GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Denial of Service Attacks - DDOS, SMURF, FRAGGLE, TRINOO

B.K.Lokesh

1st March 2001

General Background Information

The "Smurf" attack, named after its exploit program, is one of the most recent in the category of network-level attacks against hosts. A perpetrator sends a large amount of ICMP echo (ping) traffic at IP broadcast addresses all of it having a spoofed source address of a victim. If the routing device delivering traffic to those broadcast addresses performs the IP broadcast to layer 2 broadcast function noted below, most hosts on that IP network will take the ICMP echo request and reply to it with an echo reply each, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, there could potentially be hundreds of machines to reply to each packet. The "Smurf" attack's cousin is called "fraggle", which uses UDP echo packets in the same fashion as the ICMP echo packets; it was a simple re-write of "Smurf".

How to keep your site from being the source perpetrators use to attack victims

The perpetrators of these attacks rely on the ability to source spoofed packets to the "amplifiers" in order to generate the traffic which causes the denial of service. In order to stop this, all networks should perform filtering either at the edge of the network where customers connect (access layer) or at the edge of the network with connections to the upstream providers, in order to defeat the possibility of source-address-spoofed packets from entering from downstream networks, or leaving for upstream networks.

Paul Ferguson of cisco Systems and Daniel Senie of BlazeNet have written an RFC pertaining to this topic. See: ftp://ftp.isi.edu/in-notes/rfc2267.txt for more information and examples on this subject.

Additionally, router vendors have added or are currently adding options to turn off the ability to spoof IP source addresses by checking the source address of a packet against the routing table to ensure the return path of the packet is through the interface it was received on. Cisco has added this feature to the current 11.1CC branch, used by many NSP's, in an interface command '[no] ip verify unicast reverse-path'. See the "other vendors" section for 3Com information regarding this feature.

How to stop being an intermediary

This attack relies on the router serving a large multi-access broadcast network to frame an IP broadcast address (such as 10.255.255.255) into a layer 2 broadcast frame (for Ethernet, FF:FF:FF:FF:FF:FF). RFC 1812, "Requirements for IP Version 4 Routers", Section 5.3.5, specifies: --- A router MAY have an option to disable receiving network-prefix- directed broadcasts on an interface and MUST have an option to disable forwarding network-prefix-directed broadcasts. These options MUST default to permit receiving and forwarding network-prefix- directed broadcasts. --- Generally, with IP providers and IP applications as we know them today, this behaviour should not be needed, and it is recommended that directed-broadcasts be turned off, to suppress the effects of this attack.

RFC 2644, a Best Current Practice RFC by Daniel Senie, updates RFC 1812 to state that router software must default to denying the forwarding and receipt of directed broadcasts. Ethernet NIC hardware (MAC-layer hardware, specifically) will only listen to a select number of addresses in normal operation. The one MAC address that all devices share in common in normal operation is the media broadcast, or FF:FF:FF:FF:FF:FF. If a device receives a packet destined to the broadcast link-layer address, it will take the packet and send an interrupt for processing by the higher-layer routines.

© SANS Institute 2000 - 2005 Author retains full rights.

To stop your Cisco router from converting these layer 3 broadcasts into layer 2 broadcasts, use the "no ip directed-broadcast" interface configuration command. This should be configured on each interface of all routers. As of Cisco IOS version 12.0, "no ip directed-broadcast" is now the default in order to protect networks by default. "ip directed-broadcast" will be needed if your network requires directed broadcasts to be enabled.

ISP Security Summit Guidelines Developed to Defeat Internet Service Attacks by DDOS

Organisations that operate networks connected to the Internet may be serving as unwitting participants in Denial of Service (DoS) Attacks like those that hit many organisations in early February, 2000.
You can act now to reduce the chances that your network could be used to damage other networks if you implement the following two steps.

