# Global Information Assurance Certification Paper

# The Impact of Cumulative Secure and High Secure Windows 2000 Professional Security Templates on a Workstation Running SCT Banner

**GCNT Version 3.0 rev 13AUG2001**


## By: Siegfried A. Hill GSEC, GCIH


As Microsoft's products have matured, their tools for managing them have matured as well. The security template file coupled with Microsoft's management tools and the power of group policy objects in Active Directory all make for an exciting opportunity to fine-tune the control and customization of security settings in Windows 2000. I have chosen the GCNT practical as an opportunity to apply some of what I have learned in this course to the workstations I manage daily as well as share some of the difficulties I encounter. Let's get started.

### THE WORKSTATION CONFIGURATION

The system I chose as the test bed for the security template was an OptiPlex GX110 mid-tower PC. The GX110 is an X-86 based PC produced by the Dell Computer Corporation. This particular model came installed with an Intel Pentium III 667 MHz processor, 256 megabytes of physical RAM, and a 15-gigabyte Maxtor hard drive with a single NTFS partition. The 3Com 3C920 Integrated Fast Ethernet Controller (network interface) and the Intel Corporation 810 Graphics Controller (video card) are standard adapters included onboard the OptiPlex GX110 mainboard. The BIOS is the ROM BIOS PLUS Version 1.10 A02 licensed from Phoenix. An optional Creative Labs AudioPCI (Ensonique) sound card was included on this workstation.

I prepared the workstation for simulation of my organization's office environment by using a stored disk image that I normally use to prepare workstations for new employees. The disk image is a Symantec Ghost 6.5 image of a clean-installed Windows 2000 professional workstation (Version 5.0.2195 Service Pack 2 Build 2195). Before imaging, all additional applications were installed and configured as much as possible. Only the TCP/IP network protocol was used, with NETBIOS enabled over TCP/IP. I used the Windows 2000 default TCP/IP settings with the exception of a static IP address, DNS, and WINS servers settings. I applied all Windows Update Critical Patches as of 27 NOV 2001. Before I imaged the workstation I ran Microsoft Sysprep version 1.1 to clear the SIDs and install the Microsoft Sysprep mini-setup wizard. For reference I include in the appendix an example of my SYSPREP.INF and the list of critical updates.

### THE ROLE OF THE WORKSTATION

The employees of my organization use a variety of tools to perform a diversity of job functions. Some of those people rely on one or more of these tools more extensively than others depending on the role they have to perform. On average, all of the tools must perform well in order for my organization to function smoothly.

We rely on the following applications:

| | |
|---|---|
| Browsers: | Netscape Navigator 4.72 and Internet Explorer 5.5 Service Pack 2 |
| Email: | Eudora 5.1 running under "Light" mode. |
| FTP: | WSFTP LE 5.06 FTP client |
| Secure Shell Telnet: | SecureCRT version 3.0.2 |
| PDF Viewer: | Adobe Acrobat 4.05 (plug-in and standalone) |
| Productivity: | Office 2000 Professional SP1 |
| Database Client: | SCT Banner client 5.2 (Oracle forms and runtime component) |
| Data Backup: | Retrospect Backup client 5.5 |
| Antivirus: | Norton Antivirus Corporate Edition 7.50.846 (Scan Engine 4.1.0.6) |
| Scheduling: | Meeting Maker client 6.0.7 |

Installed to their respective locations:

| | |
|---|---|
| Netscape Navigator | C:\Applications\Netscape\Communicator\ |
| Navigator Profiles | C:\Program Files\Netscape\Users\ |
| Internet Explorer | C:\Program Files\Internet Explorer\ |
| Eudora | C:\Applications\Qualcomm\Eudora\ |
| WSFTP LE | C:\Applications\WS_FTP\ |
| SecureCRT | C:\Applications\SecureCRT 3.0\ |
| Acrobat | C:\Applications\Adobe\Acrobat 4.0\ |
| Office 2000 | C:\Applications\Microsoft Office\ |
| Banner | C:\orant\ |
| Retrospect | C:\Program Files\Dantz\ |
| Antivirus | C:\Program Files\NavNT\ |
| Meeting Maker | C:\Applications\Meeting Maker\ |

In addition, we rely on Microsoft File Sharing. A great deal of my organization's work hinges upon the collaboration of employees electronically via shared files. Microsoft File Sharing is also an underlying technology for our implementation of the SCT Banner client.

In my organization, almost everyone has core tasks requiring heavy use of the SCT Banner program to input and retrieve enterprise-wide data. In addition, email could arguably be considered the communication medium most crucial to maintaining our flow of information both internally and to our external partners. These two core functions must stay up and running for our employees to perform their daily operations. SCT Banner requires Microsoft File Sharing because it relies on mapped drive shares to access Oracle forms. Secure Shell Telnet and FTP is required for our programming staff to access development platforms required to customize the Banner system. The remaining applications are fairly self-explanatory as they are standard productivity tools, with the exception of the antivirus and the data backup software. These applications require little intervention from the user, but still must function as an integral aspect of supporting the successful performance of the workstation as a whole.

## THE DESIRED LEVEL OF SECURITY

My perception of the threat level to my organization's information systems is one of healthy paranoia mixed with cautious optimism. I am inclined to think that securing all our workstations with the most restrictive security settings possible would be the best thing in this age of clever hackers and electronic espionage. At the same time I do not feel that my organization is of more than passing interest to a dedicated and well-trained hacker. Therefore I feel a moderate level of security that addresses most of the known vulnerabilities should discourage the less experienced "kiddie-scripters" who are likely to be probing my workstations and also "keep honest people honest" within the organization.

## THE WORKSTATION SECURITY REQUIREMENTS

I wanted the first major objective of the security template to be concerned with securing my generic office workstations against threats from the external network. My organization deals with personal information on a daily basis, maintains up-to-date computers on a high-speed, high-bandwidth link to the Internet, and sits on a public education (EDU) domain. This resource-rich environment -coupled with the poor security reputation that EDU environments traditionally suffer- means I should be prepared to defend against intrusion attempts on our system from outside the office network.

The second major concern I wanted the security template to address is the protection of office workstations from potential internal abuse and external intrusion via the console. I consider our personnel highly trustworthy and the level of access to information, with few exceptions, is uniform across the board. This means there is little or no expectation and no real incentive for an employee to attempt unauthorized access of information on another person's workstation. The greatest potential for abuse by our personnel comes from attempts to circumvent security in the interest of efficiency.

My organization employs the common cubicle-style office layout and consequently the available physical security for individual workstations is moderate to low. The cubicles are "public-access" areas in which it is possible for an unattended workstation to be briefly accessed during "down times" (such as lunch) without anyone noticing. This opens up a potential for external attacks on our workstations directly from the console. In a much more common scenario, the easy access to workstations also tempts personnel to "station hop". Station hopping typically occurs when an employee has a problem with their workstation or wants to use another workstation because the person that is currently logged in to that workstation has an elevated privilege for which the lower-privileged individual has a "one-time" need. Although the reasons for it in my organization are well intentioned, "station hopping" obfuscates auditing and provides many opportunities for security compromise. A classic example was the situation in which the workstation operator was very careful about email attachments and potential sources of virus infection. Despite the fact this person was extremely careful, an email-based virus -that *required* a user to double-click it- infected the system. Further forensics indicated that the workstation in question had been infected from a Hotmail account (not the victim's)

that had been checked during that person's day off. As far as I could tell, the unknown Hotmail user had briefly sat down and checked their mail on the workstation because it was logged in and a web browser was readily available.

## THE SECURITY TEMPLATE

I chose the incremental "hisecws.inf" and "securews.inf" combination from the default templates included with Windows 2000 because they represent a well-understood vendor baseline and because the combination effectively provides a good foundation for addressing my concern about intrusion from the external network. In addition, the combination includes some measures for securing the console.

