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.

# Defence in Depth on the Home Front

The home Internet user is a target for intruders. The key question facing home Internet users is how they can securely access the Internet without sacrificing the required level of usability. After all if the security measures are too severe then use of the Internet will be very frustrating and either the Internet will not be accessed or more likely, the security measures will be circumvented or ignored to increase usability. This paper sets out a defense in depth approach to meet the security needs of the Windows-base...

Copyright SANS Institute
Author Retains Full Rights

AD
Symantec™
Endpoint Protection 12
The next generation of reputation-based security
Download the beta
Symantec.
Confidence in a connected world.

# Defence in Depth on the Home Front

GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b - Option 1
Thomas Harbour
April 3, 2003

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

1. Abstract ..... 1
2. Introduction ..... 1
2.1 Are Intruders Targeting the Home User? ..... 1
2.2 Principles of Information Security applied to the Home User ..... 3
2.3 The Defence in Depth Approach for the Home User ..... 4
3. Implementing the Recommended Defensive Actions ..... 6
3.1 Implementing the Network Access Layer Defensive Measures ..... 6
3.1.1 Use a firewall ..... 6
3.1.2 Disconnect from the Internet when not using it ..... 7
3.2 Implementing the Operating System Layer Defensive Measures ..... 7
3.2.1 Use a robust operating system ..... 7
3.2.2 Keep up with patch releases ..... 8
3.2.3 Make a boot/ERD disk and keep it current ..... 9
3.2.4 Use and keep up to date anti-virus software ..... 9
3.2.5 Harden the OS by turning off unnecessary clients, services and features ..... 9
3.3 Implementing the User Application Layer Defensive Measures ..... 10
3.3.1 Keep up with patch releases ..... 10
3.3.2 Do not install programs of unknown origin ..... 11
3.3.3 Disable Java, JavaScript, and ActiveX when possible ..... 11
3.3.4 Disable scripting features in e-mail programs when possible ..... 11
3.4 Implementing the Data Layer Defensive Measures ..... 11
3.4.1 Regular backups of critical data ..... 11
3.4.2 Use encryption to ensure confidentiality of sensitive data ..... 12
3.4.3 Use Strong Passwords ..... 13
3.4.4 Open E-mail Attachments with Care ..... 13
4. Comparing Three Readily Available Personal Firewalls ..... 14
4.1 Windows 2000 - Using IP Security filters as a Static Packet Filter ..... 15
4.1.1 Using a Static Packet Filter as a Firewall ..... 15
4.1.2 Overview of IP Security Filters ..... 16
4.1.3 Implementation of a Simple Firewall using IP Security filters ..... 17
4.1.4 Conclusions about this Firewall ..... 21
4.2 Windows XP Pro – Using Internet Connection Firewall (ICF) ..... 22
4.2.1 Overview of ICF ..... 22
4.2.2 Implementation of ICF ..... 23
4.2.3 Programs can change the ICF Ruleset ..... 23
4.2.4 Conclusions about this Firewall ..... 24
4.3 Windows - Using ZoneAlarm Personal Firewall ..... 25
4.3.1 Overview of ZoneAlarm ..... 25
4.3.2 Conclusions about this Firewall ..... 25
4.4 Vulnerability of Testing of the Firewalls ..... 25
5. Conclusion ..... 28
Annex A – Connections and Listening Ports ..... 29
Annex B – Highlights of Nessus Report with no Firewall/Filtering ..... 30


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Annex C – Microsoft Recommended Updates for Microsoft Windows XP Pro . 31
References ..... 32

List of Figures

Figure 1. Most common Intruder methods used against home computers ..... 4
Figure 2. Protecting the Internet-connected Home PC ..... 15
Figure 3. A Static packet filter firewall and the OSI Model ..... 15
Figure 4. Defining a Firewall Policy using IP Security filters ..... 18
Figure 5. New Rule Properties window ..... 19
Figure 6. IP Filter List window ..... 19
Figure 7. Protocol tab of the IP Filter List window ..... 20
Figure 8. Filter Action tab of the IP Filter List window ..... 20
Figure 9. Revised Firewall Policy ..... 21

List of Tables

Table 1. Summary of intrusion attempts from ZoneAlarm log files ..... 2
Table 2. Defence in Depth – Defensive Actions at each layer ..... 6
Table 3. Results of testing the Firewalls ..... 27
Table 4. Microsoft Recommended Updates for Microsoft Windows XP Pro ..... 31

© SANS Institute 2003, Author retains full rights.



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

## 1. Abstract

The home Internet user is a target for intruders. The key question facing home Internet users is how they can securely access the Internet without sacrificing the required level of usability. After all if the security measures are too severe then use of the Internet will be very frustrating and either the Internet will not be accessed or more likely, the security measures will be circumvented or ignored to increase usability.

This paper sets out a defence in depth approach to meet the security needs of the Windows-based home Internet user while maintaining usability. The four layers of defence identified and discussed are: network access; the operating system; user applications; and data. The most important layer of the defended area is the user's data, while the most neglected component is the personal firewall that operates at the network access layer.

## 2. Introduction

This section examines the threat posed to the home Internet user by intruders; how the recognized principles of information security apply to the home user; and how the defence in depth approach applies to the home user. This sets the stage for an examination of the exact steps that home user should take to reduce the vulnerability to intruders.

### 2.1 Are Intruders Targeting the Home User?

Home users are an important constituent of Internet users and their numbers continue to grow. In fact IDC Research predicts that the volume of Internet traffic generated by end users worldwide will nearly double annually over the next five years. By 2007, IDC estimates that consumers will account for 60 percent of all Internet traffic generated, versus roughly 40 percent for business users[1].

Given the importance of home usage of the Internet, the next question is whether this segment's usage of the Internet makes it an attractive target for intruders. In other words, how attractive are home users compared to traditional targets of businesses and government organizations and their users. Interestingly it turns out that in Canada in 1998, about 32% of regular home users communicated by computer from home for an employer-related purpose while 23% did so for self-employment purposes[2].

Hence it is reasonable to conclude that many home users, who are using their computers for work-related purposes, have information on their computers that comes directly from their employer. This information in some cases could be very valuable and is generally afforded lower level of protection than the same


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

information at work where firewalls, IDS and other network security devices, and knowledgeable security personnel are likely to be operational.

The case of the ex-CIA chief who was surfing the Internet using his AOL account on a home computer with top-secret data[3] serves to illustrate the danger that an individual exposes both himself and his organization to when basic security awareness is lacking.

During the preparation of this paper, a Windows 2000 computer running ZoneAlarm v3.7.098 was left connected to Internet in an "always-on" mode using a cable modem connection. Table 1 summarizes the ZoneAlarm log file entries of intrusion attempts during the 6 day period. All of the TCP connection attempts were reported in the logs as having the syn flag set and were classified as being type FWIN, i.e. the firewall blocked the inbound packets.

| Destination Port | Number of Attempts | Number of Unique Source Addresses | Role of Well-known Port |
|---|---|---|---|
| TCP/20 | 2 | 1 | FTP data |
| TCP/21 | 1 | 1 | FTP control |
| TCP/23 | 2 | 1 | telnet |
| TCP/25 | 2 | 1 | smtp |
| TCP/79 | 2 | 1 | finger |
| TCP/80 | 83 | 29 | HTTP |
| TCP/110 | 2 | 1 | POP3 |
| TCP/113 | 2 | 1 | ident/auth |
| TCP/135 | 3 | 2 | epmap |
| UDP/135 | 10 | 6 | epmap |
| TCP/143 | 2 | 1 | IMAP |
| TCP/443 | 7 | 5 | HTTPS |
| TCP/445 | 62 | 53 | Microsoft-DS |
| TCP/1399 | 1 | 1 | cadkey-licman |
| TCP/1433 | 7 | 7 | Microsoft SQL Server |
| TCP/4899 | 1 | 1 | RAdmin Port |
| TCP/5000 | 1 | 1 | commplex-main |
| TCP/6346 | 1 | 1 | gnutella-svc |
| TCP/6886 | 15 | 8 | Unassigned |
| TCP/17300 | 2 | 2 | Unassigned |
| TCP/26593 | 1 | 1 | Unassigned |
| TCP/27347 | 1 | 1 | Unassigned |
| TCP/27374 | 8 | 4 | Unassigned |
| ICMP | 3 | 3 | Echo (type:8/subtype:0) |

Table 1. Summary of intrusion attempts from ZoneAlarm log files


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The most popular port that connection attempts were made against was http (tcp/80). The second most popular was tcp/445, which is the port used by Windows 2000 hosts for SMB over TCP/IP. Some of the more interesting ports that connection attempts were made to include those associated with well-known Trojan horses[7] and role-playing games:

- TCP/5000 – Back Door Setup, Blazer5, Bubbel, ICKiller, Sockets des Troie (also the port listened to by UPnP on Windows XP).
- TCP/6886 – CrystalMush (a role-playing game based on the Crystal Singer series by Anne McCaffrey).
- TCP/17300 – Kuang2 the virus.
- TCP/27347 – Perhaps a dyslexic intruder looking for the normal SubSeven port.
- TCP/27374 – SubSeven v2.x.

There were attempts to connect to UDP/135. This traffic may be UDP broadcast traffic used by the Windows 2000/XP Messenger service to send an advertisement. The Messenger service uses UDP ports 135, 137, and 138; and TCP ports 135, 139, and 445[9].

