우에 따라서는 공격 대상 호스트에 탑재되어 있는 침입 탐지 시스템을 무력화시키기 위한 목적으로 서비스 거부 공격의 형태로 발전되어 도달 가능한 공격의 영역을 넓혀 가고 있다. 따라서, 본 논문에서는 리눅스 호스트를 이러한 공격성을 지닌 포트 스캔으로부터 안전하게 유지시키기 위해 IP 패킷과 TCP 패킷을 통합적으로 분석하는 패킷 분석 기법과 탐지 시스템 내부에서 패킷 데이터 저장 시 서비스 거부 공격에 따른 충돌을 고려한 해시 알고리즘을 이용하여 기존 탐지 시스템의 문제점을 해결하였다. 이에 본 논문의 형식은 다음과 같다. 먼저 2장에서는 기존 탐지 시스템들이 발전된 포트 스캔 공격 형태에 효과적으로 대처하지 못하는 문제점들을 짚어보고 3장~5장에서는 본격적으로 본 논문에서 제안하는 안전성을 고려한 탐지시스템의 설계와 구현 방안이 서술된다. 이어서 6장에서는 구현된 본 시스템의 실험 결과를 보인 후 마지막으로 7장에서 결론과 향후 발전 방향에 대해서 언급하고 논문을 맺도록 하겠다.

2. 기존 포트 스캔 탐지 시스템의 문제점

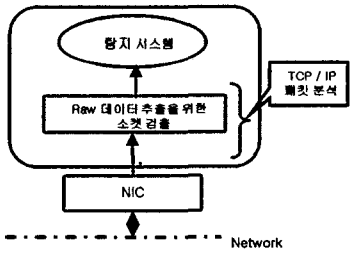
현재 개발되어 있는 포트 스캔 탐지 시스템들은 그 기능 면에서 탐지의 효율성과 편리성을 높이는데 집중하여 개발되어 있는 까닭에 오늘날 탐지 시스템 자체가 공격의 대상이 되는 상황에서는 많은 문제점들을 보이고 있다. 그중 대표적인 것이 탐지 시스템의 무력화인데 이것은 공격자가 탐지 시스템이 100% 탐지 할 수 있는 특정 패킷들을 의도적인 서비스 거부 형태로 보냄으로써 탐지 시스템을 정지시키는 공격이다. 현재 리눅스 환경을 바탕으로 개발된 탐지 시스템 중 대표적인 것은 IP를 등록시켜 운용하는 TCP Wrapper와 탐지 룰을 내장하여 탐지하는 Snort, 그리고 한국정보보호진흥원에서 개발한 RTSD등이 있다. 그러나 이상의 문제점을 근거로 볼 때 먼저 TCP Wrapper의 경우, IP를 미리 등록시켜 동작하기 때문에 지속적인 공개서비스가 필요한 웹서버에서는 효율적이지가 못할 뿐만 아니라 IP 위조에 따른 위험성이 내재되어 있다. Snort는 탐지 룰을 기반으로 다양한 공격과 스캔을 탐지할 수 있는 장점이 있는 반면 침입에 대한 로그가 IP 주소별로 관리되는 까닭에 서비스 거부 공격 시 무제한의 로그 파일 생성이라는 취약점을 지니고 있어 시스템의 안정성에 지장을 초래할 수 있다. 끝으로 RTSD 경우, 스캔 공격을 자동으로 탐지하여 이를

관리자에게 E-mail로 알리는 기능은 그 편리성에서 우수하나 이 또한 의도적인 서비스 거부 공격 시에는 무수한 E-mail 전송이라는 시스템 부하로 이어질 수 있다는 단점을 지니고 있다.

3. 소켓상의 TCP/IP Raw 데이터의 활용

지금까지 개발되어온 대부분의 IDS들은 그 형태가 네트워크를 기반으로 하고 있기 때문에 탐지를 위한 데이터 분석 시 패킷에서 TCP 패킷만을 가져와 분석하였다.

