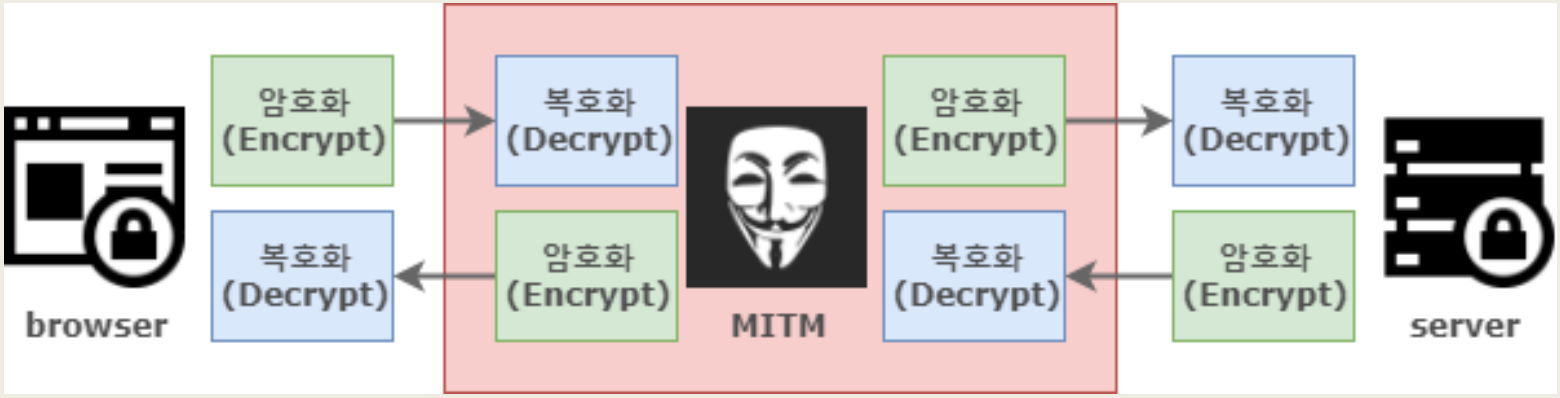
NETWORK SECURITY

한양대학교 소프트웨어융합대학 소프트웨어학부
이연준 교수

주요 사항

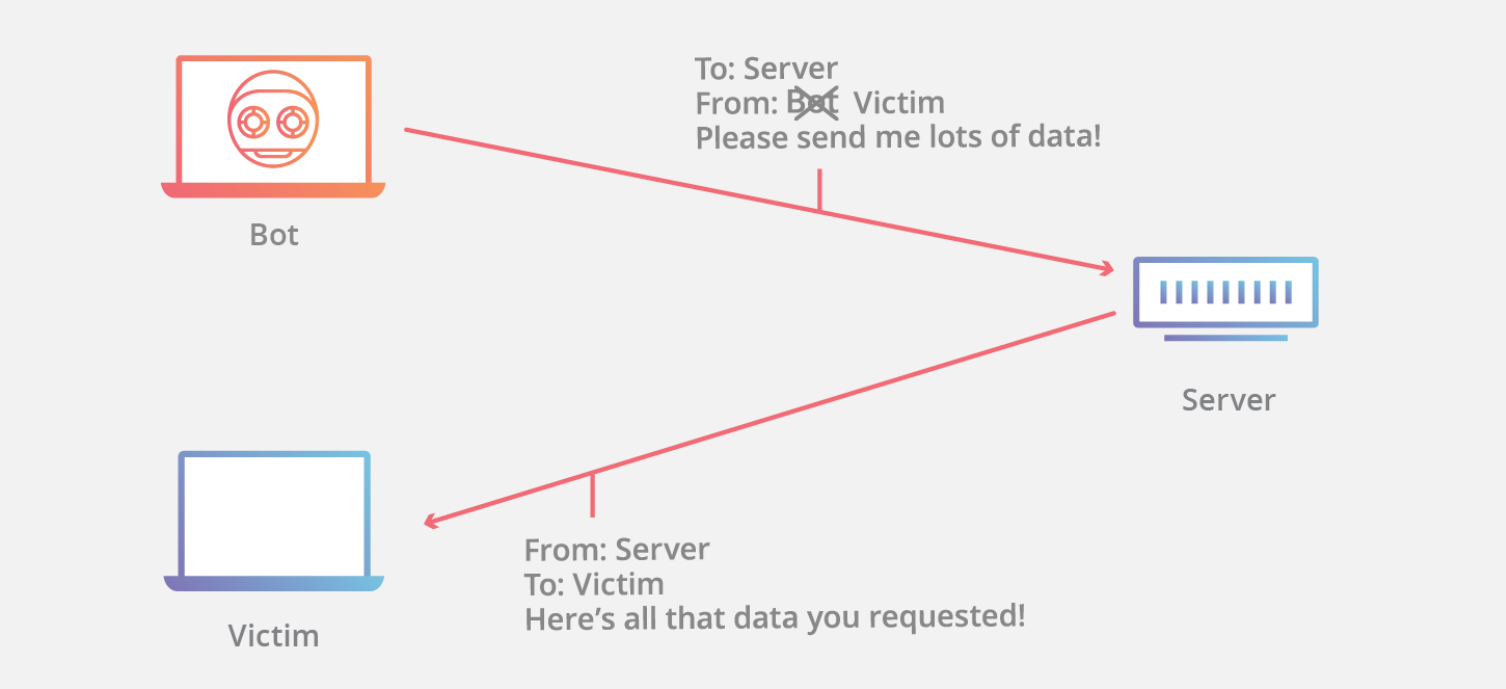
- **Sniffing / Spoofing** 에 대한 이해
- **Lab Preparation**
  - 실습 환경 구성
- **Lab Task**
- **Lab Question**
- **Evaluation**

