TCP SYN Flood - Denial of Service

Seung Jae Won
University of Windsor
wons@uwindsor.ca

Abstract

TCP SYN flooding attack is a kind of denial-of-service attack. This SYN flooding attack is using the weakness of TCP/IP. These days most computer system is operated on TCP/IP. The system using Windows is also based on TCP/IP, therefore it is not free from SYN flooding attack. In this document SYN flooding is simulated in Windows system with multiple hosts.

1. Introduction

These days many people do their job by using computers. These computers could connect each other through internet, which is based on TCP/IP. However, Transmission Control Protocol (TCP) has weakness when computers connected. Using this weakness anyone can attack the system. This attack is called TCP SYN flooding attack.

2. Transmission Control Protocol (TCP)

The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite (the other being Internet Protocol, or IP), so the entire suite is commonly referred to as TCP/IP [1]. IP performs actual delivery of data via internet, whereas TCP concerns only the data packets.

TCP connection between the two end computers is established by three-way handshake mechanism. The three-way handshake mechanism is below.

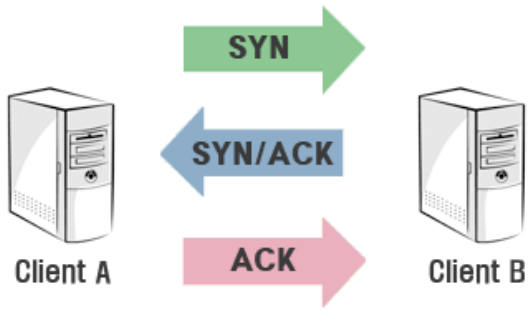


Figure 1 TCP Three-way Handshake

Step 1. Client A sends a SYN packet to Client B
Step 2. Client B sends a SYN/ACK packet to Client A
Step 3. Client A sends a ACK packet to Client B

3. TCP SYN Flood Attack

TCP SYN Flood attack uses the three-way handshake mechanism. At the first of the attack client A, an attacker, sends a SYN packet to client B. Then client B sends a SYN/ACK packet to client A. As a normal three-way handshake mechanism client A should send an ACK packet to client B, however, client A does not send an ACK packet to client B. In this case client B is waiting for an ACK packet from client A. This status of client B is called “half open”. This kind of incomplete connection is stored in Backlog Queue. After 75 seconds the incomplete connection is removed from Backlog Queue and it is disconnected.

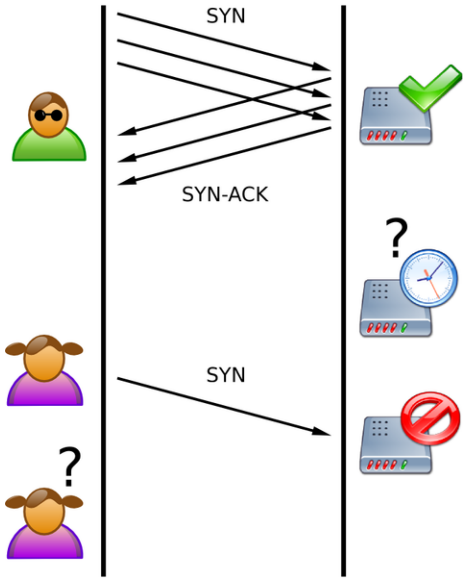


Figure 2 TCP SYN flood attack

However, if client A sends lots of SYN packets before client B removes incomplete connections from Backlog Queue, then Backlog Queue in client B is overflowed. In this case client B cannot accept TCP connection at all. This is called Denial-of-Service, and this type of attack is TCP SYN Flood Attack.

4. Tools

a. Wireshark v1.2.2 [2]

Wireshark is a network packet analyzer for various platforms, and it supports a lot of protocols.

Fetures

- Capture live packet data from a network interface.
- Available for UNIX and Windows.
- Display packets with very detailed protocol information.
- Open and Save packet data captured.
- Import and Export packet data from and to a lot of other capture programs.
- Filter packets on many criteria.

System Requirements

- Windows 2000, XP Home, XP Pro, XP Tablet PC, XP Media Center, Server 2003, Vista or Windows 2008 (XP Pro recommended)
- 32-bit Pentium or alike (recommended: 400MHz or greater), 64-bit processors in WoW64 emulation
- 128MB RAM system memory (recommended: 256MBytes or more) 75MB available disk space (plus size of user's capture files, e.g. 100MB extra)

b. Engage Packet Builder v2.2.0 [3]

Engage Packet Builder is a powerful and scriptable packet builder for windows platform.

