Global Information Assurance Certification Paper

Bruce L. Fyfe, Jr.

Building a Secure Windows® 2000 Professional Network Installation

A Best Practices Approach to Securing a Windows® 2000 Networked Workstation

Table of Contents

Section
1 Overview

Building a Secure Windows® 2000 Professional Network Installation

Overview

The Windows® 2000 Operating System (OS) was designed to be a stable and secure platform capable of running current business applications. The foundations for the Windows® 2000 architecture stem from the Windows NT Operating System. While much of the processes for securing Windows NT still apply, Windows® 2000 has been enhanced with new features and tools to improve its security.

This paper will examine these new features and explain the intent of the features as well as recommend settings that should be applied. While there are some features of Windows® 2000 such as Group Policy and Intellimirror that only apply to a Windows® 2000 domain, the scope of this paper is the Windows® 2000 Professional OS. Some of the recommended settings can and often should be implemented using Group Policy. This paper will not cover Active Directory, Group Policy or Intellimirror in any depth except to mention these technologies when appropriate.

System & Security Architecture

It is important to understand that the Windows® 2000 Professional OS can be installed in a wide variety of roles and networks. It can act as a stand-alone workstation, peer in a peer-to-peer network, or a client on a client/server network. Often is can be deployed as a mixture of these roles. A laptop running Windows® 2000 Pro could be a client on a client/server network as a stand-alone machine. As a client, Windows® 2000 support connectivity to Microsoft® Windows, UNIX or Linux, Novell and Macintosh networks natively. Windows® 2000 is a Network Operating System (NOS) built on top of the TCP/IP protocol. It was designed to support standard TCP/IP based protocols such as TCP/UDP, IP, HTTP, FTP, TFTP, SMTP, SNMP, and DNS. Also supported are security and authentication protocols such as Kerberos, IPSec and L2TP.

Section
2

Installation

Building a Secure Windows® 2000 Professional Network Installation

Installation Process

Installation of Windows® 2000 is the starting point for the process of securing the OS. The decisions made during installation have lasting effects on the security, stability and performance of the workstation. As a general installation rule, do not install unnecessary software or components. Just because you can run a web or FTP server doesn't mean you should. Software application and services can be added post installation if necessary. Software installed by default and removed later poses a risk of leaving system files or registry information that may open holes in the operating system.

Physical Security

An often-overlooked aspect of information security is the actual physical security of the machine. Often the network servers are secured in a computer room that has limited physical access to a known group of people. However, most network workstations are left in a generally unprotected environment. If these machines have the ability to store data locally then they are potential security risks.

Network workstations are usually deployed in environments that are accessible to a wide range of people including other members of the organization as well as outside entities such as janitors and guests. Therefore, a threat assessment must be done on each machine to gauge the risk of losing potential confidential information if a particular workstation was stolen or destroyed.

A recommendation for each workstation includes installing a case lock to prevent access to the internal storage devices. Secure removable media devices such as floppy disk drives, CD/DVD drives, ZIP or tape drives and any other device that could be used to transfer data to or from the workstation. If the risk of losing a particular workstation warrant an

extremely high level of physical security then a workstation may be physically confined with a cage or strapping devices.

Examine the boot process of the workstation. Determine if the computer is configured to boot from alternate devices such as floppies, CD or the network. These setting are usually stored in the BIOS EEPROM for on a PC. Most BIOS program allow you to set the boot device order and secure access to the BIOS program with a password. The recommended configuration is to allow booting form the local hard drive only and to secure the BIOS program with a password.

Standard CD or Network Based Installation

If using a standard installation from a CD-ROM disk then ensure the following steps are taken during installation:

1. Install to a NTFS partition

2. Use the Custom setup option and install only the services and components needed. Remember that it is better to add services later than to remove unnecessary files.

3. Be sure to configure a secure password for the local administrator account.

Be sure the media used to install is from a trusted source (i.e. actual media from Microsoft and not a CD-R copy of the disk). This will reduce the risk of introducing viruses or malware that have been hidden in the installation media.

RIS Installation, Ghost or Disk Cloning

The important point to keep in mind when using automated installations is that you do not have control over what is installed. If you created the image that is being installed you can be reasonably sure what is installed. If however, you are using a "standard" install that you did not create you will need to do the following:

1. Re-install latest services packs and updates.

2. Manually audit the installed software using the Add/Remove Programs utility in the Control Panel as well as visually scanning the disk directories for abnormal entries.

3. Use Task Manager and vie running processes. Manually scan these for unknown and abnormal processes. If you are unsure about what a process is try using the process name (i.e. csrss.exe)

in a Internet search engine such as Google. Often you will find out what application or service the executable belongs to.

4. Run a virus scan on the installation.

Potential risks:

1. Subversion of the source files (either changing or deletion)

    a. When using RIS this is somewhat unlikely due to the fact that RIS servers are authorized by Active Directory and work in conjunction with DHCP. However, if a DHCP server is subverted or a domain controller then RIS is vulnerable to attack.

Section 3

Post Installation

Building a Secure Windows® 2000 Professional Network Installation

Post Installation

Clean Up and Updating

Microsoft products and consequently their installation routines are designed to be user friendly. Unfortunately, this often translates in an un-secure installation. Standard installations of Windows operating system often installssoftware and services that are not required on every system. This results in a high level of compatibility but also introduces a lot more possible attack points.

The rule is: If you don't need it, don't install it. The follow up rule is: If it is installed and you are not using it, remove it. Be careful not to remove services that are required but may not be apparent. Here are some recommendations on what is and isn't recommended and/or required:

Disable alternate boot devices

Modify the BIOS program to only allow booting from specific, trusted devices such as the local hard disk. Do not allow booting from floppies or CD/DVD drives. A network boot option can be used to for remote installation but should not be used in general. Once the BIOS has been modified a password should be set to restrict access to the BIOS program. Be warned that removing the system battery for a sufficient length of time can usually reset the BIOS password. Again, physical security of the box is a base component of the security of any machine.

