韓國 컴퓨터情報學會 論文誌
第13卷 第6號, 2008. 11.

2008-13-6-3-6

DoS공격에 대한 N-IDS 탐지 및 패킷 분석 연구

천 우 성*, 박 대 우**

A Study on N-IDS Detection and Packet Analysis regarding a DoS attack

Woo-Sung Chun*, Dea-Woo Park**

요 약

본 논문은 2008년에 발생했던, 금융기관과 정부기관에 대한 DoS 공격에 대한 연구이다. 실험실 환경에서 실제 DoS 공격 툴을 이용하여 공격을 실시한다. DoS 공격을 탐지하기 위하여 네트워크에서 Snort를 이용한 N-IDS를 설치한다. 패킷을 탐지하기 위한 WinPcap과 패킷의 저장 및 분석하기 위한 MySQL, HSC, .NET Framework 등을 설치한다. e-Watch 등의 패킷 분석 도구를 통해 해커의 DoS 공격에 대한 패킷량과 TCP, UDP 등의 정보, Port, MAC과 IP 정보 등을 분석한다. 본 논문 연구를 통하여 유비쿼터스 정보화 사회의 역기능인 사이버 DoS, DDoS 공격에 대한 자료를 분석하여, 공격자에 대한 포렌식자료 및 역추적 분석 자료를 생성하여, 안전한 인터넷 정보 시스템을 확보하는데 의의가 있다.

Abstract

EThis paper is study regarding banking institution and DoS attack regarding government organization which occurred in 2008. We used a tool aggressive actual DoS You install the N-IDS which used Snort in networks in order to detect a DoS attack. Storages of Winpcap and a packet to detect a packet and MySQL, HSC, to analyze. We install NET Framework etc. E-Watch etc. analyzes Packet regarding a DoS attack of a hacker and TCP, UDP etc. information, Port, MAC and IP information etc. through packet analysis tools. There is a meaning you analyze data regarding the cyber DoS, DDoS attack that is dysfunction of Ubiquitous Information Society, and it generates forensics data regarding an invader and back-tracking analysis data, and to ensure safe Internet information system through this paper study.

▸ Keyword : Forensics, Intrusion Detection, IP Traceback, Real IP, Ubiquitous Security.

• 제1저자 : 천우성 교신저자 : 박대우
• 접수일 : 2008. 7. 24, 심사일 : 2008. 10. 6, 심사완료일 : 2008. 11. 26.
* 호서대학교 벤처전문대학원 IT응용기술학과 ** 호서대학교 벤처전문대학원 교수

Ⅰ. 서 론

2008년 3월 22일 미래에셋 금융그룹 홈페이지가 중국이 본거지인 것으로 추정되는 해커들로부터 공격을 받은 뒤, 미래에셋 측에 전화와 메신저를 통해 5000만원을 보내라고 요구했다. 미래에셋 증권 관계자는 "한국어를 구사하는 사람이 5000만원을 요구했으며 응하지 않을 경우 추가 공격을 하겠다고 위협했다"고 말했다."[1]

DoS 공격[2]은 특정 네트워크에 한꺼번에 대량의 정보를 보내 허용하는 대역폭을 모두 감소시키거나 공격대상 시스템의 자원을 고갈시켜 서비스를 못하도록 한다. 봇(Bot)은 운영체제의 취약점, 웜·바이러스의 백도어 등을 이용해 전파되는 프로그램이나 실행코드. 명령 전달 사이트와 백도어 연결 등을 통해 스팸메일 전송이나 DDoS 공격[3]에 악용되고 있다. DDOS공격 같은 분산서비스거부공격은 그림 1처럼 봇과 좀비로 감염시킨 합법적인 호스트들을 이용하기 때문에 사전에 탐지하기 어렵고, 효율적인 방어가 어렵다는 문제가 있다.

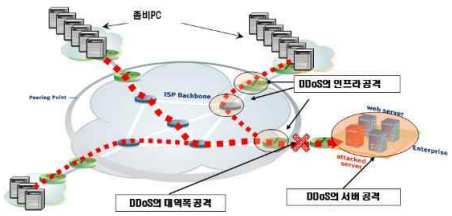

그림 1. DDoS 공격 형태
Fig 1. DDoS Attack Form

악성봇의 증가도 인터넷 보안을 크게 위협하고 있다. 악성봇에 감염된 PC가 특정 사이트를 대상으로 한 DDoS 공격에 악용되고 있어 대책 마련이 시급하다.

