# Layer별 Scanning을 사용한 취약성 분석 방법

천우성* · 박대우*

*호서대학교 벤처전문대학원 IT응용기술학과

# Method of Vulnerability Analysis from Layer Scanning

Woo-Sung Chun* · Dea-Woo Park*

*Dept. of IT Application Technology, Hoseo Graduate School of Venture

E-mail : *deux8522@gmail.com · *prof1@paran.com

## 요 약

네트워크에서 OSI 7 Layer를 기반으로 통신 프로토콜이 구현되고 있고, 인터넷은 TCP/IP Layer를 중심으로 취약성이 발견되고 공격을 당하고 있다. 본 논문은 Scanning 프로그램들을 사용하여 네트워크에 Layer별로 Scanning을 실시하고 그에 따른 취약성을 각 Layer별로 분석한다. 각 Layer별 취약점과 Scanning 프로그램에서 분석 결과들에 대한 차이점을 분석 연구한다. 분석된 결과들에 대한 Scanning 프로그램에 대한 특성을 반영한 Scanning방법에 대한 특장점을 연구하고, 각 Layer별로 보안 대응 방안을 제시한다. 본 연구의 결과는 해커의 공격에 대한 취약성을 분석과 방어를 위한 보안정책 수립에 대한 자료로 활용되어 네트워크의 보안을 강화하는데 기여 할 것이다.

## ABSTRACT

Network based on the OSI 7 Layer communication protocol is implemented, and the Internet TCP / IP Layer Based on the vulnerability is discovered and attacked. In this paper, using the programs on the network Layer Scanning conducted by the Layer-by each subsequent vulnerability analysis. Layer by Scanning each vulnerability analysis program to analyze the differences will be studied. Scanning for the studies in the program reflects the characteristics of the Scanning Features of way, and security countermeasures by each Layer is presented. The results of this study was to analyze its vulnerability to hackers and security for defense policy as the data is utilized to enhance the security of the network will contribute.

키워드

OSI 7 Layer, vulnerability, scanning, scanning tool analysis

## Ⅰ. 서 론

인터넷의 취약성과 악성 코드[1]를 감염시킨 좀비 PC등을 이용한 DDoS공격[2]은 목표 시스템과 자원에 대하여 정상적인 서비스의 지연 혹은 마비상황을 불러일으키는 공격이다. 기업에게는 업무의 마비로 피해를 유발 시키며, 금융업 등 은 기업의 신뢰도에 심각한 손상을 입힐 수 있으며, 소송에 휘말려 직 간접적인 피해보상을 해야 하는 사태를 초래할 수도 있다.

기존의 해킹 방법은 해커가 기업의 네트워크에 불법적인 방법으로 침투해서 중요한 시스템의 슈퍼 사용자 권한을 획득하고, 그 내부에 들어있는 기밀 정보를 탈취하는 것이 대표적이었다.

하지만 DDoS 공격은 기업이 대고객 서비스를 운영하고 있는 운영 서버들(웹 서버[3], DNS 서버[4] 등)과 네트워크 장비(라우터, 방화벽 등)에 임의로 조작된 양의 트래픽[5]을 급격히 상승시켜서 전송함으로서 공격 목표시스템 자체를 지연 혹은 마비시켜 버림으로써 고객들이 기업의 서비스를 이용할 수 없게 만드는 목적을 가진다.

최근의 공격 추세를 보면 기업의 개별적인 서비스 웹 사이트[6]나 기타 서버들에 대한 공격을 통해 서비스를 마비시키는 공격 형태에서 점차 인터넷서비스 제공업체의 코어(Core) 라우터[7], DNS 서버들을 직접 공격해서 인터넷 인프라[8] 자체를 완전히 마비시키는 형태로 발전해 가고 있다. 또한, 전 세계적으로는 2002년 10월에 발생했던 13개의 최상위 루트 DNS(Domain Name Service) 서버들에 대한 대규모의 무차별적 공격으로 적지 않은 혼란을 주었던 사례가 있었다.

