스니핑 기술을 이용한 데이터 통신 프로토콜 분석 및 시각화에 대한 연구

송무송[1], 조은진[2], 한해리[3], {박진호, 김영종}[*]
[1,2,3,*]숭실대학교 소프트웨어학부
e-mail: songe08@gmail.com, 98dmswls@naver.com,
hanhaeri3934@naver.com, {j.park, youngjong}@ssu.ac.kr

A Study on analysis and visualization of data communication protocol by using Sniffing technology.

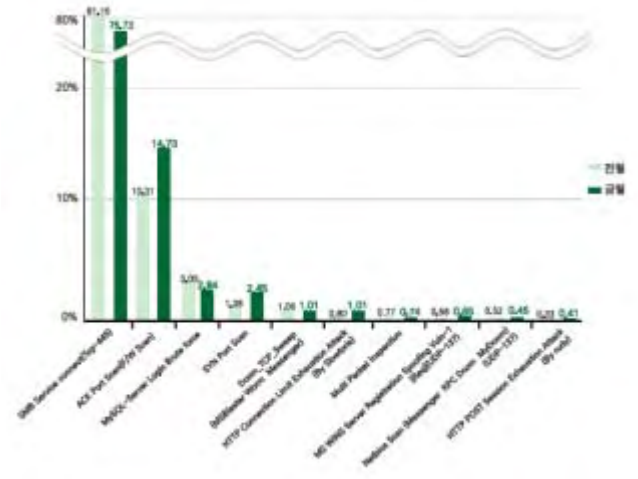
MooSong Song[1], EunJin cho[2], HaeRi Han[3], {Jinho Park, Youngjong Kim}[*]
[1,2,3,*]School of Software, Soongsil University

요 약

데이터가 오고 가는 네트워크를 사용하는 곳들에서는 패킷을 필히 수집하고 분석한다. 하지만 패킷 스캐닝을 통해 공격 대상에 대한 정보를 수집하고 2차적 공격 시나리오를 구상하는데 악용하는 경우가 발생한다. 본 시스템은 IP/TCP를 중심으로 패킷분석에 대한 전문적인 지식이 없어도 쉽게 확인 가능한 프로그램을 제공할 예정이다.

1. 서론

최근 '이글루시큐리티'에서 발표한 자료에 따르면, "ACK Port Scan(F/W Scan), MySQL-Server Login·Brute force의 순위가 상승했고, 대부분의 공격이 스캐닝 이벤트인 것으로 확인된다."고 밝혔다.



위의 자료에서 두드러지게 드러나는 SMB Service connect(TCP-445)의 경우, TCP/IP를 통해 NetBIOS 상에서 실행되는 SMB 공유를 악용하는 것으로, TCP포트 445 상에서 TCP/IP를 통해 직접 SMB에 접근하여 운영, 공격 대상이 파일 공유를 실행할 경우 공격자에 의해 2차적인 공격이 야기될 수 있다.

ACK Port Scan란 방화벽에서 불필요하게 허용중인 취약 포트를 스캔하는 공격으로, 공격자는 특정 패킷을 서버에 보내고, 돌아오는 응답·패킷을 분석해 취약한 포트의 정보를 수집할 수 있다.

SYN Port Scan은 해킹을 목적으로 공격 대상이 TCP/IP의 포트를 열어 서비스를 하는지 알아내기 위한 방법으로, 포트번호를 무작위로 SYN를 보내 서버가 응답하는 SYN/ACK를 확인한다.

즉 활발히 이용되는 공격들은 시스템을 직접적으로 파괴하는 것이 목적이 아니다. 오히려 오고 가는 패킷들을 분석하여, 공격 대상에 대한 정보를 수집해 2차적인 공격 시나리오를 계획하기 위한 목적으로 이용된다. 따라서 개발자는 접근 가능한 미사용 포트 현황을 파악할 필요가 있으며, 각종 기기 및 서버 점검 등의 보안에 주의를 기울여야 한다. 이에 필자는 대부분의 공격이 TCP/IP 프로토콜을 중심으로 이루어진다는 것에 중점을 두고, 프로토콜을 시각적으로 구현하고 보안에 대한 중요성을 파악해보려 한다.

2. 본론

2.1. 기존 패킷 분석기의 특징

기존 패킷 분석에 주로 사용되는 'Wire Shark'는 서로 다른 네트워크 프로토콜의 구조를 파악하고 각 네트워크 프로토콜이 규정한 패킷의 요약 정보를 보여주는 소프트웨어이다. 기본적인 기능은 실시간 네트워크로 데이터를 포획하고, 패킷으로부터 데이터를 읽을 수 있으며, 포획한 네트워크 데이터는 GUI나 터미널을 통해 탐색이 가능하다.

