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 Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Security Ramifications of Using Peer to Peer (P2P) File Sharing Applications

© SANS Institute 2004, Author retains full rights.

Lucas Ayers
GSEC Practical
Version 1.4b
December 20, 2003

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Table of Contents:

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

1.0 Abstract:

This paper will outline some pitfalls of using the ever popluar file sharing applicatons, also know as Peer to Peer networks (P2P). Some people seem to always be looking to get the latest software, movies, music (or anything else you could imagine) as soon as they are realesed, often before. While this can be illegal and unethical (in some cases) it still happens everyday. However most of the average users of these applications do not know that there are quite a few secuirty risks introduced to their network (both at home and at work) once the P2P applications are installed. The security implications brought by P2P applications are great for home users, but when they are installed and running on a users computer on a corporate network the consequences are even greater.

Some of the risks brought on by P2P file sharing applications include: spyware, ad ware, viruses, worms, trojans, personal information leaks & excessive bandwidth consumption just to name a few. If someone choses to use these applications they have a obligation to educate themselves about these security threats beforehand, and take as many preventive measures as possible to minimize the risks.

The point of this paper is two fold:

1) To point out some of the basic Secutity risks that are introduced once you start using P2P applications.

2) To show you how to minimize these risks as much as possible if the use of P2P applications is a nessisity.

2.0 Overview

2.1 History

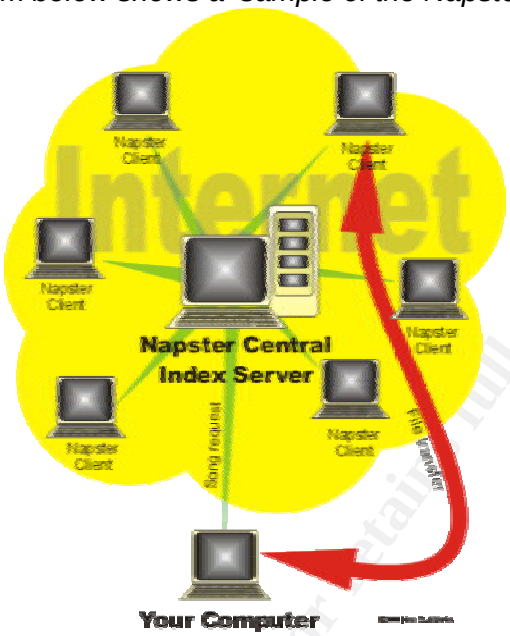
In the 1990's peer to peer sharing of files was brought to the limelight by the now infamous application Napster. Napster was devoted to the free trading of music files between users of the Napster network and became quite popualar. At its peek in Febuary 2000 Napster had a reported 1.6 million simultaneous users sharing music files [1].

Napster was created to work with a centralized server; anyone that wanted to use it needed to download and install the free Napter client. Once installed the client would connect to the server letting the server know the client was there and ready. The centralized server constantly tracked which clients were online. If another Napster user wanted to search for a file he/she would send a query to the central server, in turn the server would then search all known clients for a match. The closest matches were then sent back to the user that initiated the search. Results contained the file name, IP address and other information – once the users clicked the file they wanted to download

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

the centralized server was out of the loop – all file transfers were done directly from the Napster client to Napster client (Peer to Peer).

The diagram below shows a sample of the Napster network[2]



The recording indusrty put a halt to the Napster parade by filing lawsuits for copyright infringement which led to the shutdown of the Napster centralized servers in 2001[3].
Note: Napster is back online now but as a paid service.

2.2 Current State of P2P

Since the fall of Napster, many P2P applications have popped up trying to fill the large void that was left. They have absolutly filled the void, and then some!
Where Napster was dedicated to trading only music files, the new P2P applications have no such limitations - you can trade almost any file imaginable (text, images, music, movies, applications…..and more) using the newer P2P networks.

There are also some technical differences. Napster used a centralized server that monitored all clients and facilitated the searches and file transfers; the new P2P programs have no such centralization and allow for direct user-to-user file sharing[4]. This is more difficult to track, control and stop if needed.

