Who needs security?

A quick look at issues outside the office LAN

Jeff Nieusma, First Link Technology, Inc.

e-mail: info@firstlink.com

Last update: 2001 May 04

"…There is nothing on my home PC that a hacker would want…"

The facts

In a typical month, a small to medium ISP uses about 8 terabits of bandwidth, receives about 200,000 unsolicited, invalid, or unwanted port scans and/or intrusion attempts, and about 45,000 SPAM e-mail messages. As you might expect, all these port scans, attacks, and SPAM messages are not directed entirely at the ISP's server infrastructure; they are directed at the downstream address space, i.e. the ISP's customers (dialup, DSL, broadband, dedicated, everyone). The most common intrusion attempts are looking for NetBIOS, RPC, DNS, NFS, telnet, FTP, IMAP, and POP. The most common automated attacks are the SubSeven windows remote access Trojan, the ramen, and the lion worms.

Most ISP customers pay for connectivity and/or e-mail access. Something to note is that when an ISP customer can get to the Internet, other users on the Internet can get to them. So, as more people convert from the traditional dialup access method to DSL and broadband, they increase the window of opportunity for hackers to attack their homes.

A few details

These ports are not being scanned by accident or because some kid wants to test a new program. Hackers know how to remotely access (i.e. break into) computers using these services.

NetBIOS (ports 135 – 139) is the protocol that Microsoft systems use to communicate. It can be used to obtain machine names, user names, and shared system resources. It is used to look at and modify files on remote machines. It can also be used to look at and modify the registry on a remote machine. In short, Microsoft designed the networking functionality of Windows to allow for ease of use and workgroup functionality. Basically, it is very easy to get Windows machines to talk to each other. Security was not (and still is not) a big concern to the Microsoft way. In fact, the official response from Microsoft about how to deal with security is to install a firewall at your network border.

RPC (port 111 for UNIX and 135 for Microsoft), short for remote procedure call, is used to allow a network of computers to be used together in a "team" approach. It was designed as a convenient way to access resources, such as hard drives, CPUs, etc., on other computers. The basic idea is that when they start up, the sharable network processes register with the "portmapper." It works like an office building with no permanent cubicle assignments. As each occupant arrives for work, they grab a cubicle, then call the receptionist (the portmapper) and say, "I'm sitting in cubicle number 32775 today." Then as clients call the receptionist, they can be directed to the right phone. The theory is that if the receptionist doesn't answer the phone, no calls will be delivered. In practice, however, it doesn't always work that way. There are quite a few reported bugs and ways to remotely exploit these unpatched RPC services.

DNS (port 53), Domain Name System, is used to map names and URLs on the Internet to their respective IP addresses, which the computers need to communicate. Generally, DNS uses UDP datagrams for "quick" communications (i.e. getting IP addresses for names). TCP is only used for zone transfers (of entire domains), or when the data is too large to fit in a UDP datagram. There are many published ways to break into all but the most recently released version of the BIND DNS server software.

NFS (usually port 2049), Network File System, is the standard method for sharing files between UNIX machines. NFS, like most other RPC services, has very little security built in, and is therefore very susceptible to remote file manipulation.

Telnet (23) and FTP (21) services are easy to run brute force attacks against. Hackers can just guess at passwords until finding something that works. Of course, the telnet and FTP protocols send username and password information across the network unencrypted. So, a hacker can run a network sniffer program to grab usernames and passwords from users who run telnet and FTP. Once a hacker has this information, it becomes much easier to target particular users' machines.

IMAP (143), POP3 (110), and POP2 (109) are protocols for remote access to e-mail. These protocols use simple username/password authentication, and can therefore be used to facilitate brute force attacks, or can be monitored by sniffers for password harvesting. There are also published ways to remotely exploit each of these services.