Most of the source IP addresses only attempted one connection which perhaps indicates that they were scanning the ISP's block of IP addresses. However, there was one source IP address that repeatedly tried to connect to port tcp/80 on a daily basis. In fact this address accounted for 35% of the 83 connection attempts against tcp/80. This source IP address is in the local ISP's block of IP addresses.

## 2.2 Principles of Information Security applied to the Home User

It has been shown that the home user is of interest to intruders. Hence the home user with important work-related information, not to mention personal information such as banking details, risks exposing this information to intruders unless they have adequate security measures in place. As well there is the danger posed to organizations by unprotected home users who have VPN access into their work network.

It is widely accepted that information security is concerned with the following three fundamental principles:

- Confidentiality - information should be available only to those who rightfully have access to it


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- Integrity - information should be modified only by those who are authorized to do so

- Availability - information should be accessible to those who need it when they need it

These principles apply to the home user just as much as they would to a user on an organization's network. They translate for the home user as meaning that unwanted eyes should not be able to look through important documents (Confidentiality); that the information enter into the computer remains true (Integrity); and that it is accessible when needed (Availability).

Similarly or perhaps even more so than the business user, the home use must trade off these principles against the cost of implementing security and the impact of them on usability. Hence the key question facing home users is how they can securely access the Internet without sacrificing the required level of usability. After all if the impact of the security measures is so severe that accessing the Internet is very frustrating then either the Internet will not be accessed or else the security measures will be circumvented to gain usability. Neither of these outcomes is acceptable.

## 2.3 The Defence in Depth Approach for the Home User

A defence in depth strategy is the traditional one adopted to afford the defended area the strongest and most resilient protection. In the case of the home Internet user, the defended area is the user's data. As shown in Figure 1, defense in depth for the home user consists of defensive measures adopted in four layers, namely: network access; the operating system; user applications; and data. At the center of the defended area is the most prized component of the defended area – the user's data.

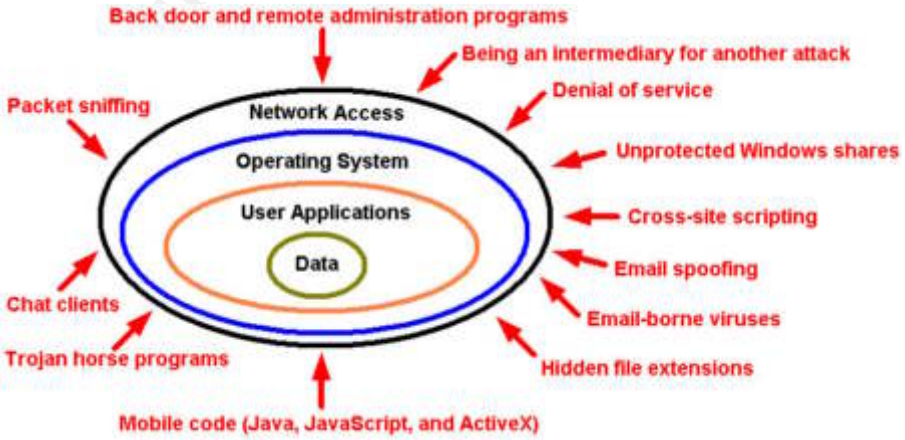


Figure 1. Most common Intruder methods used against home computers


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

This layered approach is required since even the most expensive firewall controlling network access cannot effectively control traffic content. For example, most firewalls will allow in e-mail attachments containing viruses. These viruses may be cleaned at the operation system layer by anti-virus software if they are recognized. However, if they are of an unknown type, then the final defence is at the data layer where the user opens the e-mail attachment with care.

Of courses to be effective, defensive measures at each layer must be based on the threats to the defended area. Since it is unrealistic to expect the home Internet user to be highly knowledgeable about the threat posed to them, the defensive posture must at least cater to the most common methods used by intruders to gain control of home computers. Figure 1 shows the most common intruder methods reported by CERT[4]. More detailed information on these methods is available directly from the referenced CERT URL.

The recommended defensive measures at each layer of the defence vary as shown in Table 2. This listing is not exhaustive but it is felt that it affords a reasonable level of security for home Internet users, and that it can be implemented by non-technical users without causing such frustration that it will be ignored.

Of course those who work from home should consult their system support personnel for advice as well as comply with their organization's security policy and procedures.

| Defensive Layer | Defensive Measures | Remarks |
|---|---|---|
| Network Access | Use a firewall | Hardware or software firewall |
| | Disconnect from the Internet when not using it | User training |
| Operating System | Use a robust operating system | One time activity |
| | Keep up with patch releases | Ongoing activity |
| | Make a boot/ERD disk and keep it current | Ongoing activity |
| | Use and keep up to date anti-virus software | Ongoing activity |
| | Harden OS by turning off unnecessary clients, services and features | One time activity |
| User Application | Keep up with patch releases | Ongoing activity |
| | Do not install programs of unknown origin | User training |
| | Disable Java, JavaScript, and ActiveX when possible | One time activity |
| | Disable scripting features in e-mail programs when possible | One time activity |
| Data | Regular backups of critical data | Ongoing activity |


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

| Defensive Layer | Defensive Measures | Remarks |
|---|---|---|
| | Use encryption to ensure confidentiality of sensitive data | Ongoing activity |
| | Use strong passwords | User training |
| | Open e-mail attachments with care | User training |

Table 2. Defence in Depth – Defensive Actions at each layer

## 3. Implementing the Recommended Defensive Actions

Now that defensive actions have been identified at each layer, it is necessary to discuss how these actions will be carried out for a Windows-based home Internet user.

It is also important to keep in mind that the defensive posture is weakened when one does not implement the entire defence in depth strategy that is being advocated. For example, using a firewall but having either no or outdated anti-virus software, leaves the host vulnerable to the W32/Goner Worm[6]. This worm is distributed as an e-mail file attachment and via ICQ file transfers. If ZoneAlarm was the firewall and the user executes file "gone.scr", then the worm looks for and terminates zonealarm.exe and deletes all files in the directory containing that executable. The net result in this case of failure to have implemented the entire defence in depth strategy is a host running without a firewall to protect it from an intruder's attack.

### 3.1 Implementing the Network Access Layer Defensive Measures

#### 3.1.1 Use a firewall

A firewall is the first line for defence in depth (see Figure 1). Ideally it monitors all incoming and outgoing network traffic and allows connections that are authorized, i.e. it implements an access control policy between two networks. This control protects against direct hacker attacks. As well, the firewall should be able to make the computer "invisible" on the Internet since a low profile makes the host less of a target to intruders.

For home users, a firewall typically takes one of two forms:

- Personal firewall - specialized software running on an individual computer, e.g. ZoneAlarm.
- Hardware firewall - a separate device designed to protect one or more computers, e.g. Linksys EtherFast Cable/DSL Router.

The most basic firewall is a packet filter whose access control lists (ACL) permits or blocks connections through it based on the source and destination IP address


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

and port(s) and the protocol involved. For example, a Cisco router's ACL that allows HTTP traffic from host 10.168.41.41 to any host using TCP/80 looks as follows:

access-list 101 permit tcp host 10.168.41.41 any eq 80

The problem with this approach is that the packet filter does not know if genuine HTTP traffic is using this rule or if a Trojan horse program is sending out its traffic. If the anti-virus software fails to recognize a Trojan horse program then the firewall should prevent that program from being allowed to access the Internet and doing its damaging work. A firewall that provides program-level control can prevent such access since only those applications that are classified as trusted are allowed to access the Internet.

There are several free personal firewalls that provide program-level control, including ZoneAlarm and Tiny Personal Firewall. Another free personal firewall named Internet Connection Firewall (ICF) comes with Windows XP SP1, but it only controls incoming traffic and not outgoing traffic. While Windows 2000 does not having a purpose-built firewall, it does have IP Security filters that can be used to make a static packet filter. This paper looks at ZoneAlarm, ICF and the use of IP Security filters in some detail to compare their easy of use and effectiveness.

### 3.1.2 Disconnect from the Internet when not using it

An air gap is the most effective form of firewall and its use is encouraged.

The user relying on traditional dial-up access to the Internet will likely disconnect when they are not using the connection since monthly usage limits apply and they may only have one phone line. On the other hand, home users with "always-on" broadband access services such as cable modems or DSL may be tempted to leave their computer permanently connected to the Internet. A permanent connection allows them to access their files over the Internet from a remote location. The problem is that the longer one remains connected, the longer an intruder has to locate and attack the host.

## 3.2 Implementing the Operating System Layer Defensive Measures

### 3.2.1 Use a robust operating system

The stability and security of the Windows 9x/ME operating systems has always been a concern. These concerns were largely addressed if the user employed Windows 2000 Pro but the shortcoming was its lack of ease of use on home systems[24].

With Windows XP, Microsoft offered the home user the reliability and security features found in the Windows 2000 server operating system and the ease of


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

use akin to Windows 9x/ME. Windows XP comes in Home and Professional editions. The latter is more feature rich with respect to networking features and other features such as the Encrypting File System (EFS). Nonetheless, the Windows XP Home edition includes the Internet Connection Firewall (ICF), and the NT File System (NTFS) file system that is more robust than the old Windows file system (FAT and VFAT).

### 3.2.2 Keep up with patch releases

The easiest way to do this is to use an operating system that will automatically check for available updates. Recent versions of Windows, such as Windows 2000 Pro and Windows XP, include the ability to get the latest updates for the computer's operating system, software and hardware.