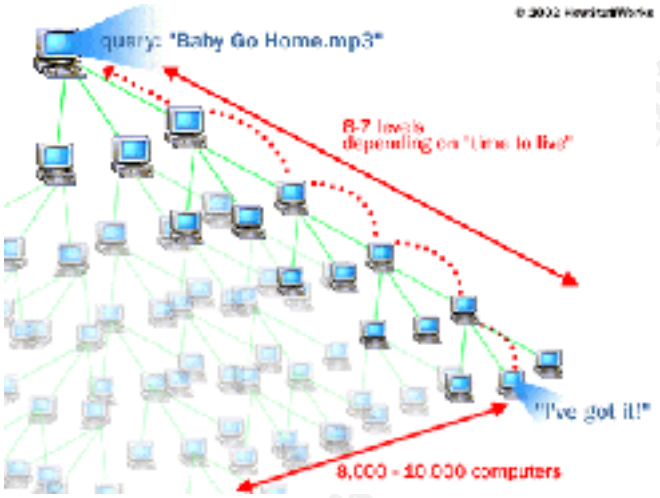
For instance when Napster was ordered to shutdown by court order – they simply had to turn off the central server/servers which completely stopped file sharing through the Napster network. Since each client needed to register with the central servers and all searches went through the central servers, without the servers there was no file sharing.

On the newer P2P networks there is no central server – so there is no way to simply turn off any server/servers and stop the sharing of files. Each computer is truly both a client and server. Every computer conducts its own searches for files we want to download – now that is not saying a single computer will search every computer by itself looking for the file we are trying to download. In one way or another, the search is

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

shared: my computer asks other clients it knows of – those computers ask clients that they know of and so on. Or on some networks there are supernodes in areas that aid in seaching, however, these supernodes are not dedicated servers, they are just user computers that happened to be elected to supernode for a period of time based on the connection speed and power of the computer. In either case, there is no single server/servers that conduct every search.

Below is a simple diagram of how the new crop of P2P applications search[5]



Below are some of the most popular programs out of the new crop of P2P applications. This list was taken from download.com's most poluar downloads. The four below were within the **top** fifteen downloads for **all** Windows applications:

THIS WEEK	Most Popular Titles in Windows Week Ending December 21	Last Week	Weeks On Chart	Downloads This Week	Total Downloads
1	Kazaa Media Desktop	1	86	2,424,896	307,970,903
4	iMesh	4	191	405,686	63,597,492
11	Morpheus	10	138	181,495	118,322,020
13	LimeWire	12	22	124,491	17,571,452

Dowload.com [6]

When you calculate the total downloads of the four applications above it comes to 507,461,867! That is correct over 500 million - now, of course, there are people who have downloaded twice or others who have one of these applications on a few different computers but in any case 500+ million is a lot of downloads! According to one report from the US Congress: reasearch done by D. Hart Research Associates shows that 41% of people who donwload files through file sharing networks are between the ages of 12 and 18[7]. Has anyone made the millions of 12-18 year olds aware of the security risks of the programs they are using? Or how to minimize these security risks? Some how I don't think so, but it needs to happen! When your computer is connected to the Internet you have an obligation to others on the Internet (since we are all neighbors) to try your best when it comes to keeping your computer secure.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

3.0 Sercuity Issues with P2P file sharing

The sections below contain overviews of some of the security risks we face when using P2P file sharing applications. This is not a catch all list since there is no way to list every possible vulnerability, new ones are being discovered everyday – it would be impossible to list every virus one might get using a P2P network – the objective of this section is to simply point out the fact that each of these risks exist.

3.1 Ad ware and Spy ware

The first security risk we will speak about are Ad ware and Spy ware. The reason we will discuss them first is that quite a few of the free P2P software comes with Spy/Ad ware in one form or another bundled with them! When you install the free version of your favorite P2P program you are also installing Ad or Spy ware! In essence once a P2P application that includes ad ware or spy ware has been installed – your security has been breeched!

What are Ad Ware and Spy ware anyway?

