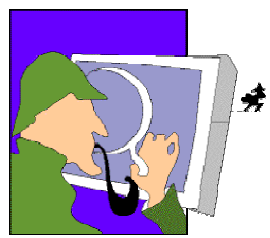
Anatomy of Denial of Service Attack and Defense in a Lab Environment

Dongqing Yuan
Department of Information Technology Management
University of Wisconsin-Stout
Yuanh@uwstout.edu

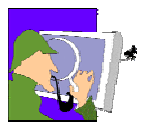
Dr. Jiling Zhong
Department of Computer Science
Troy University
Jzhong@troy.edu



23rd Annual Computer Security Application Conference
Miami, Florida 12/13/2007

Overview

- Introduction of DoS attack
- Attack 1– Target is the host
- Attack 2 – Target is the network
- Summary

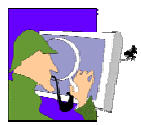


What is Denial of Service Attack?

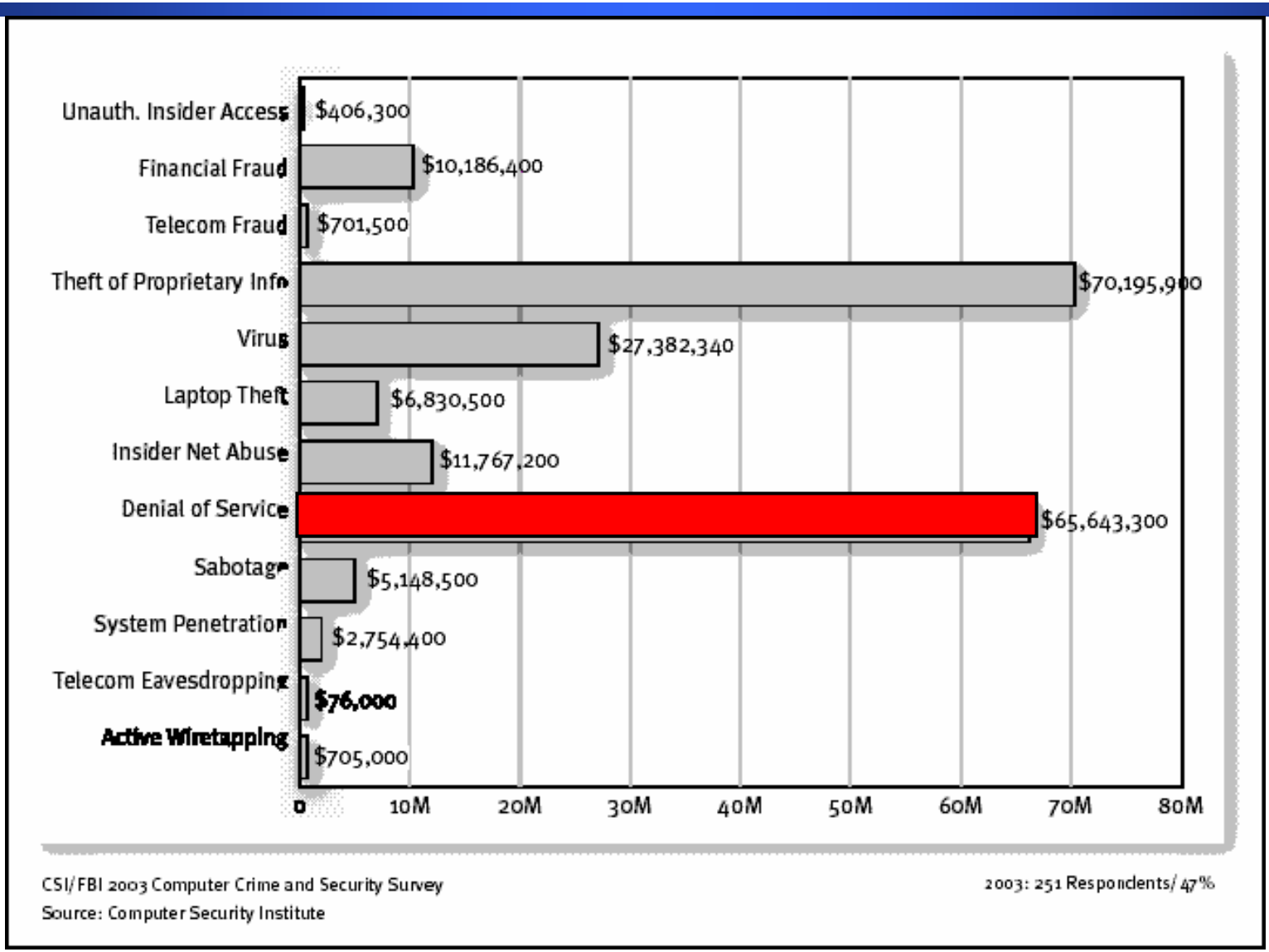
- "Attack in which the primary goal is to deny the victim(s) access to a particular resource." (CERT/CC)
- The definition covers many types of DoS
- Three basic types of DoS– Smurf, Fraggle, SYN Flood Attack.
- This study only focuses on SYN Flood Attack
  - SYN Flooding DoS attacks are the most popular DoS attacks

Why it is important to exam this attack?

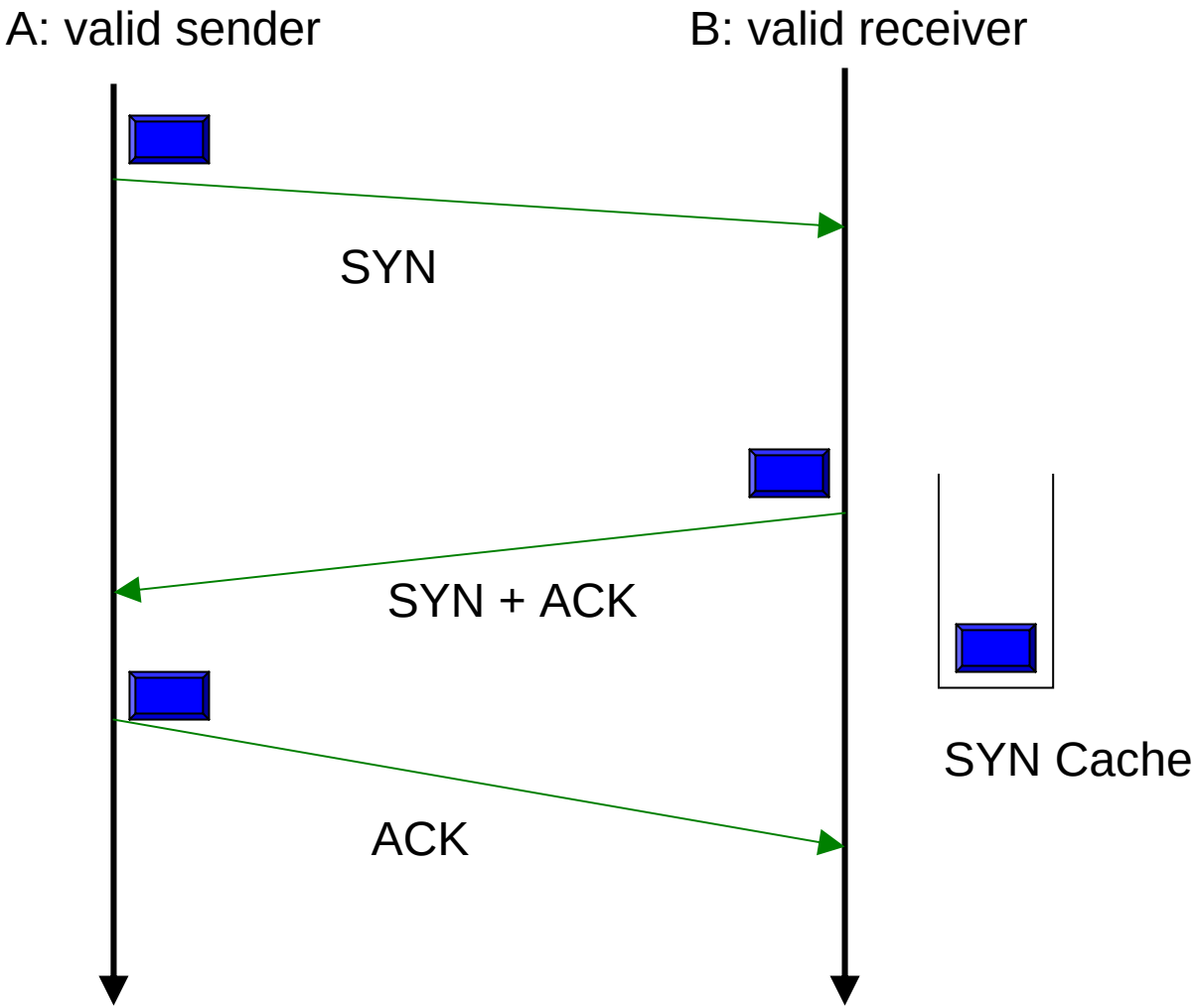
- Easier to launch the attack
- Many incentives for attackers: unauthorized use, ego, hate, disrupt competitor…
- The design of the Internet
- There is no universal solution to the attack