본 논문에서는 최근에 주공격의 대상이 되는 DoS공격에 대한 연구 분석을 실시하여, 해커의 DoS공격 툴을 이용하고 공격을 실시하고, 이를 패킷을 통해 분석하며, 분석된 패킷 분석의 내용을 통하여 DoS공격을 차단 할 수 있는 방안을 도출하여 해커의 DoS공격으로부터 안전한 네트워크 자원을 유지하는데 의의가 있다. 우리 주변에서 발생 하고 있는 해킹 사고 사례와 나날이 발전해가는 해킹 방법의 동향, 이러한 불법 침입을 이용한 침입 탐지 기법들과 네트워크에 관련한 침입탐지 방안기술 그리고 그 패킷들의 경향을 분석하는데 그 의의가 있다.

Ⅱ. 관련 연구

2.1. 해킹(Hacking)

해킹의 법률적 의미는 시스템의 관리자가 구축해 놓은 보안망을 어떤 목적에서건 무력화시켰을 경우 이에 따른 모든 행동을 해킹이라고 한다. 결국 비인가자에 의한 컴퓨터의 부당한 사용, 자료의 불법적인 열람, 유출, 변조, 삭제 및 컴퓨터시스템의 정상적인 동작과 서비스를 방해하는 해킹 범죄 행위를 말한다. 또한 다른 사람의 시스템에 몰래 침투, 사용하거나 그 속의 정보를 변조하는 행위인 시스템 해킹이 있다. 그 수법으로는 지금까지 트로이(Trojan Horse) 프로그램을 이용한 방법[4], 호스트 프로그램의 버그(Bug)나 약점을 이용한 방법[5], 특정 사용자의 암호를 이용한 방법[6] 등이 노출돼 있다.

2.2. DoS, DDoS 공격

DoS, DDoS 공격은 특정 네트워크에 한꺼번에 대량의 정보를 보내 허용하는 대역폭을 모두 감소시키거나 공격대상 시스템의 자원인 메모리, CPU 등을 고갈시켜 서비스를 못하도록 한다.

봇(Bot)은 운영체제의 취약점, 웜·바이러스의 백도어 등을 이용해 전파되는 프로그램이나 실행코드. 명령 전달 사이트와 백도어 연결 등을 통해 스팸메일[6] 전송이나 DDoS 공격에 악용되고 있다.

최근에는 DoS용 에이전트를 여러 개의 시스템에 설치하고, 에이전트를 제어해 공격자에 대한 추적을 불가능하게 하는 수법이 동원되고 있다. 그림 2처럼 DDOS공격 같은 분산서비스거부공격은 봇과 좀비로 감염시킨 합법적인 호스트들을 이용하기 때문에 사전에 탐지하기 어렵고, 효율적인 방어가 어렵다는 문제가 있다. DDOS공격은 매우 다양한 공격이 가능하고, 즉시 주목할 만한 결과를 얻을 수 있으며, 공격 방법으로는 smurf, trinoo, SYN Flooding 등이 있다[7].

DDoS 공격은 그 수법이 단순하지만, DDoS 전용 보안 장비를 설치하지 않을 경우, 위험하다. 아이템거래사이트, P2P 사이트 등을 대상으로 DDoS 공격이 시도하고, 공격 중지를 대가로 피해 업체에 금전을 요구하고 있어, 해당 업체는 서비스 중지로 인한 금전적 손실은 물론 심리적인 협박 등을 겪고 있는 실정이다.

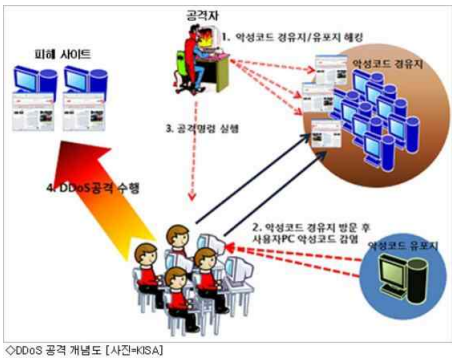

그림 2. DDoS 공격 개념도[KISA]
Fig 2. DDoS Attack Conceptualism

2.2.1. DoS 5.5 Final

인터넷상에서 유포되고 있는 DoS 공격 프로그램으로써 백신프로그램에서 이 프로그램을 감지 할 수 있다. 이 프로그램은 많은 해킹 사이트에서 다운 있는데 간단하게 패킷량[8]을 도스 커멘드 윈도우에 입력하는 방식으로 패킷량을 증가시켜 공격하는 툴로써 이 프로그램을 스파이웨어식[9]으로 다른 컴퓨터에 심어놓아 한순간 같은 시간에 같은 곳을 공격하게 하는 것이 DDoS공격이며 그것을 한 개인의 사양에 맞춰 공격할 수 있게 만든 프로그램이다.