3.1.1 Spy Ware

The following definition was taken from spykiller.com a commercial spy/ad ware removal application.
Spy Ware are evil programs that hide on your computer and do a number of harmful and annoying things without your knowledge. Spy Ware programs are known to steal information from your computer such as credit card numbers, email addresses, addresses, surfing habits, and more.[8]

3.1.2 Ad Ware

The following definition was taken directly from *spywareguide.com*
Explanation: Program that creates advertisements on your PC.
Note that many websites have their own advertising, unrelated to ad ware.
Official definition:
"Adware is any software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen. The justification for ad ware is that it helps recover programming development cost and helps to hold down the cost for the user.
Adware has been criticized for occasionally including code that tracks a user's personal information and passes it on to third parties, without the user's authorization or knowledge." [9]

Spy ware and Ad ware are often referred to as one and the same whether this is an accurate statement is the subject of debate. In either case, this class of software typically will have some sort of mechanism to track a user's computer usage (track websites viewed and the like) then give this information to an outsider. Obviously neither Ad ware nor Spy ware are things you would choose to install on you computer. They violate your privacy; and in my opinion there is no reason some marketing company should have my web browsing habits sent to them, from my computer no less.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The following list obtained from *frixo.com (which is a website dedicated to advising users of their online privacy*) shows which P2P Programs (the free versions) come bundled with spy ware that is installed automatically [10]

Software	Spy ware infected?
Kazaa	yes
Imesh	yes
Bearshare	yes
Morpheus	yes
Audio Galaxy	yes
Limewire	yes.
Xolox	optional
Grokster	yes

From frixo.com (http://www.frixo.com/sites/adoko/p2p.html)

Some steps for Reducing the risk of Ad/Spy ware will be detailed in the *Minimizing Security issues* section below.

3.2 Sharing Personal Information

The second security issue we will discuss is the sharing of personal information. Due to both user error & lack of knowledge, there are countless personal files being shared on P2P file sharing networks! The results of which can be devastating.

In one way or another all file sharing applications create a default shared folder when they are installed on your computer. Every file you want to share must be placed in this folder. Also by default all the files you download from the file sharing network are downloaded to this shared folder. Each and every file located in this folder is freely accessible to any and all users of the P2P network. While this concept sounds easy enough to understand, there are countless files being shared that should not be. These include but are not limited to the following: banking records, personal password files, credit card information, Social Security numbers, Financial software backups and the like, all being shared with the world. Obviously these are not things you want to share.

One report includes a very shocking list of some files that are being shared on P2P networks. The report can be found at the following URL:
http://reform.house.gov/UploadedFiles/P2P%20Security%20Report.pdf[11]
Part of this report shows the results of tests conducted on P2P networks looking for personal information. The results of which are truly astonishing!

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Here are just a few samples:

- Completed Tax returns
- Narcotics inventory on a Naval Ship
- Military Medical records
- Divorce correspondence
- Living wills
- Personal Email Inbox
- Also over 2,000 Microsoft money backup files.

Some of the consequences of these documents being shared include: credit card fraud, Identity theft and even a possible threat to national security when it comes to the military documents!

Some steps for educating users on how to properly share files on P2P networks will be detailed in the *Minimizing Security issues* section below.

3.3 Viruses & Worms

The next subject is the presence of Viruses and Worms on P2P networks. These malicious programs are nothing new and pose a security risk to everything we do on our computers. Whether we are surfing websites or receiving emails we need to be aware of viruses and worms. Such is the case when we are using P2P applications, the very nature of sharing files lends itself very nicely to the spreading of viruses or worms (both intentionally and unintentionally). When we download files from P2P networks, we are at risk of pretty much every virus/worm we could get through email or any other means. Viruses and worms can range in the effect they have on your systems – anything from small nuisances to completely deleting your hard drive or anything else you can imagine! There is literally no end to the possibilities.

What are Viruses and Worms anyway? What is the difference?

Below are the part of the definitions for both a Virus and a Worm directly from the SANS GSEC course book:

Virus:
A virus is a malware specimen that has the ability to replicate and possesses parasitic properties. A virus is a parasite because it cannot exist by itself; instead it must attach itself to another program The payload of the virus executes when the user launches the program to which the virus is attached.[12]

Worm:
A worm is a self-contained malware program that has the ability to spread itself without the victim's participation.[13]

In other words, a virus needs some sort of user intervention to launch its attack on our systems where a worm needs no such user intervention.

