

## 9.1 과제 주제

### 스푸핑, 스누핑, 스니핑의 차이에 대해 조사하기

#### 1. 스푸핑

스푸핑(spoofing)이라는 단어는 눈속임(spoof)에서 파생된 IT 용어이며, 직접적으로 공격자가 시스템에 침입을 하지는 않지만, 피해자가 **공격자의 악의적인 시도에 의한 잘못된 정보, 혹은 연결을 신뢰하게끔** 만드는 일련의 기법들을 의미한다. 피싱이나 스니핑과는 달리 더욱 적극적으로 피해자의 시스템이 잘못된 정보를 신뢰하고 받아들이게끔 유도하며, 피해자는 자신이 속고 있음을 알아채기 힘들다. 종류에는 DNS 스푸핑, ARP 스푸핑, IP 스푸핑이 있다.

#### 2. 스누핑

스누핑(snooping)은 엿듣다라는 뜻을 갖고 있다. 스누핑은 프로토콜 분석용 소프트웨어를 지칭하며 **네트워크상에 떠도는 중요 정보들을 몰래 획득하는 행위**를 말한다. 종류에는 IGMP 스누핑, DHCP 스누핑이 있다.

#### 3. 스니핑

스니핑(sniffing)은 **네트워크상의 데이터를 도청하는 행위**를 말한다. 공격할 때 아무것도 하지 않고 조용히 있는 것만으로도 충분하기 때문에 수동적인 공격이라고도 한다. 일반적으로 스니핑 공격은 IP 주소 필터링과 MAC 주소 필터링을 수행하지 않고 랜카드로 들어오는 전기신호를 모두 읽어 관찰하여 정보를 유출시키는 것을 의미한다.

스푸핑은 **공격자의 악의적인 시도에 의한 잘못된 정보나 연결을 신뢰하게끔 만드는 기법들로** 사용자들을 유도하여 정보를 빼가는 해킹 수법이라고 할 수 있다.

스누핑은 **네트워크 상에 떠도는 중요 정보를 몰래 획득하는 행위**이며 스니핑은 **패킷교환을 엿보는, 도청하는 행위**라고 할 수 있다. 즉 스니핑은 패킷교환을 훑쳐보는 행위에 그치지만, 스누핑은 중요 정보를 획득하는데 초점이 맞춰져 있다고 볼 수 있다.

## 9.2 과제 주제

Wireshark 를 사용하여 본인의 네트워크 인터페이스로 송/수신 되는 패킷들을 보여주는 패킷 List, 그리고 임의의 패킷 하나를 선택하여 상세 내용을 보여주는 화면을 캡처하기 (List, Details, 패킷 Bytes 가 보이도록 캡처할 것)

The screenshot displays the Wireshark network protocol analyzer interface. The top menu bar includes File, Edit, View, Go, Capture, Analyze, Statistics, Telephony, Wireless, Tools, and Help. Below the menu is a toolbar with various icons for file operations, capture control, and analysis. A display filter bar shows 'Apply a display filter ... <Ctrl-/>'. The main packet list pane shows a table of captured packets with columns for No., Time, Source, Destination, Protocol, Length, and Info. Packet 16 is highlighted in red, indicating a TCP RST, ACK segment. The details pane below the packet list shows the selected packet's structure: Frame 23 (87 bytes on wire, 87 bytes captured), Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and Domain Name System (query). The packet bytes pane at the bottom shows the raw data in hexadecimal and ASCII format.

