NT서버 실시간 접근 감시 시스템의 설계 및 구현

박정진*, 박진섭*, 김황래,** 오송석***
*대전대학교 컴퓨터정보통신공학부
**국립천안공업대학 컴퓨터과
***건양대학교 교양학부

Design and Implementation of NT-Server Real-Time Access Monitoring System

Jung-Jin Park*, Jin-Sub Park*. Hwang-Rae Kim**, Song-Seuk, Oh***
* Dept. of Computer and Communications Engineering, Daejeon University
**Dept. of Computer Engineering, Cheonan Nat'l Technical College
***Dept. of Liberal Arts, Konyang University
E-mail : jjpark@zeus.dju.ac.kr, jspark@dju.ac.kr

요 약

본 논문에서는 NT 서버가 제공하는 서비스에서 발생하는 이벤트와 서비스를 실시간으로 감시하고 보고하는 접근 감시시스템을 설계하였다. 서버시스템으로 들어오는 패킷을 분석하고, 웹서버에 남겨지는 로그, 레지스트리 정보, 네트워크 연결 세션 정보를 통하여 불법적인 접근이 발생했는지를 분석한다. 또한 그로 인한 피해가 발생했을 경우 시스템의 어느 서비스에서 불법적인 접근이 발생했고, 어떠한 피해가 발생했는지를 분석하여 신속하고 정확한 대응을 할 수 있도록 정보를 제공한다.

1. 서론

정보 산업의 급속한 성장으로 인하여 컴퓨터 시스템의 사용과 인터넷의 이용이 폭발적으로 증가하였다. 또한 H/W와 S/W의 성능향상으로 인하여 기존의 유닉스 서버시스템이 주로 이용되던 서버로 NT를 기반으로 하는 시스템의 운영이 증가하는 추세에 있다. 이러한 환경 변화에 따라 불법적인 접근으로 인한 피해의 가능성이 증가하게 되고 NT를 기반으로 하는 서버 시스템에 대한 보호가 중요한 관점으로 떠오르게 되었다.

네트워크 환경에서의 불법 접근은 정보 자산에 대한 피해를 초래하기 때문에 이러한 침입 행위는 체계적이고 정형화된 분석 방법에 의해 불법 침입 여부를 결정하는 것이 가장 효과적인 방법임에도 불구하고, 끊임없는 해킹 기법의 출현과 다양한 접근 방법 때문에 대부분의 정보시스템 관리자들이 불법적인 접근에 대한 효과적인 탐지와 분석을 하지 못하고 있다.

본 논문에서는 불법 접근의 결과에 대한 분석을 위하여 NT서버시스템의 패킷 감시, 웹 로그, 레지스트리 정보, 네트워크 연결 세션 등을 분석하는 기법에 대해서 논의한다.

2. 침입 시도 기법

2.1 확장 유니코드 문자를 이용한 시스템 내부 명령 실행

Windows NT/2000 시스템에서 IIS 웹서비스를 하는 경우에 "/"나 "\" 대신에 이에 대응되는 "확장 유니코드 문자"를 사용할 경우 서버 내에서 "../" 디렉토리와 관련된 어떤 명령어를 실행시킬 수 있는 버그가 존재한다.

http://hostname/scripts/..%c1%1c../winnt/system32/c

md.exe?/c+dir+"c:\"와 같은 URL을 웹브라우저의 Location 난에 위와 같이 요구하면 c:\ 안에서 dir를 입력한 결과를 웹브라우저를 통해 볼 수 있다. 또한 del과 같은 명령으로 파일을 삭제할 수 있다.

2.2 IIS 5.0의 원격 버퍼오버플로우 취약점

Windows 2000 Internet printing ISAPI는 사용자 요청을 처리하는 msw3prt.dll를 포함한다. msw3prt.dll에서 버퍼를 체크하지 않기 때문에 고의적으로 HTTP .print의 'Host' 필드에 대략 420바이트를 포함하여 요청하면 임의의 코드가 실행될 수 있다.

