Interested in learning more about security?

# SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

## Away from home. Securing Internet Cafes whie maximizing customer freedom

In the modern world where it is cheaper and easier than ever to stay in touch, the Internet cafe has become a shining oasis in a desert of unfamiliar sights and sounds for the modern traveler. At the same time students, gamers and traveling business people are also making use of the technology and high speed Internet access provided by Internet cafes. This essay is a real world example of steps taken by the author when hired to redesign and manage the IT aspects of 2 medium sized (100 user PCs in total) Internet cafes ...

Copyright SANS Institute

Author Retains Full Rights

AD

# Away from home. Securing Internet Cafés while maximizing customer freedom.

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4b

Option 2 - Case Study in
Information Security

Submitted by: Alex Tilley
Location: Local mentor program.
Brisbane, Australia

© SANS Institute 2005, Author retains full rights.

© SANS Institute 2005, Author retains full rights.

# Table of Contents

Abstract/Summary ..... 1
Network Design ..... 1
Original network design ..... 2
Chosen and implemented network design ..... 3
Things that could be done differently or improved upon. ..... 5
Private Information Protection. ..... 6
Original Privacy protection measures. ..... 6
Steps taken to protect customer privacy. ..... 6
Script based clearing of temp files and saved documents ..... 7
Things that could be done differently or improved upon. ..... 8
Imaging of Customer Workstations ..... 9
Original rebuild and repair process ..... 9
Implementation of an imaging process ..... 9
Things that could be done differently or improved upon. ..... 11
Anti-virus concerns and Implementation. ..... 13
Original Anti-Virus setup ..... 13
Implemented Anti-Virus setup ..... 13
Things that could be done differently or improved upon. ..... 15
Billing software and controlling physical access to workstations. ..... 16
Existing Billing System ..... 16
Implementation of a new Billing System to increase physical security ..... 17
Conclusion ..... 19
References and URL's ..... 20

# Table of Figures

Figure 1 Original Network Layout ..... 2
Figure 2 The chosen network layout ..... 4
Figure 3 Excel billing sheet ..... 16
Figure 4 Workstation's restricted application list ..... 17
Figure 5 Café Manager screen ..... 18

© SANS Institute 2005, Author retains full rights.

## Abstract/Summary

In the modern world where it is cheaper and easier than ever to stay in touch, the Internet café has become a shining oasis in a desert of unfamiliar sights and sounds for the modern traveler. At the same time students, gamers and traveling business people are also making use of the technology and high speed Internet access provided by Internet cafés.
This essay is a real world example of steps taken by the author when hired to redesign and manage the IT aspects of 2 medium sized (100 user PC's in total) Internet cafés in Europe in 2001.

Detailed will be, the main aspects of security that should be considered when running an Internet café focusing on providing customers with the most freedom possible, these aspects will be;

- The network design
- Private information protection
- The process of building and deploying ghost images
- Antivirus concerns and implementation
- Billing software and its role in increasing physical security

All sections will detail the original setup, steps taken to improve security, the reasons for those changes and a mention of how things could have been done better.

## Network Design

The basics of securing Local Area Networks (LAN's) and implementing security policies have been covered in many papers[1]. This paper will focus on the issues dealing specifically with Internet Cafés and minimizing access to personal information.

The design of a high usage network that provides maximum freedom and functionality for users in an anonymous environment is perhaps something that would make most network administrators quake with fear. One of the security principals that requires consideration is that in an Internet café, confidential data should not be stored on the workstations. Further, any information and systems critical to the business should be well protected by using standard security policies as outlined in several SANS papers[2].
With this understanding the number of devices needing to be secured rapidly diminishes to 2 or 3 computers per location, as well as a handful of network devices.



© SANS Institute 2005, Author retains full rights.

## *Original network design*

When the author was hired, the existing network layout of one café looked like the diagram below (Figure 1) (IP's have been changed)