The update process can be started manually using Internet Explorer by invoking the Windows Update option under the Tools menu. This option takes the user to the Windows Update Web site[33] and the user is then lead through the update process. The user can review and select updates to install, but this manual process can be tedious. Fortunately there is an automatic process available.

The update process can be set to run automatically using the Automatic Update applet in the Control Panel in Windows Pro 2000 and Windows XP. With this feature enabled, Windows recognizes when the user is online and uses the Internet connection to search for downloads from the Windows Update Web site. An icon appears in the system tray each time new updates are available.

The settings for automatic updating are:

1. Notify user before downloading any updates and notify again before installing them.
2. Download the updates automatically and notify user when they are ready to be installed.
3. Automatically download the updates and install them on a specified schedule.

The requirement to update and the time consuming nature of doing so is illustrated by the number of updates suggested by Microsoft for an installation of Microsoft Windows XP Professional v5.1 Build 2600.xpclient.010817-1148. As seen in Annex C, Microsoft suggests a total of 33 updates for this build. Of these 33 updates, at least 22 or 67% are directly related to security issues.


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

### 3.2.3 Make a boot/ERD disk and keep it current

A boot disk allows the user to boot from a diskette instead of the hard drive. This can prove useful in accessing the system in the event of either a security incident or hard disk failure. The process of creating such a disk(s) varies with the version of operating system that is running, but it must be done before an incident requiring its use arises.

Some versions of Windows, e.g. Windows NT, Windows 2000 and Windows XP, can use the emergency repair procedure to fix problems that may be preventing the computer from starting. This includes problems with the registry, system files, partition boot sector and startup environment. However, using the emergency repair procedure to fix the system generally requires an existing Emergency Repair Disk (ERD). This disk should be regularly updated and stored in a safe place.

An ERD is created differently depending on the version of Windows. The Backup utility in both Windows 2000 and Windows XP is used to create an ERD, while in Windows NT the “rdisk /s” command is used.

### 3.2.4 Use and keep up to date anti-virus software

In today's computing world, a user must prevent intentional intrusions into the computer that take the form of viruses, worms and Trojan horses. The most effective approach to defend against this malicious software is to install a commercial virus-detection program and use it regularly to check the computer for viruses.

Since new viruses are created every day, the latest virus signature files must be obtained when they are available to maintain effective protection. The anti-virus software should include features such as the automatic updating of its virus definition files, scanning and cleaning of both incoming and outgoing email messages, script blocking of JavaScript and VBScript, and real-time anti-virus protection.

There are a number of vendors that provide good anti-virus software with perhaps the most popular ones being McAfee and Norton[34].

### 3.2.5 Harden the OS by turning off unnecessary clients, services and features

Hardening of the operating system (OS) is a topic on its own for which there are a number of good references, such as the Center for Internet Security benchmarks[20]. However as the subject of this paper is the home user (with only one computer), only the following basic hardening steps are mentioned:

1. Turn off the “Hide file extensions for known file types” feature:


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

By default, Windows hides the file extensions of known file types. This behaviour has been used to trick users into executing malicious code, e.g. the VBS/LoveLetter worm, by making a file appear to be something it is not. For example, with the default configuration, a file named “Here is my new phone number.txt.vsb” appears to the user as a file named “Here is my new phone number.txt”. Opening this file will execute the Visual Basic Script file with potentially destructive results.

To have the file extensions displayed in Windows, uncheck the "Hide file extensions for known file types" option on the "View" tab of the "Folder options" item on the “Tools" menu. However, even with this change, some extensions are still hidden and the "NeverShowExt" registry value must be edited[5].

2. Remove the ability of others to access file shares and printers on the host since poorly protected file shares are being actively targeted[35]:

   - Disable Server Message Blocks (SMB) over TCP/IP by unselecting the “File and Printer Sharing for Microsoft Networks” option in the Network and Dial-Up Connections applet[21].

   - Disable RPC and NetBIOS over TCP/IP (NBT) by unselecting the “Client for Microsoft Networks” option in the Network and Dial-Up Connections applet[21].

   - Deny remote access to your computer by using the Local Security Policy applet to add the Everyone group to the “Deny Access to this computer from the network” policy[22] which is found in User Rights Assignment under the Local Policy.

## 3.3 Implementing the User Application Layer Defensive Measures

### 3.3.1 Keep up with patch releases

Just as new vulnerabilities appear regularly in the OS, so too they also appear in applications. Hence keeping applications patched is important. Visiting the Microsoft Security site[23] gives one access to the security bulletins and allows one to subscribe to the Microsoft Security Update e-mail alert service.

In general, the announcement of new product vulnerabilities can be monitored by subscribing to one or more of the e-mail based free security alerting services. These services describe the latest vulnerabilities and generally indicate either how to get the required patch or the workaround pending a patch release. Such services include the CERT Advisory Mailing List[36] and Security Alert Consensus[37].


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

### 3.3.2 Do not install programs of unknown origin

Installing programs of unknown origin exposes the user to the possibility of running malicious code. In general, programs to be installed should have been authored by a person or company that is trusted and the download site should be a similarly trusted source. Of course virus scanning any such program prior to installation is recommended.

### 3.3.3 Disable Java, JavaScript, and ActiveX when possible

Malicious web scripts can get to a web browser when a web developer sends such damaging code as part of the web server's response. This malicious code then ends up on the host running the browser.

The methods for disabling Java, JavaScript and ActiveX in Netscape and Internet Explorer browsers are described by CERT[25] so are not repeated here.

Unfortunately the problem is that by disabling these features, the user may find it frustrating that certain sites can no longer be effectively browsed. If the user cannot live without being able to run these scripts, then an alternative is to use a commercial anti-virus scanner that affords some level of protection against malicious scripts.

### 3.3.4 Disable scripting features in e-mail programs when possible

Since e-mail programs frequently use the same code as web browsers to display HTML formatted messages, the vulnerabilities that affect ActiveX, Java, and JavaScript are often applicable to e-mail. Apart from disabling these features, the ability to run Visual Basic Scripting (VBS) should be removed if possible.

Viruses such as ILOVEYOU contain attachments ending in .vbs which infect the host when user clicks on the attachment to open it. In order to limit the risk of infection, the Windows Scripting Host could be disabled as described on ZDNet[26]. Because of the potential adverse effects of disabling Windows Scripting Host, an alternative is to maintain an up-to-date anti-virus program and to use care when opening e-mail attachments.

## 3.4 Implementing the Data Layer Defensive Measures

### 3.4.1 Regular backups of critical data

Important files must be backed up regularly onto removable media such as floppies or recordable CD-ROM disks. This will facilitate restoration if the system is damaged either by hardware failure or malicious activity. The definition of regularly depends on the comfort level of the user, i.e. how much work is one


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

prepared to lose? A daily backup would be ideal but a weekly backup might be more practicable.

There are a variety of techniques that can be used to affect the backup. Most recordable CD-ROM drives come with software that allows the disk to be formatted as a data disk that can then be written to using a file manager such as Explorer. Floppy disk can be used for backup using software such a WinZip to compress the data files. Software backup tools are also available, e.g. Windows 2000 and XP both come with a Backup utility that is found in System Tools under Accessories.

The removable media used during the backup should be stored in a safe location away from the computer so that the media is not affected if physical damage occurs to the computer area.

3.4.2 Use encryption to ensure confidentiality of sensitive data

With the newer versions of Windows, i.e. Windows 2000 Pro and XP, the user can use the Encrypting File System (EFS) to encrypt important data files. By using such encryption, an intruder who gets through all the defence in depth layers and tries to access encrypted files or folders will be prevented from doing so. The intruder will receive an access denied message if he/she tries to open, copy, move, or rename an encrypted file or folder, unless the intruder has determined the UID and password of either the system administrator or the user who created the encrypted file.

Once a file or folder is encrypted, the user can work with the encrypted file or folder just as he/she would with any other file and folder since encryption is transparent to the user that encrypted the file. This means that the user does not have to decrypt the encrypted file before using it.

A file or a folder can be encrypted, subject to the following constraints, by using Explorer selecting the file/folder and clicking on the “Encrypt contents to secure data” attribute on the Advanced features of the properties page:

- Can only encrypt files and folders on NTFS file system volumes.
- Compressed files or folders cannot be encrypted.
- System files cannot be encrypted.

If the user should ever lose their file encryption certificate and associated private key (through disk failure or any other reason), then data recovery is available through the person who is the designated recovery agent.


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Of course if the use of EFS is not an option, then a knowledgeable user could use PGP for this sort of encryption. However, using PGP would not be transparent like using EFS. PGP Freeware is available for non-commercial use[19].

### 3.4.3 Use Strong Passwords

Whenever you are required to use a password, e.g. when the administrator account in Windows 2000 Pro is created, you should use a strong password that conforms to the following guidelines[8]:

- At least seven characters in length (the longer the better)
- Includes upper and lower case letters, numerals, symbols
- Has at least one symbol character in the second through sixth position
- Has at least four different characters in your password (no repeats)
- Looks like a sequence of random letters and numbers
- Don't use any part of your logon name for your password
- Don't use any actual word or name in ANY language
- Don't use numbers in place of similar letters
- Don't reuse any portion of your old password
- Don't use consecutive letters or numbers like "abcdefg" or "234567"
- Don't use adjacent keys on your keyboard like "qwerty"

A good way to create a strong password is by using the first letters of a phase that you can easily remember. For example, using the first letters and punctuation of the phase: "My first child Laura, was born in 1999!", the strong password of "MfcL,wbi1!" is derived.