P2P Networks add a new twist to the Virus/Worm war - there is a new crop of viruses and worms that have begun to creep through the P2P community. These are viruses and worms that were specifically designed to spread through P2P networks!

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The following are parts from a definition of P2P worms taken from F-secure.com at:
http://www.f-secure.com/v-descs/p2pworm.shtml[14]

NAME: ***P2P worm***

A peer-to-peer network (P2P) worm is usually a standalone program that spreads using P2P (peer-to-peer) networks. There are a few well-known P2P networks - Gnutella, Kazaa, Morpheus and so on.

The most widespread are Kazaa P2P network worms. A Kazaa P2P worm usually locates Kazaa client shared folder and copies itself there with an attractive name, for example with a name of a popular song or movie. Sometimes such worms replace real movie or sound files with their copies and add executable or double extension to such files.

When other people search P2P network for certain files and that get a match on an infected computer, they download the matched file and run it unaware that they are actually downloading a worm that used a fancy name or replaced the original content. A worm activates on their systems, copies itself to their P2P client share folder and thus continues its spreading cycle.

Most famous P2P worms: Kitro, Lolol, Benjamin, Roron

In summary: with P2P networks as with any other type of file download (FTP, HTTP, email ….) there is the inherent risk of viruses and worms. However, P2P networks are becoming a direct target of these malicious programs and this will likely continue to increase in the coming months and years.

Some steps for reducing the risk of viruses and worms on P2P networks will be detailed in the *Minimizing Security issues* section below.

3.4 Trojans and Backdoors

A Trojan is a piece of mailware that is hidden inside another piece of software, trojans can not replicate. Trojans open backdoors - giving the creators the ability to completely control your computer remotely. There are several well known Trojan programs including SubSeven and Back Orifice. These are both programs that give their creator/controller remote access to your computer with rights to do just about anything they want.

Some examples of what they are able to do remotely include:

- Delete files
- Change the registry
- Open and close the cd-rom
- Monitor your keystrokes on a keyboard
- Look at and edit your personal files
- Watch your Web cam
- Monitor what you do on your computer

These nasty pieces of software are typically hidden inside a legitimate program (also called wrapping). This is why they are named Trojans or Trojan Horses – they are named after the famed Trojan Horse of Troy, where enemy Greek soldiers hid inside a large horse and then came out at night to take over Troy.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Once the Trojan is installed the program will notify the creator via email, website or other means, telling him all the information he needs to connect and take remote control of your computer (IP address, port…….). There are other Trojans that upon being installed will conect to an IRC channel (that the creator configures) and wait there for further orders. Some Trojans can be configured either way!

Once an attacker gets his/her hands on your personal information this can lead to: credit card fraud, bank accounts being cleared out, identity theft and more.

Trojans are also useful to attackers for reasons other than stealing your personal information. Attackers can use your computer as a jumping point to break into other computers – this way the trace would lead back to your compromised computer and not back to the true attacker. They can also launch DOS (denial of service) attacks from your computer, which is basically the attacker making your computer slam a victim computer (a Web server for example) with data, this can keep the victim computer from servicing valid request. The same would also be the case for DDOS attacks (Distributed Denial of Service Attacks) which is similar to the DOS attack described already except the attack comes from many computers the attacker has control of – for example hundreds of computers even thousands (one of which is yours) all attacking a web site. In both cases (DOS and DDOS) if the attacker uses your computer in the attack, any firewall logs, IDS logs… will have your IP addresses listed, not the attackers.

Besides the risk of downloading a file (from other users) that may be hiding a Trojan, there are quite a few cases where the free versions of P2P applications were found to have a Trojan included in the installation package. One article on such a case can be found here: http://www.wired.com/news/privacy/0,1848,49430,00.html [15]

Some steps for Reducing the risk of Trojans on P2P networks will be detailed in the *Minimizing Security issues* section below

3.5 By-passing Perimiter Security

The perimeter of your network is the location where your network ends and the Internet begins. It is also called the edge of your network. This is a very sensitive area that needs to be guarded. Everyone needs to protect their borders from the wild internet, whether you are a fortune 500 company or a home user. This is the location where at a bare minimum, a firewall is installed; preferably there will be layers of security at this location such as an edge router doing packet filtering, then a firewall doing state-full inspection and Network Address Translation (NAT). Even a home user should have some type of firewall at the edge of their network; firewalls are no longer for corporate networks only.

