Subject: INTRODUCTION TO NETWORKING
Posted by fl00d3d on Thu, 18 Sep 2003 14:58:49 GMT
View Forum Message <> Reply to Message

This is going to be a long message, so sit tight for a bit.

I know there are a lot of you out there that DO know the basics of networking and how to open the ports on your firewalls (usually software) ...but on the flipside I also know there are a lot of you out there (based on reading these forums) that DO NOT know the basics of networking. Therefore I'll cover a couple of the basics that should at least help you understand what some of these guys are saying.

IP addresses are used to route information. I think we all know this by now. However, the way that networking devices process the information that is sent is a different story.

A normal hub broadcasts information to every computer that is plugged into it. Therefore if you have 4 computers on your network (one of which is connected to someone's game server) -- every time the game server sends information to "you" it sends it to the other 3 computers too. And unless you have an intelligent hub, the signal is usually degraded.

A router FORWARDS information based on networking layer of the OSI model. (*note* the website I just linked to may or may not have accurate information. The OSI model was developed by the ISO, and you may wish to check their website out). This is the most common method of "internet sharing" found among simple broadband users.

NAT (Network Address Translation) is a technology developed to save real-world IP addresses. Rather than having 5 real world IP addresses for your network, you can have 1 then the other 4 can have "fake" (or internal) IP addresses. Here's the basics on how NAT works.
(1) A computer with a fake (or internal) IP address such as 192.168.1.2 wants to connect to the game server 66.92.46.127. The data is encapsulated into a packet with the ultimate destination saved in the header of that packet.
(2) This packet is forwarded to the gateway (more info about this in a second) which in this case is a NATing device. The NAT goes into the header of the packet and strips away the old source address (which was 192.168.1.2) and replaces it with the NATing device's real world IP address.
(3) The game server gets a request from the NATing device to connect. The game server connects and sends replies back to the NATing device.
(4) When the replies reach the NATing device, it strips the desination information from itself to the computer that originally sent the request (in this case 192.168.1.2).

The problem is when the NATing device has built in firewall which by default prohibits traffic between 'segments' of the internal network or blocks ICMP traffic from the internet (which makes you look like you have a horrible ping ... or even NO ping).

The default gateway is different for every computer. Look at it this way: if your computer wants to send information to my computer, it can't because its not directly connected and it can't find it. It needs to be forwarded. The way it is forwarded is through each computer's default gateway. So your computer sends the information to your router (which is your computer's default gateway) which forwards it to your ISP's network (which is your router's default gateway) who continues to

forward it ...

For the person that was woried about svchost.exe ---- this is a normal process. This service is used for anything that uses a dynamic link library (.dll) file. They're typically a resource hog. You can download tweaking programs if you want to try and help the situation. One can be found HERE.

Now, back to the DMZ issue. A firewall is essentially a "host based" product that monitors and blocks ports. Ports are used to communicate information between computers. If your NAT device/router has a built in firewall its probably going to block any ports above 1024 by default unless you enable them. Which, if you know anything about GameSpy and Renegade port configurations, most of them are above this range. One way to resolve the problem is to DMZ (Demilitarized Zone). This makes it so anything coming from the internet doesn't have to go through the NAT firewall. I've found that this usually still causes networking problems. If you use dial up, I would recommend NOT using a router, NATing device, or NAT firewall. If you want to connect multiple computers, I would just buy a $40 hub from Best Buy.

As for SOFTWARE FIREWALLS such as Zone Alarm or Norton Internet Security (NIS). DO NOT just disable them just because you can't play the game. YES it is definitely true that the firewall software uses a lot of resources, but trust me it's worth it. You have NO IDEA how often people get hacked and don't even know it. And unless you want your identity stolen or your computer crashed, get a firewall. I recommend Norton products. They're easy to use and provide decent security. Plus it's normally packaged with antivirus software.

Find a list of ports that is needed for what you're doing. Every program uses different ports. GameSpy uses like 10 ports, Renegade uses like 10 completely different ports, WOL uses its own ports, etc. I have a complete lists of all these ports on my site. Unfortunately I'm doing maintenance on my network so the webserver is not running (and the webpage is not available).

If you guys have any other networking related or security related questions, please feel free to ask me. I'll answer any question you have. I honestly know a little bit of everything ... and if I don't I know where to get the answers. I'm here to help you if you need it.

~fl00d3d~
cryptowizard@speakeasy.net