그러나, 이것은 결과적으로 무수한 동일 패킷이 들어오더라도 적절한 조절 없이 무한정 분석을 하게 되는 결과로 인해 상황에 따라서는 의도적인 서비스 거부 공격과 같은 공격에 노출될 수밖에 없었다. 이것은 결국 지금에 이르러 특정 패킷을 정확히 탐지해 낼 수 있는 효과적인 탐지 시스템이 오히려 공격의 목표물이 되는 결과를 낳게 되는 원인으로 작용하게 되었다. 따라서 본 논문에서는 이러한 문제점을 개선하기 위해 [그림 1]과 같이 소켓 상에서 IP와 TCP 패킷을 동시에 분석하는 방법을 제안하고 있다.



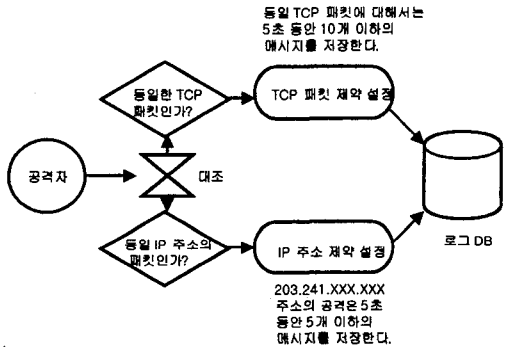
[그림 1] 소켓 분석을 통한 Raw 데이터 분석

이 방법은 IP 패킷 내의 송신측 IP 주소 부분의 정보를 활용함으로써 만일 탐지가 확실히 보장되는 특정 데이터를 짧은 동일 시간대에 무수히 많이 보내는 경우에 있어서, 시스템이 그러한 공격적 상황에 대응되는 TCP 패킷들이 동일 시간대에 동일 IP의 송신측 주소를 가진다는 것을 파악할 수 있게 해준다. 따라서, 이럴 경우에는 즉시 그와 같은 무의미한 데이터들을 즉시 폐기함으로써 탐지 시스템을 보호할 수 있게 되는 것이다.

4. 탐지 시스템 안정성을 위한 선택적 로그 저장 기법

탐지 시스템은 기본적으로 빈번하게 일어나는 모든 이벤트에 관한 정보를 하드디스크나 프린터 등 어느 곳에 기록하던지 로그로써 남기는 것이 필수적이다. 하지만, 시스템이 가지고 있는 자원의 공간은 한정되어 있을 수밖에 없다. 결국, 이것은 로그 정보를 기록할 수 있는 저장 공간이 없을 경우에는 결과를 잃어버리거나 그로 인해 시스템이 정지해 버리게 됨을 뜻한다.

오늘날, 해커들은 이러한 문제점들을 잘 알고 있을 뿐만 아니라 취약점으로 적극 활용하고 있기에 해커들 중에는 이렇게 로그 정보를 남기지 않게 하기 위해 무수히 많은 프로세스를 발생시키는 서비스 거부 공격과 같은 해킹을 시도하는 경우가 빈번하다. 그 중에서도 짧은 시간에 적은 노력으로 가장 높은 효과를 볼 수 있는 공격은 단연 무수히 많은 패킷들을 보내는 것이다. 따라서, 대부분 이런 경우 로그 데이터 저장을 중지하던지, 아니면 오래된 결과 데이터를 새로운 데이터로 바꾸는 작업이 필수적이다. 하지만, 실시간으로 공격이 이루어지는 상황에서 한정된 시스템으로 이러한 작업을 효율적으로 운용하는 것은 결코 쉬운 일이 아니다. 까닭에, 본 논문에서는 이 문제점에 대한 한가지 해결책으로 약간의 제약 사항을 두고자 한다. 바로 그러한 형태가 [그림 2]와 같이 공격 형태와 발신지 주소에 따른 일정 수준의 조건에 따라서 로그 정보를 기록하는 것이다.