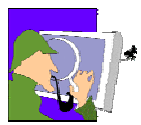


Dollar Amount of Losses by Type

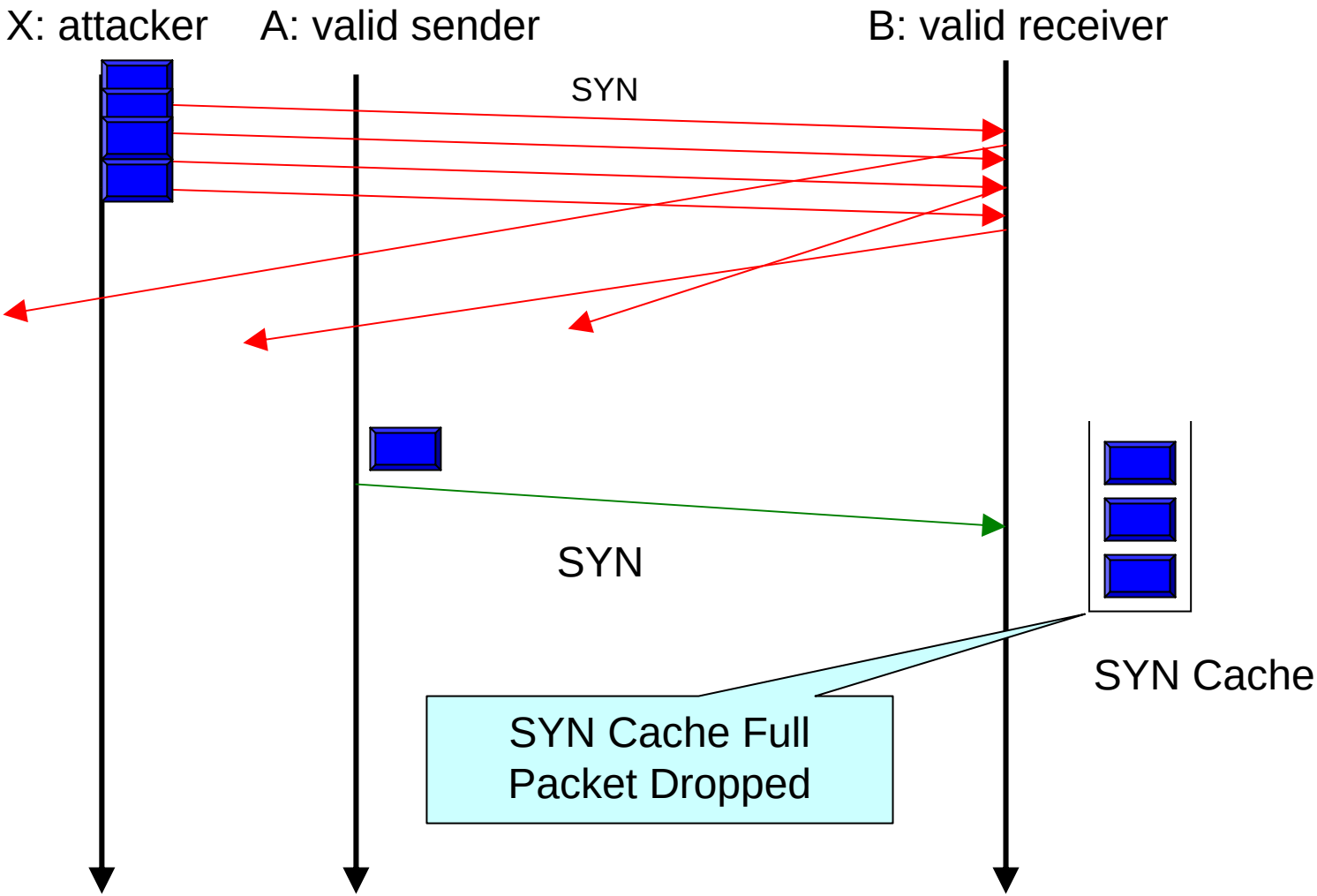


TCP is susceptible to DoS attacks



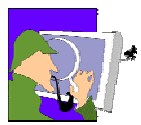


TCP is Susceptible to DoS Attacks



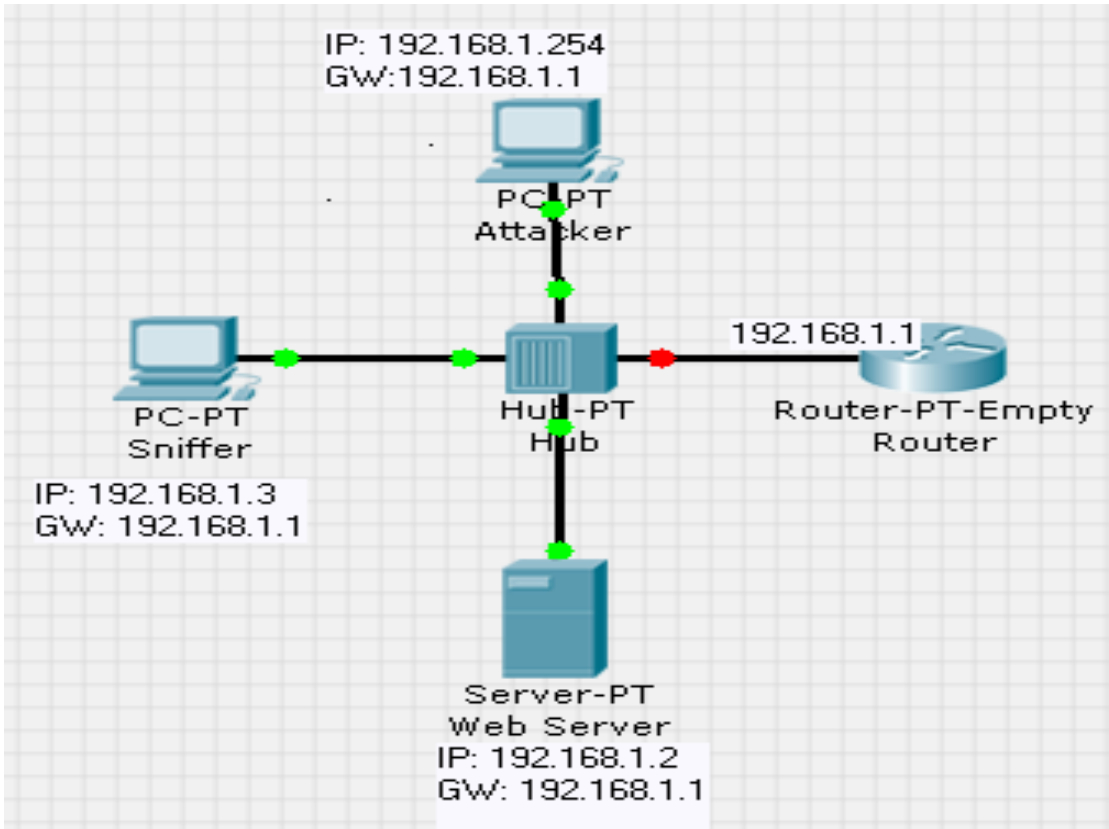
DoS Tools

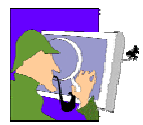
- There are lots of DoS tools.
- In our simulation, we use Datapool. Datapool is a powerful DoS tool that includes 106 DoS attacks.
- http://packetstormsecurity.org/DoS/datapool2.0.tar.gz



Attack 1– Target is the End Node

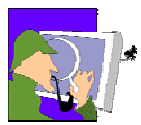
- Topology: A hub connect web server, sniffer and attacker.





