Network-Based Denial of Service Attacks

Trends, Descriptions, and How to Protect Your Network

Craig A. Huegen <chuegen@cisco.com>

Cisco Systems, Inc.

NANOG 12 Interprovider Operations BOF

Cisco Systems

980209_dos.ppt

Trends

- **Significant increase in network-based DoS 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

Profiles of Participants

- **Tools of the Trade**
  - Anonymity
  - Internet Relay Chat
  - Cracked super-user account on well-connected enterprise network
  - Super-user account on university residence hall network
  - “Throw-away” PPP dial-up accounts
- **Typical Victims**
  - IRC Users, Operators, and Servers
  - Providers who eliminate troublesome users’ accounts

Goals of Attacks

- **Prevent another user from using network connection**

  “Smurf” attacks, “pepsi” (UDP floods), ping floods

- **Disable a host or service**

  “Land”, “Teardrop”, “Bonk”, “Boink”, SYN flooding, “Ping of death”

- **Traffic monitoring**

  Sniffing

“Smurfing”

- Very dangerous attack

  Network-based, fills access pipes

  Uses ICMP echo/reply packets with broadcast networks to multiply traffic

  Requires the ability to send spoofed packets

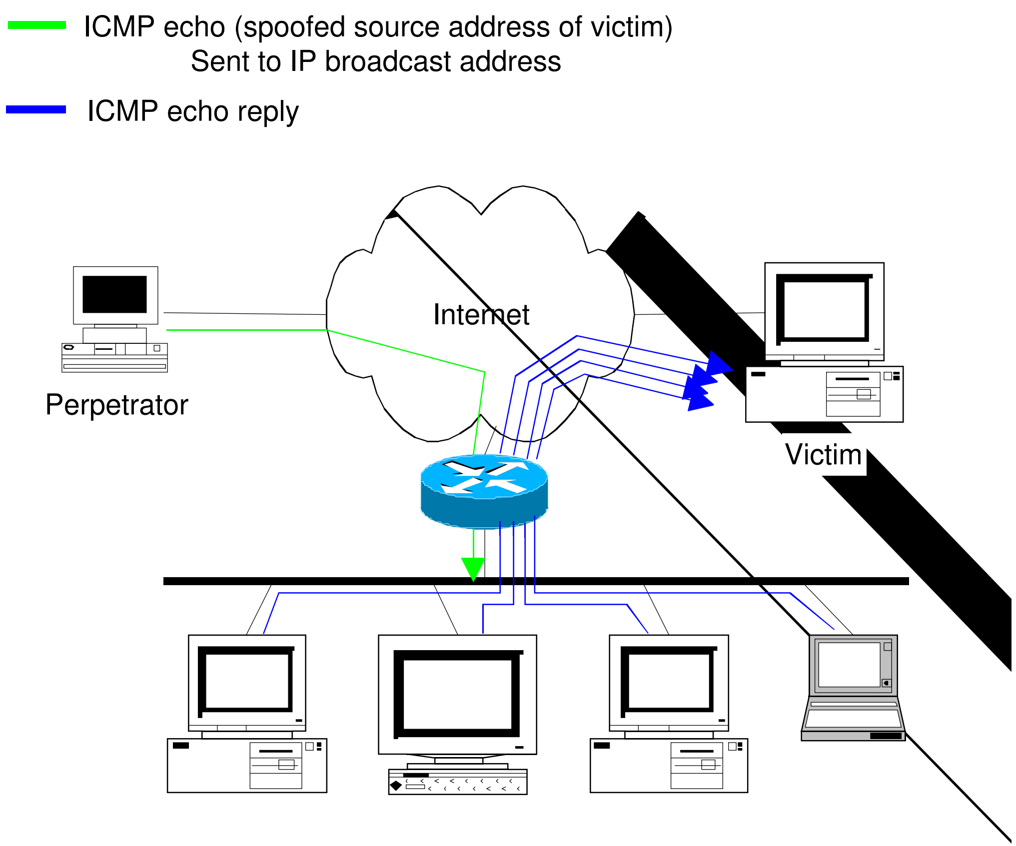
- Abuses “bounce-sites” to attack victims