Microsoft provides the following detail on these templates:

Chapter 13, Windows 2000 Professional Resource Kit [9]

> "The Secure template focuses on making operating system and network behavior more secure by changes such as removing all members of the Power Users group and requiring more secure passwords. The secure template does not focus on securing application behavior. This template does not modify permissions, so users with the proper permissions can still use legacy applications, even though all members are removed from the Power Users group by defining the Power Users group as a restricted group.
>
> The High Secure template increases the security defined by several of the parameters in the secure template. For example, while the Secure template might enable SMB Packet Signing, the High Secure template would require SMB packet signing. While the Secure template might warn on the installation of unsigned drivers, the High Secure template blocks the installation of unsigned drivers. In short, the High Secure template configures many operational parameters to their extreme values without regard for performance, operational ease of use, or connectivity with clients using third party or earlier versions of NTLM. The High Secure template also changes the default access permissions for Power Users to match those assigned to Users. This allows administrators to grant Users privileges reserved for Power Users, such as the ability to create shares, without having to give those users unnecessary access to the registry or file system. The High Secure template is primarily designed for use in an all-Windows 2000 network because the settings require Windows 2000 technology. Using High Secure templates in an environment with Windows 98 or Windows NT can

cause problems. "

Because I mostly deal with Windows 2000 workstations and servers, the limitations on communications with down-level clients did not bother me. The fact that communication is restricted when dealing with less secure and more commonly available down-level clients was encouraging to me because it reduces the amount of sources for potential intrusion. I wanted to take the opportunity and aim high with my security standards, then reduce them as needed, with an eye toward "denying all, allowing by exception".

Although a good overview, the Microsoft description of the templates was not good enough to give me a good idea of what I might be getting in for with these templates. Using the 'Security Configuration and Analysis' MMC, I combined the two above templates in one database and then exported the resulting combination to a template called "hisecws_differential.inf" (See Appendix). I then used the 'Security Templates' MMC to view the template and export the listing of each setting to a text file. I then concatenated the resulting collection of text files into a document so I could see in one flat file what I would be doing to the workstation. From this listing I got a good idea that the security template I had selected would improve my network security quite a bit. Unfortunately, I also discovered the template yielded less options than I had hoped for improving workstation security at the console.

Here is an explanation of the security settings enabled by the template that are relevant to my security concerns:

**Console security enhancements**

```
Security Options
Policy                                                  Computer Setting

Disable CTRL+ALT+DEL requirement for logon               Disabled
Do not display last user name in logon screen            Enabled
Smart card removal behavior                              Lock Workstation
```

The options available from any of this type of security template are very meager for configuring console security. The three settings that *are* in this template are not trivial, however.

*Security Options*

The first of these settings ensures that no unauthorized person can walk up to a logged-out workstation and sit down at it and start working. The fact that you are required to use a system-interrupt level key combination also provides some measure of certainty that a keystroke logger has not been installed to record your password when you log in. The next setting makes it just that much harder for an unauthorized person to try logging onto your station. If they do not know your password *and* they do not know your user ID, then it is that much harder for them to try and break in. The third and last setting is useful if you are using smart card technology in conjunction with or in replacement of passwords. This is actually a very nice option, but requires the installation of extra hardware and a user disciplined enough to remember to remove their smart card when they leave their computer. All of these settings rely on the user properly logging off the workstation for the security to work. In the case of my test workstation, the third setting

had no effect because I did not have a smart card reader installed on it.

**Network security enhancements:**

**Security Options**

| Policy | Computer Setting |
|---|---|
| Automatically log off users when logon time expires (local) | Enabled |
| Additional restrictions for anonymous connections | No access without explicit anonymous permissions |
| Digitally sign client communication (always) | Enabled |
| Digitally sign client communication (when possible) | Enabled |
| Digitally sign server communication (always) | Enabled |
| Digitally sign server communication (when possible) | Enabled |
| LAN Manager Authentication Level | Send NTLMv2 response only\refuse LM & NTLM |
| Secure channel: Digitally encrypt or sign secure channel data (always) | Enabled |
| Secure channel: Digitally encrypt secure channel data (when possible) | Enabled |
| Secure channel: Digitally sign secure channel data (when possible) | Enabled |
| Secure channel: Require strong (Windows 2000 or later) session key | Enabled |

The options for securing the network are more numerous than those for the console, and the settings enabled in the template have a greater positive impact.

*Security Options*

Automatically logging off users when logon times expire allows you to force off network users who are connected to the computer when their logon hours (not assignable through this template) are exceeded. Otherwise, the default action is to not allow users to logon outside of their logon time, but allow them to stay connected to the workstation after their logon time window has elapsed [1]. This strictly enforces usage times, helping you block any suspicious after-hours network activity. Additional restrictions for anonymous connections means that null user sessions to gather NETBIOS information and anonymous remote access to the registry will be blocked. This can negatively impact some down-level clients that require a null user session. Digitally sign client communication (always) and digitally sign server communication (always) both supercede their "(when possible)" counterpart settings. These settings force the requirement that server message block (SMB) communications of both the client and server services of the workstation be digitally signed with cryptographic keys. If unable to contact a similarly configured server or contacted by a client not using digitally signed SMB communications, the SMB communication will fail. It is important to note that SMB is the underlying basis for Microsoft File Sharing [2]. Secure channel encryption and signing (always) supercedes the other two settings that require those "(when possible)". This means that the workstation will always want to talk securely in "code" when attempting to connect to a domain controller. If the domain controller is unable to handle or not configured to offer digital encryption or digital signatures, the workstation will refuse to connect. This would be a Bad Thing. With this enabled all domain controllers must be running at least NT with Service Pack 4 [3]. The requirement for a strong session key ensures that any digitally encrypted or digitally signed communications uses a strong 128-bit cryptographic key to protect the communication between the workstation and the domain controller. Only Windows 2000 and later domain controllers have 128-bit session keys. All of these cryptographic requirements help prevent your network traffic from being intercepted and viewed, or even worse,

modified and reinserted onto the network. The digital signatures prevent communications from being tampered with and the encryption prevents the communications from being tapped. Last but not least, LAN Manager Authentication Level determines how well your network logon ID and password are protected as they are processed on the system and transmitted across the network. An improper value for this setting can make it trivial to reveal the most fiendishly crafted password in the world. The setting applied by this template prevents less secure down-level clients from getting passed your User ID and password in a less secure format. This means that Windows 95, Windows 98 and pre-Service Pack 4 NT workstations would need to be patched up before they could communicate properly with your workstation [4].

**Combined console and network security enhancements:**

**Password Policy**

| Policy | Computer Setting |
|---|---|
| Enforce password history | 24 passwords remembered |
| Maximum password age | 42 days |
| Minimum password age | 2 days |
| Minimum password length | 8 characters |
| Passwords must meet complexity requirements | Enabled |
| Store password using reversible encryption for all users in the domain | Disabled |

**Account Lockout Policy**

| Policy | Computer Setting |
|---|---|
| Account lockout duration | 0 |
| Account lockout threshold | 5 invalid logon attempts |
| Reset account lockout counter after | 30 minutes |

**Audit Policy**

| Policy | Computer Setting |
|---|---|
| Audit account logon events | Success, Failure |
| Audit account management | Success, Failure |
| Audit directory service access | Not defined |
| Audit logon events | Success, Failure |
| Audit object access | Success, Failure |
| Audit policy change | Success, Failure |
| Audit privilege use | Success, Failure |
| Audit process tracking | No auditing |
| Audit system events | Success, Failure |

The remaining settings of interest are ones that affect the system security as a whole and therefore are of interest for securing both the console and the network interface.

*Password Policy*

The password history requirement prevents users from reusing old passwords that may have been inadvertently revealed to an unauthorized user during the time they were in use. The maximum password age means that the user must select a new password after using the current one for 42 days. At one point this was thought to be a sufficiently short enough amount of time since brute force cracking attempts of encrypted passwords picked off the network could not be completed in under 42 days. This is not the case with the current level of technology. Even so, forcing a frequent change of the password can ameliorate the impact of such practices as "one-time" sharing of a password. Unfortunately, this can backfire by encouraging users to write their new password down

on a sticky note to remember it. In our organization I would prefer to go with a longer period to discourage the sticky note. A minimum password age of two days prevents a user from changing their password 24 times in one minute so they can go back to using their beloved favorite password. While the former steps help protect an account in case the password has already been compromised, the minimum password length of eight characters and the password complexity enforcement helps protect the password from being broken. The eight-character minimum does two things. If the password is to be handled at any time by an NT system, it will be processed into two seven-character chunks. If the password is seven characters or less, one of those chunks will be empty, reducing the task of cracking the password in half. The other thing an eight or more character password does is define the minimum number of permutations that the password could possibly be. The longer the password, the more random arrangements of letters a brute-force cracking program has to go through before finding the right combination. The password complexity requirement forces a password to use a diversity of characters to further increase the permutation space of the password. With this setting enabled, any new passwords created on the system must have at least three of the following four things: Uppercase characters, Lowercase characters, Symbols such as !@#$, and numbers. Storing passwords using reversible encryption means that you essentially have stored the passwords in a plain text file. This is another Bad Thing. This should always be disabled [5].

