<수업내용>

🡺 최종적인 알고리즘

fp = pcap\_open(..........);

unsigned char packet[65535]; // max packet size is 65535

build\_packet(packet);

pcap\_sendpacket(fp, packet, ......);

htons() : (Host to network short)

Host 시스템에서 Network로 short 형 데이터를 보낼 때  바이트 오더를 바꾸어주는 함수

<HOMEWORK>

1) Send a SYN packet to the server.

1-1)

- Modify your sniffer such that it can send a SYN packet instead of sniffing.

-- break out of the while loop after capturing the first SYN packet.

-- display the packet in raw bytes.

-- kill the server and the client (manually)

-- run the original sniffer

-- rerun the server

-- send the captured SYN packet to the server

-- check if you can see this packet in the original sniffer

-- check if you can see the ACK packet from the server.

\*If the captured SYN packet shows checksum=0, do not send as it is: you have to compute the checksum by yourself (checksum offload case).

(\* If you have "fatal bad memory block" error, change win10pcap to wpcap. Delete win10pcap and reinstall wpcap.)

따라서, win10cap 을 삭제한 후, wpcap 을 install 해주었습니다.



텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

1-2)

- Modify the sniffer further such that it re-computes ip and tcp checksum.

-- break out of the while loop after capturing the first SYN packet.

-- copy them into another buffer: pkt\_data=>packet

-- set ip\_check\_sum and tcp\_check\_sum to zero

-- recompute ip\_check\_sum

-- recompute tcp\_check\_sum

-- display the packet in raw bytes. this should be same as pkt\_data

-- kill the server and the client (manually)

-- run the original sniffer

-- rerun the server

-- send packet to the server

-- check if you can see this packet in the original sniffer

-- check if you can see the ACK packet from the server.

<IP 체크섬값 구하는 방법>

텍스트이(가) 표시된 사진

자동 생성된 설명

IP Header cheacksum은 IP 헤더의 오류를 검증하기 위해서 사용되는 필드이다.계산방식은 다음과 같다. 1. Version 필드 값부터 목적지IP 필드 값까지 모두 더한다.(단, 체크섬 필드 값은 제외하고 합산)2. 합산 값의 첫 번째 값을 뒤의 4자리 값과 합산한다.3. 더한 값을 2진수로 표기한 후 해당 값을 보수화4. 보수화 값을 16진수로 표현 = 체크섬 값

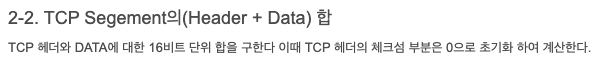
<TCP 체크섬 값 구하는 방법>

테이블이(가) 표시된 사진

자동 생성된 설명









회로이(가) 표시된 사진

자동 생성된 설명

텍스트이(가) 표시된 사진

자동 생성된 설명

값이 다르게 출력되었습니다. 이는 제가 실수했음을 의미합니다.

2) Implement a stealth scanner.

- Modify the packet sender such that it sends a SYN packet to all possible ports in the server. Detect which ports are live by finding out those who respond with SYN/ACK. You may need seperate sniffer for such detection.

(\* If you have "fatal bad memory block" error, change win10pcap to wpcap. Delete win10pcap and reinstall wpcap.)