5.8.1

Denial Of Service Attacks

And ICMP Flooding

Objective

At the end of this lab students will understand how ICMP echo requests and replies work, and how a ping flood could affect a network connection.

Information for Laboratory

A. Students will utilize Windows XP
B. Students will utilize Cisco routers and or Cisco switches

Student Preparation

The student will have completed the prerequisite lab Bandwidth Monitoring, and will have completed the requisite reading. The student will require paper for notes and should be prepared to discuss the exercises upon completion.

You will need access to a Windows XP workstation, and at least one Cisco router or switch on the local network with telnet access.

Warning

ICMP floods can saturate a networks available bandwidth. This lab is intended to show the effects of ICMP flood attacks. The instructions in the lab are strictly written for class room testing only.

Estimated Completion Time

60 Minutes

Internet Control Message Protocol (ICMP), documented in RFC 792, is a required protocol tightly integrated with IP. ICMP messages, delivered in IP packets, are used for out-of-band messages related to network operation or mis-operation. Some of ICMP's functions are to:

Assist Troubleshooting: ICMP supports an Echo function, which just sends a packet on a round-trip between two hosts. Ping, a common network management tool, is based on this feature. Ping will transmit a series of packets, measuring average round-trip times and computing loss percentages.

Announce network errors: Such as a host or entire portion of the network being unreachable, due to some type of failure.

Announce network congestion: When a router begins buffering too many packets, due to an inability to transmit them as fast as they are being received, it will generate ICMP Source Quench messages. Directed at the sender, these messages should cause the rate of packet transmission to be slowed.

Announce Timeouts: If an IP packet's TTL field drops to zero, the router discarding the packet will often generate an ICMP packet announcing this fact.

ICMP Flooding

A denial of service attack that sends a host more ICMP echo request ("ping") packets than the protocol implementation can handle.

Smurf attack

Smurf attacks work by sending a ping packet to the broadcast address of a network, using a spoofed source IP address. The source IP address is the actual target. When all the clients of

the network respond to the ping packet, they will all be sending a reply to the single spoofed address. It is this multiple response that is the actual DoS attack, overwhelming the spoofed target system. On a multi-access broadcast network, there could potentially be hundreds of machines to reply to each packet.

Step 1: Understanding network broadcast addresses

Every IP network has a unique network and broadcast address. Broadcast addresses are in fact used to broadcast packets. Any packets sent to a broadcast address on a multi-access broadcast network, will be sent to and processed by each host on that network.

A lot of new IP devices do not support ICMP echo via broadcasts, so by pinging a broadcast address, you may not receive any or all the replies.

Step 2: Ping your network broadcast address from Windows

From START, Run, type cmd in the Open box and click OK.

Type ipconfig and press enter

From here you can see your IP address and subnet mask. The given subnet mask of 255.255.255.0 denotes a full class C subnet. The network address in this case would be 10.0.0.0 and the broadcast would be 10.0.0.255.

Next, from the command prompt, type ping your broadcast

address. Ex. ping 10.0.0.255

```
U:\>ping 10.0.0.255

Pinging 10.0.0.255 with 32 bytes of data:

Reply from 10.0.0.51: bytes=32 time<1ms TTL=128
Reply from 10.0.0.51: bytes=32 time<1ms TTL=128
Reply from 10.0.0.51: bytes=32 time<1ms TTL=128
Reply from 10.0.0.51: bytes=32 time<1ms TTL=128

Ping statistics for 10.0.0.255:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Your results may vary from the output above. The important item to notice is that you sent an ICMP echo to your broadcast address, in this case 10.0.0.255, and got a reply back from a different address.

Microsoft Windows XP does not support ICMP echo messages via broadcasts, so you will not get replies back from any Windows XP computers. Remember, this test network has several old IP devices used only to show ICMP echo replies via a broadcast. In the real world, the IP stack on these devices would be out of date, and should be immediately upgraded.

Step 3: Ping your network broadcast address from a Cisco device

Note: Your instructor or lab assistant will have instructions on how to telnet to the Cisco device.

From the command prompt, telnet to your available Cisco router or switch, and enable Exec mode.

In Exec mode, enter the command ping and press enter.

Enter the information as follows…

Protocol [IP]: press enter to accept

Target IP address: enter your network broadcast address

Repeat count [5]: 1 and press enter

Datagram size [100]: press enter to accept

Timeout in seconds [2]: press enter to accept

Extended commands [n]: press enter to accept

Sweep range of sizes [n]: press enter to accept

At this point, the ping command has all the information it needs, and will process the command.