본 논문에서는 인터넷의 구조적인 취약점을 분석함에 있어 통신 프로토콜의 기본인 OSI 7 Layer[9]에 대해 각 계층별로 어떤 취약점을 가지

고 있는지 해커의 입장과 보안 담당자의 입장에서 여러 가지 Scanning 프로그램을 사용하여 각 Layer별로 Scanning을 실시하고 분석한다. 분석된 결과들에 대해 Scanning 프로그램에 대한 특성을 반영한 Scanning방법에 대한 특장점을 연구하고, 각 Layer별로 보안 대응 방안을 제시한다.

## II. 관련연구

### 2.1. OSI 7 Layer

OSI 모델(Open Systems Interconnection Reference Model)은 국제표준화기구(ISO)에서 개발한 모델로, 컴퓨터 네트워크 프로토콜 디자인과 통신을 계층으로 나누어 설명한 것이다.

계층별로 살펴보면 물리 계층(Physical layer), 데이터 링크 계층(Data link layer), 네트워크 계층(Network layer), 전송 계층(Transport layer), 세션 계층(Session layer), 표현 계층(Presentation layer), 응용계층(Application layer)으로 이루어져 있다.

표 1. OSI 7 Layer & TCP/IP Model

| OSI 7 Layer Model | | TCP/IP Model |
|---|---|---|
| 7 | Application | Application |
| 6 | Presentation | |
| 5 | Session | |
| 4 | Transport | Transport |
| 3 | Network | Internet |
| 2 | Data link | Data link |
| 1 | Physical | Physical |

### 2.2. 인터넷 TCP/IP layer와 취약점

#### 2.2.1. Application Layer

TCP/IP의 Application Layer는 소프트웨어가 실행되는 계층이다. 이들 프로그램은 사용자의 직접적인 입력을 받기 때문에 키보드 후킹 프로그램이나 키로거 등에 취약하다.

#### 2.2.2. TCP Layer

OSI 7 Layer의 Transport 계층에 속하는 TCP는 전송과 관련된 통제를 하는 계층이다. 전송은 반드시 수신하는 곳이 있다는 것을 전제로 하며 수신하는 쪽과의 접속이 선행되어야 한다. 이로 인해 취약점이 발생하는데, TCP 통신을 받으면 응답을 하고 상대방의 대답을 기다리는 세션이 발생하여, 상대방이 대답을 하지 않을 경우 필요 없는 세션으로 계속 남게 되며, 시스템을 느리게 만들고 누적되면 시스템을 마비시킨다.

#### 2.2.3. IP Layer

IP Layer는 Network Layer에서 기능을 수행한다. IP Layer의 중요한 기능은 주소 배정과 경로 선택에 있다. IP Layer는 상위 TCP Layer로부터 받은 데이터를 패킷이라는 단위로 처리한다. 이 패킷 안에는 상위와 데이터와 헤더가 포함되어 있다. IP layer 에서는 IP주소가 가상화 되면서 실제 통신이 이루어지는 주체를 속이는 통신이 발생하고, 이를 추적하기 어려운 취약점이 있다.

#### 2.2.4. Network Interface Layer

Network Interface Layer는 OSI 7 Layer의 Data Link Layer와 Physical Layer가 합해진 Layer로서 상위계층의 데이터에 대한 논리적, 물리적 전송에 관여하는 계층이다. Network Interface Layer에서는 전송 시에 정해진 순서에 따라 데이터를 전송하게 되는데, 전송 순서를 어긋나게 할 경우 데이터의 전송이 불가능해지는 취약점이 있다.

