영남대학교 정보보호동아리 @Xpert
박종덕 (cryapple@nate.com)

스위치 환경에서의 패킷 스니핑 (Packet Sniffing)

* 0. 목 차

1. 스니핑의 정의

2. 스위치 환경에서의 스니핑 방법
   - Mirroring Port, Switch Jamming, ARP Redirect, ARP spoofing, ICMP Redirect,,,

3. 모의해킹 1
   - 스위치의 미러링 포트를 통한 스니핑 (윈도우기반, Ethereal 사용)

4. 모의해킹 2
   - ARP Redirect 를 이용한 스니핑 (리눅스기반, Dsniff 사용)

5. 스니핑 방지법

* 1. 스니핑(Sniffing)이란?

◉ 해킹 기법으로서의 스니핑은 네트워크 상에서 자신이 아닌 다른 상대방들의 패킷 교환을 엿듣는 것을 의미한다. 간단히 말하여 네트워크 트래픽을 도청(Eavesdropping)하는 과정을 스니핑 이라고 할 수 있다. 이런 스니핑을 할 수 있도록 하는 도구를 스니퍼(Sniffer)라고 한다.

* 2. 스위치 환경에서의 스니핑 방법

- 스위치(스위칭허브)란?

  - 근거리통신망 구축시 단말기의 집선 장치로 이용하는 스위칭 기능을 가진 통신장비로 통신 효율을 향상시킨 허브이다. 대역폭이 커서 여러개의 포트입력을 동시에 받을 수 있으며 수신 단말기의 주소 번지를 파악하여 특정 포트로만 데이터를 보낼 수 있다.

- 스위치 환경에서는 스니핑이 안되는가?

  - 스위치허브는 원래의 목적이 네트워크 트래픽을 줄이고 스니핑을 방지하고자 개발된 장치이다. 따라서 더미허브에 비하면 스니핑이 까다롭지만 미러링 포트를 이용하거나(주로 네트워크 장애 발생시 문제점을 파악하기 위해 사용됨) Switch Jamming, ARP Redirect, ARP Spoofing, ICMP Redirect 등의 기법들을 이용하면 스니핑이 가능하다.

* 2. 스위치 환경에서의 스니핑 방법

◉ 방법 1. 미러링 포트(=모니터 포트)를 통한 스니핑

- 미러링(Mirroring) 포트란? 스위치에 존재하는 모든 포트에서 이동하는 데이터들을 복제하여 보내주는 포트. 따라서 스위치 내부에서 이동하는 정보를 모두 볼 수 있으며, 이를 이용하여 스니핑이 가능하게 되는 것이다. 원래의 목적은 네트워크 장애 발생시 문제점을 파악하기 위함이다.

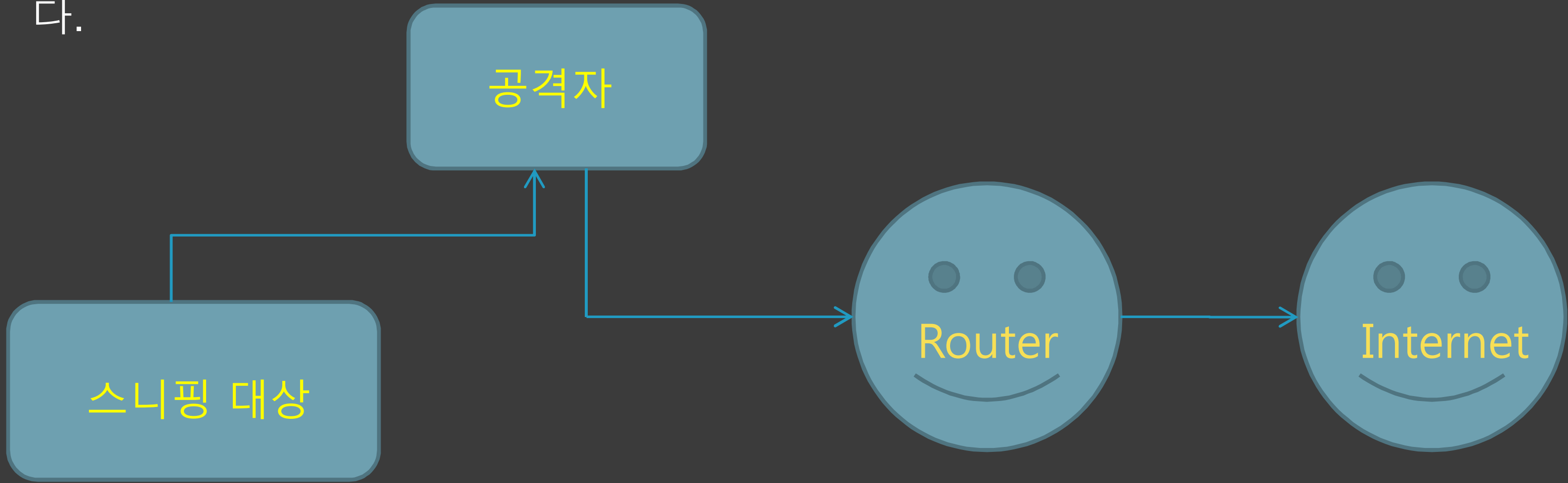
◉ 방법 2. Switch Jamming

- 스위치들은 주소 테이블이 가득차게 되면 모든 포트로 트래픽을 브로드캐스팅하게 된다. 따라서 공격자는 위조된 MAC 주소를 지속적으로 네트워크에 흘림으로서 스위칭 허브의 주소 테이블을 오버플로우 시켜 다른 네트워크 세그먼트의 데이터를 스니핑 할 수 있게 된다. 이 방법을 사용하게 되면 스위칭 허브가 더미 허브처럼 동작하므로 통신속도가 느려지게 된다.

* 2. 스위치 환경에서의 스니핑 방법

◉ 방법 3. ARP Redirect

- ARP(Address Resolution Protocol) 의 취약점을 이용하여 스니핑 하는 방법. 공격자는 자신이 라우터인 것처럼 위조된 ARP Reply 패킷을 주기적으로 브로드 캐스팅하여 스위칭 네트워크상의 모든 호스트들이 공격하고 있는 호스트를 라우터로 믿게끔 만든다. 결국 네트워크의 모든 트래픽은 공격자를 통해서 외부와 연결되므로 스니핑이 가능하게 된다. 공격자는 반드시 IP Forwarding을 이용하여 모든 트래픽을 게이트 웨이로 포워딩 해주어야만 한다.



* 2. 스위치 환경에서의 스니핑 방법

◉ 방법 4. ARP spoofing

- ARP Redirect와 마찬가지로 ARP Protocol의 취약점을 이용하여 스니핑 하는 방법이다. 공격자는 자신의 MAC 주소를 타켓호스트의 MAC주소로 위장하는 ARP 패킷을 네트워크에 브로드 캐스팅하면 된다. 결국 호스트의 모든 트래픽은 공격자의 호스트로 들어오게 되고 스니핑도 가능해 진다. ARP Redirect와 마찬가지로 공격자 호스트로 오는 트래픽을 원래의 호스트로 릴레이 해주어야만 연결이 끊지지 않고 지속적으로 스니핑을 할 수 있다.