```
Router#ping
Protocol [ip]:
Target IP address: 10.0.0.255
Repeat count [5]: 1
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 1, 100-byte ICMP Echos to 10.0.0.255,

Reply to request 0 from 10.0.0.206, 9 ms
Reply to request 0 from 10.0.0.72, 33 ms
Reply to request 0 from 10.0.0.205, 17 ms
Reply to request 0 from 10.0.0.202, 17 ms
Reply to request 0 from 10.0.0.20, 17 ms
Reply to request 0 from 10.0.0.55, 17 ms
Reply to request 0 from 10.0.0.62, 13 ms
Reply to request 0 from 10.0.0.67, 13 ms
Reply to request 0 from 10.0.0.63, 13 ms
Reply to request 0 from 10.0.0.71, 13 ms
Reply to request 0 from 10.0.0.64, 13 ms
Reply to request 0 from 10.0.0.22, 13 ms
Reply to request 0 from 10.0.0.200, 13 ms
Reply to request 0 from 10.0.0.2, 13 ms
Reply to request 0 from 10.0.0.68, 13 ms
Reply to request 0 from 10.0.0.5, 13 ms
Reply to request 0 from 10.0.0.6, 9 ms
Reply to request 0 from 10.0.0.7, 9 ms
Reply to request 0 from 10.0.0.73, 9 ms
Reply to request 0 from 10.0.0.51, 9 ms
Router#
```

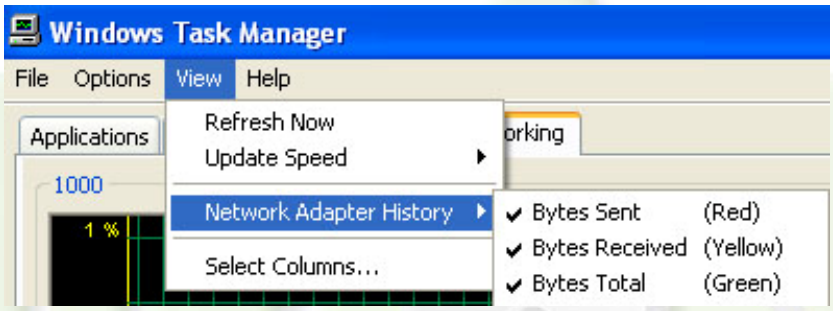
As you can see from the example above, by pinging the broadcast address of the local network from a Cisco device, all the different replies are shown. Note: the replies that you see are all from old IP devices. None of the replies are from the Windows computers on the network, as Windows IP stack