Packet filtering: is basically the concept of forwarding or denying packets based on layer 3 or layer 4 information. This is done through the use of an access list. An access list can be configured to allow or deny packets based on IP address, Protocol, port numbers. After an access list is created it needs to be assigned to an interface either inbound or outbound.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Below is a sample of a simple access list on a Cisco router that will block pings except from one specific host (and the replies to those pings):

```
access-list 150 permit icmp host 10.1.1.1 any echo
access-list 150 permit icmp any host 10.1.1.1 echo-reply
access-list 150 deny   icmp any any echo
access-list 150 deny   icmp any any echo-reply
access-list 150 permit ip any any
```

It is important to note that access lists process from the top down, so order is very important once there is a match the router will take the appropriate action (Permit/Deny) and then stops processing the access list. It is also important to note that at the end of an access list there is a deny all statement.

Firewall State-full Inspection: is basically the concept of tracking connections, and allowing or denying access for each packet based on the "state" of the connection. Each packet that goes from the inside network to the outside world is placed in a table. When the reply from the outside world returns to the firewall – it is allowed through if there is a match in the table. The table is filled up dynamically as packets transverse the firewall.

A lot of time and money are spent both purchasing and configuring these perimeter devices. But the use of P2P File sharing networks can completely by-pass all these security measures and give outside computers access to our internal network. This is the case because when you launch the file sharing application it establishes a connection to the file sharing network, this connection is then left open so users of the file sharing network can access files on your system.

Some steps to try and keep people from By-passing Perimeter Security by using P2P File Sharing networks will be detailed in the *Minimizing Security issues section below.*

3.6 Bandwith consumption

The final risk of P2P we will discuss is the excessive bandwidth these applications take up. Some studies show that 60% of all internet traffic is due to the use or P2P applications[16]. The amount of bandwidth being used by P2P applications (searches, keep-a lives, downloads and the like) can be enough to degrade service for everyone. One of the main goals of information security it to protect the "availability" of our systems and information. If too much traffic is on the network due to P2P applications, there could be times where a vital application is unable to communicate on the network. This would be an example of the systems availability being threatened, even though the system is up and running, hasn't been hacked and has no viruses – the system is still unavailable – due to bandwidth consumption

Some steps to try and manage the bandwidth consumed by P2P File Sharing networks will be detailed in the *Minimizing Security issues section below.*

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

4.0 Minimizing Security issues

Before we begin discussing individual concepts to reduce security risks, we need to discuss the entire process of minimizing security risks as a whole. The best security designs come from a layered approach to security, also know as Defense in Depth. No single layer of security can protect us from every possible risk. Only through a well thought out and layered serurity model can any security design begin to be effective. Think of it this way: if you have the strongest front door in the world with the best locks possible, but your windows do not lock – is your house safe? No; it is not! You need a layered approch:

Strong Storm door that locks
Strong inner door with Good locks
Quality locking windows
Gated grounds
Quality Alarm system
Motion sensors
Security Guard
Guard Dogs
….and so on

All this security does come with a price – usability! Would you enjoy living in a house with security guards roaming around your halls and guard dogs prowling your yard? Probably not! There is a balance we all must find between security with liveability – the same thing applies to our information systems. If every aspect of our computer systems were completely locked down for security - we would greatly suffer in productivity. But if everything was free and open to make things easy to use – we would be robbed blind!

Every person and organization is unique, we all have different opinons of where that balance lies. It is up to each individual (or policy makers for a company) to decided where his/her comfort level is and build a security structure to match that.

4.1 Block users from installing applications

This is one of the most successful ways you can block the use of risky software. Not just file sharing applications but, Instant messaging, games or any other applications. Not all users need to have the right to install software - in fact most do not!