  Traffic multiplied by a factor of 50 to 200

  Low-bandwidth source can kill high-bandwidth connections

- Similar to ping flooding, UDP flooding but more dangerous due to traffic multiplication

“Smurfing” (cont’d)



“Smurfing” trend

- Smurf attacks are still “in style” for attackers
- Significant advances made in reducing the effects

  Education campaigns through the use of white paper and other education by NOCs has reduced the average “smurf” attack from 80 Mbits/sec to 5 Mbits/sec

- Most attacks can still inundate a T1 link

“Land”

- Goal is to severely impair or disable a host or its IP stack
- Connects address and port pair to itself
- Requires the ability to spoof packet source addresses
- Requires the victim’s network to be unprotected against packets coming from outside with own IP addresses

“Teardrop”, “Bonk”, “Boink”, “Ping of Death”

- **Goal is to severely impair or disable a host or its IP stack**
- **Use packet fragmentation and reassembly vulnerabilities**
- **Require that a host IP stack be able to receive a packet from an attacker**

SYN flooding

- Goal is to deny access to a TCP service running on a host
- Creates a number of half-open TCP connections which fill up a host’s listen queue; host stops accepting connections
- Requires the TCP service be open to connections from the victim

Sniffing

- **Goal is generally to obtain information**
  - **Account usernames, passwords**
  - **Source code, business critical information**
- **Usually a program placing an Ethernet adapter into promiscuous mode and saving information for retrieval later**
- **Hosts running the sniffer program is compromised using host attack methods**

Prevention Techniques

- **How to prevent your network from being the source of the attack:**

  Apply filters to each customer network

  Allow only those packets with source addresses within the customer's assigned netblocks to enter your network

  Apply filters to your upstreams

  Allow only those packets with source addresses within your netblocks to exit your network, to protect others

  Deny those packets with source addresses within your netblocks from coming into your network, to protect your network

- **This removes the possibility of your network being used as an attack source for many attacks which rely on anonymity**

Prevention Techniques

- **How to prevent being a "bounce site" in a "Smurf" attack:**

  Turn off directed broadcasts to networks:

  Cisco: Interface command "no ip directed-broadcast"

  Proteon: IP protocol configuration "disable directed-broadcast"

  Bay Networks: Set a false static ARP address for bcast address

  Use access control lists (if necessary) to prevent ICMP echo requests from entering your network

  Encourage vendors to turn off replies for ICMP echos to broadcast addresses

  Host Requirements RFC-1122 Section 3.2.2.6 states "An ICMP Echo Request destined to an IP broadcast or IP multicast address MAY be silently discarded."

  Patches are available for free UNIX-ish operating systems.

Prevention Techniques

- Technical help tips for Cisco routers
  - BugID CSCdj35407 - “fast drop” ACL code
  - BugID CSCdj35856 - ACL logging throttles
- Unicast RPF checking
- Interprovider Cooperation
  - Stories from the field
  - Publish proper procedures for getting filters put in place and tracing started

References

- **White paper on “smurf” attacks:**

  http://www.quadrunner.com/~chuegen/smurf.txt

- **Ingress filtering:**

  ftp://ds.internic.net/internet-drafts/draft-ferguson-ingress-filtering-03.txt

- **MCI’s DoSTracker tool:**

  http://www.security.mci.net/dostracker/

- **Other DoS attacks:**

  “Defining Strategies to Protect Against TCP SYN Denial of Service Attacks”

  http://www.cisco.com/warp/public/707/4.html

  “Defining Strategies to Protect Against UDP Diagnostic Port Denial of Service Attacks”

  http://www.cisco.com/warp/public/707/3.html

Author

Craig Huegen

<chuegen@cisco.com>

Questions?