Covert all partitions to NTFS

If during the initial setup the system partition was not formatted with NTFS it should be converted immediately. NTFS partitions support full access control to the file (object) level. NTFS also is faster than FAT or FAT32 on larger disks.

To convert the partition to NTFS open a command prompt and use the **convert** program.

C:\>convert volume /FS:NTFS /NoSecurity

volume Specifies the drive letter (followed by a colon, e.g. C:), mount point, or volume name.
/FS:NTFS Specifies that the volume is to be converted to NTFS.
/NoSecurity Allows access to all files to everyone (DO NOT USE!!!)

Remove un-needed services and software

One of the biggest problems with Windows® 2000 installations is the abundance of un-necessary services and software. Windows evolved from a user centric model that took the approach of opening everything because it is easier to use. Obviously this was not the secure methodology.

One service that is not needed on a workstation is the Server service. The server service can be disabled on all workstations that are not sharing local resources. Computers not running the Server service cannot share their resources nor will they show up in the Browse list under My Network Places.

The Computer Browser service does not need to run on workstations. This service allows the workstation to maintain a browse list of available resources. Not only is this a potential security problem but also causes an over use of the workstation resources such as CPU time and network connectivity.

The Error Reporting service is a feature with good intentions that may be a potential problem. When a Windows® 2000 machine encounters a problem with a program of service the Error Reporting service can send the relevant information to Microsoft® for analysis. If this information is intercepted it could divulge information about the PC that would be useful to hackers.

Here is a list[1] of required services for a generally secured workstation. All other services should only be run after establishing a required need and evaluating the impact to the security posture of the machine.

- DNS Client
- EventLog
- IPSec Policy Agent
- Logical Disk Manager

- Network Connections Manager
- Plug & Play
- Protected Storage
- Remote Procedure Call
- Remote Registry Service
- RunAs service
- Security Accounts Manager
- Workstation (OPTIONAL: required for connection to remote resources)

Rename or disable default accounts

Because Windows® 2000 has some built in accounts that have predictable names, it is prudent to change the names of these accounts. While this does not make these accounts more secure it does make it more difficult to a would be intruder to guess the user name for a target account. Rename the Administrator and Guest accounts.

The Guest account should always be disabled. If the workstation is connected to a Windows domain you can also disable the local administrator account. Before you disable the administrator account, be sure that there is access to an account that is a member of the local Administrators group. If the machine is connected to a Windows domain the Domain Administrators group should be listed in the local Administrators group.

The following information is contained in Microsoft® support document Q281140.

To disable the local administrator account[2]:

1. Log on as Administrator, or as a user with administrator permissions.
2. Clicking Start, point to Programs, point to Administrative Tools, and then click Local Security Policy.
3. In the left pane, expand the Local Policies node, and then click User Rights Assignment.
4. In the right pane, double-click Deny access to this computer from the network.
5. In Local Security Policy Setting, click Add.
6. In the Users and Groups box, click the Administrator account, and then click Add.
7. Click OK, click OK, and then quit the Local Security Settings console. You must restart your computer for the new security setting to take effect.

Install latest Service Pack

Microsoft® maintains Windows® 2000, like Windows NT previously, through the application of Service Packs. Service Packs are essentially a composite of the various fixes to the OS that have been release. Microsoft® released several "hot-fixes" between Service Packs. It is preferable to install one Service Pack instead of multiple hot-fixes. Hot fixes can cause problems if applied in the wrong order. Please review Microsoft® article Best Practices for Applying Service Packs, Hotfixes and Security Patches.

Remember that if you add or remove a service or software to a Windows® 2000 machine that updated files may be replaced. It is highly advisable to re-apply the currently installed Service Pack after installing or removing software on a machine. Additionally, use the Hotfix Checker utility (Hfnetchk.exe, described in Microsoft® Q315665) available from Microsoft® to verify which hotfixes (if any) have been installed.

Service packs and hot-fixes can be downloaded from the Microsoft web site, usually free of charge.

Check Windows Update and Security Sites

The Windows Update (http://windowsupdate.microsoft.com/) web site also will check the system for Service pack installation as well as subsequent security fixes. Microsoft has begun to release Security and Update "roll up" updates that contain a variety of fixes that has been release since the last Service Pack. The Windows Update site offers a good place to get the vast majority of the most current update in a easy to use format. Pay particular attention to the Critical Updates and recommended Updates sections.

The Microsoft Baseline Security Analyzer will also check the current installation for common security configuration errors and hotfixes. It will then generate a report that provides easy to understand, color coded information on the security issue and how to fix it. Once the appropriate actions have been taken a second scan can confirm the fixes have been plied correctly to the system.

Section 4

User Rights

Building a Secure Windows® 2000 Professional Network Installation

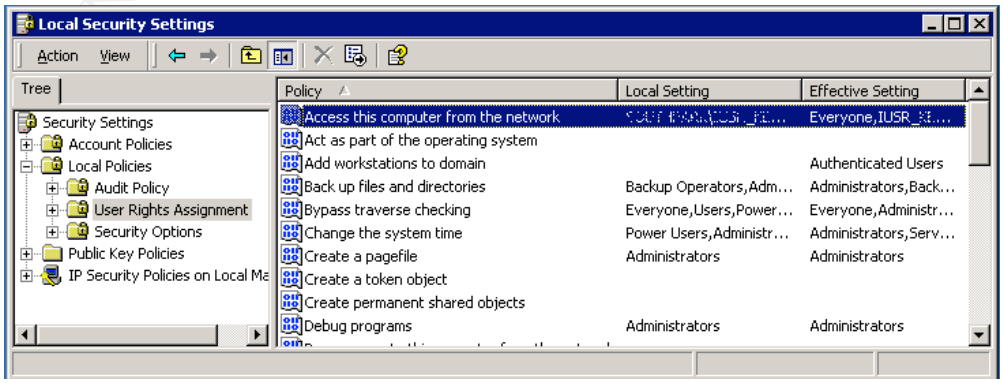
User Rights

Rights vs. Permissions

In a Windows environment user security administration can be achieved through the used of rights and permissions. User rights are typically actions the user is allowed to perform. An example of a user right is "Log on locally" which allows a user or group to log on to the workstation from the console. Permissions are assigned to objects such as files, folders and printers that define which groups and/or users have access to the object. Examples of permissions include the ability to Read, Write or Modify an object such as a file or folder. A good security policy combines the use of restricting user rights and permissions to allow access to network resources.