2.3. 공격 대상 중요 자원

2.3.1. CPU

컴퓨터의 가장 중요한 부분으로, 프로그램의 명령을 해독하여 그에 따라 실행하는 장치. 컴퓨터에서 구성단위 중 기억, 연산, 제어의 3대 기능을 종합하는 것이라고 할 수 있다. 입출력 장치, 외부 기억 장치와 더불어 컴퓨터 시스템을 구성한다.

2.3.2. Memory

컴퓨터를 비롯한 디지털 기기에서 매우 중요한 장치인 디지털 기억 장치를 가리키는 용어. 컴퓨터에서는 내부 기억 장치와 외부 기억 장치로 분류된다. 기억 장치의 종류에는 집적 회로(IC)를 이용한 반도체 기억 장치, 자기 기록 방식을 응용한 자기 기억 장치, 광디스크를 이용한 광 기억 장치 등이 있다.

2.3.3. Packet

데이터 전송에서 사용되는 데이터의 묶음. 패킷 전송은 두 지점 사이에 데이터를 연속적으로 전송하지 않고, 전송할 데이터를 적당한 크기로 나누어 패킷의 형태로 구성한 다음 패킷들을 하나씩 보내는 방법을 사용한다. 각각의 패킷은 일정한 크기의 데이터뿐만 아니라 데이터 수신처, 주소 또는 제어부호 등의 제어 정보까지 담고 있다. 보통 한 패킷은 1,024비트의 데이터를 담을 수 있다.

2.3.4 Traffic

전신, 전화 등의 통신 시설에서 통신의 흐름. 개개의 호 보류 시간에 관계없이 발생한 호의 수를 호 수라고 하고, 호 수와 평균 보류 시간의 곱을 트래픽 양, 단위 시간당 트래픽양을 트래픽 밀도라고 한다. 트래픽양의 단위를 얼랑(ERL)이라고 한다. 1얼랑은 1회선이 전송할 수 있는 최대 호량, 즉 단위 시간 내에 1회선이 쉴 새 없이 점유될 때의 트래픽양이다. 또 1/36얼랑을 100초호(秒呼)라고 한다.

2.4. 패킷 분석 도구

2.4.1. e-Watch

링크 상에 존재하는 모든 패킷을 읽어 들여 분석한다. 이때 MAC주소[10] 또는 IP주소[11]를 사용하거나 프로토콜을 이용하여 패킷을 선별적으로 수집한다. IP 주소 필터는 IP 패킷 중에서 송신지 IP주소나 수신지 IP주소가 필터에 설정되어 있는 해당 IP 주소가 같을 경우에만 수집하고 다를 경우에는 수집하지 않는다. 마찬가지로 MAC주소 필터링과 프로토콜 필터링 또한 마찬가지로 설정되어 있는 필터링 내용과 인터페이스 카드로부터 드라이버를 통해 수신한 패킷 의 해당 내용이 동일할 경우만 패킷을 수집한다. 그림 3에서와 같이 e-Watch는 거의 모든 표 준 프로토콜을 분해/분석할 수 있으며, 특히 내장된 SNMP 컴파일러는 네트워크 관리 시 전송되는 SNMP의 오브젝트들을 분석할 수 있다. 또한 e-Watch는 멀티 스레드 방식으로 설계되어 있어, 패킷 분석과 및 표시를 동시에 수행 가능하다. 그리고 패킷 수집한 결과를 보여주는 창은 요약, 상세, 및 16진수코드를 보여주는 창으로 구분되어 있고 수집된 패킷의 내용은 각 창에 표시되며, 이들은 상호 연동된다. 수집된 패킷은 파일로 저장이 가능하며, 저장된 패킷을 선택하면 패킷의 내용을 볼 수 있다.

2.5. 정보보호시스템 IDS, IPS

2.51. IDS(Intrusion Detection System)

컴퓨터 내부 네트워크와 시스템의 비정상적인 사용, 오용, 남용 등을 실시간으로 탐지하는 시스템으로, 내부 사용자의 불법적인 행동(기밀 유출 등)에 대해 네트워크 패킷을 탐지하는 N-IDS와 내부의 중용한 자원인 서버 등을 집중 감시하고 침입을 탐지하는 HIDS가 있다.

