취약점 진단 스크립트를 이용한 보안도구 우회공격 탐지 시스템 설계

박명호, 육상조, 이 극
한남대학교 컴퓨터공학과

Design of Detection System against Security Tool Evasion Attack using a VDS(Vulnerability diagnostication Script)

Myung-Ho Park, Sang-Jo Youk, Geuk Lee
Dept. of Computer Engineering, Hannam University

요 약

최근에 침입 탐지 시스템은 네트워크 보안의 강화를 위해서 방화벽과 침입탐지 시스템 상호간의 연동으로 침입자의 연결 상태를 차단하는 방법도 개발되었다. 하지만 방화벽뿐만 아니라 침입탐지 시스템도 공격자에 의한 우회공격에 대해서는 아직 상당부분 방어할 수 없다. 또한 우회공격 탐지 모듈도 기존의 IDS와 Rule의 중복이 불가피하다, 본 논문은 취약점 진단 스크립트를 통해 IDS의 취약점 진단 후 IDS우회탐자공격 시스템의 Rule을 최적화 하여 우회공격을 효율적으로 탐지 해내는 시스템을 제안한다.

1. 서론

최근에 침입 탐지 시스템은 네트워크 보안의 강화를 위해서 방화벽과 침입탐지 시스템 상호간의 연동으로 침입자의 연결 상태를 차단하는 방법도 개발되었다. 하지만 방화벽뿐만 아니라 침입탐지 시스템도 공격자에 의한 우회공격에 대해서는 아직 상당부분 방어할 수 없다. 침입탐지시스템은 크게 다음과 같은 두.가지의 문제점을 가지고 있다. 네트워크 상에 흐르는 패킷을 완전히 감지해 내지 못한다. 일반적으로 침입탐지시스템은 통신망에 흐르는 패킷을 캡처해서 침입인지, 아닌지를 먼저 확인하게 된다. 즉 캡처 된 패킷을 침입탐지 시스템의 데이터베이스와 비교하여 특정한 패턴의 패킷이 캡처되면 침입으로 간주하게 되는 것이다. 그러나 패킷 크기가 아주 작거나 부하 집중 시 침입탐지시스템의 패킷 캡쳐율은 내우 낮아진다. 둘째 악의적인 목적을 가지고 침입탐지시스템을 우회 공격하는 해킹기법에 대한 방어 기법을 가지고 있지 않다. 침입탐지시스템을 우회하기 위한 공격 기법으로 네트워크상의 정보 교환 시 IP 패킷을 몇 개의 작은 패킷으로 나누어서 전송되고 목적지 시스템에서 재 조합되는 것을 이용한 IP fragmentation 기법이 있다. Fragrouter, Whisker, IDSWakeup 등과 같은 공격툴 들은 IP fragmentation 기법을 이용한 침입탐지시스템 우회 공격 도구이다.[1]

이와 같은 현재 침입탐지시스템이 가지는 문제점은 정보보호를 위해 설치한 침입탐지시스템의 존재 의미를 무색하게 하여 목적지 시스템을 파괴하고 정보를 유출하는 등의 막대한 피해를 입힐 수 있다. 국내 침입탐지시스템의 수준은 과거보다는 많은 발전은 있지만 침입탐지시스템 우회 공격에 대해서 아직도 많은 연구가 필요하다.

본 논문에서는 취약점 진단 스크립트를 이용하여 침입탐지 우회공격을 탐지할 수 있는 시스템을 설계 및 개발한다. 취약점 진단 스크립트를 이용한 IDS 우

회공격 모델을 설계하기 위하여 2장에서 침입탐지 시스템 그리고 3장에서는 취약점 진단 스크립트를 이용한 IDS 우회공격 탐지시스템 모델을 제안하기 위한 취약점 분석의 평가 절차에 대해서 설명하고, 4장에서는 취약점 진단 스크립트를 이용한 IDS 우회공격 탐지 시스템 모델을 제안하고 설계한다. 마지막으로 5장에서 결론 및 향후연구로 끝을 맺는다.

2. 침입탐지 시스템

IDS는 Intrusion Detection System(침입탐지시스템)의 약자로, 단순한 접근 제어 기능을 넘어서 침입의 패턴 데이터베이스와 Expert System을 사용해 네트워크나 시스템의 사용을 실시간 모니터링하고 침입을 탐지하는 보안 시스템이다. 또한 IDS는 허가되지 않은 사용자로부터 접속, 정보의 조작, 오용, 남용 등 컴퓨터 시스템 또는 네트워크 상에서 시도됐거나 진행중인 불법적인 예방에 실패한 경우 취할 수 있는 방법으로 의심스러운 행위를 감시하여 가능한 침입자를 조기에 발견하고 실시간 처리를 목적으로 하는 시스템이다.