Standard Rights Settings

The user rights for a Windows® 2000 machine can be viewed and set through the Local Security Settings MMC. To access this MMC open Control Panel, then open Administative Tools then double click the Local Security Policy icon.



User Right	Default Setting	Recommended Setting
Access This Computer from Network	Administrators, Backup Operators, Power Users, Users, Everyone	Administrators, Backup Operators, Power Users, Users
Act as Part of the Operating System		*Not Assigned*
Add Workstations to a Domain		*Not Assigned*
Back Up Files and Directories	Administrators and Backup Operators	Administrators and Backup Operators
Bypass Traverse Checking	Administrators, Backup Operators, Power Users, Users, Everyone	Administrators, Backup Operators, Power Users, Users
Change the System Time	Administrators, Power Users	Administrators
Create a Token Object		*Not Assigned*
Create Permanent Shared Objects		Administrator
Create a Pagefile	Administrators	Administrators
Debug Programs	Administrators, Local System	Administrators, Local System
Deny Access to This Computer from the Network		Guest
Deny Logon as a Batch Job		Guest
Deny Logon as a Service		Guest
Deny Local Logon		Guest
Enable Trusted for Delegation on User and Computer Accounts		Administrator
Force Shutdown from a Remote System	Administrator	Administrator
Generate Security Audits	Local System	Local System

Increase Quotas		Administrator
Increase Scheduling Priority	Administrators	Administrators
Load and Unload Device Drivers	Administrators	Administrators
Lock Pages in Memory		*Not Assigned*
Log On Locally		Domain Users or Users
Log On as a Batch Job	Local System	Local System
Log On as a Service	Administrators, Backup Operators, Power Users, Users, Guest	Administrators, Backup Operators, Power Users, Users
Manage Auditing and Security Log	Administrators	Administrators
Modify Firmware Environment Values	Administrators, Local System	Administrators, Local System
Profile a Single Process	Administrators, Local System	Administrators, Local System
Profile System Performance	Administrators, Local System	Administrators, Local System
Replace a Process-Level Token	Local System	Local System
Restore Files and Directories	Administrators, Backup Operators	Administrators, Backup Operators
Shut Down the System	Administrators, Backup Operators, Power Users, Users	Administrators, Backup Operators, Power Users, Users
Take Ownership of Files or Other Objects	Administrators	Administrators

Section
5 File & Object Permissions

Building a Secure Windows® 2000 Professional Network Installation

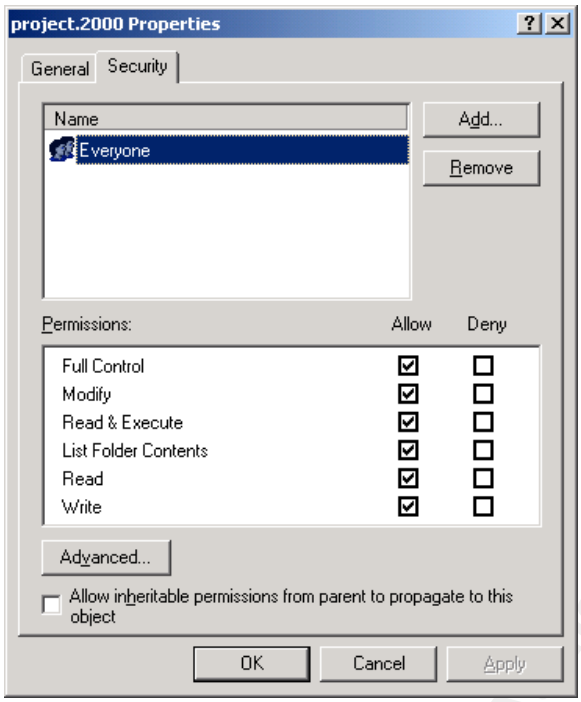
File & Object Permissions

Files, folders, users, groups, printer are all objects. Windows NT/2000/XP relies on objects for enforcing security. Access to objects are either permitted or denied to other objects. For example, access to a folder object can be permitted to the group object Users and denied access to the user object Guest.

Each object has a property (or attribute) that is called an Access Control List (ACL) which is in turn created from a collection of Access Control Entries (ACEs). You can think of a ACL as a key ring and contains many different keys (the ACEs).

Restricting Object Access

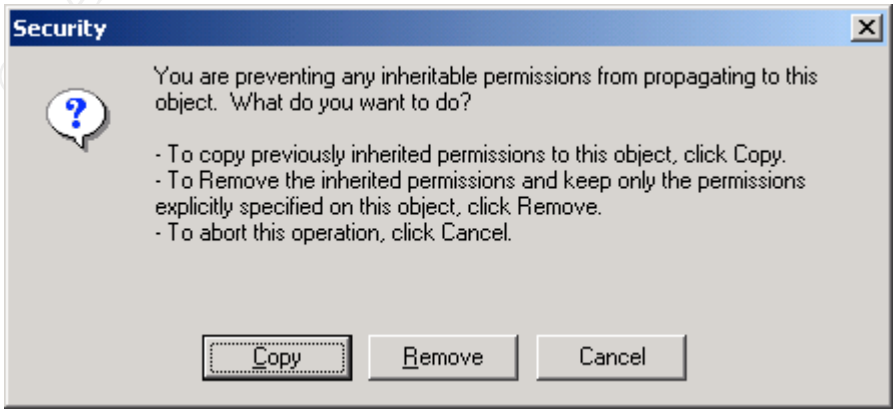
When an object (file, folder, etc) is created the default permission that is assigned to it is the group Everyone has Full Control. This is not advisable for obvious reasons. To set and restrict the permissions of an object, right click the object and click Properties. Click the Security tab. Select the Everyone group and click the remove button. Click the Add button and select the appropriate groups and/or users to assign permissions to and assign the necessary permissions.



