네트워크상의 서비스 거부 공격 감시 시스템 설계

최 민 석, 이 종 민, 김 용 득
아주대학교 전자공학부
전화 : 031-219-2372 / 핸드폰 : 017-528-2461

The Implmentation of monitoring system for the attack of network service denial

Min-Suk Choi, Jong-Min Lee, Yong-Deak Kim
Dept. of Electronics Engineering, Ajou University
E-mail : tuscani@comnet.ajou.ac.kr

Abstract

This paper deals with a denial of service is about without permission knocking off service, for example through crashing the whole system. Another definition is that denial of service is seeing to that someone don't get what they paid for. The Network Denial of service Attack Detection System designed and implemented through suggested algorithm can detect attacking from the outside among denial of service attacks. It shown that designed system gives the system administrator the opportunity to detect denial of service attack.

Ⅰ. 서론

인터넷 상용망의 증가에 따라 인터넷 접속이 쉬워졌고 이로 인해 단순한 정보와 자원의 공유를 넘어 전자 결제, 전자 상거래 등의 편리함이 제공되고 있다. 그러나 그에 따른 부정적인 측면 또한 발생하고 있는데 시스템으로부터 허가 받지 않은 침입자로 하여금 정보를 자유롭게 접하도록 하는 것이다. 현재 국내에는 여러 가지 침입자 탐지 시스템의 개발에 관한 연구가 활발히 진행되고 있지만 서비스 거부 공격에 대한 연구는 미비하다. 본 논문에서는 관련 이론을 정립하고 서비스 거부 공격에 대한 원인을 분석하여 설계한 네트워크 서비스 거부 공격 감시 시스템을 설명하고 그 수행결과를 보였다.

Ⅱ. 이론적 배경

네트워크 상에서의 침입을 탐지하는 시스템은 다음과 같이 제시된다.

첫째 침입 감지 전문가 시스템(IDES)[1]은 침입 감지를 위해 복잡한 통계 방법과 알려진 침입 수법, 시스템 취약성, 그리고 각 기관의 보안 정책을 내재한 전문가 시스템을 사용하는 포괄적인 시스템이다. 전문가 시스템은 이미 알려진 침입 방법을 이용하여 침입을 감지하기 때문에 대상 시스템의 특수한 환경을 충분히 고려할 수 있는 반면 대상 시스템의 상황 변화로 인한 지식의 갱신이 어렵다.

둘째, 유닉스를 위한 상태 분석 툴은 UNIX 환경 하에서 실시간 침입탐지 도구로서 상태 분석 툴[2]의 기본적인 설계 기법을 UNIX 환경에 적용하여 구현한 것이다. 상태 분석 툴은 컴퓨터 침입을 표현하기 위한 새로운 접근 방식으로, 침입 과정을 상태 변화의 순서로 나타내고 있다. 즉, 어떤 침입을 성공적으로 달성하는 데 필요한 과정을 초기 상태에서 목표 상태에 도달하기까지의 단계들을 컴퓨터 사용 측면에서 표현하여 나타낸다.

Ⅲ. 서비스 거부 공격 기법

서비스 거부 공격[3][4]이란 공격 대상 호스트의 자원을 낭비시켜 목표 시스템의 기능을 저하시키거나 서비스를 제공할 수 없게 하는 것으로 크게 내부 사용자와 외부 사용자로부터의 공격으로 나뉘어 진다.

먼저 내부 사용자로부터의 공격은 한 사용자가 너무 많은 프로세스를 수행하여 다른 사용자가 시스템을 사용하지 못하게 하는 것으로 이는 프로세스 낭비와 메모리 부족 현상을 초래할 수 있다. 외부 사용자로부터의 공격은 잘못된 소스주소를 이용하여 UDP 서비스(echo, time, daytime, chargen)들을 반복시킴으로써 시스템의 부하를 크게 한다. 패킷의 내용에 상관없이 들어오는 패킷의 소스 주소로 결과를 돌려주는 UDP 서비스 사이에 연결이 일어나면 각 서비스는 서로 패킷을 계속 주고받아 서비스 거부를 일으키게 된다. TCP 연결은 클라이언트가 TCP 헤더에 동기 신호가 설정된 연결 요청 패킷을 서버에 전송하면 정상적인 경우, 서버는 IP 헤더에 지정된 클라이언트 주소로 SYN/ACK를 회신하고 클라이언트는 다시 ACK를 서버로 전송하여 연결을 맺게 된다. 그러나 IP 헤더의 클라이언트 주소를 잘못된 호스트 주소로 위장한 경우, 대상 서버는 연결을 완결 짓지 못한 채 타이머가 종료될 때까지 대기하게 되고 이 동안에 다른 TCP연결 요청은 무시된다. 그림1-1은 정상적인 TCP 연결 설정 절차를 보여주며, 그림1-2는 호스트 A가 X로 위장하여 호스트 B를 공격하는 절차를 나타낸다.[5]