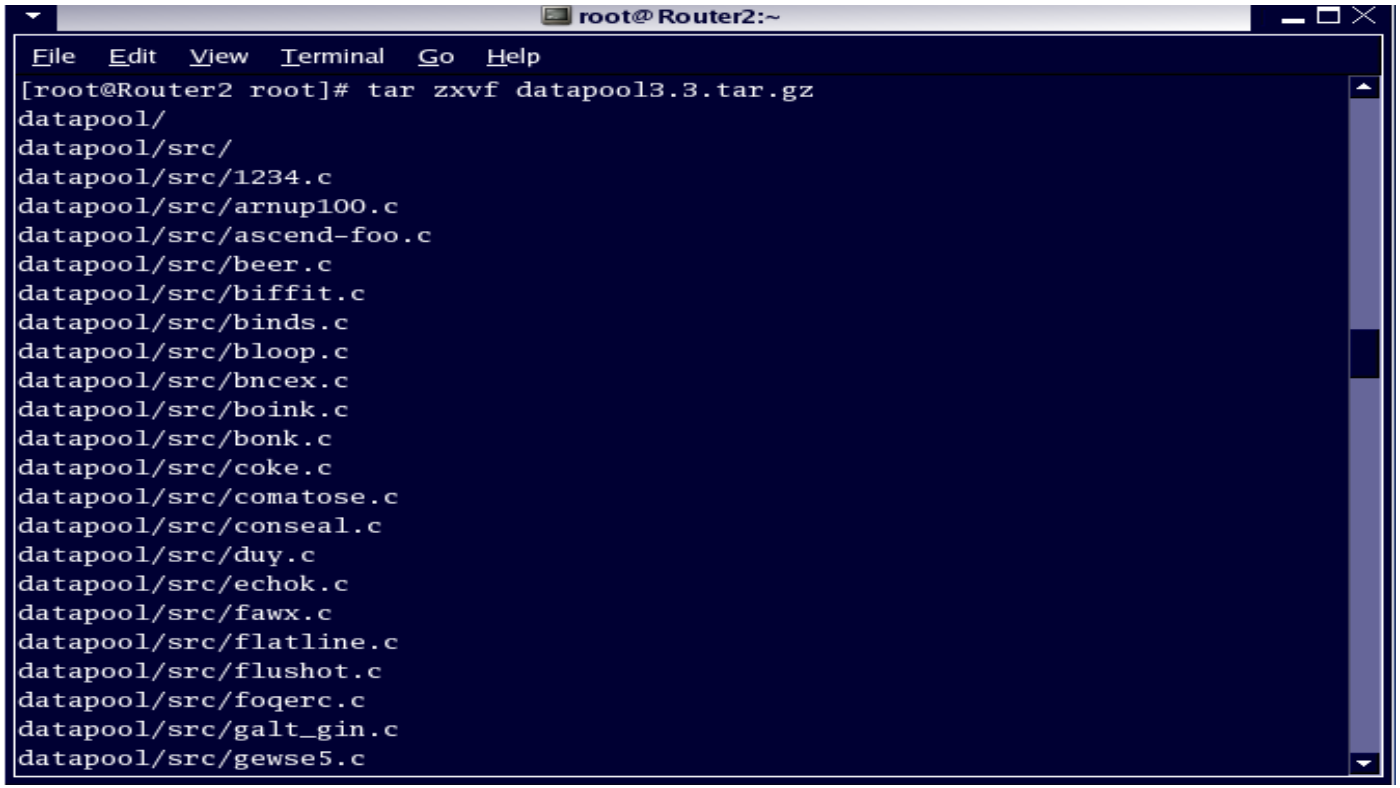
Lab Requirement for Attack 1

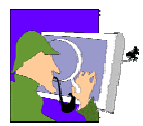
- A Linux machine is set up as an HTTP Server, the IP address of which is 192.168.1.2.
- A Windows XP computer is set up as a Sniffer running Ethereal, which is a program that turns a computer's NIC card into promiscuous mode to gather all packets on the wire. The Sniffer's IP address is 192.168.1.3.
- Another Linux machine is set up as an Attacker, running Datapool. The attacker's IP address is 192.168.1.254.



Extract the DoS tool

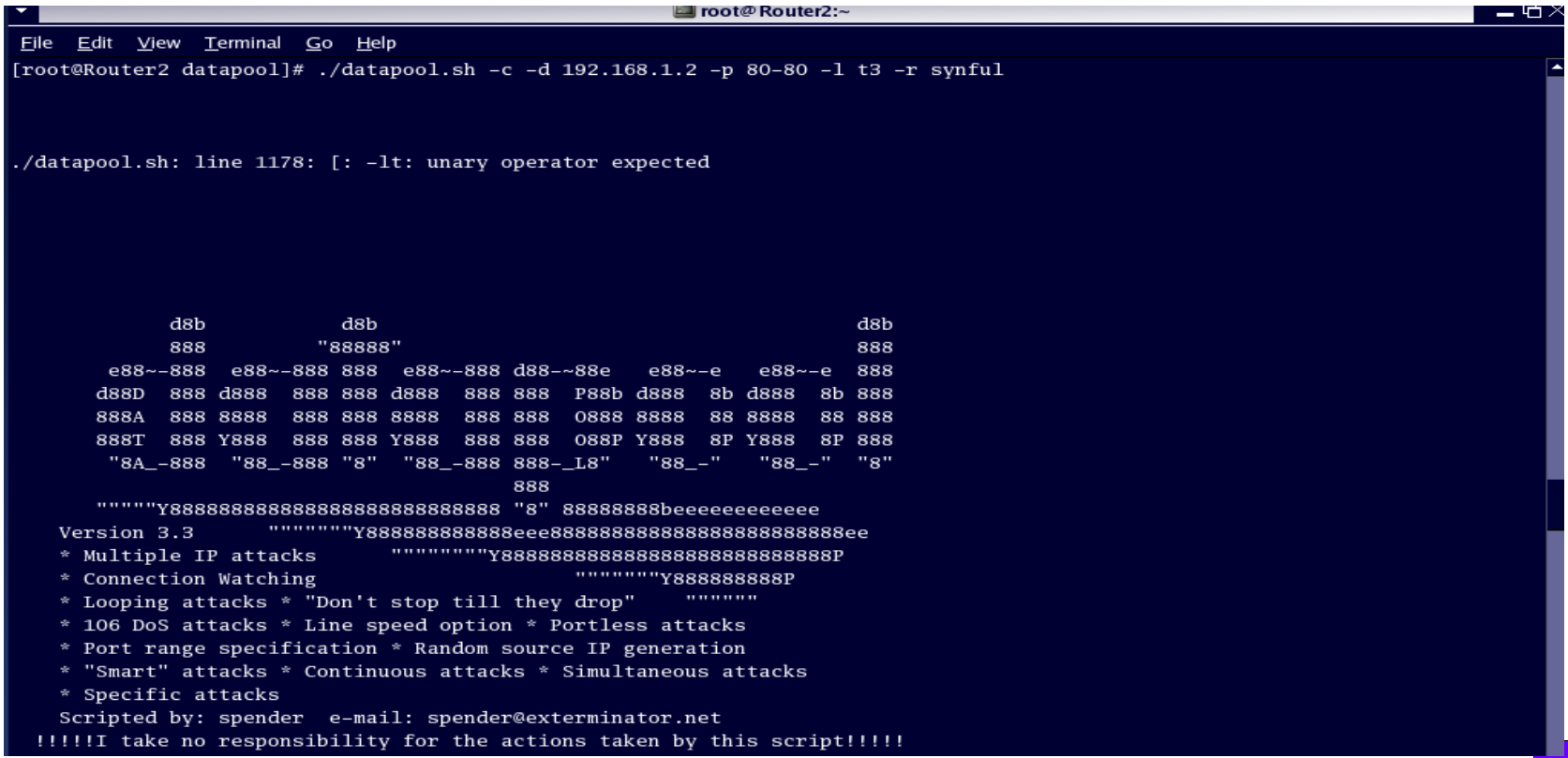
Download the Datapool and extract the file.