Inheritance

Windows 2000 has a feature called inheritance that can affect the security profile of an object. Files and folders are most often the focus of inheritance. Notice the check box in the graphic above called "Allow inheritable permissions from parent to propagate to this object". If this box is checked, the permissions from the parent object (usually the folder in which the file or folder is contained) will be applied to the object. If inheritance is allowed, you will not be able to set any custom attributes on the object.

If you want to expand upon the inherited permissions you can copy the permissions to the object by checking the box to allow inheritance and click Apply. After the system has set the permissions uncheck the box. You will be prompted on what you wish to do:



Simply choose Copy (this will maintain the permissions of the parent object) and modify the permissions to your required specifications.

Restricting System File Access

Most system critical files are stored in the *%systemroot%*\system32 directory. By default the permissions for this folder offer adequate security. These permissions should be verified to ensure that groups such as Everyone and users like Guest do not have access to them.

Windows 2000 loads the base system files it needs into memory at boot. In a default setting these files can be access and modified while in memory. It is therefore recommended that you modify[4]:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager
Value Name: **ProtectionMode**
Data Type: REG_DWORD (DWORD Value)
Value Data: 0 = disabled, **1 = enabled** (Default is 0)

Restricting Registry Access

Because the registry contains vital and confidential information about the system it is recommended that access be restricted[3]. Local access to the registry is usually obtained through either the regedit.exe or regedt32.exe utilities. By setting permissions on these files to allow Administrators only to access them you can tighten local access to the registry. Remote access to the registry can be restricted by modifying the registry. This process is outlined in Microsoft Knowledge Base (KB) article How to Restrict Access to the Registry from a Remote Computer (Q153183).

Restricting Shared Folder Access

By default, when a folder is shared, the share permissions are set to allow the group Everyone the Full Control permission. If the shared folder is located on a NTFS partition and the folder and it's contents are protected by correct ACLs then this is not a huge issue. However, shared resources should always have the permissions set on the share itself. This can help protect against misconfigured ACLs on the target folder and its contents.

Share permissions are use in conjunction with the NTFS permissions on the target folder(s) and files. If there is a conflict between the share and object permissions the most restrictive permission rules are enforced.

Restricting Server Service

The Server service is only required if the workstation is used to share its local folders or printers. Therefore, it is recommended that the Server service be disabled on workstations. This is analogous to not running the "File and Print Sharing" on a Windows 9x machine.

Section
6

Auditing

Building a Secure Windows® 2000 Professional Network Installation

Auditing

Setting a baseline security audit

A good baseline for audited event is outlined in the recommended setting in Section 7 of this paper. Typical events can usually be logged for Success, meaning the event completed successfully, of Failure, meaning the event did not complete successfully.

Audited events can be viewed using the Event Viewer utility. Event Viewer can be found in the Administrative Tools or by running the eventvwr.exe program. There are actually three logs inside the Event Viewer window.

Application log

The application log contains events logged by applications or programs. For example, a database program might record a file error in the application log. Program developers decide which events to monitor and therefore are often overlooked. Most Microsoft® software will log events with meaningful data while some applications do not log events at all.

Security log

The security log records events such as valid and invalid logon attempts, as well as events related to resource use, such as creating, opening, or deleting files or other objects. An administrator can specify what events are recorded in the security log. For example, if you have enabled logon auditing, attempts to log on to the system are recorded in the security log.

System log

The system log contains events logged by Windows® 2000 system components. For example, the failure of a driver or other system component to load during startup is recorded in the system log. The event

types logged by system components are predetermined by Windows® 2000.

Additional objects & actions to audit

Audit privilege use

By auditing privileged use, you can monitor the use of user rights. A case can be made to at least audit failed attempts to utilize user rights. For example, by auditing failed instances of user rights you may detect failed attempts to log on locally or remotely to a workstation aside from the logon events.

Using Event Viewer

Monitoring the system for unusual events is often your first indication that a system is vulnerable or has been compromised. It is highly recommended that the System log be checked for logon events. Note any events that occurred at odd times or a large number of failed events. These may indicate a potential problem or a successful attack. It is important to follow up on the events with the users that caused them.

Section 7

Local Security Policies

Building a Secure Windows® 2000 Professional Network Installation

Security Policies

Account Policies

Take care when setting security policies that they are not too restrictive for your specific environments and that they cannot be used in a DoS attack against you. For example, an account lockout duration of a significant length of time coupled with a low threshold of bad attempts that force a lockout can be used to deny the right to logon to a system. Also, policies that are too restrictive, such as unreasonable password length, complexity or life span can cause users to become confused or worse yet to write their password down in an unsecured location. The following setting are recommendation but should be weighed against a specific environments security needs.

Password Policies

Policy Name	Explanation & Default Setting	Recommended Setting
Enforce password history	Determines the number of unique new passwords that have to be associated with a user account before an old password can be reused. The value must be between 0 and 24 passwords. Default: 0	**6**
Maximum password age	Determines the period of time (in days) that a password can be used before the system requires the user to change it. You can set passwords to expire after a number of days between 1 and 999, or you can specify that passwords never expire by setting the number of days to 0. Default: 42	**60**
Minimum	Determines the period of time (in days)	**15**

password age	that a password must be used before the user can change it. You can set a value between 1 and 999 days, or you can allow changes immediately by setting the number of days to 0. Default: 0	
Minimum password length	Determines the least number of characters that a password for a user account may contain. You can set a value of between 1 and 14 characters, or you can establish that no password is required by setting the number of characters to 0. Default: 0	**8**
Passwords must meet complexity requirements	Determines whether passwords must meet complexity requirements. If this policy is enabled, passwords must meet the following minimum requirements: • Not contain all or part of the user's account name • Be at least six characters in length • Contain characters from three of the following four categories: • English uppercase characters (A through Z) • English lowercase characters (a through z) • Base 10 digits (0 through 9) • Non-alphanumeric characters (e.g., !, $, #, %) Complexity requirements are enforced when passwords are changed or created. Default: Disabled.	**Enable**
Store password using reversible encryption for all users in the domain	Determines whether Windows® 2000 stores passwords using reversible encryption. This policy provides support for applications that use protocols that require knowledge of the user's password for authentication purposes. Storing passwords using reversible encryption is essentially the same as storing plaintext versions of the	**Disabled**

	passwords. For this reason, this policy should never be enabled unless application requirements outweigh the need to protect password information. Default: Disabled	