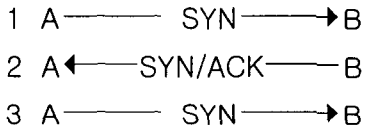

그림 3-1. TCP 연결 설정 절차

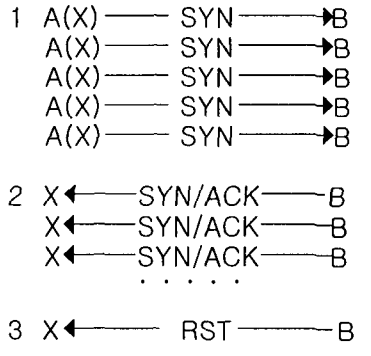

그림 1-4. TCP SYN 넘침 공격 절차

Ⅳ. 서비스 거부 공격 감시 시스템 설계

본 논문에서 설계한 네트워크 서비스 거부 공격 감시 시스템의 전체 구성은 그림 2와 같다. 호스트로 들어오고 나가는 모든 패킷은 로그수집기에 의해 로그로 기록되고, 분석기는 공격과 관련이 있는 로그만을 선택하여 검색기로 보낸다.

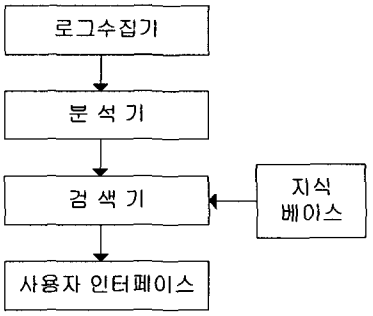

그림 2. 서비스거부공격감시시스템

검색기는 분석기를 통과한 로그들을 지식 베이스로 이미 알려진 공격 형태와 비교하여 공격 여부를 탐지한 후 그 결과를 사용자 인터페이스로 보냄으로써 사용자가 그에 대한 조치를 취하게 한다.

4.1 로그 수집기

시스템으로 드나드는 모든 패킷을 감시 시스템에서 사용하기 위한 로그 포맷으로 기록하는 역할을 수행한다. 본 논문에서는 로그 기록 도구로, windump 버전 3.6.2를 이용하여 필요한 로그 레코드를 수집하였다. 그림3은 로그 레코드의 자료 구조를 나타낸다.

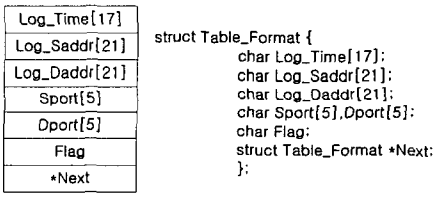

그림 3. 로그레코드의 데이터구조

로그 레코드의 각 필드는 로그가 기록된 시간, 소스 주소, 소스 포트, 목적 주소, 목적 포트, TCP Flag의 세트된 상태를 나타낸다. 로그 수집기에 의해 기록된 로그는 분석기의 입력으로 보내진다.

4.2 분석기

로그 수집기에서 보내온 로그 데이터들을 입력으로 받아, 서비스 거부 공격과 무관한 데이터를 분류해내는 역할을 수행한다. 검색 알고리즘은 그림 4와 같다.

```
For each Log_record
        If Log_record.field in Log_Table
            then pass Log_record to 검색기
        Endif
Endfor
```

그림 4. 분석기 알고리즘

본 논문에서 구현한 로그 테이블의 구조는 그림 5와 같다.

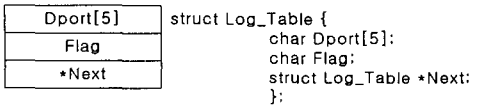

그림 5. 로그 테이블 구조

로그 테이블의 각 필드는 목적 포트, 세트된 상태비트, 다음 로그 테이블에 대한 포인터를 나타낸다. 수집된 로그중 목적 포트와 플래그를 비교하여 일치하는 데이터만 골라내어 검색기의 입력으로 보낸다.