### 3.4.4 Open E-mail Attachments with Care

Before opening any email attachments, the user should check if they recognize the sender of the attachment and have a good idea of why the attachment is being sent. However, recognizing the sender is not enough since some viruses such as Melissa, sent copies of themselves out as attachment to all addressees found in the Microsoft Outlook address book on the infected system.

A good approach to opening an attachment is as follows:

1. Check if you recognize the sender of the attachment and know why the attachment is being sent.

2. Be very suspicious of amusing or enticing programs since this type of social engineering is sometimes used by malicious code for its propagation.

3. If you decide open the attachment then ensure that the anti-virus software's virus definitions are up-to-date and then proceed as follows:


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- save the file to your hard disk
- scan the file using the anti-virus software
- open the file

## 4. Comparing Three Readily Available Personal Firewalls

The use of a personal firewall is an essential component of the defence in depth strategy. However, it is perhaps the most neglected component by the non-technical home Internet user. The reason for this is probably that while these users by now recognize the need to use anti-virus software, they are simply unaware of the role of and protection afforded by a personal firewall. Unfortunately many users are not even aware that their operating system, be it Windows 2000 Pro or Windows XP, includes firewalling capability.

In this section, the following readily available personal firewalls for current Windows operating systems are examined:

- IP Security filters on Windows 2000
- Internet Connection Firewall (ICF) on Windows XP
- ZoneAlarm on Windows

These are software-based firewalls that do not cost the home user anything to acquire since both IP Security Filters and ICF are included with the operating system while ZoneAlarm is free for personal use.

We'll compare the easy of use and effectiveness of these firewalls. The goal of this comparison is to determine which is the most convenient one for the non-technical home user to use while affording adequate protection. While none of these firewalls is an ICSA-certified one[17], they are useful for the home user.

Rules for these firewalls will be based on the paranoid policy of "that which is not expressly permitted is prohibited" rather than its permissive opposite policy of "that which is not expressly prohibited is permitted". While the former policy requires more work when a new service is required, it is more secure.

Figure 2 shows where the personal firewall fits into the connection of a home PC to the Internet. Obviously the personal firewall is not a discrete component, rather it is software that runs on the home PC, but it's shown separately for clarity. As illustrated, the goal of the personal firewall is to ensure that traffic from intruders cannot reach the home PC – understanding that the firewall will not block attachments bearing malicious code.


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

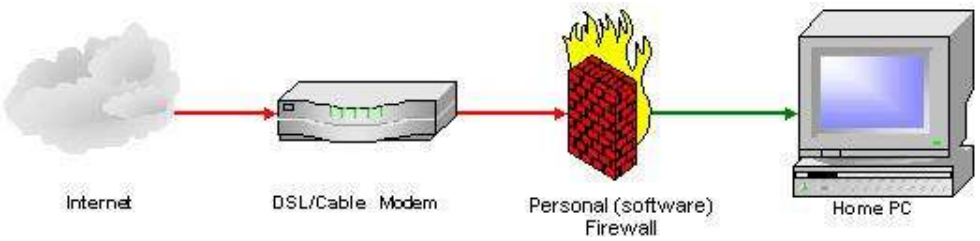


Figure 2. Protecting the Internet-connected Home PC

## 4.1 Windows 2000 - Using IP Security filters as a Static Packet Filter

### 4.1.1 Using a Static Packet Filter as a Firewall

A static packet filter is one of the simplest and least expensive forms of firewall. With static packet filtering, each packet trying to ingress to or egress from the host is checked against a set of user-defined rules. These rules are based on the following criteria:

- Source IP address and port
- Destination IP address and port
- protocol

As shown in Figure 3, a static packet filter firewall works at the network layer (Layer 3) of the OSI Model[18].

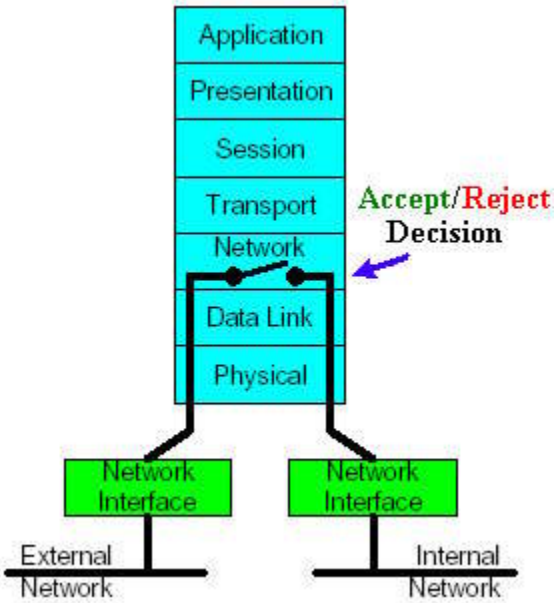


Figure 3. A Static packet filter firewall and the OSI Model


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

The basic problem with this packet filtering approach is that the user requires some sophistication to build and maintain this firewall. Simple packet filters such as IP Security Filters, do not keep track of the connections and do not automatically allow the reverse connections. For example, if you define a filter that allows HTTP traffic from the local subnet to a web server on the host, but you also wish to allow this machine to browse Web sites outside of the local subnet, care must be taken in building the rules to ensure that the source and destination ports are defined correctly for each instance.

Furthermore, IP filtering operates at the network layer so it only understands the connections themselves and nothing about the applications using the network connections. The problem arises when an intruder uses a permitted well-known port to connect to another well-known port listening on the screened host. For example, consider the case of a packet filter that allows external connections from a source port of tcp/80 to any destination port. Now by default the screened host is listening on the microsoft-ds port (tcp/445). The vulnerability is that the packet filter cannot stop an intruder from connecting to tcp/445 with a program that uses tcp/80 as its source port. Users of nmap can do this by using the "-g <portnumber>" option to set the source port number used in scans.

Similarly static packet filter implementations that allow DNS (53) or FTP-DATA (20) packets to come through and establish a connection are at risk, since an intruder can masquerade as FTP or DNS servers by modifying their source port.

### 4.1.2 Overview of IP Security Filters

Windows 2000 users have no personal firewall as part of the operating system. However, the Windows 2000 IP Security filters can serve as a static packet filter thereby affording basic firewalling capability. When used this way, IP Security filters allow the user to selectively permit and deny traffic. However the tools to monitor and troubleshoot such an implementation are largely non-existent.

Windows Internet Protocol Security (IPSec) is designed to encrypt data as it travels between two computers, protecting it from modification and interpretation if anyone were to see it on the network. An administrator must first define how the two computers will trust each other, and then specify how the computers will secure their traffic. This is done by creating an IPSec policy using the IP Security Policy Management snap-in and then assigning it.

A stateless packet filter based on IP Security Filters is built from user-defined rules. The rules are evaluated from the most specific to the least specific in the following order[14]:

For IP addresses:

1. My IP Address


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

2. Specific IP Address Defined
3. Specific IP Subnet
4. Any IP Address

For Protocols/Ports

1. Specific Protocol/Port combination
2. Specific Protocol/Any Port
3. Any Protocol

One important point is that the default “All IP traffic” rule does not apply to broadcast, multicast (224.0.0.0 through 239.255.255.255), Kerberos (tcp/88 or udp/88), RSVP (IP protocol 46) and ISAKMP (IKE) (udp/500) traffic[15]. If Kerberos authentication is not required then both the exemption for it and RSVP can be removed by adding the NoDefaultExempt=1 value to the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPSEC key[16].

4.1.3 Implementation of a Simple Firewall using IP Security filters

The first step is to ensure that the “IPSEC Policy Agent” service is started.

To create a firewall, add the IP Security Policy Management snap-in to a Microsoft Management Console (MMC) and then use the Create IP Security Policy to create a policy named "Firewall Policy". While name of the policy is arbitrary, it ought to be descriptive.

Figure 4 shows the beginning of the definition of a simple firewall. There are two general rules that block all IP and ICMP traffic to the host. To make Internet access useful, rules must now be defined that allow the traffic that the user wants in and out of the host. Rules for HTTP and DHCP traffic have already been defined in this example but DNS traffic is required to facilitate browsing. The definition of the rule for permitting DNS traffic will illustrate how the existing rules were added.