3. 관련 연구

3.1 패킷 모니터링

패킷 모니터링(Packet Monitoring)은 네트워크 상에서 흘러 다니는 패킷을 수집하여 분석할 수 있도록 하는 일련의 작업을 말하며, 이러한 모니터링을 하기 위해서는 Libcap, Wpcap, RawSocket, NDIS(Network Driver Interface Specification)등을 사용한다. NIC를 통해서 시스템으로 유입되고 유출되는 패킷 정보를 수집하여 네트워크를 통한 침입을 분석하기 위한 정보로 이용한다.

3.2 레지스트리(Registry)

레지스트리는 운영체제에서 부팅시 필요한 정보 및 시스템의 설정에 관한 정보를 한곳에 저장하기 위한 장소이다. 레지스트리 설정 값의 종류에는 시스템에 설치된 하드웨어 정보, 응용프로그램 정보, 사용자 계정 설정 정보, 시스템에 관련된 각종 서비스 툴, 시스템에 설치된 네트워크 프로토콜 정보 등이 있다.

3.2.1 레지스트리의 구조

▶ 레지스트리 서브 트리

서브 트리	역 할
HKEY_CLASS_ROOT	정보파일들을 응용프로그램과 연결시켜줌
HKEY_CURRENT_USER	로그 온 사용자에 대한 프로필 정보
HKEY_LOCAL_MACHINE	시스템의 모든 정보를 가지고 있는 장소
HKEY_USERS	현 시스템에 로그온하여 활성화되어 있는 사용자들의 프로필정보
HKEY_CURRENT_CONFIG	현 시스템의 하드웨어 정보 프로필과 소프트웨어 프로필을 가지고 있는 곳

3.3 웹 로그

웹과 관련된 로그는 기본적으로 웹 로그는 Windows 2000 서버의 경우에는 11개의 필드, Windows NT 서버의 경우에는 16개의 필드, 그리고 FTP 로그의 경우에 Windows 2000 서버는 5개의 필드, Windows NT 서버의 경우는 웹 로그와 같은 16개의 필드로 구성되어 있다.

3.4 네트워크 연결 세션

일반적으로 시스템이 사용하는 포트가 아닌 다른 열려진 포트를 확인하기 위하여 연결된 세션을 확인한다. 연결 세션을 확인하기 중요한 연결 상태를 보면 다음과 같다.

▶LISTEN
포트가 열려져, 연결 요청을 기다리는 상태이다.

▶SYN-SENT
로컬 시스템의 클라이언트 어플리케이션이 원격 호스트에 능동적인 개설을 요청한다.
TCP는 Synchronize flag를 설정한 시작 세그먼트를 전송하며, 원격 시스템도 역시 Synchronize flag를 설정한 시작 세그먼트로 응답할 것을 기다린다.

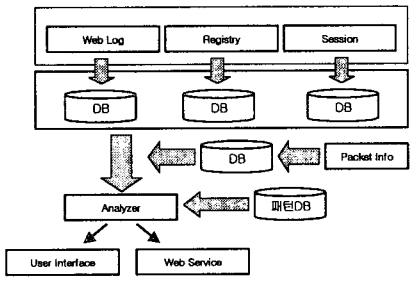
▶ESTABLISHED
가상회선이 작동. 3단계 핸드쉐이킹 과정이 완료되면 두 시스템은 이 상태에 들어간다.

▶CLOSED
아무 일도 발생하지 않음. 회선은 종결되었고, TCP는 가상회선에 사용하였던 모든 자원을 놓는다.

4. 도구의 구현 결과 및 분석

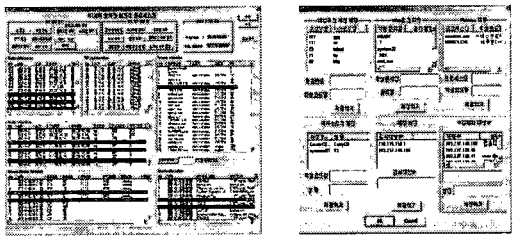
[그림 1]은 NT서버 실시간 이벤트 감시시스템의 전

체적인 흐름을 나타낸다. 정보를 수집하는 모듈들을 통해서 수집한 정보를 데이터베이스에 저장하고 축약한다. 저장된 정보를 분석모듈을 통하여 패턴을 적용하고 관리자에게 분석정보를 제공한다.