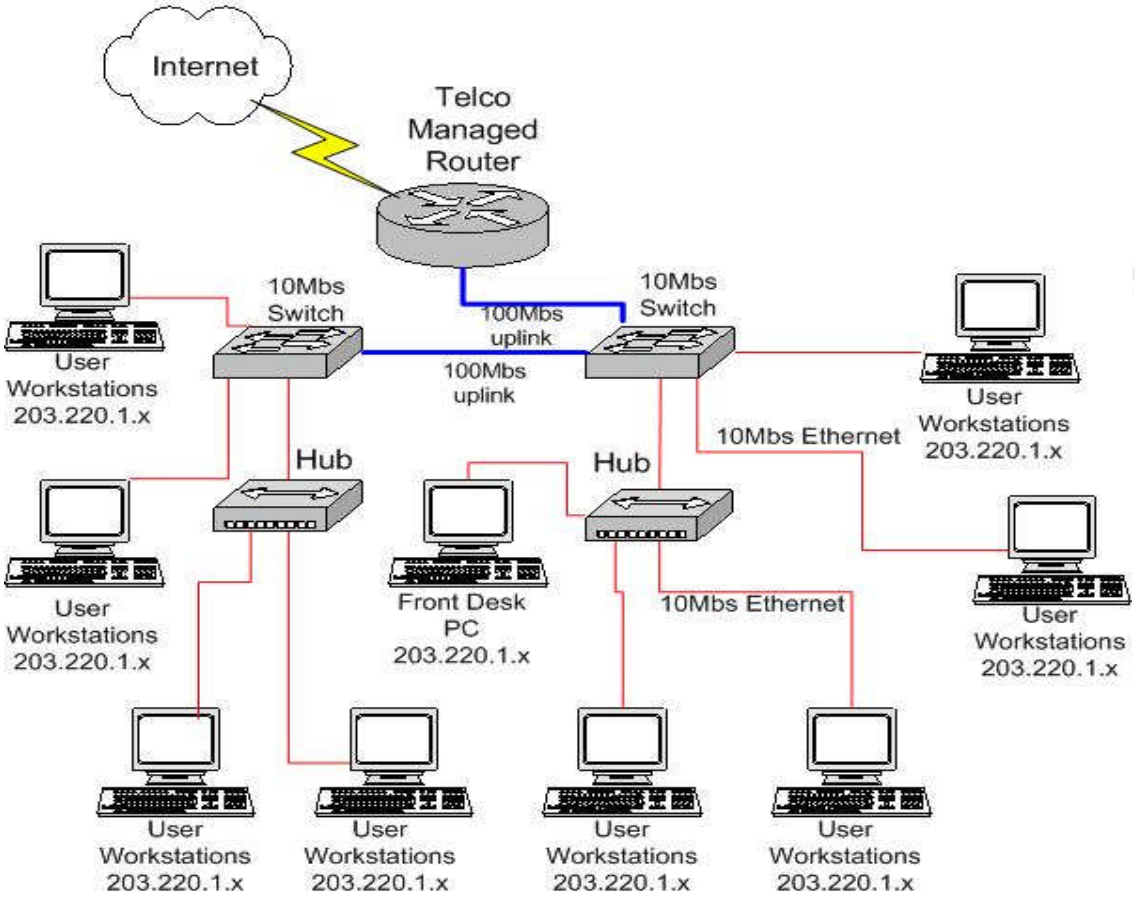


**Figure 1 Original Network Layout**

All workstations had a direct connection to the Internet with an Internet routed IP address. Network Address Translation (NAT) was not implemented. Also many machines were connected to hubs as the existing 10Mbs switches ran out of available ports.

There were no build images or imaging process with each machine being fixed as best as possible by staff, or if staff could not fix the problem, an onsite tech support company would be called to fix a single machine (a very costly process). Anti virus software was installed on the desktops but was found to have been deactivated on many machines, most having no scheduled signature updates at all. Billing was done by a spreadsheet with the customer's start time and end time being manually entered with a resulting cost being displayed as each



© SANS Institute 2005, Author retains full rights.

customer left. There was no clearing of “temp” directories or other personal data, with all manner of personal information being available for any user on that workstation at any time.

These factors, when combined, served to create an almost unworkable system. Approximately 20% of workstations were unavailable at any given time due to system crashes, lack of disk space and resource exhaustion. All workstations were slow to respond due to the amount of unnecessary applications running (including spyware, adware and other malware) and the extreme fragmentation of file systems. Billing was not accurate and amounted to little more than an “honor system”.
Further, security was non-existent with key loggers and other means of information thievery having unrestricted access to the personal information of hundreds of customers every day.

## Chosen and implemented network design

When all of these factors were identified and bought to the attention of management, along with the invoices for onsite technical support callouts, the administrator was basically given carte blanche to redesign the current café and also fit-out and build a new 50 seat Internet café that was to be located in close proximity to the original café. The cost of this project was a factor, with all purchases having to be justified to management. The network layout that was chosen for these particular Cafés is illustrated in Figure 2.

© SANS Institute 2005, Author retains full rights.



© SANS Institute 2005, Author retains full rights.

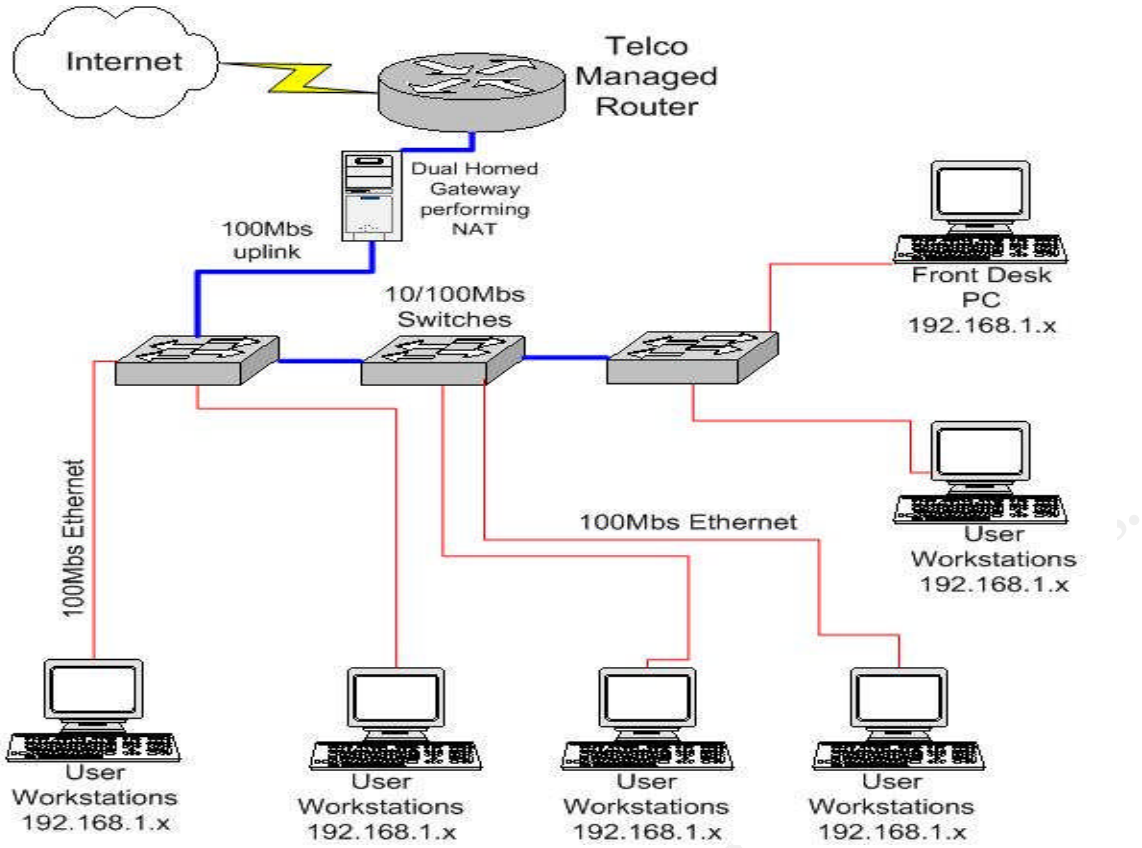


**Figure 2 The chosen network layout**

Evident in this layout is that there is a single entry/exit point to the Internet. There are only 2 computers that could possibly hold sensitive information and could be considered mission critical (the Front Desk/Billing PC and the Gateway Server).