Account Lockout Policies

Policy Name	Explanation & Default Setting	Recommended Setting
Account lockout duration	Determines the number of minutes a locked-out account remains locked out before automatically becoming unlocked. The available range is 1 to 99,999 minutes. You can specify that the account will be locked out until an administrator explicitly unlocks it by setting the value to 0. Default: None	**30**
Account lockout threshold	Determines the number of failed logon attempts that causes a user account to be locked out. A locked-out account cannot be used until it is reset by an administrator or until the lockout duration for the account has expired. You can set a value between 1 and 999 failed logon attempts, or you can specify that the account will never be locked out by setting the value to 0. Default: Disabled.	**5**
Reset account lockout counter after	Determines the number of minutes that must elapse after a failed logon attempt before the failed logon attempt counter is reset to 0 bad logon attempts. The available range is 1 minute to 99,999 minutes. Default: None	**30**

Local Policies

Audit Policy

Policy Name	Explanation	Recommended Setting
Audit account logon events	Audits each instance of a user logging on to or logging off from another computer in which this computer is used to validate the account.	**Success & Failure**
Audit account management	Audits each event of account management on a computer. Account management events include the following: • A user account or group is created, changed, deleted, renamed, disabled, or enabled. • A password is set or changed.	**Success & Failure**
Audit directory service access	Determines whether to audit the event of a user accessing an Active Directory object that has its own system access control list (SACL) specified.	**Disabled**
Audit logon events	Audits every time a user logs on to, logs off from, or makes a network connection to this computer.	**Success & Failure**
Audit object access	Determines whether to audit the event of a user accessing an object—for example, a file, folder, registry key, printer, and so forth—that has its own system access control list (SACL) specified.	**Failure**
Audit policy change	Audits every incidence of a change to user rights assignment policies, audit policies, or trust policies.	**Success & Failure**
Audit privilege use	Determines whether to audit each instance of a user	**Success & Failure**

	exercising a user right.	
Audit process tracking	Audits detailed tracking information for events such as program activation, process exit, handle duplication, and indirect object access.	**Success & Failure**
Audit system events	Audits restarts or shut downs of the computer or when an event occurs that affects either the system security or the security log.	**Success & Failure**

Section
8 Network Configuration

Building a Secure Windows® 2000 Professional Network Installation

Network Configuration & Settings

Protocols

The general rule in protocol use is “the fewer the better”. Simplicity is often the friend of security. By not having to keep track of multiple protocols and the weaknesses associated with each will decrease the administration of the system. In general only use TCP/IP as the network protocol.

Services

Windows Services are often overlooked in the security planning of workstation class systems. However, by default Windows installs many services that are not required for functionality that can and should be either removed or at least disabled.

Server Service

The Server service is one of the most common services running on workstations that are unnecessary. Unless the workstation needs to be able to share files/folders and/or printers the Server service can often be disabled without any interference to the normal function of the machine. A side benefit to disabling the Server service is that without this service running the computer will not show up in the browse list of the domain.

Task Scheduler

If you do not need to schedule tasks on a workstation, disable this service. The scheduler can be used to schedule attacks during time when the machine is not in use and therefore may not be detected.

BE WARY OF THE FOLLOWING

NetMeeting Remote Desktop Sharing

This can allow remote control of the local desktop by NetMeeting. Users should not be allowed to start this service.

Routing and Remote Access

This service can be used to allow direct dial into the system. Disable this service on workstations.

SNMP Service

Due to the recent vulnerabilities in SNMP it is highly recommended that workstation not run the SNMP protocol. Be aware that this could affect monitoring software that uses SNMP to poll managed devices.

Routing

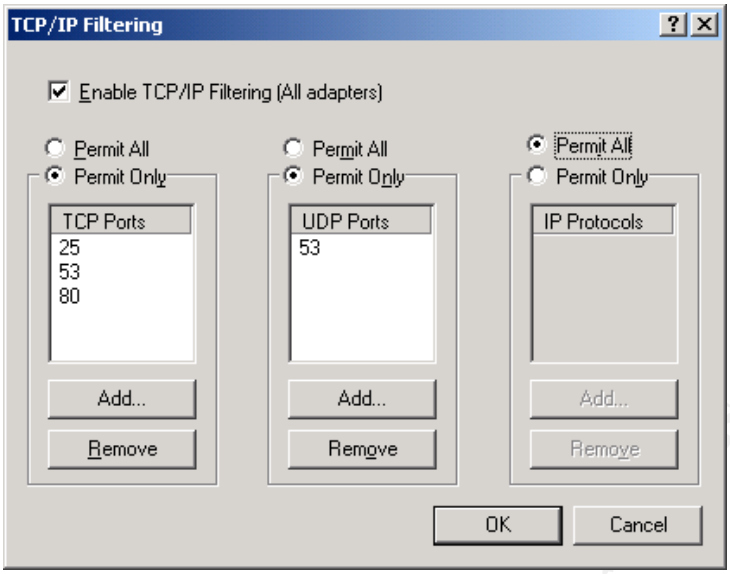
Workstation should not be enabled to router network traffic. The routing and remote access service should not be allowed on workstations. If workstations are used as routers it is highly advisable that the only be deployed as internal routers that are not connected to any foreign or public networks. Remember that user account information can and often is cached into workstation configuration and having a system exposed to un-trusted networks offers a prime hacking target.

Protocol Filtering

Windows allows the TCP/IP protocol to filter traffic at the workstation level. By default the entire TCP/IP protocol stack is enabled. It is recommended that filters be set to only allow traffic on specific ports. Remember to enable ports that allow “normal” functions within a domain. Protocols such as SMTP, HTTP, DNS, Kerberos and LDAP may all be appropriate.