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

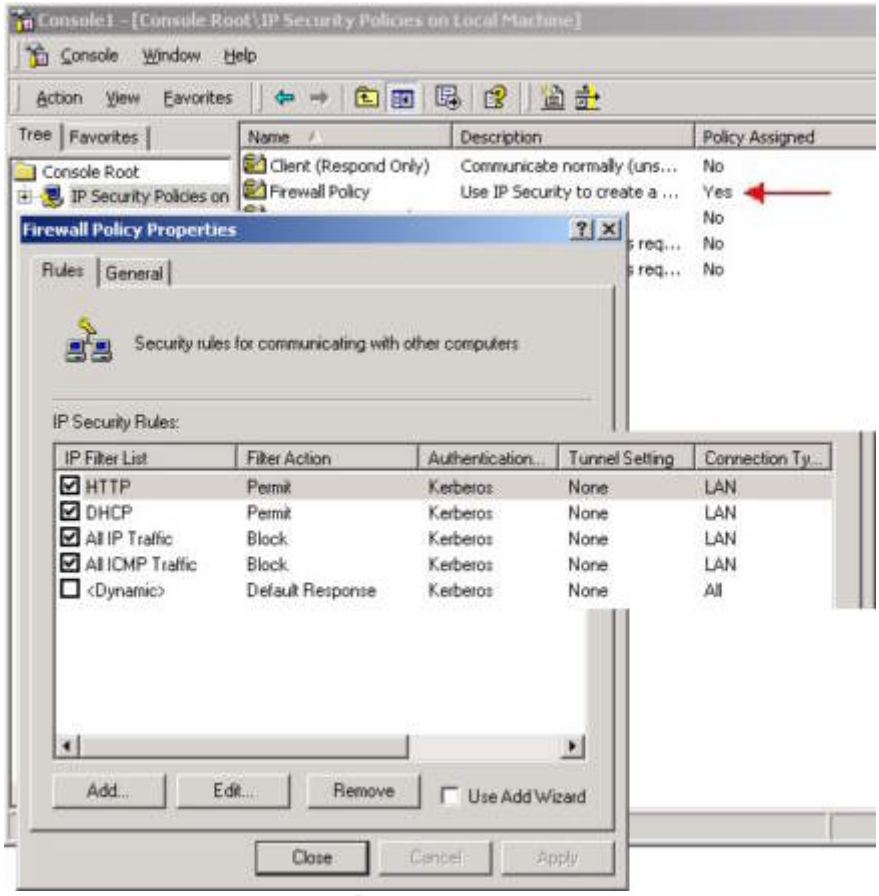


Figure 4. Defining a Firewall Policy using IP Security filters

The following steps illustrate how to expand the ACL to control additional traffic. In this case DNS traffic is to be allowed for name resolution.

1. Click on the Add button of the Firewall Policy Properties window (the "Use Add Wizard" has been disabled, see Figure 4).

2. Click on the Add button of the New Rule Properties window (see Figure 5) and the IP Filter List window appears.


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

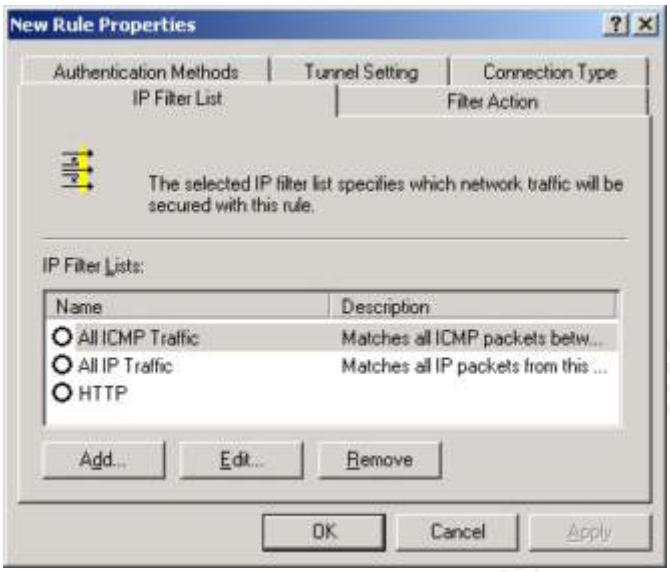


Figure 5. New Rule Properties window

3. In the IP Filter List window, enter DNS in the Name field, and then click on the Add button and the Filter Properties window appears (see Figure 6).

   - On the Addressing tab, use the defaults (with the Mirrored option selected, there is no need to create a separate egress and ingress rule for DNS).

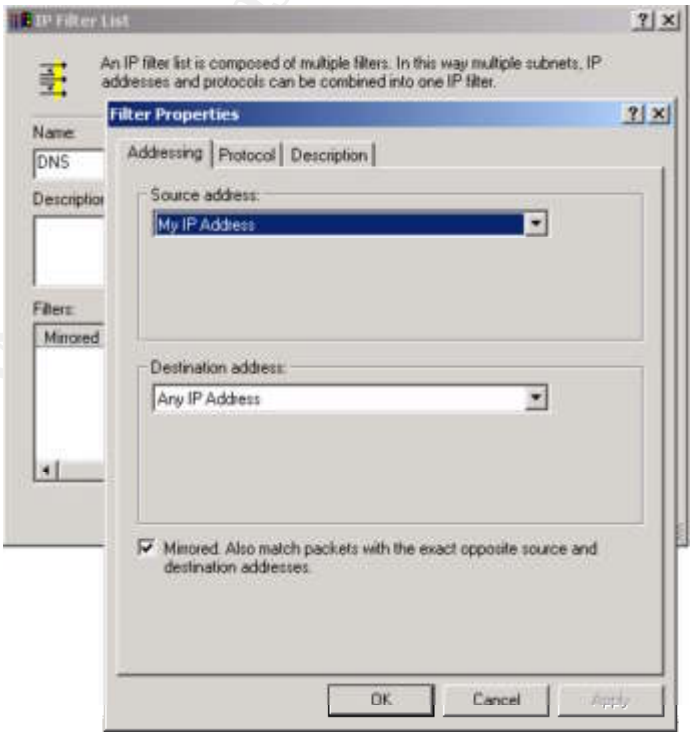


Figure 6. IP Filter List window


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- On the Protocol tab, set the port to udp/53 as the destination with any port as the source (see Figure 7).

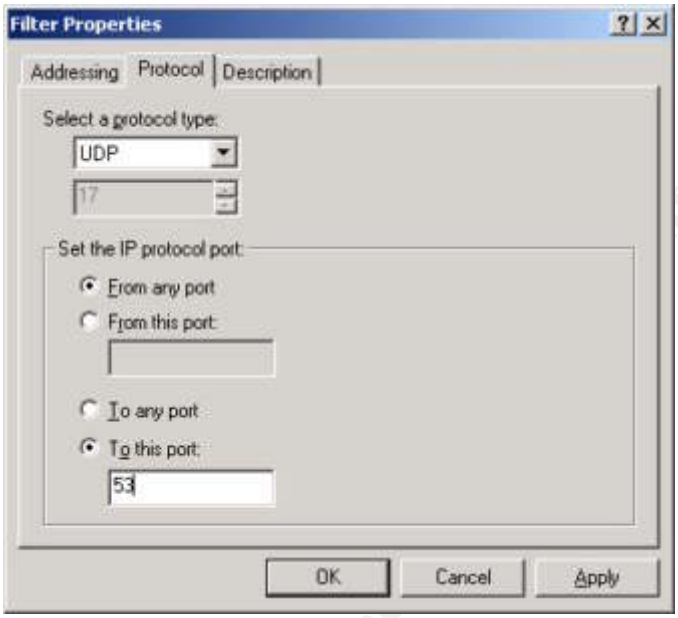


Figure 7. Protocol tab of the IP Filter List window

4. Back on the New Rule Properties window (see Figure 5):

   - On the IP Filter List tab, select the new DNS rule.

   - On the Filter Action tab (see Figure 8), select the Permit filter action.

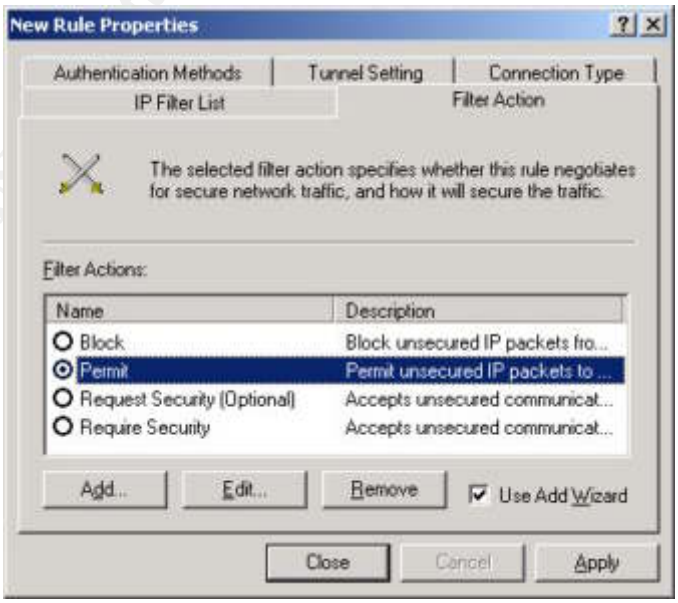


Figure 8. Filter Action tab of the IP Filter List window


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

- The defaults on the other tabs should be fine in most cases.

5. On the Firewall Policy Properties window ensure that the DNS rule is selected (see Figure 9).

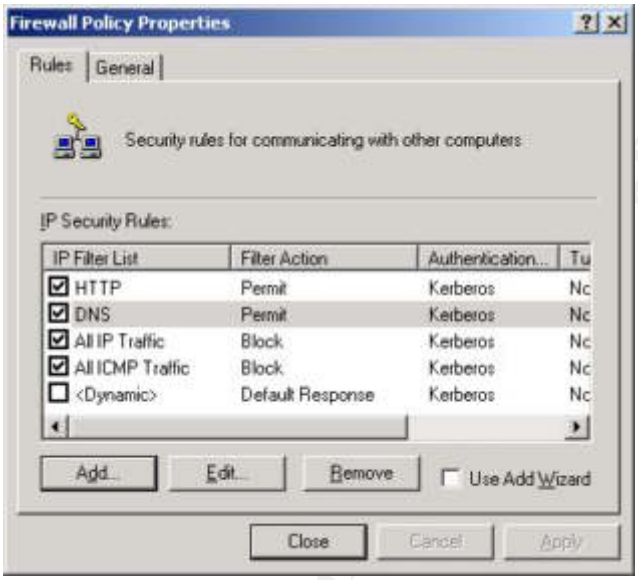


Figure 9. Revised Firewall Policy

6. The revised Firewall Policy takes effect immediately since it was already assigned (see Figure 4).

So with the Firewall Policy now allowing both HTTP and DNS traffic, the user can browse most sites on the Internet.

