Global Information Assurance Certification Paper

Using Security Templates and Group Policy to Secure Windows Servers

By

Chet A. Duncan
GSEC Practical – V1.4b

Table of Contents

Introduction

Securing an operating system is a challenge, but also a necessity. One obstacle to securing the operating system is ensuring that all of the servers are correctly configured for security. Of course, the start of securing the server is the build, but afterward there are other settings that must be put in place to properly secure any server.

Active Directory group policies provide a mechanism to assist with just this task in a Windows 2000 environment. Using group polices provides central management, consistent security settings on servers or desktops, and a means to quickly update settings when necessary. Group policies are intended to be an integral *part* of a complete security strategy, not *the* security strategy. This document describes how you can secure a Windows 2000 server using group policies.

General Approach

As in many things, it is important to devise a plan, or approach, for accomplishing the goal. Properly implementing server security and group policies is no exception. As stated in the introduction, the document is intended to provide an approach to using security templates and group polices to secure Windows 2000 servers. The general steps followed are:

1. Designing the OU Structure
2. Securing the Server
3. Creating the security template
4. Creating the group policies
5. Testing
6. Appling the policies

Of course, every environment is different, so you may find that some modifications of the details are necessary. In addition, documentation is important for maintaining and communicating what group policies are being put into a production environment.

Designing the OU Structure

Proper design of your OU structure is critical to an effective implementation of group policy. As a quick review, keep in mind that group policies are processed local, site, domain, then OU; with the closest OU taking precedence over all others. Settings such as Block Inheritance, No Override, and Disabled also effect how policies are inherited. In addition, security settings within the GPO also effect the application of group policy. As a rule, keep these various means of filtering to a minimum as they add administrative complexity. Adding OUs to your directory does not adversely effect Active Directory, therefore use the OUs to make administration easier (Wahlen).

Beyond these points, there are two other considerations for creating an OU structure: administration roles and server roles. Administration roles can be influenced by organization, geography, politics, etc. This of course will vary from organization to organization. For this illustration, a centrally managed server environment is assumed.

Server roles should also be defined in the context of security and functional needs. One approach is to define a base security policy applicable to all servers, then apply an incremental policy at the child OU. However, you can also create a separate policy for each server group and apply it directly to the corresponding OU. Both work, it is a matter of choice.

For example, there may be extranet and intranet web servers, file servers, application servers, database servers, and, of course, domain controllers. Each of these servers has a unique set of services and applications running and each will require a different level of security. With this in mind, the OU structure would start with a 'Servers' OU, with child OUs corresponding to each server role. See the illustration below.

One set of servers that should not be moved from the default OU are the domain controllers. Removing them may cause other problems as there are references, or pointers, to the domain controllers in Active Directory (Wahlen).

Securing the Server

The next step is deciding how to secure the server, and to document these settings. There is no 'one' way to secure a server. Everything depends upon the business needs and the server environment. There is documentation available on the internet that documents how to harden a server (I.e. "Microsoft Windows 2000 Security Hardening Guide," Haney), but these may be too restrictive for

your needs. What they can offer is a place to start since it is easier to 'open up' a server than it is to lock one down. Some general guidelines are provided here, but keep in mind the purpose is using group policy to apply the security settings.

Server Build

Start with a minimal server build, installing ONLY what is needed for the server to operate. For example, IIS is installed by default. If you don't use IIS, don't install IIS. After you have your base server build, or incremental build, then it is time to begin the review of the group policy options and decide which to use for the servers.

Selecting the Policy Settings

In reviewing the group policy options, you may want to review the server that represents the build, or role, that you are securing. The reasoning is this: As you install new services they will become visible within the Policy Editor | Windows Settings | Security Settings | System Services. This helps to ensure that you do not miss anything. Finally, all of the settings discussed here are found under the **Computer Configuration** part of the Policy Editor.

Furthermore, as you research specific settings for securing a server, you will find that some registry settings are not available through the existing list of options found under **Windows Settings | Security Settings**. These other registry settings can be added by modifying the sceregvl.inf file. Keep in mind these changes will only be visible on workstations or servers that have this updated sceregvl.inf file. In addition, after modification you must re-register the dll scecli.dll (run the command 'regsvr32 scecli.dll') (Komar, 299).