New 10/100Mbs Switches were implemented which made for much faster imaging of workstations (covered in more detail in a following section) and also provided much more security as the original usage of hubs provided attackers with an easy means to sniff traffic on the network using free tools like *Ethereal* [3] and thus capture personal information from other customers.

All workstations were given static Bogon[4] (Non-Internet routable) Addresses (192.168.1.x) and were NAT'ed through the single Internet "gateway" server. This server was connected to the uplink port of one of the new 10/100mbs switches, it also had a second Network Interface Card (NIC) that was directly connected to the router this meant that the only method of getting to the Internet was through this gateway.

This new network layout was a marked improvement on the original design. The easier management and greater security were accompanied by the significant improvement in speed that meant that the networked games that were available were now much faster and more reliable. This resulted in a large increase in the number of gaming customers.



© SANS Institute 2005, Author retains full rights.

## Things that could be done differently or improved upon.

The network design that was employed is still mostly currently viable. One thing that could be done is to investigate the deployment of an Intrusion Detection or Prevention System (IDS/IPS) between the gateway and the Internet that does both INGRESS and EGRESS[5] filtering. This would help to mitigate the risks of attackers using the café to launch attacks on external parties. It should be noted however that due to the extraordinarily broad range of applications in use, base lining the IDS/IPS (getting the system to a point where it recognizes malicious traffic, gives minimal false positives and does not block legitimate traffic) could prove to be quite a challenge! Therefore the benefits when weighed against the amount of effort required to administer an IDS/IPS should be thoroughly understood before deploying such a system.

Deployment of a firewall between the gateway and the Internet is another option. In order to protect both internal clients and the Internet INGRESS and EGRESS filtering would be advantageous. However due to the wide range of applications (and therefore TCP ports and other protocols needed) in use means that usability would have to be weighed against security. All traffic except for TCP port 80 (HTTP) and 443 (HTTPS) traffic could be blocked both incoming and outgoing, this would give users basic web browsing which would be sufficient for many customers but much potential revenue would be lost when people realize that their own personal needs (telnet/ftp/terminal services etc.) will not be met and take their business elsewhere. Again the implementation of a firewall would have to be weighed against what freedoms you wish to give your customers.

Given the fact that the only single points of failure on the network are the Gateway server and front desk (billing) PC, a host-based firewall/IDS system such as Zone alarm or Tiny personal firewall[6] could be installed on these two systems. This will help protect these mission critical systems and will leave the customers with the freedom to do as they wish.

One other thing to consider would be a Caching Proxy for web and ftp traffic such as Microsoft's Internet Security and Acceleration (ISA) server[7].
This would have the benefits of cutting down download traffic and, through the use of the site blocking functions, known banner and pop-up ad sites could be blocked making for a better customer experience and therefore more repeat business.



© SANS Institute 2005, Author retains full rights.

# Private Information Protection.

## Original Privacy protection measures.

The café's policy was that no personal information should be stored on the workstations by customers. However this was not clearly communicated to customers. There was no means to remove personal data accidentally stored on these workstations. Coupled with the lack of any imaging procedure (rebuilding the workstations to a base build and thus wiping any information stored on the hard drive), this resulted in a staggering amount of personal letters, flight and hotel booking forms (including credit card numbers) and almost every other form of personal information conceivable being available to any user of any workstation at any time. It was accessible simply by browsing the hard drive or looking through the recently opened files list in applications like Microsoft Word. This situation was obviously unacceptable and was dealt with by using the various means that follow.

## Steps taken to protect customer privacy.

All workstations were clearly labeled indicating that the hard drives would be periodically wiped and that no personal information should be kept on them. If they needed to save data users were encouraged to send it to a webmail account for storage or floppy disks were available for purchase if they preferred.

> **N.B.** Some regular customers were given special dispensation to have their data (virus checked) stored on the gateway server, this data was then copied back to the particular workstation that these users were working on at the time, when they were done it was saved and copied back to the server. These were authors and students working on large documents that would not fit on a floppy or that were critical enough that it was agreed they would be stored locally in addition to a floppy disk or webmail as an added layer of redundancy. This was done out of kindness and also to keep the return business of these heavy use (5+ hours most days) customers.

Language barriers were an issue with this labeling as many users spoke little or no English. However as the majority of users who were responsible for storing data on the hard drives seemed to be English speaking students and business people, this did not turn out to be an issue.
These steps were deemed to be sufficient such that it could be argued that any personal information kept on the workstations is there at the user's own peril.



© SANS Institute 2005, Author retains full rights.

Nonetheless, steps were still taken to minimize the availability of any information to other users of these workstations. The best ways to accomplish this were found to be the script based clearing of the "*temp*", web browser cache and "*my documents*" folders and the periodic imaging of these workstations.

## Script based clearing of temp files and saved documents

All programs that allowed a change in their temp directory and/or default save-to directories were set in the base image to use *c:\temp* as temporary storage and *c:\saved* to save data. Internet Explorer was also set to use *c:\temp* as its local caching directory.
A simple dos batch script was written:

```
@echo off
Echo Clearing Temp Files
attrib -h -s -r c:\temp\* /S
attrib -h -s -r c:\saved\* /S
deltree /Y c:\temp\
deltree /Y c:\saved\
deltree /Y c:\windows\recent\
Echo All done
```

This script first sets the attributes of files within the specified directories to not be *hidden, system* or *read only,* ensuring that all files will be able to be deleted. It then runs the *Deltree* program which recursively deletes all files and folders stored below the start point. The "/Y" switch is to automatically answer "yes" to any prompts as the program would prompt for user intervention before deleting a directory.
The line dealing with the *C:\windows\recent* folder is to clear out any entries from the *"Start-> Documents"* menu. This stops people seeing shortcuts to the recent documents other users have opened.