On a corporate network a lot of time is spent packaging and testing applications to verify each and every application will function properly. If everyone is granted the right to install software and they are free to download and install whatever applications they want – what is the point of the packaging and testing? Lock all user accounts down to plain users and take away install rights – the only people that need install rights are IT personnel.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

For home users - again not everyone needs install rights! This can be an easy way to keep track of your children's internet access, besides all the net-nanny type programs – if we lock down the administrative rights of children's accounts there is no way they could be installing these P2P networks and opening up our computers to these massive security holes. We can easily make ourselves the administrators with full rights and our kids account can be limited to simple users with no rights!

The term for this limiting of access rights is known as: **The principle of least privilege.** This means to only give users the bare minimum access rights they need to do their job! Or for a home network – give children the bare minimum rights to do their home work and maybe chat with friends.

4.2 Ad Ware & Spy Ware

The most successful way to keep your computer Ad ware and Spy ware clean when you use P2P applications is to only install known Ad/Spy ware free versions! Most of which you have to pay for! The whole reason the free versions are free is because they include these Ad/Spy ware – advertisers pay the applications developers to keep the end users cost down (or Free) and in turn the developers include versions of the advertiser's ad/spy ware.

Also the principle of least privilege can help here as well:
If a user "needs" to have a P2P file sharing application on his/her computer but she/he has no rights to install software, there is no way he/she can install the free version that contains Ad/Spy ware! Someone from IT must install it for him/her and will install the approved Version, which is Ad/Spy ware free.

4.3 Sharing Personal Information

It appears most of the sharing of personal files is due to user error – where a user mistakenly shares documents they didn't mean to. While this is not a true technical issue like firewall rule sets or router access lists, it is very much a Security issue. Informing users about security and making everyone aware of the consequences of their actions, is one of the most imports tasks any security office has.

There are also issues with the wizards and setup programs of some of these file sharing applications used during installation. The wizards will ask the user if they want to search for the location of typical files people share. If you happen to have a bunch of music files located in your "My Documents" folder (this is a typical location people have personal files on their computers), the setup program will share that whole folder with the rest of the P2P network. Not just the music you meant to share, but everything in that folder!

There are also concerns surrounding the participation level of each user of the file sharing network. The more files you share the higher your rating is on the network, so some users share their entire computer or large parts of it with the file sharing network just to have a better rating - all without being aware of the consequences.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The best practice would be to not allow the system to search for files to share, only have a single shared folder on your computer. Anything you would like to share going forward, you can manually move to the single shared directory.

4.4 Viruses/Worms

The first step in virus protection is the same for all virus risks (email, ftp, P2P) so it is nothing new. We **need** to install virus protection on all of our computers. This is a well documented and well known rule - every computer needs virus protection - **PERIOD**. Some quality virus protection can be purchased from: Symantec (http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155)[17] and MacAfee (http://us.mcafee.com/virusInfo/default.asp?cid=9043) [18]

The second step is to enable real-time monitoring which allows the virus scanner to continually scan the system for viruses, not just a scan of the system at set intervals. When set-up this way, it is much more secure – every email you receive, every email you send and every file you download is scanned for viruses in real-time.

The Third step is to continually update your virus definitions. New viruses are discovered everyday and you need to update the definition files your virus scanner uses. I like to have my computer use the automatic update feature that is included with most virus scanners. I set the system up to check for updates every night at 3am – this all happens automatically.

4.5 Trojans

The first step in protecting your system from trojans is the same as the Virus section above; we need to install virus protection. Just about all virus scanners these days are also capable of finding Trojans. Also the same as above, we need real-time monitoring enabled and need to keep our definition files up-to-date!

The second step is to install a Trojan scanner. These pieces of software are no where near as popular as virus scanners. As such many people have either never heard of them or think their virus scanner detects Trojans so why bother with a dedicated Trojan scanner. A Trojan scanner was developed solely to find Trojans! The developer of these applications live and breathe Trojans. Virus scanners were developed to find viruses and worms – but threw in the ability to find Trojans as an add-on or after though if you will. Virus scanners are great at finding viruses and worms but they are not in the same class when it comes to finding Trojans. One high quality Trojan scanner is called TDS (**T**rojan **D**efense **S**uite) and information can be found at the following URL: http://tds.diamondcs.com.au/ [19]