침입이란 시스템에 대한 고의적 불법적인 행위를 말하며 시스템의 불법침입, 중요정보의 유출 및 변경, 훼손, 불법적인 사용, 그리고 컴퓨터 바이러스 및 서비스거부 등과 같은 구체적인 형태로 나타난다. 침입탐지시스템은 이러한 불법적인 침입행위를 신속하게 감지하고 대응하는 소프트웨어를 말하며 간단하게는 로그파일분석에서부터 복잡한 실시간 침입탐지시스템까지 다양한 소프트웨어가 존재한다. 침입탐지 기법은 크게 비정상적인 침입탐지 기법과 오용침입탐지 기법으로 나눌 수 있다.[5]

침입탐지 시스템은 침입 탐지를 하는 데이터 소스에 따라 호스트 기반 침입탐지 시스템과 침입탐지 시스템 그리고 네트워크 기반 침입탐지 시스템으로 구분된다. 침입 탐지의 모델에 따라서 오용(Misuse)탐지 시스템과 변칙(anomaly) 탐지 시스템으로 구분된다.

2.1 데이터 소스기반의 침입탐지 시스템

침입탐지 시스템은 침입 탐지를 하는 데이터 소스에 따라 호스트 기반 침입탐지 시스템과 네트워크 기반 침입탐지 시스템으로 구분된다.

(1) 호스트 기반 침입 탐지 시스템

호스트기반의 침입탐지시스템은 개별 컴퓨터 상에서 클라이언트를 실행하고, 개별 컴퓨터별로 공격을 감지하도록 돼 있다. 호스트기반의 침입탐지시스템이 가진 문제점은 보호하려는 모든 시스템 내에 설치해야 한다는 것이다. 그러면 각 호스트의 운영체제와 프로토콜 스택을 수정할 수도 있다. 만약 수정하게 되면 운영체제가 업그레이드될 때 다시 운영체제가 깨질 수 있기 때문에 문제가 될 수 있다.

(2) 네트웍 기반 침입 탐지 시스템

네트워크 기반의 침입탐지 시스템들은 통상 전 네트워크 세그먼트를 감시하는 전용의 시스템들이다. 대부분의 경우 Firewall 외부 네트워크 세그먼트나 내부의 주요 네트워크 세그먼트에 설치한다. 네트워크 기반의 IDS는 네트워크 상에 흘러다니는 모든 패킷들을 검사하여 알려진 공격들이나 의심스러운 행동에 대하여 분석하게 된다.

2.2 침입 탐지 모델 기반의 침입 탐지

침입탐지 시스템 탐지 방법은 은 침입 탐지 모델 기반에 따라 비정상 침입 탐지 방법과 부정사용 침입 탐지 방법으로 분류할 수 있다.[10]

(1) 비정상 침입 탐지 방법

비정상 탐지 모델은 주로 학계나 연구소에서 주로 연구되고 있는 방식으로 정상적인 사용자의 조작 또는 시스템의 예상되는 행위에 대한 정보를 이용하여 시스템의 동작이 이를 벗어나는 정보를 이용하여 탐지를 한다. 비정상 탐지 모델은 이를 위하여 통계적인 방법을 주로 이용하므로 통계기반 탐지 (Statistical-based Intrusion Detection)라고도 한다.

(2) 부정사용 침입 탐지 방법

시스템의 알려진 취약점들을 이용하여 공격하는 행위들을 사전에 공격에 대한 특징 정보를 가지고 있다가 탐지하는 방법으로, 시스템 감사기록 정보에 대한 의존도가 높고 상대적으로 구현 비용이 저렴하다. 그러나, 알려진 공격기법에 대한 탐지능력만을 가지고 있기 때문에 최신 공격기법에 대한 계속적인 연구가 필요하다.

3. VDS를 이용한 IDS우회공격탐지시스템 설계

3.1 시스템 구성 및 설계

(1) 취약점 진단 스크립트

취약점 진단 스크립트는 위험기반 분석 프로세스를

기반으로 만들어져있다. 자산 분석대신에 시스템에 가장 위험도가 높은 공격들을 'alert' 중간의 위험을 갖는 공격들을 'log' 기타 우회공격들을 'Pass'로 분류하였다. 우회공격을 테스팅 하기 위하여 스크립트의 위험도를 설정하여 구동 후 기존의 IDS의 우회공격 취약점을 분석하게된다.