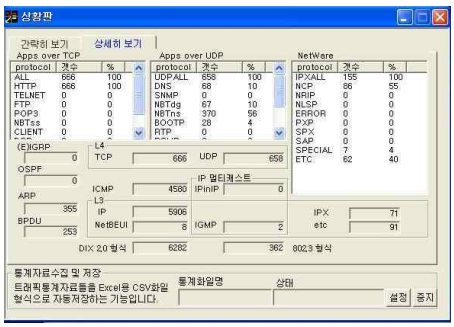

그림 3. e-Watch 패킷분석도구
Fig 3. e-Watch Packet Analysis tool

탐지방법으로는 해커의 행동패턴을 룰로 저장하여 비교하는 오용탐지(Misuse Detection)[12]와 통계적인 침입을 계산하여 임계치를 벗어나는 사건을 탐지하는 비정상탐지(Anomaly Detection)방법 등이 있다.

2.5.2. IPS(Intrusion Prevention System)

IPS(침입방지시스템)는 네트워크에서 공격 서명을 찾아내어 자동으로 보안 조치를 취함으로써 비정상적인 트래픽을 중단시키는 보안 솔루션. 수동적인 방어 개념의 침입 차단 시스템이나 IDS(침입탐지시스템)의 약점인 침입 경고 이전에 공격을 중단시키는 데 초점을 둔, 침입 유도 기능과 자동 대처 기능이 합쳐진 개념의 솔루션이다. 또한 해당 서버의 비정상적인 행동에 따른 정보 유출을 자동으로 탐지하여 차단 조치를 취함으로써 인가자의 비정상 행위를 통제할 수 있다. 그림 4와 같은 환경으로 이루어진다.

III. DoS공격 툴, N-IDS, 패킷분석 설치

DoS공격 툴과 N-IDS 및 패킷분석기 툴을 설치하고 실험할 환경은 그림 4와 같이 구성되어져 있다.

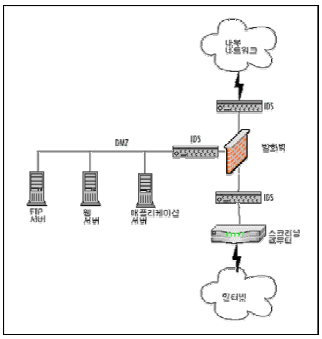

그림 4. 연구 환경
Fig 4. Research & Development System

3.1. DoS 공격 툴 설치

DoS공격 툴을 실행하게 하기 위해서는 백신프로그램을 일시적으로 정지 시키고 설치하고 실행을 시켜야 한다. 공격 툴을 백신프로그램에 감지하여 치료 시에 삭제되기 때문이다. 그림 5는 DoS 5.5 버전을 실행한 화면이다.

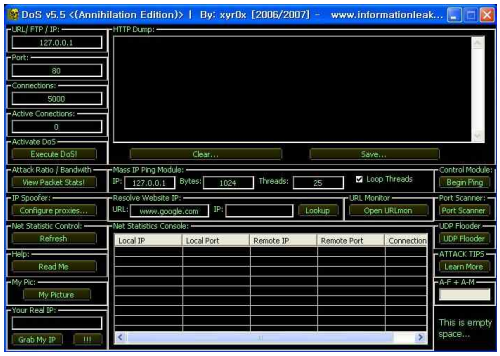

그림 5. DoS 공격 툴
Fig 5. DoS Attack Tool

3.2. N-IDS 설치

IDS의 기능을 가지고 있는 Snort 는 실시간 트래픽 분석과 IP 네트워크 상에서 패킷 로깅이 가능한 네트워크 침입 탐지 시스템으로 패킷 수집 라이브러리인 libpcap에 기반한 네트워크 스니핑(Sniffing) 엔진과 손쉽게 편집 가능한 탐지 rule을 통해, 네트워크 트래픽을 감시하고 보안 위반 사항을 모니터링 할 수 있는 도구이다. Snort는 프로토콜 분석, 내용 검색과 매칭, 버퍼오버플로우 공격, 포트스캐닝, CGI 공격, SMB 스캐닝, OS 정보 획득 시도 등의 다양한 공격과 스캐닝을 탐지할 수 있다.

3.2.1. WinPcap 설치

WinPcap은 범용 패킷 캡처 라이브러리인 libpcap의 window 버전으로 Snort가 패킷 캡처를 수행하기 위해 반드시 필요하다. WinPcap 최신버전[13]을 더블 클릭하면 자동으로 설치되며 별도의 설정 없이 간편하게 사용 가능하다.