The third step in Trojan protection is to try and cut off their communication with the outside world. We could do this in a couple of ways, or both if possible. First, we can block ports of well known Trojans at the perimeter firewalls. Second, we can install a host-based firewall (firewall software installed on user desktops) on each computer that can be configured to allow or deny network access on a per application basis.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

A list of the common default ports used by Trojan's can be found at the following URL: http://www.simovits.com/nyheter9902.html [20]

There are many host based firewalls on the market today; most of the top virus protection companies also offer desktop firewalls. A pretty good article on personal firewalls can be found on the Security Focus website at the following URL: http://www.securityfocus.com/infocus/1750 [21]

4.6 By-passing Perimiter Security

One common setup on firewalls is to allow everything from the internal network out to the internet. But deny everything coming from the internet that is not a response to a request on the inside network.

Let's take a look at how this looks:

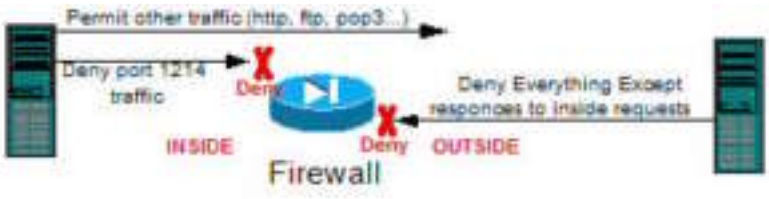
The first change we must make in trying to keep our perimeter secure "in spite of" our internal users, is to stop trusting everyone on the inside network! When it comes to stopping File sharing networks we will need to block at least the default ports on the firewall for as many of the well know File Sharing networks as we can.

A short list of the default ports used by some P2P file sharing applications can be found here: http://www.practicallynetworked.com/sharing/app_port_list.htm#Multimedia [22]

For our example we will block the default Kazaa port of 1214 on our Pix firewall.
We will do this by creating an access list that denies all internal devices from accessing any outside IP address on port 1214 both TCP and UDP. Then we apply this list to the inside interface on our firewall.

```
access-list outbound deny tcp any any eq 1214
access-list outbound deny udp any any eq 1214
access-list outbound permit ip any any
access-group outbound in interface inside
```

Now let's take a look at what this looks like:



© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The problem with blocking the P2P applications by their default port numbers is that the developers of these applications have already thought of this. Kazaa for example will try random port if the default port is being blocked; it will even try to go out on port 80 which cannot be blocked because this is the same port http works on by default.

However, blocking the default ports will work on older versions of software and will also work to keep some of the less knowledgeable users who do not realize they can manually change the ports these applications use. So the blocking of known ports can definitely be a plus when you are trying to get as many layers of security as possible.

4.7 Bandwidth Consumption

The final section of this document will highlight ways to reduce the excessive amounts of bandwidth used by peer to peer file sharing applications. As stated earlier the excessive amount of bandwidth used for these P2P applications could result in vital systems being unavailable – this is something we need to avoid at all costs.

The first step we can take is to not allow any of our documents to be shared. We can completely empty our shared folder and we can also turn off sharing. There is information on how to do this from within the Kazaa application at the following URL: http://www.kazaa.com/us/help/guide_settings.htm#settings8 [23]
If we still want to share files but want to limit the amount of bandwidth used, there are settings included with Kazaa to limit Maximum Bandwidth**,** Traffic Limits and others. A description of each of these settings can be found at the following URL: http://www.kazaa.com/us/help/guide_settings.htm#settings2 [24]

However, the steps above leave everything to the end user. In order for any of them to work the user:

1) Need to be informed of the excessive bandwidth these applications use up
2) Has to want to reduce the bandwidth he/she is using
3) Needs to know about the features mentioned above

If those three steps are not met, nothing will get done. We need to be able to limit these applications from the network side and stop leaving it up to the user!

Network Based Application Recognition (NBAR) is a function we can perform on Cisco routers which is used to identify applications at layers 4 through 7 of the OSI model. NBAR is a QoS (Quality of Service) tool that can be used to identify what application a packet is for. NBAR can tell if a packet is part of a P2P file transfer and then take some form of action such as marking it for later inspection (maybe to be rate limited – which is discussed later) or just drop the packet. NBAR has the ability to recognize both;

FastTrack applications (Kazaa for example)
Gnutella applications (Morpheus or LimeWire for example)

So what can we do once we have identified a packet is from a File Sharing Application?