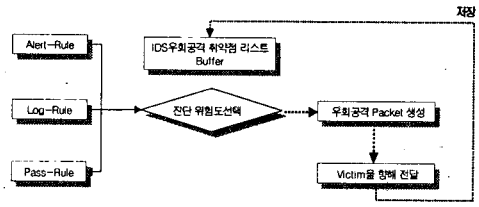

그림 1. 취약점 진단 스크립트 구성도

취약점 진단 스크립트는 3개의 Rule로 구성이 되어진다. Alert,Log,Pass가 그것이다. 처음 취약점 진단을 위해 룰 타입을 선택하고 그 Rule에 맞추어 패킷을 Libnet 또는 Raw-Socket을 이용하여 조립하게 된다.

다음은 취약점 진단 스크립트의 처리과정을 도식화한 것이다.

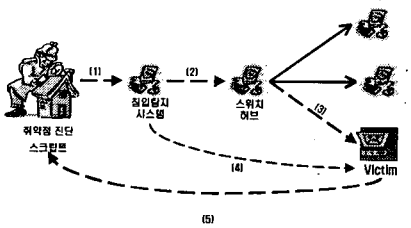

그림 2. 취약점 진단 스크립트 처리과정

취약점 진단 스크립트에서의 처리과정은 스크립트가 가지고 있는 위험기반 Rule인 'alert' 또는 'log' 또는 'Pass'유형의 우회공격 타입을 설정 후 구동을 하게된다. 해당하는 위험도를 가진 공격이 Victim호스트에 행해지게 된다. [1]번과정 에서는 패킷의 공격 위험도에 따른 공격이 시행되어 기존의 침입탐지 시스템을 거치는 과정을 보여준다. 여기서 침입탐지 시스템은 취약점 진단 스크립트에서 만들어진 패킷에 대해 대비를 하게된다. 상용으로 나오는 IDS는 기본적인 우회탐지 기능이 있으므로 Fragmentation과 같은 공격에 대해서는 탐지 해낼 것이다. 하지만 그 외의 최신 공격유형에 대해서는 탐지를 하지 못하고 [2]번 과정 스위치허브를 거쳐서 [3]번 과정인 목적지인 Victim호스트에 패킷을 전달하게 된다. Victim호스트에 도착한 위험도 있는 패킷들은 기록되어지게된다. [4]번 과정에서 침입탐지 시스템은 몇몇의 우회공격 패킷들을 탐지한 결과를 Victim에게 보내주어서 실제로 기존의 IDS가 탐지하지 못하고 우회된 공격이 어떤 것인가를 검사 하게된다. 실제 기존의 IDS에서 탐지 못한 우회공격 리스트들이 다시 취약점 진단 스크립트에 전달이 되어 취약점 진단스크립트는 기존의 IDS가 취약한 공격 리스트를 얻게되어 이 취약점을 파일형태로 저장하게 된다.

(2)IDS우회공격 탐지 시스템

IDS우회공격 탐지 시스템은 취약점진단 스크립트에서 얻은 기존의 IDS 의 우회공격에 대한 취약점 정보를 이용해서 탐지를 하게된다. 처리과정은 그림과 같다.

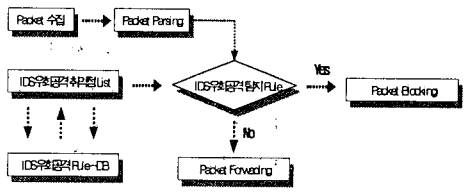

그림 3. IDS우회공격 탐지 시스템 흐름도

패킷수집 모듈은 Libpcap을 이용해서 패킷의 정보를 분석하게된다. LAN의 형태에 따라 Enternet 10BaseT 또는 IPX망을 검사하게 된다. 그리고 Ethernet헤더,IP헤더,TCP 또는 UDP헤더 정보를 파싱하여 Rule구조체 담고 유지하게 된다.

3.2 전체 구성도

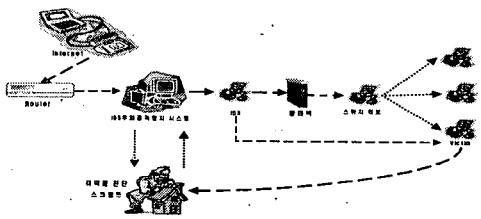

그림 4. 전체 구성도

먼저 취약점 진단 스크립트에서 생성한 공격 패킷을 IDS를 통과 시켜 스위치 환경에 하에 있는 Victim 호스트에 전달하게 된다. 물론 이때 IDS우회공격 탐지 시스템은 구동하지 않는다. 그후 IDS탐지 해낸 공격과 그렇지 않은 공격 유형을 Victim호스트가 IDS에게 자료를 받아 정리하게된다., 그런 후에 Victim호스트는 취약점 정보를 IDS우회공격 탐지 시스템에 전달하게 된다. 그러면 그 정보를 토대로 IDS우회공격 탐지 시스템은 실제 탐지 할 룰을 재조립하고 글 Rule에 맞추어 IDS우회공격을 탐지 및 Blocking 해내게 되는 것이다. 이렇게 함으로써 실제 IDS와 IDS우회공격 탐지 시스템상의 탐지 Rule의 중복을 없애서 효율적이고 빠른 탐지가 이루어지게 된다. 또한 기존의 여러 플랫폼에 영향을 받지 않고 IDS우회공격 탐지 시스템을 사용할 수 있는 장점을 또한 가지게 된다.