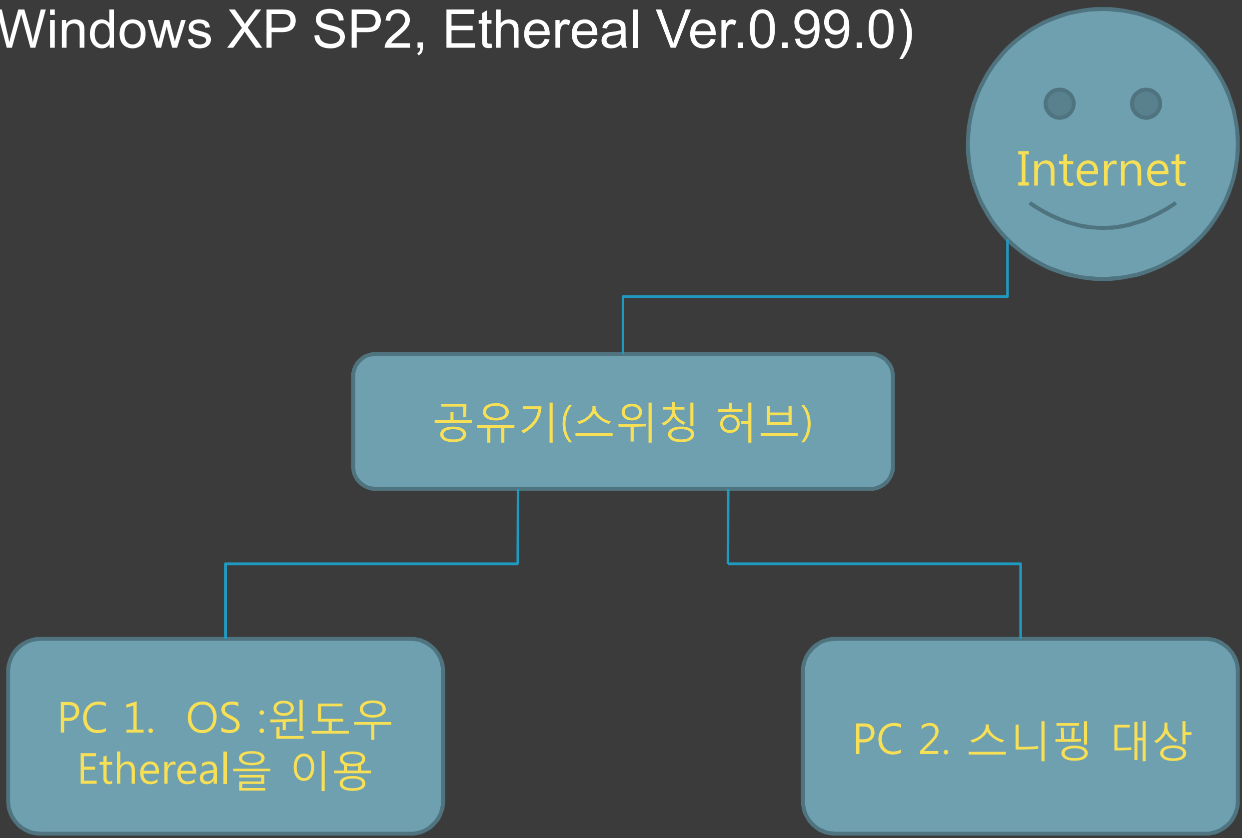
◉ 방법 5. ICMP Redirect

- ICMP(Internet Control Message Protocol) Redirect 메시지는 네트워크에 라우터가 여러 개일 경우 호스트의 라우팅 경로를 수정하여 패킷을 최적의 경로로 보내도록 알려주는 역할을 하는데 이를 이용하여 스니핑을 하는 방법이다. 공격자는 타켓 호스트에 자신이 라우터이고 최적의 경로라고 수정된 ICMP Redirect 메시지를 보내어 스니핑한다. 마찬가지로 포워딩은 필수이다.

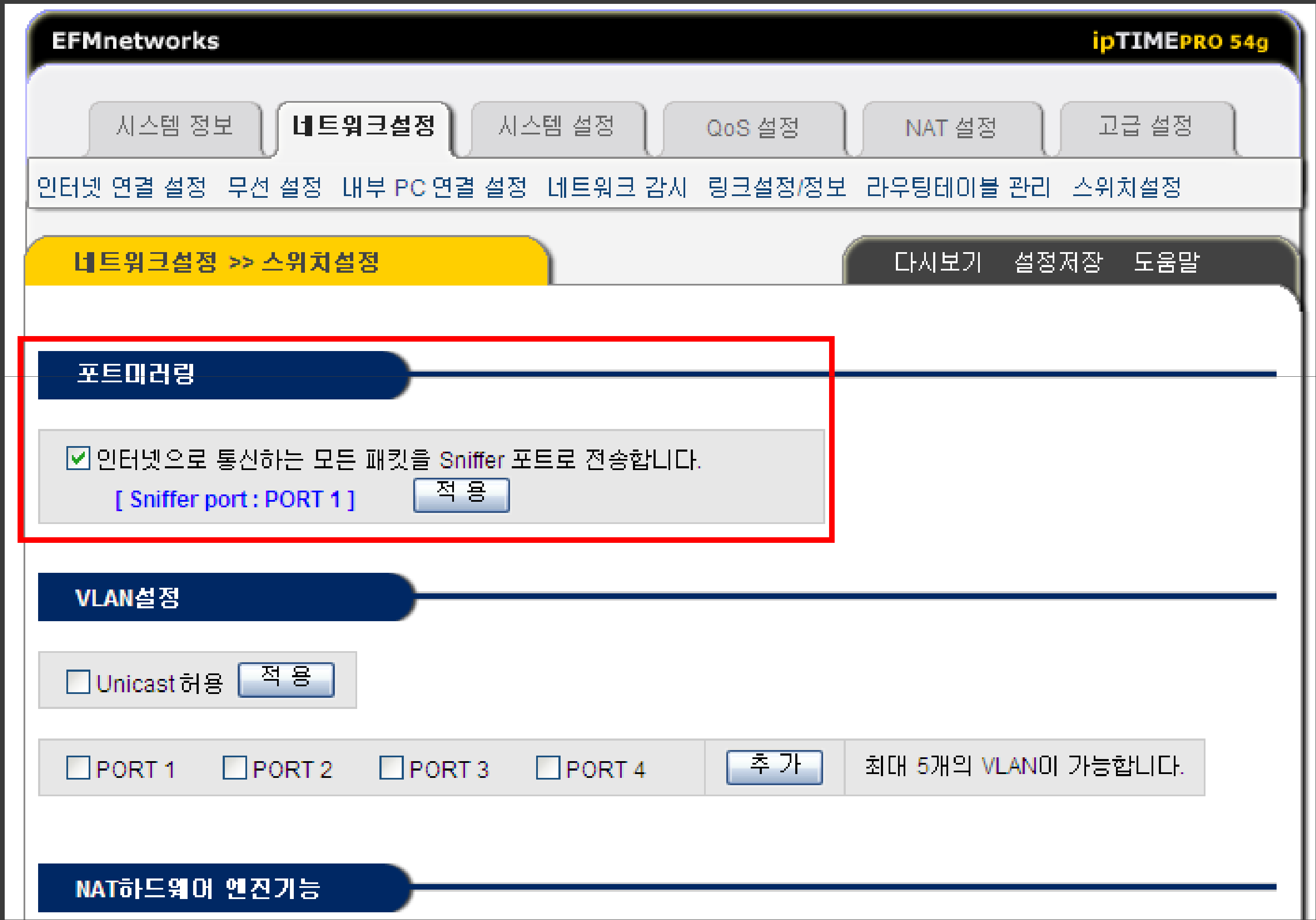
* 3. 모의해킹 1 (스위치의 미러링 포트를 통한 스니핑)