4.3 검색기

분석기를 거쳐 입력된 로그 레코드를 지식 베이스의 규칙 테이블과 비교하여, 공격 유형과 일치하는 데이터를 분류해낸다. 서비스 거부 공격은 일정한 형태를 가진 패킷의 반복으로 파악될 수 있는 데, 이 반복되는 일정한 형태를 가지는 로그 레코드의 명세를 규칙 테이블에 텍스트 파일 형태로 그림 6과 같이 정의한다.

```
#Rule Table
#TCP port(telnet) 서비스 거부 공격
RULE 1.
dport = 23.
flag = SYN.
#TCP port(ftp) 서비스 거부 공격
RULE 2.
dport = 21.
.....
```

그림 6. 규칙 테이블

위 파일은 시스템 구동 초기에 규칙 테이블 읽기 모듈에 의해 자료 구조의 형태로 저장되는데 그 구조는 그림 7과 같다.

```
struct Rule_Table_Format {
        int Rule;
        char Dport[5];
        char Flag;
        };
struct Rule_Table_Format *Rule_Ptr[MAXRULE];
```

그림 7. 규칙 테이블의 구조

공격 탐지를 위해 검색기는 위에서 얻은 규칙번호를 이용하여 검지테이블에서 해당 로그의 정보를 찾아낸다. 검지 테이블은 검색기로 입력된 모든 로그에 대한 정보가 저장되어 있는 테이블로 그림 8의 구조를 가진다.

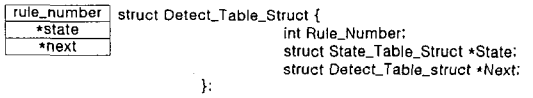

그림 8. 검지 테이블 구조

또한 검지 테이블의 빠른 검색을 위해 검지 테이블 포인터라는 테이블을 사용하는데 그 구조는 그림 9와 같다.

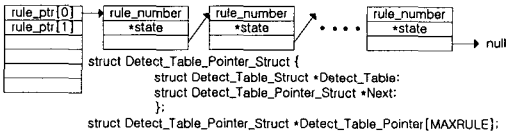

그림 9. 검지테이블 포인터 구조

그림 9내의 연결 리스트 모양은 검지 테이블 포인터에 해당하는 규칙 번호에 따라 연결된 검지 테이블의 단일 링크드 리스트를 보여준다. 규칙 테이블에서 찾은 규칙 번호로 검지 테이블 포인터에서 해당 검지 테이블을 찾아 단일 링크드 리스트를 따라가며 로그 레코드와 검지 테이블의 상태멤버의 내용을 비교하여 일치할 경우 카운트를 수행한다. 여기서 상태멤버는 상태 테이블로 구성되며 구조는 그림 10과 같다.

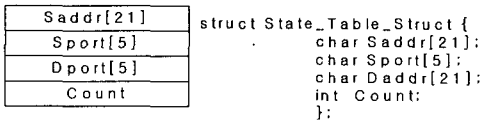

그림 10. 상태 테이블의 구조

카운트 수행은 일정한 공격횟수를 넘을 경우 공격으로 판단하기 위해서이다. 상태 테이블에서 일치되는 로그 기록이 없는 새로운 로그 레코드는 검지 테이블과 검지 테이블 포인터에 추가된다. 검색기의 전체적인 알고리즘은 그림 11과 같다.

```
For each Log_Record
  If log_record match in Rule_Table then
    locate 해당 rule in Rule_Pointer_Table
    For each row pointer in the linked list
      If state in Detect_Table match with Log_Record then
        state.count = state.count + 1
        If state.count achieved attack number then
          pass the Detect table to 사용자 인터페이스
          delete the Detect table from Detect_Table_Pointer
        Endif
      else duplicate the row into a new row
        update the new row to the Detect_Table
        add 해당 rule to Detect_Table_Pointer
Endif Endfor Endif Endfor
```

그림 11. 검색기 알고리즘

검색기의 결과는 사용자 인터페이스를 통해 일정한 텍스트의 형태로 관리자에게 알려져 서비스 거부 공격 여부를 알 수 있게 한다.

V. 서비스 거부 공격 측정 실험

본 논문에서 구현한 네트워크 서비스 거부 공격 감시 시스템은 윈도우즈 2000이 적재된 펜티엄 800을 CPU로 하는 PC에서 측정 실험을 하였다. 시뮬레이션의 수행을 위해 먼저 네트워크를 통해 전달되는 각종 패킷을 모아

야 한다. 본 시뮬레이션은 호스트가 서비스 거부 공격을 당하고 있다는 전제하에 수행된다. 앞의 내용을 기반으로 하여 구성한 서비스 거부 공격 감시 시스템의 모습을 그림 12에 보였다.