4. 결론 및 향후 연구과제

현재 인터넷의 표준 프로토콜인 TCP/IP는 보안을 고려하여 프로토콜로 설계되지 않았기 때문에 구조상 취약점을 가지고 있고 운영체제 또한 비 상업용부터 상업용 운영체제에 이르기까지 모든 운영체제가 자체의 취약성을 가지고 있다. 이런 취약성에 대한 공격에 탐지를 위한 NIDS가 개발되어져 있으나 우회공격에 취약하다. [1]

현재 국내외적으로 여러 종류의 침입탐지시스템이 개발되어 있다. 이들은 침입을 정보 접근, 정보 조작, 시스템 무기력 화 등에 대한 고의적이면서도 불법적인 시도의 잠재 가능성으로 정의하고 시스템 또는 전산망 침입탐지 연구 필요성의 인식과 함께 지속적인 발전을 이루어 왔다. 그러나 침입탐지시스템의 발전에 따라 이를 우회 공격하는 기법도 날로 증가되고 지능적으로 되어 가는 문제를 항상 안고 있는 실정이다. . 이에 본 논문에서는 NIDS의 단점은 IDS우회공격에 대한 탐지를 가능하게 하는 우회공격 탐지 시스템과 취약점진단을 통해 기존의 IDS와 호환성을 극대화하고 Rule의 검사의 중복을 없앤 시스템의 설계 및 구현하였다. 또한 타 침입탐지 우회공격 시스템에 비해 탐지시간의 감소를 입증하였고 플랫폼 독립적인 시스템의 개발을 이루게 되었다.

향후연구 과제는 위험기반으로 취약점을 분류하는 것에 대한 표준화가 필요하며 최대한 실시간으로 패킷을 블로킹 해내는 기술이 필요하다. 또한 IDS우회공격 탐지 시스템에서 포워딩 시 패킷 재조립과정에 대한 Delay를 줄이는 것이 관건이다. 방화벽수준만큼의 실시간 블로킹이 이루어져야한다. 또한 계속 변화하는 IDS,우회공격 기술에 대해서 따라가기 위해 CVE(Common Vulnerabilities and Exposures)와 연동하여 취약성 DB를 유지 및 이용하는 시스템을 구축하는 것이 향후 과제이다.

[참고문헌]

[1]"Stephen Judy" 네트워크 침입탐지 시스템과 해킹 분석 핸드북 2000, 인포북

[2] 박정호 외, "호스트기반 침입탐지 시스템 개발에 관한 연구", 한국정보보호센터, 12., 1998.

[3] Vern Paxson, "Bro:A System for Detecting Network Intruders in Real-time", Lawrence Berkeley Natinal Laboratory, January., 1998, LBNL-41197

[4] Steven McCanne, Van Jacobson, "The BSD Packet Filter; A New Architecture for User-level Packet Capture", December 19, 1992

[5] Fred Cohen, "50 ways to Defeat Your Intrusion Detection System"
http://all.net/

[6] Brad Sanford, "IP Fragmentation and Fragrouter",
http://www.sans.org/infosecFAQ/encryption/IP_frag.html, 2000

[7] 최용락 외 3인 "통신망 정보 보호", 1997, 도서출판 그린

[8] Steve Schupp "Limitation of Network Intrusion Detection",December 1, 2000., - http://www.sans.org

[9] D.E. Denning, "An Intrusion-Detection Model", IEEE Trans on Software Engineering, No. 2, Feb., 1998.

[10] M. Esmaili, R. Safavi-Naini, and J. Pieprzyk, "Intrusion Detection: a Survey", ICCC '95, PP409-414.

[11] T.F. Lunt, "A Survery of Intrusion Detection Techniques", Computer & Security", Vol. 12, No. 4, Jun., 1993.

국문 : 본 연구는 한국과학재단 지역협력연구센터(R12-2003-004-02000-0)지원으로 수행되었음

영문 : This work was supported by a grant No.(R12-2003-004-02000-0) from Korea Science & Engineering Foundation