No.	Time	Source	Destination	Protocol	Length	Info
2	1.000886	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
3	1.542149	192.168.0.10	108.177.97.188	TCP	55	49813 → 5228 [ACK] Seq=1 Ack=1 Win=1027 Len=1
4	1.598536	108.177.97.188	192.168.0.10	TCP	66	5228 → 49813 [ACK] Seq=1 Ack=2 Win=270 Len=0 SLE=1 SRE=2
5	1.999235	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
6	2.996728	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
7	3.936747	192.168.0.1	224.0.0.1	IGMPv2	60	Membership Query, general
8	3.946864	192.168.0.10	224.0.0.251	IGMPv2	46	Membership Report group 224.0.0.251
9	3.946906	192.168.0.10	224.0.0.252	IGMPv2	46	Membership Report group 224.0.0.252
10	3.999957	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
11	4.998766	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
12	5.447150	192.168.0.10	239.255.255.250	IGMPv2	46	Membership Report group 239.255.255.250
13	5.998195	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
14	7.004619	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
15	7.560055	192.168.0.10	14.0.112.31	TCP	54	24043 → 80 [FIN, ACK] Seq=1 Ack=1 Win=0 Len=0
16	7.560114	192.168.0.10	14.0.112.31	TCP	54	24043 → 80 [RST, ACK] Seq=2 Ack=1 Win=0 Len=0
17	7.998866	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
18	8.999381	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
19	9.539909	192.168.0.10	72.25.64.2	TCP	55	49849 → 443 [ACK] Seq=1 Ack=1 Win=1023 Len=1 [TCP segment of a reassembled...
20	9.686912	72.25.64.2	192.168.0.10	TCP	60	443 → 49849 [ACK] Seq=1 Ack=2 Win=512 Len=0
21	9.999139	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
22	11.001596	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
23	11.537570	192.168.0.10	210.220.163.82	DNS	87	Standard query 0x0001 PTR 82.163.220.210.in-addr.arpa
24	11.539285	210.220.163.82	192.168.0.10	DNS	117	Standard query response 0x0001 PTR 82.163.220.210.in-addr.arpa PTR bns1.h...

> Frame 23: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF\_{1DB68A61-DA2F-4C0B-BD7F-5977B5A4BD3C}, id 0  
> Ethernet II, Src: ASRockIn\_fa:0f:e3 (70:85:c2:fa:0f:e3), Dst: EFMNetwo\_c1:9b:13 (88:36:6c:c1:9b:13)  
> Internet Protocol Version 4, Src: 192.168.0.10, Dst: 210.220.163.82  
> User Datagram Protocol, Src Port: 58717, Dst Port: 53  
> Domain Name System (query)

```
0000 88 36 6c c1 9b 13 70 85 c2 fa 0f e3 08 00 45 00 61 . . . p . . . . . E .
0010 00 49 20 dc 00 00 00 11 e2 e6 c0 a8 00 0a d2 dc . I . . . . .
0020 a3 52 e5 5d 00 35 00 35 39 1f 00 01 01 00 00 01 . R . ] 5 5 9 . . . . .
0030 00 00 00 00 00 00 02 38 32 03 31 36 33 03 32 32 . . . . . 8 2 163 22
0040 30 03 32 31 30 07 69 6e 2d 61 64 64 72 04 61 72 0 210 . in -addr . ar
0050 70 61 00 00 0c 00 01 pa . . . . .
```

wireshark\_이더넷KJRB1.pcapng | Packets: 85 · Displayed: 85 (100.0%) · Dropped: 0 (0.0%) | Profile: Default

### 9.3 과제 주제

cmd 상에서 입력한 nslookup 과 WireShark 를 사용하여 www.google.com 명령 실행한 결과 캡쳐하기

이더넷

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
36	1.629814	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
37	2.631065	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
38	3.631195	192.168.0.10	192.168.0.255	UDP	305	54915 → 54915 Len=263
39	3.767760	192.168.0.10	210.220.163.82	DNS	70	Standard query 0x0004 A google.com
40	3.769507	210.220.163.82	192.168.0.10	DNS	86	Standard query response 0x0004 A google.com A 172.217.175.238
41	3.769804	192.168.0.10	210.220.163.82	DNS	70	Standard query 0x0005 AAAA google.com
42	3.771410	210.220.163.82	192.168.0.10	DNS	98	Standard query response 0x0005 AAAA google.com AAAA 2404:6800:4004:80a::2...
43	4.174326	142.250.196.106	192.168.0.10	UDP	202	443 → 52463 Len=160
44	4.174557	142.250.196.106	192.168.0.10	UDP	68	443 → 52463 Len=26
45	4.177373	192.168.0.10	142.250.207.42	QUIC	1392	Initial, DCID=e0f548b2b9e71e77, PKN: 1, CRYPTO, CRYPTO, PING, PADDING, PI...
46	4.177529	192.168.0.10	142.250.207.42	QUIC	117	0-RTT, DCID=e0f548b2b9e71e77
47	4.177639	192.168.0.10	142.250.207.42	QUIC	559	0-RTT, DCID=e0f548b2b9e71e77
48	4.183901	192.168.0.10	142.250.196.106	UDP	75	52463 → 443 Len=33
49	4.234680	142.250.207.42	192.168.0.10	QUIC	1392	Initial, SCID=e0f548b2b9e71e77, PKN: 1, ACK, PADDING
50	4.243841	142.250.207.42	192.168.0.10	QUIC	1392	Protected Payload (KP0)
51	4.244088	142.250.207.42	192.168.0.10	QUIC	664	Protected Payload (KP0)
52	4.244092	192.168.0.10	142.250.207.42	QUIC	120	Handshake, DCID=e0f548b2b9e71e77
53	4.244139	192.168.0.10	142.250.207.42	QUIC	75	Protected Payload (KP0), DCID=e0f548b2b9e71e77
54	4.244406	142.250.207.42	192.168.0.10	QUIC	68	Protected Payload (KP0)
55	4.275558	142.250.207.42	192.168.0.10	QUIC	146	Protected Payload (KP0)
56	4.275558	142.250.207.42	192.168.0.10	QUIC	67	Protected Payload (KP0)
57	4.275673	192.168.0.10	142.250.207.42	QUIC	75	Protected Payload (KP0), DCID=e0f548b2b9e71e77
58	4.396569	142.250.207.42	192.168.0.10	QUIC	336	Protected Payload (KP0)

> Frame 39: 70 bytes on wire (560 bits), 70 bytes captured (560 bits) on interface \Device\NPF\_{1DB68A61-DA2F-4C0B-BD7F-5977B5A48D3C}, id 0

> Ethernet II, Src: ASRockIn\_fa:0f:e3 (70:85:c2:fa:0f:e3), Dst: EFMNetwo\_c1:9b:13 (88:36:6c:c1:9b:13)

> Destination: EFMNetwo\_c1:9b:13 (88:36:6c:c1:9b:13)

> Address: EFMNetwo\_c1:9b:13 (88:36:6c:c1:9b:13)

> ....0. .... = LG bit: Globally unique address (factory default)

> ....0. .... = IG bit: Individual address (unicast)

> Source: ASRockIn\_fa:0f:e3 (70:85:c2:fa:0f:e3)

> Address: ASRockIn\_fa:0f:e3 (70:85:c2:fa:0f:e3)

> ....0. .... = LG bit: Globally unique address (factory default)

> ....0. .... = IG bit: Individual address (unicast)

> Type: IPv4 (0x0800)

> Internet Protocol Version 4, Src: 192.168.0.10, Dst: 210.220.163.82

> User Datagram Protocol, Src Port: 56202, Dst Port: 53

> Domain Name System (query)

0000 88 36 6c c1 9b 13 70 85 c2 fa 0f e3 08 00 45 00 .61...p. ....E.

0010 00 38 21 53 00 00 80 11 e2 80 c0 a8 00 0a d2 dc .81S....

0020 a3 52 db 8a 00 35 00 24 d9 47 00 04 01 00 00 01 .R..5.\$ .G.....

0030 00 00 00 00 00 06 67 6f 6f 67 6c 65 03 63 6f .....g oogle-co

0040 6d 00 00 01 00 01 m.....

명령 프롬프트 - nslookup

Microsoft Windows [Version 10.0.18363.1854]  
(c) 2019 Microsoft Corporation. All rights reserved.

C:\Users\장지혁>nslookup

기본 서버: bns1.hananet.net

Address: 210.220.163.82

> www.google.co.kr

서버: bns1.hananet.net

Address: 210.220.163.82

권한 없는 응답:

이름: www.google.co.kr

Addresses: 2404:6800:4004:822::2003

142.251.42.131

> google.com

서버: bns1.hananet.net

Address: 210.220.163.82

권한 없는 응답:

이름: google.com

Addresses: 2404:6800:4004:80a::200e

172.217.175.238

>

Source or Destination Hardware Address (eth,addr), 6 byte(s) | Packets: 85 · Displayed: 85 (100,0%) · Dropped: 0 (0,0%) | Profile: Default

빨간 선이후 DNS 와 패킷을 교환하는 기록 시작