For example, if you want to disable the Auto Generation of 8.3 File Names, you need to set the following registry setting: NtfsDisable8dot3NameCreation DWORD 1. To add this to the list of options open c:\winnt\inf\sceregvl.inf and enter the following line:

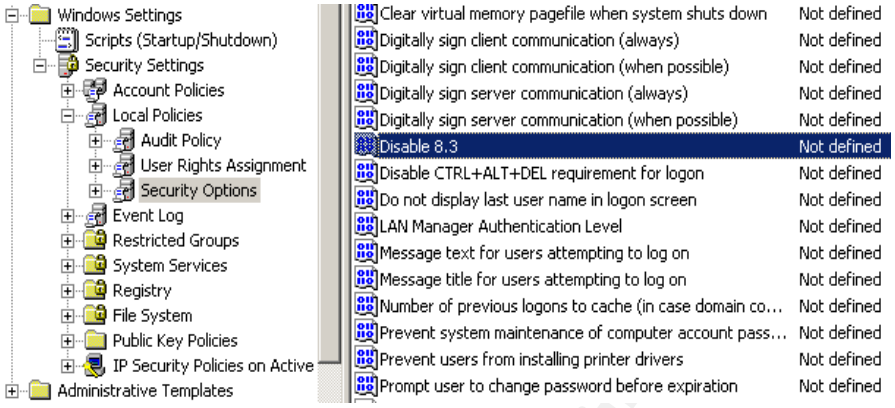
MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisable8dot3NameCreation,4,Disable 8.3,0

Save the modified file (backup the file before making the modification) and then re-register scecli.dll. The format of the entry, taken from the sceregvl.inf file, is:

```
; First field: Full Path to Registry Value
; Second field: value type
;       ; REG_SZ             ( 1 )
;       ; REG_EXPAND_SZ ( 2 )  \\ with environment variables to expand
;       ; REG_BINARY       ( 3 )
;       ; REG_DWORD       ( 4 )
;       ; REG_MULTI_SZ    ( 7 )
```

; third field: Display Name (localizable string),
; fourth field: Display type 0 - boolean, 1 - number, 2 - string, 3 – choices

After registering the scecli.dll you will see the option within the policy editor.



You can now disable 8.3 through group policy.

Finally, remember the policy refresh defaults:

- 90 minutes for member servers
- 5 minutes for domain controllers
- Security settings are re-applied every 16 hours

Software Settings

Software Settings is the first option in the group policy list of options. Software Settings is not specifically a security option, but can be used to install service packs and other software necessary for properly securing or protecting a server. One example is anti-virus software. Placing this in a group policy helps to ensure that all servers, within the OU, have anti-virus software installed.

Windows Settings

Windows Settings is the next group of policy options. Contained with these options are **Scripts** and **Security Settings**. The focus of discussion here is on the **Security Settings**.

Windows Settings – Security Settings

Under the **Security Settings** you can control:

- Account Policies
- Local Policies
- Event Log
- Restricted Groups
- System Services
- Registry

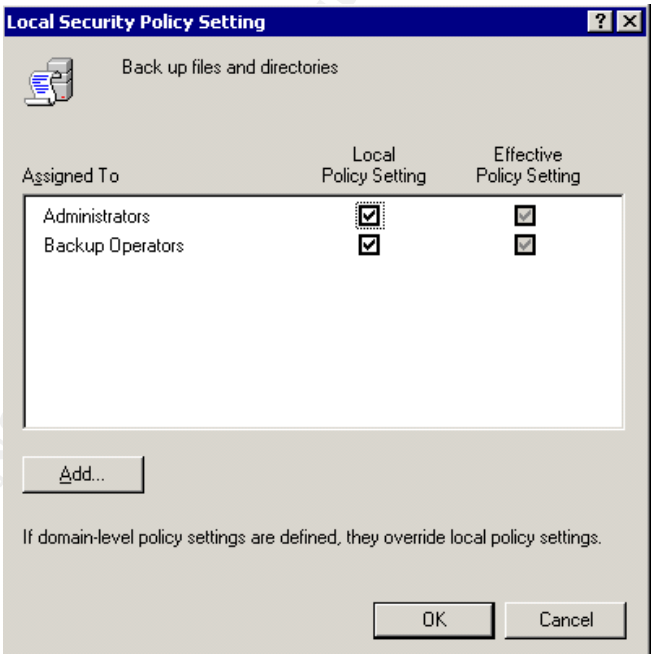
- File System
- Public Key Policies
- IP Security Policies on Active Directory

There is plenty of documentation describing what each of these categories do, so I am not going to repeat them in detail. However, I will provide a few highlights.