*Account Lockout Policy*

The account lockout policy settings prevent an unauthorized person from logging in from the network or the console by repeatedly trying to guess another person's password. This template configures the workstation so that after 5 consecutive failed attempts to logon, the account will be made temporarily unusable, or "locked out". The lockout duration value of zero means that the account will remain locked until an administrator unlocks it, and the reset counter value of 30 minutes means that if 30 minutes elapse between any of the failed attempts prior to a lockout, the counter for the number of consecutive failed attempts returns to 0. This setting is a bit restrictive for my organization because it could lead to denial of service by a hacker. Using an automated tool at 6:00 PM on a Friday, a hacker could quickly attempt to log onto all our accounts, 5 times each, with a blank password. A better setting would be for the account to automatically "unlock" after 30 minutes.

*Audit Policy*

The audit policy here is more aggressive than I need. Tracking all logon events (successes and failures) is important both to know when someone has been beating on your defenses and to know if they made it in or not. For the same reason, knowing other failed and successful operations is important. I would definitely change to “failures” those items set as "No auditing". If for nothing else, I want to be aware of trouble with the workstation. An important exception to the rule here of "more is better" would be system events, where successes are so frequent that the log would fill with trivial entries very quickly. My preference would be to set it to just log failures.

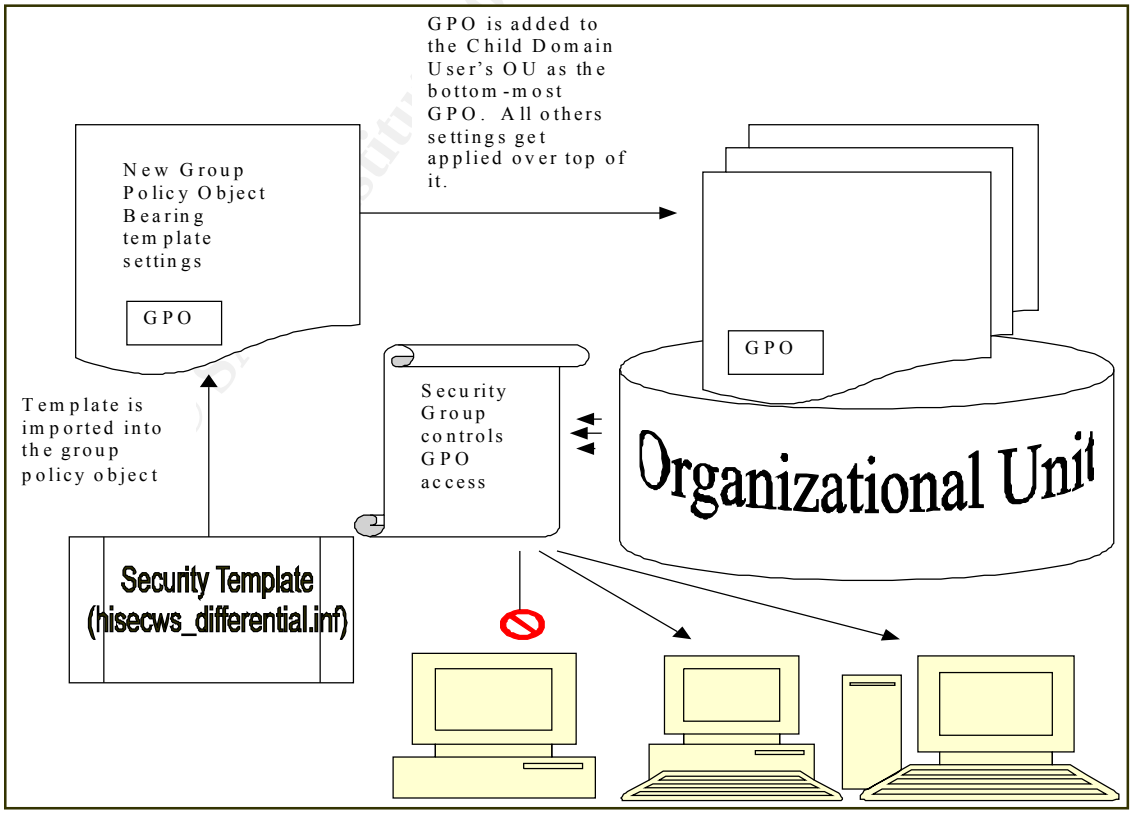
## How This Template Would Be Propagated and Maintained

I would apply this template to member workstations in a child domain of the enterprise using Active Directory group policy. The affected user accounts reside in the enterprise root domain and are contained in a single OU dedicated to the child domain's user subset. This OU has group policy management privileges delegated to the child domain administrator.

I would layer a new group policy object for the OU under the existing group policy objects. I would then import the combination template "hisecws_differential.inf" into 'Computer Configuration:Windows Settings:Security' for the new group policy object [6].

Access to this new group policy object (and therefore the security policy) would be controlled using membership in a universal security group, "HISECWS_DIFFERENTIAL", created for the policy. The ACLs set on the group policy object would include this new "HISECWS_DIFFERENTIAL" universal security group. The group policy object would be placed as a low, if not the lowest, priority group policy object so exceptions to the policy could be enabled as needed. This follows a "deny all, allow by exception" approach to applying the security measures. The policy would be installed or maintained and refreshed at each login and at the 90 +or- 30-minute default refresh interval for Active Directory group policy replication.

The security template would be distributed and maintained by importing it into a group policy object.



## TESTING FOR THE CORRECT APPLICATION OF THE SETTINGS

I decided to use bad logons, a null session connection, and down-level client drive-mapping to test for the correct application of the template. The settings I was trying to put through their paces were account lockout, additional restrictions for anonymous connections, and LAN Manager Authentication levels. The template passed these tests completely.

*Account lockout:*

To test the account lockout settings, I tried to log in at the console as user "JQPUBLIC" with an incorrect password. I was able to repeat this 5 times. On the sixth try I got the following error message:

> Error Message Title: Logon Message
> Error Message Body:
> "Unable to log you on because your account has been locked out,
> please contact your administrator. <OK>"

I waited two hours and then tried to log back in to see if the indefinite lockout was still in place. I got the same error message as above. When I opened the information for the user account under the 'Computer Management' MMC the account was marked as locked out. Resetting the account allowed me to log back on under the JQPUBLIC user account.

*Restricted Anonymous Logon*

I issued the following classic reconnaissance command from a Windows 2000 command prompt window:

> "net use \\hisecws\ipc$ /user:"

and had returned:

> "System error 67 has occurred.
> The network name cannot be found."

To make sure the IPC$ pipe was intact, I issued the command:

> "net use \\hisecws\ipc$ /user:administrator

and was prompted to provide a password for the account.

*LAN Manager Authentication Requirement*

To test the strict requirement for NTLMv2 authentication, I first attempted to map the administrative share \\hisecws\c$ from a Windows 2000 workstation using LM and NTLM authentication. It was not until I altered the mapping workstation's LAN Manager Authentication Level to "Send NTLMv2 response only" that I was able to successfully map the drive. When it was failing, the dialog box to put in a user ID and password would always return after attempting to submit my credentials. The session behaved as if I had provided the wrong user ID or password.

## THE STRESS TEST

I tested the following applications for normal operation:
SCT Banner client, Eudora Light, Netscape Navigator, Adobe Acrobat Reader, MeetingMaker, Norton Antivirus, Microsoft Word, SecureCRT, WSFTP LE, and Drive Mapping (file sharing).

*Some Special Test Considerations*

My machines participate in a Windows 2000 domain that applies Group Policy changes to the default computer security, so I had to take additional steps to prepare the test workstation. After running the mini-setup wizard and joining the PC to a workgroup instead of the domain, I applied the base system setup ("setup security.inf") template to restore the default security settings. I then cumulatively applied the secure ("securews.inf") and high secure ("hisecws.inf") templates. I then restarted the PC to ensure that the security policy changes were properly applied. I used the 'Security Configuration and Analysis' Microsoft Management Console (MMC) console to apply the "setup security.inf" template, combine and apply the "securews.inf" and "hisecws.inf" templates, and then later to troubleshoot the settings.