◉ 테스트 환경

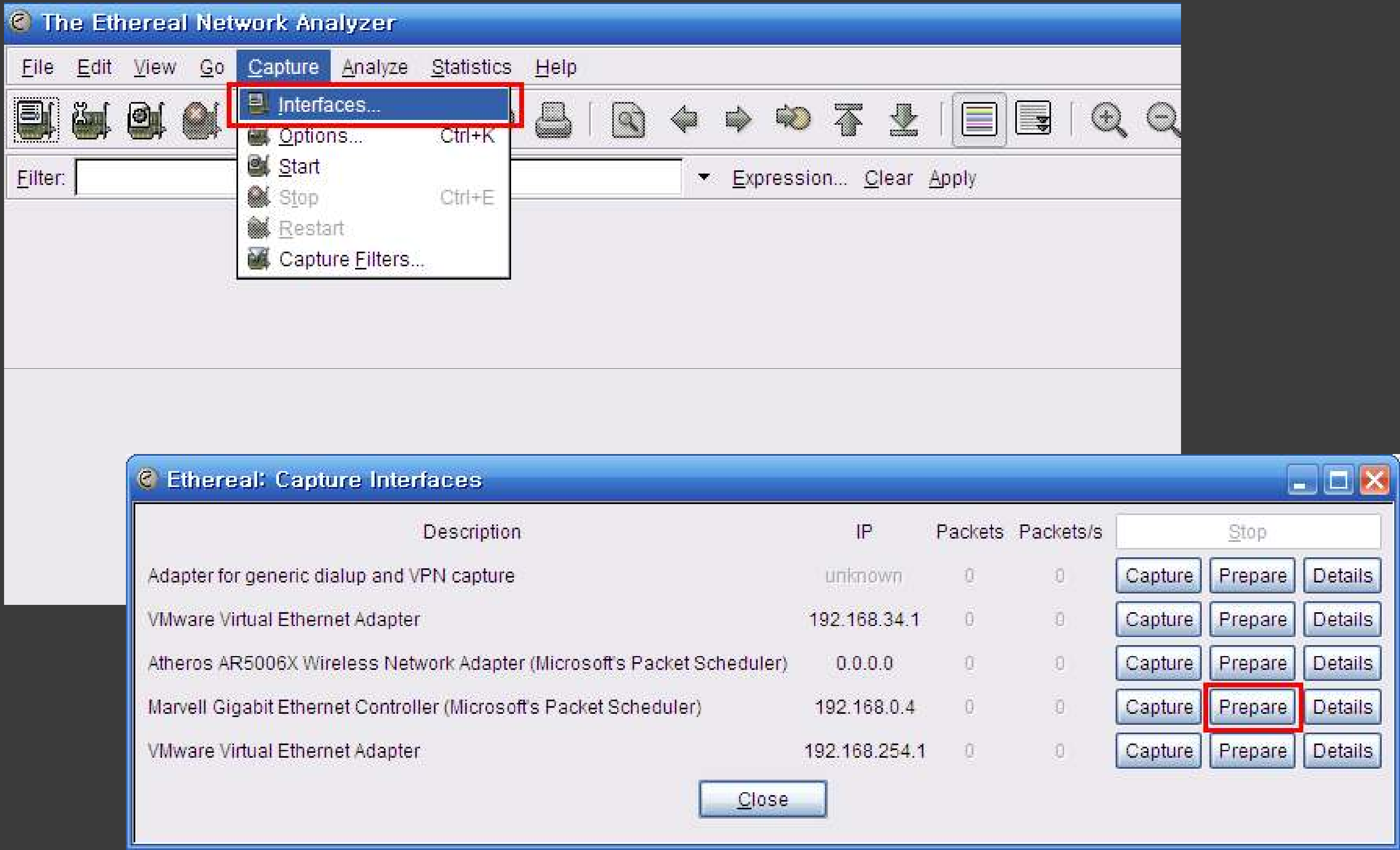
- 스위치의 미러링 포트를 통한 스니핑.
  (Windows XP SP2, Ethereal Ver.0.99.0)



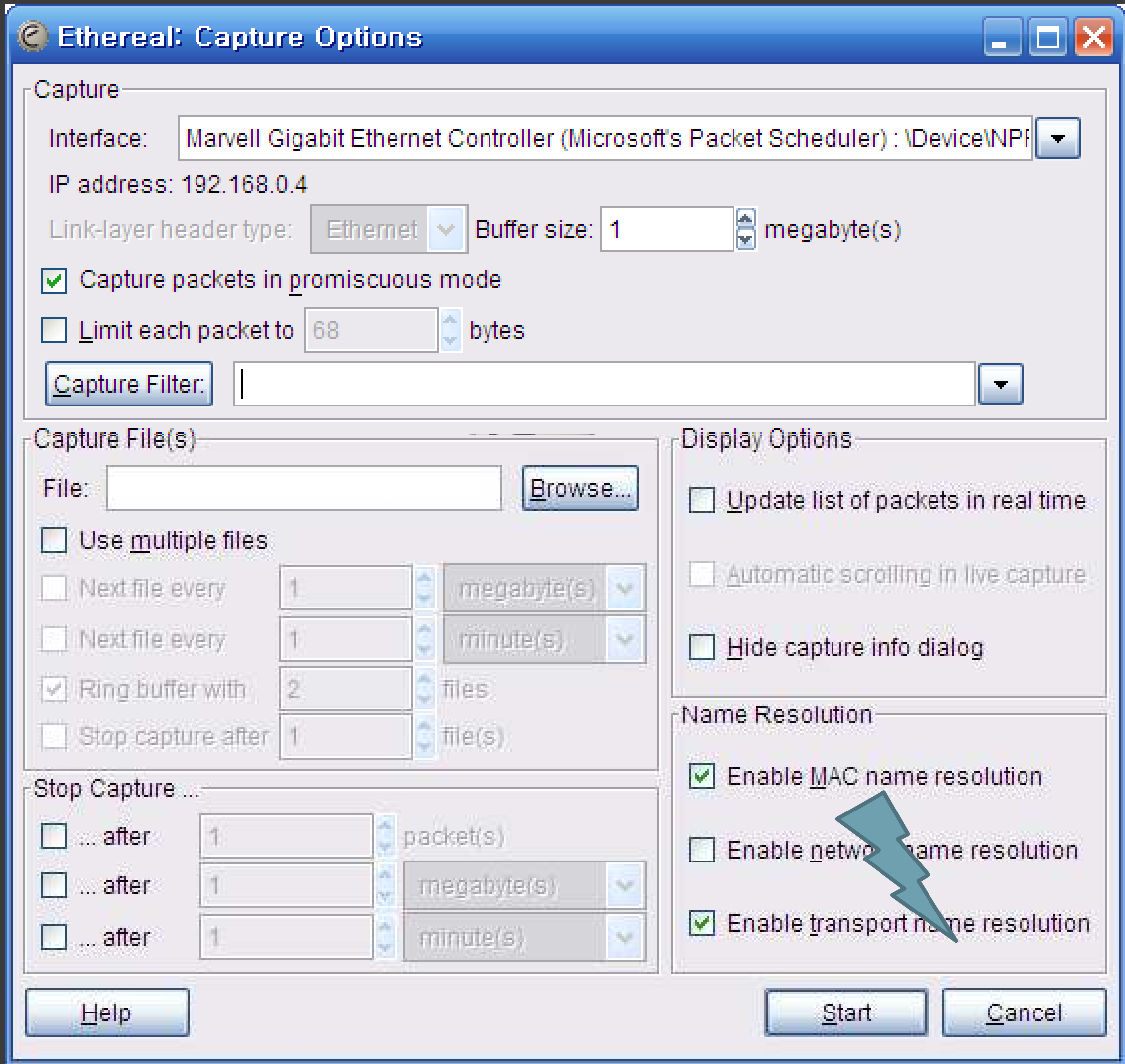
* 3. 모의해킹 1 (스위치의 미러링 포트를 통한 스니핑)