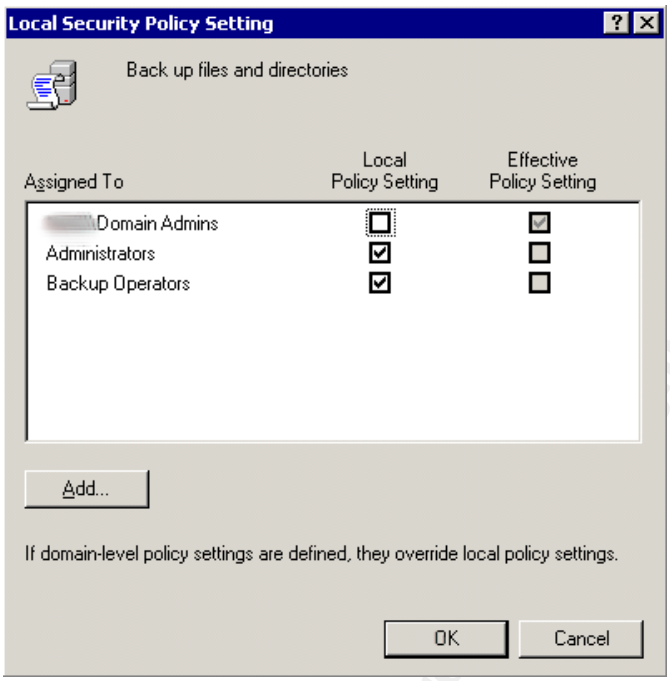
First, Account Policies are usually applied at the domain level. As a rule, Microsoft recommends against modifying the Default Domain Policy, but Account Policies are the one exception (Wahlen). The rule here is to make passwords difficult to guess, or hack, and change passwords on a regular basis (I.e. 30 days).

Second, it is important to remember that these policies take precedence over local policies. This may be an issue for servers that may have unique applications or functions. Two examples here are **Local Policies | User Rights Assignment** and **Restricted Groups**.

The User Rights Assignment assigns groups or users to specific security settings. For example, **Backup files and directories** contain, by default, a list of local groups (Administrators, Backup Operators) that have rights to this function.



If you were to place only DOMAIN\Domain Admins in this option, then the effective setting would allow ONLY the DOMAIN\Domain Admins group to have rights. All other local groups would have the access removed.



In the case of **Restricted Groups**, any existing membership in the local groups will be replaced. It is important to be aware of how these settings take effect because it is possible to negatively affect and application or service running on the server.

Auditing is important for tracking down suspicious activity on your servers, and, therefore, should be implemented. Two considerations are the amount of space available for storing the logs and information overload. Again, each administrator must make the decision as to what will and will not be audited. The NSA's documentation recommends the following (Haney, 30):

Audit account logon events	Success, Failure
Audit account management	Success, Failure
Audit directory service access	No auditing (desktops and member servers) Failure (DCs)
Audit logon events	Success, Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No Auditing
Audit system events	Success, Failure

The settings are found under **Event Log | Settings for Event Logs.**

Another important policy is the **System Services**. Services running on the server expose the server to possible attacks. Therefore, it becomes important to reduce the server's exposure by disabling unnecessary services. Like the server build, it is best to run the least number of services possible. Below is a sample that Microsoft uses in its baseline security template ("Microsoft Solution for Securing Windows 2000 Server." 6-36).

- Alerter
- Application Management
- ClipBook
- Distributed Transaction Coordinator
- Fax Service
- Indexing Service
- Internet Connection Sharing
- License Logging Service
- Messenger
- NetMeeting Remote Desktop
- Network DDE
- Network DDE DSDM
- QoS Admission Control (RSVP)
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Removable Storage
- Routing and Remote Access
- RunAs Service
- Smart Card
- Smart Card Helper
- Task Scheduler
- Telephony
- Telnet
- Uninterruptible Power
- Utility Manager

Group policy also gives you the ability to set security on registry entries as well as the file system. If there is a need to secure specific entries or directories consistently across the environment, these are the options to use. This policy can help maintain proper security through the re-application of security the policy (every 16 hours by default) whether or not the policy has changed. Once again, improper settings can cause an application to stop functioning, so test thoroughly.

As an added level of security, you can use PKI certificates. To help with the administration of PKI certificates, Public Key Policies help control, such things as, which certificate authorities systems can use and how enrollment of certificates take place. PKI is subject on it own, not is scope of this document.

Another security component often over looked is IPSec, or IP Security Policies on Active Directory (Riley). If you are in a Window 2000 Server and 2000/XP client environment, implementing this policy should have no effect on the ability of your servers and client to operate. Select **Secure Server (Require Security)** from the IPSec configuration options.

However, if there are clients running 95/98/Me then IPSec cannot be used. If you know which servers these clients connect to, then those servers can be configured to **Client (Respond Only)** or **Server (Request Security)** from the IPSec options. This implementation aids in preventing a rogue laptop that is plugged into your network from connecting to a server.