- Egress Filtering to Stop Spoofed IP Packets from Leaving Your Network
- Stop Your Network from Being Used as a Broadcast Amplification Site

These two steps should be implemented immediately, and detailed instructions for doing this are provided below. Broad application of these two steps can significantly reduce the threat posed by DoS Attacks.
Step One: Egress Filtering to Stop Spoofed IP Packets from Leaving Your Network
Purpose: To prevent your network from being the source of spoofed (i.e. forged) communications that are often used in DoS Attacks.
Action: Ensure that your routers and firewalls are configured to forward IP packets only if those packets have the correct Source IP Address for your network. The correct Source IP Address(es) would consist of the IP Network Addresses that have been assigned to your site. It is important to do this throughout your network, especially at the external connections to your Internet or upstream provider.
Step 1.1: Deny Invalid Source IP Addresses
All organisations connected to the Internet should only allow packets to leave their network with valid Source IP Addresses that belong to their network. This will minimise the chance that your network will be the source of a Spoofed DoS Attack. This will not prevent Distributed DoS attacks coming from your network with valid source addresses.
In order to implement this you will need to know the IP network blocks that are in use at your site. If you do not know this information at this time, then please skip to Step 1.2, and come back to this step once you have that information.
Preventing Spoofed Source IP Address traffic can be accomplished with filtering on routers, firewalls, and hosts. Here is a generic example of what the filter needs to look like.
Permit Your Sites Valid Source Addresses to the Internet
Deny All Other Source Addresses
On the router(s) connected to your ISP(s), if the interface IP address on the link connecting to the ISP is not out of one of your site's IP blocks, you should also permit packets with the interface IP address.
For detailed instructions on implementing this filtering please select the platform that you are using from the list in the "Step One: Detailed Directions" section below.
Step 1.2: Deny Private & Reserved Source IP Addresses
This step is not necessary if you were able to fully complete Step 1.1.
If you are unsure what address space is in use at your site, then you should at least deny Private (RFC 1918) and Reserved Source IP Addresses.
The following is a list of source addresses that should be filtered.
0.0.0.0/8 - Historical Broadcast
10.0.0.0/8 - RFC 1918 Private Network
127.0.0.0/8 - Loopback
169.254.0.0/16 - Link Local Networks
172.16.0.0/12 - RFC 1918 Private Network
192.0.2.0/24 - TEST-NET
192.168.0.0/16 - RFC 1918 Private Network
224.0.0.0/4 - Class D Multicast
240.0.0.0/5 - Class E Reserved

© SANS Institute 2000 - 2005 Author retains full rights.

248.0.0.0/5 - Unallocated
255.255.255.255/32 - Broadcast
If you are using Network Address Translation (NAT), you need to make sure that you perform this filtering between your NAT device and your ISP, and you should also verify that your NAT device configuration only translates address used and authorised for your internal address space.
Denying Private and Reserved Source IP Addresses can be accomplished with filtering on routers, firewalls, and hosts. Please select the platform that you are using from the list in the "Step One: Detailed Directions" section below.
Step One: Detailed Directions for Egress Filtering
Please select the router, firewall, or host that you use from the list below for detailed instructions on how to implement Egress Filtering to Stop Spoofed IP Packets for the particular platform that you are using.

- Bay
- Cabletron SSR
- Cisco

Step Two: Stop Your Network from Being Used as a Broadcast Amplification Site
Purpose: To ensure that your network can not be used as a Broadcast Amplification Site to flood other networks with DoS attacks such as the "smurf" attack.
Action: Configure all of your systems (routers, workstations, servers, etc.) so that they do not receive or forward Directed Broadcast traffic.
Step 2.1: Disable IP Directed Broadcast on all Systems
Detailed directions for doing this are available for the following systems.

- Bay
- Cisco

For all other systems, please go to http://users.quadrunner.com /chuegen/smurf/ where you'll find Craig Huegen's authoritative page containing instructions for many other types of systems.
The following systems have Directed Broadcast disabled by default. However, these systems may have a way to turn this behavior back on. Please select the link for your platform for information on making sure that the system is in the default state, and does not allow directed broadcasts.

- Cabletron SSR
- FreeBSD
- Microsoft Windows Workstation & Server 3.5 & 3.5.1

For Windows NT 4.0, the default behaviour for answering broadcast packets was changed in Service Pack 4. The latest Service Packs for NT can be obtained from Microsoft at http://support.microsoft.com/support/kb/articles/Q152/7/34.ASP
Step 2.2: Test your network to determine if it is an amplification site.
To test your network to see if it is acting as an amplification site you can use the "ping" command to send an ICMP Echo Request packet to the Network Base IP Address of your network(s) and the Broadcast IP Address of your network(s).
You will need to know your Network Base IP Address and your Broadcast IP Address. You may find the CIDR Table helpful in determining these addresses for your network.
From a machine on the Internet side of your router (i.e. off your site) ping both the Network Base Address (x.x.x.0 for a /24 aka Class C) and the Broadcast Address (x.x.x.255 for a /24 aka Class C) of an internal subnet with a number of machines on it.
Please select from the following list of operating systems for detailed instructions on using the ping command and analysing the output to determine if your network is a Broadcast Amplification site.