MITM(Man In The Middle)



Sniffing

Spoofing


To: Server
From: Bot Victim
Please send me lots of data!
Bot
Server
From: Server
To: Victim
Here's all that data you requested!
Victim

Snoofing (Sniffing + Spoofing)

LAB PREPARATION

실습 환경 구성 준비

- 실습에 사용될 **Package** 설치
  - **sudo apt-get install xinetd**
  - **sudo apt-get install telnetd**

- **Packet** 분석을 위해 **Wireshark** 설치

실습 환경 구성 준비

- 설정 파일 수정
  - **sudo vi /etc/xinetd.conf**

```
# Simple configuration file for xinetd
#
# Some defaults, and include /etc/xinetd.d/

#default off
service telnet
{
        disable = no
        flags = REUSE
        socket_type = stream
        wait = no
        user = root
        server = /usr/sbin/in.telnetd
        log_on_failure = USERID
}

defaults
{

# Please note that you need a log_type line to be able to use log_on_success
# and log_on_failure. The default is the following :
# log_type = SYSLOG daemon info

}

includedir /etc/xinetd.d
~
```

LAB TASK

Sniffing – (1)

- 다음 코드를 통해 **ICMP** 패킷을 제대로 읽어들이는지 확인
  - **sniff1.py**

```
#!/bin/bin/python

from scapy.all import *

def print_pkt(pkt):
        pkt.show()

pkt = sniff(filter='icmp', prn=print_pkt)
```

- 작성 후 **sudo python sniff1.py**로 실행
- 다른 **VM**이나 로컬에서 **ping**을 보내 패킷을 읽는지 확인

Sniffing – (2)

- 이전 코드를 이용하여 다음 세 가지 코드를 작성하고 결과를 캡처할 것
  - **TCP** 패킷만 **sniffing**
  - **23**번 포트를 통한 **TCP** 통신**(telnet)**만 **sniffing**
  - **80**번 포트를 통한 **TCP** 통신**(http)**만 **sniffing**
  - 특정 **subnet**에서만 오는 **packet**만 **sniffing**

  (단**,** 특정 **subnet**은 현재 **VM**이 속한 서브넷으로 한다**)**
  - 다음 코드들은 **sniff2~4.py**와 같은 순서로 작성할 것

Spoofing

- 다음 코드를 통해 **ICMP** 패킷이 변조되어 전송되는지 확인
  - **spoof.py**

```
#!/bin/bin/python

from scapy.all import *

print("Sending Spoofed ICMP Packet.....")
ip = IP(src="...", dst="...")
icmp = ICMP()
pkt = ip/icmp
pkt.show()
send(pkt, verbose=0)
```

- 작성 후 **sudo python spoof.py**로 실행
- **Wireshark**를 통해 발신 **IP**가 변조되어 전송된 것을 확인

LAB QUESTION

Lab Question

1. **Sniffing**은 **Passive Sniffing**과 **Active Sniffing**으로 나뉘어 집니다. 이 둘의 차이를 설명하세요.

2. **Spoofing** 공격 기법으로는 **IP Spoofing, ARP Spoofing, E-mail Spoofing, DNS Spoofing**이 있습니다. 각 공격 기법에 대해 간략하게 설명하세요.

Evaluation

- **Lab Task** 진행
  - **3**개의 **Task**에서 진행한 과정을 캡처하고 설명할 것
- **Lab Question**
  - 주어진 문항에 대한 답과 해결 방안에 대해 간략하게 서술
- **Lab Task** 수행 결과를 위와 같이 명시한 대로 캡처하여 **MS Word** 또는 **PDF** 파일로 결과를 제출할 것.
  - 파일 형식 준수하지 않을 시 감점

Evaluation

- 과제 제출 기한 : 2019/12/02 23:59
- 과제 제출 시 메일 제목 및 파일명은 ‘본인 이름_학번’으로 제출
  - 예) 이석원_2019101059
  - 지연 제출의 경우 메일 제목 앞에 [지연제출]이라고 명시할 것
- sevenshards00@gmail.com으로 보낼 것.

Q&A