[그림 2] 조건별 로그 정보의 저장

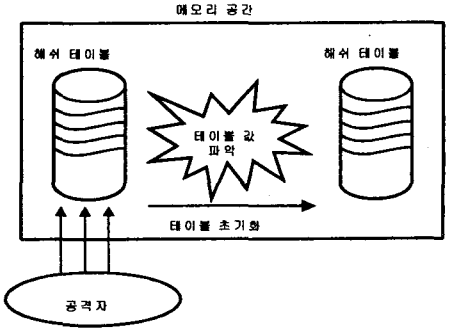
다시 말해, 짧은 동일 시간대에서 발생하는 발신지 주소는 다르지만 무수한 "동일한 형태의 TCP 패킷에 대해서는 몇 초 동안에 몇 개 이하의 메시지를 저장하라"고 설정하게 되면 동일 패킷이 아무리 들어오더라도 그에 대한 로그 데이터의 저장은 한정된 범위에서 이루어져 결과적으로 시스템 자원을 보호할 수 있게 되는 것이다.

물론, IP 패킷에 관한 조건으로는 같은 상황에서 TCP 패킷 형태는 다를지라도 " IP 패킷 내의 동일 주소를 가진 패킷들은 몇 초 동안에 몇 개 이하의 메시지를 저장한다"라는 식으로 대처가 이루어지게 된다.

5. 충돌을 고려한 해시 알고리즘의 설계

본 논문에서 제안하는 포트 스캔 탐지 시스템에서는 패킷 분석을 위해 여러 패킷 데이터들을 소트하고 자료를 찾는 알고리즘으로 특정 경우에 최적화를 고려하여 해시 알고리즘을 활용하였다. 여기서 특정 경우란 지금까지의 설명에서와 같은 공격자가 탐지가 용이한 패킷만을 가지고 서비스 거부 공격을 가할 경우를 말한다. 따라서, 본 논문에서 제안하는 탐지 시스템은 발신지 주소 데이터를 쉽게 찾기 위해 평균적으로 데이터를 찾는 시간이 이진 탐색보다 빠른 해시 테이블을 사용하였다. 그

러나, 탐지 시스템의 안전성을 위해서는 최악의 경우를 항상 고려해야 할 필요성이 있다. 즉, 공격자는 오히려 이러한 해시 테이블의 특성을 역이용하여 해시 충돌을 일으키기 위한 목적으로 자신의 발신지 주소를 인위적으로 선별하여 대량으로 보낼 수 있다. 이것은 탐지 시스템에 있어서는 치명적일 수밖에 없다. 더구나 탐지 시스템이 서비스 거부 공격을 통한 쓸모 없는 데이터를 많이 가지고 있게 될수록 시스템의 부하는 높아지고 결과적으로 다른 프로세스들이 CPU를 사용할 시간이 줄어드는 결과를 낳게 된다 따라서 본 논문에서는 이 문제를 [그림 3]과 같이 해시 충돌 횟수를 제한함으로써 해결하였다.

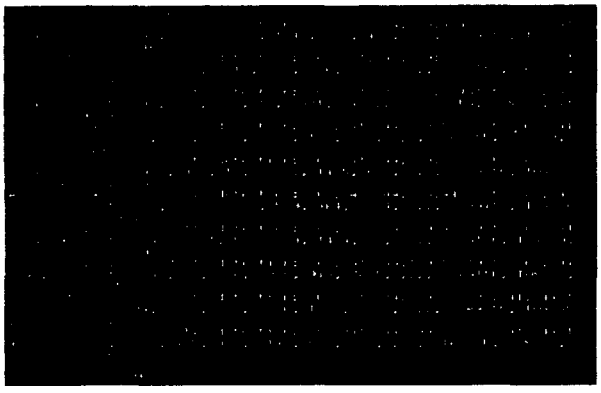


[그림 3] 충돌을 고려한 해시 알고리즘

즉, 해시 테이블이 제약 사항에 도달했을 경우 오래된 같은 해시 값에 대한 데이터를 버리는 방식을 택한 것이다. 결과적으로 이 개선 사항 역시나 TCP/IP 패킷을 이용한 일차적 시스템 보호 방안과 마찬가지로 메모리 공간상에서 패킷 데이터 저장 시 일어날 수 있는 충돌 과정으로 인한 시스템 위협 요소들을 고려한 조치인 것이다.