### 2.3 Scanning 종류와 Scanning Tools

#### 2.3.1 Scanning 종류

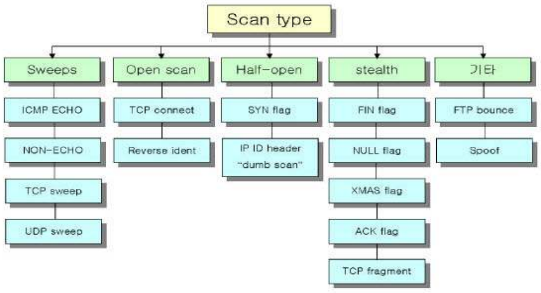


그림 1. scanning 종류

그림 1의 Sweep 이라는 것은 돌아본다는 말 그대로 해당 네트워크를 돌면서 살아있는 호스트,port를 찾는 것을 의미한다. ICMP ECHO (ping), Non-EC HO ICMP, TCP Sweep, UDP Sweep이 있다.

Open Scan 은 완전한 연결을 하는 scan으로서, scan결과의 신뢰성은 매우 높지만 정상적인 3-way handshake 를 모두 수행하기 때문에 타겟 호스트에 로그가 남으며 탐지되기도 쉽다. TCP connection, Reverse ident가 있다. SYN TCP flag와 IP ID Header TCP Scanning이 있다.

#### 2.3.2. Zenmap(nmap)

Zenmap은 네트워크 탐색, 관리, 인벤토리, 보안 감사용도로 사용해온 보안 tool이다. 로우 IP 패킷을 사용해 네트워크상에서 이용 가능한 호스트와 서버의 운영체제 종류와 버전, 패킷 필터나 방화벽 종류 등을 알아낸다. 또한 각종 옵션을 사용해 방화벽과 침입탐지시스템을 탐색해내고 이를 우회하여 scan이 가능하다.

#### 2.3.3. 7th Sphere Portscan

7th Sphere Portscan은 port scanning tool 로서 지정한 타켓 IP의 원하는 port를 검색 할 수 있다. 발견된 포트숫자를 또는 열려있는 소켓을 보여주고, 검색의 속도도 조절이 가능하여 방화벽 등의 필터링을 회피할 수 있도록 하였다.

2.3.4. Free Port Scanner

Free Port Scanner는 TCP기반 scanning tool로서 타겟의 IP주소와 TCP port를 입력하여 검사할 수 있다. 분석한 IP의 열린 port와 그에 대한 상세 분석 내용을 알려준다.

2.3.5. Angry IP Scanner

Angry IP Scanner는 IP Class 기반 tool로서 검색할 IP범위의 컴퓨터들에 FTP, HTTP, telnet, 특정port telnet이 가능한 도구이다. 간편한 사용법과 설치하지 않아도 실행이 가능하다.

## Ⅲ. Layer 별 Scanning과 취약점 분석

3.1. Physical Layer

데이터가 컴퓨터에서 네트워크로 빠져나가는 실제의 물리적인 장비(Lan card, 케이블 등)를 정의 하는 계층이다. Bit 신호로 표현되는 물리 링크의 활성화/비활성화 및 링크 유지를 나타낸다. (Cable, Connector, Bit 등)

3.2. Data link Layer

네트워크 케이블 같은 실제 미디어에 데이터를 올리고 데이터를 소멸 시키는 방법 등을 정의 한다. 물리 링크를 통한 신뢰성 있는 데이터 전송 기능을 제공한다. 물리적 주소 체계, 네트워크 토폴로지, 네트워크 접속, 오류 통지, 흐름 제어, 프레임 순차적 전송 등을 관여한다. (Ethernet, Token Ring, FDDI, PPP, Frame-relay 등)

3.3. Network Layer

네트워크 내부와 외부 네트워크 간의 메시지 주소를 지정한다. 네트워크 내에 있는 두 호스트 간의 연결성을 제공하고 경로 선택을 한다. (IP, IPX, Apple Talk 등)

3.4. Transport Layer

오류가 없는 데이터 전달 보장한다. 시스템에 발생하는 데이터를 분할하고 재조립 한다. 오류 검사, 흐름 제어 기능을 하여 신뢰성 있는 데이터를 전송 한다. (TCP, UDP)