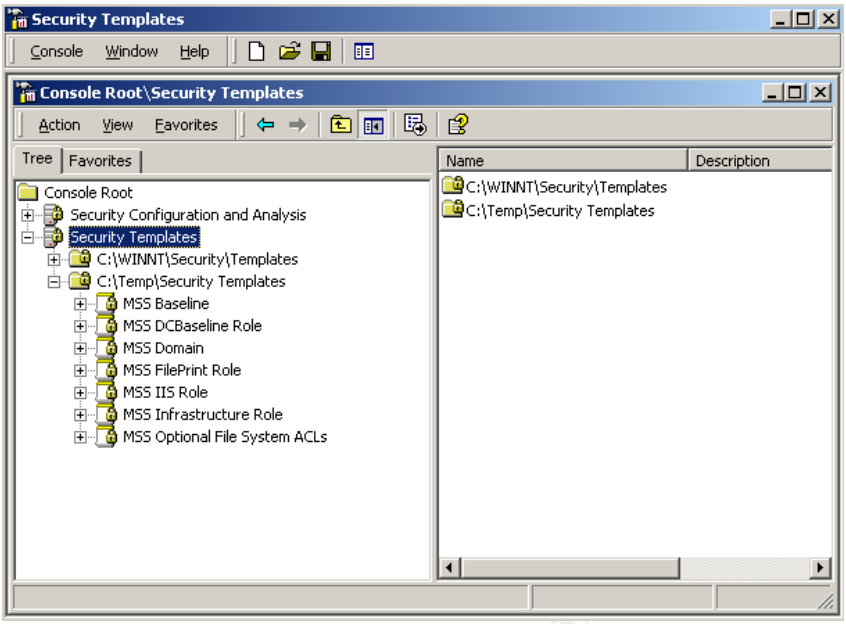
Creating the Security Template

After determining and documenting the settings for securing the servers, the next step is to create a security template. This is accomplished by using the MMC snap-in Security Templates. If you are going to use an existing baseline template and modify it then select the template using Security Templates and save it under a different name. Simply *right click* on the template you want use, and then *select* **Save As**.

Do not modify existing templates, as you may have to start over or reapply the original template to a server in order to remove an existing policy. Some registry and security settings are 'tattooed' to the server, and are not removed when the group policy is removed.

You can add search paths for additional templates to the Security Templates MMC for those templates that are downloaded from sites, such as Microsoft's Security site, or NSA's Security Recommendation Guides site. To 'load' new templates follow these steps:

1. *Select* and then *right click* **Security Templates**.
2. Then *select* **New Template Search Path…**
3. Browse to the directory where the templates are located, and *click* **OK**.
4. You should now see the templates from the new directory.



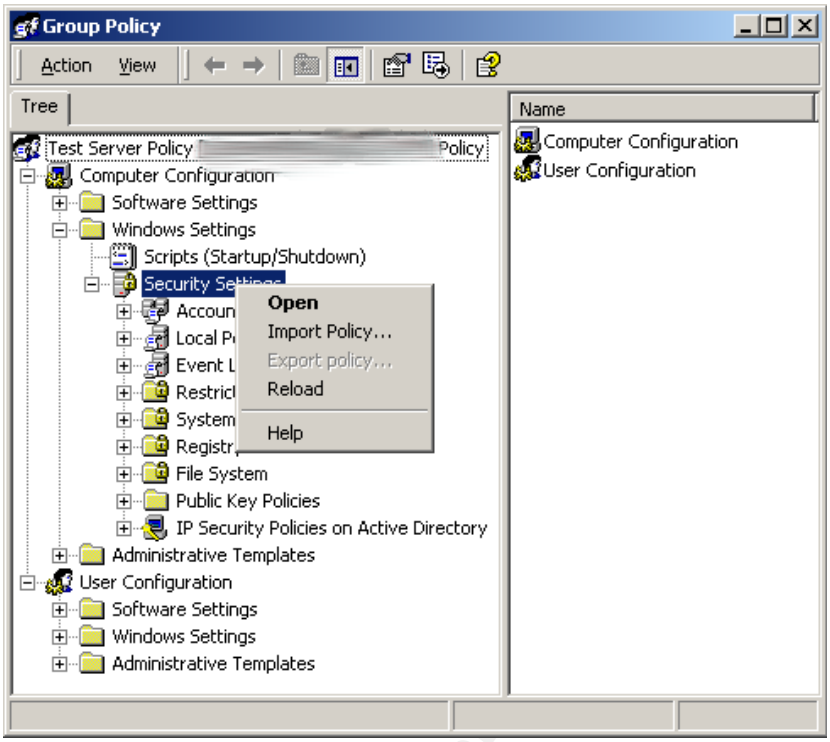
Now select and save the template you want to use as the basis for your new security template under a different name. Highlight the new template and begin going through the settings and configure them accordingly. Save the changes and close Security Templates when you are finished modifying the new security template.