A line calling this script was added to the *autoexec.bat* file so that whenever the machines were rebooted this cleanup would take place. Staff were encouraged to run this script on workstations that were running poorly. This was mostly an ad-hoc method of clearing personal data when the opportunity arose.

> **N.B.** This script is detailed here as an example of how simple methods can help protect the privacy of customers. It was written for the Windows 98 Operating system which was current at the time. Due to Operating system changes it does not work on the Windows XP Operating system. A variant written for Windows XP is detailed in the ***"****Things that could be done differently"* section below.



© SANS Institute 2005, Author retains full rights.

This script was by no means perfect. Many other file locations that may have contained personal information could have been added. However boot time was a consideration and this script did help in keeping the hard drives clear of some personal data and the old temp and cache files that tended to slow things down and fill up the hard drives.

## *Things that could be done differently or improved upon.*

The private information clearing script detailed previously still has much use as a basic brute force method of removing people's private data. It should be modified and upgraded as much as possible to reflect the locations that new operating systems (OS) and applications store their temporary data (if these locations cannot be set manually). There are many other commercially available tools that work within the OS and can clear a much larger range of personal data *"historykill"*[8] is one that has proven effective**,** although given the tight budgets most small businesses operate under perhaps a small Visual Basic (VB) script that operates within the OS itself as a scheduled task could be written if regular reboots will not be feasible.

The proliferation of spyware and adware coupled with the wide variety of uses customers have for Internet café workstations means that any customer workstation will be flooded with these applications on an hourly basis. Regular imaging is the best way to eradicate this menace from particular machines but where this is not possible one of the many spyware scanning and removing programs such as "*Adaware*"[9] could prove useful, however the free version is only free for personal use, therefore a large scale distribution could prove costly. An alternative can be found in the modern Antivirus systems. Many of the latest versions of desktop antivirus (that are covered in more detail below) incorporate spyware/adware detection as well as detecting and removing many keyloggers and other information thieving programs.

As mentioned previously below is a simple directory clearing script that can be run as a batch (.bat) file at boot time or when trouble shooting.

***XP temp clearing script***

```
@Echo Off
Echo Clearing Temp Files.
attrib -R -A -S -H /S /D c:\temp\*
attrib -R -A -S -H /S /D c:\saved\*
rmdir c:\saved /s /q
rmdir c:\temp /s /q
mkdir c:\saved
mkdir c:\temp
Echo all done
```



© SANS Institute 2005, Author retains full rights.

This script first sets the attributes of files within the specified directories to not be *hidden, system* or *read only,* ensuring that all files will be able to be deleted.
It then runs the "*rmdir"* program with the /Q (quiet) and /S (delete from all sub directories) switches set. This deletes these directories and all sub directories quickly and easily. The script then runs the "*mkdir"* program that re-creates the deleted directories *c:\saved* and *c:\temp*.

# Imaging of Customer Workstations

## Original rebuild and repair process

Initially there was no method of rebuilding workstations. As stated above, any workstation that was experiencing crashes, slow response times or that would not boot was simply marked as unavailable to customers. If staff could not diagnose or fix the problem an Onsite technical support company was called to fix the problem workstation.
This process resulted in significant costs and very poor uptime (about 20% of workstations were unavailable at any one time) but most important were the security aspects of this situation;

- The personal information saved intentionally or accidentally to the hard drives was freely available to all subsequent users for months.

- Keyloggers and other Malware (programs written with malicious intent) were identified as running on a number of workstations with logs of all keystrokes made on the workstations affected being stored for months. These logs were stored in clear-text (unencrypted) this meant that normal customers as well as unscrupulous persons had access to the credit card numbers, User Id's and passwords of many customers for an extended period of time.

## Implementation of an imaging process

It was decided that imaging the workstations was the best way to maximize workstation uptime and, most importantly, imaging was the best way to remove all possible personal data and minimize the window of time for Keyloggers and Malware to be actively gathering confidential information.

Imaging is the process of creating a single large file (called the Image) that contains the complete file structure of a hard drive, and then overwriting the existing hard drive of the target workstation with this image, thus creating exact


© SANS Institute 2005, Author retains full rights.

clones of the clean image and wiping any data on the target hard drive. This Imaging was done via Symantec's Norton Ghost program[10],

The Images were built as follows;

- The operating system and all available security and system patches/updates were installed onto a freshly formatted hard drive.
- All unnecessary system components were removed.
- Antivirus software was installed and updated with the latest Signatures and system (scan engine) upgrades
- The latest versions of all applications used by customers were loaded and tested for functionality (a time consuming process).
- The "*msconfig.exe"* tool was run and anything other than necessary system and antivirus processes were disabled from running on system startup, making for a quicker (re)boot time.
- The workstation was rebooted and then given a complete virus and "*Adaware*" scan to remove any spyware or adware that may have been installed.
- The workstation was rebooted with an image disk, and a full image of the partition was taken and stored on the "Gateway" image server

Two separate Ghost images were created using the above method; these images were constantly being updated as new security patches and software versions were released. Two separate images were needed as hard drive space was limited and these workstations were also used to play a large variety of LAN games. Therefore, a separate image was created that contained none of the international language tools (Japanese/Korean language converters and chat programs etc.) or work related tools (Microsoft Office etc.), yet contained all the latest games and patches.

The workstations were imaged on an ad-hoc basis i.e. If they were to malfunction severely enough that to fix the problem would take more than the approximate 10 minutes that it would take to image the machine. The images were stored on the "gateway", the ghost server program was running constantly so that all a staff member had to do to image a workstation was to reboot the workstation with the build disk in the drive and it would automatically load the image over the network.

Once per week at night after the Café had closed, all of the workstations were imaged. For this weekly imaging, the server would be switched to multicast mode and told to wait for 5 connections before sending the image, after 5 workstations were rebooted from the ghost boot disks the image would be sent out to all 5 simultaneously. Once the 5 had finished receiving the image (roughly 10 minutes) the next 5 workstations would be done and so forth. It was a time


© SANS Institute 2005, Author retains full rights.

consuming process taking approximately 6 hours to completely image all 100 workstations across the two Cafés (50 workstations per Café).