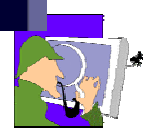




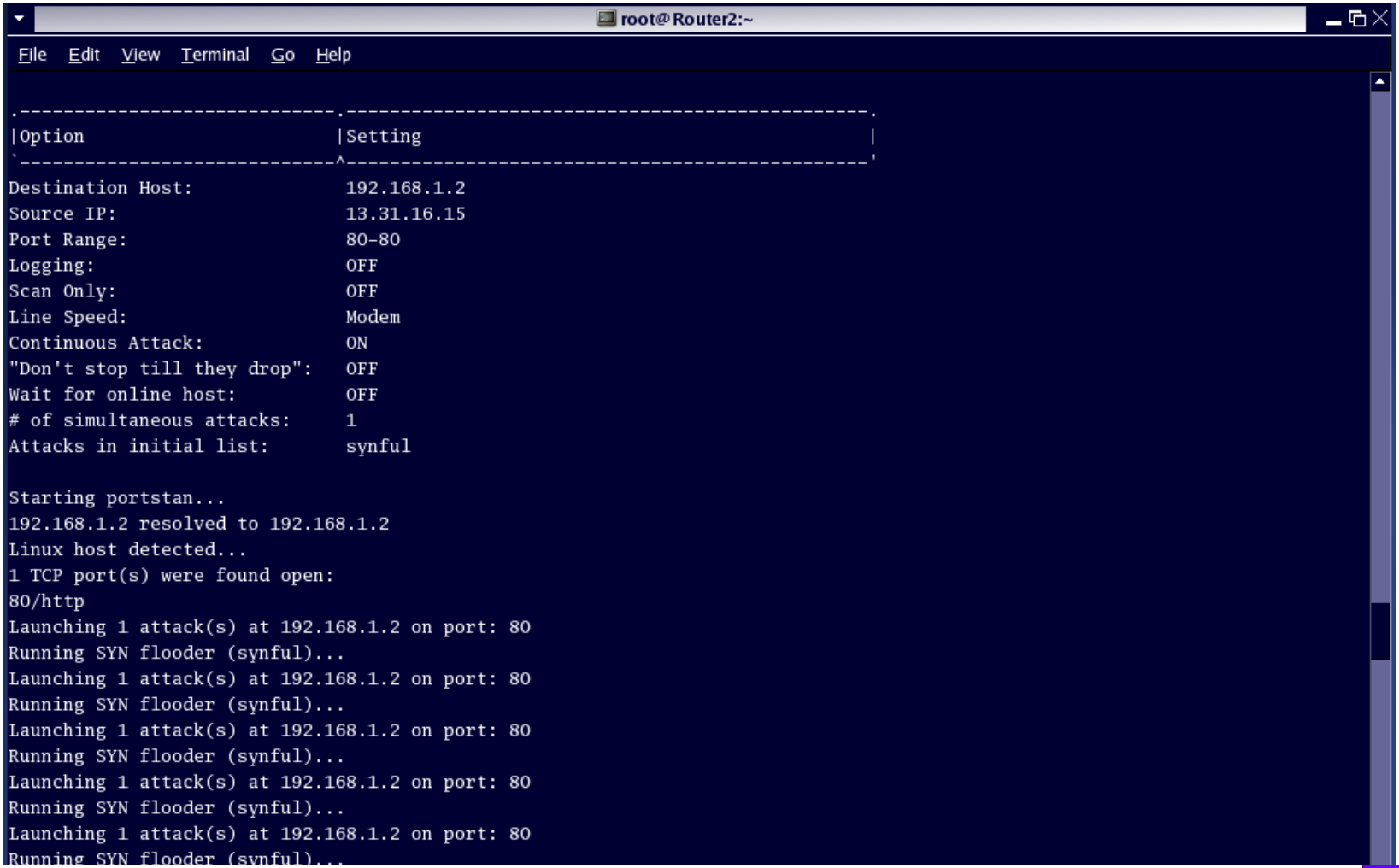
Lauching the DoS attack to the server

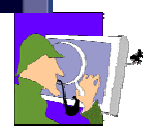
We launch the DoS SYN flood attack by running *datapool.sh* with our HTTP Server as the destination, 80 as the port, T3 as the line speed, and *sinful* as the attack type



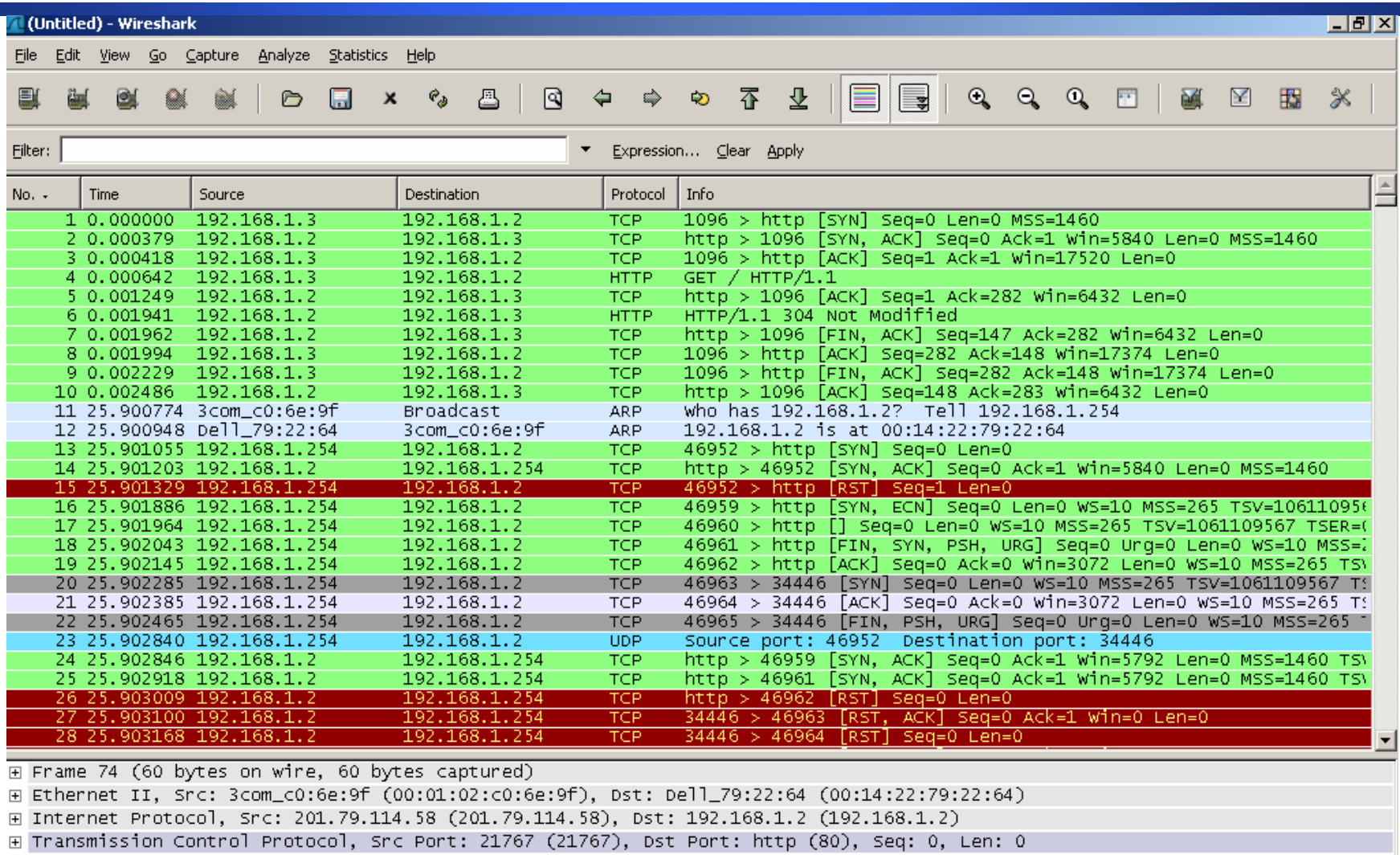


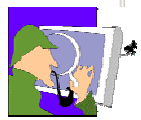
Attacking…


root@Router2:~
File Edit View Terminal Go Help
.----------------------------.---.
|Option |Setting |
`----------------------------^---'
Destination Host: 192.168.1.2
Source IP: 13.31.16.15
Port Range: 80-80
Logging: OFF
Scan Only: OFF
Line Speed: Modem
Continuous Attack: ON
"Don't stop till they drop": OFF
Wait for online host: OFF
# of simultaneous attacks: 1
Attacks in initial list: synful
Starting portstan...
192.168.1.2 resolved to 192.168.1.2
Linux host detected...
1 TCP port(s) were found open:
80/http
Launching 1 attack(s) at 192.168.1.2 on port: 80
Running SYN flooder (synful)...
Launching 1 attack(s) at 192.168.1.2 on port: 80
Running SYN flooder (synful)...
Launching 1 attack(s) at 192.168.1.2 on port: 80
Running SYN flooder (synful)...
Launching 1 attack(s) at 192.168.1.2 on port: 80
Running SYN flooder (synful)...
Launching 1 attack(s) at 192.168.1.2 on port: 80
Running SYN flooder (synful)...

