NETWORK SECURITY

한양대학교 소프트웨어융합대학 소프트웨어학부
이연준 교수

주요 사항

- **TCP/IP 공격 기법에 대한 이해**
- **Lab Preparation**
  - 실습 환경 구성
- **Lab Task**
- **Lab Question**
- **Evaluation**

TCP / IP Layer

OSI 7 Layer

L7	응용 계층 (Application Layer)
L6	표현 계층 (Presentation Layer)
L5	세션 계층 (Session Layer)
L4	전송 계층 (Transport Layer)
L3	네트워크 계층 (Network Layer)
L2	데이터 링크 계층 (Data Link Layer)
L1	물리 계층 (Physical Layer)

TCP/IP 4 Layer

L4	응용 계층 (Application Layer)
L3	전송 계층 (Transport Layer)
L2	인터넷 계층 (Internet Layer)
L1	네트워크 엑세스 (Network Access Layer)

DoS 공격 유형

- 네트워크의 대역폭이나 하드 디스크 공간 및 **CPU** 계산 시간과 같은 컴퓨팅 자원을 고갈하는 공격 → 자원 고갈 공격 **(REDoS)**
- 라우팅 정보와 같은 네트워크 구성 정보의 무력화
- 물리적인 네트워크 구성 요소를 무력화
- 이 중에서 가장 빈번하게 발생하면서 동시에 막기 힘든 유형의 공격은 자원 고갈 공격

TCP Flag

TCP Flag	Explanation
SYN (Synchronization)	**TCP** 연결을 설정할 때 가장 먼저 보냄
ACK (Acknowledgement)	상대방으로부터 패킷을 수신했음을 알림
RST (Reset)	재설정, 양방향에서 동시에 일어나는 중단 작업
PSH (Push)	받은 데이터를 즉시 목적지인 **Application** 계층으로 전송
URG (Urgent)	긴급한 데이터를 전송할 시 사용
FIN (Finish)	**TCP** 연결을 종료할 때 사용

Flooding Attack

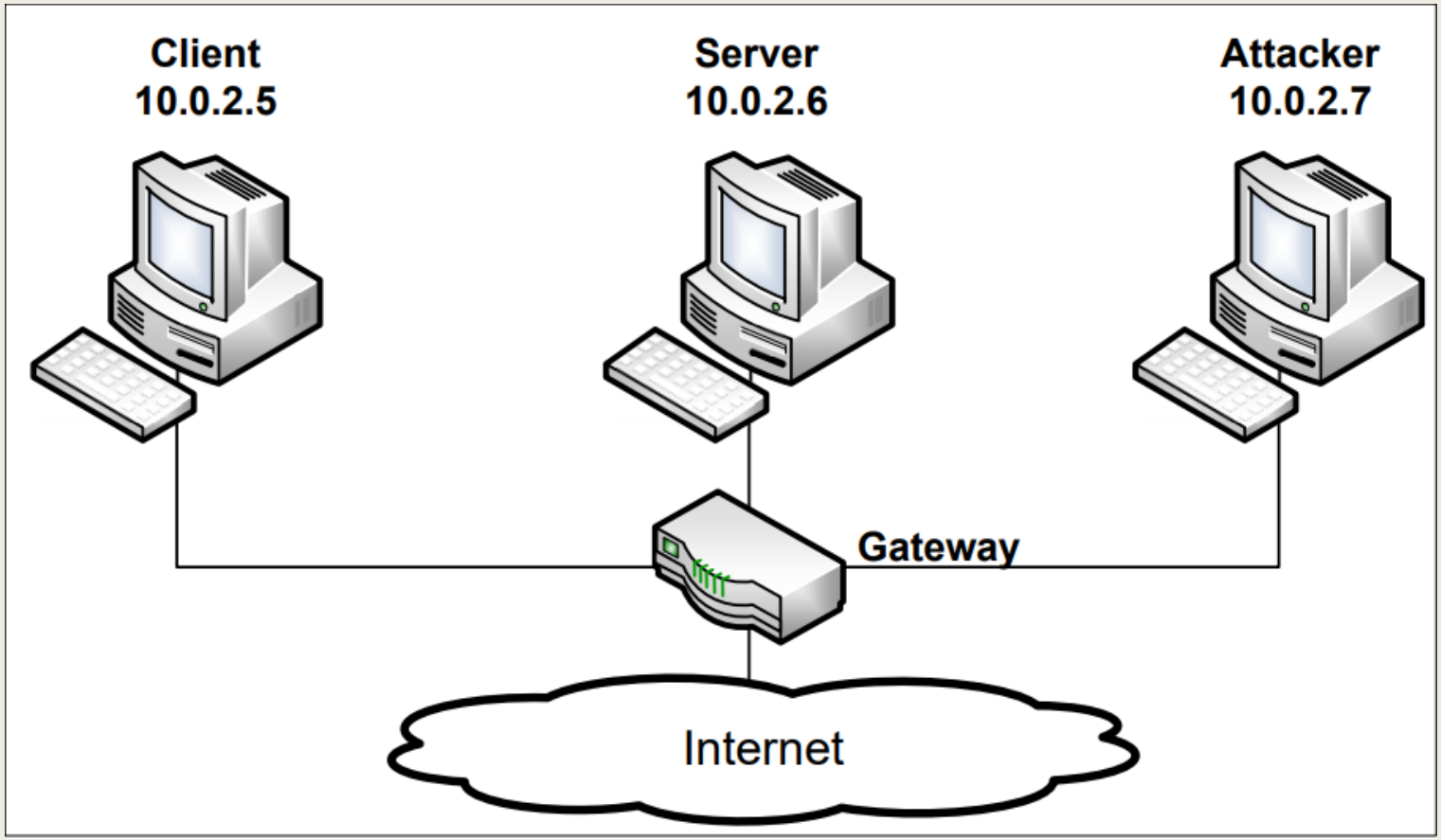
- **Flooding Attack**은 **SYN, RST, ACK** 등의 다양한 **Flag**를 통해 **Server**에서 처리하기 힘들 만큼 다량의 **Packet**을 전송하여 부하를 발생시키는 공격 기법이다.
- 그 중에서도 **SYN Flooding**은 가장 전통적인 **DoS** 공격 기법 중 하나이며 과도한 연결 요청을 통해 **Server**에 부하를 발생 시키는 공격이다.
- **RST Flooding**은 과도한 연결 중단 요청을 통해 다른 **Client**와 **Server**간의 정상적인 통신을 불가능하게 하는 공격이다.

