효율적인 네트워크 스캐닝 탐지 시스템의 설계 및 구현

이현주*, 한영주*, 김희승*, 정태명**
*성균관대학교 컴퓨터공학과
이동형 응급의료 정보 시스템 개발센터
**성균관대학교 정보통신공학부
e-mail : {hjlee98, yjhan, hskim}@imtl.skku.ac.kr, tmchung@ece.skku.ac.kr

Design and Implementation of Efficient detection System for Network Scanning

Hyun-Joo Lee*, Young-Ju Han*, Tae-Myung Chung**
*Cemi: Center for Emergency Medical Informatics,
Dept. of Computer Engineering, Sungkyunkwan University
**School of Information &.Communication Engineering, SungKyunKwan University

요 약

일반적으로 해커들은 네트워크상에 있는 목표(Target) 시스템에 대해 공격을 시도하기 위한 사전 단계로 포트 스캐닝(Port Scanning)을 통한 정보 수집의 단계를 선행하게 된다. 이 때, 사용되는 포트 스캐닝 기술은 이미 여러가지 방법이 알려져 있으며, 네트워크 관리자의 입장에서는 정상적인 네트워크 접속과 포트 스캐닝 공격을 구분해야만 한다. 본 논문에서는 네트워크를 통한 공격의 가장 많은 부분을 차지하고 있는 스캐닝 공격을 빠르고 효율적으로 탐지할 수 있는 룰 기반의 침입 탐지 시스템을 커널레벨과 응용레벨에서 설계하고 구현하였다.

1. 서론

우리나라는 물론 전세계적으로 네트워크의 발전 속도는 양적인 팽창과 더불어 그 구조가 날로 복잡해지고 있으며, 이와 비례해서 각종 해킹 사건들이 늘어가고 있는 추세이다. 한국정보보호진흥원(KISA)에서 매월 발표하는 "침해 사고 접수 및 처리 현황"을 보면 연도별로 해킹 건수는 매년 급격하게 증가하고 있으며, 공격 수법 또한 다양해지고 있음을 알 수 있다[12][13]. [표 1]은 1996 년부터 인터넷 사용자의 증가에 따른 침해사고 접수현황을 나타낸 것으로 인터넷 사용자 증가율 대비 침해사고 증가율이 매년 증가하고 있음을 보여주고 있다.

본 논문은 보건복지부 보건의료기술진흥사업회 지원에 의하여 이루어진 것임(과제번호: 02-PJ3-PG6-EV08-0001)

[표 1]인터넷 사용자의 증가에 따른 침해사고의 접수현황

년도	접수 건수	침해사고증가율 (전년대비)	인터넷사용자 수(명)	인터넷사용자증가율 (전년대비)
`96	147	-	731,000	-
`97	64	-44%	1,634,000	124%
`98	158	147%	3,103,000	90%
`99	572	262%	10,860,000	250%
`00	1,943	240%	19,040,000	75%
`01	5,333	174%	24,380,000	28%
`02	38,677	625%	-	-
`03	85,023	112%	-	-

[표 2]는 2003 년도에 집계한 통계 자료로, 많이 이용되는 해킹 수법들을 분류한 표이다[12]. 공격의 형태를 보게 되면 악성 프로그램의 사용, E-mail 관련 공격과 함께 취약점 정보수집 공격이 가장 높은 비율을

차지하고 있음을 볼 수 있다. 이는 해커들이 해킹을 시도하기 전 시스템에 대한 사전 정보 수집의 단계로 취약점 스캐닝 방법을 많이 사용하고 있다는 의미이다[14].

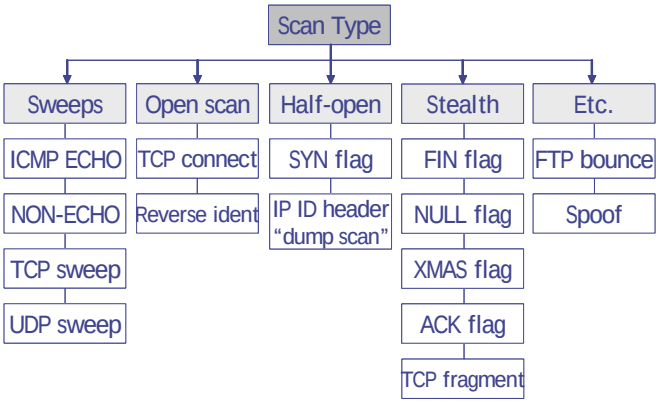
[표 2] 공격수법

구분	건수	비고
사용자 도용	46	개인 사용자 계정 도용 등
S/W 보안 오류	1620	-
버퍼오버플로우 취약점	1160	snmp, named/bind 등의 취약점 이용
구성, 설정 오류	9899	사용자 권한 설정 오류
악성 프로그램	5837	spida 웜, 윈도우즈 트로이목마 등
프로토콜 취약점	0	-
서비스 거부 공격	30	서비스 거부
E-main 관련 공격	6900	스팸메일 관련 공격
취약점 정보수집	4937	named/bind, ftpd, rpc 취약점 스캔
사회 공학	0	-