*The Testing Conditions*

I performed all testing while logged in under user "JQPUBLIC". "JQPUBLIC" only had membership in the Windows 2000 User local group. I evaluated event logs while logged in as "JQPUBLIC" using the 'runas' command to open an 'Event Viewer (local)' MMC console under the administrator account. I made all troubleshooting modifications while I was logged in under the local administrator account.

SCT Banner Oracle Client
* * * * * * * * * * * * * * * * * * * *

*The Test*

Log into and quit out of SCT Banner successfully.

*The Problem*

I immediately ran into trouble with the SCT Banner client, but not because of the Oracle Runtime component. Rather, a helper program written in-house was designed to modify a file with the assumption that the user has write privileges to the "%SystemRoot%\Program Files" folder. This is explicitly blocked for Users by the default Windows install and for Power Users by the template.

The same file and another couple of files included with the helper program's distribution also retained insufficient privileges for non-administrative users to run the helper program. The files were set with ACLs only for Administrators and the System. In addition, permissions inheritance was left unselected. Presumably these files had been copied to the distribution package from a folder location on the development platform that did not allow permissions inheritance.

*The Details*

The first error message I received was due to the incorrect privileges for the file to be

modified:

> Error Message Title: C:\Program Files\uu\md5.dll
> Error Message Body:
> "DLL File could not be created. Probable cause of error is that you cannot write to the disk or directory shown above. <OK>"
>
> -immediately followed by-
>
> Error Message Title: Fatal Error
> Error Message Body:
> "DLL(s) not found or created <OK>"

The error condition coincided with these event log entries:

> 2 consecutive Security Event Log entries:
> Source: Security
> Category: Privilege Use
> Event ID: 577
> Description:
> "Privilege Service Called:
>
> | | |
> |---|---|
> | Server: | Security |
> | Service: | - |
> | Primary User Name: | JQPUBLIC |
> | Primary Domain: | HISECWS |
> | Primary Logon ID: | (0x0,0x7D5DA) |
> | Client User Name: | - |
> | Client Domain: | - |
> | Client Logon ID: | - |
> | Privileges: | SeIncreaseBasePriorityPrivilege |

The error messages clearly pointed to the problem files and the event log entries hinted that the issue was an NTFS permissions problem.

*The Fix*
Setting the User local group's permission to "Modify" on the "md5.dll" file fixed the problem. I also reset the permissions inheritance on the other files to keep the application of ACLs consistent throughout the folder.

*Another Problem*
Once the helper program could readily access all the files it needed to run properly, I encountered a problem with the part of the process that maps a drive connection to a shared folder on a remote server. The error message implied a user ID problem; the server allows anonymous access, but refuses user IDs with names like Administrator or System because those are reserved account names. The error you get if you accidentally try to run the SCT Banner client while logged in under one of these accounts is identical

to the one I got this time.

*The Details*

> Error Message Title: Sorry...
> Error Message Body:
> "The current username and password is not allowed to connect to \\banner_servername\BANNER, would you like to try using a different username and password? <Yes><No><Cancel>"

I was stumped for a bit until I attempted to test Microsoft File Sharing by opening a shared folder on my own workstation. As a result of that investigation I recognized that the fix for that problem also fixed this problem with Banner.

Microsoft File Sharing
* * * * * * * * * * * * * * * * * * * *

*The Test*
Try to locate and open a shared folder on my personal workstation.

*The Problem*
I was stopped before I could even browse my machine in "Computers Near Me".

*The Details*
The error message I got was enigmatic, so I went to Microsoft's very useful http://www.technet.com and found a Q Article that pointed me in the right direction to look. I searched on the key phrase of the error message:

> Error Message Title: Computers Near Me
> Error Message Body:
> "\\computername is not accessible. The account is not authorized to log in from this station. <OK>"

*The Fix*
The phrase "account is not authorized to log in from this station" seemed odd to me since I wasn't trying to log into the secured workstation, but from it to another workstation. Even though this error message left much to the imagination, the Q Article 281648 it led to squarely placed the blame on one or more of the four security options that set the encryption of client and server communications on the workstation. By process of elimination I discovered that disabling the "Digitally sign client communication (always)" option fixes the problem. The option in question can be found in the Local Security Policy MMC - Security Settings:Local Policies:Security Options. This fix not only resolved the file sharing problem, but the Banner forms drive mapping as well [7].

Eudora Light 5.1 Email Client
* * * * * * * * * * * * * * * * * * * *

*The Test*
Send a message to myself. Check that message. Delete the message. Empty the trash mailbox. Look up my email address in Directory Services.

*The Problem*
I was disappointed that the normally portable and simple Eudora client crashed hard on me coming right out of the gate. I was 0 for 3 and not very happy. Eudora complained about not being able to access a component file and, once I closed that error message, the entire application proceeded to crash and burn complete with a Dr. Watson log entry. By now a veteran and somewhat suspicious, I checked the permissions on the file in question and discovered to my nasty surprise that the file in question had the same lack of permission inheritance that the troubling Banner helper file suffered from. The file, and a couple others that caused trouble after I fixed the first one, all are created on first use of Eudora. Had I not first run Eudora once while logged on as administrator, the program would not have crashed. However, the next normal user to try and share Eudora would have then suffered the fate I did as JQPUBLIC. The files are created with the permissions of the owner, of course, so they work for that person and any administrator. They do not inherit the permissions automatically to let other users share the same Eudora installation. This means that multiple users will not be able to use the same install of Eudora unless the permissions inheritance is checked for these files.

*The Details*
It wasn't pretty:

> Error Message Title: Eudora
> Error Message Body:
> "Could not open the file C:\Added
> Software\Qualcomm\Eudora\descmap.pce for reading.
> Cause: Access permission denied. File may be marked as read
> only or locked (13) <OK>"
>
> -immediately followed by-
>
> Error Message Title: Program Error
> Error Message Body:
> "Eudora.exe has generated errors and will be closed by Windows.
> You will need to restart the program. An error log is being
> created. <OK>"

The error condition coincided with these event log entries:

> Application Event Log entry:
> Source: Dr. Watson
> Event ID: 4097
> Description:
> "The application, , generated an application error The error

occurred on 11/27/2001 @ 21:13:36.208 The exception generated
was c0000005 at address 77E86674 (InterlockedDecrement)"

-and-

2 consecutive Security Event Log entries:
Source: Security
Category: Privilege Use
Event ID: 577
Description:
"Privilege Service Called:

| | |
|---|---|
| Server: | Security |
| Service: | - |
| Primary User Name: | JQPUBLIC |
| Primary Domain: | HISECWS |
| Primary Logon ID: | (0x0,0x7D5DA) |
| Client User Name: | - |
| Client Domain: | - |
| Client Logon ID: | - |
| Privileges: | SeIncreaseBasePriorityPrivilege |

*The Fix*
The files that were involved were "descmap.pce" and "LinkHistory.dat". Resetting them to inherit permissions and give the User local group "modify" privileges fixed the problem. I was then able to perform all the functions of the test successfully.

*More Trouble*
But I wasn't quite out of the woods. Upon closing Eudora, the following error message appeared:

Error Message Title: Eudora
Error Message Body:
"Could not rename file from
C:\DOCUME~1\JQPUBLIC\LOCALS~1\Temp\eudB8.tmp to
C:\Added Software\Qualcomm\Eudora\DsQuery.lst. <OK>"

-with-

2 consecutive Security Event Log entries:
Source: Security
Category: Privilege Use
Event ID: 577
Description:
"Privilege Service Called:

| | |
|---|---|
| Server: | Security |
| Service: | - |

| | |
|---|---|
| Primary User Name: | JQPUBLIC |
| Primary Domain: | HISECWS |
| Primary Logon ID: | (0x0,0x7D5DA) |
| Client User Name: | - |
| Client Domain: | - |
| Client Logon ID: | - |
| Privileges: | SeIncreaseBasePriorityPrivilege |

The file "DsQuery.lst" was Eudora's parting shot at me. It was presumably created as a by-product of the ldap Directory search I did as part of the test. Like the other two files, it was easy to fix by correcting the ACLs for it.

*Tech Tip*

A quick and dirty test to I used to see if inheritance was not set on all files:

- Select a group of files in question and call up the properties for all of them at once.
- Select the security tab. Look for an error message to pop up:

  Error Message Title: Security
  Error Message Body:
  "The permissions cannot be displayed because they are different between *filea.ext* and *fileb.ext*, .... Do you wish to reset the permissions on all the selected items? <Yes><No>"

  Click "<No>" and look to see what the security permissions differences might be. Keep in mind that this is a broad-brushed tool. Security differences can be subtle, such as a difference in object ownership or audit settings.