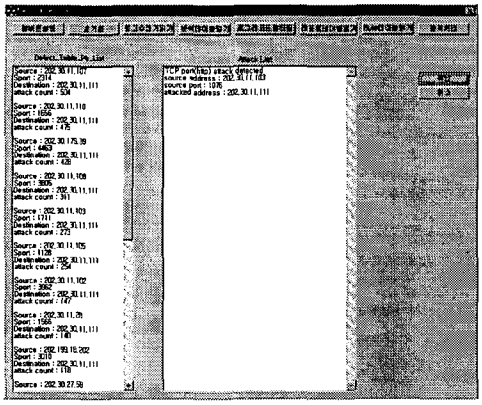

그림 12. 서비스 거부 공격 감시 시스템

각 버튼은 앞에서 설명한 각각 단계에 대한 수행을 차례로 하기 위해 나열한 것이다. 왼쪽 부분의 표시창은 로그 레코드를 나타낸 것으로 구조체 안의 공격 카운트 필드에 공격횟수가 기록되어 있다. 오른쪽 부분은 정해진 횟수가 넘어 공격으로 인식되면 공격리스트로서 나타나게 된다. 표 1은 공격리스트의 예를 나타낸다.

번호	소스주소	공격횟수
1	202.30.11.103	674
2	202.30.11.107	504
3	202.30.11.110	475
4	202.30.179.39	428
5	202.30.11.108	311
6	202.30.11.105	254
7	202.30.11.102	147
8	202.30.11.28	140
9	202.199.18.202	118
10	202.30.27.58	80
11	202.107.218.130	77
12	202.109.197.232	46
13	202.30.22.109	35
14	202.30.21.53	14
15	210.117.65.45	11
16	210.107.207.190	7
17	61.43.167.118	1
	총 공격 회수	3322

표 1. 공격 리스트

공격횟수를 600으로 설정하면 위의 예에서 1번의 소스 주소가 차단되어야할 공격이 되고 나머지는 허용된 공격이 된다. 따라서 모든 주소가 같은 비율로 접속을 계속하고 있다면, 다음과 같은 공격 차단율을 얻을 수 있다.

$$\frac{(3322-2648)}{3322} \times 100 = 20.29\%$$

총 공격회수 : 3322
차단된 주소의 공격 회수 : 674
허용된 주소의 공격 회수 : 2648

이는 본 논문에서 제안한 네트워크 서비스 거부 공격 감시 시스템의 긍정적인 결과를 나타낸다. 이렇게 함으로서 공격 의도가 없는 사용자에게 불편함을 주지 않고 침입자를 알아내어 막을 수 있는 감시 시스템을 구현할 수 있다.

VI. 결론

네트워크를 통한 정보 교환과 다양한 서비스 제공과 함께 사용자의 정보를 보장하는 가용성에 대한 인식이 높아지게 되었고 이에 가용성을 손상시키려는 서비스 거부 공격에 대한 이해가 필요하게 되었다. 본 논문에서는 서비스 거부 공격을 탐지하여 알려주는 감시 시스템을 구현하였다. 네트워크를 통해 이동하는 패킷으로부터 로그 파일을 생성하고 로그 수집기에 의해 로그 레코드로 변환 후 분석기와 검색기를 통해 공격여부를 탐지하게 된다. 시뮬레이션을 통해서 약 20%정도의 공격 감소율을 얻을 수 있다는 것을 보였다. 본 논문에서 설계된 시스템에는 이미 알려진 공격을 탐지하므로 실시간 감시는 할 수 없다. 하지만 서비스 거부 공격 침입 감시 시스템의 실현과 사용자 인터페이스로 보다 편리하게 네트워크를 모니터링 할 수 있도록 설계함으로 관리자의 현실적인 감시 시스템의 구현이 가능함을 보였다.

참고문헌

[1] T. Lunt et al., "A Real time Intrusion Detection Expert System(IDES)", Technical report, Computer Science Laboratory, SRI International, May 1990

[2] Koral Ilgun, "USTAT: A Real-Time Intrusion Detection System for UNIX", University of California, July 1992.

[3] 분산 환경에서의 서비스거부 공격 분석보고서 http://cert.certcc.or.kr/paper/tr1999/1999010/tr1999010.html

[4] 네트워크 스캔공격 탐지 통계 분석, http://cert.certcc.or.kr/paper/tr2000/2000-09/tr2000-09.html

[5] Dittrich,"The "Tribe Flood Network" distributed denial of service attack tool", October 21, 1999