Some of the larger Cafés use a process that automatically images their workstations as soon as the customer ends his or her session. This would not have worked in the cafés in question as the extremely high customer turnover meant that it was not feasible to have the workstations constantly down for even 5 minutes at a time as customers came and went.

Availability (having the workstations available to paying customers) was balanced with security (removal of personal data and narrowing the window of time for malware to gather information) and the coupling of ad-hoc imaging with the once per week scheduled imaging was decided to be the best (and most realistic) combination.

## Things that could be done differently or improved upon.

There have been many advances in the field of deploying an SOE and mass imaging of workstations. The use of floppy disks to boot workstations so they connect to an Image server has been surpassed by the use of a client server arrangement. As stated above, Symantec's Ghost Corporate[11] program now supports "diskless imaging" where many workstations can be rebuilt from a controlling console at once without the need to manually insert a floppy disk and select the image for each individual workstation.

With the implementation of this technology all workstations could be imaged often (daily, 12 hourly or indeed at any interval required) in a small amount of time to give customers fresh clean environments to work from at every visit.

It cannot be stressed enough that the proper use of this technology is the administrator's best defense against the use of workstations as *"Zombies"* for DDOS attack and as SPAM relays.

A Zombie computer is defined as "A computer that has been implanted with a daemon that puts it under the control of a malicious hacker without the knowledge of the computer owner"[12]. (Webopedia)

The proper use of this technology is also the greatest and most cost effective tool available to effectively remove the threat posed by personal information left on hard drives. It also stops other information thievery by rendering the window of time that a keylogger could gather information and store it for retrieval by an unscrupulous party so small as to make it a much less attractive prospect.

No matter what Imaging tool is used, the more often workstations can be imaged the less security and functionality headaches the administrator will face.



© SANS Institute 2005, Author retains full rights.

If possible all workstations should be imaged between customers. This is not always practical and a schedule should be worked out based on the needs of each particular café.

© SANS Institute 2005, Author retains full rights.



© SANS Institute 2005, Author retains full rights.

# Anti-virus concerns and Implementation.

## Original Anti-Virus setup

Viruses and worms are constantly bombarding workstations at Internet Cafés. Their very nature enables this (people use Internet Cafés to check webmail, transfer files and visit favorite websites).

The original anti-virus setup was close to useless. Desktop anti-virus was supposed to be installed on all workstations but the reality was that many workstations did not have any anti-virus installed or running. The anti-virus software that was installed on workstations was severely crippled. It had out of date signature files, had many aspects of the scanning disabled (mostly it would seem by customers) or was set to take no action on detecting an infected file. All of the options within the anti-virus software were available to customers to change or disable at their will. This coupled with the fact that all workstations were on fully published IP addresses and many were infected with Trojans that made them act as "*zombies*" for Distributed Denial of service attacks or as SPAM relays, meant that these 100 workstations were as much a threat to the Internet at large as they were to the Cafés internal network.

## Implemented Anti-Virus setup

The defense against viruses that was implemented was not perfect (especially not when compared with tools available today) but it was functional and helped to avoid too many major outbreaks of viruses or worms.
Aspects of Anti-viral protection that were investigated and/or implemented were:

- **User education**
  User education is normally the first level of protection against virus and worm attacks, in an Internet café environment effective user education is close to an impossibility. This is because due to the nature of Internet Cafés (in Europe especially), a large portion of customers speak little or no English.
  An attempt at user education was made by affixing small labels to the monitors that displayed the icons commonly used by webmail sites to signify that an attachment is infected with malware and a message stating that if an attachment had these icons please do not click on it.
  This was quickly abandoned as next to useless because of the language barriers.


© SANS Institute 2005, Author retains full rights.

- **Desktop Antivirus**
  Norton Antivirus was installed on the base image and therefore on all workstations. This was setup with as stringent a policy as possible; all files were scanned on any action (copy/open/create/run etc.) A consideration with this policy was that it possibly made for very high system overheads. These concerns were balanced with the need to protect the network and maintain as high an uptime as possible for all workstations.
  After implementation of the strict virus scanning policy it was noticed that concerns about system overheads were for the most part unfounded as the workstations were mostly used for web browsing and word processing, neither of which activities are commonly very resource intensive.

  As network games (which are resource intensive) were also available the scanning settings were loosened on this image to provide for the best system performance for games while still giving protection against any downloaded patches or upgrades for these games.

  The Anti-virus software's control panel was password protected thereby removing the ability of customers to change scanning settings.
  If a virus was detected on a workstation the policy was to delete by default. This policy of quiet deletion without notification did cause some confusion but the majority of users who downloaded an attachment that then disappeared would attempt it again and on the second attempt the "infected" icon displayed next to the webmail's attachment would make more sense. Those customers who did not download viruses via webmail and who were confused about what was happening to their files would attract a member of staff's attention who would quickly explain the situation.

  This policy of deletion without notification worked well because as well as minimizing the need for staff intervention, it also removed the option for the customer to "do nothing" with an infected file which inevitably led to a virus riddled workstation.
  Also scanned and quietly deleted/stopped from running was malicious Internet content (ActiveX and Java script) because a large amount of web based Java script and ActiveX malware is circulating, to have the user get a warning every time a malicious Java script or ActiveX component was detected and deleted/terminated would have seriously impeded the experience of the customers.

  If deletion was unsuccessful the anti-virus software was setup to blue screen the PC with a message that a virus was found and to contact a member of staff.
  This method breached the language barrier because as the machine became useless while blue screened the customer would have no choice but to see a member of staff who would then take appropriate action (Most


© SANS Institute 2005, Author retains full rights.

often moving the user to a different workstation and immediately imaging the infected workstation).

- **Anti Virus Signature Updates.**
  As stated the heavy and constant use of webmail, file transfers and “odd” website browsing created a situation where the antivirus software critically needed to be kept up to date. The adopted policy was that the desktop anti-virus would check for new signature updates every 6 hours. Due to the lack of centralized management this meant that every workstation would go out to the Internet to seek updates, significant network overheads were expected but due to the speed of the link and the relative small size of antivirus signature updates no real speed issues were ever noticed.