  Note: *filea.ext* and *fileb.ext* would be actually be the names of two of the selected files in question.

- If the error doesn't pop up, your files all have the same setting and can be ruled out.

Netscape 4.72 and Acrobat 4.01 Plug-in
* * * * * * * * * * * * * * * * * * * *

*The Test*

Open a Netscape browser session, manipulate and print from online Leave Entry and Reporting, and open a PDF document in the Acrobat Reader plug-in.

*The Problem*

I started the Netscape Navigator program and was prompted to create a new user profile. Not a good sign if I wanted to break my losing streak. The profile had been pre-setup before the machine was imaged. I went through the steps, changing the profile name to make a new profile in the same directory: "C:\Program Files\Netscape\Users\".

Optimistically, I clicked finish. 0 and 4. Netscape crashed and burned harder than Eudora.

*The Details*
I naturally started looking for obvious permission problems on the NTFS volume. For some reason unknown to me, Netscape will install to the folder I asked it to but still place the user profiles in the "%SystemRoot%\Program Files\" folder. This was my first area to target, but that was not effective at all.

> Error Message Title: Program Error
> Error Message Body:
> "netscape.exe has generated errors and will be closed by Windows.
> You will need to restart the program. An error log is being
> created. <OK>"
>
> -with-
>
> 2 consecutive Security Event Log entries:
> Source: Security
> Category: Privilege Use
> Event ID: 577
> Description:
> "Privilege Service Called:
>
> | | |
> |---|---|
> | Server: | Security |
> | Service: | - |
> | Primary User Name: | JQPUBLIC |
> | Primary Domain: | HISECWS |
> | Primary Logon ID: | (0x0,0x7D5DA) |
> | Client User Name: | - |
> | Client Domain: | - |
> | Client Logon ID: | - |
> | Privileges: | SeIncreaseBasePriorityPrivilege |

*The Fix*
The event logs were not helping me much with this one, so I decided to set auditing on the HKLM\Software key to see if there was some problem with Netscape's access to the registry. After not making much progress with this, I decided to drop back and punt with a Google Search on the web. Within 10 minutes I had the offending registry permissions and the permissions on the single file buried in "%SystemRoot%\WINNT\" all straightened out [8].

The registry keys and the action Netscape was trying to perform on them are in the table below. (This is excerpted from the web page [8]). The permissions that need to be set are "modify" and you must be sure to go into the "advanced" screen and check the box that forces the permissions to be copied to all child objects.

In the case of the HKEY_Classes_Root (HKCR) hive entries that have CLSID as the subkey, the proper permissions should be set on the enclosing key, not the subkey CLSID. For example, if you are setting the permission on "HKCR\Netscape.Registry.1\CLSID", you would apply the registry permissions to "HKCR\Netscape.Registry.1" and force the permissions to copy down to the CLSID subkey. For all others, the key indicated will be the key that you want to assign permissions to. If you wish, you may try to optimize the amount of permission you give the User group by using as a guide the action that the webpage's author indicated Netscape was attempting.

**Netscape Registry Permission Targets**

CreateKey
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm

CreateKey
HKLM\System\CurrentControlSet\Control\MediaProperties\PrivateProperties\Joystick\Winmm

OpenKey
HKLM\SOFTWARE\Netscape\Netscape Navigator\Users\

CreateKey
HKCR\CLSID\{481ED670-9D30-11ce-8F9B-0800091AC64E}

OpenKey
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\App Paths\netscape.exe

CreateKey
HKCR\Netscape.TalkNav.1\CLSID

CreateKey
HKCR\Netscape.Registry.1\CLSID

CreateKey
HKCR\Netscape.Help.1\CLSID

CreateKey
HKCR\Netscape.Network.1\CLSID

CreateKey
HKCR\NetscapeMarkup\CLSID

CreateKey
HKCR\CLSID\{61D8DE20-CA9A-11CE-9EA5-0080C82BE3B6}\ProgID

The single file for which permissions need adjusting is the "nsreg.dat" and it resides in the C:\WINNT folder. This file needs to be set to "modify" for the Users local group. Once I patched up the permissions for Netscape, I was able to perform all the tests of Netscape Navigator successfully.

MeetingMaker 6.0.7
* * * * * * * * * * * * * * * * * * * *

*The Test*
Open, configure, and log on to a MeetingMaker calendar session.

*The Result*
All systems go! My losing streak was broken. I successfully configured, selected, and logged on to a server and retrieved my schedule.

*The Rest is History*
Norton Antivirus Corporate Edition 7.50.846 (Scan Engine 4.1.0.6)
* * * * * * * * * * * * * * * * * * * *

The automatic LiveUpdate of the virus definitions were successful. I was able to successfully initiate a manual scan of the C: drive.

Microsoft Word 2000 (9.0.3821 SR-1)
* * * * * * * * * * * * * * * * * * * *

I was able to open a blank document, enter text, and save it successfully. I then opened the same document, edited it, and saved it successfully. For good measure I spell-checked and printed the document successfully.

SecureCRT 3.0.2
* * * * * * * * * * * * * * * * * * * *

I successfully configured SecureCRT with the licensing information and session configuration data. I then logged into the development server with a secure telnet session without incident. I successfully configured an FTP port forward to work with WSFTP LE.

WSFTP_LE 5.06
* * * * * * * * * * * * * * * * * * * *

I successfully configured a localhost session to work with the SecureCRT session. I then successfully logged into the development server through the SecureCRT port forwarding. I successfully transferred files to and from the server as well as successfully deleting remote and local files.

## IN CONCLUSION

I would say the template performed the security role it was designed for very well, but as it currently stands it could not be deployed on my organizations' workstations. The fact that it forced the Power User group into the User group's privilege role means that many of the default permissions taken for granted by our core software –Eudora, Banner, and Netscape- were not available. In a few areas noted earlier, such as password duration and the client communication encryption the template was a little too aggressive. I think the shortcomings of the template are not insurmountable and are all due to the conditions required by the applications installed on the workstation. I think the adjustments to make this template quite functional are rather minor, and ones that mostly focus on the proper configuration of the ACLs for the User local group account. I would recommend including the specific registry key and file permission modifications needed to make Banner, Eudora, and Netscape function under the User account as a smaller add-on "compatibility" template. This could then be tweaked as needed to meet the changes of the particular programs.

I would have to remove from the original template the security option forcing client communication to always be encrypted. Otherwise file sharing and Banner will not function properly. If, at some time in the future, the Banner form servers enable encryption, I could quickly restore the setting. The registry and file permission changes are so trivial that their impact on the workstation security is negligible. The client encryption being optional will reduce the SMB communication security somewhat, but at this time the cost of keeping it is too great.

The option for using the template as a documented and physical file that then can be imported by layers into the group policy is a great thing for gaining visibility on my various layers of organization security policy while at the same time gathering them into one pot. The only area I would like to see improved is the template formatted into a more human-readable document. Something that looks more like an XML file would be nicer.

After an initial struggle configuring the permissions, the combination template of Secure and High Secure templates improved the level of security on the test workstation without adversely impacting the operation of the workstation.