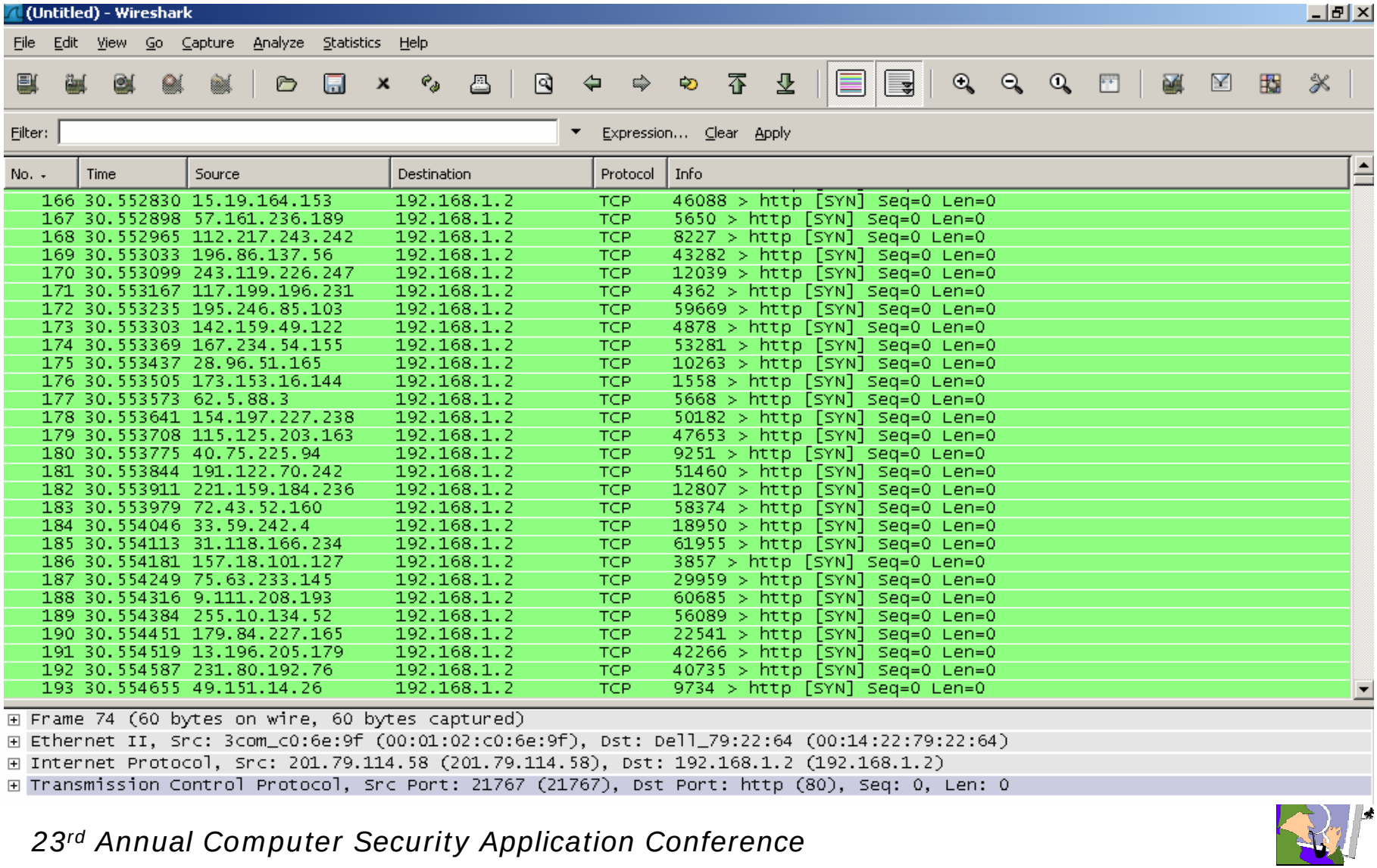


Sniffer Shows a Normal Three-way Handshake



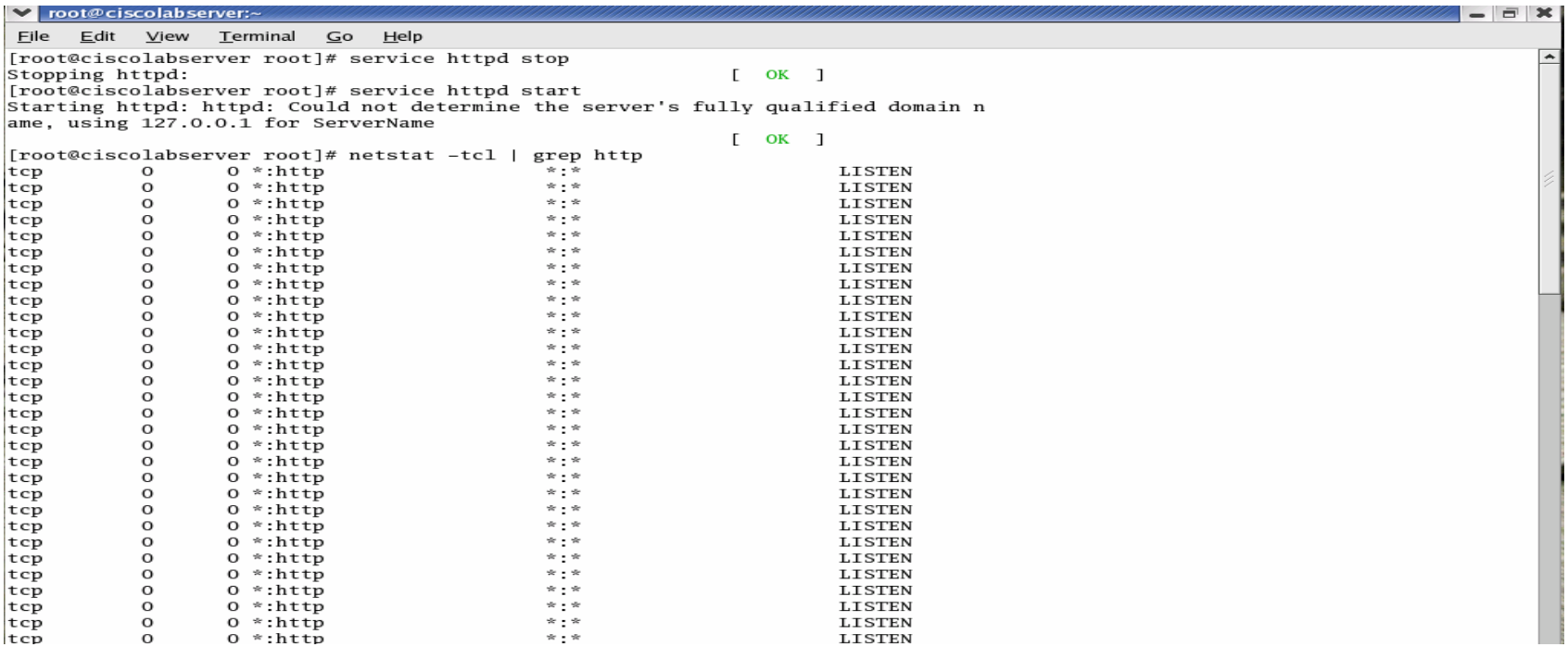


Sniffer Shows SYN Flooding Packets



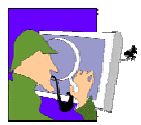
Pending Half-connections

Pending half-connections waiting in the SYNRECVD state in the Server



Analyzing

- Upon analyzing the data captured, we find that the attacker sends packets at a rate of 13568/s, with the size of each packet being 60 bytes.
- It takes approximately 21 packets to consume a 10 Mbps line, causing our server to stop answering any requests. This attack would theoretically have accomplished this at 0.0015 seconds;
- However, due to processing time and propagation delay, our client does not receive notification of the crash until 0.0029 seconds.



Defend Solution 1: Rate-limiting

Rate-limiting: Limit the number of the connections per second.