3.2.2. MySQL 설치

MySQL은 경량 DBMS로 Snort의 로그나 이벤트를 저장하기 위해 연동된다. MySQL 5 는 최근까지 개발 버전이었으며 Snort 2.4.3 과의 연동에 일부 문제가 있다. MySQL 4.1.15 는 현재 시점에서 안정 버전 중 최신 버전[14]이므로 이 버전을 사용하여 설치한다.

3.2.3. Snort 설치

Snort 최신버전[15]을 설치한다. 설치 프로그램의 GPL 라이센스 확인에 동의하고 나면 아래와 같이 DB 연동 설정에서는 MySQL과 연동할 예정이므로 디폴트 값을 그대로 선택한다.

설치할 패키지도 디폴트로 선택하고 Snort 설치 디렉터리를 묻는 화면이 나오면 자신이 원하는 다른 디렉터리를 선택해준다. Snort 설정 파일에서 해당 디렉터리의 절대 경로를 참조하기 때문에, Snort 설정을 편하게 하기 위해서는 디폴트 값인 C:₩Snort를 선택하여 설치한다. Snort는 설정 과정이 Linux 환경이 디폴트이며 Windows에서 사용하려면 설정과정을 거쳐야 한다. 그림 6은 Snort를 실행시켜 패킷을 탐지하고 있는 화면이다.

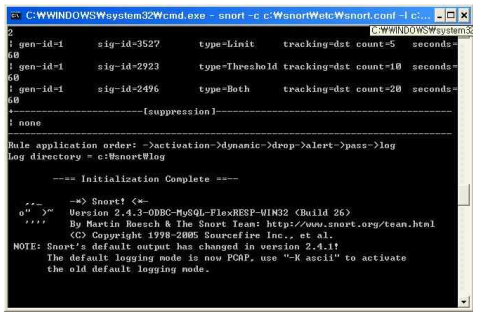

그림 6. Snort
Fig 6. Snort

3.2.5. .NET Framework HoneyNet 설치

컴퓨터에 이미 .NET Framework 가 깔려있다면 아무 문제가 없으나 깔려있지 않다면 마이크로소프트 사이트에서 .NET Framework 1.1[16] 재배포 가능 버전을 다운받아 설치하고, 필히 윈도우 업데이트를 수행하여 .NET Framework 1.1 서비스팩(SP 1)을 설치한다.

3.2.5. .NET Framework HoneyNet 설치

HSC(Honeynet Security Console)[17]은 IDS, 방화벽 로그, Unix 시스템의 syslog, TCPDump 등 다양한 보안 도구의 로그 정보를 취합하여 실시간 모니터링을 수행할 수 있도록 설계된 시스템으로 일종의 ESM 시스템이다. Snort IDS와의 연동을 염두에 두고 다양한 통계 정보, 패킷 분석, nslookup, whois, ping 등 침입자 역추적에 필요한 네트워크 유틸리티 지원 기능을 포함하고 있으며, 상관관계 분석 기능을 제공하여 발생된 이벤트에 대한 상세 분석을 지원한다.

HSC가 내부적으로 .NET Framework에 의존하기 때문이다. 이제 activeworx 사 홈페이지에서 HSC을 다운받아 설치한다.

라이센스와 사용자명과 소속 기관 부분에 대해 적절한 값을 선택하여 다음으로 넘어간다. 설치 디렉터리는 적절한 디렉터리로 변경해주거나 디폴트 상태에서 다음을 선택한다.

이후에 나오는 화면에서 [install]을 선택하면 아래와 같이 최종 설치가 완료된다.

그림 7은 허니넷을 실행하여 자신의 컴퓨터주소로 들어오는 패킷들을 탐지해내서 GUI형식 그림형식으로 보여지고 있다.

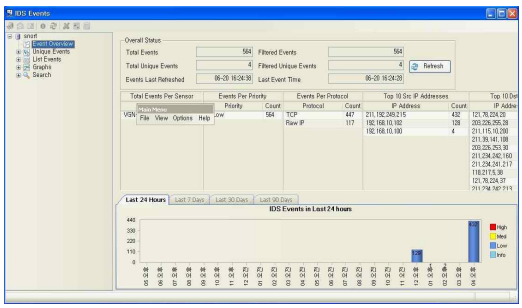

그림 7. 허니넷
Fig 7. HoneyNet

3.3. 패킷 분석 도구(e-Watch) 설치

별도의 설치 과정 없이 실행파일만 실행하면 처음에 NIC값을 찾는데 거기에서 자신의 네트워크 카드가 무엇인지 설정해주고 접속하면 된다. 실행 후 프로그램에서 환경설정만 해주면 된다. 그림 8과 같이 설치가 된 화면이다. 이제 패킷 수집을 시작하면 패킷을 수집하게 되고 그 수집과정을 볼 수 있다.

