Global Information Assurance Certification Paper

Defending Networks from SYN Flooding In Depth
Adam L. Rice
December 6, 2000

Introduction

The SYN flood attack came out of the underground and into the public spotlight the first week of 1996 on an attack on the New York-based ISP Panix Public Access Network Corp. The weakness in the connection-oriented TCP transportation protocol was known and understood for many years prior to the Panix attack, but its attack, which lasted a week, signaled the coming out of complied tools that were designed to attack the protocol's fundamental weakness.

Since 1996 the SYN flood has made news with attacks against the FBI, the White House, NYSE web sites, along with many others. The use of random spoofed source IP numbers on the IP headers made tracing the attacks back to the source nearly impossible. Hackers developed 'Zombie" hosts to attack targets in unison from a master machine. The technique, now famous, is referred to as the distributed denial of service attack. It uses many machines to coordinate attacks, and in many cases without the owner's knowledge or consent. The result is the same. The target computer fills a very small queue of half open port connections. Once the queue (also called a Backlog) is full, no other connections can be made until a connection times out and the memory space cleared, or the connection is complemented, which moves the connection out of the queue into an application level memory buffer. The computer stops answering requests on the attacked port once the Backlog threshold is reached. In the case of web servers, the attacks are aimed at ports 80 or 443. Once overwhelmed, the Web server stops working as designed and the attack is successful. Below is estimated backlog number of several popular OSs. The number is obviously very small considering the DoS tools can generate hundreds of SYN requests a minute.

OS	Backlog	BL+Grace	Notes
SunOS 4.x.x:	5	8	
IRIX 5.2:	5	8	
Solaris			
Linux 1.2.x:	10	10	Linux does not have this grace margin.
FreeBSD 2.1.0:		32	
FreeBSD 2.1.5:		128	
Win NTs 3.5.1:	6	6	NT does not appear to have this margin.
Win NTw 4.0:	6	6	NT has a pathetic backlog.

Taken from Phrack Magazine, Volume Seven, Issue Forty-Eight, File 13 of 18

How it works:

The source code for SNY flood engines and distributed denial of service engines, both zombie and master code, is easily found on the web. In some cases no knowledge other than following a well designed windows GUI is required to point the program at a target and press the appropriate start button. Regardless of software type, if it is a solo effort, or if it is a Distributed effort, the mechanisms are very much the same.

The DoS attack does two things: It sends a flood of single SYN TCP/IP package to a destination IP number and destination port and the source IP numbers of those packets are spoofed. Here is what happens. The packet is routed over the Internet to the destination target. The ability of the packet to route out of the gateway router of the originating network is a problem we will discuss in a few moments. The destination target, a web server, will receive a SYN packet requesting a connection on port 80. The Web server will reply with an ACK packet. The destination of the ACK packet is spoofed. If the spoofed IP number is legitimate, the computer that happens to correspond to the spoofed IP will simply send a RST (reset) package because it will have no idea why the target machine is sending an it an ACK. Each of the SNY requests will take a space in the OS's backlog waiting for an ACK package that will never arrive. The end result is that the target quickly depletes it backlog and the attacker will try to maintain a density of SYN requests to ensure the backlog never has the ability to clear. It is like trying to drain your bathtub with a fire hose in it. Water will fall down the drain, but far too much water is being poured in, and soon enough the tub will over flow. Once the backlog fills the server will stop accepting SYN packages, stopping the service until the backlog clears.

Because the source IP numbers of the offending packets are spoofed the ability of the victim to trace the

attacker or to filter requests by source IP is impossible. What is a vulnerable organization to do?