## REFERENCES


[1] Windows NT/2000 Tips, Tricks, Registry Hacks and more... 4235 » The 'Automatically log off users when logon time expires' Group Policy should be re-titled?, 2001
URL: http://www.jsiinc.com/SUBI/tip4200/rh4235.htm (29 NOV 2001)

[2] Microsoft network client: Digitally sign communications (always), 2001
URL:http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/proddocs/568.asp
(29 NOV 2001)

[3] Microsoft description of "Domain member: Digitally encrypt or sign secure channel data (always)", 2001
URL:http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/proddocs/587.asp
(29 NOV 2001)

[4] Microsoft description of "Network security: LAN Manager authentication level", 2001
URL:
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/proddocs/576.asp
(29 NOV 2001)

[5] Microsoft description of "Store password using reversible encryption for all users in the domain", 2001
URL:http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/winxppro/proddocs/505.asp
(29 NOV 2001)

[6] Methods Used to Apply Security Settings Throughout an Enterprise (Q216735), 18 OCT 2001
URL: http://support.microsoft.com/support/kb/articles/Q216/7/35.ASP
(29 NOV 2001)

[7] Error Message: The Account Is Not Authorized to Login from This Station (Q281648), 17 MAR 2001
URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q281648
(29 NOV 2001)

[8] Netscape v4.72 on Windows 2000, 5 JUL 2001
URL: http://duke.usask.ca/~uhl/netscape/netscape472.html (29 NOV 2001)

[9] Chapter 13, Windows 2000 Professional Resource Kit, 2001
URL:
http://www.microsoft.com/technet/prodtechnol/windows2000pro/reskit/part3/proch13.asp
(29 NOV 2001)

# APPENDIX

### *Critical Updates Installed*

- Security Update, November 20, 2001 "Windows Media Player .asf processor contains unchecked buffer" MS01-56
- Security Update, November 13, 2001 "13 NOV Cumulative Patch for Internet Explorer" MS01-055
- Security Update, June 7, 2001 "Predictable Name Pipes Could Enable Privilege Elevation via Telnet" MS01-031
- Windows 2000 Service Pack 2
- Internet Explorer 5.5 Service Pack 2 and Internet Tools
- High Encryption Pack for Windows 2000

### *Sample of Sysprep.inf File Used for Test Configuration*

```
;SetupMgrTag
[Unattended]
    InstallFilesPath=C:\sysprep\i386
    TargetPath=\WINNT
    OemSkipEula = Yes
[GuiUnattended]
    OEMSkipRegional=1
    TimeZone=35
    OemSkipWelcome = 1
    OEMDuplicatorstring=GX110_GhostImage_ZIG27NOV2001
[UserData]
    FullName="Authorized User"
    OrgName=University Development, Virginia Tech
    ProductID=XXXXX-XXXXX-XXXXX-XXXXXX-XXXXX
[Branding]
    BrandIEUsingUnattended = Yes
[URL]
    Home_Page = http://www.vt.edu/
[FavoritesEx]
    Title1 = "Va. Tech Computer Help Center.url"
    URL1 = "http://www.ucs.vt.edu/"
[Display]
    BitsPerPel=16
    Xresolution=800
    YResolution=600
    Vrefresh=75
[RegionalSettings]
    LanguageGroup=1
[OEM_Ads]
    Background=WarMemorial.bmp
[SetupMgr]
    DistFolder=C:\sysprep\i386
    DistShare=win2000dist
[Identification]
    JoinDomain=XXXXXXXXXX
[Networking]
    InstallDefaultComponents=No
[NetClients]
    MS_MSClient=params.MS_MSClient
```