Creating the Group Policies

When creating group policies it is a good idea to either start in a lab/dev environment, or a test OU. You do not want to apply a new policy before testing.

To create a new group policy:

1. Open Active Directory Users and Computers and navigate to your test OU.
2. *Right click* the OU and *select* **Properties**.
3. *Select* the Group Policy tab and click **New**.
4. Name your policy
5. Click **Edit** and navigate to the **Security Settings**.
6. *Right click* on **Security Settings**, and select **Import Policy…**



At this time you can also set other options that may be found under **Administrative Templates**. When you are complete, simply close the policy editor and *click* **OK** on the OU properties dialog box.

Testing

After you have the policy created, it is now time for testing. ***It is very important to properly test as some security settings may prevent applications from working***. Testing should be thorough and documented. In addition, it is recommended to follow some kind of change control, or at least notify people prior to putting the new policy into production.

Appling the Policies

Group Policies are not stored in the OU. What you see is a link to the actual store. So, to implement a policy on a specific OU, you must link to the Group Policy Object.

1. Open Active Directory Users and Computers and navigate to the OU.
2. *Right click* the OU and *select* **Properties**.
3. *Select* the Group Policy tab and click **Add**.
4. *Select* the **All** tab.
5. Highlight the Group Policy Object and *click* **OK**, then **Close**.

Your Group Policy is now in effect and will be applied during the next refresh. If you want to implement the policy immediately on a server, go to the server and enter this command at the command line:

Secedit /refreshpolicy machine_policy /enforce

Either way, you should now have servers with the appropriate level of security.

Conclusion

Group policies function as part of a security strategy, and are not intended to be a complete security strategy standing alone. Securing your server environment is a critical function of server administration. The challenge is administering the security in an effective and efficient manner. Using group policies to assist in securing Windows servers reduces the administrative overhead, and helps to ensure consistent security configuration throughout the server environment. However, this needs to be viewed as *part of a* security strategy, not *the* security strategy. Other security components such as physical, network, and application security must also be included within the security strategy.

Furthermore, all of the organizations security guidelines (which include group policy) must be reviewed and updated on a regular basis. Leveraging tools such as group policy eases the task of implementing required security changes in the environment.

References

Haney, J. "Guide to Securing Microsoft Windows 2000 Group Policy: Security Configuration Tool Set." 3 December 2002. Windows 2000 Security Recommendation Guides. National Security Agency. 28 May 2003 http://www.nsa.gov/snac/win2k/guides/w2k-3.pdf

Komar, Brian, and Ben Smith with Microsoft Security Team. Microsoft Windows Security Resource Kit. Redmond: Microsoft Press, 2003

"Microsoft Windows 2000 Security Hardening Guide." 11 April 2003. Microsoft TechNet. Microsoft. 22 May 2003 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/win2khg/default.asp

"Microsoft Solution for Securing Windows 2000 Server." 5 Feb. 2003. Microsoft TechNet. Microsoft. 22 May 2003 http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/prodtech/windows/secwin2k/default.asp

Moskowitz, Jeremy. Windows 2000 Group Policy, Profiles, and IntelliMirror. Alamada: Sybex, 2001

Posey, Brien. "Working With Windows 2000 Security Templates, Part 1." 2002 Brien Posey Technical Writing. Brien Posey. 28 May 2003 http://www.brienposey.com/kb/working_with_windows_2000_security_templates,_part_1.asp

Posey, Brien. "Working With Windows 2000 Security Templates, Part 1." 2002 Brien Posey Technical Writing. Brien Posey. 28 May 2003 http://www.brienposey.com/kb/working_with_windows_2000_security_templates,_part_2.asp

Whalen, BJ. "Configuring Windows Using Group Policy." TechEd 2003. Microsoft Corp. Dallas, Tx. 6 June 2003.

Riley, Steve. "IPSec Internals and Implementation Examples." TechEd 2003. Microsoft Corp. Dallas, Tx. 6 June 2003.

Shinder, Deb. "Securing Data in Transit with IPSec." 17 Feb. 2003. WindowsSecurity.com. 8 June 2003 http://www.windowsecurity.com/articles/Securing_Data_in_Transit_with_IPSec.html

Last Updated: July 22nd, 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
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
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 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
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 San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
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
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 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