LAB PREPARATION

실습 환경 구성 준비

- 실습에 사용될 **Package** 설치
  - **sudo apt-get install netwox**
  - **sudo apt-get install scapy**
- 설치 된 **VM** 복제
  - 실습에서 사용될 **VM**은 총 **3**대
  - **Server, Client, Attacker**
  - **VM**이 설치된 디렉토리로 이동하여 복사한 후 **VM**에 이를 등록
  - 이동한 것인지 복사한 것인지 여부를 물어볼 때는 복사했다고 선택
  - 다음에 보일 예시는 절대적인 것이 아니므로 본인의 **IP**를 잘 확인하여 실습환경을 설정할 것

실습 환경 구성 준비


Client
10.0.2.5
Server
10.0.2.6
Attacker
10.0.2.7
Gateway
Internet

LAB TASK

SYN Flooding

- 공격 대상은 **Server**로 하며, 공격자는 **Attacker**로 지칭
- **Server**에서 **SYN** 패킷을 받아들일 수 있는 **size**를 확인
  - **sudo sysctl –q net.ipv4.tcp_max_syn_backlog**
- 이후 **SYN Cookie**가 동작하고 있는지 확인
  - **sudo sysctl –a | grep cookie**
  - **sudo sysctl –w net.ipv4.tcp_syncookies=0 (동작 X)**
  - **sudo sysctl –w net.ipv4.tcp_syncookies=1 (동작 O)**
- 동작 중이라면 동작을 중단시키고 실습을 진행

SYN Flooding

- **Attacker**에서는 **Netwox**를 통해 **SYN Flooding** 공격을 **Server**에 실행
- **Netwox**를 이용한 **SYN Flooding** 용례
  - **netwox 76 –i ip –p port [-s spoofip]**
  - **ip**는 공격 대상지 **ip**
  - **port**는 공격 대상지의 **port**
- **Port**는 **80**번 포트를 사용
- 공격이 진행되는 동안 웹 브라우저를 통해 **Server**의 사이트에 접속이 잘 되는지 확인
- 또한 **Server**에서 **netstat –na** 명령어를 통해 **SYN** 패킷이 들어오는 양을 확인할 것

SYN Flooding

- 이후 **SYN Cookie**를 다시 동작시킨 후에 웹 브라우저를 통해 접속이 잘 되는지 확인할 것
- 또한 **netstat –na**를 통해 **SYN** 패킷이 들어오는 데 변경된 점이 있는지 확인할 것

RST Flooding

- 공격 대상은 **Server**와 **Client**로 하며, 공격자는 **Attacker**로 지칭
- **Attacker**에서는 **Netwox** 및 **Scapy**를 이용하여 **RST Flooding** 공격을 **Server**와 **Client**에 실행
- **Netwox**를 이용한 **RST Flooding** 용례
  - **netwox 78 –d device_name –f filter -s spoofip**
  - **device_name**은 네트워크 카드의 이름
  - **filter**에서 공격 대상지 **IP**와 포트를 설정
  - **spoofip**는 **linkb**로 설정
- **Port**는 **22**번 포트를 통해 **ssh** 연결을 두절 시키도록 함
- 공격이 진행되는 동안 **ssh** 연결이 유지되는지를 확인

RST Flooding

- **Scapy를 사용할 경우 (Skeleton Code)**
  - 파일명 : **rst_ssh.py**

```
#!/usr/bin/python
from scapy.all import *

ip  = IP(src="@@@@", dst="@@@@")
tcp = TCP(sport=@@@@, dport=@@@@, flags="@@@@", seq=@@@@, ack=@@@@)
pkt = ip/tcp
ls(pkt)
send(pkt,verbose=0)
```

LAB QUESTION

Lab Question

1. 실제로 **DoS (DDoS, DRDoS** 포함) 공격에는 다양한 유형의 공격들이 존재합니다. 그 중에서도 **Flooding** 공격은 **SYN**과 **RST** 이외에도 다양한 플래그를 통해 공격이 가능합니다. 이와 관련된 **Flooding** 공격들을 조사하여 간략하게 정리하여 설명하세요. (**SYN**과 **RST**를 포함하여 최소 **6**개 이상)

Evaluation

- **Lab Task** 진행
  - **2**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 : 2019/11/25 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