### *Securews.inf and Hisecws.inf combined into Hisecws_differential*

```
[Unicode]
Unicode=yes
[System Access]
```

```
MinimumPasswordAge = 2
MaximumPasswordAge = 42
MinimumPasswordLength = 8
PasswordComplexity = 1
PasswordHistorySize = 24
LockoutBadCount = 5
ResetLockoutCount = 30
LockoutDuration = -1
RequireLogonToChangePassword = 0
ClearTextPassword = 0
[System Log]
RestrictGuestAccess = 1
[Security Log]
MaximumLogSize = 10240
AuditLogRetentionPeriod = 0
RestrictGuestAccess = 1
[Application Log]
RestrictGuestAccess = 1
[Event Audit]
AuditSystemEvents = 3
AuditLogonEvents = 3
AuditObjectAccess = 3
AuditPrivilegeUse = 3
AuditPolicyChange = 3
AuditAccountManage = 3
AuditProcessTracking = 0
AuditAccountLogon = 3
[Registry Values]
machine\system\currentcontrolset\services\netlogon\parameters\signsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\sealsecurechannel=4,1
machine\system\currentcontrolset\services\netlogon\parameters\requirestrongkey=4,1
machine\system\currentcontrolset\services\netlogon\parameters\requiresignorseal=4,1
machine\system\currentcontrolset\services\netlogon\parameters\disablepasswordchange=4,0
machine\system\currentcontrolset\services\lanmanworkstation\parameters\requiresecuritysig
nature=4,1
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enablesecuritysign
ature=4,1
machine\system\currentcontrolset\services\lanmanworkstation\parameters\enableplaintextpas
sword=4,0
machine\system\currentcontrolset\services\lanmanserver\parameters\requiresecuritysignatur
e=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\enablesecuritysignature
=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\enableforcedlogoff=4,1
machine\system\currentcontrolset\services\lanmanserver\parameters\autodisconnect=4,15
machine\system\currentcontrolset\control\session manager\protectionmode=4,1
machine\system\currentcontrolset\control\session manager\memory
management\clearpagefileatshutdown=4,1
machine\system\currentcontrolset\control\print\providers\lanman print
services\servers\addprinterdrivers=4,1
machine\system\currentcontrolset\control\lsa\restrictanonymous=4,2
machine\system\currentcontrolset\control\lsa\lmcompatibilitylevel=4,5
machine\system\currentcontrolset\control\lsa\fullprivilegeauditing=3,0
machine\system\currentcontrolset\control\lsa\crashonauditfail=4,0
machine\system\currentcontrolset\control\lsa\auditbaseobjects=4,0
machine\software\microsoft\windows\currentversion\policies\system\legalnoticetext=1,
machine\software\microsoft\windows\currentversion\policies\system\legalnoticecaption=1,
machine\software\microsoft\windows\currentversion\policies\system\dontdisplaylastusername
=4,1
machine\software\microsoft\windows\currentversion\policies\system\disablecad=4,0
machine\software\microsoft\windows nt\currentversion\winlogon\scremoveoption=1,1
machine\software\microsoft\windows nt\currentversion\winlogon\passwordexpirywarning=4,14
machine\software\microsoft\windows nt\currentversion\winlogon\cachedlogonscount=1,10
machine\software\microsoft\windows nt\currentversion\winlogon\allocatefloppies=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatedasd=1,0
machine\software\microsoft\windows nt\currentversion\winlogon\allocatecdroms=1,0
machine\software\microsoft\windows nt\currentversion\setup\recoveryconsole\setcommand=4,0
machine\software\microsoft\windows
nt\currentversion\setup\recoveryconsole\securitylevel=4,0
machine\software\microsoft\non-driver signing\policy=3,0
machine\software\microsoft\driver signing\policy=3,2
```

```
[Group Membership]
*S-1-5-32-547__Memberof =
*S-1-5-32-547__Members =
[Registry Keys]
"users\.default\software\microsoft\protected storage system provider",1,"D:AR"
"users\.default\software\microsoft\netdde",2,"D:P(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;C
O)"
"users\.default",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;
;CO)"
"machine\system\currentcontrolset\services\tcpip",2,"D:(A;CI;GR;;;WD)"
"machine\system\currentcontrolset\services\eventlog",2,"D:(A;CI;GR;;;WD)"
"machine\system\currentcontrolset\hardware profiles",1,"D:AR"
"machine\system\currentcontrolset\enum",1,"D:AR"
"machine\system\currentcontrolset\control\wmi\security",2,"D:P(A;CI;GR;;;BA)(A;CI;GA;;;SY
)(A;CI;GA;;;CO)"
"machine\system\currentcontrolset\control\securepipeservers\winreg",2,"D:P(A;CI;GA;;;BA)(
A;;GR;;;BO)"
"machine\system\currentcontrolset\control\productoptions",2,"D:(A;CI;GR;;;WD)"
"machine\system\currentcontrolset\control\print\printers",2,"D:(A;CI;GR;;;WD)"
"machine\system\currentcontrolset\control\keyboard layouts",2,"D:(A;CI;GR;;;WD)"
"machine\system\currentcontrolset\control\keyboard layout",2,"D:(A;CI;GR;;;WD)"
"machine\system\currentcontrolset\control\contentindex",2,"D:(A;CI;GR;;;WD)"
"machine\system\currentcontrolset\control\computername",2,"D:(A;CI;GR;;;WD)"
"machine\system\controlset010",1,"D:AR"
"machine\system\controlset009",1,"D:AR"
"machine\system\controlset008",1,"D:AR"
"machine\system\controlset007",1,"D:AR"
"machine\system\controlset006",1,"D:AR"
"machine\system\controlset005",1,"D:AR"
"machine\system\controlset004",1,"D:AR"
"machine\system\controlset003",1,"D:AR"
"machine\system\controlset002",1,"D:AR"
"machine\system\controlset001",1,"D:AR"
"machine\system\clone",1,"D:AR"
"machine\system",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;
;CO)"
"machine\software\microsoft\windows\currentversion\policies",1,"D:AR"
"machine\software\microsoft\windows\currentversion\installer",1,"D:AR"
"machine\software\microsoft\windows\currentversion\group policy",1,"D:AR"
"machine\software\microsoft\windows
nt\currentversion\winlogon",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY
)(A;CI;GA;;;CO)"
"machine\software\microsoft\windows
nt\currentversion\windows",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)
(A;CI;GA;;;CO)"
"machine\software\microsoft\windows nt\currentversion\time
zones",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"machine\software\microsoft\windows
nt\currentversion\svchost",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)
(A;CI;GA;;;CO)"
"machine\software\microsoft\windows
nt\currentversion\setup\recoveryconsole",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)
(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"machine\software\microsoft\windows
nt\currentversion\secedit",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)
(A;CI;GA;;;CO)"
"machine\software\microsoft\windows
nt\currentversion\profilelist",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;
;SY)(A;CI;GA;;;CO)"
"machine\software\microsoft\windows nt\currentversion\perflib\009",1,"D:AR"
"machine\software\microsoft\windows
nt\currentversion\perflib",2,"D:P(A;CI;GR;;;IU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)
"
"machine\software\microsoft\windows
nt\currentversion\inifilemapping",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;G
A;;;SY)(A;CI;GA;;;CO)"
"machine\software\microsoft\windows nt\currentversion\image file execution
options",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"machine\software\microsoft\windows
nt\currentversion\fontmapper",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;
SY)(A;CI;GA;;;CO)"
```

```
"machine\software\microsoft\windows nt\currentversion\font
drivers",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"machine\software\microsoft\windows
nt\currentversion\efs",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;C
I;GA;;;CO)"
"machine\software\microsoft\windows
nt\currentversion\drivers32",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;S
Y)(A;CI;GA;;;CO)"
"machine\software\microsoft\windows
nt\currentversion\classes",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)
(A;CI;GA;;;CO)"
"machine\software\microsoft\windows
nt\currentversion\asrcommands",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;
;SY)(A;CI;GA;;;CO)(A;CI;SDGWGR;;;BO)"
"machine\software\microsoft\windows
nt\currentversion\aedebug",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)
(A;CI;GA;;;CO)"
"machine\software\microsoft\windows
nt\currentversion\accessibility",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA
;;;SY)(A;CI;GA;;;CO)"
"machine\software\microsoft\windows nt\currentversion",2,"D:(A;CI;GR;;;WD)"
"machine\software\microsoft\systemcertificates",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;G
A;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"machine\software\microsoft\secure",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI
;GA;;;SY)(A;CI;GA;;;CO)"
"machine\software\microsoft\protected storage system provider",1,"D:AR"
"machine\software\microsoft\netdde",2,"D:P(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA;;;CO)"
"machine\software\classes",2,"D:(A;CI;GR;;;WD)"
"machine\software",2,"D:P(A;CI;GR;;;BU)(A;CI;GR;;;PU)(A;CI;GA;;;BA)(A;CI;GA;;;SY)(A;CI;GA
;;;CO)"
[File Security]
"c:\winnt\web",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)
(A;OICI;GA;;;CO)"
"c:\winnt\twain_32",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;
;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\temp",2,"D:P(A;CI;0x100026;;;BU)(A;CI;0x100026;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;
;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\tasks",1,"D:AR"
"c:\winnt\system32\wbem\mof",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A
;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\system32\wbem",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OIC
I;GA;;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\system32\spool\printers",1,"D:P(A;CI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;B
A)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\system32\shellext",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A
;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\system32\setup",1,"D:AR"
"c:\winnt\system32\repl\import",1,"D:(A;OICI;SDGXGWGR;;;RE)"
"c:\winnt\system32\repl\export",1,"D:(A;OICI;SDGXGWGR;;;RE)"
"c:\winnt\system32\repl",1,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OIC
I;GA;;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\system32\reinstallbackups",1,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA
;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\system32\ntmsdata",1,"D:AR"
"c:\winnt\system32\mui",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI
;GA;;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\system32\ias",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\system32\grouppolicy",1,"D:AR"
"c:\winnt\system32\dtclog",1,"D:AR"
"c:\winnt\system32\drivers",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;
OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\system32\dllcache",2,"D:P(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\system32\dhcp",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OIC
I;GA;;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\system32\config",2,"D:P(A;CI;GXGR;;;BU)(A;CI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;
GA;;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\system32\catroot",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;
OICI;GA;;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\system32\appmgmt",1,"D:AR"
"c:\winnt\system32",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;
;;SY)(A;OICI;GA;;;CO)(A;OICI;GXGR;;;WD)"
```

```
"c:\winnt\speech",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;
SY)(A;OICI;GA;;;CO)"
"c:\winnt\security",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;
;;SY)(A;OICI;GA;;;CO)"
"c:\winnt\repair",2,"D:P(A;CI;GXGR;;;BU)(A;CI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(
A;OICI;GA;;;CO)"
"c:\winnt\registration",1,"D:AR"
"c:\winnt\profiles",1,"D:AR"
"c:\winnt\offline pages",1,"D:AR"
"c:\winnt\msagent",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;
;SY)(A;OICI;GA;;;CO)"
"c:\winnt\java",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY
)(A;OICI;GA;;;CO)"
"c:\winnt\explorer.exe",2,"D:(A;;GXGR;;;WD)"
"c:\winnt\driver
cache",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;
GA;;;CO)"
"c:\winnt\debug",1,"D:AR"
"c:\winnt\csc",1,"D:AR"
"c:\winnt\connection
wizard",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI
;GA;;;CO)"
"c:\winnt\addins",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;
SY)(A;OICI;GA;;;CO)"
"c:\winnt",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;O
ICI;GA;;;CO)(A;;GXGR;;;WD)"
"c:\program
files",2,"D:P(A;OICI;GXGR;;;BU)(A;OICI;GXGR;;;PU)(A;OICI;GA;;;BA)(A;OICI;GA;;;SY)(A;OICI;
GA;;;CO)"
"c:\ntldr",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"c:\ntdetect.com",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"c:\ntbootdd.sys",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"c:\config.sys",2,"D:P(A;;GXGR;;;BU)(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"c:\boot.ini",2,"D:P(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
"c:\autoexec.bat",2,"D:P(A;;GXGR;;;BU)(A;;GXGR;;;PU)(A;;GA;;;BA)(A;;GA;;;SY)"
[Version]
signature="$CHICAGO$"
Revision=1
```

### *Summary of Hisecws_differential.inf Policies and Computer Settings*

(Note: registry and file system listings have been ommitted.)

**Password Policy**

| Policy | Computer Setting |
|---|---|
| Enforce password history | 24 passwords remembered |
| Maximum password age | 42 days |
| Minimum password age | 2 days |
| Minimum password length | 8 characters |
| Passwords must meet complexity requirements | Enabled |
| Store password using reversible encryption for all users in the domain | Disabled |

**Account Lockout Policy**

| Policy | Computer Setting |
|---|---|
| Account lockout duration | 0 |
| Account lockout threshold | 5 invalid logon attempts |
| Reset account lockout counter after | 30 minutes |

**Kerberos Policy**

| Policy | Computer Setting |
|---|---|
| Enforce user logon restrictions | Not defined |
| Maximum lifetime for service ticket | Not defined |
| Maximum lifetime for user ticket | Not defined |
| Maximum lifetime for user ticket renewal | Not defined |
| Maximum tolerance for computer clock synchronization | Not defined |

**Audit Policy**

| Policy | Computer Setting |
|---|---|
| Audit account logon events | Success, Failure |
| Audit account management | Success, Failure |
| Audit directory service access | Not defined |
| Audit logon events | Success, Failure |
| Audit object access | Success, Failure |
| Audit policy change | Success, Failure |
| Audit privilege use | Success, Failure |
| Audit process tracking | No auditing |
| Audit system events | Success, Failure |

