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.

## Securing an IIS 5.0 Web Server on Windows 2000 using Security Tools and Templates

This paper attempts to give an overview of the security guides, tools and templates available from Microsoft, and to describe the basic steps involved in applying the tools and templates. The commonalities and differences between the security templates available are highlighted, and how several of these tools and templates can be used together to benefit from the settings made by each one is described. As an example the securing of a standalone Windows 2000 Web Server is discussed, and an appropriate sequence of use (i...

Copyright SANS Institute

Author Retains Full Rights

AD

# Securing an IIS 5.0 Web Server on Windows 2000 using Security Tools and Templates

Graeme McLintock CEng.

## 1 Introduction

Recently, Microsoft has made great efforts to improve the security of Windows 2000 systems by, amongst other measures, introducing further security guides and tools. The Microsoft Strategic Technology Protection Program [5] offers guides, patches, hotfixes and tools (e.g. hfnetchk ), bringing Microsoft's security offerings under one roof. Although, the latest program from Redmond undoubtedly improves access to security information direct from the OS manufacturer many of the suggestions are not new. Indeed, with such a wealth of patches, hotfixes, security templates and lockdown tools now available the system administrator is literally spoilt for choice.

The majority of the guides and documents available on windows security have focused on recommended security configuration settings, or on the functionality of one tool or security template. Examining the individual configuration settings recommended in the guide or made by the tool or template concerned. However, this paper attempts to give an overview of the security guides, tools and templates available from Microsoft, and to describe the basic steps involved in applying the tools and templates.

The commonalities and differences between the security templates available are highlighted, and how several of these tools and templates can be used together to benefit from the settings made by each one is described. As an example the securing of a standalone Windows 2000 Web Server is discussed, and an appropriate sequence of use (i.e. apply the **baseline**, **IIS incremental** and **hisecweb** templates then the IIS lockdown tool) for the tools and templates for IIS 5.0 web servers is suggested.

## 2 Tools and Guides Available

The documentation and tools available for securing windows systems has grown rapidly in recent years. To gain an insight into the basic configuration settings described and manipulated by the security tools a comprehensive description is available in the NSA Windows 2000 Security Recommendation Guide [21].

Some of the important security guides available on the network:

- **Guides to Baseline Security**
  - *Windows 2000 - New installation* [6]



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

    - *Windows 2000 - Existing installation* [7]
  - **Baseline Security Checklists**
    - Windows 2000 Server [8]
    - Internet Information Services 5.0 [9]
  - **Service Pack Installation and Deployment Guide**
    - Windows 2000 [10]
  - **Security Operations Guide for Windows 2000 Server**
    - http://www.microsoft.com/TechNet/security/prodtech/windows/windows2000/staysecure/DEFAULT.asp [11]
  - **From Blueprint to Fortress: A Guide to Securing IIS 5.0**
    - IIS 5.0 [12]

Patches from Microsoft provide the latest fixes to emerging bugs and plug exploits. Microsoft regularly bundles these fixes into a Service Pack for the operating system. Patches, in particular security patches, are also made available for software applications, and are intermittently rolled up into one package.
The most important service packs for a standalone web server are:

- Windows 2000 Service Pack 2 [13]
- Internet Information Services 5.0 Security Rollup [14]

Microsoft also offers a number of security tools in the Microsoft Security Tool Kit [15], which contains amongst others the following:

- Microsoft Baseline Security Advisor [16]

  The Microsoft Baseline Security Analyzer (MBSA) is a recently released tool based on hfnetchk (see below), which analyses the security configuration of windows systems. The settings for Windows 2000, Internet Information Server (IIS) 5.0, and SQL Server 2000 are checked, amongst other application software packages (e.g. MS-Office). MBSA is a convenient way of checking whether or not the patches on a server are up to date, and whether basic security settings are fulfilled. The basic settings for the operating system and IIS are also covered by security templates (e.g access rights), but the settings for the application software (e.g. non-blank SA password in SQL Server 2000) are useful. However, you must apply this tool to your system before applying security templates that disable the “server” service (i.e. NetBIOS on the local computer) otherwise many of the checks cannot be carried out.

- Internet Information Services Lockdown Wizard [17]

  Using the IIS Lockdown Wizard the administrator can alter the security settings on a web server using one of the application software templates provided (e.g. MS-Commerce Server 2000). This tool also installs URLscan and can be used to undo changes made previously using this tool. The


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

changes made to the system are aimed at securing against illicit web access. Apart from IIS configuration the Lockdown Wizard alters the ACLs of the directories on the server by adding DENY rules for the anonymous web user (i.e. IUSR_***) and the out-of-process web applications account (i.e. IWAM_***). It can be tricky to reapply the changes to ensure the DENY rules have not been lost after other ACL modifications which may have reset the ACL (e.g. from a security template like baseline.inf). The only way to reapply the Lockdown Wizard changes is by first undoing the changes previously applied (i.e. uninstalling the lockdown tool).