As stated previously this implementation was by no measure perfect.
It was functional and did its job well, however with more up to date software many things could be done to make for better defense in depth in regards to Anti-Virus technology.

## Things that could be done differently or improved upon.

The advances in desktop antiviral solutions have been huge. A single application running on the desktop can now detect and remove not only viruses but Spyware, Keyloggers, malicious/dangerous ActiveX and Java script content and much more (the Norton anti-virus and Mcafee anti-virus packages are two examples).
The scanning Policy that is set should be as stringent as possible, passwords should be used to negate the possibility of customers disabling or altering Anti-viral software.

The use of a nominated server on the LAN (for instance the Internet gateway) that all desktops connect to to get the latest antivirus updates also has been made easier making for greater control and cutting the amount of bandwidth used and downloaded amounts down to a fraction of what it could be with all workstations going directly to the Internet to retrieve updates.
Signatures should be updated at least every 6 hours to give good protection. With the use of a gateway server these updates could even be pushed to the workstations as they become available at an even smaller interval (perhaps ever hourly).

Antivirus is one item on which costs should not be cut. The implementation of a modern antivirus product such as Norton, Mcafee or Trend[13] has many benefits; reduced downtime, reduced administration time (cost) and better privacy protection are just a few.


© SANS Institute 2005, Author retains full rights.

The Implementation of a gateway style virus scanning is also a possibility when coupled with a caching proxy gateway.
A solution such as Trend's "*Interscan WebProtect 3.1 for ISA*"[14] will add an extra defensive layer by stopping viruses and worms before they get to the desktop

# Billing software and controlling physical access to workstations.

## Existing Billing System

As mentioned in the network design section above, the original billing system was by means of a spreadsheet.
All workstations were numbered (PC01 – PC50) when a customer arrived staff would direct him or her to an available workstation and enter the start time in the Cell for that PC. On departure the customer quoted this workstation number, the end time was entered into the next cell on the spreadsheet and a formulae would then (rounded to the nearest half hour) determine the amount of money owed.
A Sample of this is below in Figure 3

| Workstation | Start Time | End Time | Cost |
|---|---|---|---|
| PC01 | 13:00 | 13:30 | € 3 |
| PC02 | 13:10 | 13:50 | € 3 |
| PC03 | 11:16 | still in use | n/a |
| PC04 | 12:00 | 13:30 | € 9 |
| PC05 | 12:03 | 13:45 | € 9 |
| PC06 | 12:40 | 13:00 | € 3 |

**Figure 3 Excel billing sheet**

The three major problems with this system were:

- The badly maintained state of the workstations meant that many would not work at all or would crash as a customer was using them. This often resulted in the customer moving to another workstation to continue working without notifying staff; this made it almost impossible to keep an accurate record of who was where and for how long.

- The fact that unused workstations were not screen locked in any way made it very easy for people to come in at busy times, use a workstation without notifying staff and then when they came to pay dispute the bill or; as no accurate arrival time was recorded (staff would set the start time as being whenever they noticed someone sitting at that workstation), the customer would end up being charged far less than they should have.


© SANS Institute 2005, Author retains full rights.

- There was no logging or historical record to compare with the cash register receipts, therefore there was no way for management to see how much use workstations got or daily takings from computers alone (Coffee and snacks were also available).

## Implementation of a new Billing System to increase physical security

A new billing system was needed to address the above issues and in doing so increase the physical security of workstations.
Many different billing systems were trialed however only one addressed all these issues. It was Lappasoft's "Internet Café Administrator"[15] this system is a client server type arrangement. It worked as follows:
A small client is installed on the workstation that runs on startup. This client is set to connect back to the server (the front desk PC) and then lock the workstation displaying whatever graphic or document you would like until it was unlocked for use by a member of staff from the front desk server console.

This Client also had the ability to restrict what the customer could do by disabling access to the task manager etc. Also it had the ability to display only a selected few icons and thus stop the user from having full functionality on the workstation. Figure 4 below[16] (Sourced from www.lappasoft.com) illustrates this.

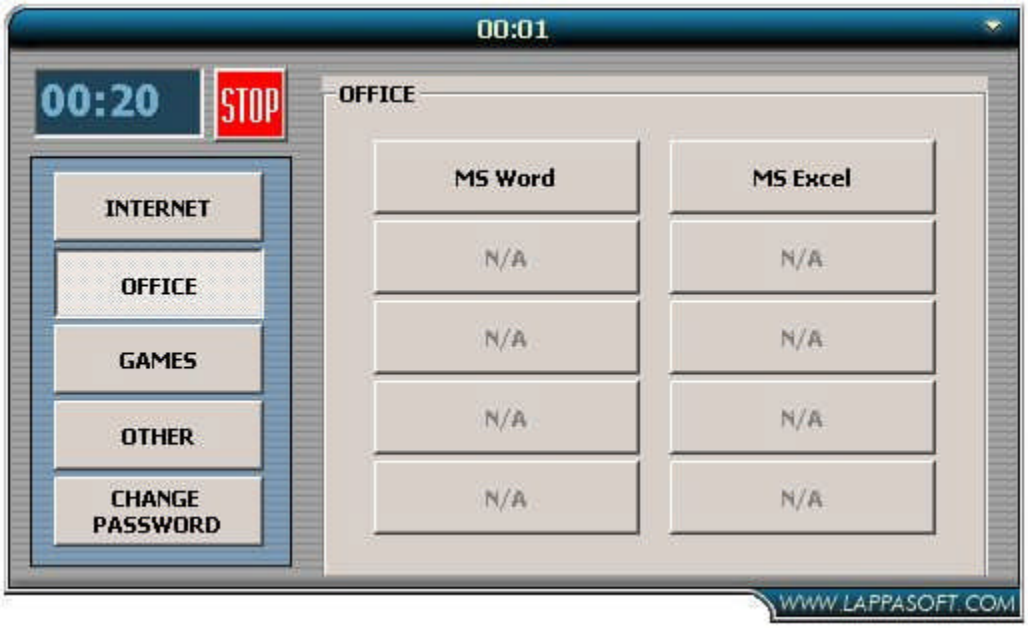


**Figure 4 Workstation's restricted application list**

These options were investigated and access to the task manager was disabled. But it was decided that we would leave the workstations with fully functional


© SANS Institute 2005, Author retains full rights.

desktops as this freedom was the reason why many customers kept using our Cafés.