그러나 기존의 패킷분석기가 가지고 있는 특징은 프로토콜의 다양성이라는 장점을 유지하기 위해, 데이터 표현에 대한 디스플레이가 사용자 친화적이지 않다. 또한 전문적 지식이 뒷받침되지 않으면 해당 패킷을 분석한 결과 데이터도 일반인들에게는 이해될 수 없다는 단점이 있다.

2.2. 패킷 시각화 프로그램 구현 시 요구사항

따라서 필자가 구현하고자 하는 패킷 스니핑 프로그램은 기존의 패킷 분석 프로그램과 차별점을 두어, 전문적 지식이 전무한 일반인들도 편리하게 사용할 수 있는 패킷 분석 프로그램으로서 시각화 될 예정이다.

구현하고자 하는 프로그램은 기존의 패킷 분석기가 제공해주는 기능과 같이 순서대로 패킷을 나열하며, 해당 패킷의 프로토콜 종류를 명시한다. 또한 mac 및 port number와 capture time을 명시함으로 서 기본적인 패킷 분석기의 기능을 갖출 예정이다.

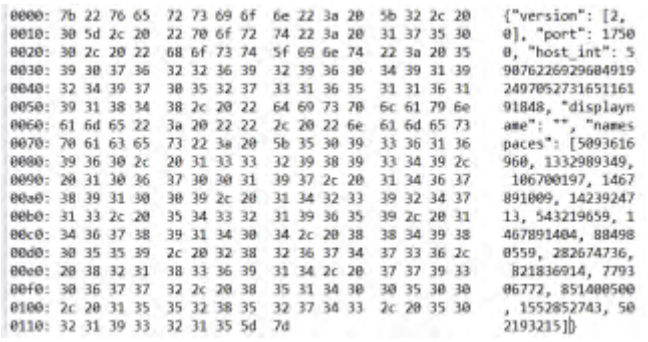
그러나 기존 패킷 분석기에서는 단순히 Source IP 와 Destination IP에 대한 단순한 정보만을 보여주었다면, 해당 프로그램의 User의 local address를 파악하여 이를 중심으로 사용자 친화적이게 User – Sever 의 구조로서 시각화할 예정이다.

이에 더해, 도메인 네임, 데이터 사이즈 및 total size, 라스트 패킷 타임, duration 또한 메인 화면에서 제공함으로써 패킷 분석에 대한 용이함을 제공할 예정이다.

2.3. 구현 방식 요약

우선적으로 사용자 친화적인 인터페이스를 구현하기 위한 목적과 시각적으로 편리한 인터페이스를 구현하기 위한 목적이 있기 때문에, JAVA로 패킷 스니핑 프로그램을 구현할 것이다.

C와 C++을 기반으로 한 pcap을 이용하여 구현했던 기존의 Wire Shark와 달리, JAVA를 기반으로 패키 스니핑 기술을 구체화해야 한다. 따라서 libpcap과 winpcap의 래퍼 라이브러리인 jnetpcap을 사용하여 프로그램을 구현할 것이다.



▲캡처한 패킷. - 헥사값임을 확인 가능

jnetpcap 라이브러리를 이용하여 캡처한 패킷 정보들은 정제되어있지 않은 헥사값이다. 따라서 필자는 정제되어있지 않은 헥사값에서 IP header 부분을 찾아내어 그 구조에 맞게 분할하여 분석한다. 분석 내용을 바탕으로 TCP프로토콜을 사용하는 패킷만을 남기고 다른 패킷들은 제거한다. 그 후 IP Datagram부분을 TCP header와 data 부분으로 분할하고, TCP header 구조에 맞게 분석한다. 이후 분석한 내용을 사용자가 쉽게 정보들을 파악할 수 있도록 보다 더 사용자 친화적인 인터페이스로서 구현한다.

ACKNOWLEDGMENT

"본 연구는 과학기술정보통신부 및 정보통신기술진흥센터의 SW중심대학사업의 연구결과로 수행되었음 (2018-0-00209-001)"

참고문헌

[1] 이글루시큐리티, "월간 공격 서비스 동향 및 분석", 월간보안동향 2019 02월호, p8-p13

[2] 홍승표, 김규완, 김재민, 우민정, 오득환, 이해연 (2018). 실시간 패킷 분석 시스템 개발. Proceedings of KIIT Summer Conference, 265-266.

[3] 임솔, 이계주, 김소연, 황인태, 김대진 (2014). IEEE 802.15.4a IR-UWB 패킷 분석기 설계 및 구현. 한국 정보통신학회논문지, 18(12), 2857-2863.

[4] 김경애, "11월 가장 빈번했던 사이버공격 유형 5가지", 보안뉴스, 2018년 12월 5일자, https://www.boannews.com