* 3. 모의해킹 1 (스위치의 미러링 포트를 통한 스니핑)



* 3. 모의해킹 1 (스위치의 미러링 포트를 통한 스니핑)

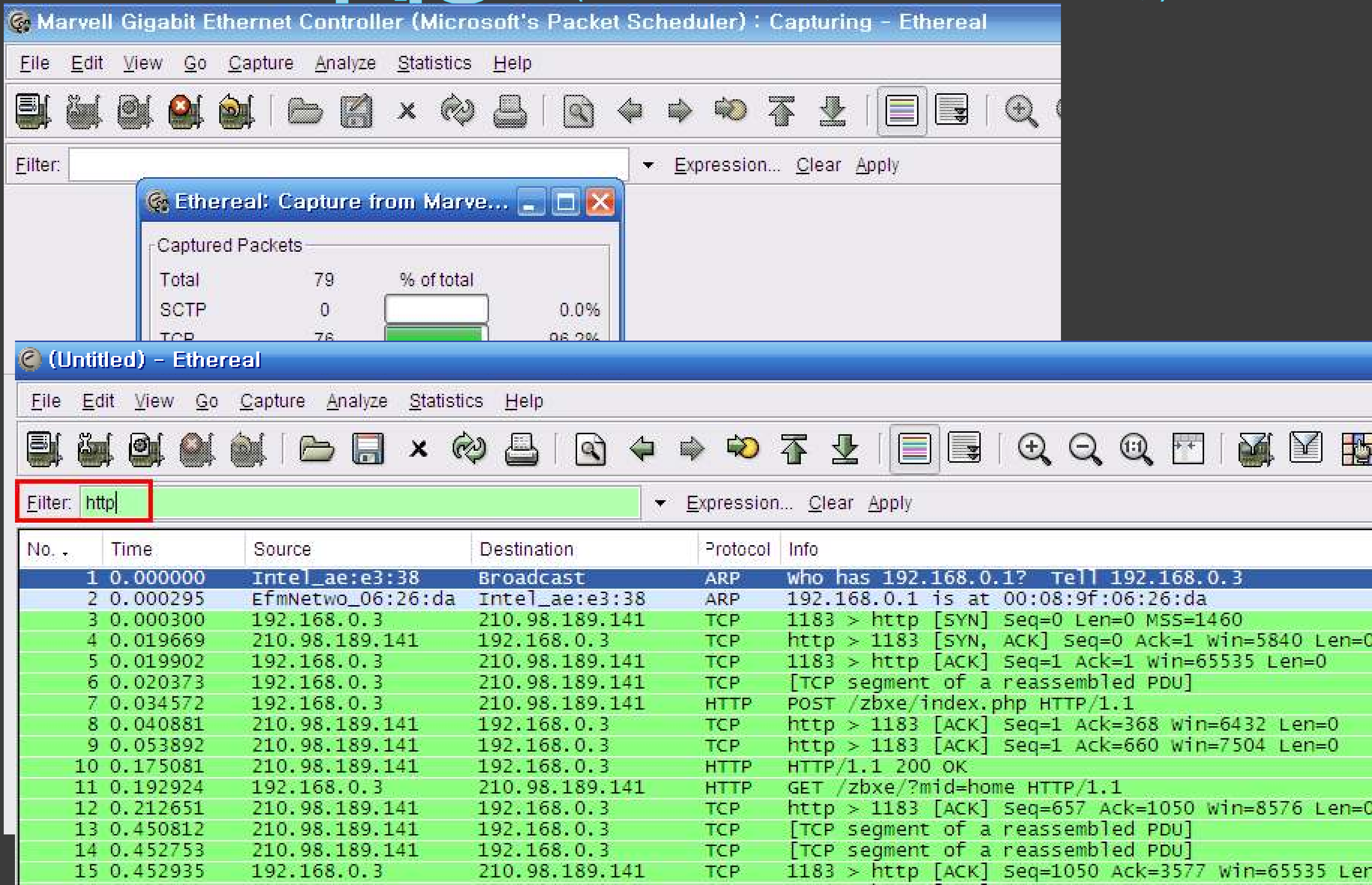


* 3. 모의해킹 1 (스위치의 미러링 포트를 통한 스니핑)