4.1.4 Conclusions about this Firewall

A firewall based on IP Security Filters is a static packet filter which is fast and inexpensive. This type of firewall can be effective under the following restrictive conditions:

1. Implementation is by relatively sophisticated user who updates it as required.

2. The protected host has a static environment with clearly defined services required.

3. The protected host has been hardened to remove necessary services so that an intruder cannot use port redirection to connect to these services.


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Even under these conditions, the lack of tools to monitor and troubleshoot this firewall may prove too great a stumbling block. Probably the best use for this firewall is to learn about static packet filters - it is not for the average home Internet user.

## 4.2 Windows XP Pro – Using Internet Connection Firewall (ICF)

### 4.2.1 Overview of ICF

The basic functionality of ICF is shown in Figure 3. However unlike the IP Security Filter-based firewall, ICF is a stateful firewall since it monitors all aspects of the communications that cross its path and inspects the source and destination address of each message that it handles. To prevent unsolicited traffic from the Internet side of the connection from entering the private side, ICF keeps a table of all communications that have originated from the host itself. All inbound traffic from the Internet is compared against the entries in the table. Inbound Internet traffic is permitted through to the host if there is a matching entry in the table showing that the communication exchange originated from the host.

ICF can be configured to allow traffic that originates from the Internet through to the host. For example, if the host is a web server then enabling ICF's HTTP service allows unsolicited HTTP traffic through to the web server.

ICF supports user configurable logging, although it is not enabled by default. ICF security logging can record the following:

- Log dropped packets - Logs all dropped packets that originate from either the home or small office network or the Internet.

- Log successful connections - Logs all successful connections that originate from either the home or small office network or the Internet.

A sample of the ICF log follows:

```
#Verson: 1.0
#Software: Microsoft Internet Connection Firewall
#Time Format: Local
#Fields: date time action protocol src-ip dst-ip src-port dst-port size tcpflags tcpsyn tcpack
tcpwin icmptype icmpcode info

2003-03-22 21:44:25 OPEN TCP 172.20.12.85 172.20.12.84 3004 445 - - - - - - - -
2003-03-22 21:44:31 DROP UDP 172.20.12.84 172.20.12.255 137 137 78 - - - - - - -
2003-03-22 21:44:37 OPEN TCP 172.20.12.85 172.20.12.84 3006 80 - - - - - - - -
2003-03-22 21:45:11 CLOSE TCP 172.20.12.85 172.20.12.84 3006 80 - - - - - - - -
```


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

### 4.2.2 Implementation of ICF

The ICF is not enabled by default. To enable the Internet Connection Firewall:

1. Click on the Start button and then go to Settings and select Network Connections.
2. Click on Local Area Network and then click on the Properties button.
3. On the Advanced tab select the option to “Protect my computer and network by limiting or preventing access to this computer from the Internet”.
4. Clicking the Settings button on the Advanced tab allows one to set the following options:

    - Services tab – Specify the services running on the host that Internet users can access (this should not be required for most home Internet users).
    - Security Logging tab – If desired, logging can be specified for dropped packets and successful connections.
    - ICMP tab – If desired, certain types of ICMP traffic can be allowed into and out of the host.

Note that network connectivity problems can arise if ZoneAlarm is installed along with ICF[27].

### 4.2.3 Programs can change the ICF Ruleset

While a user with administrator rights can change the configuration of the ruleset, so too can applications designed to use ICF’s API. However, this feature can open the firewall to probing by a determined intruder. To illustrate this, consider that when ICF is activated, by default the Windows Messenger service opens random high TCP and UDP ports for its use through the firewall. For example during testing, "msmsgs 14117 TCP" and "msmsgs 14895 UDP" services were added to the ICF. Hence an exhaustive nmap scan of TCP and UDP ports found these ports as shown:

```
Port        State       Service
14117/tcp   open        unknown
14895/udp   open        unknown
```

Once the intruder knows these ports, nmap can be run against the TCP port to determine the operating system. For example, running "nmap -sN -P0 -O -p 14117 -v 172.20.12.85" results in the following output:

```
nmap (V. 3.00) scan initiated Sun Mar 23 16:50:03 2003 as: /usr/bin/nmap -sN -P0 -O -p
14117 -v -oN ./sN_P0_O_v_172.20.12.85_14117.txt 172.20.12.85
```


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

```
Warning:  OS detection will be MUCH less reliable because we did not find at least 1
open and 1 closed TCP port
Interesting ports on  (172.20.12.85):
Port       State       Service
14117/tcp  open        unknown
Remote operating system guess: Windows XP Professional RC1+ through final release
TCP Sequence Prediction: Class=random positive increments
                         Difficulty=14847 (Worthy challenge)
IPID Sequence Generation: Incremental

# Nmap run completed at Sun Mar 23 16:51:56 2003 -- 1 IP address (1 host up) scanned
in 113 seconds
```

Hence Windows XP's default behaviour when the ICF is activated, exposes the host to an intruder without any involvement by or notification of the user.

### 4.2.4 Conclusions about this Firewall

The ICF is a stateful firewall that has the following attractions:

1. Implementation is straightforward by a non-technical user.
2. The default configuration of ICF is its most secure posture.
3. Its stateful nature protects the user against an intruder using port redirection.
4. Basic logging of permits and denies is supported, however no real time notification is available.
5. It is integrated into the operating system and supported by Microsoft.

On the other hand, ICF has some caveats:

1. The major shortcoming of this firewall is that it is built exclusively as outward facing protection, that is it controls neither the host's outbound traffic nor programs connecting to Internet hosts.
2. The ICF programmatic API allows ICF aware applications, such as Windows Messenger, to open up "holes" in the ICF to allow incoming traffic. While this is useful for programs that require inbound connections, it is done without requesting user authorization.

Probably the best use of this firewall is by the basic home Internet user who wants security but does not feel comfortable installing, configuring and maintaining a third party firewall.


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

## 4.3 Windows - Using ZoneAlarm Personal Firewall

### 4.3.1 Overview of ZoneAlarm

ZoneAlarm is personal firewall software that is free for personal and non-profit use (excluding government and educational entities). ZoneAlarm is compatible with Microsoft Windows 98/Me/NT/2000 and XP. It can be downloaded from http://www.zonelabs.com/.

ZoneAlarm is a stateful packet-filtering firewall with the ability to control applications that try to get out to the Internet. This egress control gives the user the ability to restrict how applications interact with outside hosts and well as possible notification if the host becomes infected by a Trojan that seeks to call home.

The installation and setup of ZoneAlarm is well documented in numerous papers[30,31] so the interested reader is referred to those sources. However it is worthwhile to note that ZoneAlarm has an access permissions option that allows the user to surf the web and retrieve e-mail without any further configuration. This option allows out the following applications access to the Internet:

- Default Web browser (e.g. iexplorer.exe) – Allows browsing.
- Windows Web component: Generic Host Process (svchost.exe) – Various services that are run from dynamic-link libraries (DLLs)[32].
- Windows Web component: Services and Controller App (services.exe) – Allows DNS.

### 4.3.2 Conclusions about this Firewall

ZoneAlarm is a stateful packet-filtering firewall with the ability to control applications that try to get out to the Internet. This type of firewall can be effective if it is implemented is by a user with more than basic user skills who takes the time to read up on its operation.

The tools to monitor and troubleshoot this firewall are good in include hyperlinks to detailed information on ZoneLabs' web site.

## 4.4 Vulnerability of Testing of the Firewalls

Table 3 shows the results of testing the three firewalls described in this paper. These tests consisted of running Nessus 2.0.1, nmap 3.00, Gibson Research Corporation's Shields up and Sygate Online Services against the firewalls. Other tests results and more in depth ones are available on the Internet, for example, SecurityFocus has a report on the ICF[28].


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

As can be seen, according to these tests, the host was adequately protected by each of the firewalls such that the host would not be an easy and attractive target for intruders.

