2020년 5월 17일 일요일

5월 셋째 주(성준)

유해사이트 차단 우회

<이번주 진행 상황>

ip,tcp 헤더 조작을 위해 raw socket을 사용하는데, raw socket 코드 작성에 앞서 패킷에 필요한 체크섬값을 계산하기 위한 코드를 진행을 하였습니다. 코드작성중 애러가 있습니다. 덤프해놓은 패킷을 pcap_open_offline() 함수를 이용하여 똑같은 패킷을 가지고 디버그 중인데 TCP 패킷마다 제가 계산한 값과 같은 값도 있고 다른 값도 있는 오류가 있습니다.

기존에 공개된 체크섬 계산하는 코드가 있지만 직접 해보기 위해 코드를 작성중 이지만 진전이 없다고 생각되면 공개된 체크섬 계산코드를 사용할 예정입니다.

체크썸 계산 방법

1. pseudo header 생성

필드명	크기(바이트)	설명
Source IP	4	출발지 IP
Destination IP	4	목적지 IP
Reserved (항상 0)	1	8비트 항상 0 이다.
프로토콜	1	IP에더에서 알아낸 프로토콜 필드 값 으로써, TCP 체크섬의 경우는 TCP프로토콜을 의미하는 6이 된다.
TCP 길이	2	TCP 헤더 + DATA의 총 길이(바이트)

    1. pseudo header를 만들어 2byte씩 묶어서 나열한다.
    - c0 a8 f6 82 0c a8 f6 81 00 06 00 e6

2. TCP segment(Heaer + Data)의 2byte 단위 합을 구한다.
3. checksum 부분은 0으로 입력하고 기존 체크섬 값은 비교용으로 사용한다.
4. Pseudo Header 합 + TCP Segment(TCP header field+ Data) = x
5. x 의 값이 2byte를 초과한다면 올림수를 x 값에 더해준다
    - ex) x = 0x12345 (x>>16) + (x&0xFFFF) = 0x2346
6. 위의 결과를 가지고 1의 보수를 취해준다 = 0xDCB9 = check sum

<다음주 진행 상황>

현재 코드작성한 코드를 점검하여 체크섬 계산에 성공을 한다면 raw socket 개발에 시작을 하겠습니다. 그러나 계속해서 체크섬 계산에 실패한다면 공개된 코드를 이용하여 적용하도록 하겠습니다.