The TCP/IP filtering can be enabled in on the Advanced tab for the protocol properties. Remember to exclude anyone other than Administrators for being able to change protocol settings. The ports are filtered based on destination port numbers.

NOTE: TCP/IP filter is advisable only if IPSec in not an option.



Recommended ports to allow[5]:

TCP port numbers:

- Port 80--HTTP - Allows requests to be made to a HTTP server
- Port 139--NetBIOS - Allows NBT traffic

UDP port numbers:

- Port 53--DNS Lookup – DNS queries. Port 53 TCP is not required by DNS clients.
- Port 137--NBNS – Used by WINS in necessary for name resolution

IP port numbers:

- Port 1--ICMP
- Port 2--IGMP
- Port 3--GGP
- Port 4--IP in IP encapsulation
- Port 5--ST stream
- Port 6--TCP
- Port 7--Often used for Computer Based Training
- Port 8--EGP

IP Security (IPSec)

IP Security is preferable to filtering because it offers secure encrypted communications for all IP dependant protocols. IPSec can be configured via Group Policy in an Active Directory domain or in a local security policy. There are three IPSec polices defined for Windows® 2000:

Client (Respond only)

Communicate normally (unsecured). Use the default response rule to negotiate with servers that request security. Only the requested protocol and port traffic with that server is secured. The client will respond to a server that is IPSec enabled.

Server (Request Security)

For all IP traffic, always request security using Kerberos trust. Allow unsecured communication with clients that do not respond to request.

Secure Server (Require Security)

For all IP traffic, always require security using Kerberos trust. Do NOT allow unsecured communication with untrusted clients.

The recommended setting is the Server setting that will request IPSec if available.

Internet Connection Sharing (ICS)

Like routing, the Internet Connection Sharing is a service that should not be allowed on workstations. ICS enabled systems are often directly connected to public networks. The ICS service acts as both a router and proxy service. These services are better left to hardware devices that do not contain the sensitive information that is stored in most workstations.

Dial Up

Allowing Dial-up connectivity from a networked workstation opens a security hole to the network to which the workstation is attached. Unless this is absolutely required, disable to ability of users to created dial-up connections. Better yet, remove any device that allows dial-up access from the machine.

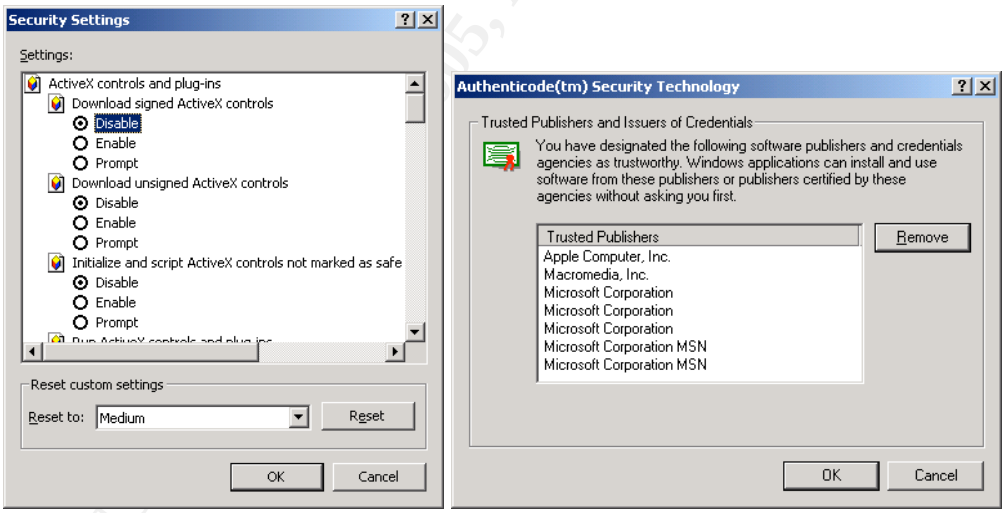
Section 9

Additional Software

Building a Secure Windows® 2000 Professional Network Installation

Additional Software

To prevent a user from downloading and installing software that may compromise the security of the system it is advisable to configure the system to refuse to run software that has not been "signed" by a trusted vendor. Application and plug-ins are digitally signed by manufacturers to prevent tampering with the code.



Windows® 2000 Professional Resource Kit

The Microsoft® Windows® 2000 Professional Resource Kit contains a lot of useful information about the Windows system architecture and security. A solid understanding of Windows security should be derived from the understanding of the underlying infrastructure.

Additionally, the Resource Kit contains many useful tools for implementing and troubleshooting security issues. Included in these tools are:

System Scanner

System Scanner for Windows is a security assessment solution for Microsoft® ® Windows® 2000, Microsoft® Windows NT version 4.0, Microsoft® ® Windows® 95, and Microsoft® ® Windows® 98. It performs nearly 300 vulnerability checks including:

- Extensive system baseline capabilities, including file, registry, and user
- Browser-specific vulnerabilities
- Comprehensive IIS/PWS checks
- Presence of well known TCP/IP-based services
- NetBIOS checks
- Java vulnerabilities
- Microsoft® Office vulnerabilities
- Windows 95 Policy Editor misconfigurations
- Susceptibility to denial of service attacks
- Configuration of virus scanners
- Registry security checks
- User policy configuration checks
- Remote access checks and modem checks

To install System Scanner

1. Insert the Microsoft® Windows® 2000 Resource Kit companion CD in your CD-ROM drive.
2. When the setup screen appears, click Explore the CD.
3. In the <cdroot>\apps\systemscanner directory, double-click sysscansetup.exe.
4. Follow the directions that appear on your screen.

Anti-virus Software

Many security threats such as DoS attacks, Trojan program access and data destruction can and often are delivered in the form of a computer virus. To guard against such attacks it is important to actively use Anti-virus detection and removal software. Several vendors such as Symantec, McAfee and Sybari offer anti-virus software.