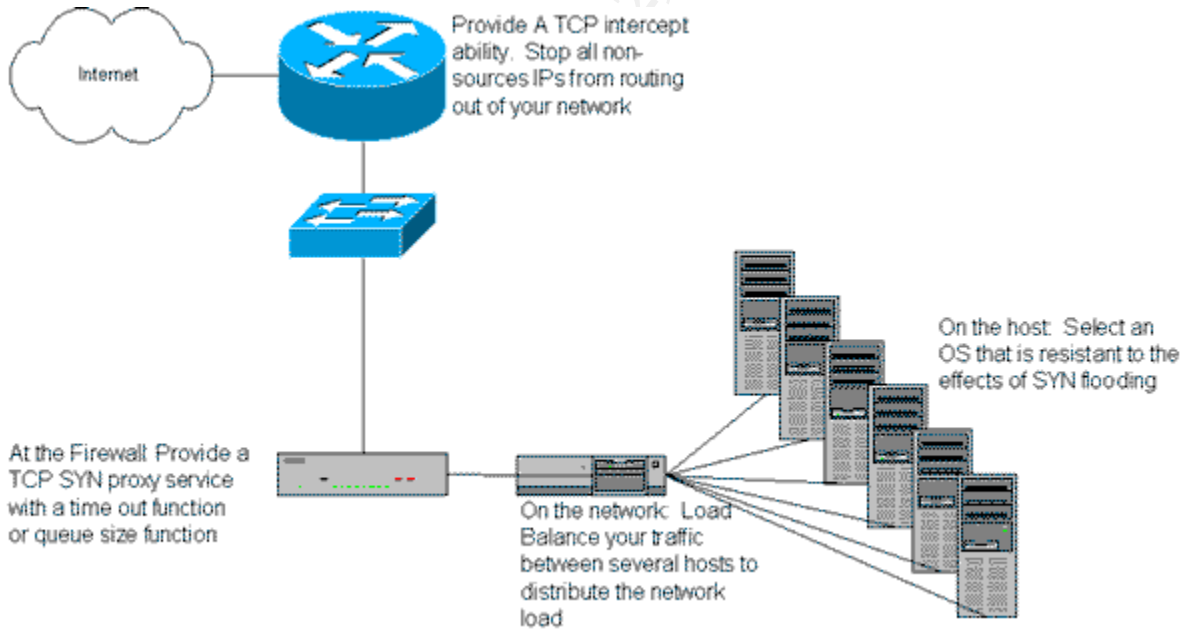
A SYN flood DoS cannot be stopped against a publicly assessable server. It can be slowed down and the success of the attack can be mitigated with as defense in depth and by organizations taking basic steps to prevent themselves from being the unknowing platforms of DoS attacks. A successful DoS attack will stop a service for an extended period of time. A DoS attack that closes a web site for ten minutes is not a success by any measure and might not even be noticed. The attackers will want to keep the attack up until people notice what is going on. An attack in secret does not fit the MO of the attackers. Some attacks last for weeks. Some are fought without public knowledge because they are not successful. Some are stopped. Services are always degraded but if an organization can absorbed the attack for long enough they will win the battle.

Defense in Depth

The defense against a SNY flood DoS attack must start at an organizations boarder router and continue through the network all the way to the target host. Most current technical solutions to SYN flood attacks have a real impact on the speed and response a network. In some cases human intervention to turn on SYN flood protection might be needed once an attack is identified.

Boarder routers

Boarder routers of organizations usually represent the delineation between an organizations line of control and responsibility and the wild world. The first line of defense against a SYN flood must start here. Boarder routers represent the first organizational network device a packet travels through on the way to the target host. If an organization has more than one ingress and egress point on their network, then all those devices are considered ‘boarder’ devices.



Depending on the brand and or model of router an organization uses, most have a configuration option that allows the user to intercept and monitor TCP connections. Half open connection, the hallmark of the SYN flood, is monitored and when a threshold is crossed then a predetermined action will occur.

Half open connections are normal behavior on the Internet so rather than create a denial of service inadvertently on your own network; an understanding of ‘normal’ traffic must be established prior to setting a threshold. Once that threshold is crossed then the router can begin aggressive filtering of SYN connections.

Here is how it works on Cisco devices, but the concept is pretty much what the industry uses:

You set a limit of half open connections that can be established through the router. Once the limit is crossed, the router will begin to drop connections at a specified rate or limit. The aggressive interception value is usually

half of the threshold. Configuration limits to turn off the aggressive threshold are available, as well if time or total connections are what set off the aggressive TCP intercept filtering.

SNY requests à Threshold limit of 50 à Crossed à Aggressive limit set to 25 before the next new half open connection causes the first to be droppedà SYN requests drop below predefined limit à Aggressive filtering stopped.

The greatest impact on this layer of protection is performance. The use of ACLs to only use TCP interception filters for specific networks or Hosts is probably necessary to insure reasonable performance to the rest of your network if the aggressive limit is reached on the router. Not all the spoofed SYN packets will be stopped. Many will, but not all. Many legitimate requests on slower networks will be stopped as well.