- FreeBSD 3.0
- Linux (RedHat 6.1)
- Solaris

Another way to test your network is to go to some of the public web sites that provide a way to test your network from a remote location.
Please be aware that these sites are operated by independent third parties, and that you should use them at your own risk. If your site is in really poor shape it may get added to a "blacklist" that can then be used by attackers to identify your site as a good broadcast amplification site. Because of this you are strongly encouraged to self test with the ping commands listed above first.

- http://www.netscan.org
- http://www.powertech.no/smurf/

© SANS Institute 2000 - 2003 Author retains full rights.

Step 2.3: Require that Vendors Disable IP Directed Broadcast by Default
When you purchase new systems, require that the vendor disable receipt and forwarding of directed broadcast packets as specified in RFC 2644.
From RFC 2644:

> A router MAY have a configuration option to allow it to receive directed broadcast packets, however this option MUST be disabled by default, and thus the router MUST NOT receive Network Directed Broadcast packets unless specifically configured by the end user.
>
> A router MAY have an option to enable receiving network-prefix- directed broadcasts on an interface and MAY have an option to enable forwarding network-prefix-directed broadcasts. These options MUST default to blocking receipt and blocking forwarding of network-prefix-directed broadcasts.

Based on this you should be asking your vendors to ship systems with Directed Broadcast disabled by default. At the very least the vendor should provide a mechanism to disable Directed Broadcasts. Some vendors already disable IP directed broadcast by default in the latest versions of their software, but many do not. Please help educate these other vendors by pointing them to RFC 2644.

References

Defining Strategies to Protect Against TCP SYN Denial of Service Attacks
http://cio.cisco.com/warp/public/707/4.html

Defining Strategies to Protect Against UDP Diagnostic Port DoS Attacks
http://cio.cisco.com/warp/public/707/3.html

Cisco command documention to turn off directed broadcasts
http://www.cisco.com/univercd/cc/td/doc/product/software/ios113ed/cs/csprtn1/csipadr.htm#xtocid748113

3Com command documentation to turn off directed broadcasts
http://infodeli.3com.com/infodeli/tools/bridrout/u_guides/html/nb101/family/REF/ip4.htm#190

3Com command documentation to disable source spoofing
http://infodeli.3com.com/infodeli/tools/bridrout/u_guides/html/nb101/family/REF/firewal3.htm#1823

Paul Ferguson's
http://www.denialinfo.com/
Dave Dittrich'
http://www.washington.edu/People/dad/
Cisco Newsflash on the DDoS Issue
http://www.cisco.com/warp/public/707/newsflash.html
Cisco White Paper on Rate Limiting
http://www.cisco.com/univercd/cc/td/doc/product/software/ios120/12cgcr/qos_c/qcpart4/qcpolts.htm

ISP-oriented paper on traceback
http://www.cs.washington.edu/homes/savage/traceback.html
Steve Bellovin's NANOG presentation on DDOS Attacks
http://www.research.att.com/~smb/talks/nanog-dos/index.htm
Fred Cohen's papers
Managing Network Security
http://all.net/journal/netsec/0004.html

A Note On Distributed Coordinated Attacks
http://www.all.net/books/dca/top.html

© SANS Institute 2000 - 2003 Author retains full rights.

HIP Protocol Proposals written by R. Moskowitz, ICSA.net:
A Note On Distributed Coordinated Attacks
http://www.ietf.org/internet-drafts/draft-moskowitz-hip-arch-01.txt
Host Identity Payload
http://www.ietf.org/internet-drafts/draft-moskowitz-hip-01.txt
Host Identity Payload Implementation
http://www.ietf.org/internet-drafts/draft-moskowitz-hip-impl-00.txt
Improving Security on Cisco Routers
http://www.cisco.com/warp/public/707/21.html
Characterizing and Tracing Packet Floods Using Cisco Routers
http://www.cisco.com/warp/public/707/22.html
RFCs:
RFC 2644 Changing the Default for Directed Broadcasts in Routers
ftp://ftp.isi.edu/in-notes/rfc2644.txt
RFC 2267 Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing
ftp://ftp.isi.edu/in-notes/rfc2267.txt
SANS Global Incident Analysis Center
http://www.sans.org/giac.htm

© SANS Institute 2000 - 2005, Author retains full rights.