[그림 1] 전체 구조

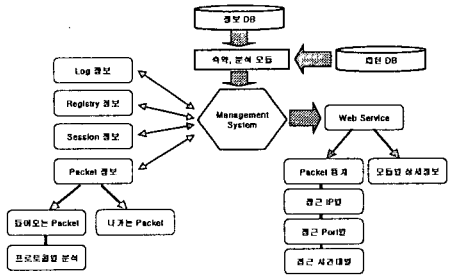
[그림 2]를 통하여 불법적인 접근에 대한 전체적인 상황을 파악할 수 있다. 업데이트되는 정보를 확인함으로써 어떠한 침입이 이루어졌는지를 확인한다. 불법적인 접근 패턴과 일치하면 표시를 하도록 하였다.



[그림 2] 시스템 주화면과 패턴

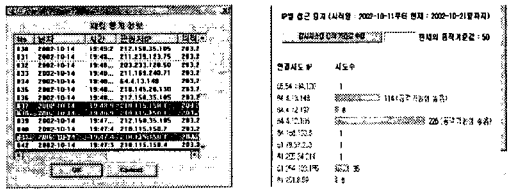
NT서버 실시간 이벤트 감시시스템을 동작시키기 위하여 우선적으로, 패킷 모니터링을 시작한다. 수집된 패킷의 분석을 통하여 서버시스템으로의 데이터 유입과 유출을 판별하여 이상 징후로 판단 시에 감시시스템을 동작시킨다.

침입에 대한 패턴적용은 네트워크 연결 모듈에 대해서는 백도어나 악성 프로그램이 사용하는 포트를 적용하고, 웹 로그는 접근을 시도하려는 페이지와 쿼리의 실행과 성공여부, 레지스트리 패턴은 시스템에 악성 프로그램이 설치되어있는지 확인한다. 그리고, 패킷에 관한 패턴은 이전 분석 정보를 바탕으로 특정 감시대상 IP를 관리하고, 수집대상에서 제외할 IP를 등록하여 수집데이터의 양을 축약하도록 한다. 모든 패턴 정보는 데이터베이스화하여 체계적으로 관리된다.



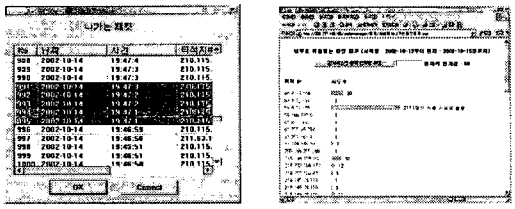
[그림 3] 시스템 흐름도

[그림 4]는 서버시스템으로 유입되는 패킷을 분석하여 어느 IP에서 몇 번의 접근 시도가 발생했는지를 통계적인 그래프를 통하여 확인한다. 특정 IP로부터 접근 시도를 감시함으로써 해당 IP들에 대한 접근 제어를 효과적으로 할 수 있다.



[그림 4] 유입되는 패킷 정보

[그림 5]는 서버 시스템으로부터 패킷이 어느 IP로 이동하는지에 대한 통계 정보를 보여주고 있다. 주요 감시대상 IP가 접근을 했을 경우에는 다른 색으로 표시되고 있다.



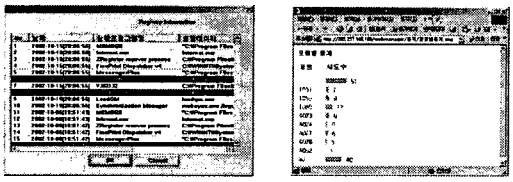
[그림 5] 유출되는 패킷 정보

서버 시스템으로부터 유입되고 유출되는 패킷의 양에 이상이 발생 시, 시스템에 정보를 유출하는 백도어나 트로이잔 또는 다른 시스템으로 공격을 발생시키는 악성 프로그램이 존재하는지를 판단하기 위해 레지스트리 정보를 분석한다.