Firewalls

The next layer of defense against the SNY Flood attack will come at the firewall. Most firewalls built today are designed to enable a form of protection against SYN floods. Firewalls are better suited to fight firewalls because they tend to be designed to examine packets and maintain connection and state information of session traffic.

Many firewalls use state tables to keep track of the number of half open connections that are being passed through to a host, and once the limit is exceeded, the first one in the queue is the first open dropped. Some firewalls act as proxies intercepting the session, waiting for the three-part handshake to complete, and then set up the session with the host. Most of the limits are set by number of half open connections and time in the SYN queue.

Once again the issue affecting this layer of defense is the cost of performance. It does not filter by legitimate packet, but by a predefined threshold. Legitimate packets will be dropped, and illegitimate packets will get through.

Load Balancing

The last network defense against SYN floods is to distribute the flood against as many hosts or network devices as possible. In the case of commercial web sites or corporate sites that are well known and have considerable through put the load balancing is probably all ready in place.

An Alteon web switch or Cisco LD are both load balancing products that maintain state information to insure contiguous sessions between multiple hosts. Obviously it is better to have 100 physical machines absorbing a SYN flood than a single host. It is possible to load balance firewall as well using the same technology.

Host Protection

Many OS vendors are advertising a systems level resistance to SYN flood type attacks. Most of the information that has been reviewed indicates that the protective mechanisms are small and ineffectual to a large-scale attack. Increasing the addressable memory to the Backlog is not the best approach be cause even if the number was increased exponentially. A typical SNY flood engine could over whelm the Backlog, and by allocating more memory to the Backlog, degrade the performance of the host.

Obviously some OSs are more resistant than others. By design Windows products couple the IP stacks very closely to the OS kernel making a fault in the network stack a more dangerous thing than a UNIX type OS.

Conclusion

You cannot stop a SNY flood attack. You can layer your defenses so that the attack does not succeed. Success by the attackers definition is to bring a service down for a extended period of time. It is a battle to push as many of the SYN requests that are spoofed into the bit basket as possible while giving legitimate requests a chance of still getting through. The tuning of the layered defense is key to success. An administrator might have to tighten up defenses as the intensity of an attack increases and slacken the defenses as the attack decreases. An availability problem will always result from these attacks, but the measure of success is not to be shut down.

Logging during the attack will be of limited use due to the spoofed source IP number. Some logging might be

useful as a signature for the increase in service requests.

To prevent your organization from being a stepping off point for a DoS attack configure your boarder router to never rout any IP traffic that has a source IP that does not fall within your network range. This will prevent a computer on your network from sending out a flood of SYN requests with spoofed IP addresses. If your router is configured to prevent the routing of none approved IPs, then the SYN attack would be stopped before it started.

Defense in layers allows a network to distribute the flood and push as much of the spoofed SNY requests into the bit bucked before the packets get to the host. What might have began as a Fire hose of data can be whittled down to a garden hose, which will cause a computer to slow as SYN requests move through the Backlog or time out, but it will not stop ALL legitimate sessions from getting through the systems backlog and into to a service port.

References:

1. Sullivan, Eamonn. " New form of attack unleashed on the Internet" 16 September, 1996 URL: http://www.zdnet.com/eweek/news/0916/16epanix.html#top

2. "CERT® Advisory CA-1996-21 TCP SYN Flooding and IP Spoofing Attacks". September 19, 1996. URL: http://www.cert.org/advisories/CA-1996-21.html

3. daemon9 / route / infinity, "Project Neptune", Phrack Magazine, Volume Seven, Issue Forty-Eight, File 13 of 18 July 1996 Guild Productions, kid. URL: http://ndk.parallel.ch/synflood.htm

4. Paller, Alan and Pethia, Rich . "Consensus Roadmap for Defeating Distributed Denial of Service Attacks. A Project of the Partnership for Critical Infrastructure Security
Version 1.10" February 23, 2000. URL: http://www.sans.org/ddos_roadmap.htm#3

5. Cisco IOS Release 11.2, TCP Intercept. URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios112/intercpt.htm#23257

6. Kaeo, Merike "Designing Network Security", Cisco Press, 1999, pg. 127