Be sure to find a package that can monitor not only input from local devices such as floppies and CD/DVD disks but network access such as e-mail. Also, any good anti-virus package will have a feature that can automatically update its definition database(s). This is essential to keep up with the over 57,000 virus threats[6] known to date.

Personal Firewall

A personal firewall is often an easy and informative tool to provide workstation level security. My recommendation is using Zone Lab's Zone Alarm firewall. It is straight forward to setup and is easily configured. It is quite informative to review the firewall logs and see how many probes are detected by a machine attached to a public network.

Personal firewalls, like their larger cousins the corporate firewalls, work by filtering IP ports and addresses. Zone Alarm can be configured to prompt

the user when local software attempts to access or service the network and when a remote system tries to connect to the local system. It is not uncommon for a system connected to a public network to be probed hundreds of time a day.

Section
10 Summary & Conclusions

Building a Secure Windows® 2000 Professional Network Installation

Summary & Conclusion

Windows 2000 is a powerful, flexible and secure operating system if the properly configured system administrator is educated, proactive and vigilant. By understanding the operating system processes, maintaining the operating system with updated code and reviewing the system and audit logs, Windows 2000 security is a reality.

Securing computer systems is not a static process but rather a dynamic endeavor similar to a chess game. Each security issue is both a potential problem and a challenge that is countered by education and action. An effective strategy is require to implement an acceptable security posture for a machine, implement the plan and adapt the process to address an ever changing set of security threats.

Section
11

Appendix A

Building a Secure Windows® 2000 Professional Network Installation

Checklists

Basic Security Considerations

Use this check list to establish a secure baseline configuration:

- ☐ **Provide Physical Security for the machine**
- ☐ **Use NTFS on all partitions**
- ☐ **Rename local Administrator account**
- ☐ **Create a dummy Administrator account**
  Another strategy is to create a local account named "Administrator", then giving that account no privileges and impossible to guess +10 digit complex password. This should keep the script kiddies busy for a while. If you create a dummy Administrative account, enabled auditing so you'll know when it is being tampered with
- ☐ **Rename & Disable the Guest Account**
  A good name for the Guest Account is “hacker” or “badguy”. These will definitely stand out when auditing your event logs.
- ☐ **Remove all unnecessary accounts**
  Again, if the are
- ☐ **Create 2 accounts for Administrators**
  This goes against the previous caveat, but this is the exception to the rule. Create one regular user account for your Administrators for reading mail and other common tasks, and a separate account (with a more aggressive password policy) for tasks requiring administrator privileges. Have your Administrators use the "Run As" command available with Windows® 2000 to enable the access they need. This prevents malicious code from spreading through your network with admin privileges
- ☐ **Replace the "Everyone" Group with "Authenticated Users" on file shares**
  Remember that “Everyone” includes user such as Guest.
- ☐ **Create a password policy**
  Create a password policy that reflects the needs of the organization.

Remember the policies that are too stringent can cause problem just as policies that are too loose. Don't allow users to use easily guessed passwords but on the same not, most password do not need to be 15 characters either.

Enable Auditing

At the very minimum, implement auditing the following events:

Account logon events	Success, failure
Account management	Success, failure
Logon events	Success, failure
Object access	Failure
Policy change	Success, failure
Privilege use	Success, failure
System events	Success, failure

☐ **Password protect the screensaver**
Set the screensaver to activate after 5 minute of inactivity. Remember to check the box to password protect the station. This will guard against people leaving their workstation unattended during breaks, lunchs and if they "forget" to log off before leaving for the day.

☐ **Always run Anti-Virus software**
Make sure that the anti-virus software support e-mail and web content scanning as well as automatic updating of the signature databases.

☐ **Secure your Backup media**
Backup media contains sensitive and confidential information and can be restored on alternate hardware. Store the tapes in a secure, off site location. Tapes left on-site need to be stored in a media rated fire safe.

☐ **Check Microsoft® 's web site for the latest Service Packs & hot-fixes**

Mid Level Security Measures

☐ **Disable local Administrator Account**
If the system is a member of a domain and the Domain Admins group has been added to the local Administrators group then you may opt to disable the local administrator account for added security.

☐ **Don't allow unmonitored modems in your environment**
Restrict who has modems and is allowed to use dial-up networking. A physical inventory of connected computer is essential for identifying potential attack vectors.

☐ **Shut down unnecessary services**
Windows® 2000 comes with services such as IIS or Personal Web Server (PWS), and RAS that can open holes into your operating system. Malicious programs can run quietly as services without anyone knowing. Be aware of all the services that all run on your servers and audit them periodically. Here are the most common service that can be considered essential. Asterisks identify non-essential services that may alter the

functionality of the system and should be tested before removing:

- DHCP Client*
- DNS Client
- EventLog
- IPSec Policy Agent
- Logical Disk Manager
- Netlogon
- Network Connections Manager
- Plug & Play*
- Protected Storage
- Remote Procedure Call
- Remote Registry Service
- RunAs service
- Security Accounts Manager
- Workstation*

Implement IPSec

Set permissions on the security event log

The event log files are not protected by default, so permissions should be set on the event log files to allow access to Administrator and System accounts only.

Store all sensitive documents on file servers

This will aid in securing data but also in disaster recovery efforts. It also limits the need to physically secure the workstation.

Prevent the last logged-in user name from being displayed

Advanced Security Settings [7]

☐ **Set a power on password**

Protect your PC's BIOS for tampering. Set the BIOS to only allow a boot from the hard drive. Then set a password to control access and changes to the BIOS to prevent subversion. Remember that without physical security of the machine this is easily subverted by resetting the BIOS manually or removing the system backup battery.

☐ **Disable DirectDraw**

This prevents direct access to video hardware and memory which is required to meet the basic C2 security standards. Disabling DirectDraw may impact some programs that require DirectX (games), but most business applications should be unaffected. To disable it edit the Registry:
HKLM\SYSTEM\CurrentControlSet\Control\GraphicsDrivers\DCI and set the value for Timeout (REG_DWORD) to 0

☐ **Disable the default shares**

- **Drive_letter$**

Root of each partition. Only members of the Administrators or

Backup Operators group can connect to these shared folders.