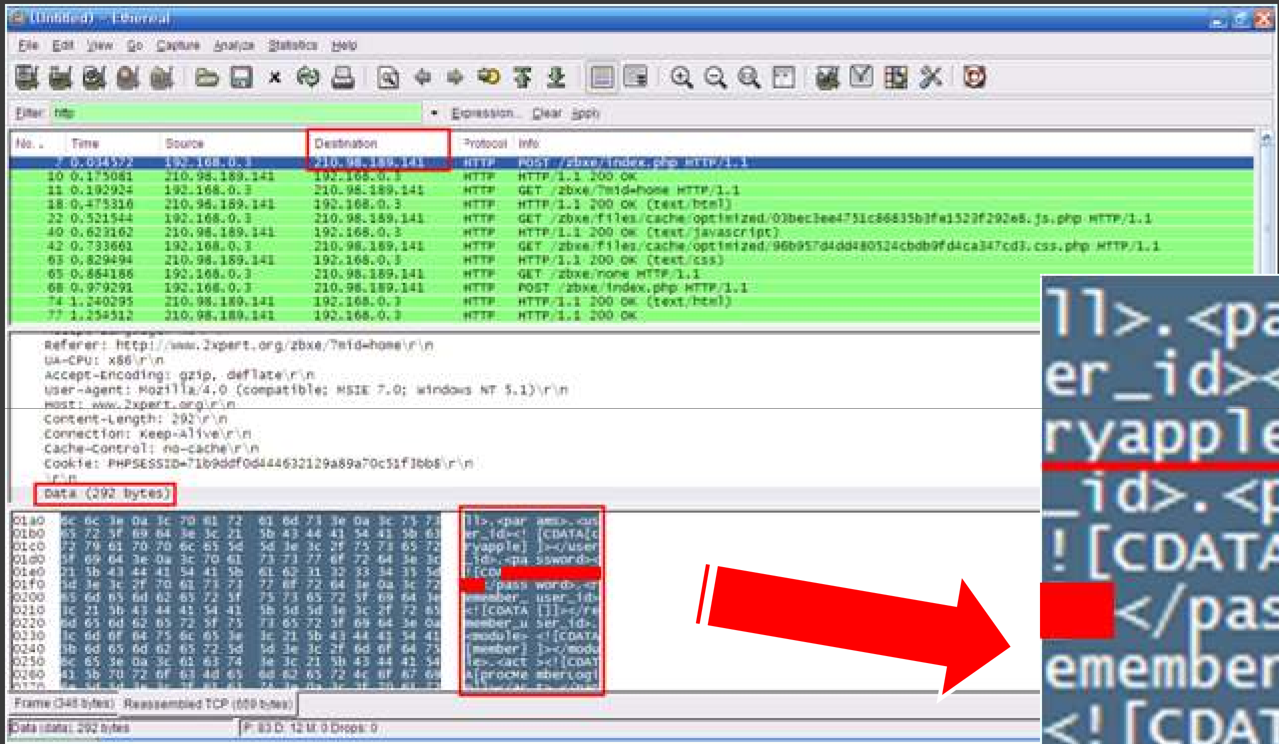
스니핑 대상
PC에서 로그인!!

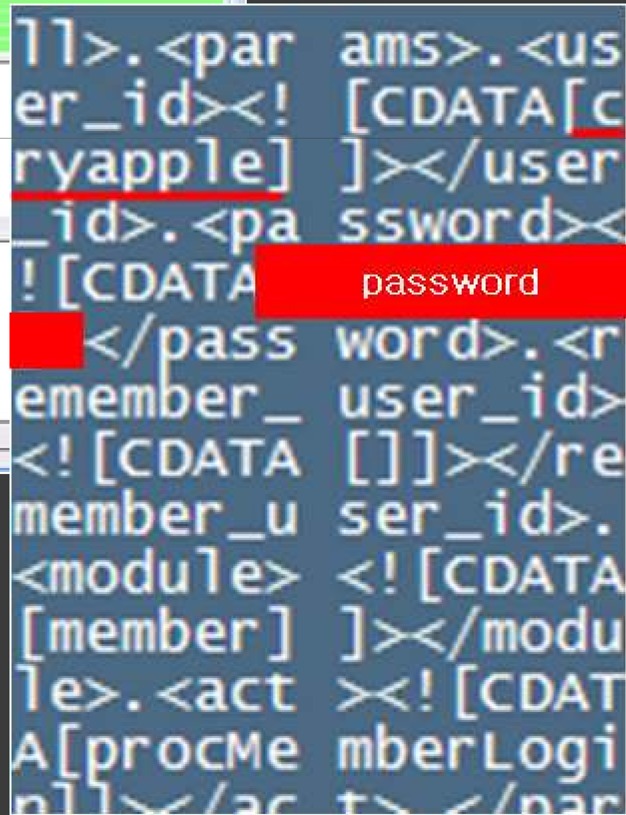
스니핑 대상 PC

* 3. 모의해킹 1 (스위치의 미러링 포트를 통한 스니핑)



* 3. 모의해킹 1 (스위치의 미러링 포트를 통한 스니핑)

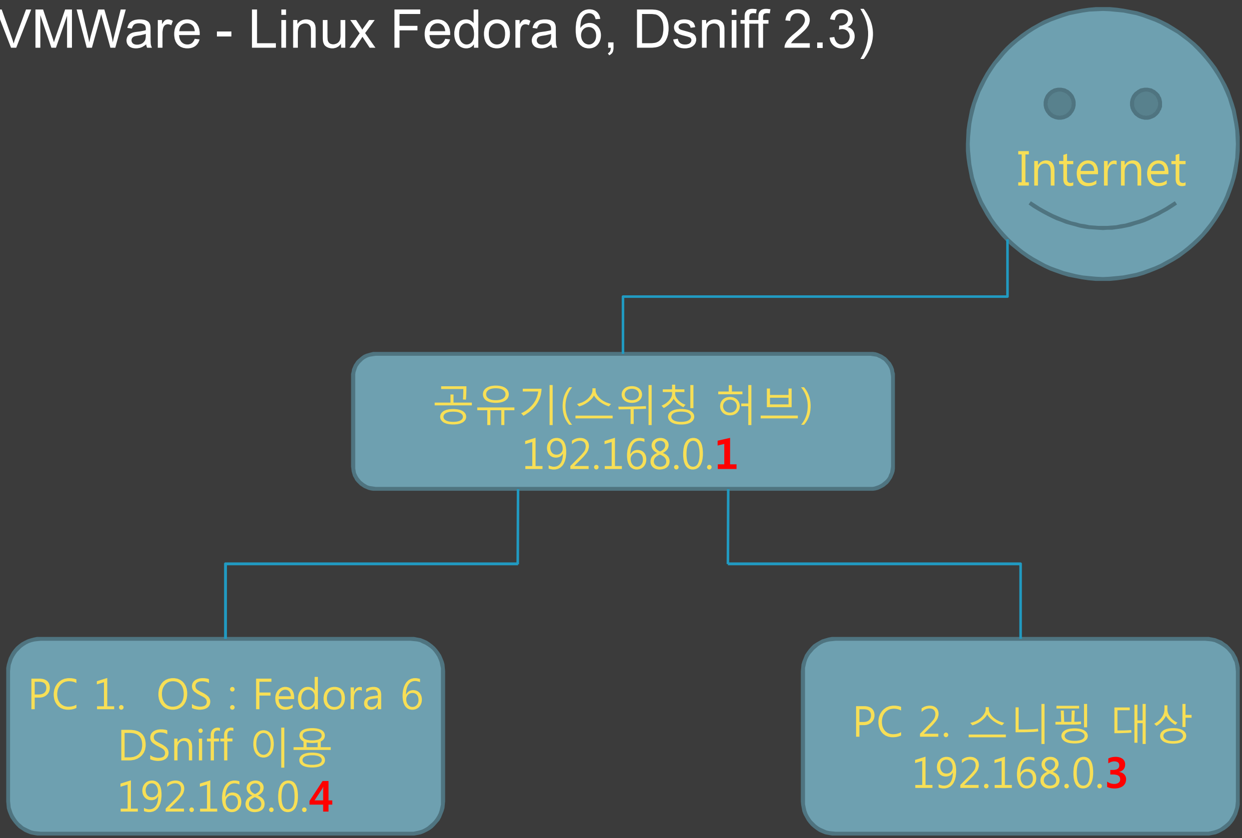




* 4. 모의해킹 2

◉ 테스트 환경

- ARP Redirect을 이용한 스니핑.
  (VMWare - Linux Fedora 6, Dsniff 2.3)



* 4. 모의해킹 2

◉ 테스트 환경(Dsniff 설치순서 // 사용된 Tools // 주의사항)

설치순서 및 사용된 Tools

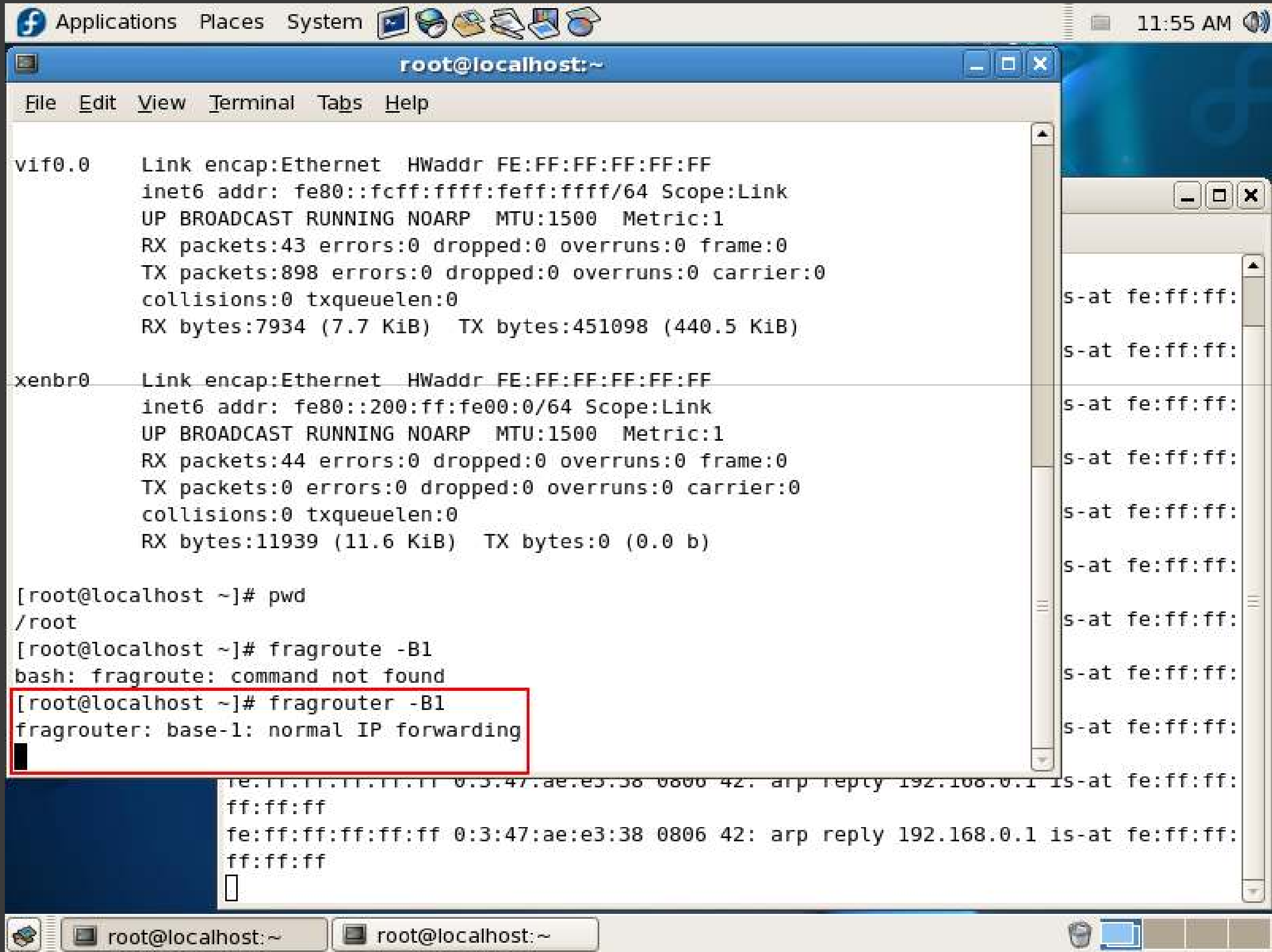
1. libpcap-0.9.4
2. fragrouter-1.6
3. berkeley DB-2.7.7
4. libnet-1.0.2a
5. libnids-1.18
6. dsniff-2.3
7. ettercap

* 아래 설치 순서는 必
Berkeley DB -> libnet -> libnids -> dsniff

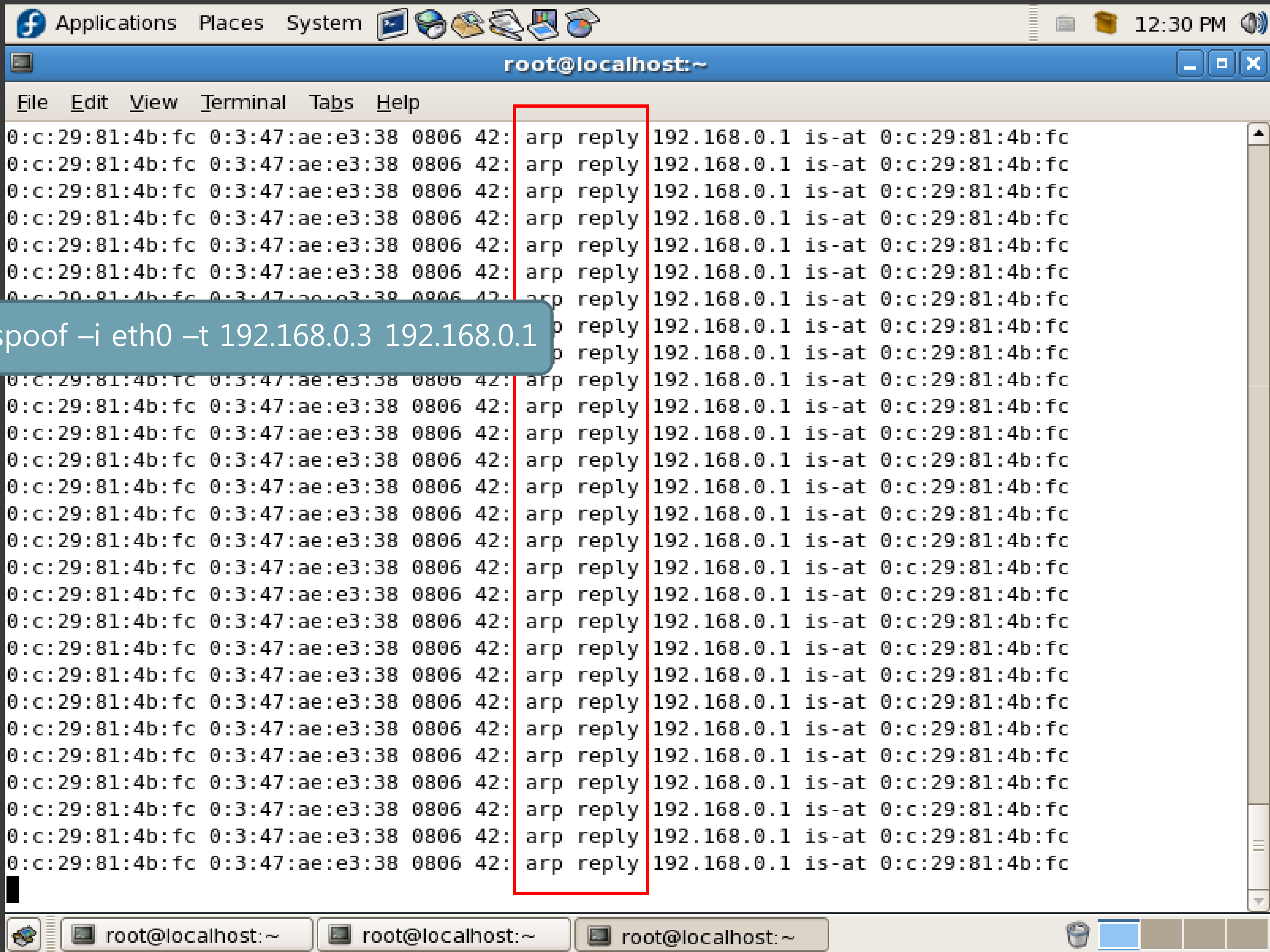
* Berkely DB
꼭 Ver 1.8.5와 호환모드로..!
\# ./configure –enable-compat185