| Test | No firewall (baseline) | IP Security Filters on W2K | ZoneAlarm | ICF on Win XP |
|---|---|---|---|---|
| Nessus 2.0.1 | Security hole and warnings found (see Annex B) | The remote host is considered as dead - not scanning | The remote host is considered as dead - not scanning | - 14117/tcp open<br>- OS guess of Windows XP Professional |
| nmap -sT -P0 -O -v -p 1-65535 | Ports 135, 139, 445, 1025, 1470 are reported as Open | - 88/tcp closed<br>- no OS guess | No results after 2 hours | No results after 2 hours |
| nmap -sT -O -v -I | Not run (see above results) | 1 IP address (0 hosts up) | 1 IP address (0 hosts up) | 1 IP address (0 hosts up) |
| nmap -sS -O -v | - Ports 135, 139, 445, 1025, 1470 are reported as Open<br>- Port 1 reported as Filtered | 1 IP address (0 hosts up) | 1 IP address (0 hosts up) | 1 IP address (0 hosts up) |
| nmap -sF -P0 -O -v -p 1-65535 | All 65535 scanned ports are: closed | - 88/tcp closed<br>- no OS guess | No results after 2 hours | No results after 2 hours |
| nmap -sF -O -v | Not run (see above results) | 1 IP address (0 hosts up) | 1 IP address (0 hosts up) | 1 IP address (0 hosts up) |
| nmap -sU -P0 -O -v -p 1-65535 | Ports 135, 137, 138, 445, 500, 514, 1026 are reported as Open | No results after 10 hours | 1 IP address (0 hosts up) | No results after 2 hours |
| nmap -sU -O -v | Not run (see above results) | 1 IP address (0 hosts up) | 1 IP address (0 hosts up) | 1 IP address (0 hosts up) |
| Sygate Online Services – Quick Scan[11] | - Ports 20, 21, 23, 25, 53, 59, 79, 80, 110, 113, 443, 1080, 5000, 8080 are reported as Closed<br>- Ports 135 and 445 are reported as Open[iii]<br>- Port 139 reported as Blocked[i]<br>- ICMP (type 8) reported as | - Ports 20, 21, 23, 25, 53, 59, 79, 80, 110, 113, 135, 139, 443, 445, 1080, 5000, 8080 are reported as Blocked[i]<br>- ICMP (type 8) reported as Blocked[i] | - Ports 20, 21, 23, 25, 53, 59, 79, 80, 110, 113, 135, 139, 443, 445, 1080, 5000, 8080 are reported as Blocked[i]<br>- ICMP (type 8) reported as Blocked[i] | - Ports 20, 21, 23, 25, 53, 59, 79, 80, 110, 113, 135, 139, 443, 445, 1080, 5000, 8080 are reported as Blocked[i]<br>- ICMP (type 8) reported as Blocked[i] |


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

| Test | No firewall (baseline) | IP Security Filters on W2K | ZoneAlarm | ICF on Win XP |
|---|---|---|---|---|
| | Open[iii] | | | |
| Sygate Online Services – Stealth Scan[11] | - Ports 20, 21, 23, 25, 53, 59, 79, 80, 110, 113, 443, 1071, 1080, 8080 are reported as Closed[ii]<br>- Port 139 reported as Blocked[i]<br>- Port 445 is reported as Opened[iii] | - Ports 20, 21, 23, 25, 53, 59, 79, 80, 110, 113, 139, 443, 1080, 2369, 8080 are reported as Closed[ii]<br>- Port 445 is reported as Opened[iii] | - Ports 20, 21, 23, 25, 53, 59, 79, 80, 110, 113, 139, 443, 445, 1080, 1085, 8080 are reported as Blocked[ii] | - Ports 20, 21, 23, 25, 53, 59, 79, 80, 110, 113, 139, 443, 445, 1080, 1085, 8080 are reported as Blocked[ii] |
| Shields Up! – Test My Shields! [12] | - Port 139 does not appear to exist<br>- Unable to connect with NetBIOS | - Port 139 does not appear to exist<br>- Unable to connect with NetBIOS | - Port 139 does not appear to exist<br>- Unable to connect with NetBIOS | - Port 139 does not appear to exist<br>- Unable to connect with NetBIOS |
| Shields Up! – Probe My Ports![12] | - Ports 21, 23, 25, 79, 80, 110, 113, 143, 443, 5000 are reported as Closed[iv]<br>- Ports 135, 445 reported as Open[v]<br>- Port 139 is reported as Stealth[vi] | Ports 21, 23, 25, 79, 80, 110, 113, 135, 139, 143, 443, 445, 5000 are reported as Stealth[vi] | Ports 21, 23, 25, 79, 80, 110, 113, 135, 139, 143, 443, 445, 5000 are reported as Stealth[vi] | Ports 21, 23, 25, 79, 80, 110, 113, 135, 139, 143, 443, 445, 5000 are reported as Stealth[vi] |

[i] Sygate defines "blocked" as meaning that no response is received[10].
[ii] Sygate defines "closed" as meaning that there is nothing listening at a specific port[10].
[iii] Sygate defines "opened" as meaning that indicates that the host is actively listening and ready to accept incoming connections to that specific port[10].
[iv] GRC defines "Closed" as meaning that a probe of the port responds with a Reset[12].
[v] GRC defines "Open" as meaning that the host is actively listening and ready to accept incoming connections to that specific port [12].
[vi] GRC defines "Stealth" as meaning that there is no evidence that a port exists at this IP address[12].

Table 3. Results of testing the Firewalls

The difference between the Sygate Quick and Stealth scan results for tcp/445 of the IP Security Filters on Windows 2000 merits an explanation. A Quick scan of tcp/445 (microsoft-ds) reports this port as blocked while a Stealth scan reports it as being open. Using Ethereal, a protocol analyzer, the following results are seen:


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Trace of a Stealth scan of tcp/445:

```
207.33.111.35:80 > 172.20.12.246:445: S 3307885200
172.20.12.246:445 > 207.33.111.35:80: S 1427800488 ack 3307885201
207.33.111.35:80 > 172.20.12.246:445: R 3307885201
```

Trace of a Quick scan of tcp/445:

```
207.33.111.35:49487 > 172.20.12.246:445: S 889111176
```

Hence a Stealth scan is able to complete the three-way TCP handshake while the Quick scan is not.

As previously discussed, IP filtering operates at the network layer so it does not understand anything about the application using the network connections, only about the connections themselves. Since the IP filter allows external connections from a source port of tcp/80 to any destination port, then the packet filter cannot stop an intruder from connecting tcp/445 using a program with tcp/80 as its source port. It is this opening that the Stealth scan exploits. Unlike a Cisco IOS-based router, IP Security Filters cannot be used to specify that only established TCP connections are allowed in.

IP Security Filters can be used to prevent the Stealth scan being able to connect to tcp/445 by creating a filter that prevents any source port from connecting to a destination port of tcp/445. If internal hosts must connect to tcp/445 then exceptions can be created for them.

## 5. Conclusion

The home Internet user is a target for intruders and requires a defence in depth approach to securely use the Internet while observing the fundamental security principles of confidentiality, integrity and availability. This paper has presented such an approach based on specific actions at the network access; the operating system; user applications; and data layers. It is also important to keep in mind that the defensive posture is weakened when one does not implement the entire defence in depth strategy that is being advocated.

The actions forming the recommended approach are summarized in Table 2. It is felt that following this approach is reasonably straightforward such that the non-technical user will not become so frustrated that the recommended security measures will be ignored.

Finally this paper recommends that users running Windows XP should use either ICF or a more advanced personal firewall such a ZoneAlarm. The basic home user may feel more comfortable using ICF, while the more technically able user will probably prefer the more advanced firewall.


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

## Annex A – Connections and Listening Ports

The following is the output of the “netstat -an” command on the default installation of Windows 2000 Pro used for this paper:

```
Proto  Local Address          Foreign Address        State

TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1470           0.0.0.0:0              LISTENING
TCP    172.20.12.246:139      0.0.0.0:0              LISTENING
UDP    0.0.0.0:135            *:*
UDP    0.0.0.0:445            *:*
UDP    0.0.0.0:514            *:*
UDP    0.0.0.0:1026           *:*
UDP    172.20.12.246:137      *:*
UDP    172.20.12.246:138      *:*
UDP    172.20.12.246:500      *:*
UDP    127.0.0.1:1028         *:*
```

The following is the output of the “netstat -an” command on the default installation of Windows XP Pro used for this paper:

```
Proto  Local Address          Foreign Address        State
TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
TCP    0.0.0.0:1025           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1027           0.0.0.0:0              LISTENING
TCP    0.0.0.0:1470           0.0.0.0:0              LISTENING
TCP    0.0.0.0:5000           0.0.0.0:0              LISTENING
TCP    127.0.0.1:3001         0.0.0.0:0              LISTENING
TCP    127.0.0.1:3002         0.0.0.0:0              LISTENING
TCP    127.0.0.1:3003         0.0.0.0:0              LISTENING
TCP    172.20.12.85:139      0.0.0.0:0              LISTENING
TCP    172.20.12.85:14117    0.0.0.0:0              LISTENING
UDP    0.0.0.0:135            *:*
UDP    0.0.0.0:445            *:*
UDP    0.0.0.0:500            *:*
UDP    0.0.0.0:514            *:*
UDP    0.0.0.0:1026           *:*
UDP    0.0.0.0:1028           *:*
UDP    0.0.0.0:3007           *:*
UDP    127.0.0.1:123          *:*
UDP    127.0.0.1:1900         *:*
UDP    172.20.12.85:123      *:*
UDP    172.20.12.85:137      *:*
UDP    172.20.12.85:138      *:*
UDP    172.20.12.85:1900     *:*
UDP    172.20.12.85:7671     *:*
UDP    172.20.12.85:14895    *:*
```


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

## Annex B – Highlights of Nessus Report with no Firewall/Filtering

The following is a partial output from Nessus when run against the Windows 2000 Pro host without any firewall or IP filtering in place.

| 5.1.1.1.1 Analysis of Host | | |
|---|---|---|
| **Address of Host** | **Port/ Service** | **Issue regarding Port** |
| 172.20.12.246 | loc-srv (135/tcp) | Security warning(s) found |
| 172.20.12.246 | netbios-ssn (139/tcp) | Security hole found |
| 172.20.12.246 | microsoft-ds (445/tcp) | Security notes found |
| 172.20.12.246 | NFS-or-IIS (1025/tcp) | Security notes found |
| 172.20.12.246 | uaiact (1470/tcp) | No Information |
| 172.20.12.246 | general/udp | Security notes found |
| 172.20.12.246 | general/tcp | Security warning(s) found |
| 172.20.12.246 | general/icmp | Security warning(s) found |
| 172.20.12.246 | netbios-ns (137/udp) | Security warning(s) found |
| 172.20.12.246 | unknown (1026/udp) | Security notes found |

© SANS Institute 2003, Author retains full rights.