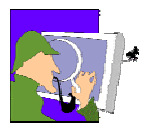
root@ciscolabserver:/usr/local/src/virus

File Edit View Terminal Go Help

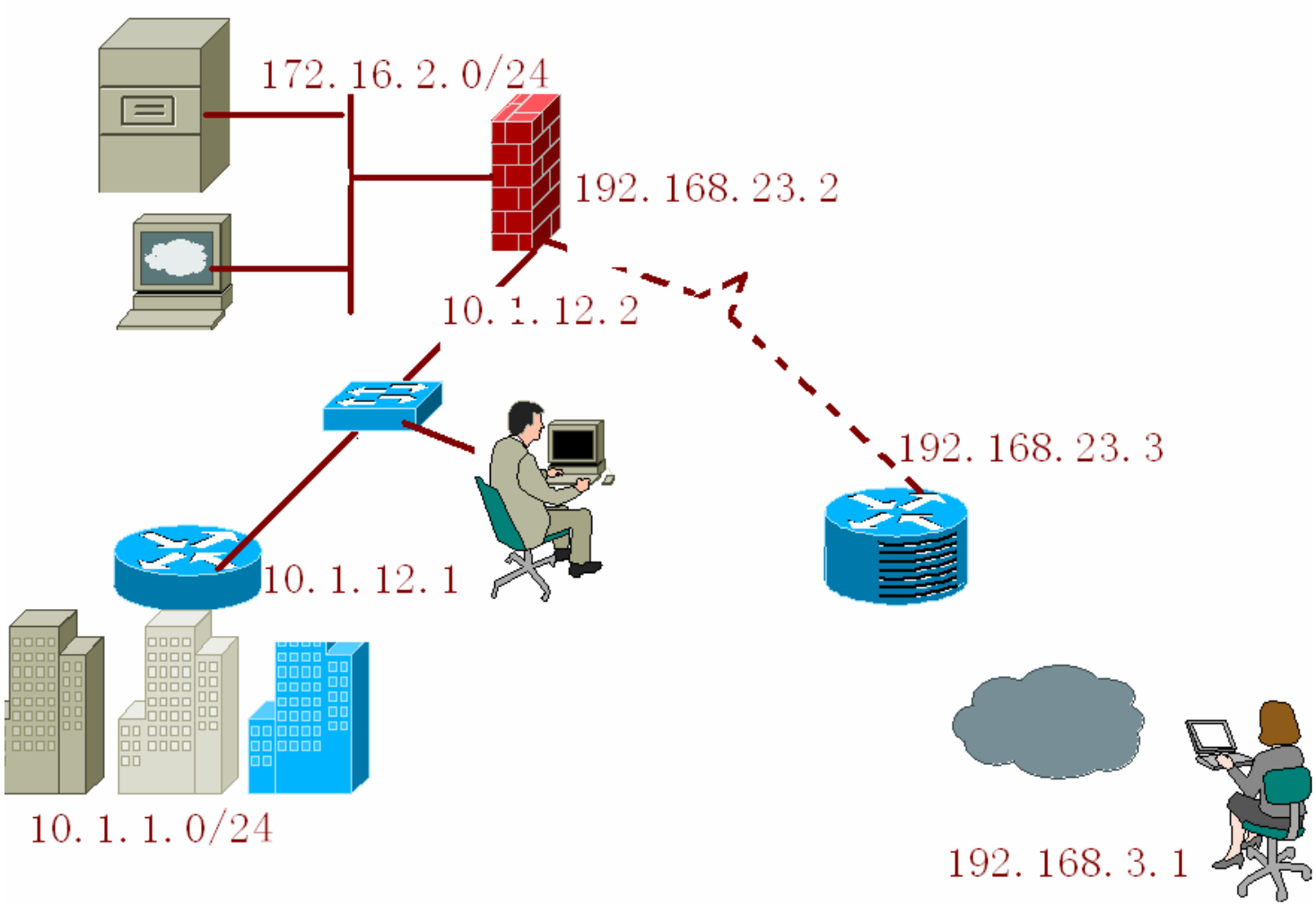
```
#!/bin/bash

iptables -F
iptables -X
iptables -Z

/bin/echo "0">/proc/sys/net/ipv4/icmp_echo_ignore_all
/bin/echo "1" > /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
/bin/echo "1" > /proc/sys/net/ipv4/conf/all/log_martians

#iptables -N syn-flood
#iptables -A INPUT -i eth0 -p tcp --syn -j syn-flood
#iptables -A syn-flood -m limit --limit 1/s --limit-burst 4 -j RETURN
#iptables -A syn-flood -j DROP
iptables -A INPUT -p TCP -i eth0 -m limit --limit 1/s --limit-burst 4 -j DROP

iptables -A INPUT -i eth0 -p icmp -m state --state ESTABLISHED,RELATED -j ACCEPT

iptables -A OUTPUT -o eth0 -p icmp -m state --state NEW,ESTABLISHED,RELATED -j ACCEPT
~
~
~
~
~
~
~
```

Defend Solution 2--SYN Cookies

- *Shipped with Linux and FreeBSD*, but unfortunately not enabled by default
- *Accepts SYN even if table is full, simply don't keep state-> reconstruct using cookie(seq#)*
- *# echo 1>/proc/sys/net/ipv4/tcp_syncookies*

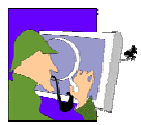


Attack 2—Target is on the Network



Lab Requirement for Attack 2

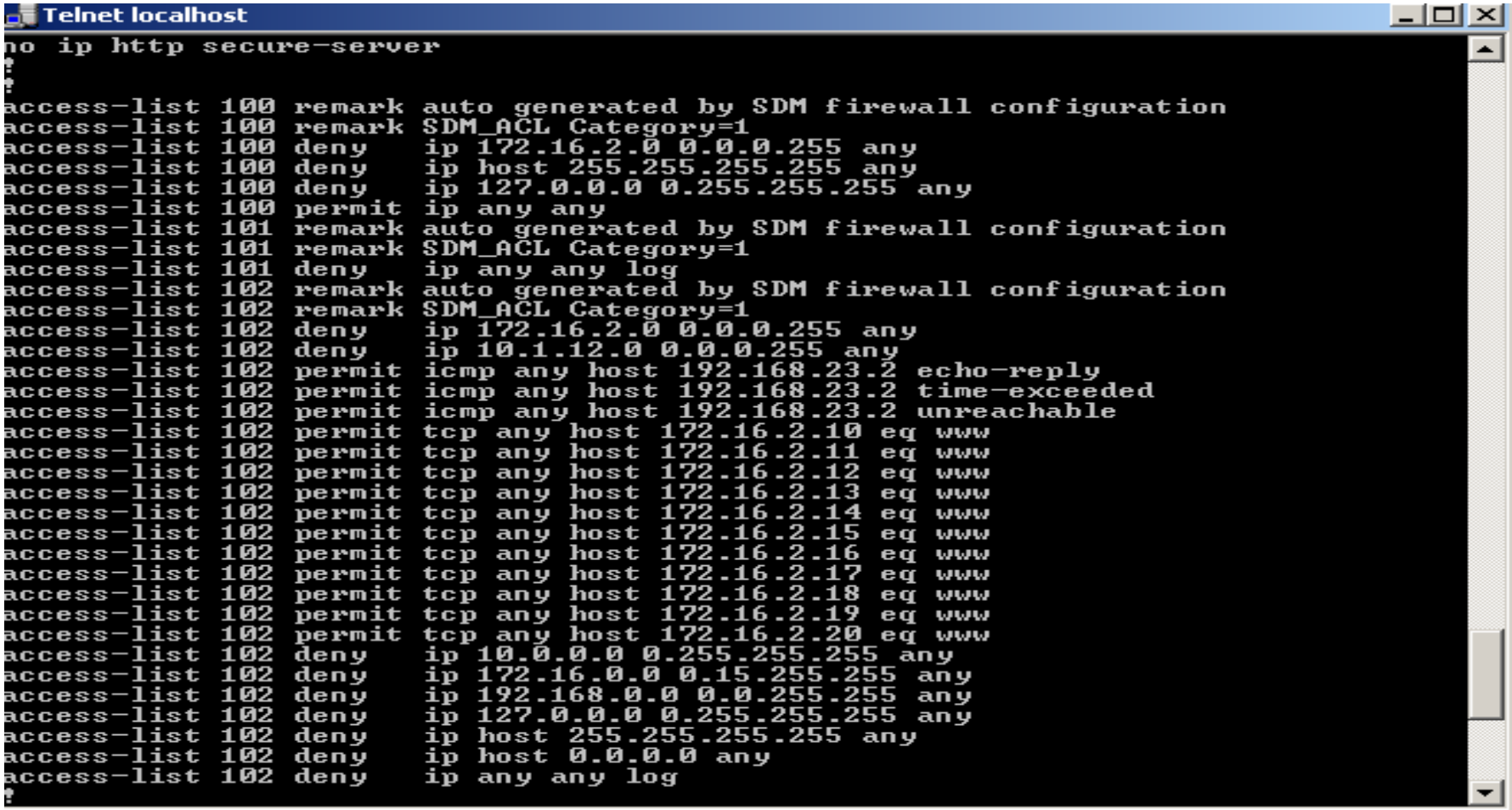
- There are three segments of network– Inside, outside, and DMZ.
- Inside network is the network we need protect.
- DMZ has web server and other services that cab be reached both from inside and outside.
- We use CISCO routers 7200 running IOS 12.4 for this attack.