- URLScan Security Tool

UrlScan is an ISAPI filter that filters HTTP requests to avoid malicious requests. The latest version only comes with the IIS Lockdown Wizard tool. The standard filter settings can be read and configured after installation in C:\WINNT\system32\inetsrv\urlscan\urlscan.ini. The standard settings restrict, for example, the set of verbs to PUT, GET and POST and filters out requests containing exe, bat, cmd and com file extensions. Also, directory traversal using "../" and alternate stream access using ":" (i.e. to prevent the storage of hidden data within an NTFS file, see [23] for a description of alternate streams). However, you may want to additionally restrict access using pipes "|" and ">", in this case add these to the [DenyUrlSequences] section of urlscan.ini.

- HFNetChk (Command Line Hot Fix Check Tool) [18]

The Hfnetchk tool checks the patch status of a windows system with the list of recommended patches from Microsoft. The list of recommended patches and hot fixes can be accessed online to facilitate easy regular assessment of a system running amongst other packages: Windows 2000, Internet Information Server (IIS) and SQL Server 2000. However, you must apply this tool to your system before applying security templates that apply IPsec filtering to restrict Internet access otherwise this tool will fail to access the list of recommended patches online. Alternatively, it is possible to download the current recommended list of patches and to analyze the system against a local list offline, which will be necessary for maintenance checking of a deployed web server.

- QChain

A further useful tool is QChain, which can be used to safely install a number of hotfixes without rebooting between each installation. This tool eases the application of patches not yet available in a rollup package or service pack.

- Security Configuration and Analysis [19]

One of the most important security tools is the Security Configuration and Analysis MMC snap-in (or secedit.exe from the command line). This tool is available on all Windows 2000 systems (don't be put off by the Microsoft


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

documentation [19] referring to the Windows XP resource kit) and is very useful as it allows the system administrator to automate many of the security configuration tasks, e.g. setting file ACLs, setting registry entries, setting auditing policy, or user account access rights. To automate the setting of a configuration option a security template is required. The use of secedit is similar to the much mentioned Group Policy for Windows 2000 (i.e. gpedit.msc from the command line), and indeed the settings that can be made used secedit.exe templates cover the security settings of Group Policy. To use secedit a database must be created that holds one security policy template and, after analyzing the local system, the current system settings. The template can be viewed, modified, compared to the system settings, and applied to the system to modify the system settings. How effective this tool is depends largely on the template in use. It is essentially up to the administrator to evaluate the security recommendations made in guides, and to create his/her own template. However, Microsoft supplies a number of templates which can be used as a starting point; making use of these is discussed in detail below.

The above overview of the security tools and guides available makes apparent that the informed use of security templates is the most important method of ensuring the security of server systems. A description of the context for applying security templates, and a discussion of the effects of the various “standard” templates available follows below.

# 3 Basic Server Installation

To put the web server “hardening” suggestions into context this section briefly describes typical recommendations [26, 27], covering the operating system and patches, for the basic installation of a Windows 2000 based IIS 5.0 web server prior to applying the security tools documented below.

## 3.1 Operating System

- Always start with a clean system to ensure that no extraneous programs or viruses are already on the system.
- Consider creating extra partitions for the operating system, application data (e.g. databases, web site files or upload directories) and a separate partition for backups.
- Do not connect the server to a network during installation, only connect it after the server has been hardened.
- Install the latest U.S. English operating system if possible, as hotfixes and patches are made most readily available for this operating system version.
- Install only the TCP/IP protocol if possible, definitely not NetBIOS.
- Do not install any additional network services (e.g. file or print sharing).
- Install the latest Service Pack (currently Windows 2000 Service Release 2), removing any possibly vulnerable backup files after a trial period.


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

- Install the Windows 2000 High Encryption Pack if for some reason Service Release 2 is not being installed. Service Release 2 automatically installs high encryption (128 bit) making the High Encryption Pack superfluous.
- After installing the operating system ensure that the first boot device is set to be the hard disk, and use the floplock utility to lock the floppy drive if appropriate.

### 3.2 Service Packs and Hotfixes

- Install any application software, e.g. database systems, before applying the relevant system patches.
- Install any relevant Security hotfixes, currently Security Roll-Up Package 1 for Windows 2000 SR2 (w2kSR2SRP1) is recommended.
- Install IIS patches on a web server, currently "Cumulative Patch for Internet Information Services (Q319733)" contains all relevant patches.
- Re-install the Service Pack and patches after installing a new component (e.g. DHCP Server) and use the **Microsoft Baseline Security Analyzer**, or the **hfnetchk** command line utility directly, to check if the current configuration on your server is up to date and has all the appropriate security patches.