* 나머지는 그냥
\# ./configure && make && make install

* 4. 모의해킹 2 (ARP Redirect 를 이용한 스니핑)

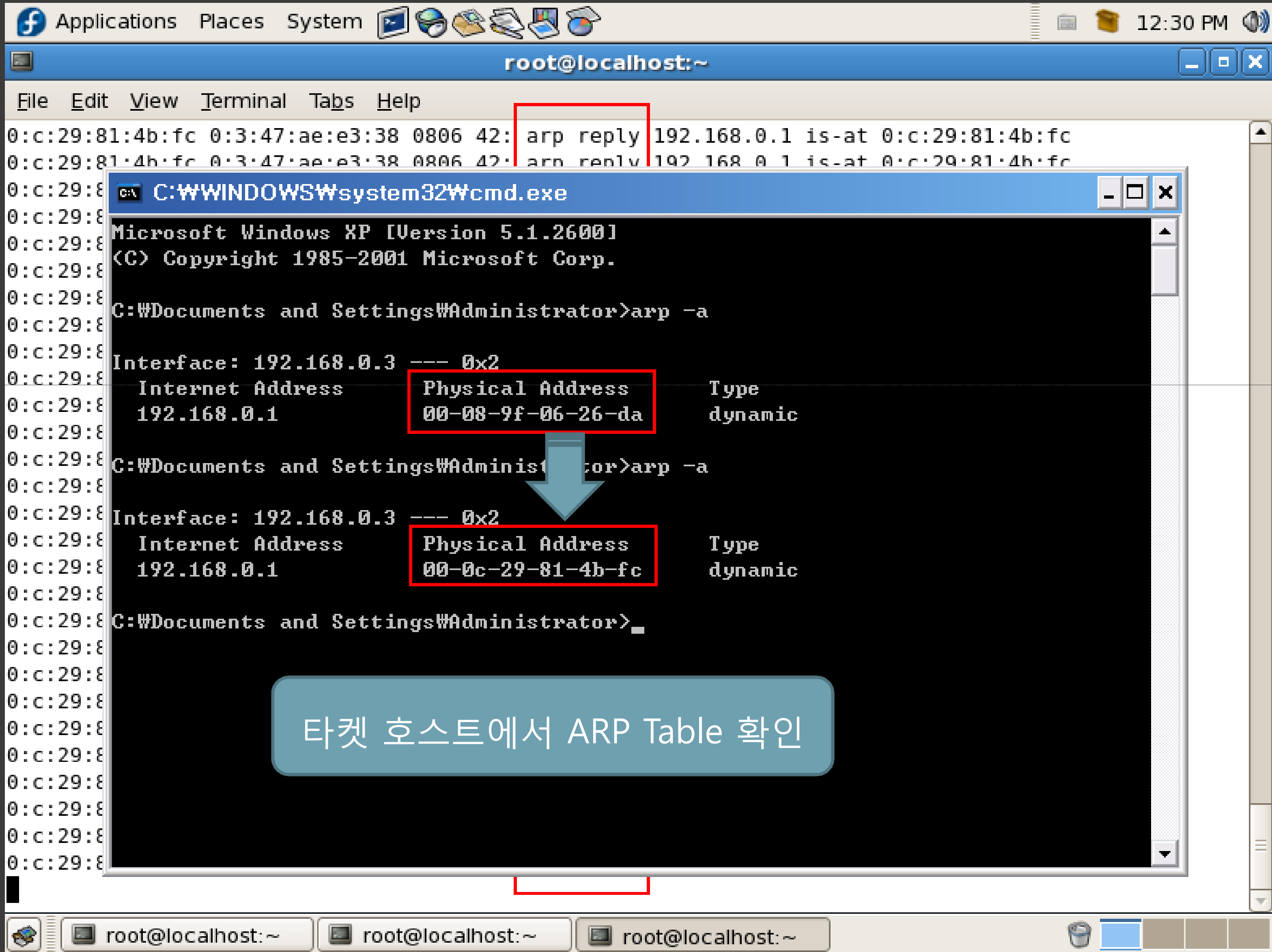


* 4. 모의해킹 2 (ARP Redirect 를 이용한 스니핑)