Fetures

- Packet injection starting from link layer (MAC address spoofing)
- Custom payload in hex format / ASCII format
- Scripting engine
- Great for Firewall and IDS testing

Requirements

- Windows 2000 / XP
- WinPCAP 3.1 / 4.0

5. Project

A. System Configuration

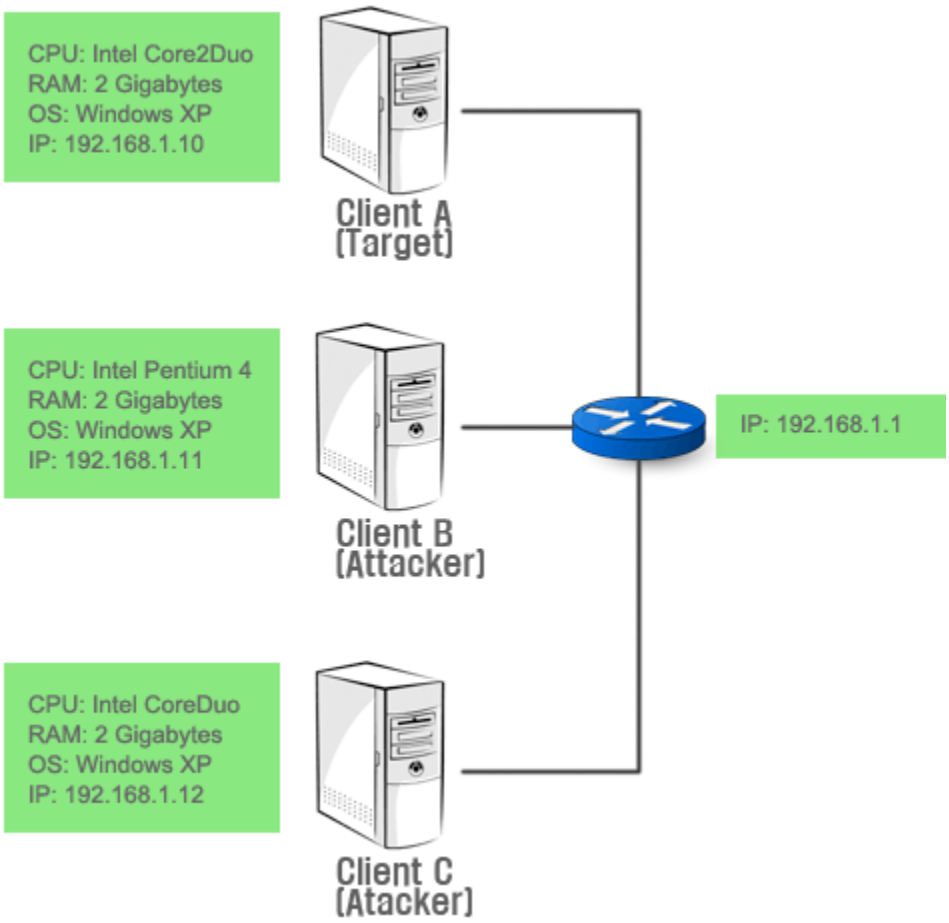


Figure 3 System Configurarion

B. Issues

- How to make SYN packets and send SYN packets

I use Engage Packet Builder to make SYN packets. This program is easy to build packets.

Step 1. We need to choose network interface. In my project I use wired network card.

Step 2. We should put source IP address and TCP port number. Also, we need to put target host's IP address and TCP port number.

Step 3. Choose one of TCP flags. In the project we use SYN flag.

Step 4. Put any number to send packets.

Step 5. Click Send button.

