Global Information Assurance Certification Paper

Bill Ellis

Bill_Ellis_GSEC

Securing Windows 2000 Locally

Computer hacking and cracking are problems plaguing businesses and major corporations today. The Department of Defense is also plagued by these new cyber-criminals. New laws and fines are being instituted as we speak. These new criminals are elite groups that for the most part do their evil deeds just for bragging rights.

A major security problem for networked systems is hostile, or at least unwanted, trespass (hacking) by users or the insertion of illegal software into networks. Some of the Hackers unwanted access could take the form of an unauthorized logon to a machine, or, in the case of an unauthorized user, acquiring privileges or performing actions beyond those that have been authorized.

Many times in today's corporate environment, System Administrators are under extreme pressure to increase productivity by getting a system online and operational quickly. Once an Administrator installs a system, the first priority is to please management and show that it is up and running. While the main focus to the Administrator is to save time and money for the company, there is an underlying tragedy waiting to happen. Failing to take extra security measures can cost a company thousands, if not hundreds of thousands of dollars in down time and possibly the respect of their clients. There are companies that are now offering "Cyberinsurance" [1]. These companies will underwrite your company for a nominal fee and if you ever get hacked, the Cyberinsurance company will pay up. I'm sure in the future this type of insurance will become very expensive.

Although no system is completely safe from an intruder, we are going to discuss different tricks of the trade that you can do locally on your Windows 2000 computers that will stop the unskilled hacker and slow down the true professional. Since Windows 2000 is one of Microsoft's latest and greatest, we are going to assume you use Windows 2000 Professional through out your network.

Loading the Microsoft Management Console

Microsoft has implemented an easier way for Systems Administrators to configure security settings on Windows 2000. Windows 2000 has a GUI (Graphical User Interface) called the MMC (Microsoft Management Console). The MMC has tools that you can use to view and administer computer components, users and groups, components and security settings. You can add one or more of these tools, called snap-ins, to the console by following the procedure below.

You can run the Microsoft Management Console (mmc.exe) by clicking on **Start→ Run → MMC** and then select **Console → Add/Remove Snap-in.** Next you will click on

Add and select **Security Configuration And Analysis**. After you choose the Security Configuration and Analysis Snap-in, click **OK** then click **OK** again [2].

To avoid having to reload the snap-in every time the MMC is exited and reopened, save the current console settings by performing the following:

In the **Console** menu, select "**Save"**. By default, the file will be saved in the Administrative Tools menu of the currently logged-on user. Enter the file name under which the current console settings will be saved. From then on, the console can be accessed from **Start → Program Files → Administrative Tools**.

Configuring a Security Template

With Windows 2000, you have the ability to configure a security template that can be used on the local machine and easily copied to other machines. The following steps should be followed to configure a system using the Security Configuration and Analysis snap-in:

First, right-click on the **Security Configuration and Analysis** node and select **Analyze Computer Now.** In the **Perform Analysis** dialog box, enter the error log file path. Then click **OK**. The system will perform an analysis of the local system. Next, you will have the opportunity to configure each security item. I am going to give you a very basic baseline that I have used in the past to secure Windows 2000 Professional computers**. Just remember, this is a baseline and should only be used as a recommended guide.**

Password Policy

Policy	**Local Setting**
Enforce password History	24 passwords remembered
Maximum password age	60 Days (could be shorter)
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

Password Policies are very important in securing a local system.

- Enforcing a lengthy password history keeps users from re-using previously used passwords for a very long period of time.
- Maximum and minimum password age is also very critical. Most password cracking tools can crack a password within specific time periods. If a password consists of dictionary words, it could be cracked rather easily and quickly. This is why it is important to ensure the Maximum password age is a short period of time to keep a hacker from cracking a users password. It is also very important to set a

minimum password age. Leaving the password age at 0 will allow the user to change the password immediately.

- Minimum password length should be set at a minimum of 8 characters. Password cracking tools are easily launched against your network. These tools can take an encrypted password and crack it in a very short time. The longer you make your passwords the harder it will be to crack them. You should also have your users use non-dictionary type words. I have found that using at least 8 characters for a password length and non-dictionary words, the longer it takes L0pht crack to crack it [3]. L0pht crack is a great tool and any Security Systems Administrator should have it in his or her toolbox. Just remember to get permission in writing from your management before you try and crack an individual's password.
- Enabling Passwords must meet complexity requirements in Windows 2000 uses a dll (dynamic link library) called passfilt.dll. This dll forces users to format their passwords to include a combination of: numbers, lower case letters, upper case letters, special characters and cannot be the users logon name.
- Store password using reversible encryption for all users in the domain is not a very good idea. This stores a password using two-way hashes and can be cracked very easily.