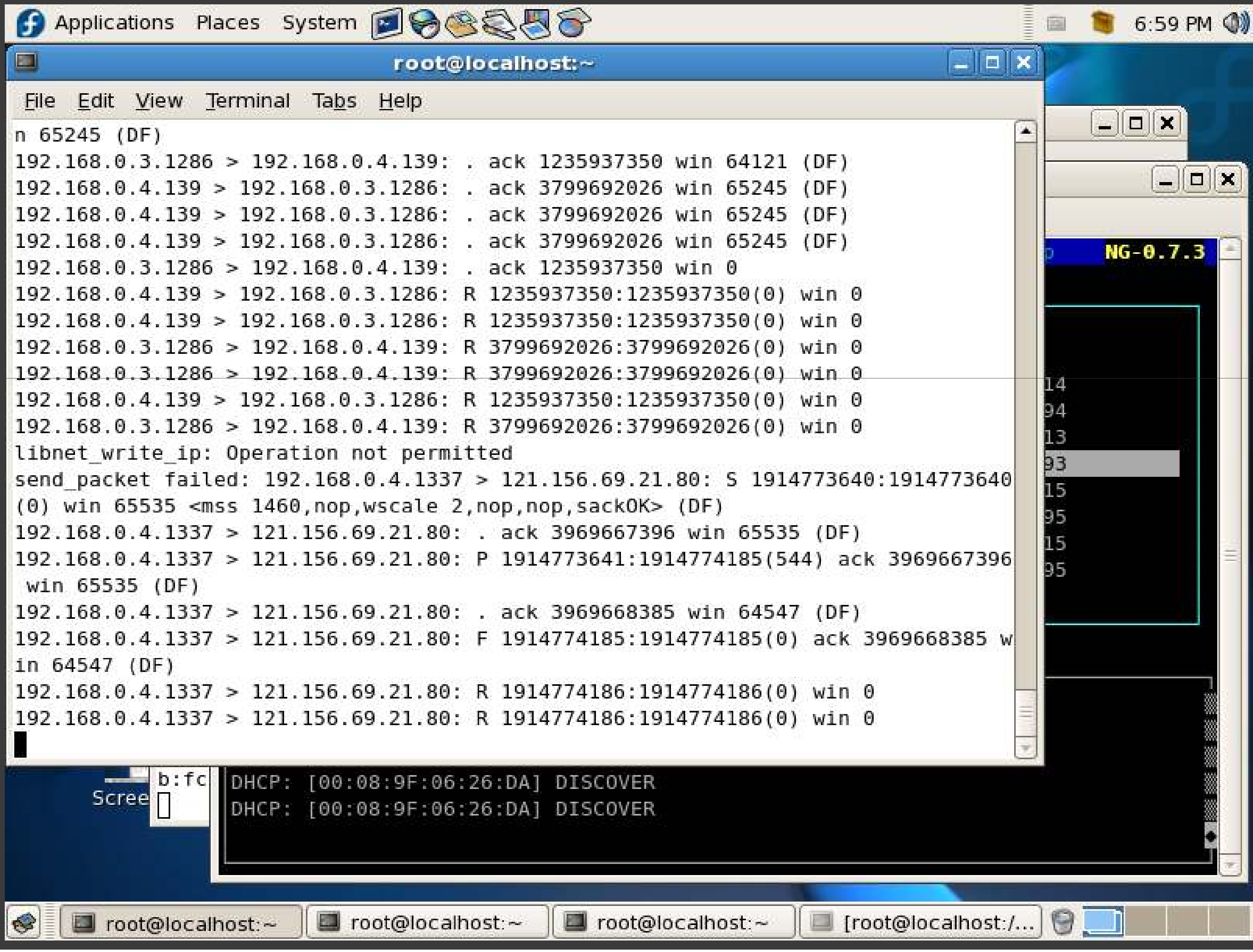


arpspoof –i eth0 –t 192.168.0.3 192.168.0.1

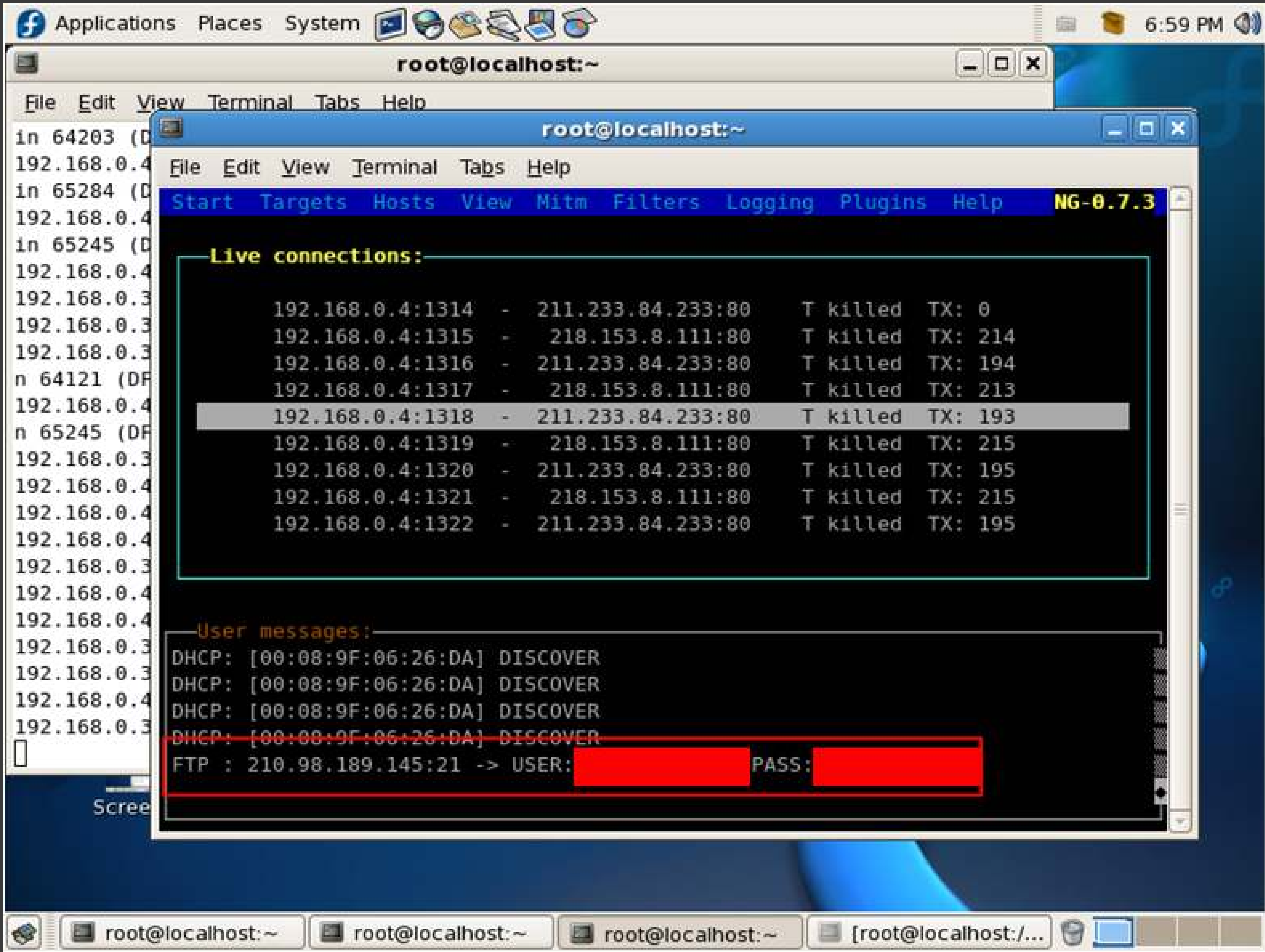
* 4. 모의해킹 2 (ARP Redirect 를 이용한 스니핑)



* 4. 모의해킹 2 (ARP Redirect 를 이용한 스니핑)



* 4. 모의해킹 2 (ARP Redirect 를 이용한 스니핑)



* 5. 스니핑 방지법

- ARP Table을 Static으로.
- 중요 패킷의 암호화.
  - SSH, SSL등의 암호화 프로토콜 사용
- 스니핑 탐지툴 사용.
  - AntiSniff, sentinel, XARP 등등

* 스위치 환경에서의 패킷 스니핑 *
(Packet Sniffing)

- 참 고 -

- http://www.certcc.or.kr/
- http://www.monkey.org/~dugsong/
- http://ettercap.sourceforge.net/
- http://www.googls.co.kr/ 검색
- http://네이버 큰형님/

* 스위치 환경에서의 패킷 스니핑 *
(Packet Sniffing)

Q & A

…

감사합니다 (*^^*)