위의 자료에서도 알 수 있듯이 스캐닝 공격은 가장 많이 사용되는 공격 수법의 한 형태로 침입 탐지 시스템에서 이를 탐지하는 것은 가장 중요하게 갖추어야 할 요소중에 하나라고 할 수 있다.

2. 관련 연구

목표 네트워크 내에 살아있는 네트워크 서비스를 식별하기 위한 효과적이고도 보편적인 방법은 포트 스캐닝을 통해 정보를 획득하는 방법이다. 해커들이 사용하는 포트 스캐닝 기술은 그 형태에 따라 [그림 1]과 같이 5 개의 그룹으로 분류할 수 있는데[2][4][6], 세부절을 통해 각각에 대해 간단하게 살펴보도록 하겠다.



[그림 1] 네트워크 스캐닝 기법

2.1 Ping Sweeps

목적지의 시스템이 살아있는지 여부 혹은 포트가 열려 있는지를 알아보는 형태의 공격이다.

ICMP ping 을 이용해서 공격 목표 기관에서 사용하거나 소유하고 있는 IP 주소와 네트워크 범위를 알아내는 방법, ICMP 를 이용하지 않고 TIMESTAMP, ADDRESS MASK REQUEST 같은 Non-Echo ICMP 프로토콜을 이용해서 목표 시스템에 대한 정보를 얻어오는 방법, 그리고 TCP 3-way handshake 를 이용하거나 UDP 포트의 ICMP PORT UNREACHABLE 메시지를 이용해서 목표 시스템의 생존 여부를 알아 내는 방법 등이 사용되고 있다.

2.2 Open Scan

목표 시스템의 접근 가능한 서비스를 식별하는 방법으로 TCP 의 3-way handshake 를 이용한 TCP connect 스캐닝 방법이 있고, root 로 실행되는 데몬을 찾기 위한 Reverse Ident 스캐닝 방법이 있다.

2.3 Half-Open Scan

이 방법은 TCP 연결을 완전히 맺지 않아 로깅 기법을 교묘하게 피할 수 있는 스캐닝 방법이다.

SYN 플래그를 설정해서 TCP 패킷을 보내는 TCP flag 스캐닝과 “dumb”호스트를 이용하는 IP ID header TCP 스캐닝 기법이 있다.

2.4 Stealth Scan

새로운 형태의 스캐닝 공격 방법으로 한 개의 플래그 비트를 설정해서 전송하는 방법(FIN flag probe 스캐닝, NULL flag probe 스캐닝, XMAS flag 스캐닝), 여러 비트를 설정한 패킷을 한꺼번에 보내서 분석하는 방법, 패킷을 수 천개의 작은 조각으로 나눠서 보내는 방법 등이 사용되고 있다[10].

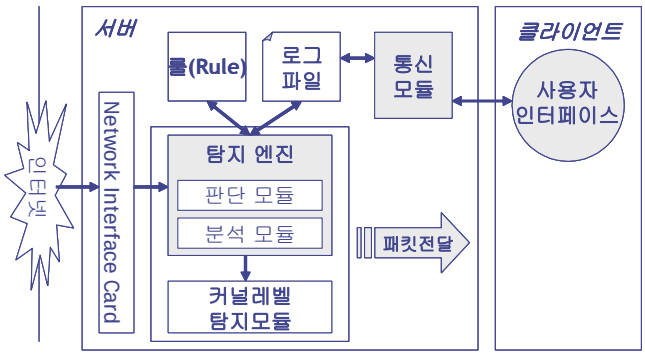
2.5 기타

그 밖에 FTP bounce 스캐닝 공격, sniffer 기반의 위조된 TCP 스캐닝 공격 등이 있다.

3. 네트워크 스캐닝 공격 탐지 기법 설계

본 장에서는 구현한 네트워크 스캐닝 공격 탐지 모듈에 대한 구성과 사용자 인터페이스 등 세부적인 사항들에 대해서 살펴본다.

아래의 [그림 2]는 스캐닝 공격 탐지 모듈의 전체 구조를 나타낸다.



[그림 2] 전체 시스템 구성도

본 시스템은 크게 서버측 프로그램과 클라이언트측 프로그램으로 나뉜다.

서버측 프로그램은 네트워크 경계에 위치하여 관리

네트워크 내부로 들어오는 모든 패킷을 수집하고, 수집한 패킷에 대해 공격에 해당하는 패킷인지 여부를 판단해서 관리자에게 알려주는 역할을 담당한다.

클라이언트측 프로그램은 서버로부터 탐지된 공격 상황을 관리자에게 통지하고 후속 조치를 취할 수 있도록 부가정보를 제공한다.

3.1 공격 탐지 과정 및 모듈별 기능

서버측 프로그램은 경계 네트워크에 설치되어 네트워크 인터페이스 카드(NIC)의 Promiscuous 모드를 통해 자신의 관리 네트워크 내로 들어오는 모든 패킷을 수집하게 된다.

Libpcap 라이브러리를 이용해 수집된 패킷은 응용 레벨에서 구현한 탐지 엔진에서 공격 여부가 판단된다.

탐지 엔진은 분석 모듈과 판단 모듈로 구성되는데, 먼저 분석 모듈은 수집된 패킷을 타입별로 분류하고, 특정한 형태의 자료 구조로 메모리에 저장하는 역할을 한다. 판단 모듈은 분석 모듈에서 저장한 정보를 지속적으로 룰과 비교하면서 공격 기법별 침입 여부에 대해 검사를 하고, 공격인 경우 로그파일에 해당 내용을 저장하고 그렇지 않은 경우에는 커널에 이를 알려 보다 빠른 패킷 포워딩을 할 수 있도록 해준다. 이러한 처리는 커널 레벨에서의 빠른 속도와 어플리케이션 레벨에서의 높은 보안성을 동시에 만족시켜줄 수 있는 장점을 갖게 한다.

효율적인 침입 판단을 위해서 응용 레벨에서는 [그림 4]와 같은 자료 구조를 사용했다.

통신 모듈은 로그 파일을 실시간으로 모니터링 하고 있다가 침입에 해당하는 기록이 갱신되면 즉시 사용자에게 해당 내용을 전송해 준다.

사용자 인터페이스는 탐지 엔진으로부터 탐지해낸 침입에 대해 상세한 정보를 사용자에게 알려주는 역할을 한다.

3.2 구현상의 특징

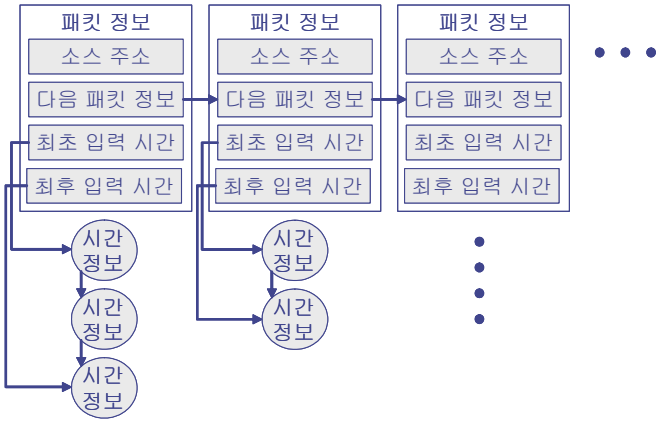
침입 탐지를 위한 정책은 알려진 스캐닝 공격에 대해 대응할 수 있도록 룰(rule)로 정의 되어있고, 룰에 정의된 정책에 위반되는 패킷에 대해서는 사용자에게 경고(alert)를 해주게 된다.

룰로 정의된 정책은 [그림 3]의 형태로 작성되어 있다. 공격자의 스캐닝 공격 타입(Type)에 따라 공격 상태(Condition)라고 판단이 되면, 그에 따른 행동(Action)을 취하게 되는 구조이다.

Type	*Condition*	*Action*

[그림 3] 룰의 구조

예를 들어, TCP SYN 스캔의 경우에는 같은 소스 IP 주소에서 목적지 포트 번호만을 달리하는 SYN 패킷이 특정 시간안에 보통의 패킷보다 많은 수가 들어올 것이므로 상태(Condition)는 단위 시간당 들어오는 패킷의 임계치 값으로 설정되어 있다. 해당 패킷이 처음 들어온 시간과 가장 최근에 들어온 시간을 비교해서 상태에 정의되어 있는 임계치보다 많은 수의 패킷이 들어오면 행동(Action)에 정의된 대로 관리자에게 경고를 해주거나 포트를 막는 등의 조치를 취하게 된다.