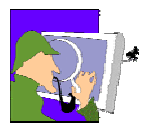


Solution 1--CBAC Firewall

- CBAC will check the access control list first, if the packets don’t match the list, the packets are dropped.
- If match, CBAC inspects all the outgoing packets and maintains state information for every session. CBAC create temporary openings for outbound traffic at the firewall interface.
- The return traffic is allowed in only if it is the part of the original outgoing traffic.

Solution 1--CBAC Firewall





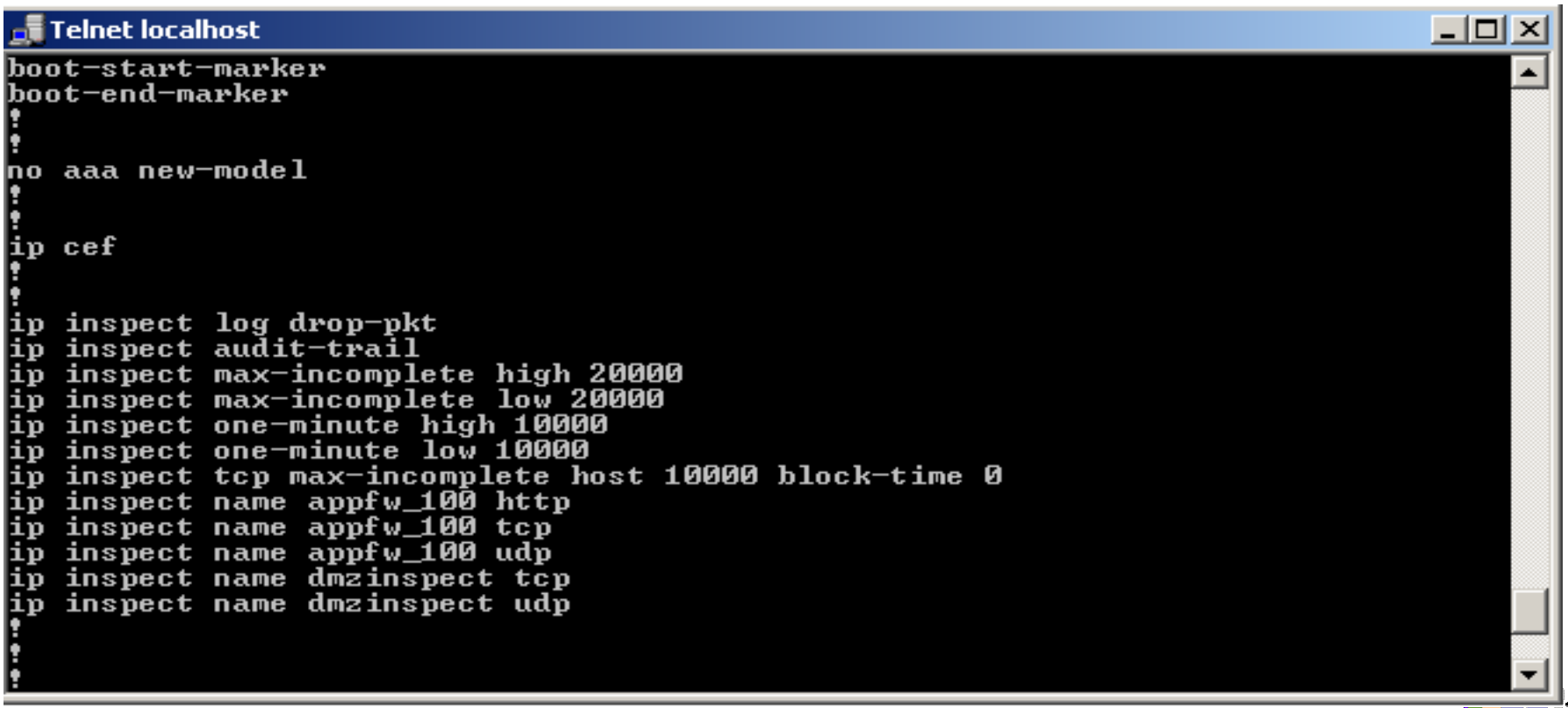
Solution 1--CBAC Firewall

Telnet localhost

```
!
!
interface Loopback0
 description $FW_DMZ$
 ip address 172.16.2.1 255.255.255.0
 ip access-group 101 in
 ip inspect dmzinspect out
!
interface FastEthernet0/0
 description $FW_INSIDE$
 ip address 10.1.12.2 255.255.255.0
 ip access-group 100 in
 ip inspect appfw_100 in
 duplex half
!
interface Serial1/0
 description $FW_OUTSIDE$
 ip address 192.168.23.2 255.255.255.0
 ip access-group 102 in
 ip verify unicast reverse-path
 serial restart-delay 0
 clock rate 64000
!
interface Serial1/1
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 shutdown
 serial restart-delay 0
!
interface Serial1/3
 no ip address
 shutdown
 serial restart-delay 0
!
```

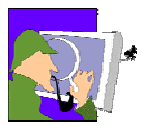
Solution 1--CBAC Firewall

CBAC provides strong protection against denial-of-service (DoS) attacks. It logs real-time alerts if it detects a DoS attack, and it uses the following commands to prevent DoS attacks:

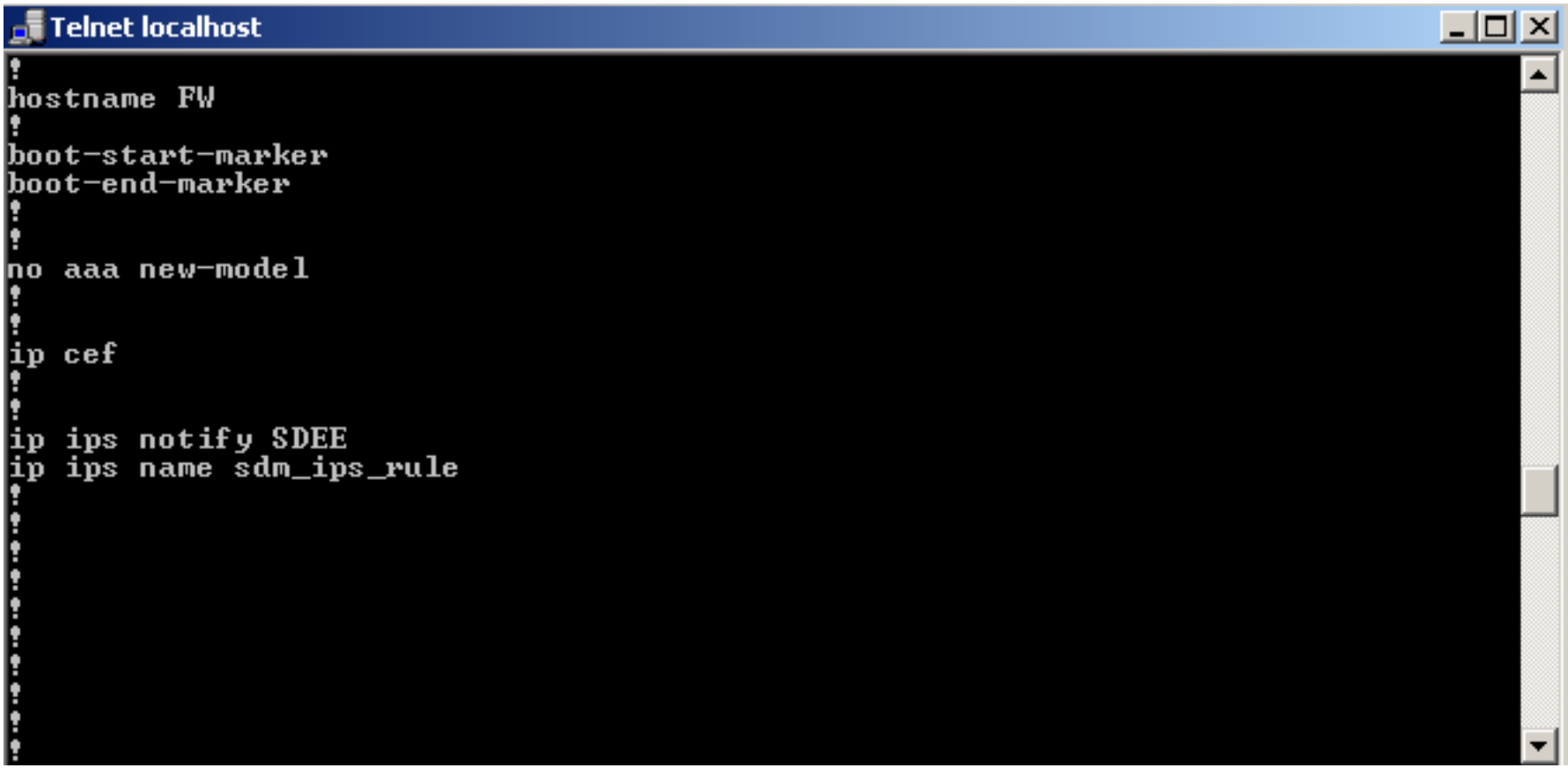


Solution 2– Intrusion Prevention System(IPS)