The server display shows an Icon for each workstation arranged to resemble the actual physical location of each workstation with a colour coding system showing the status of the workstation. The colour codes were:
Multi-coloured(rainbow): Workstation in use
Blue: Workstation available
Black: Workstation not responding (rebooting, shutdown or crashed).
The administration screen is displayed below (Figure 5) (Sourced from www.lappasoft.com) [16]

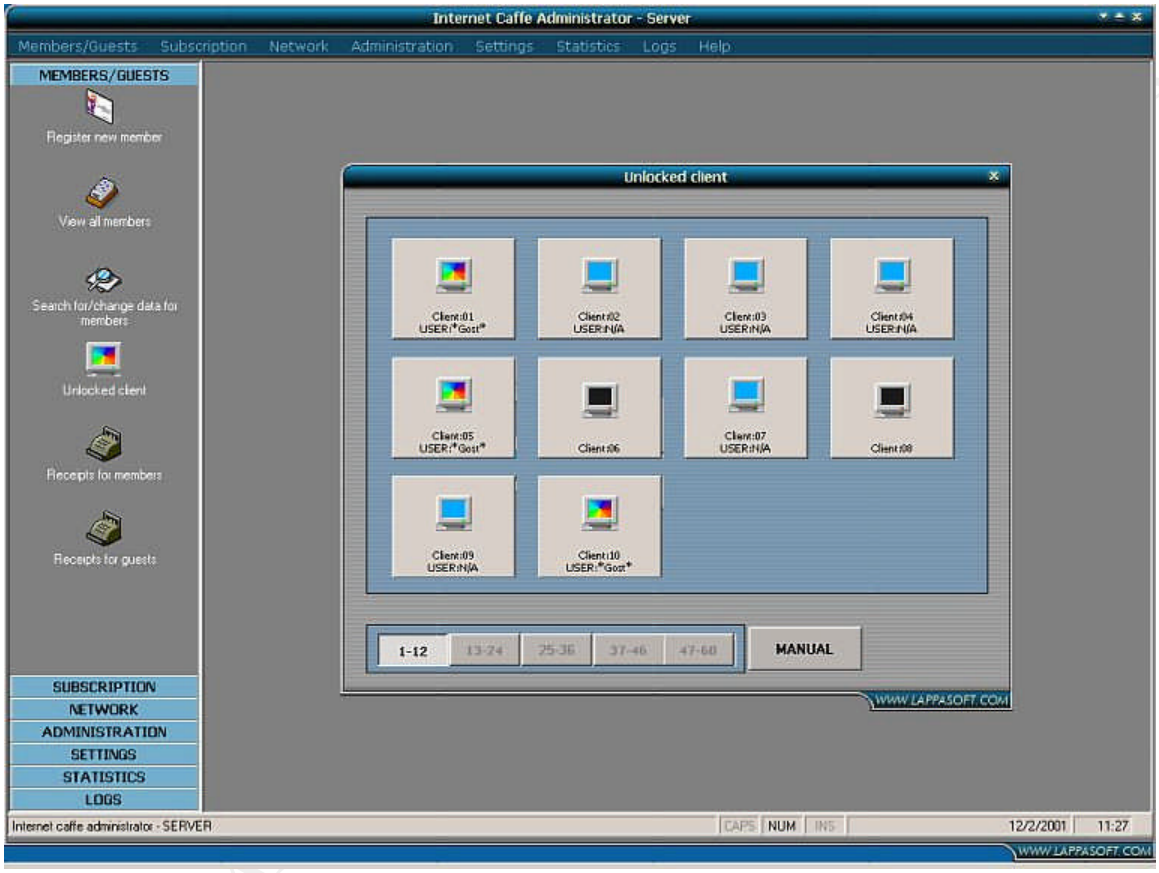


**Figure 5 Café Manager screen**

When a customer came in staff could see at a glance which workstations were available, direct the customer to that workstation and then unlock the workstation to allow for use.
When the customer came to pay, the workstation would be locked and the exact time of use and amount to be paid were displayed.
If a workstation was not unlocked from the console by staff or by entering in an administration password at the workstation, the desktop was unavailable and the


© SANS Institute 2005, Author retains full rights.

workstation was useless. This helped stop customers using workstations without notifying staff.

From the console staff could also reboot and shutdown the workstations (individually or many at once). Staff could also bring up the task manager for the selected workstations and shutdown the client software if the workstation needed maintenance.
This system also had good reporting functionality, with exact time, date and cost breakdowns available as well as historical data.

Billing software is mentioned in this essay as it provides for better physical security of workstations; it provides staff with much more control over the use of workstations, it provides management with better reporting and it also provides an easy way to do mass reboots (which had the benefit of fixing many problems immediately as the workstations were running Windows 98 and many common problems with Windows 98 could be fixed by rebooting).
Rebooting the workstations meant that the personal information temp and cache clearing script ran. Staff were encouraged to reboot workstations a few times a day as it took no effort and had many positive effects.

The Billing system described above is by no means the only system available it was simply the system that best addressed the security issues identified.

## Conclusion

It is hoped that from this paper the reader will come away with an understanding of the few simple steps that can be taken by an administrator at an Internet Café to protect the personal information of customers while leaving them with the freedom to use the time they have paid for on the Internet as they choose.

This paper was not meant as the be all and end all manual to running an Internet café's IT. Rather as the author's methods of keeping workstations available, protecting customers and reducing the workload on staff.