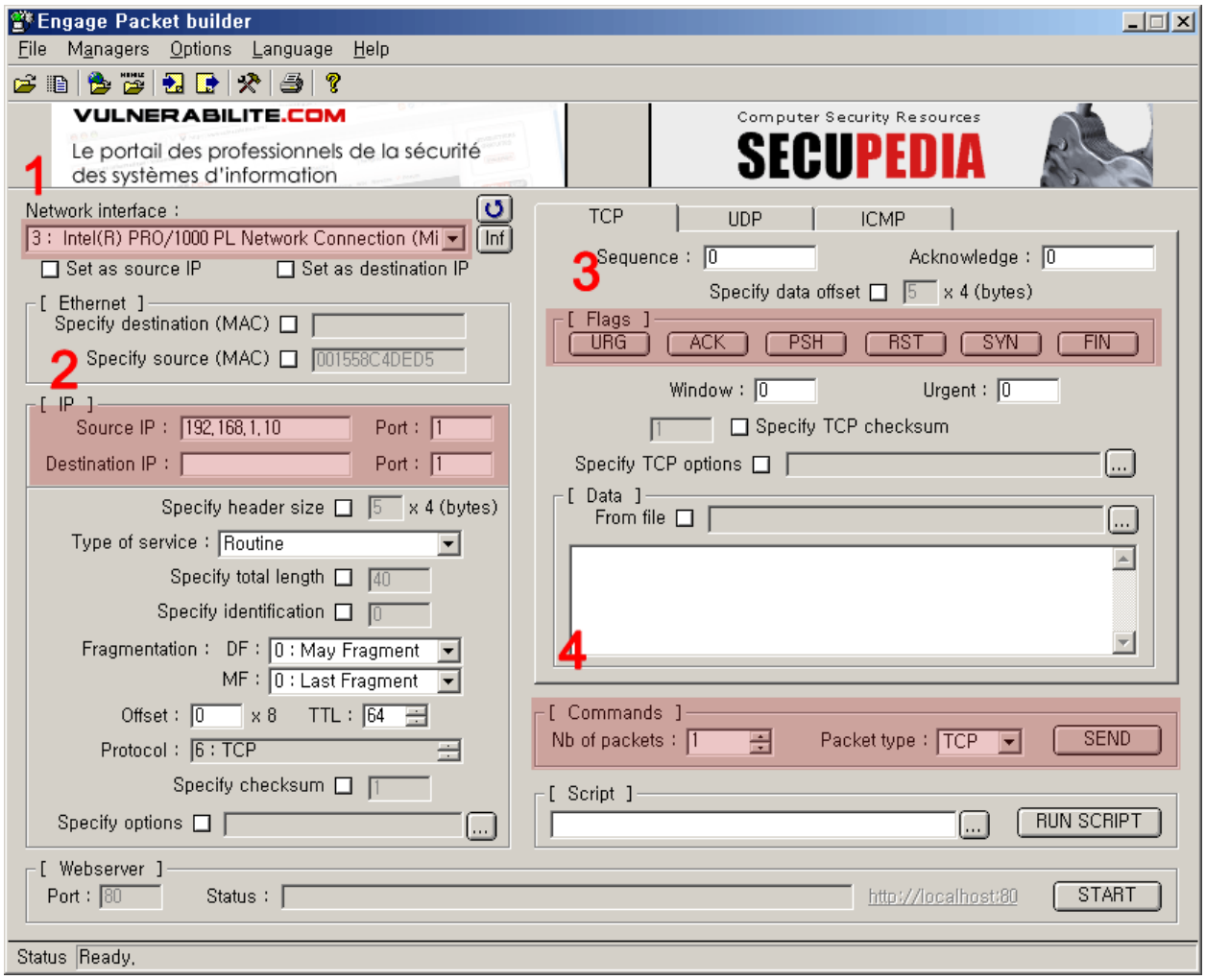


Figure 4 Engage Packet Builder

- How to analyze packets

I am going to use Wireshark to analyze packets.

Step 1. Click Capture Options

Step 2. Choose a network card to capture packets.

Step 3. (optional) To show particular type of packets we can choose a filter.

Step 4. Click Start.