3.5. Session Layer

통신채널을 설정하고 유지 및 관리 한다. (multi-user 용 컴퓨터로의 login이나 file전송 등이 이 Layer를 통해서 이루어진다.) 통신을 하고자 하는 두 호스트 간 연결을 설정, 관리, 종료한다. 효율적인 데이터 전송 처리, 서비스 종류 설정, 상위 계층에서 발생하는 문제에 예외 보고 기능을 수행한다. (NFS, ASP, X-Window System 등)

3.6. Presentation Layer

데이터가 표시되는 공통의 형식을 추가 한다. (코드 체계가 다른 컴퓨터간의 코드 변환이나, 데이터 압축 등) 한 시스템 응용계층에서 넘겨받은 정보를 다른 시스템 응용계층이 읽게 해준다. (JPG, BMP, MIDI, WAV, AVI, MPEG 등)

3.7. Application Layer

응용프로그램들이 서로 상호 작용하는 방법을 정의 한다. 사용자와 가장 가까운 OSI 계층으로 사용자 어플리케이션에 네트워크 서비스를 제공한다.(Telnet, HTTP, FTP, SMTP 등)

## Ⅳ. Layer 별 Scanning tool 특장단점 분석

4.1. Zenmap(nmap)

Zenmap은 그림 2처럼 nmap의 사용자 편의를 향상시킨GUI 버전으로서 port와 서비스 scan이 가능한 tool인데, 특히 OS scan이 가능하여 Guessing 기법으로 대상의 OS를 알려주는 장점이 있다.

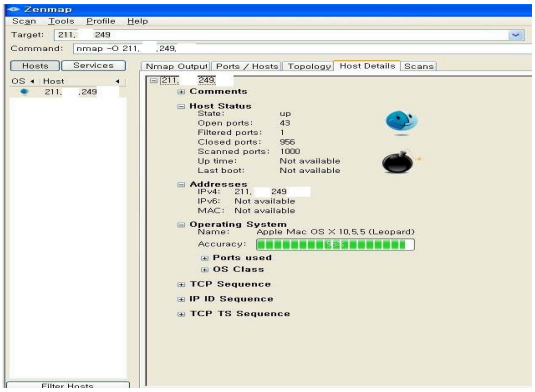


그림 2. Zenmap의 GUI scan 결과

4.2. 7th Sphere Portscan

7th Sphere Portscan은 Port Scanning tool로서 1번부터 65536 번까지 모든 port를 scan하여 열려있는 port를 찾아주어 서버나 PC의 취약점을 분석하여 주는 tool 이다.


그림 3. 7th Sphere Portscan의 scan 결과

4.3 Free Port Scanner

Free Port Scanner 는 TCP port scanning tool 로서 검색을 원하는 IP의 port를 scanning하여 해당 port에서 실행되고 있는 서비스의 상세한 정보를 알려주게 된다.

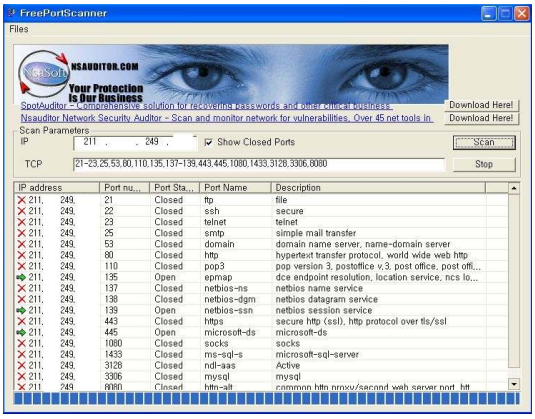


그림 4. Free Port Scanner의 scan 결과

4.4 Angry IP Scanner

Angry IP Scanner는 IP scanning tool로서 IP를 기반으로 검색하고 Host 상태와 Host Name를 알려주며, ping(응답속도)을 보여준다. 찾은 호스트로의 ftp, telnet, http, 등의 접속도 가능하다.