The access that a modern Internet café offers its customers can be as restricted as the administrator wishes it to be. The methods presented here have been geared at allowing the customer the freedom to do whatever he or she wishes with the time they are paying for while protecting their personal information as completely as possible.
If people are comfortable and do not feel restricted, they will stay longer and come back again.
Internet Cafés should be an enjoyable, hassle free and safe place for customers and staff alike.



© SANS Institute 2005, Author retains full rights.

## References and URL's


[1] Some Papers of Note Include:

Ford, Douglas. 8 Simple Rules For Securing Your Internal Network.
November 6, 2003
URL: http://www.sans.org/rr/papers/index.php?id=1254

Oxenhandler, Daniel. Designing a Secure Local Area Network
January 30, 2003
URL:http://www.sans.org/rr/papers/index.php?id=853

[2] Setty, Harish. System Administrator - Security Best Practices
August 16, 2001
URL: http://www.sans.org/rr/papers/index.php?id=657

Microsoft. Windows 2000 Server Baseline Security Checklist
URL: http://www.microsoft.com/technet/security/chklist/w2ksvrcl.mspx

Microsoft. Threats and Countermeasures Guide. April 23, 2003
URL: http://www.microsoft.com/technet/security/topics/hardsys/tcg/tcgch00.mspx

[3] Ethereal is available free to download from
URL: http://www.ethereal.com

[4] Bogon addresses. RFC 1918
URL: http://www.faqs.org/rfcs/rfc1918.html

[5] Carter, Jeff. Egress Filtering v 0.2. February 29 2000
URL: http://www.sans.org/y2k/egress.htm

[6] Zone Alarm personal firewall.
URL: http://www.zonelabs.com
Tiny firewall.
URL: http://www.tinysoftware.com

[7] Internet Security and Acceleration server home page. August 09, 2004
URL: http://www.microsoft.com/isaserver/

[8] HistoryKill
URL: http://www.historykill.com/

[9] Adaware
URL: http://www.lavasoftusa.com

[10] Norton Ghost 2003
URL: http://www.symantec.com/sabu/ghost/ghost_personal/




© SANS Institute 2005, Author retains full rights.

[11] Symantec Ghost Corporate Edition
URL: http://sea.symantec.com/content/product.cfm?productid=9

[12] Webopedia. "zombie definition"
URL: http://isp.webopedia.com/TERM/Z/zombie.html

[13] Anti-virus URL's
Symantec (Norton Antivirus.)
URL: http://www.symantec.com/smallbiz/nav/
Mcafee Antivirus
URL: http://www.mcafee.com/
Trend Antivirus
URL: http://www.trendmicro.com

[14] Interscan WebProtect for ISA
Trend Antivirus
URL: http://www.trendmicro.com/en/products/gateway/iswp-isa/evaluate/overview.htm

[15] Internet Café Administrator version 2.0
URL: http://www.lappasoft.com/

[16] Figures sourced from Lappasoft
URL: www.lappasoft.com

© SANS Institute 2005, Author retains full rights.



© SANS Institute 2005, Author retains full rights.

Last Updated: September 3rd, 2015

# Upcoming SANS Training

**Click Here for a full list of all Upcoming SANS Events by Location**

| | | | |
|---|---|---|---|
| SANS Crystal City 2015 | Crystal City, VAUS | Sep 08, 2015 - Sep 13, 2015 | Live Event |
| SANS Network Security 2015 | Las Vegas, NVUS | Sep 12, 2015 - Sep 21, 2015 | Live Event |
| SANS Seoul 2015 | Seoul, KR | Sep 14, 2015 - Sep 19, 2015 | Live Event |
| Data Breach Investigation Summit & Training | Dallas, TXUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Baltimore 2015 | Baltimore, MDUS | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Perth 2015 | Perth, AU | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS Tallinn 2015 | Tallinn, EE | Sep 21, 2015 - Sep 26, 2015 | Live Event |
| SANS ICS Amsterdam 2015 | Amsterdam, NL | Sep 22, 2015 - Sep 28, 2015 | Live Event |
| SANS Bangalore 2015 | Bangalore, IN | Sep 28, 2015 - Oct 17, 2015 | Live Event |
| SANS DFIR Prague 2015 | Prague, CZ | Oct 05, 2015 - Oct 17, 2015 | Live Event |
| SANS Seattle 2015 | Seattle, WAUS | Oct 05, 2015 - Oct 10, 2015 | Live Event |
| SANS Tysons Corner 2015 | Tysons Corner, VAUS | Oct 12, 2015 - Oct 17, 2015 | Live Event |
| SOS: SANS October Singapore 2015 | Singapore, SG | Oct 12, 2015 - Oct 24, 2015 | Live Event |
| SANS Gulf Region 2015 | Dubai, AE | Oct 17, 2015 - Oct 29, 2015 | Live Event |
| SANS Cyber Defense San Diego 2015 | San Diego, CAUS | Oct 19, 2015 - Oct 24, 2015 | Live Event |
| SANS Tokyo Autumn 2015 | Tokyo, JP | Oct 19, 2015 - Oct 31, 2015 | Live Event |
| SANS South Florida 2015 | Fort Lauderdale, FLUS | Nov 09, 2015 - Nov 14, 2015 | Live Event |
| SANS Sydney 2015 | Sydney, AU | Nov 09, 2015 - Nov 21, 2015 | Live Event |
| SANS London 2015 | London, GB | Nov 14, 2015 - Nov 23, 2015 | Live Event |
| Pen Test Hackfest Summit & Training | Alexandria, VAUS | Nov 16, 2015 - Nov 23, 2015 | Live Event |
| SANS Hyderabad 2015 | Hyderabad, IN | Nov 24, 2015 - Dec 04, 2015 | Live Event |
| SANS Cape Town 2015 | Cape Town, ZA | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| SANS San Francisco 2015 | San Francisco, CAUS | Nov 30, 2015 - Dec 05, 2015 | Live Event |
| SANS Milan 2015 | OnlineIT | Sep 07, 2015 - Sep 12, 2015 | Live Event |
| SANS OnDemand | Books & MP3s OnlyUS | Anytime | Self Paced |