Account Lockout Policy

Policy	Local Setting
Account lockout duration	30 minutes
Account lockout threshold	3 invalid logon attempts
Reset account lockout counter after	30 minutes

Account Lockout Policies are also a very crucial part of securing your local Windows 2000 systems.

- The Account lockout duration can be set from 0-99999 minutes. If you set it to 0 then the account will stay locked out until the administrator unlocks it. A value of 30 minutes is a good start. If a user gets locked out they will call and let you know.
- Account lockout threshold is a very important and effective way to keep a hacker at bay. If a user (or hacker) inputs the incorrect password 3 times or more, the account will be locked. This can be set from 0 – 999 logon attempts. If you set it to 0 then the account will not be locked out.
- The policy "Reset account lockout counter after" should be set at 30 minutes. This value is used to keep a watch over the "Account lockout threshold". If a user tries to login and fails 3 times within 30 minutes, the account will lock out.

This next section is a little more in-depth but is a very important part of securing your Windows 2000 systems. Local Policies include: Audit Policy, User Rights Assignment and Security Options. Below I have put together a recommended guide for securing **Local Policies:**

Audit Policy

Policy	Local Setting
Audit account logon events	Failure
Audit account management	Success, Failure
Audit directory services access	No auditing
Audit logon events	Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No auditing
Audit systems events	Success, Failure

An audit policy is a very effective tool to keep watch over your systems. Unfortunately, systems administrators rarely take the time to put this policy into effect. If the administrator is proactive and implements an audit policy, the logs are rarely viewed. When auditing system events, be careful not to audit success and failure for everything. Choose only the events that are most critical for your environment and your policy. If you choose everything, it will fill up your event log with too much information.

You can configure the size and properties of the logs by right clicking on **My Computer** and selecting **Manage.** You will see the Computer Management screen open. In the left window you will see the **Event Viewer** folder. Click on the plus sign to open the Event Viewer folder. Right click on each folder labeled: Application, Security and System and select properties. On the properties page you can change the log size and elect what the system will do when the log file becomes full. **See Figure 1.**

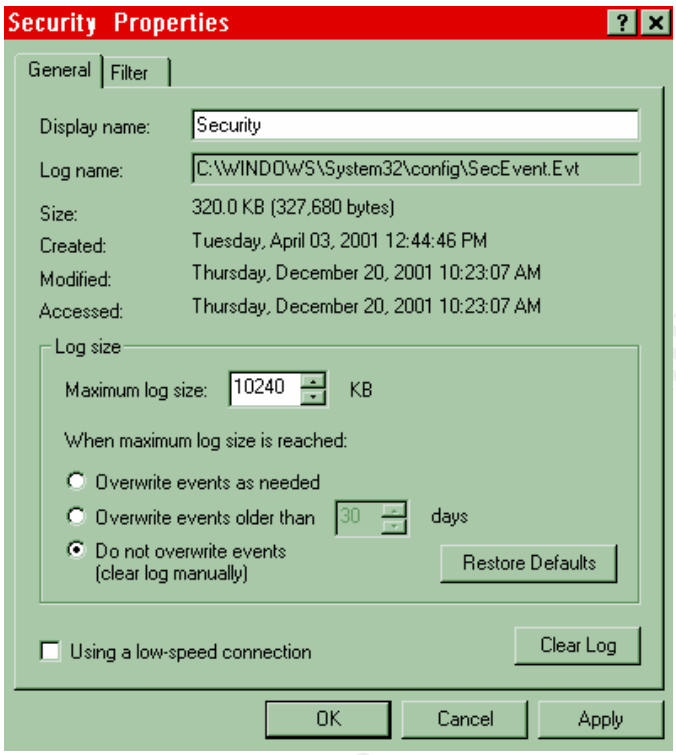

Figure 1

- Auditing account logon events is a good beginning in your auditing policy. If a user logs onto another computer and the local computer authenticated the logon, it will be recorded. Keeping track of where users go in a network is a good way to know where people are gaining access.
- Auditing success and failure on account management, records any changes to the Security Account database. This will let you know when someone either creates accounts, change them or delete them.
- I leave Audit directory service access as "No auditing" because we are configuring a local Windows 2000 system that is not in an Active Directory Domain.
- Auditing logon events keeps track of who logs in or out and what network connections are made. This is one of the most important actions you could take in auditing. If a hacker tries to gain access to your system or network and you have your audit policy to record failed logons, you will see the attempts. In turn, if you do not have auditing in place for logon events, you will never see the hacker's attempts.
- Audit object access watches for any attempt to access files (and directories) or printers. I set this Audit policy to "Failure". I want to know when someone is trying to access an object that they are not supposed to.
- Audit policy change is set to "Success, Failure" because we want to know if and when someone changes either the security policy or the audit policy.
- Setting the local setting to "failure" on Audit privilege use will record when someone unsuccessfully tries to use privileges that were not assigned to him or her.