SubSeven is the most common trojan tromping around the Internet today. It is one of the few hacker software packages that has an ongoing development effort, it is very easy to use and extremely powerful. SubSeven allows a hacker to remotely control a victim's machine, talk through the speaker, flip the screen over, etc. It also has propagation software, such as port scanners, and can be configured in a master/slave hierarchy where the master machine can tell slaves what to do.

Worms typically spend their life cycle breaking into machines. Once they break in, most worms use all the resources available to them to break into as many other machines as they can. In some cases, worms have destructive payloads, and in some cases, all they do is cover their tracks and attempt to propagate. The most common worms on the Internet today, lion and ramen, break into UNIX machines through documented and long published holes. Other worms take advantage of the convenience features of Microsoft operating systems and the gullibility of users. Typically, these propagate via e-mail attachments, and some have destructive payloads.

But, what does a hacker want with my home PC?

Although it would probably be pretty easy to pull your tax return off your computer, most hackers are not interested in reading it. Some would be interested in helping you with your on-line banking, however. Since most on-line banking systems only require simple password authentication, and because Microsoft software is very helpful in "remembering" your passwords, access to your accounts would be pretty easy to obtain. Also, since most people use the same password for everything, hackers have been targeting home PCs as an avenue for accessing corporate networks. It is becoming more common for people to have VPN access from home to their networks at work. Since most home computers have very little security, it is much easier for hackers to get into corporate networks through these "back doors."

Most users can detect when they are accessing the Internet. If they are sitting in front of their machine, pulling up pages, they are accessing the Internet. We say "most users" because many people don't realize that if they enable the auto-update feature of their anti-virus software (you do have anti virus software, don't you?) then their computer randomly accesses the Internet to get these updates, sometimes when the user is asleep. The big questions here are: How does a user know when a hacker attacks? How does a user know if their machine is a SubSeven slave? How does a user know if their machine is being used as a drone in a smurf attack?

Intrusion Detection Systems, either network based or host based, can keep track of this activity, and in some cases, curtail it. For a home network with one or two Microsoft systems, it is highly recommended to install personal firewall software, such as BlackICE Defender, or ZoneAlarm, or something similar. These packages are a combination of IDS and firewall software and are a very cost effective way to protect your systems from unauthorized use.

If your home or small office has a network, a small firewall appliance, may be a better option. One option is to setup a low-cost dual-NIC machine, (e.g. Linux), strip out all the network services, setup ipchains (or ipfw, etc), and use it as a firewall and network intrusion detection system. Even though this is a small capital investment, it may be well worth the investment to pay an expert to configure this environment, and provide enough training to be able to review the logs and recognize the warning signs of impending doom. The big question is, how much time and money will it cost to lose some or all of the network?

What about NAT?

Network Address Translation (NAT) allows a network to use "non-routable" addresses instead of more expensive, harder to obtain, routable address space. Please don't be fooled. NAT does not provide security, it is simply a way to avoid paying for expensive routable address space. It is trivial for a hacker to get to your machines in an insecure non-routable address environment.

So, now what?

It is time to start asking ISPs to provide more security options to their customers. An ISP can block known malicious network traffic at their border and save the headache of routing it, as well as saving the bandwidth of sending attack traffic to all their customers. It is also more cost effect for the ISP to build a large virus scanning system for e-mail, than for every down-stream customer to implement this functionality. Basically, how much is a customer willing to pay for a more secure upstream connection?

Bibliography

http://www.sans.org/ is a very helpful general source of information about security
http://www.securityfocus.com/ is another general source of security information
http://www.whitehats.com/library/worms/ is Max Vision's recent Internet worm library
http://www.simovits.com/nyheter9902.html is Simovits Consulting's list of trojan ports
http://www.linux-firewall-tools.com/linux/ports.html is a list of commonly probed ports
http://www.robertgraham.com/pubs/firewall-seen.html is a list of answers to commonly asked questions regarding firewalls
http://www.networkice.com/ is the company website for BlackICE Defender
http://www.zonelabs.com/ is the company website for ZoneAlarm