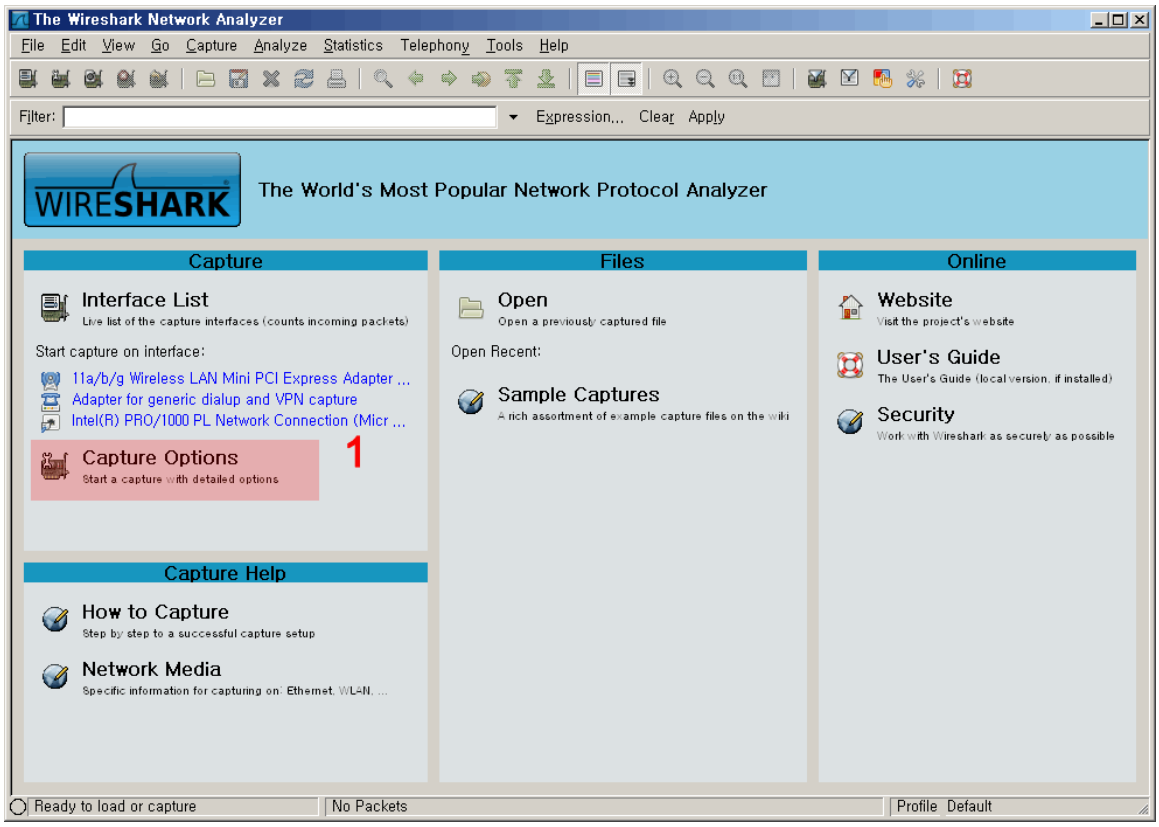


Figure 5 Wireshark

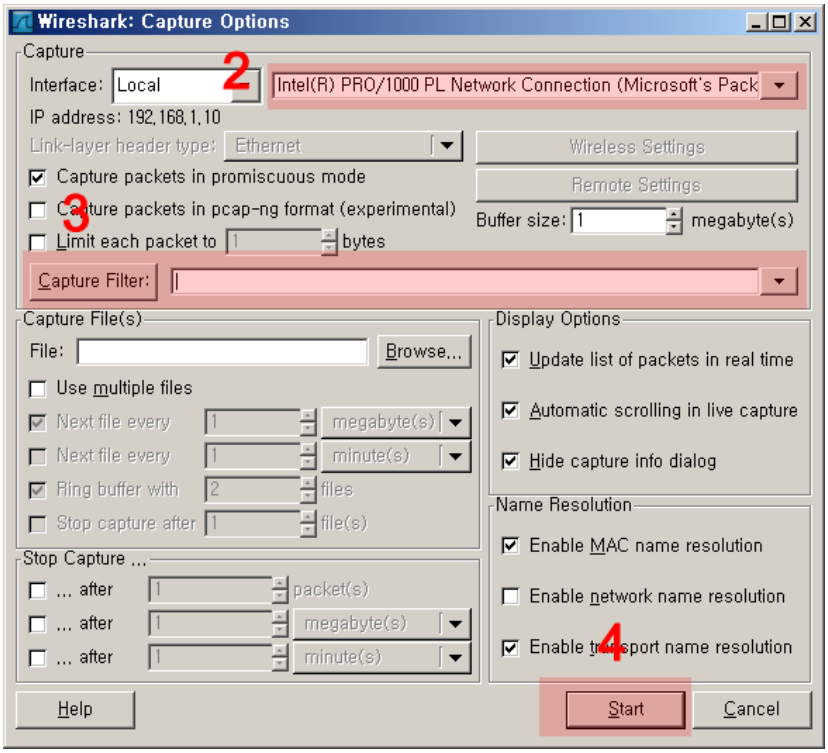


Figure 6 Wireshark Capture Options

- How to detect SYN flood attacks

In Wireshark I am going to analyze some packets. If TCP SYN packets are coming very quickly, then the system could be attacked.

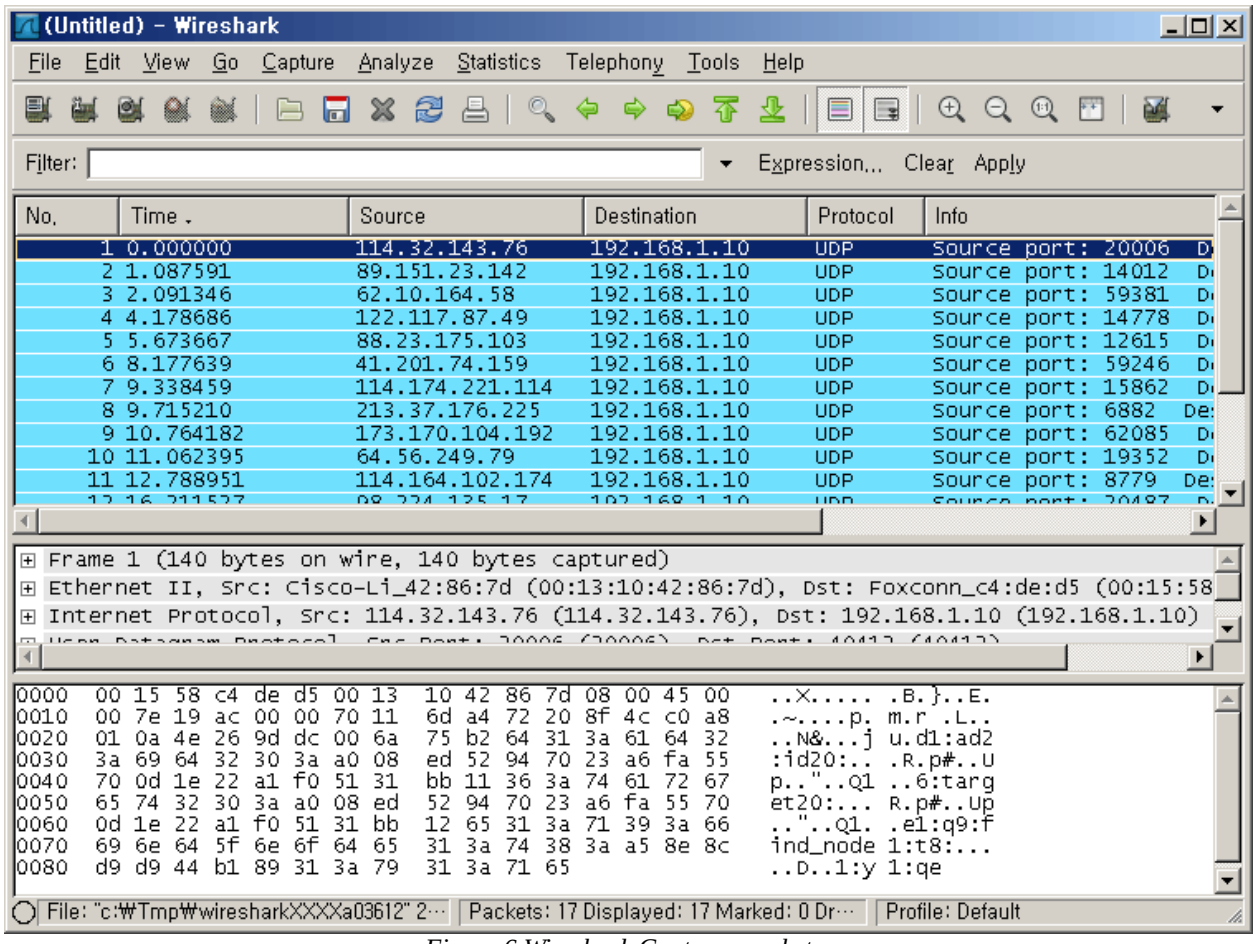
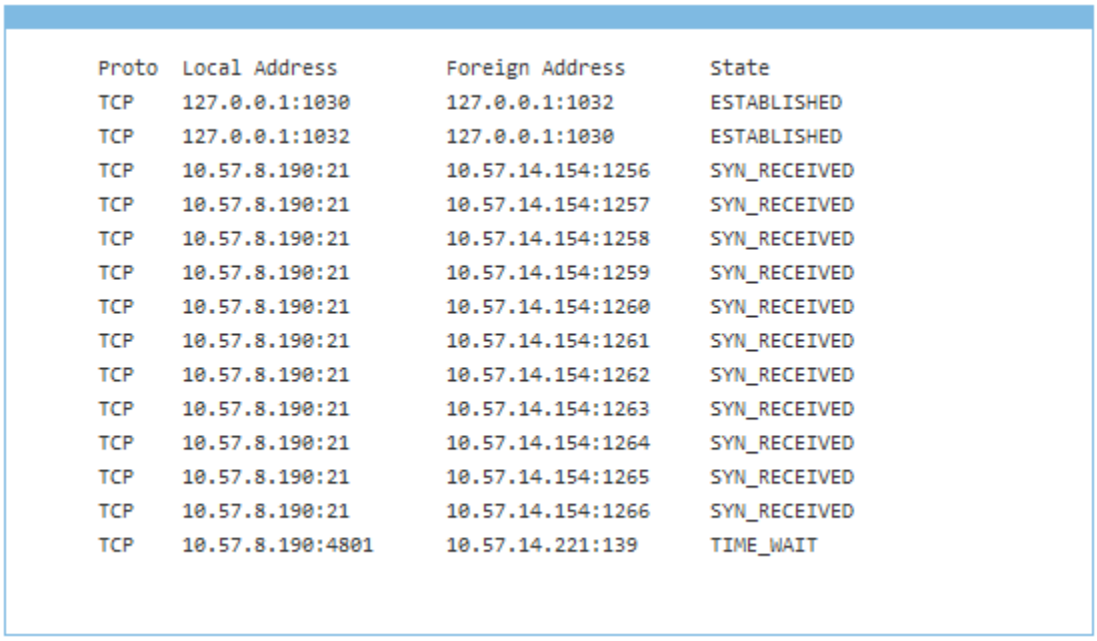