6. 실 험

제안된 시스템은 리눅스 환경에서 C로 구현하였으며 패킷 캡쳐를 위해 시스템 독립적이고 이식성이 뛰어난 libpcap 모듈을 적용하였다. [그림 4]는 본 시스템이 실제로 포트 스캔 도구로 가장 많이 활용되는 nmap을 연속적으로 수행했을 때의 탐지 결과를 보여주는 그림이다.



[그림 4] 탐지 시스템의 결과 화면

[그림 4]에서 알 수 있듯이 본 시스템은 연속적인 공격 시 일정 수준까지는 탐지 결과 화면을 로그 파일 형식으로 모니터에 보이지만, 서비스 거부 공격으로 간주될 정도로 짧은 시간 동일 IP에서 지속적인 공격이 이어질 경우에는 더 이상 패킷을 메모리 상에 남기지 않고 동시에 로그 파일도 생성하지 않는 것을 알 수 있다. 이로써 본 시스템은 기존 시스템과는 달리 공격적 의도를 가진 연속적 패킷에 대해 시스템의 안정성을 나타내고 있음을 알 수 있다.

7. 결론 및 향후 방향

본 연구에서는 기존에 개발되어 있는 탐지 시스템들이 서비스 거부 공격에 따른 탐지 시스템 자체가 공격 목표가 되었을 경우 이에 적절하게 대응하지 못한다는 결론에 비추어 이를 해결하고자 좀 더 안전하게 유지시킬 수 있는 시스템을 제안하였다. 본 논문에서 제안하는 시스템은 실험 결과를 토대로 볼 때 기존의 시스템과는 구별되는 안전성이라는 면에서 일정 수준의 효과를 보장하고 있다. 이 결과는 지금까지의 탐지 시스템들이 보안이라는 목표에 접근하기 위한 최선의 방법으로 탐지율의 향상과 로그 파일의 실시간 확보라는 중요성에만 취중 했던 점들로 인해 파생되고 있는 보안의 허점을 부각시키고 아울러 탐지 시스템의 안정성 확보라는 측면에서 그 해결 방안을 보여 주고 있는 것이라 할 수 있다. 그러나 본 시스템은 그 운용 범위가 단일 로컬 상의 개인 호스트로 지정되어 있는 한계점과 안전성에만 편중되어 대응에는 미흡한 부분을 드러내고 있다. 따라서 향후에서는 분산 네트워크 망에서 다양한 경로를 통해 들어오는 포트 스캔 패킷들을 효과적이고 신속하게 분석하기 위한 알고리즘의 개선과 로그 저장과 더불어 탐지 시스템의 안전성 유지와 공격자 차단이라는 적극적 대응 수단에 대한 연구를 추진해 나갈 예정이다.

참고 문헌

[1] 김선숙, 오시형 역, "TCP/IP 시큐리티 실험", 성안당, 2001
[2] 박종서, "정보보안전문가 시스템 보안", 이에듀닷컴, 2001
[3] Martin Roesch, "Snort-Lightweight Intrusion Detection for Networks", Phrack Magazine Vol.8
[4] Http://www.microsoft.com/technet/security/intel.asp
[5] Chrostppher Klaus, "Stealth Scanning-Bypassing Firewalls/SATAN Detectors", 2000
[6] Stephen Northcutt, Judy Novak "Network Intrusion Detection An Analyst's Handbook"
[7] 이현우, 이상엽, 정현철, 정윤종, 임채호, "Analysis of Large Scale Network Vulnerability Scan Attacks and Implementation of the Scan-Detection tool", 1999