## 4 Advanced Web Server Configuration

Having completed the basic installation of the operating system and application software the system should then be “hardened” by altering the standard system configuration. Rather than document individual configuration changes, the preferable method is to provide a security policy template.

### 4.1 Basic Security Configuration using Templates

An effective way to manipulate the security settings of Windows systems is using Group Policy (gpedit) or Local Security Policy (secedit). Using the Security Configuration and Analysis MMC Snap-In (secedit) a security template can be loaded and applied to the system. N.B. only one template can be loaded into each database as no merging of subsequent templates occurs. This method of configuration also allows the use of the recommended settings as supplied by Microsoft in standard template files.

The most important templates for web servers supplied by Microsoft are:

baseline.inf: supplied with the **Microsoft Security Operations Guide for Windows 2000 Server** as a base configuration

hisecweb.inf: supplied together with **IIS Incremental.inf** with **From Blueprint to Fortress: A Guide to Securing IIS 5.0** **[12]**

The serious problem is then which template should I use?



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

As the Security Configuration and Analysis tool does not merge templates it can be difficult to decide what settings are made exclusively by each template. This information about the differences can of course be a very useful source of information for any security professional.

## 4.2 Template Comparison

Comparing the settings in two templates can be done by starting two instances of the Security Configuration and Analysis MMC Snap-In and loading each template file in a separate database. This can be very tedious, as not only the settings made by each template are displayed. This is also not very effective if you are versioning a template and wish to see the differences. Comparing template files by hand using a text editor can be difficult as the order of settings in template file is not significant and may vary.
Using the snap-in (secedit) to export created templates is also of limited use as these differ in layout to the source templates from Microsoft.

To alleviate the task a script for comparing templates and only displaying non-identical settings or settings unique to one template has been written (see source code in Appendix A and example output in Appendix B). To use the script Perl must be installed on the system. The Windows binary version can be downloaded from ActiveState (http://www.activestate.com/Products/Download/Get.plex?id=ActivePerl). After installing Perl the template comparision script can be started as follows:

> Perl infdiff.pl [-v] <template filename1> <template filename2>
> *e.g. perl infdiff.pl baseline.inf hisecweb.pl*

An example showing the results of comparing baseline.inf with hisecweb.inf is shown in Appendix B. The example in Appendix B shows only the differences, for brevity. The entries are listed separately in a list for each inf file showing the settings made that contradict those made by the other template file. These are the settings that would be overwritten should you apply the two templates to a single system. The optional verbose argument [-v] causes the infdiff script to output all changes made only by one or the other script as well as all differing settings.

The remainder of this section highlights some of the differing settings made by the 3 policy templates *baseline*, *hisecweb* and *IIS Incremental*.

Generally speaking, there are many more file ACL modifications in the **baseline** template than the **hisecweb** template. The files and directories whose attributes are only modified by the baseline template are listed in Appendix C as generated by the infdiff.pl script using the [–v] verbose option. The modifications themselves are written in the Security Descriptor Definition Language, a good and short


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

description of which can be found in [22]. The files affected are mainly the special boot files in the \ directory and executables in the \windows and \windows\system32 directories, whereby the access rights are mainly restricted to local administrator and SYSTEM accounts.

**Baseline** sets many more access restrictions on registry keys than **hisecweb** does. These ensure that hardware profiles, font libraries, and policies cannot be manipulated by users without sufficient privileges.

The registry value settings contained in **hisecweb** go further than **IIS Incremental** and are more appropriate to a web server than **baseline**'s. The most significant differences are described here.

**hisecweb** suggests not requiring a logon to change the password, this may be to allow IIS to modify the IUSR_*** password. But if you intend to update the IUSR_*** password manually and not to give the IIS process control over the password, then you can set this entry to 1 as **baseline** does.

**RequireLogonToChangePassword = 0**

**hisecweb** sets the AuditLogRetensionPeriod to 0, i.e. overwrite as needed, whereas **baseline** suggests 2, i.e. Never Overwrite Events (Clear Log Manually). For a web server it may be more appropriate to overwrite the event log to avoid DoS attacks. But if you are evaluating the log data as part of your web service this may be inappropriate.

**AuditLogRetentionPeriod = 0**

Both **hisecweb** and **IIS Incremental** (hereafter **IISinc**) restrict the NetworkLogon access right. These settings use well known security identifiers (see the description in [24]):

```
[Privilege Rights]
SeNetworkLogonRight = *S-1-5-11        //i.e. authenticated users

[Group Membership]
*S-1-5-32-547__Memberof =       //i.e. no members of Power Users group
*S-1-5-32-547__Members =        // allowed in the built-in system domain
```

**Baseline** sets the SynAttackProtect registry setting to 2, but **IIS Incremental** and **hisecweb** both reduce the protection level to 1 to allow IIS to function more effectively [25] by speeding up the creation of new TCP/IP connections at a slightly increased risk of DoS attacks.

MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\SynAttackProtect=4,1


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Naturally, both **IIS Incremental** and **hisecweb** start the IISadmin and Web Publishing services automatically.

There are many more windows services restrictions in **baseline.inf** than **hisecweb.inf**. But **hisecweb** does disable the RemoteRegistry service. However it enables the PolicyAgent, which is not needed on a standalone server. These entries use the Security Descriptor Definition Language [22], to disable the PolicyAgent setting change the “PolicyAgent,2,…” to “PolicyAgent,4,…” in the template file using notepad.

```
RemoteRegistry,4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)
S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"

PolicyAgent,2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(
A;;CCLCSWLOCRRC;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;
;;SY)"
```

Auditing of COM object access is restricted to failures by **hisecweb**, whereas **baseline** audits successful object use. As logging successful object use can quickly fill the log on a web server the **hisecweb** setting is more useful.

```
AuditObjectAccess = 2
AuditPrivilegeUse = 3
```

The above comparison shows that the "**baseline.inf**" template supplied with the Microsoft Security Operations Guide for Windows 2000 Server should be used as a base configuration. For web servers use the templates "**baseline.inf**"+"**IIS Increment.inf**"+"**hisecweb**.inf". To apply a template, copy the inf file to %windir%\security\templates and use the Group Policy MMC snap-in for the Local Computer to set, and the Security Configuration and Analysis MMC Snap-In to check the settings. Apply these settings only **after** installing application software. To apply multiple templates create a separate database per template using the Security Configuration and Analysis MMC Snap-In (N.B. the snap-in does not merge files as entries in the configuration database are not overwritten during a subsequent import) and apply these in the following correct order (for a web server):

1. baseline.inf
2. IIS Incremental.inf
3. hisecweb.inf


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

### 4.3 Web Server Lockdown

Having made the policy changes required to the operating system and services using a combination of template files the final step is to "harden" the IIS process itself.
This should be followed on web servers by applying the IIS Lockdown tool, which ***amends*** the ACLs on files to "deny" anonymous web users access (as opposed to **baseline.inf** which ***replaces*** the ACLs on files with ones restricting access with "allow" settings). The IIS lockdown tool also installs the URLscan tool, which is to be highly recommended as a further line of defense, by restricting the syntax of acceptable URLs thus avoiding numerous exploits.

## 5 Conclusions

The security tools available from Microsoft are largely concerned with checking for and installing hotfixes and patches. The many guides mentioned in this document testify to the complexity of the topic of security configuration or "hardening". However, the advent of policy templates has made the server "hardening" process much simpler, quicker and more reliable. The remaining problem is not really writing a template, rather choosing the correct template from those on offer. A clear method of comparison, as described in this document, allows the easy assessment of the suitability of the many templates on offer, and the construction of an individual template containing the required settings. Rather than waste time learning the standard settings made by all templates, more time can be spent concentrating on the more subtle settings suggested only by some templates.
For web servers a currently appropriate selection of templates is to apply the **baseline**, **IIS incremental** and **hisecweb** templates supplied by Microsoft in that order, and then to finally apply the IIS lockdown tool.


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

## References


[1] Bys, Cory, "Securing Windows 2000 Server " (May 2001)", 20 May 2001, URL:http://rr.sans.org/win2000/sec_server.php

[2] Cook, Malcolm, "Securing Windows 2000 With Security Templates": Securing Windows GCNT Practical Assignment, Aug. 2001, URL:http://www.giac.org/practical/Malcolm_Cook_GCNT.doc

[3] Courington, David S. "A Step-by-Step Guide to Securing Windows 2000 for Use as a Internet Server", 29 March 2001, URL:http://rr.sans.org/win2000/win2000_sec.php

[4] L'Abbe, Colleen, "Hisecweb.inf – An Analysis", 23 Nov. 2001, URL:http://rr.sans.org/win2000/hisecweb.php

[5] Microsoft Corp. "Microsoft Strategic Technology Protection Program", 1st March 2002, URL: http://www.microsoft.com/security/mstpp.asp

[6] Microsoft Corp. "Installing and Securing a New Windows 2000 System", Microsoft Security Tool Kit, 2001, URL:http://www.microsoft.com/technet/security/tools/tools/w2knew.asp

[7] Microsoft Corp. "Installing and Securing an Existing Windows 2000 System", Microsoft Security Tool Kit, 2001, URL:http://www.microsoft.com/technet/security/tools/tools/w2kexist.asp

[8] Microsoft Corp. "Windows 2000 Server Baseline Security Checklist", 2001, URL:http://www.microsoft.com/technet/security/tools/chklist/w2ksvrcl.asp