Figure 6 Wireshark Captures packets

Another way to verify that the system is under SYN flood attack is using **netstat** command. If you type the command, **netstat –n –p tcp**, then you can see the following. If a large number of connections are in the SYN_RECEIVED state, it is possible that the system is under attack [4].



Proto	Local Address	Foreign Address	State
TCP	127.0.0.1:1030	127.0.0.1:1032	ESTABLISHED
TCP	127.0.0.1:1032	127.0.0.1:1030	ESTABLISHED
TCP	10.57.8.190:21	10.57.14.154:1256	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1257	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1258	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1259	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1260	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1261	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1262	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1263	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1264	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1265	SYN_RECEIVED
TCP	10.57.8.190:21	10.57.14.154:1266	SYN_RECEIVED
TCP	10.57.8.190:4801	10.57.14.221:139	TIME_WAIT

Figure 8 SYN_RECEIVED

- How to protect system from the attacks

Microsoft recommends changing registry. I will do this end of the project.

C. Simulation

I installed Apache Web Server On host A. This program uses TCP port 80. On host B and C I installed Engage Packet Builder. A TCP SYN packet is sent by host B and host C thorough TCP port 80 to TCP host A. To use TCP port 80 of host B and host C we need to start virtual web server supported by Engage Packet Builder at the bottom. I send a packet from host B to host A for a test.