- The Intrusion Detection system is an add-on module to the IOS Firewall Feature Set. It has 59 of the most common attack signatures to detect intrusion. When IPS detects suspicious activity, it logs the event and can either shut down the port or send an alarm before network security is compromised.



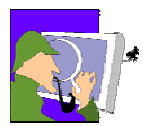
Solution 2– Intrusion Prevention System(IPS)



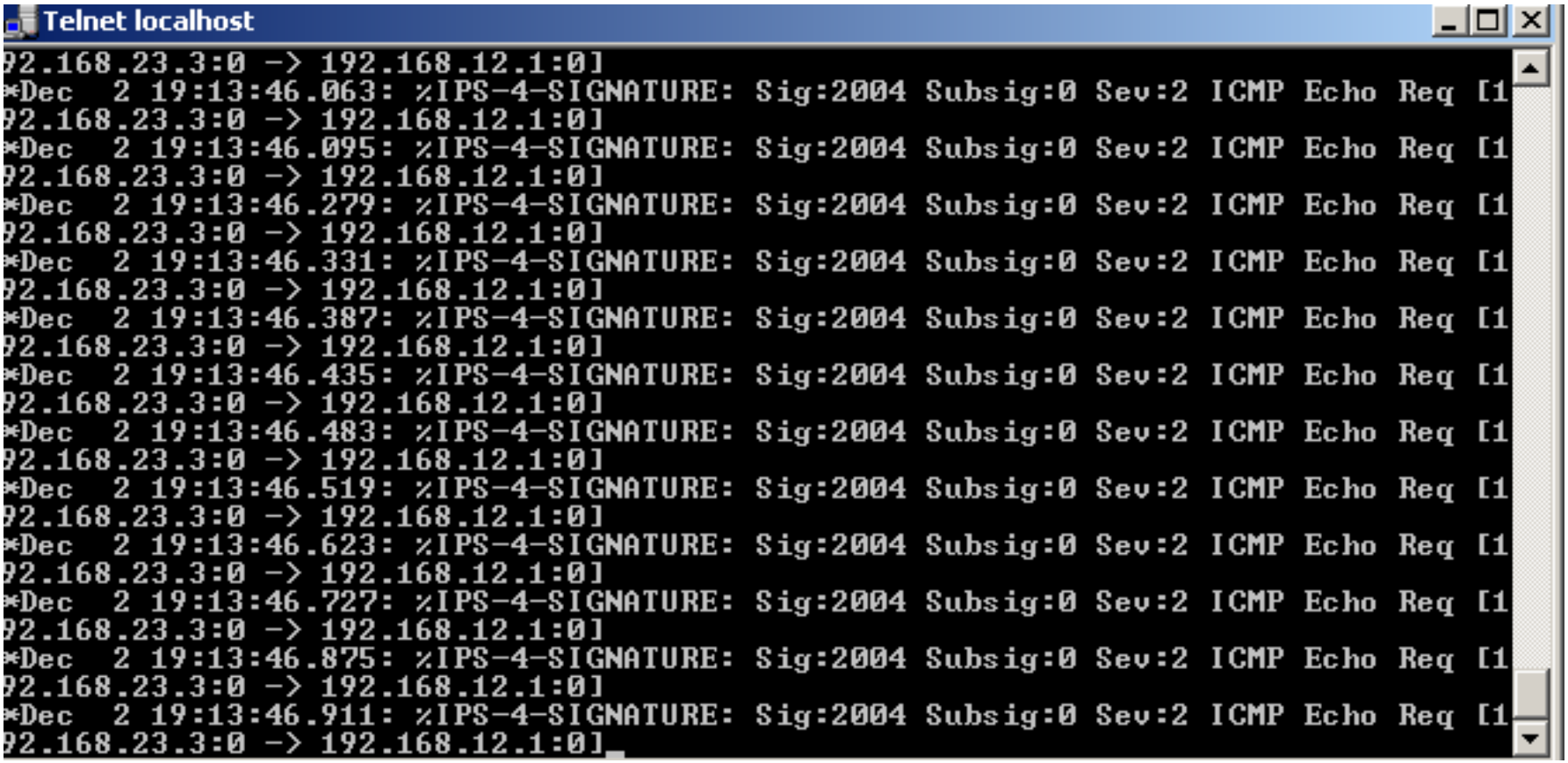
Solution 2– Intrusion Prevention System(IPS)

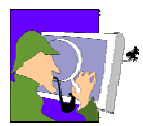
Telnet localhost

```
!
!
interface FastEthernet0/0
 ip address 192.168.12.2 255.255.255.0
 ip virtual-reassembly
 duplex half
!
interface Serial1/0
 ip address 192.168.23.2 255.255.255.0
 ip ips sdm_ips_rule in
 ip virtual-reassembly
 serial restart-delay 0
 clock rate 64000
!
interface Serial1/1
 no ip address
 ip virtual-reassembly
 shutdown
 serial restart-delay 0
!
interface Serial1/2
 no ip address
 ip virtual-reassembly
 shutdown
 serial restart-delay 0
```

Signature is triggered





Attacking is failing…

root@Router2:~/datapool

File Edit View Terminal Go Help

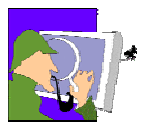
```
Running SYN flooder (synful)...
Continuing attack...he's not dead yet...
Launching 1 attack(s) at 192.168.1.2 on port: 80
Running SYN flooder (synful)...
Continuing attack...he's not dead yet...
Launching 1 attack(s) at 192.168.1.2 on port: 80
Running SYN flooder (synful)...
Continuing attack...he's not dead yet...
Launching 1 attack(s) at 192.168.1.2 on port: 80
Running SYN flooder (synful)...
Continuing attack...he's not dead yet...
Launching 1 attack(s) at 192.168.1.2 on port: 80
Running SYN flooder (synful)...
Continuing attack...he's not dead yet...
Launching 1 attack(s) at 192.168.1.2 on port: 80
Running SYN flooder (synful)...
Continuing attack...he's not dead yet...
Launching 1 attack(s) at 192.168.1.2 on port: 80
Running SYN flooder (synful)...
Continuing attack...he's not dead yet...
Launching 1 attack(s) at 192.168.1.2 on port: 80
Running SYN flooder (synful)...
Killed
[root@Router2 datapool]#
```

Build A free DoS Attack World

- Customer side–Be a good citizen. How? Using Egress Filtering: Authenticate Source IP of locally generated packets.
- ISP side-Using Ingress Filtering: Authenticate source IP of packets from customer.
- Host—updated OS, patches.
- Stateful Firewall inspect incoming and outgoing packets and create temporary hole in the firewall.
- IPS-An ounce of prevention is worth a pound of cure.

Summary

- Denial of Service attacks represent a fundamental threat to today's Internet
- DoS attacks cost significant losses
- Rate-limiting
- SYN cookies
- Firewall
- IPS



Reference

[1]http://www.ethereal.com

[2]http://packetstormsecurity.org/DoS/datapool2.0.tar.gz

[3] *TCP-LP: A Distributed Algorithm for Low Priority Data Transfer,* In *IEEE INFOCOM 2003*.

[4] A. Kuzmanovic and E. Knightly. Low-Rate TCP-Targeted Denial of Service Attacks. In Proceedings of ACM SIGCOMM '03, Karlsruhe, Germany, August 2003.

[5]http://www.cisco.com

[6] http://www.cert.org/

[7] ftp://ftp.isi.edu/in-notes/rfc2267.txt