ignores ICMP echo requests from broadcast addresses.

Step 4: Ping flooding

Open the Task Manger on your Windows XP workstation. Click on the Networking tab at the top. From View, set the Update Speed to high, and Network Adapter History to enable Bytes Sent, Received, and Total.

Note: Red is bytes sent, Yellow is bytes received, and Green is total bytes. You will notice that ICMP requests received, are the same size being sent.



Leave the network monitor open and visible.

Next, from the Cisco device, type ping and press enter

Enter the information as follows…

Protocol [IP]: press enter to accept

Target IP address: enter your workstations IP address, as you are pinging yourself to watch the affect of your available bandwidth.

Repeat count [5]: 1000 and press enter

Datagram size [100]: 999999999 press enter to accept

Notice the device will state that 18024 is the largest datagram size allowed.

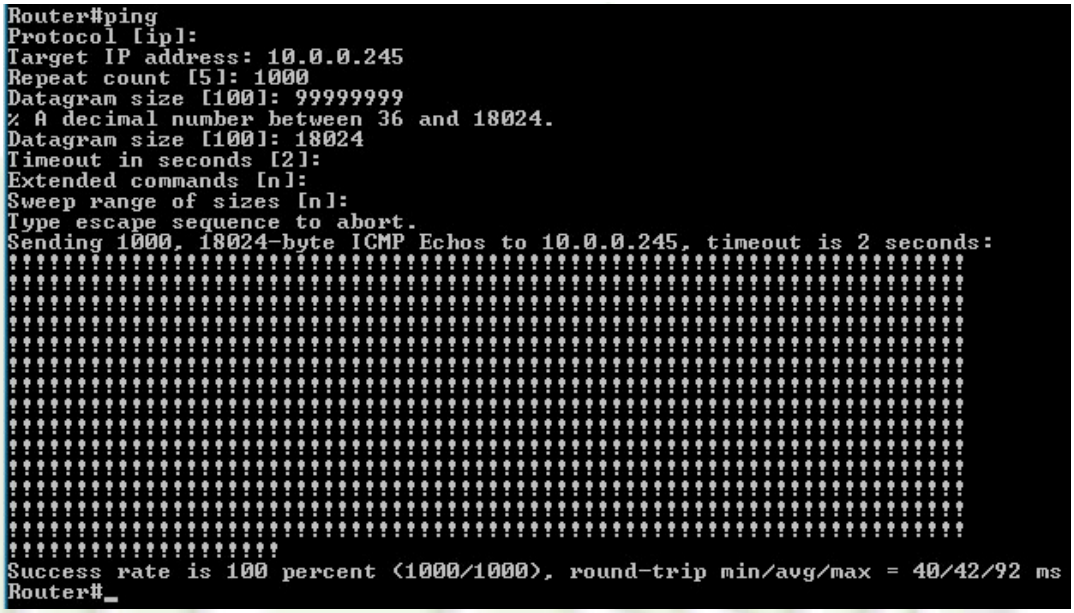
Datagram size [100]: 18024 press enter to accept

Timeout in seconds [2]: press enter to accept

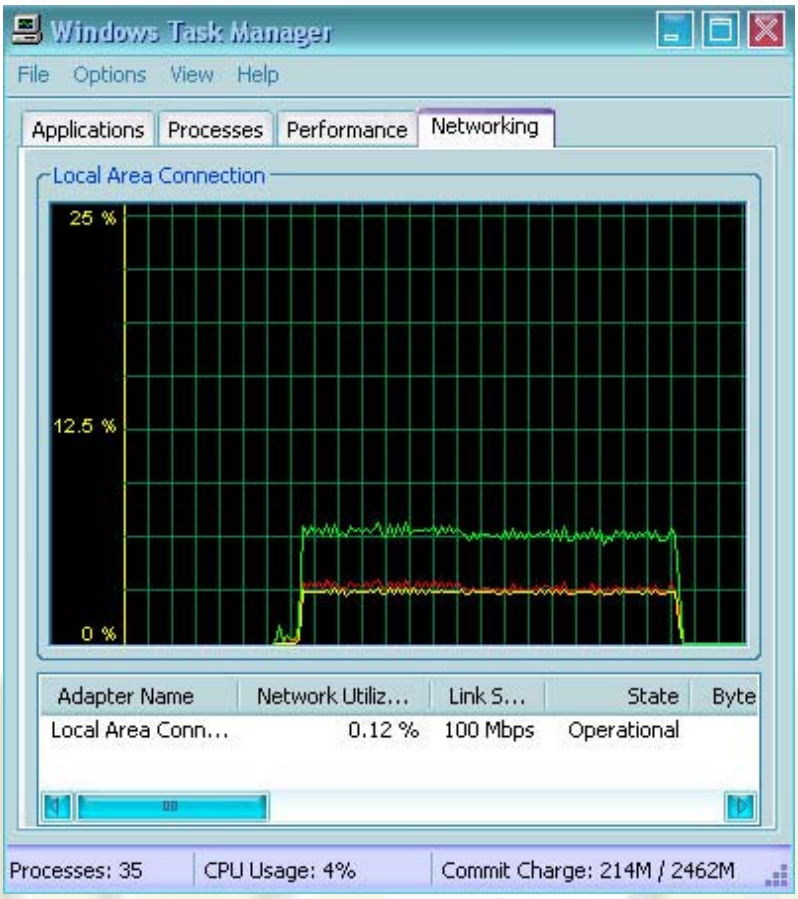
Extended commands [n]: press enter to accept

Sweep range of sizes [n]: press enter to accept

At this point, the ping command has all the information it needs, and will process the command.



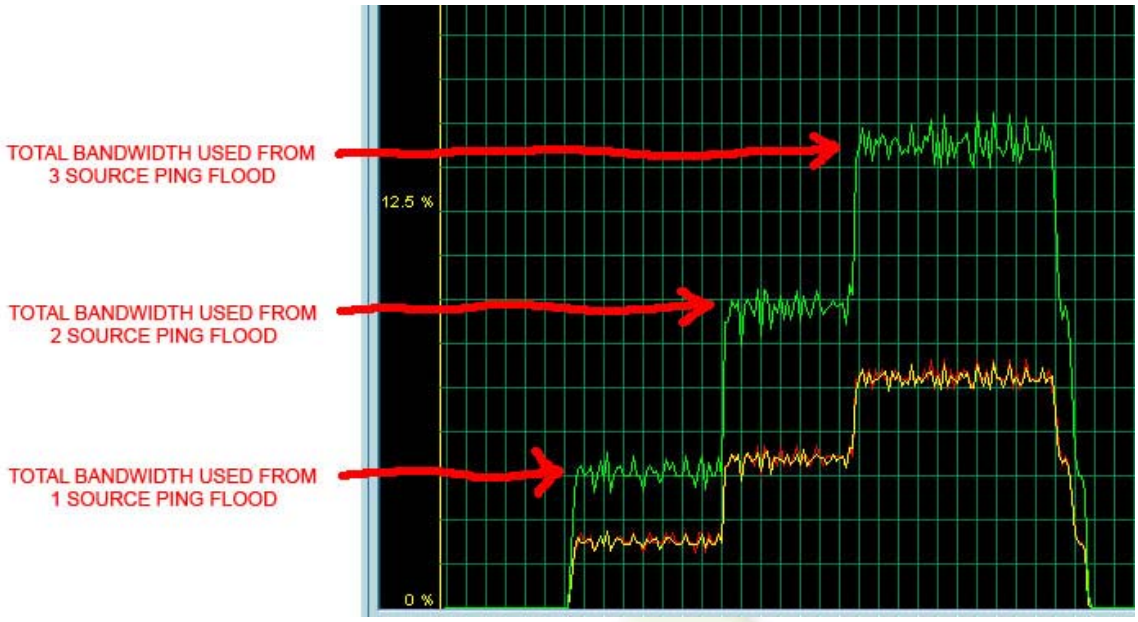
Notice the network monitor, your bandwidth usage should go up as the example below.



Step 5: Ping flood from multiple sources – Simulated Smurf attack

In this section, there are 3 Cisco routers all setup to ping flood the same address. If your lab permits, telnet to all available Cisco routers, and ping your IP address. Notice the used bandwidth in the network monitor.

This flooding of network bandwidth is the basis of the DOS Smurf attack. By pinging the broadcast address of a network with a spoofed source IP address, you would be sending all this ICMP traffic to the victim, flooding their connection. The example above only has 3 hosts, what would happen if all 254 hosts on the local network were to flood one address?



Step 6: Analysis

1) For which applications is ICMP flooding best suited?

2) After working with these utilities, what about ICMP flooding do you feel you should study further? Why?

3) Why should you disable ICMP echo replies via broadcasts.

4) What do you think would happen to the victim of a smurf attack?

Summary Discussion

A classroom discussion should follow the lab. Review the lab questions and your analyses as a group. Share your experiences and knowledge with the class.

Appendix:

The OS environment for this lab was Windows XP Professional, Version 2002, Service Pack 2 (8/04).