[그림 6]을 통하여 악성 프로그램의 존재 유무를 확

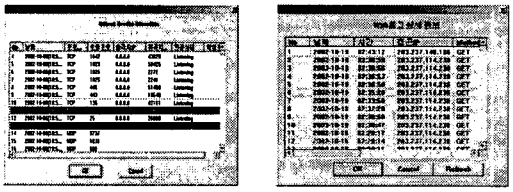
인하기 위한 레지스트리 정보를 분석한다.

또한 서버시스템의 포트별 연결 시도 수를 확인함으로써 어느 포트가 공격받을 가능성이 높은 지의 여부를 판단하는데 도움을 준다.



[그림 6] 레지스트리 정보와 포트별 접속통계

네트워크 연결 분석 모듈에서는 서버시스템에서 대기하고 있는 포트와 연결되어있는 포트를 확인함으로써 백도어 등이 실행되고 있는지를 분석하고, 연결된 원격 IP를 확인한다.



[그림 7] 네트워크 연결 정보와 웹 로그 정보

웹 로그 분석 모듈은 로그 저장 디렉토리의 .log형태의 텍스트 파일을 분석한다. 웹 로그파일 정보는 불법적으로 수정이나 삭제될 수 있기 때문에 실시간으로 정보를 데이터베이스에 저장한다.

불법적인 접근이나 공격 즉, 유니코드 접근 방법이나 코드레드와 같은 접근을 탐지한다. 기록되어 있는 여러 필드정보 중 cs-uri-stem과 cs-uri-query 필드는 요청한 페이지와 그 페이지에 요구되는 쿼리를 확인할 수 있다.

웹 로그 분석을 통하여 서버시스템에 대해 불법적인 접근이나 공격을 시도하는 원격지 IP에 대하여 차단 등의 조치를 취하도록 서버시스템 관리자에게 권고한다.

5. 결론

본 논문에서는 지속적으로 증가하고 있는 NT서버 시스템의 피해를 최소화하고, 불법적인 접근에 대해 신속하게 대응할 수 있는 정보를 제공한다.

서버시스템으로 유입되는 패킷을 실시간으로 수집하여 침입의 징후를 신속하게 판단하고, NT서버 시스템에서 제공하는 웹 로그, 레지스트리 정보, 네트워크 연결 세션 정보를 수집하여 관리자가 한눈에 알아볼 수 있도록 정보를 제공한다. 따라서 관리자는 공격의 유형과 피해의 정도를 추측할 수 있다. 또한 시스템의 어느 부분이 취약한지를 파악하여 발생했던 불법적인 접근에 대하여 향후 예방 조치를 취할 수 있는 정보와 기회를 제공할 수 있다.

향후 연구과제로는 새로운 패턴의 주기적인 추가와 새롭게 등장하는 해킹기법을 탐지, 분석할 수 있는 기능을 추가하고, 사용자의 인터페이스를 확장 보완함으로써 더욱 기능적이고 효율적인 시스템으로 개선할 수 있을 것이다.

[참고문헌]

[1] "Passive Vulnerablility Detection"
Network Security Wizard, 1999

[2] "Web Hacking:Attacks and Defense"
Stuart McClure, Saumil Shah, Shreeraj Shah 저 2002

[3] "악성 코드(malicious code) 대응지침 "
http://www.certcc.or.kr/paper/tr2002/tr2002_06/malicious_code.html

[4] "해킹피해시스템(Windows NT) 분석절차"
http://www.certcc.or.kr/paper/tr2001/tr2001-03/Windows NT.html

[5] "침해사고 대응방법 및 절차"
http://www.certcc.or.kr/paper/cert.html

[6] "해킹피해시스템 분석 및 복구 절차"
http://www.certcc.or.kr/paper/tr2000/2000-02/tr2000-02.html

[7] "TCP/IP 네트워크"
정진욱 외 2명 진영사, 1999

[8]" 네트워크 침입탐지와 해킹분석 핸드북"
Judy Novak, Stephen Northcutt 저 2001