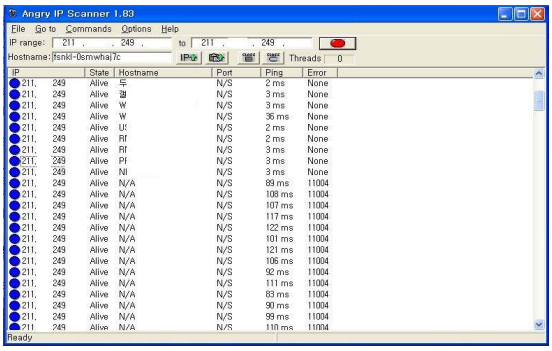


그림 5. Angry IP Scanner의 scan 결과

## V. 결 론

해커의 공격 방법이 기존의 관리자권한 획득 방식에서 서비스 거부 공격인 DoS, DDoS 공격처럼 기업이 대 고객 서비스를 운영하고 있는 운영서버들(웹 서버, DNS 서버 등)과 네트워크 장비(라우터, 방화벽 등)에 임의로 조작된 엄청난 양의 공격성 트래픽을 전송해서 시스템 자체를 지연 혹은 마비시켜 버림으로써 고객들이 기업의 서비스를 이용할 수 없게 만드는 방법으로 변모하였는데, 이는 통신구조 자체를 공격하는 것으로서 중대한 공격 중 하나이다.

이를 보완하기 위하여 인터넷의 구조적인 취약점에 있어 가장 기본적인 OSI 7 Layer에 대해 각 계층별로 어떤 취약점을 가지고 있는지 해커의 입장과 보안 담당자의 입장에서 여러 가지 Scanning 프로그램을 사용하여 각 Layer별로 Scanning을 실시하고 분석하며, 분석된 결과들에 대해 Scanning 프로그램에 대한 특성을 반영한 Scanning방법에 대한 특장점을 연구하였다.

본 논문으로 해커의 공격에 대한 취약성을 분석과 방어를 위한 보안정책 수립에 대한 자료로 활용되어 네트워크의 보안을 강화하는데 기여 하였다. 향후 연구로는 Layer별 scanning tool 제작 등을 하는 것이 필요하다.

## 참고문헌

[1] 곽미숙, 김아빈, 김윤희, “통합적인 악성코드 수집 및 모니터링 시스템의 설계 및 구현”, 한국정보기술학회논문지, 제 8권 제 2호, pp. 117-125, 2010. 2.

[2] 천준호, 신동규, 장근원, 전문석, "DDoS 공격에 대한 방화벽 로그 기록 취약점 분석", 정보보호학회논문지, 제 17권 제 6호, pp. 143-148, 2007. 12.

[3] 성경, 김석수, 박길철, “라운드로빈 부하균형을 통한 웹 서버 클러스터 고속화 처리기법”, 한국해양정보통신학회논문지, 제 8권 제 7호, pp.1524-1531, 2004. 11.

[4] S Suzuki, Y Shinjo, T Hirotsu, K Itano, K Kato, “Capability-based egress network access control by using DNS server“, Journal of Network and Computer Applications, vol. 30 no. 4, nov 2007.

[5] 최선웅, “무선 랜 성능 향상을 위한 링크 계층 트래픽 제어 알고리즘”, 한국해양정보통신학회논문지, 제 12권 제 4호, pp.758-765, 2008. 4.

[6] 이미숙, 손재근, “숙박업체 웹 사이트 서비스 품질이 고객 만족도 및 충성도에 미치는 영향”, 대한관광경영학회논문지, 제 23권 제 3호, pp.119-138, 2008. 11.

[7] Haoyu Song, Fang Hao, Murali Kodialam, “T.V. Lakshman, IPv6 Lookups using Distributed and Load Balanced Bloom Filters for 100Gbps Core Router Line Cards“, IEEE INFOCOM, 2009.

[8] 강선무, “미래인터넷 연구와 지식기반사이버 인프라”, 전자공학회지, pp.63-72, 2009. 3.

[9] 여명호, 김유미, 유재수, "무선 센서 네트워크를 위한 에너지 효율적인 이중 레이어 분산 클러스터링 기법", 정보과학회논문지, 제 35권 제 1호, pp.84-95, 2008. 2.