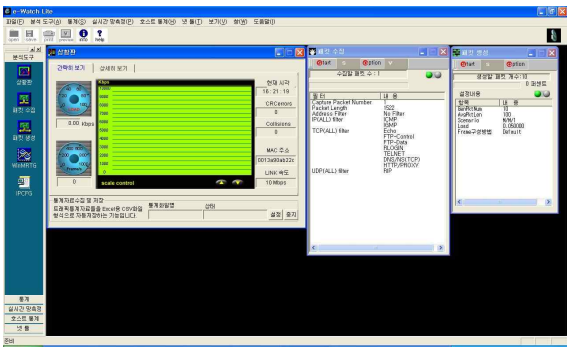

그림 8. e-Watch
Fig 8. e-Watch

Ⅳ. DoS공격과 N-IDS 침입탐지 및 패킷분석 연구

4.1. DoS 공격

인터넷 네트워크에서 해커의 Real IP를 숨기기 위해, 목표 웹서버에 우회 접속한 다음, 이메일, 유해성 게시물을 통한 접속을 하고, 웹서버의 권한 탈취하여 해킹으로 이어진다. 그림 9에서 DoS공격은 커멘드 윈도우에 PING을 증가시켜서 한 IP로만 일정량의 패킷들을 정해진 시간에 계속 보내는 것이다. 이것이 많아지면 네트워크 트래픽을 처리하는 허용되는 용량을 벗어나게 되면 네트워크 처리 가용성이 줄어들어 시스템이 다운이 되는 것이다.

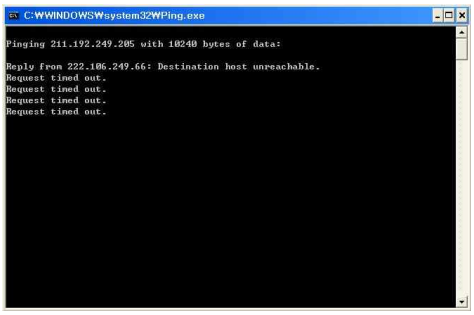

그림 9. Ping 공격
Fig 9. Ping Attack

4.2. N-IDS 침입탐지

4.2.1. DoS 공격 탐지

다른 컴퓨터에서 DoS 패킷 공격이 시작되면 Snort와 e-Watch에서 그 패킷을 수집하게 되고, Snort에서 패킷을 수집한 것을 GUI로 보여주기 위해 HoneyNet과 연동하여 보여지고, DB에 저장하게 되며 Snort 룰과 비교를 하여 패킷의 위험도를 색깔별로 표시되어 HoneyNet에 보인다. e-Watch는 그 패킷의 정보량과 지금 네트워크 상태를 보여준다.

4.3. Dos공격에 대한 N-IDS 탐지 분석

4.3.1. DDoS 공격 탐지 및 차단 분석

HoneyNet과 e-Watch에서 모니터링하면서 HoneyNet에서 위험성이 있는 패킷의 IP 주소를 알아낼 수 있고 그것에 대해 대응할 수 있다. e-Watch에서는 패킷량을 볼 수 있는데 패킷의 용량이 유난히 많은 패킷에 IP주소를 알 수 있고 그것에 대해 대응할 수 있다. 그림 10과 같이 패킷량이 급격히 증가됨을 알 수 있는데 이것이 DoS 공격을 받고 있다는 것이다.

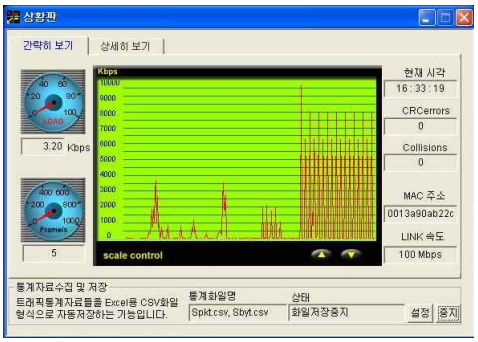

그림 10. DoS 공격 탐지
Fig 10. DoS Attack Detect

4.4. Dos공격에 대한 N-IDS 탐지 패킷 분석

4.4.1. IP Spoofing 공격 탐지 및 차단 분석

HoneyNet에서 패킷의 위험도에 따라 색깔을 다르게 하여 그 패킷의 그 등급이 나눠지며 이것을 바탕으로 하여 이미 DB에 저장되어 있거나 Rule파일과 같이 지금까지의 해킹 패턴들을 모아놓은 자료에서 분석을 하여 위험성을 알 수 있다.