[그림 4] 패킷 정보 저장 데이터 구조

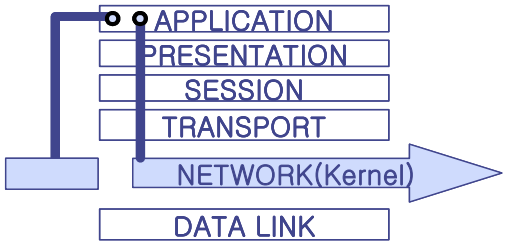
본 구현에서는 효율적이고 빠른 탐지를 위해 두 가지의 특징적인 방법을 사용하였다.

먼저 응용 레벨에서의 저장 구조를 위와 같이 단순화했다. 위의 저장 구조가 갖는 특징은 각 패킷의 정보의 2 중 구조화 및 저장 정보의 간략화를 통해서 유지해야하는 데이터의 양을 크게 줄였다는 점이다. 스캐닝 탐지 시스템은 네트워크의 경계에서 모든 패킷을 검사해야하는 시스템이므로 빠른 처리를 하지 못하면 내부 사용자의 사용성을 저해하는 요소가 될 수 있다. 때문에 처리 속도를 위해 연산량이 작아야 되고, 데이터를 저장하는 방법에 있어서도 높은 효율성이 요구된다. 본 구현에서는 공격 패킷에 대한 정보를 위와 같은 구조에 저장함으로서 분석에 필요한 데이터를 위한 저장 메모리를 일정 수준 이상 사용하지 않고 효율적으로 사용할 수 있었다. 또한 시간만을 단순 비교 하기 때문에 연산 속도가 빠르다는 장점도 갖게 되었다.

본 구현에서는 또한, Firewall 에서 새롭게 등장한 패킷 필터링 개념인 'Adaptive Proxy'의 개념을 응용해서 프로그램을 구현하였다. Adaptive Proxy 는 패킷 검사의 초기에는 Application level 에서 검사를 진행하다가 안전하다고 판단이되면 Network level 로 내려가서 filtering 기능만을 수행하게 하는 방법으로, 앞에서도 언급한 바와 같이 어플리케이션 프락시의 높은 보안성과 동시에 패킷 필터링의 빠른 속도를 갖을 수 있다는 장점을 갖고 있다[1].

구현된 탐지 프로그램도 이와 마찬가지로 응용계층에서 먼저 룰과 비교를 하고 공격이 아닌 경우 연속되는 패킷에 대해서는 커널 레벨에서 바로 다음 서브 네트워크로 통과 시키는 작업을 수행하게 된다. 이는 네트워크를 통과하는 수 많은 패킷을 응용 레벨에서 모두 검사하는데 따르는 부담을 줄여준다.

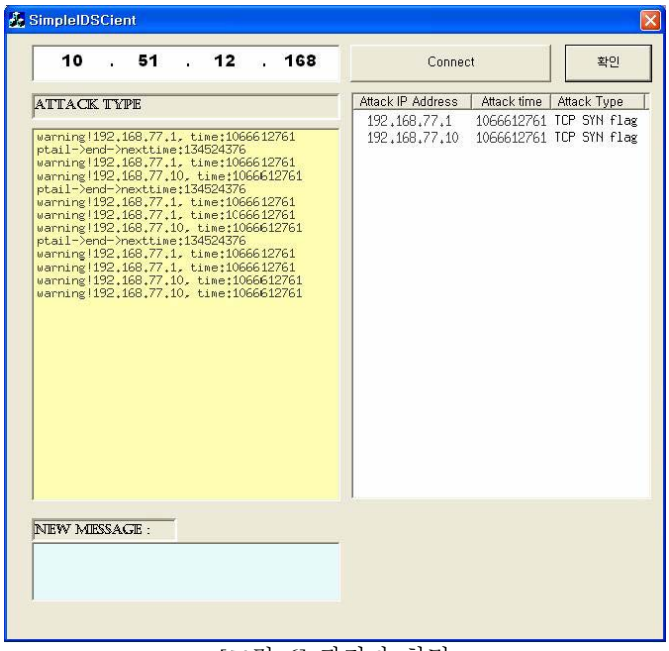
[그림 5]은 본 논문에서 구현한 포트 스캐닝 탐지 프로그램이 OSI 7 레이어 스택상에서 패킷을 수집하는 과정을 개념적으로 보여주고 있다[1].



[그림 5] 패킷 수집 과정

[그림 6]은 관리자가 보게되는 화면으로 네트워크 스캐닝 툴로 널리 사용되고 있는 NMAP[10]을 통해 스캐닝을 한 후 이를 탐지하는 것을 보여주고 있다.

관리자는 스캐닝 공격에 대해 언제, 어떤 호스트로부터 어떠한 공격이 이루어졌는지만 알면 적절한 조치를 취할 수가 있으므로 로그 파일에는 공격이 일어난 시간과 공격을 시도한 소스 IP 주소, 그리고 공격 타입만을 저장하게 된다. 화면 우측에 있는 내용은 로그 파일을 파싱해서 관리자에게 보여주는 부분을 나타내고 있다.



[그림 6] 관리자 화면

4. 포트 스캔 탐지 시스템 구현

4.1 개발환경

· 운영체제 : Red Hat Linux 7.3 (kernel 2.4.21), Windows XP

· 개발 언어 : gcc 3.2.2, Visual C++ 6.0

· 패킷 수집 라이브러리 : libpcap version 0.7

4.2 구현

서버측 모듈의 구성에 있어서, 패킷의 계속적인 수집과 분석, 로그 기록을 병렬적으로 동시에 처리하고 각각의 프로세스간 간섭을 막기 위해서 멀티스레드로 구성하였다. 클라이언트 측도 마찬가지로 서버로부터 지속적인 정보수집과 관리자에게 정보를 전달하는 일련의 과정을 동시에 처리하기 위해 역시 멀티스레드로 구성하였다.

서버측 모듈은 gcc 를 기반으로 패킷 수집을 위해 공용적으로 널리 사용되는 libpcap 라이브러리를 사용하여 개발을 하였다.

커널 레벨에서의 패킷 처리를 위해서는 netfilter 를 사용하였으며, 응용레벨과의 통신은 proc 파일 시스템을 이용했다.

클라이언트측은 사용자에게 친숙한 인터페이스를 제공하기 위해 Visual C++로 개발하였다.

5. 결론 및 향후목표

본 논문에서 구현한 시스템은 네트워크를 통한 스캐닝 공격에 대해 다른 응용분야에서 사용중인 개념을 응용해 효율적이고 보다 빠른 탐지 능력을 갖도록 구현하였다. 본 구현은 TCP 플래그를 이용한 공격 등 알려진 형태의 공격들에 대해 대부분 탐지가 가능하다.

본 논문에서 구현한 스캐닝 탐지 시스템은 침입탐지 시스템의 일부 기능만을 구현한 것으로 향후 완전한 침입 탐지 시스템으로의 확장을 목표로 하고 있다.

참고문헌

[1] A Grauntlet Firewall Executive White Paper, “Adaptive Proxy Firewalls”, Network Associates.

[2] Dethy, “Examining port scan methods - Analysing Audible Techniques”, synnergy.net, 2001.

[3] Fyodor, “Remote OS detection via TCP/IP Stack Fingerprinting”, Phrack magazine volume 8 issue 54 article 9, October 18 1998. URL : http://www.phrack.com

[4] Fyodor, “The Art of Port Scanning”, Phrack 51 magazine volum 7 issue 51 article 11. URL : http://www.phrack.com

[5]. Joseph, S. and Tommy, G., “Intrusion Detection: Systems and Models”, 2002.

[6] Marco D.V., "A Review of Port Scanning Techniques", ACM SIGCOMM, 1999.

[7] Noureldien A.Noureldien, Izzeldin M.Osman “A Stateful Inspection Module Architecture”, IEEE, 2000.

[8] Sundaram, A., “An Introduction to Intrusion Detection”, DC, 1990. Crossroads: The ACM Student Magazine,2,4,1996, Hyperlink: acm.org/Crossroads, 1996.

[9] Theuns Verwoerd, Ray Hunt, “Intrusion detection techniques and approaches”, Dec. 2001.

[10] 유성철, “Analyzing NMAP”, OPRIX, ?.

[11] 정현철, “IP Fragmentation 을 이용한 공격기술들”, 한국정보보호진흥원(KISA), 2001.3.

[12] 한국정보보호진흥원(KISA), “해킹 바이러스 통계 및 분석 월보” , http://www.krcert.or.kr/, 2003. 12.

[13] 한국정보보호진흥원(KISA), "2002 년 6 월 침해 사고 접수 및 처리 현황”, http://www.krcert.or.kr/, 2002.3.

[14] 한국정보보호진흥원(KISA) 기술문서, “네트워크 공격기법의 패러다임 변화와 대응방안”, http://www.krcert.or.kr/, 2000. 12.