[9] Microsoft Corp. "IIS 5.0 Baseline Security Checklist", 2001, URL:http://www.microsoft.com/technet/security/tools/chklist/iis5cl.asp

[10] Microsoft Corp. "Windows 2000 Service Pack Installation and Deployment Guide", 2001, URL:http://www.microsoft.com/windows2000/zipdocs/sp2deploy.exe

[11] Microsoft Corp. "Security Operations Guide for Windows 2000 Server", URL:http://www.microsoft.com/TechNet/security/prodtech/windows/windows2000/staysecure/DEFAULT.asp

[12] Microsoft Corp. "From Blueprint to Fortress: A Guide to Securing IIS 5.0", June 2001, URL:http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/iis/deploy/depovg/securiis.asp

[13] Microsoft Corp. "Windows 2000 Service Pack 2" 16 May 2001, URL:http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/default.asp




© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

[14] Microsoft Corp. "Cumulative Patch for IIS 5.0":Microsoft Security Bulletin MS01-044, 15 Aug. 2001, URL:http://www.microsoft.com/technet/security/bulletin/ms01-044.asp

[15] Microsoft Corp. "Microsoft Security Tool Kit Contents", 1 March 2001, URL:http://www.microsoft.com/security/kitinfo.asp

[16] Microsoft Corp. "Microsoft Baseline Security Advisor", 4 April 2002, URL:http://www.microsoft.com/technet/security/tools/Tools/MBSAhome.asp

[17] Microsoft Corp. "Internet Information Services Lockdown Wizard" Version 2.1, URL:http://www.microsoft.com/technet/security/tools/tools/locktool.asp

[18] Microsoft Corp. "HFNetChk (Hotfix Network Checker Tool)": Microsoft Knowledge Base Article – Q303215, 2 Juli 2001, URL:http://www.microsoft.com/technet/security/tools/tools/hfnetchk.asp

[19] Microsoft Corp. "Using the Security Configuration and Analysis Snap-In". URL:http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/winxppro/reskit/prdd_sec_hchg.asp

[20] Napernikov, Boris, "What Does It Take to Harden an IIS Web Server", 19 Feb. 2002, URL:http://rr.sans.org/win2000/harden_IIS.php

[21] National Security Agency. "NSA Windows 2000 Security Recommendation Guide", 27 Dec. 2001, URL: http://nsa2.www.conxion.com/

[22] Stanford University. "Overview of Active Directory Security", 4 June. 2002, URL: http://windows.stanford.edu/docs/ADSecurityOverview.htm

[23] Crucial Security. Whitepaper: "An Analysis of Alternate Data Streams" 2002, URL: http://www.crucialsecurity.com/ADSwhitepaper.pdf

[24] Stansted Univ. Windows Infrastructure: "Glossary of Windows Terms" 2002, URL: http://windows.stanford.edu/docs/glossary.htm

[25] Internet Security Systems: "SynAttackProtect Description" 2002, URL: http://www.iss.net/security_center/advice/Reference/Registry/HKLM/System/CurrentControlSet/Services/Tcpip/Parameters/SynAttackProtect/default.htm

[26] Norberg, Stefan: "Securing Windows NT/2000 Servers for the Internet" 2001, O'Reilly & Associates Inc. ISBN: 1-56592-768-0

[27] Zwicky, Elizabeth, et al: "Building Internet Firewalls" 2000, O'Reilly & Associates Inc. ISBN: 1-56592-871-7



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

## Appendix A

The following is the source code for the perl script **infdiff.pl**:

```
# (c) Graeme McLintock, Siemens Dematic AG 2002

sub read_file();
sub read_values();
sub read_keys();

$sysroot = $ENV{"SystemRoot"};
$sysdir = $sysroot . "\\SYSTEM32";
$sysdrive = $ENV{"SystemDrive"};
$progfiles = $ENV{"ProgramFiles"};

$sysroot =~ s/\\/\\\\/g;
$sysdir =~ s/\\/\\\\/g;
$progfiles =~ s/\\/\\\\/g;

$argctr = 0;
$verbose = 0;
$file1name = $ARGV[$argctr++];
if ($file1name =~ /-v/i) {
      $verbose = 1;
      $file1name = $ARGV[$argctr++];
}
$file2name = $ARGV[$argctr++];

if ($file1name eq "" || $file2name eq "") {
      print "Usage: perl infdiff.pl [-v] <INF filename> <INF filename>";
      exit();
}


&read_file ($file1name, \%file1);
&read_file ($file2name, \%file2);


print "==== $file1name ====\n";
foreach $x (sort(keys(%file1))) {
      print "\t$x :\n";
      $val1 = $file1{$x};
      $val2 = $file2{$x};
      foreach $y (sort(keys(%$val1))) {
            $vval1 = uc($$val1{$y});
            $vval2 = uc($$val2{$y});
            if ($vval2 eq "") {
                  if ($verbose) { print "only\t\t$y = $$val1{$y}\n"; }
            }
            elsif ($vval1 ne $vval2) {
                  print "diff\t\t$y = $$val1{$y}\n";
            }
      }
}
print "==== $file2name ====\n";
foreach $x (sort(keys(%file2))) {
```