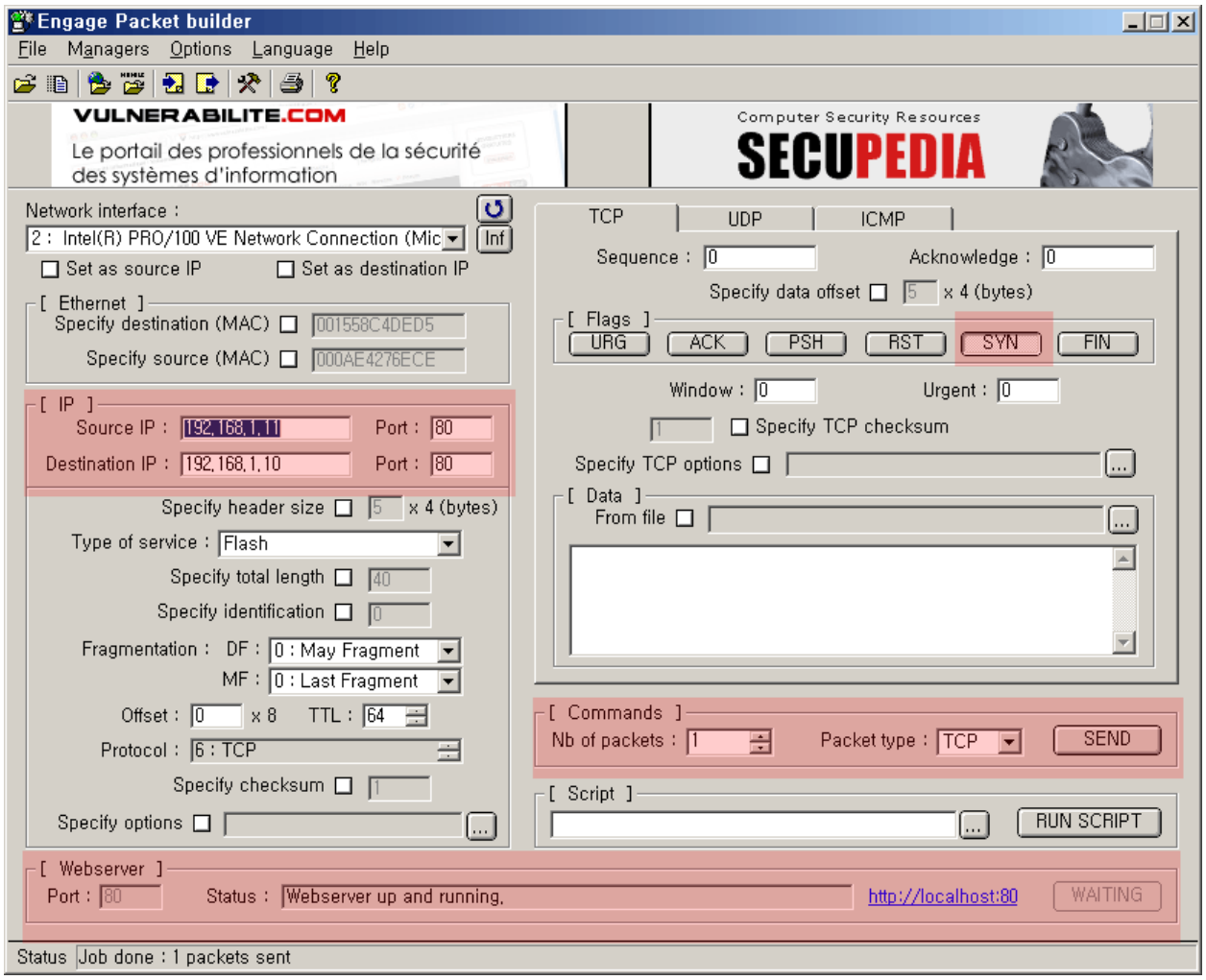


Figure 9 Sending a packet using Engage Packet builder

On host A I received the SYN packet from host B.

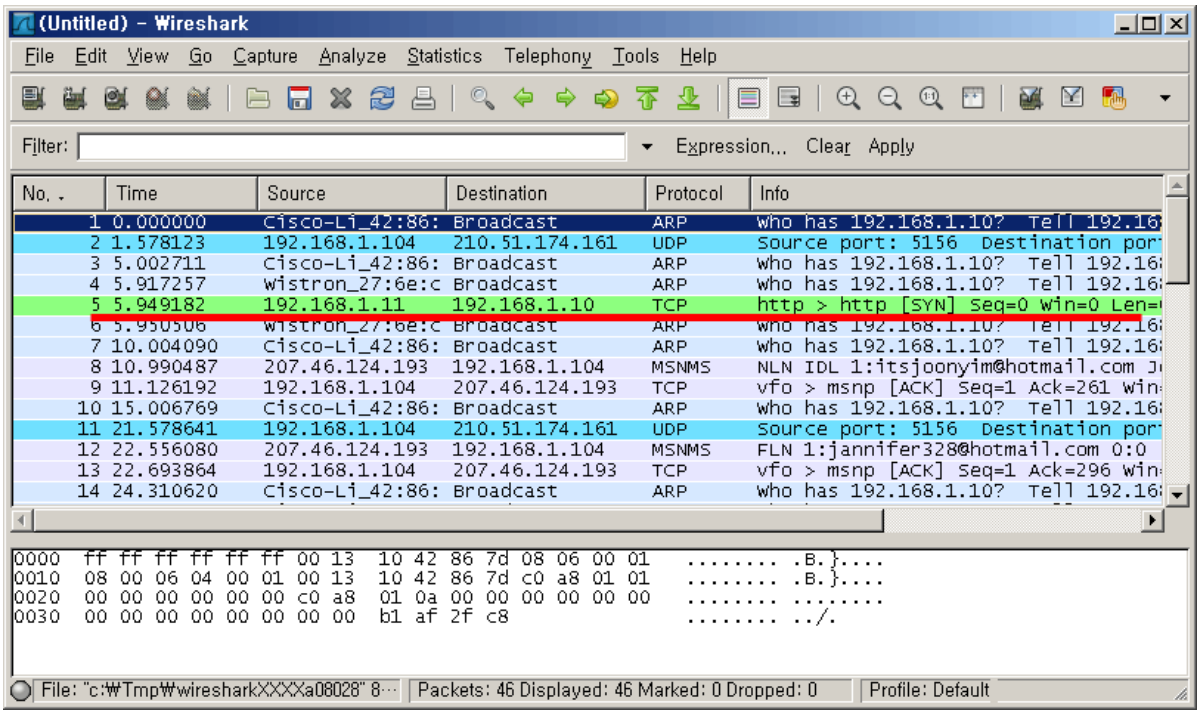


Figure 10 SYN packet captured

Now I am going to send a lot of SYN packets to host A from host B and host C. I apply TCP filter to Wireshark to see only TCP packets.

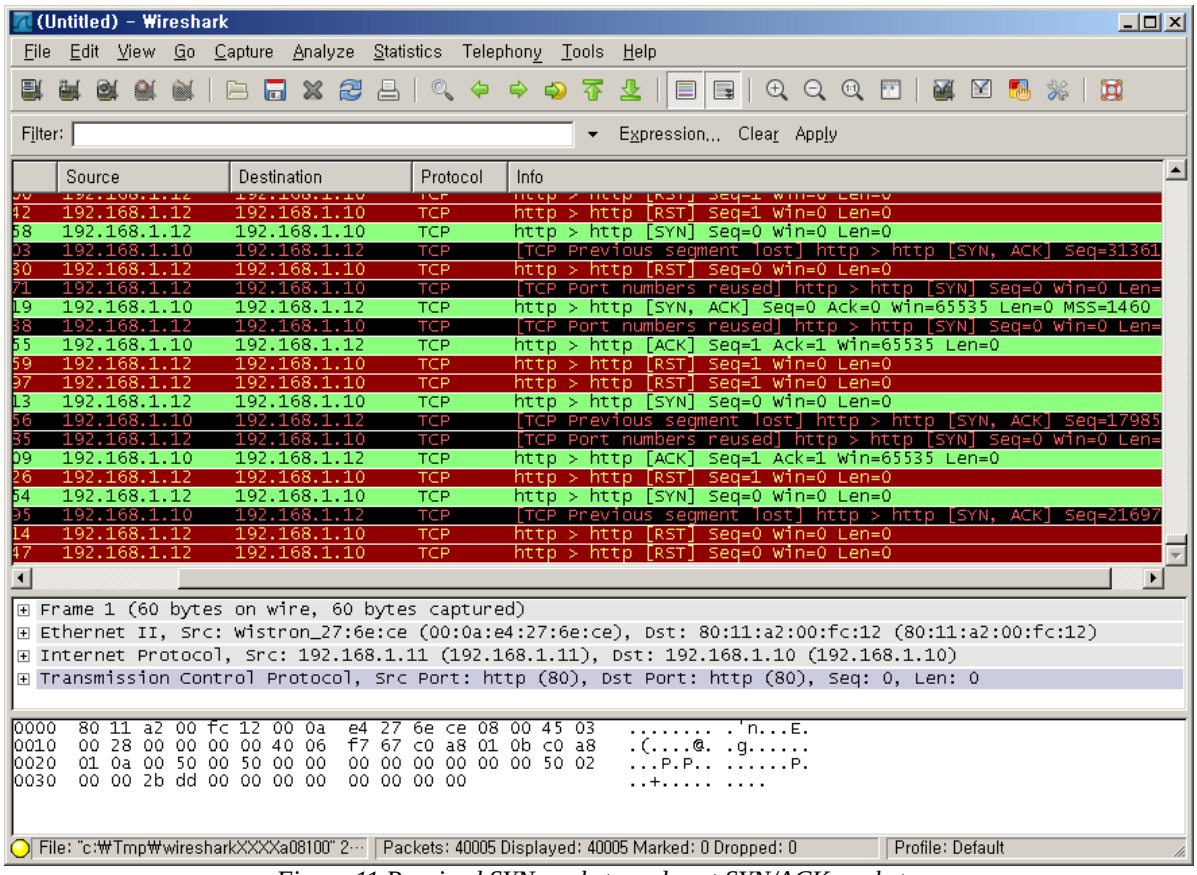


Figure 11 Received SYN packets and sent SYN/ACK packets

After the test I wanted to change source IP address and port. Then I made spoofed packets and sent to host A from host B. However, host A did not send SYN/ACK packets to spoofed IP. I guess that the router or the OS prevents spoofed packets by itself.