- **ADMIN$**

%SYSTEMROOT% This share is used by the system during remote administration of a computer. The path of this resource is always the path to the Windows® 2000 system root.

- **IPC$**

Temporary connections between servers using named pipes essential for communication between programs. It is used during remote administration of a computer and when viewing a computer's shared resources

- **PRINT$**

%SYSTEMROOT%\SYSTEM32\SPOOL\DRIVERS Used during remote administration of printers. Required to share local printers.

Disable Dump File Creation

Unless you are in a development environment the dump files are useless anyway. However, they do contain the information in the pagefile at the time of the stop which can contain sensitive information.

Encrypt the Temp Folder

Applications use the temp folder to store copies of files while they are being updated or modified, but they don't always clean the folder when you close the program. Encrypting the temp folder provides an extra layer of security for your files.

Lock down the Registry

Clear the Paging File at shutdown

The Pagefile is the temporary swap file Windows NT/2000 uses to manage memory and improve performance. However, some 3rd party programs may store unencrypted passwords in memory, and there may be other sensitive data cache as well. You can clear the pagefile at shutdown by editing the Registry Key HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management and changing the data value of the ClearPageFileAtShutdown value to 1

Disable the ability to boot from a floppy or CD ROM on physically unsecured systems. Remember to secure the BIOS.

Disable AutoRun for CD-ROM drives on physically unsecured systems.

Remove the OS/2 and POSIX Subsystems

To remove the OS/2 and POSIX subsystems:

1. Delete the \winnt\system32\os2 directory and all of its subdirectories.
2. Use the Registry Editor to remove the following registry entries:
   Key: HKEY_LOCAL_MACHINE\SOFTWARE
   Subkey: Microsoft® \OS/2 Subsystem for NT
   Entry: delete all subkeys

Key: HKEY_LOCAL_MACHINE\SYSTEM
Subkey: CurrentControlSet\Control\Session Manager\Environment
Entry: Os2LibPath
Value: delete entry

Key: HKEY_LOCAL_MACHINE\SYSTEM
Subkey: CurrentControlSet\Control\Session Manager\SubSystems
Entry: Optional
Values: delete entry

Key: HKEY_LOCAL_MACHINE\SYSTEM
Subkey: CurrentControlSet\Control\Session Manager\SubSystems
Entry: delete entries for OS2 and POSIX

The changes take effect the next time the computer is started. Remember to update the emergency repair disk to reflect these changes.

Installation

- ☐ **Know where you are installing from**
- ☐ **Format partitions NTFS**
- ☐ **Use custom setup** and choose only required software and services
- ☐ **Consider removing administrative shares** (C$, Admin$, etc.)

User Rights

- ☐ **Access This Computer from Network**
  Allow only authenticated user this right. You can further lock in down if the workstation is not providing any network services by allowing on Administrators this right.
- ☐ **Create Permanent Shared Objects**
  Administrators only. This prohibits user from permanents sharing printers and more importantly files on the network. If the Server service is disabled then this is somewhat redundant.
- ☐ **Deny Access to This Computer from the Network**
  Assign this to the Guest account. While the guest account is disabled this is one more precaution.
- ☐ **Deny Logon as a Batch Job**
  Assign this to the Guest account and Users group. While the guest

account is disabled this is one more precaution.

- ☐ **Deny Logon as a Service**
  Assign this to the Guest account and Users group. While the guest account is disabled this is one more precaution.
- ☐ **Deny Local Logon**
  Assign this to the Guest account. While the guest account is disabled this is one more precaution.
- ☐ **Force Shutdown from a Remote System**
  Administrators only
- ☐ **Log On Locally**
  Assign this to the Domain Users and Domain Admins groups
- ☐ **Log On as a Batch Job**
  Administrators only.
- ☐ **Log On as a Service**
  Administrators only.
- ☐ **Manage Auditing and Security Log**
  Administrators only.
- ☐ **Take Ownership of Files or Other Objects**
  Administrators only

Permissions

☐	**Require NTFS partition for file level security and encryption**
☐	**Change default permissions** on local objects and shared resources and file/folders to represent those groups and/or users that require access. Do not leave default permissions intact.

Section
12

Appendix B

Building a Secure Windows® 2000 Professional Network Installation

Security Utilities

Microsoft has created a new tool, the Microsoft Baseline Security Analyzer (MBSA), to analyze Windows systems for common security misconfigurations. MBSA runs on Windows 2000 and Windows XP systems and will scan for missing hot-fixes and vulnerabilities in the following products: Windows NT 4.0, Windows 2000, Windows XP, Internet Information Server (IIS) 4.0 and 5.0, SQL Server 7.0 and 2000, Internet Explorer (IE) 5.01 and later, and Office 2000 and XP.
MBSA uses a version of HFNetChk to scan for missing hot-fixes and service packs for Windows, IIS, and SQL Server on the local machine as well as remote machines. Individual security reports for each computer scanned will be displayed an HTML in a browser like interface.
This utility can be downloaded at:
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsahome.asp

Section
XX

Bibliography

Building a Secure Windows® 2000 Professional Network Installation

Cited Sources

1. http://www.systemexperts.com/tutors/HardenW2K101.pdf, page 6
2. http://support.Microsoft.com/search/preview.aspx?scid=kb;en-us;Q281140
3. http://support.microsoft.com/default.aspx?scid=kb;EN-US;q153183
4. http://www.winguides.com/registry/display.php/281/
5. http://www.earthweb.com/article/0,,10456_625111,00.html
6. http://vil.mcafee.com/default.asp?
7. http://www.labmice.net/articles/securingwin2000.htm

Misc. Sources

3 Ways to Secure Your Windows NT / 2000 Servers

8. http://security.technow.com/articles/3.ways.secure.nt.2000.htm

Microsoft Baseline Security Analyzer

9. http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/Tools/mbsahome.asp

Microsoft® Personal Security Advisor

10. http://www.microsoft.com/technet/mpsa/start.asp

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor