컴퓨터 네트워크 팀 프로젝트

- Raw socket을 활용한 패킷 분석 프로그램

9팀
2017152022 안윤빈
2015154023 양현용
2016156035 채윤원
2015154040 한승훈

설계 목표

- 네트워크 상에서 전달되는 **패킷을 캡처, 분석**하는 raw socket 프로그램 구현
- 구현된 프로그램으로 **세가지 프로토콜(http, dns, smtp)**에서 송수신되는 **패킷을 분석**
- 프로그램**(traceroute)**에서 경유되는 라우터들 간에 송수신되는 **패킷을 분석**
- 올바른 결과를 확인하기 위해 **와이어샤크(Wireshark)와 비교**

설계 환경

OS : 리눅스(유닉스)

구현 언어 : C

설계 방향

- C언어로 리눅스 환경에서 RAW SOCKET을 이용해 통신하는 클라이언트 프로그램 생성
- 생성된 클라이언트 프로그램으로 http, dns, smtp, traceroute에서 송수신되는 패킷 캡처
- 캡처된 패킷 헤더(TCP, UDP, IP, Application)를 분석하며 송수신 과정을 이해

설계 내용

1. 클라이언트와 서버 사이에 송수신되는 **패킷을 캡처**한다.

2. 패킷에 대한 **정보**를 프로그램이 넘겨 받는다.

3. **헤더의 정보**를 읽어 **네트워크 계층**의 프로토콜을 분류한다.

4. **트랜스포트 계층**의 프로토콜을 분류한다.

5. **응용 프로그램 계층**의 프로토콜을 분류한다.

6. 각 프로토콜의 **헤더정보**와 **페이로드 데이터**를 프로그램 화면에 출력한다.

기대 효과

✓ 구현한 분석 프로그램을 사용해 각 계층의 헤더 부분에 존재하는 여러 가지 패킷들을 분석하며 강의에서 배웠던 네트워크의 내부 흐름에 대한 세부적인 지식 획득

✓ 패킷 캡처, 분석 프로그램을 raw socket을 사용해 직접 구현하면서 해당 프로그램의 내부적인 동작 과정과 동작에 필요한 지식 학습