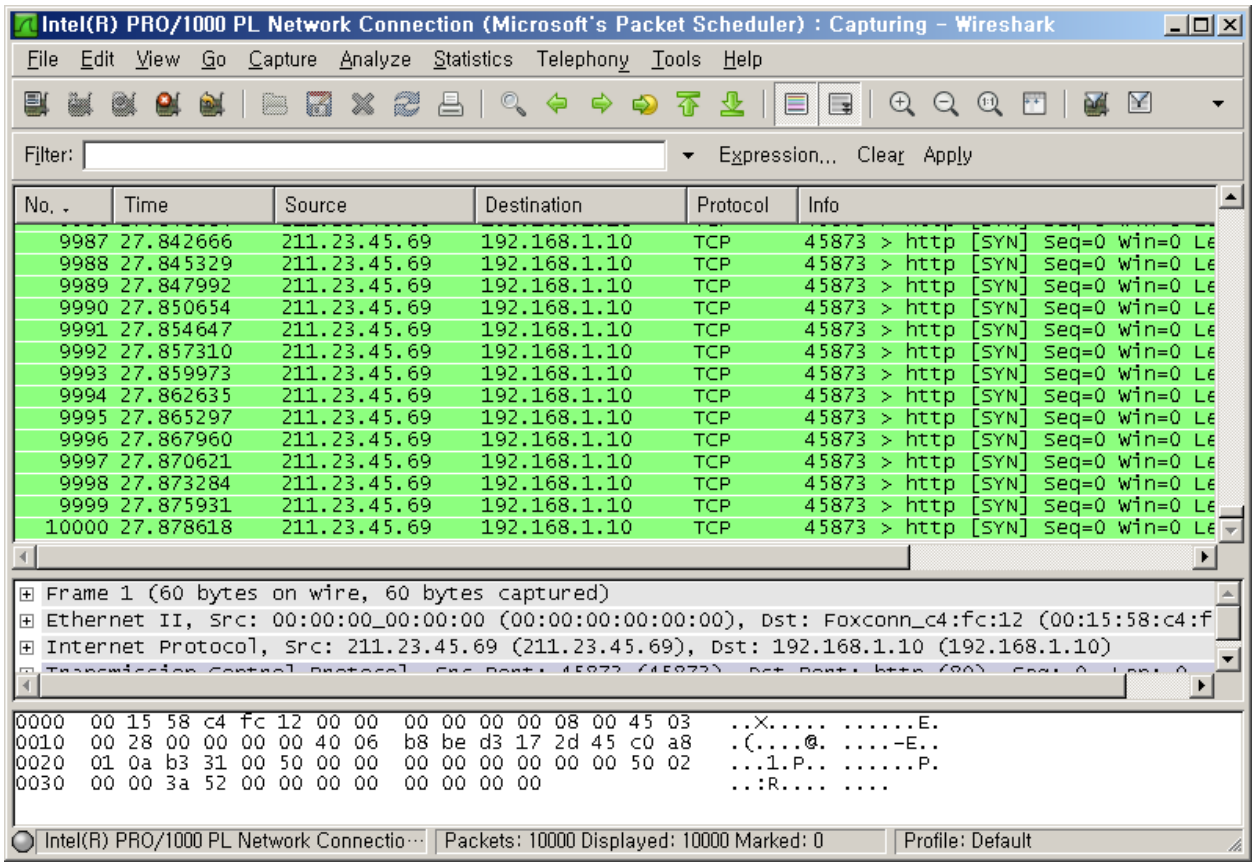


Figure 12 SYN packets

6. Protecting System against SYN flood attack

There are many ways to prevent TCP SYN flood attack. I introduce a way to protect Windows system from SYN flood attack. Microsoft recommends followings registry values.

i. Enable SYN attack protection
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpIp\Parameters
Value name: SynAttackProtect
Recommended value: 2
Valid value: 0,1,2
Description: Causes TCP to adjust retransmission of SYN-ACKS. When you configure this value the connection responses timeout more quickly in the event of a SYN attack. A SYN attack is triggered when the values of **TcpMaxHalfOpen** or **TcpMaxHalfOpenRetried** are exceeded.

ii. Set SYN Protection Thresholds
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\TcpIp\Parameters
Value name: TcpMaxPortsExhausted
Recommended value: 5
Valid value: 0-65535
Description: Specifies the threshold of TCP connection requests that must be exceeded before SYN flood protection is triggered.
Value name: TcpMaxHalfOpen
Recommended value data: 500
Valid value: 100-65535
Description: When SynAttackProtect is enabled, this value specifies the threshold of TCP connections in the SYN_RCVD state. When SynAttackProtect is exceeded, SYN flood protection is triggered.

Value name: TcpMaxHalfOpenRetried
Recommended value data: 400
Valid value: 80-65535
Description: When **SynAttackProtect** is enabled, this value specifies the threshold of TCP connections in the SYN_RCVD state for which at least one retransmission has been sent. When **SynAttackProtect** is exceeded, SYN flood protection is triggered.[5]

7. Conclusion

This document introduced the concepts of TCP connection and TCP SYN flood attack. In the project, the attacks from host B and host C to host A failed. However, if there are lots of SYN attacks to a particular system, the attacks could succeed. Therefore, system administrators should prepare the attacks by using packet analyzing tools or Intrusion Detection System (IDS).

8. Reference

[1] Wikipedia: Transmission Control Protocol http://en.wikipedia.org/wiki/Transmission_Control_Protocol, Accessed October 9, 2009
[2] Wireshark http://www.wireshark.org/about.html, Accessed October 9, 2009
[3] Engage Security http://www.engagesecurity.com/products/engagepacketbuilder, Accessed October 9, 2009
[4] Internet server unavailable because of malicious SYN attacks http://support.microsoft.com/default.aspx?scid=KB;en-us;142641&, Accessed October 17, 2009
[5] How To: Harden the TCP/IP Stack http://msdn.microsoft.com/en-us/library/aa302363.aspx, Accessed October 15, 2009
[Figure 2] File:Tcp synflood.png http://en.wikipedia.org/wiki/File:Tcp_synflood.png, Accessed October 15, 2009
[Figure 8] Internet server unavailable because of malicious SYN attacks http://support.microsoft.com/default.aspx?scid=KB;en-us;142641&, Accessed October 17, 2009