Global Information Assurance Certification Paper

How complicated is home protection?

Dale Hillman
November 23, 2000

Concept of threat

A common belief by some computer users is that hackers/crackers only go after large corporations such as the semi-recent attack on Yahoo. After all, why should someone interfere with just one person when there is much more challenge originating from a large entity and the subsequent prestige from a successful attack? "It's pretty admirable to take down Yahoo."[1] This ideology could not be further from the truth and can be correlated to that of theft. If it ain't nailed down, it will be stolen.

Not only do attackers fail to discriminate in their mischief; they even go so far as to target small businesses and home connections. Also, with the advent of high bandwidth home connections such as DSL, cable, and satellite services, attackers can use these connections as a depot to further their mayhem. Some of these high bandwidth connections also use static IP's. That coupled with 24 hours a day, 7 days a week connection is like hanging a neon sign taunting hackers. A new type of attack called a "tribal flood"[1] consists of a virus that is spread to as many computers that can be found with a permanent Internet connection. Then at a predetermined time the infected machines become "zombies" and coordinate an attack programmed into the virus.[2] Imagine what would happen if you worked in downtown New York City and consciously touched every person you could during one day. Then the next day every one of those people you touched walked into the streets of the city and just stood there. Traffic would come to halt (even for New York City). This is possibly how Yahoo's DoS attack took place earlier this year.

Type of threat

There are two main areas of threat I'd like to discuss here; internal, and external.

An internal threat is generally user based. Someone either brings in a virus via removable media or attempts to circumvent your security, sometimes unintentionally. This could be either your nine-year-old son at home or that pesky worker in cubicle 1A that feels security is overly emphasized. The worst type of internal threat falls into the malicious software area such as a Trojan. Once it is planted it could transmit out to the Internet your most private of information. These are sometimes the hardest to block because normal users may not know the present danger, like walking on the surface of a frozen lake that could break through at any time.

An external threat is normally someone or something that is actively attacking or attempting to break into your network. This is generally an actual hacker/cracker using tools to determine your security vulnerabilities to further his attack or is already actively attacking your network.

The Choices

Now that a user knows he/she is vulnerable at home, what is one to do about it? There have been many software alternatives available for years now such as WinProxy, MS Proxy, MS Internet Sharing, and actual firewall programs like ZoneAlarm. These programs offer a fair amount of flexibility if you know how to configure them. Another alternative is the booming home router or gateway, which usually consists of a small hub using Network Address Translation (NAT), and some form of firewall built in. NAT is the basically a hack created in the early 1990's to allow many machines share one IP address but expanded to the security realm. It allows all traffic out and keep track of the local IP that sent information out of the home network. When an external machine requests to send information through the NAT it checks to see if one of the internal IP's requested anything from the incoming IP recently. If there isn't a match the packet is refused.[3]

The proxies offer Internet sharing, web site caching, NAT, and some even do VPN's. A VPN is a Virtual Private Network where two sites build a secure tunnel over the Internet to share private information. Microsoft's own Internet Sharing was created to allow multiple machines to share one line and claims to allow a home network with file and print sharing to take place but there is very little information about this and the supposed security. The proxies are more powerful allowing packet filtering and port control within the firewall. Other programs like Zonelabs free ZoneAlarm, Norton Internet Security 2000, and BlackIce Defender allow a range of customizing and powerful features like real-time intrusion detection and virus protection. The proxies require an additional machine to be the gateway to the Internet for all other computers behind it on the network. The firewall programs do not require additional hardware but have to be installed on each individual machine.

The hardware alternatives start as little as $100 for a simple one-in one-out type connection and can add 4-8 port 100 Base switched hubs for $50-100 more. This better facilitates home networking and can offer the same level of convenience and protection as the software alternatives. Companies like Linksys, D-Link, Netgear, ZyXel, and others have jumped on the bandwagon to offer these products as well. They can also be too limited if options are not configurable or too complicated as well. The ZyXel 310 had the most power of the bunch but can lose users when trying to telnet via a serial cable to do the updates. Most others do updates via on-screen menus through a browser and offer port forwarding and filtering service for those who are running servers and for those DSL users with dynamic IP's, DDNS automatically connects your server to the rest of the world every time you get a new IP. Linksys even incorporated flashable BIOS to further add to its versatility but allowing features to added at a later date.[4]

Am I safe now?