**User rights assignments**

| Policy | Computer Setting |
|---|---|
| Access this computer from the network | Not defined |
| Act as part of the operating system | Not defined |
| Add workstations to domain | Not defined |
| Back up files and directories | Not defined |
| Bypass traverse checking | Not defined |
| Change the system time | Not defined |
| Create a pagefile | Not defined |
| Create a token object | Not defined |
| Create permanent shared objects | Not defined |
| Debug programs | Not defined |
| Deny access to this computer from the network | Not defined |
| Deny logon as a batch job | Not defined |
| Deny logon as a service | Not defined |
| Deny logon locally | Not defined |
| Enable computer and user accounts to be trusted for delegation | Not defined |
| Force shutdown from a remote system | Not defined |
| Generate security audits | Not defined |
| Increase quotas | Not defined |
| Increase scheduling priority | Not defined |
| Load and unload device drivers | Not defined |
| Lock pages in memory | Not defined |
| Log on as a batch job | Not defined |
| Log on as a service | Not defined |
| Log on locally | Not defined |
| Manage auditing and security log | Not defined |
| Modify firmware environment values | Not defined |
| Profile single process | Not defined |
| Profile system performance | Not defined |
| Remove computer from docking station | Not defined |
| Replace a process level token | Not defined |
| Restore files and directories | Not defined |
| Shut down the system | Not defined |
| Synchronize directory service data | Not defined |
| Take ownership of files or other objects | Not defined |

**Security Options**

| Policy | Computer Setting |
|---|---|
| Additional restrictions for anonymous connections | No access without explicit anonymous permissions |
| Allow server operators to schedule tasks (domain controllers only) | Not defined |
| Allow system to be shut down without having to log on | Not defined |
| Allowed to eject removable NTFS media | Administrators |
| Amount of idle time required before disconnecting session | 15 minutes |
| Audit the access of global system objects | Disabled |
| Audit use of Backup and Restore privilege | Disabled |
| Automatically log off users when logon time expires | Not defined |
| Automatically log off users when logon time expires (local) | Enabled |
| Clear virtual memory pagefile when system shuts down | Enabled |
| Digitally sign client communication (always) | Enabled |
| Digitally sign client communication (when possible) | Enabled |
| Digitally sign server communication (always) | Enabled |

| | |
|---|---|
| Digitally sign server communication (when possible) | Enabled |
| Disable CTRL+ALT+DEL requirement for logon | Disabled |
| Do not display last user name in logon screen | Enabled |
| LAN Manager Authentication Level | Send NTLMv2 response only\refuse LM & NTLM |
| Message text for users attempting to log on | <BLANK> |
| Message title for users attempting to log on | <BLANK> |
| Number of previous logons to cache (in case domain controller is not available) | 10 logons |
| Prevent system maintenance of computer account password | Disabled |
| Prevent users from installing printer drivers | Enabled |
| Prompt user to change password before expiration | 14 days |
| Recovery Console: Allow automatic administrative logon | Disabled |
| Recovery Console: Allow floppy copy and access to all drives and all folders | Disabled |
| Rename administrator account | Not defined |
| Rename guest account | Not defined |
| Restrict CD-ROM access to locally logged-on user only | Disabled |
| Restrict floppy access to locally logged-on user only | Disabled |
| Secure channel: Digitally encrypt or sign secure channel data (always) | Enabled |
| Secure channel: Digitally encrypt secure channel data (when possible) | Enabled |
| Secure channel: Digitally sign secure channel data (when possible) | Enabled |
| Secure channel: Require strong (Windows 2000 or later) session key | Enabled |
| Secure system partition (for RISC platforms only) | Not defined |
| Send unencrypted password to connect to third-party SMB servers | Disabled |
| Shut down system immediately if unable to log security audits | Disabled |
| Smart card removal behavior | Lock Workstation |
| Strengthen default permissions of global system objects (e.g. Symbolic Links) | Enabled |
| Unsigned driver installation behavior | Do not allow installation |
| Unsigned non-driver installation behavior | Silently succeed |

**Settings for Event Logs**

| Policy | Computer Setting |
|---|---|
| Maximum application log size | Not defined |
| Maximum security log size | 10240 kilobytes |
| Maximum system log size | Not defined |
| Restrict guest access to application log | Enabled |
| Restrict guest access to security log | Enabled |
| Restrict guest access to system log | Enabled |
| Retain application log | Not defined |
| Retain security log | Not defined |
| Retain system log | Not defined |
| Retention method for application log | Not defined |
| Retention method for security log | As needed |
| Retention method for system log | Not defined |
| Shut down the computer when the security audit log is full | Not defined |

**Restricted Groups**

| Group Name | Members | Member Of |
|---|---|---|
| Power Users | | |

**System Service**

| Service Name | Startup | Permission |
|---|---|---|
| Alerter | Not defined | Not defined |
| Application Management | Not defined | Not defined |
| ClipBook | Not defined | Not defined |
| COM+ Event System | Not defined | Not defined |
| Computer Browser | Not defined | Not defined |
| DefWatch | Not defined | Not defined |
| DHCP Client | Not defined | Not defined |
| Distributed Link Tracking Client | Not defined | Not defined |
| Distributed Transaction Coordinator | Not defined | Not defined |
| DNS Client | Not defined | Not defined |
| Event Log | Not defined | Not defined |
| Fax Service | Not defined | Not defined |

| | | |
|---|---|---|
| Indexing Service | Not defined | Not defined |
| Internet Connection Sharing | Not defined | Not defined |
| IPSEC Policy Agent | Not defined | Not defined |
| Logical Disk Manager | Not defined | Not defined |
| Logical Disk Manager Administrative Service | Not defined | Not defined |
| Messenger | Not defined | Not defined |
| Net Logon | Not defined | Not defined |
| NetMeeting Remote Desktop Sharing | Not defined | Not defined |
| Network Connections | Not defined | Not defined |
| Network DDE | Not defined | Not defined |
| Network DDE DSDM | Not defined | Not defined |
| Norton AntiVirus Client | Not defined | Not defined |
| NT LM Security Support Provider | Not defined | Not defined |
| Performance Logs and Alerts | Not defined | Not defined |
| Plug and Play | Not defined | Not defined |
| Print Spooler | Not defined | Not defined |
| Protected Storage | Not defined | Not defined |
| QoS RSVP | Not defined | Not defined |
| Remote Access Auto Connection Manager | Not defined | Not defined |
| Remote Access Connection Manager | Not defined | Not defined |
| Remote Procedure Call (RPC) | Not defined | Not defined |
| Remote Procedure Call (RPC) Locator | Not defined | Not defined |
| Remote Registry Service | Not defined | Not defined |
| Removable Storage | Not defined | Not defined |
| Retrospect Client | Not defined | Not defined |
| Routing and Remote Access | Not defined | Not defined |
| RunAs Service | Not defined | Not defined |
| Security Accounts Manager | Not defined | Not defined |
| Server | Not defined | Not defined |
| Smart Card | Not defined | Not defined |
| Smart Card Helper | Not defined | Not defined |
| System Event Notification | Not defined | Not defined |
| Task Scheduler | Not defined | Not defined |
| TCP/IP NetBIOS Helper Service | Not defined | Not defined |
| TCP/IP Print Server | Not defined | Not defined |
| Telephony | Not defined | Not defined |
| Telnet | Not defined | Not defined |
| Uninterruptible Power Supply | Not defined | Not defined |
| Utility Manager | Not defined | Not defined |
| Windows Installer | Not defined | Not defined |
| Windows Management Instrumentation | Not defined | Not defined |
| Windows Management Instrumentation Driver Extensions | Not defined | Not defined |
| Windows Time | Not defined | Not defined |
| Workstation | Not defined | Not defined |

Last Updated: July 27th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Virginia Beach 2017 | Virginia Beach, VA | Aug 21, 2017 - Sep 01, 2017 | Live Event |
| SANS Network Security 2017 | Las Vegas, NV | Sep 10, 2017 - Sep 17, 2017 | Live Event |
| SANS vLive - SEC505: Securing Windows and PowerShell Automation | SEC505 - 201709, | Sep 18, 2017 - Nov 13, 2017 | vLive |
| Secure DevOps Summit & Training | Denver, CO | Oct 10, 2017 - Oct 17, 2017 | Live Event |
| SANS San Francisco Winter 2017 | San Francisco, CA | Nov 27, 2017 - Dec 02, 2017 | Live Event |
| San Francisco Winter 2017 - SEC505: Securing Windows and PowerShell Automation | San Francisco, CA | Nov 27, 2017 - Dec 02, 2017 | vLive |
| SANS Cyber Defense Initiative 2017 | Washington, DC | Dec 12, 2017 - Dec 19, 2017 | Live Event |
| SANS Southern California- Anaheim 2018 | Anaheim, CA | Feb 12, 2018 - Feb 17, 2018 | Live Event |
| SANS OnDemand | Online | Anytime | Self Paced |
| SANS SelfStudy | Books & MP3s Only | Anytime | Self Paced |