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
        print "\t$x :\n";
        $val1 = $file1{$x};
        $val2 = $file2{$x};
        foreach $y (sort(keys(%$val2))) {
                $vval1 = uc($$val1{$y});
                $vval2 = uc($$val2{$y});
                if ($vval1 eq "") {
                        if ($verbose) { print "only\t\t$y = $$val2{$y}\n"; }
                }
                elsif ($vval1 ne $vval2) {
                        print "diff\t\t$y = $$val2{$y}\n";
                }
        }
}
print "==== done ====\n";


sub read_file() {
        local($filename, $filed) = @_;
        local($status,%filevals,$line);

        $status = "";

        open (IFILE, "$filename") || die "Error: cannot open $filename";
        $line = <IFILE>;
        FOO: while (!eof(IFILE)) {
                if ($line =~ /^;/) {  # comment
                        $line = <IFILE>;
                        next FOO;
                }
                if ($line =~ /^\[(version)\]/i || # version
                    $line =~ /^\[(System Access)\]/i ||
                    $line =~ /^\[(System Log)\]/i ||
                    $line =~ /^\[(Security Log)\]/i ||
                    $line =~ /^\[(Application Log)\]/i ||
                    $line =~ /^\[(Event Audit)\]/i ||
                    $line =~ /^\[(Application Log)\]/i ||
                    $line =~ /^\[(Privilege Rights)\]/i ||
                    $line =~ /^\[(Registry Values)\]/i ) {
                        my (%filevals) = ();
                        $keyname = $1;
                        $line = &read_values (\*IFILE, \%filevals);
                        $$filed{$keyname} = \%filevals;
                        next FOO;
                }
                if ($line =~ /^\[(Registry Keys)\]/i ||
                    $line =~ /^\[(File Security)\]/i ||
                    $line =~ /^\[(Service General Setting)\]/i ) {
                        my (%filevals) = ();
                        $keyname = $1;
                        $line = &read_keys (\*IFILE, \%filevals);
                        $$filed{$keyname} = \%filevals;
                        next FOO;
                }
                $line = <IFILE>;
        }
        close (IFILE);
```



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
}

sub read_values() {
      local($ifile, $filed) = @_;
      local ($line,$k,$v);
      while ($line = <$ifile>) {
            if ($line =~ /^\[/) { return $line; }
            if ($line =~ /^;/) { next; }  # comment
            if ($line =~ /([^=]+)=([\S ]+)/) {
                  $k = uc($1);
                  $v = $2;
                  $k =~ s/\s+$//; $k =~ s/^\s+//;
                  $v =~ s/\s+$//; $v =~ s/^\s+//;
                  $$filed{$k} = $v;
            }
      }
      return;
}

sub read_keys() {
      local($ifile, $filed) = @_;
      local ($line,$k,$v);
      while ($line = <$ifile>) {
            if ($line =~ /^\[/) { return $line; }
            if ($line =~ /^;/) { next; }  # comment
            if ($line =~ /([\da-fA-F]*)(=*)([^,]+), *(\d+,) *([\S ]+)/)
{
                  $k = uc($3);
                  if ($2 eq "") { $k = uc($1 . $3); }
                  $v = $4 . $5;
                  $k =~ s/[\s"]+$//; $k =~ s/^[\s"]+//;
                  $v =~ s/\s+$//; $v =~ s/^\s+//;
                  $k =~ s/^($progfiles)/%PROGRAMFILES%/i;
                  $k =~ s/($sysdir)$/%SYSTEMDIRECTORY%/;
                  $k =~ s/^($sysroot)/%SYSTEMROOT%/;
                  $k =~ s/^($sysdrive)/%SYSTEMDRIVE%/;
                  $$filed{$k} = $v;
            }
      }
      return;
}
```


© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

## Appendix B

The following is a comparison of the templates **hisecweb** and **baseline** compiled using the **infdiff** perl script:

```
==== hisecweb.inf ====
    Application Log :
    Event Audit :
diff                AUDITOBJECTACCESS = 2
diff                AUDITPRIVILEGEUSE = 3
    Privilege Rights :
    Registry Values :
diff                MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM\LEGALNOTICECAPTION = 1,A
T T E N T I O N !
diff                MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM\LEGALNOTICETEXT = 1,This
is a private computer system. <add your own text using the MMC Security Templates tool>
diff                MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\LSA\FULLPRIVILEGEAUDITING = 3,1
diff                MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\LSA\LMCOMPATIBILITYLEVEL = 4,1
diff                MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\TCPIP\PARAMETERS\DISABLEIPSOURCEROUTING = 4,1
diff                MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\TCPIP\PARAMETERS\SYNATTACKPROTECT = 4,1
    Security Log :
diff                AUDITLOGRETENTIONPERIOD = 0
    Service General Setting :
diff                DHCP =
4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
diff                IISADMIN =
2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
diff                POLICYAGENT =
2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
diff                REMOTEREGISTRY =
4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
diff                W3SVC =
2,"D:AR(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;SY)"
    System Access :
    System Log :
    version :
==== baseline.inf ====
    Application Log :
    Event Audit :
diff                AUDITOBJECTACCESS = 3
diff                AUDITPRIVILEGEUSE = 2
    File Security :
    Registry Keys :
    Registry Values :
diff                MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM\LEGALNOTICECAPTION = 1,
diff                MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM\LEGALNOTICETEXT = 1,
diff                MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\LSA\FULLPRIVILEGEAUDITING = 3,0
diff                MACHINE\SYSTEM\CURRENTCONTROLSET\CONTROL\LSA\LMCOMPATIBILITYLEVEL = 4,5
diff                MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\TCPIP\PARAMETERS\DISABLEIPSOURCEROUTING = 4,2
diff                MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\TCPIP\PARAMETERS\SYNATTACKPROTECT = 4,2
    Security Log :
diff                AUDITLOGRETENTIONPERIOD = 2
    Service General Setting :
diff                DHCP =
2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
diff                IISADMIN =
4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
diff                POLICYAGENT =
4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
diff                REMOTEREGISTRY =
2,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
diff                W3SVC =
4,"D:(A;;CCLCSWLOCRRC;;;IU)(A;;GA;;;BA)(A;;GA;;;SY)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)"
    System Access :
    System Log :
    version :
==== done ====
```



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

## Appendix C

The following is a list of the file security configuration changes only carried out by the **baseline** template and not by the **hisecweb** template (compiled using the **infdiff** perl script):

```
only	%PROGRAMFILES% =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only	%SYSTEMDIRECTORY% =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)(A;CIOI;GRGX;;;WD)"
only	%SYSTEMDRIVE%\ =
2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;AU)(A;OICI;FA;;;SY)"
only	%SYSTEMDRIVE%\AUTOEXEC.BAT =
2,"D:PAR(A;CIOI;FA;;;BA)(A;CIOI;0x1200a9;;;AU)(A;CIOI;FA;;;SY)"
only	%SYSTEMDRIVE%\BOOT.INI = 2,"D:PAR(A;CIOI;FA;;;BA)(A;CIOI;FA;;;SY)"
only	%SYSTEMDRIVE%\CONFIG.SYS =
2,"D:P(A;CIOI;GXGR;;;AU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)"
only	%SYSTEMDRIVE%\DOCUMENTS AND SETTINGS = 1,"D:PAR"
only	%SYSTEMDRIVE%\INETPUB =
2,"D:PAR(A;OICI;FA;;;BA)(A;OICI;0x1200a9;;;WD)(A;OICI;FA;;;SY)"
only	%SYSTEMDRIVE%\IO.SYS = 2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)"
only	%SYSTEMDRIVE%\NTDETECT.COM = 2,"D:PAR(A;CIOI;FA;;;BA)(A;CIOI;FA;;;SY)"
only	%SYSTEMDRIVE%\NTLDR = 2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)"
only	%SYSTEMROOT% =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)(A;CIOI;GRGX;;;WD)"
only	%SYSTEMROOT%\ADDINS =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only	%SYSTEMROOT%\CONNECTION WIZARD =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only	%SYSTEMROOT%\CSC = 1,"D:AR"
only	%SYSTEMROOT%\DEBUG = 1,"D:AR"
only	%SYSTEMROOT%\DRIVER CACHE =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only	%SYSTEMROOT%\EXPLORER.EXE = 2,"D:(A;CIOI;GRGX;;;WD)"
only	%SYSTEMROOT%\JAVA =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only	%SYSTEMROOT%\MSAGENT =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only	%SYSTEMROOT%\OFFLINE PAGES = 1,"D:AR"
only	%SYSTEMROOT%\PROFILES = 1,"D:AR"
only	%SYSTEMROOT%\REGEDIT.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only	%SYSTEMROOT%\REGISTRATION = 1,"D:AR"
only	%SYSTEMROOT%\REPAIR = 2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only	%SYSTEMROOT%\SECURITY =
2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only	%SYSTEMROOT%\SPEECH =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only	%SYSTEMROOT%\SYSTEM32\APPEND.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only	%SYSTEMROOT%\SYSTEM32\APPMGMT = 1,"D:AR"
only	%SYSTEMROOT%\SYSTEM32\ARP.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only	%SYSTEMROOT%\SYSTEM32\AT.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only	%SYSTEMROOT%\SYSTEM32\ATTRIB.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only	%SYSTEMROOT%\SYSTEM32\CACLS.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only	%SYSTEMROOT%\SYSTEM32\CATROOT =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only	%SYSTEMROOT%\SYSTEM32\CHANGE.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only	%SYSTEMROOT%\SYSTEM32\CHCP.COM = 2,"D:PAR(A;OICI;FA;;;BA)"
only	%SYSTEMROOT%\SYSTEM32\CHGLOGON.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only	%SYSTEMROOT%\SYSTEM32\CHGPORT.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only	%SYSTEMROOT%\SYSTEM32\CHGUSER.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only	%SYSTEMROOT%\SYSTEM32\CHKDSK.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
```