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

## Annex C – Microsoft Recommended Updates for Microsoft Windows XP Pro

Table 4 lists the 33 updates/patches recommended by Microsoft for an installation of Microsoft Windows XP Professional v5.1 Build 2600.xpclient.010817-1148. Of these 33 updates, at least 22 or 67% are directly security related.

Applying Windows XP Service Pack 1a will bring XP up to Build 2600.xpsp1.020828-1920.

| 5.1.1.1.1.1.1 Recommended Update | Description |
|---|---|
| Windows XP Service Pack 1a | Provides the latest security, reliability, and performance updates |
| 810847: February 2003 | Cumulative Patch for Internet Explorer 6 |
| Q328676 | Security Update (Outlook Express 6) |
| Security Update, February 14, 2002 | Internet Explorer 6 |
| Q329441 | Critical Update |
| Q324096 | Security Update (Windows XP) |
| Q323172 | Security Update (Windows XP) |
| Q326830 | Security Update (Windows XP) |
| Q324380 | Security Update (Windows XP) |
| Q313450 | Security Update |
| Q311967 | Security Update |
| System Recovered Error Message Update | Eponymous |
| Security Update, February 13, 2002 | MSXML 2.6 and 3.0 |
| Security Update, February 12, 2002 | Unchecked Buffer in SNMP Service |
| Critical Update, February 10, 2002 | Stop 0xED on mounting volume |
| Critical Update, February 9, 2002 | Background Intelligence Transfer Service |
| Security Update, December 17, 2001 | Unchecked Buffer in Universal Plug and Play |
| Remote Assistance Connection | Cannot Establish a Remote Assistance Connection |
| Q309521 | Windows XP Update Package, October 25, 2001 - security |
| Q329390 | Security Update |
| Q329115 | Security Update (Windows XP) |
| 328310 | Security Update |
| 810577 | Security Update |
| 814078 | Security Update (Microsoft Jscript version 5.6, Windows 2000, Windows XP) |
| Q327696 | Internet Information Services Security Roll-up Package |
| Q318138 | Security Update (Windows XP) |
| Q323255 | Security Update (Windows XP) |
| Q329048 | Security Update |
| Windows XP Application Compatibility Update, April 2002 | Eponymous |
| Windows Messenger 4.6 Connectivity Update | Eponymous |
| 810030 | Microsoft VM Security Update |
| 329170 | Security Update |
| 811630 | Critical Update (Windows XP) |

Table 4. Microsoft Recommended Updates for Microsoft Windows XP Pro


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

## References


1. IDC Research: *Worldwide Net traffic to rise*. URL: http://www.nua.ie/surveys/?f=VS&art_id=905358733&rel=true (3 March, 2003).

2. Statistics Canada: Internet use by households. URL:http://www.statcan.ca/Daily/English/990423/d990423b.htm (1998).

3. CNN.com: Ex-CIA chief surfed Web on home computer with top-secret data. URL:http://www.cnn.com/2000/US/02/03/cia.deutch/ (February 3, 2000).

4. CERT Coordination Center: Home Network Security. URL:http://www.cert.org/tech_tips/home_networks.html (December 5, 2001)

5. JSI FAQ: Some extensions are still hidden after unchecking the option in Windows 2000 Explorer? URL:http://www.jsiinc.com/SUBH/tip3600/rh3613.htm

6. CERT Coordination Center: CERT Incident Note IN-2001-15. URL:http:// www.cert.org/incident_notes/IN-2001-15.html (December 4, 2001)

7. SANS: Intrusion Detection FAQ - What port numbers do well-known trojan horses use? URL: http://www.sans.org/resources/idfaq/oddports.php (updated 2/9/01)

8. Microsoft: Checklist: Create Strong Passwords. URL: http://www.microsoft.com/security/articles/password.asp

9. Microsoft: Messenger Service Window That Contains an Internet Advertisement Appears. URL: http://support.microsoft.com/?id=330904 (January 31, 2003)

10. Sygate: Frequently Asked Questions - Sygate Technologies Security Scan. URL: http://scan.sygate.com/prescanfaq.html

11. Sygate Online Services. URL: http://scan.sygate.com/

12. Gibson Research Corp: Shields UP! URL: http://grc.com/x/ne.dll?rh1ck2l2

13. Nmap network security scanner man page. URL: http://www.insecure.org/nmap/data/nmap_manpage.html



© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

14. Klemencic, Joe. “Windows IP Security Filters”. URL: http://conferences.fnal.gov/hepix/powerpoint/ wed/klemencic_430.ppt (October 23, 2002)

15. Microsoft: Traffic That Can--and Cannot--Be Secured by IPSec. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;253169

16. Microsoft: IPSec Does Not Secure Kerberos Traffic Between Domain Controllers. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;254728

17. ICSA Labs Certified PC Firewalls. URL: http://www.icsalabs.com/html/communities/pcfirewalls/cert_prods.shtml (February 1, 2003)

18. Viacomsoft: KnowledgeShare - Firewall Q&A. URL: http://www.vicomsoft.com/knowledge/reference/firewalls1.html.

19. PGP Corporation: Freeware Details. URL: http://www.pgp.com/products/freeware.html

20. Center for Internet Security: Windows 2000 Professional Operating System Level 2 Benchmark Consensus Baseline Security Settings. URL: https://www.cisecurity.org/tools2/win2000/W2K-Pro.pdf (November 4, 2002).

21. Microsoft: Deny access to this computer from the network. URL: http://www.microsoft.com/technet/prodtechnol/winxppro/proddocs/534.asp.

22. JSI FAQ: 5913 Unbinding Client for Microsoft Networks does NOT disable shares in Windows 2000? URL: http://www.jsiinc.com/SUBL/tip5900/rh5913.htm.

23. Microsoft Security and Privacy site. URL: http://www.microsoft.com/security/.

24. CommWeb: Windows XP finally brings real security to the desktop. URL: http://www.commweb.com/article/NMG20011004S0009 (October 5 2001).

25. CERT Coordination Center: Frequently Asked Questions About Malicious Web Scripts Redirected by Web Sites. URL: http://www.cert.org/tech_tips/malicious_code_FAQ.html (February 2, 2000).

26. ZDNet Review: How to turn off Windows Scripting Host. URL: http://netscape.zdnet.com/zdhelp/stories/main/0,5594,2568111,00.html (May 16, 2001).


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

27. Microsoft: "Ping: Transmit Failed, Error Code 65" Error Message When You Attempt to Ping Another Computer. URL: http://support.microsoft.com/?kbid=316414.

28. SecurityFocus HOME Infocus: Windows ICF Can't Live With it, Can't Live Without it. URL: http://online.securityfocus.com/infocus/1620 (August 22, 2002).

29. SecurityFocus HOME Infocus: Securing Privacy, Part Two: Software Issues. URL: http://www.securityfocus.com/infocus/1573 (April 25, 2002).

30. Curtis Elliott: ZoneAlarm – A Free Solution for Home Security. URL: http://www.sans.org/rr/homeoffice/zonealarm.php (October 1, 2002).

31. SecurityFocus HOME Guest Feature: Configuring ZoneAlarm Securely. http://www.securityfocus.com/guest/11486 (Mar 29, 2002)

32. Microsoft: Description of Svchost.exe in Windows 2000. URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;250320 (October 11, 2002)

33. Microsoft: Windows Update Web site. URL:http://v4.windowsupdate.microsoft.com/en/default.asp

34. PC Magazine: Recent Reviews (Antivirus) http://www.pcmag.com/category2/0,4148,4796,00.asp

35. CERT Coordination Center: CERT Advisory CA-2003-08 Increased Activity Targeting Windows Shares. URL: http://www.cert.org/advisories/CA-2003-08.html (March 11, 2003).

36. CERT Coordination Center: The CERT Advisory Mailing List. URL: http://www.cert.org/contact_cert/certmaillist.html.

37. SANS: Newsletters and Digests. URL: http://www.sans.org/newsletters/.


© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: August 28th, 2015

# Upcoming SANS Training

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

| | | | |
|---|---|---|---|
| **FOR578 Cyber Threat Intelligence** | **Tysons Corner, VAUS** | **Aug 31, 2015 - Sep 04, 2015** | **Live Event** |
| **SANS Milan 2015** | **Milan, IT** | **Sep 07, 2015 - Sep 12, 2015** | **Live Event** |
| **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** |
| **SANS Tallinn 2015** | **Tallinn, EE** | **Sep 21, 2015 - Sep 26, 2015** | **Live Event** |
| **SANS Perth 2015** | **Perth, AU** | **Sep 21, 2015 - Sep 26, 2015** | **Live Event** |
| **SANS Baltimore 2015** | **Baltimore, MDUS** | **Sep 21, 2015 - Sep 26, 2015** | **Live Event** |
| **Data Breach Investigation Summit & Training** | **Dallas, TXUS** | **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** |
| **SOS: SANS October Singapore 2015** | **Singapore, SG** | **Oct 12, 2015 - Oct 24, 2015** | **Live Event** |
| **SANS Tysons Corner 2015** | **Tysons Corner, VAUS** | **Oct 12, 2015 - Oct 17, 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 Chicago 2015** | **OnlineILUS** | **Aug 30, 2015 - Sep 04, 2015** | **Live Event** |
| **SANS OnDemand** | **Books & MP3s OnlyUS** | **Anytime** | **Self Paced** |