DoS 공격이 탐지된 패킷은 본 논문의 분석 결과로 공격을 하고 있는 시스템의 Scr IP주소를 알 수 있고, MAC주소도 모니터링 할 수 있으며, 현재 공격에 이용되는 서비스를 포트를 통해서 알 수 있다. DoS 공격에 따른 위험도를 분석하고 위험순위(Priority)를 분석하여 공격자의 IP와 연결되어 있는 통신망을 역추적을 한다.

WhoIS를 이용하여 공격자의 위치를 찾거나, 경찰청 사이버테러대응센터, KISA의 CERT/CC에 공격자에 대한 통보를 하여, 인터넷망을 차단하거나 게이트웨이에서 그 프로토콜을 차단하는 등 자신의 자원을 보호한다.

그림 11과 그림 12와 같이 DoS 공격을 탐지하여 모니터링 하는 것으로 DoS 공격에 따른 패킷량이 늘어나고 패킷의 용량도 확인할 수 있고 IP주소와 MAC 주소도 모니터링 함으로써 시스템의 취약부분을 확인하고 외부의 공격으로부터 내부 자원들을 보호하기 위해 모니터하는 것이다. 패킷의 용

량을 높이는 것은 영상파일이나 음악 파일이고 이 파일들은 한 번에 정보전송용량을 초과하는 네트워크 트래픽을 유발시켜 CPU, 메모리, 라우터 등의 정보처리 능력을 저해시킬 수 있는 방법으로 사용된다.

또 다른 방법은 일정량의 패킷을 한 번에 여러 우회 경로의 Agent등을 통하여 동시에 여러 번 DDoS 공격을 실행하는 방식이 있다. DDoS공격은 서비스의 가용성 자원을 마비시키는 공격으로 패킷들의 무차별한 트래픽 유도로 인해 발생하는 것을 볼 수 있다.

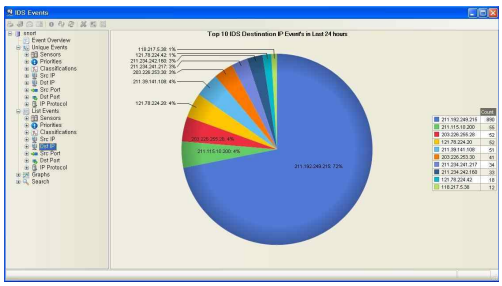

그림 11. DoS 패킷 분석
Fig 11. DoS Packet Analysis

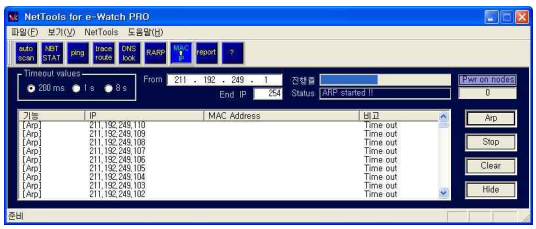

그림 12. IP 주소와 MAC 주소 찾기
Fig 12. Trace of IP Address to MAC Address

V. 결론

본 논문에서는 정보화 사회에 대한 역기능으로 불법적인 해킹, 정보유출, 프라이버시 침해, 금융적인 피해 등이 지속적으로 확산되고 있는 상황에서 DoS 공격에 대한 모니터링과 그 패킷에 대한 탐지와 분석 연구이다. 실험실 환경에서 실제 DoS 공격 툴을 이용하여 공격을 실시한다. DoS 공격을 탐지하기 위하여 네트워크 상에서 Snort를 이용한 N-IDS를 설치하고, 패킷을 탐지하기 위한 WinPcap과 패킷의 저장 및 분석하기 위한 MySQL, HSC, .NET Framework 등을 설치한다. e-Watch 등의 패킷 분석 도구를 통해 해커의 DoS 공격에 대한 패킷량과 TCP, UDP 등의 정보, Port, MAC과 IP 정보 등을 분석한다. 일반적인 IP 접속 자료와 침입탐지 후에 치명적인 공격은 Green, Yellow, Orange, Red 등급으로 분류하여 Red 등급으로 분류되어 차단된 패킷의 Real IP 자료를 실시간으로 모니터링하고 그 자료의 MAC 주소까지 파악했다. 본 논문 연구를 통하여 유비쿼터스 정보화 사회의 역기능인 사이버 DoS, DDoS 공격에 대한 자료를 분석하여 공격자에 대한 포렌식자료 및 역추적 분석 자료를 생성하여 안전한 인터넷 정보 시스템을 확보하는데 의의가 있다.

향후 연구에서는 유비쿼터스와 IPv6 환경에서의 다양한 해커의 침입에 대한 실시간 Real IP 역추적에 대한 연구와 그 패킷의 정보량을 제한을 두어 서비스가 중지되는 현상을 막는데 대한 연구가 필요하다.

참고문헌

[1] 중국서 미래에셋 홈페이지 해킹. 사회. 중앙일보. 최현철기자. http://article.joins.com/article/article.asp?Total_ID=3083429 2008. 03. 22.

[2] 천재홍, 박대우. “VoIP의 DoS 공격 차단을 위한 IPS의 동적 업데이트엔진”.한국컴퓨터정보학회 논문지, 제10권 제5호, pp217-226, 2006.12.

[3] Christos Siaterlis , Vasilis Maglaris, One step ahead to multisensor data fusion for DDoS detection, Journal of Computer Security, v.13 n.5, p.779-806, October 2005.

[4] Y. Zhang and V. Paxson, “Detecting Stepping Stones,”Proceedings of 9th USENIX Security Symposium, Aug. 2000.

[5] 박대우, 임승린. “해커의 공격에 대한 지능적 연계 침입방지시스템의 연구”. 한국컴퓨터정보학회논문지. 2006.05

[6] 이인희, 박대우. “VoIP 서비스의 스팸 공격에 대한 차단 연구.” 한국컴퓨터정보학회논문지, 제11권 제5호. 2006. 11.

[7] http://www.kisa.or.kr 한국정보보호진흥원. 2008. 5.

[8] 이준엽 외 4인, “IP역추적을 위한 새로운 접근: 패킷손실 기반의 논리적 전송경로 추정” 한국정보보호학회 논문지, 제12권 3호, 2002. 6.

[9] 박대우, 서정만. “Phishing, Vishing, SMiShing 공격에서 공인인증을 통한 정보침해 방지 연구”.한국컴퓨터정보학회 논문지, 제12권 제2호, pp175-184,

2007. 5.
[10] 김태봉, 최운호, “역추적 기술의 동향 및 적용 사례 분석” 한국정보보호학회, 제15권1호. 2005. 2.
[11] 박대우, 서정만. ‘TCP/IP 공격에 대한 보안 방법 연구.’ 한국컴퓨터정보학회논문지, 제10권 제5호, pp217-226, 2005. 11.
[12] Deawoo Park. "A study about dynamic intelligent network security systems to decrease by malicious traffic". International Journal of Computer Science and Network Security, V.6, N.9B. pp 193-199. Sep. 2006.
[13] Winpcap. http://www.winpcap.org 2008. 5.
[14] MySQL. http://www.mysql.org 2007. 11.
[15] Snort. http://www.snort.org 2008. 3.
[16] .NET Framework 1.1. http://www.microsoft.com 2007.
[17] Honeynet Security Console. http://www.activeworx.org 2008. 4.

저 자 소 개

천 우 성

2006년 숭실대학교 전산원 졸업
2006년 한국교육개발원 멀티미디어학 전공 (공학사)
2008년 호서대학교 벤처전문대학원 IT응용기술학과 (석사과정)
<관심분야> 정보보호, 역추적기법, 공격패킷 분석, 유비쿼터스 보안

박 대 우

1998년 숭실대학교 컴퓨터학과(공학석사)
2004년 숭실대학교 컴퓨터학과(공학박사)
2000년 매직캐슬정보통신 연구소 소장, 부사장
2004년 숭실대학원 정보과학대학원 정보보안학과 겸임조교수
2006년 정보보호진흥원(KISA) 선임연구원
2007년 호서대학교 벤처전문대학원 조교수
<관심분야> 정보보호, 유비쿼터스 네트워크 및 보안, 보안 시스템, CERT/CC, Forensic, VoIP 보안, 이동통신 및 WiBro 보안, Cyber Reality, IT-Convergence