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
only            %SYSTEMROOT%\SYSTEM32\CHKNTFS.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\CIPHER.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\CLUSTER.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\CMD.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\COMMAND.COM = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\COMPACT.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\CONFIG =
2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\SYSTEM32\CONVERT.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\CSCRIPT.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\DEBUG.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\DFSCMD.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\DHCP =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\SYSTEM32\DISKCOMP.COM = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\DISKCOPY.COM = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\DLLCACHE =
2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\SYSTEM32\DOSKEY.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\DRIVERS =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\SYSTEM32\DTCLOG = 1,"D:AR"
only            %SYSTEMROOT%\SYSTEM32\EDLIN.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\EXE2BIN.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\EXPAND.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\FC.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\FIND.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\FINDSTR.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\FINGER.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\FORCEDOS.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\FORMAT.COM = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\FTP.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\GROUPPOLICY = 1,"D:AR"
only            %SYSTEMROOT%\SYSTEM32\HOSTNAME.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\IAS =
2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\SYSTEM32\IISRESET.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\IPXROUTE.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\LABEL.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\LOGFILES =
2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\SYSTEM32\LOGOFF.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\LPQ.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\LPR.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\MAKECAB.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\MEM.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\MMC.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\MODE.COM = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\MORE.COM = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\MOUNTVOL.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\MSG.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\MUI =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\SYSTEM32\NBTSTAT.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\NET.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\NET1.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\NETSH.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\NETSTAT.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\NSLOOKUP.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\NTBACKUP.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\NTMSDATA = 1,"D:AR"
only            %SYSTEMROOT%\SYSTEM32\NTSD.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
```



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

```
only            %SYSTEMROOT%\SYSTEM32\PATHPING.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\PING.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\PRINT.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\QUERY.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\RASDIAL.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\RCP.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\RECOVER.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\REGEDT32.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\REGINI.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\REGISTER.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\REGSVR32.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\REINSTALLBACKUPS =
1,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\SYSTEM32\REPL =
1,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\SYSTEM32\REPLACE.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\REPL\EXPORT = 1,"D:(A;CIOI;GRGWGXSD;;;RE)"
only            %SYSTEMROOT%\SYSTEM32\REPL\IMPORT = 1,"D:(A;CIOI;GRGWGXSD;;;RE)"
only            %SYSTEMROOT%\SYSTEM32\RESET.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\REXEC.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\ROUTE.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\RSH.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\RUNAS.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\RUNONCE.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\SECEDIT.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\SETPWD.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\SETUP = 1,"D:AR"
only            %SYSTEMROOT%\SYSTEM32\SHADOW.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\SHARE.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\SHELLEXT =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\SYSTEM32\SNMP.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\SNMPTRAP.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\SPOOL\PRINTERS =
1,"D:P(A;CI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\SYSTEM32\SUBST.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\TELNET.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\TERMSRV.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\TFTP.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\TRACERT.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\TREE.COM = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\TSADMIN.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\TSCON.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\TSDISCON.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\TSKILL.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\TSPROF.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\TSSHUTDN.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\USRMGR.COM = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\WBEM =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\SYSTEM32\WBEM\MOF =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\SYSTEM32\WSCRIPT.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\SYSTEM32\XCOPY.EXE = 2,"D:PAR(A;OICI;FA;;;BA)"
only            %SYSTEMROOT%\TASKS = 1,"D:AR"
only            %SYSTEMROOT%\TEMP = 2,"D:P(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\TWAIN_32 =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
only            %SYSTEMROOT%\WEB =
2,"D:P(A;CIOI;GRGX;;;BU)(A;CIOI;GA;;;BA)(A;CIOI;GA;;;SY)(A;CIOI;GA;;;CO)"
```



© SANS Institute 2002, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 1st, 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 |