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Well, a lot of things. We can drop it, send a packet to low priority queue (everything else goes out first) – or rate limit it. Rate limiting is basically limiting the amount of bandwidth an application or protocol can take up on an interface.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Below is an example of using NBAR on a router to drop all packets the router thinks are for P2P file transfers:

```
class-map match-any p2p
  match protocol kazaa2 file-transfer "*"
  match protocol fasttrack file-transfer "*"
  match protocol gnutella file-transfer "*"
policy-map stopp2p
  class p2p
   drop
!
interface FastEthernet0/0
 ip address 10.10.10.1 255.255.255.252
 ip nat inside
 service-policy input stopp2p
```

This is a very, very usefully tool. A very good description can be found on Cisco's website at the following URL: http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087cd0.html [25]

5.0 Conclusion

I would like to take this opportunity to note that the point of this paper is not to scare people away from using P2P networks. There are legitimate and valuable reasons to use them. The use of such applications is a personal choice for a home user and is the choice of policy makers on corporate networks. The word choice being the key word here - to make a wise choice the decision maker must be aware of his/her options as well as the pros and cons of each option. In this specific decision we must at least weigh the security risks with the rewards we will reap through the use of P2P file sharing networks and come to an informed decision. As with any decision we make in life, an informed decision is always better than a decision made with little or no information.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

6.0 Reference

[1] Neo-Napsters Proliferate in the Wake of Napster's Demise
http://www.broadbandweek.com/news/010820/010820_through_new.htm

[2] How File Sharing Works

http://computer.howstuffworks.com/file-sharing1.htm

[3] Neo-Napsters Proliferate in the Wake of Napster's Demise
http://www.broadbandweek.com/news/010820/010820_through_new.htm

[4] File Sharing Programs and Peer to Peer networks Privacy and Security Risks
http://reform.house.gov/UploadedFiles/P2P%20Security%20Report.pdf

[5] How a Gnutella client finds a song

http://computer.howstuffworks.com/file-sharing3.htm

[6] Download.com most popular list:
http://download.com.com/3101-2001-0-1.html?tag=dir

[7] File Sharing Programs and Peer to Peer networks Privacy and Security Risks
http://reform.house.gov/UploadedFiles/P2P%20Security%20Report.pdf

[8] http://www.spykiller.com/about.html

[9] Ad Ware definition
http://www.spywareguide.com/category_show.php?id=5

[10] Spy Ware in P2P applications
http://www.frixo.com/sites/adoko/p2p.html

[11] File Sharing Programs and Peer to Peer networks Privacy and Security Risks
http://reform.house.gov/UploadedFiles/P2P%20Security%20Report.pdf

[12] SANS GSEC Course book Section IV – Secure Communications page 1056

[13] SANS GSEC Course book Section IV – Secure Communications page 1057

[14] F-Secure Virus Descriptions : P2P worm

http://www.f-secure.com/v-descs/p2pworm.shtml

[15] What They Know Could Hurt You
http://www.wired.com/news/privacy/0,1848,49430,00.html

[16] Peer-to-peer traffic - friend or foe?
http://www.nwfusion.com/edge/columnists/2003/0707bleed.html

[17] Norton Antivirus
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=155

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

[18] MacAfee virusscan
http://us.mcafee.com/virusInfo/default.asp?cid=9043

[19] Trojan Defense Suite from DiamondCS
http://tds.diamondcs.com.au/

[20] Simovits Consulting - Ports used by Trojans

http://www.simovits.com/nyheter9902.html

[21] Security Focus Home User Security: Personal Firewalls

http://www.securityfocus.com/infocus/1750

[22] Special Application Port List

http://www.practicallynetworked.com/sharing/app_port_list.htm#Multimedia

[23] Kazaa Help - Sharing
http://www.kazaa.com/us/help/settings8

[24] Kazaa Help – Advanced
http://www.kazaa.com/us/help/guide_settings.htm#settings2

[25] Cisco systems - Network-Based Application Recognition
http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a0080087cd0.html

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Last Updated: May 27th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 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