Which alternative you decide to go with depends on your needs, technical expertise and

budget. After deciding which product to go with how do you know you are safe? A few well respected web sites offer free scanning to check just such a thing such as www.secure-me.net and grc.com to name a few. Both sites offer a free basic TCP/UDP port scan. A basic Windows based PC with file and print sharing turned off will offer a response but deny the connection. This acknowledgement lets the potential hacker know that there is a live machine at that particular IP address, what OS it is running on and consumes very little time as the machine will respond instantly. A properly functioning firewall will operate in "stealth mode" which will basically look like a dead IP. This not only gives the hacker little information it also takes up a significant amount of time and resources for the hacker while the scan repeatedly tries to connect at certain ports and has to wait for the request to time out.

There can also be an internal threat. Up until now I have only addressed the outsider-wanting-in threat. The above alternatives help to prevent an attack or hack. If a virus or Trojan found its' way into your machine via a program you installed or a corrupted email it is a whole new game when your computer wants to send information outside of your network. Email is not the only way to contract such a problem either. Napster, a widely popular program used to distribute MP3 songs on millions of computers worldwide does not authenticate the files it transmits. The user actually connects to others strange machines to browse and download what they have to offer while offering what they have in turn. Napster simply checks to see that the file contains the proper header information to be an MP3 file such as the frequency it was recorded at, song name, etc. A recent program called Wrapster became available that allows any program to be imbedded into an MP3. It does require that both sides have the software installed for it to work but this is an omen for what is possible.[5] Once this file has entered your system it can attempt to transmit out. Steve Gibson of grc.com created a program called "LeakTest" which attempted to simulate "internal extrusion". This program would attempt to send data from your machine to a predetermined IP on the Internet through your firewall by simply opening port 21 and simulating an FTP client connection. This sounds ridiculously simple, but every firewall and router tested failed with the exception of ZoneAlarm. Version 2.0 of "LeakTest" is close to coming out and programs like this will help to separate the real firewalls from the ones that jumped on the bandwagon just to make a buck. Most manufacturers are attempting to patch this vulnerability now. The reason this works is that most firewalls do not check outbound traffic and the few that do only try to authenticate to a know list of "acceptable" programs that could use such ports. Symantec's Norton Internet Security 2000 program for instance had 152 approved FTP programs. All a virus' executable has to do is name itself one of these files to be allowed access to port 21. ZoneAlarm went a step further and generates a "Cryptographic Signature" for permitted programs to insure that these programs were what they claimed to be. ZoneAlarm is free as well.[6]

This should not deter people from using high bandwidth connections or the Internet in general but to better inform users on the potential for trouble. These tools along with a good anti-virus program will go a long way to protecting your investment, your time, and your privacy. Hopefully the hacker will then move on to the next guy with less

protection.

References

1. Featherly, Kevin. “Yahoo Attack May Have Been 'Tribal Flood' – Expert”, Newsbytes, 08 Feb 2000. Quote by Patrick Taylor (Dec 17,2000)
   URL: http://www.newsbytes.com/pubNews/00/143526.html

2. Spanbauer, Scott. “5 Reasons We (Still) Love Dial-up”, PC WORLD, pg. 96, Jan 2001, (Dec 17, 2000)

3. Hasenstein, Michael. “IP Network Address Translation”, 1997 (Nov 23,2000)
   URL: http://www.suse.de/~mha/linux-ip-nat/diplom/

4. Various authors, Reviews Section for Routers (Dec 13, 2000)
   URL: http://www.speedguide.net/

5. Radcliff, Deborah. “Napster gaffes”, July 17, 2000 (Dec 8, 2000)
   URL: http://www.computerworld.com/cwi/story/0,1199,NAV47-68_STO47133,00.html

6. Gibson, Steve. “Internet Connection Security for Windows users”, Dec 14, 2000 (Dec 17, 2000)
   URL: http://grc.com/lt/howtouse.htm

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: May 28th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event