- Audit process tracking is left as "No Auditing" because it will record every time someone starts or exits a program. This would generate too much information during a business day.
- Audit system events are set to "Success, Failure" because we want to record when someone shuts down a system or boots a system.

The one main reason a Systems Administrator may not set auditing on the local systems is because it can create a ton of information that needs to be reviewed. Unfortunately the Administrator does not have the time to review all of this audit information and in turn fails to implement auditing on their network.

The next item we will configure is User Rights. User rights are assigned to individuals or groups depending on what their effective rights should be. When determining what a users rights should be, remember to restrict an individual to only having the rights to do their job.

User Rights Assignment

Policy	Local Settings
Access this computer from the network	Administrators, Authenticated Users
Act as part of the operating system	*None*
Add workstations to domain	*None*
Back up files and directories	Administrators, Backup Operators
Bypass traverse checking	Authenticated Users
Change the system time	Administrators
Create a page file	Administrators
Create a token object	*None*
Create permanent shared objects	*None*
Debug programs	*None*
Deny access to this computer from the network	Guests
Deny logon as a batch job	*None*
Deny logon as a service	*None*
Deny logon locally	Guests
Enable computer and user accounts to be trusted for delegation	*None*
Force shutdown from a remote system	Administrators
Generate security audits	*None*
Increase quotas	Administrators
Increase scheduling priority	Administrators
Load and unload device drivers	Administrators
Lock pages in memory	*None*
Log on as a batch job	*None*
Log on as a service	*None*
Log on locally	Administrators, Authenticated Users

Manage auditing and security log	Administrators
Modify firmware environment values	Administrators
Profile single process	Administrators
Profile system performance	Administrators
Remove computer from docking station	Administrators, Authenticated Users
Replace a process level token	*None*
Restore files and directories	Administrators, Backup Operators
Shut down the system	Administrators, Authenticated Users
Synchronize directory service data	*None*
Take ownership of files or other objects	Administrators

Assigning User Rights is a very effective way of controlling what a user can do on a Windows 2000 system. A good practice when assigning user rights is to give only the rights that will enable the employee to do his job and nothing more. There are many different user rights but I will briefly cover a few of the most critical settings.

- Access this computer from the network should only be set for Administrators and Authenticated Users. This setting should only allow either an administrator or a user who is authenticated by Windows.
- Act as part of the operating system should be given to no one.
- Add workstations to domain should be given to no one. (Domain only)
- Rights to backup files and directories should only be given to administrators and backup operators only.
- Create a page file should only be given to administrators. If you allow a user to create a page file, they could disable the system if they do not know what they are doing.
- Deny access to this computer from the network should be set to deny guests or any other users or groups you wish.
- Deny logon locally should also be set to deny for guests or other individuals or groups that you want to keep from accessing this particular machine.
- Administrators should be the only ones able to force a shutdown from a remote system.
- Manage auditing and security logs should only be assigned to administrators. If anyone has the right to manage audit and security logs, they will be able to delete them and this is one way a hacker covers their tracks.
- Restore files and directories should be reserved for administrators and backup operators only.
- Take ownership of files or other objects should be set to only allow administrators this privilege.

Properly configuring the Security Options on the local computer can thwart a hacker from gaining access to your systems. Microsoft has given the whole world access to your computer and the following settings can take some of it away. In order to set these security options in the past you had to have knowledge of editing the registry. Microsoft has made it allot easier for us by providing a GUI interface to do this.

Security Options

Policy	**Local Settings**
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	Disabled
Allowed to eject removable NTFS media	Administrators
Amount of idle time required before disconnecting session	30 minutes
Audit the access of global system objects	Enabled
Audit use of Backup and Restore privilege	Enabled
Automatically log off users when logon time expires (local)	Enabled
Clear virtual memory pagefile when systems shuts down	Enabled
Default user screensaver enabled	Enabled
Default user screensaver password protection is enabled	Enabled
Default user screensaver program	Logon.scr
Default user screensaver timeout value	900
Digitally sign client communications (always)	Disabled
Digitally sign client communication (when possible)	Enabled
Digitally sign server communication (always)	Disabled
Digitally sign server communication (when possible)	Enabled
Disable CTRL+ALT+DEL requirement for logon	Disabled
Disable the CD Rom autorun feature	Disabled
Do not allow caching of roaming profiles	Enabled
Do not display last user name in logon screen	Enabled
LAN Manager Authentication Level	Send NTLMv2 responses only/refuse LM & NTLM

Policy	Local Settings
Message text for users attempting to log on	Check with your legal representative (you need to warn a hacker that he is trespassing. The court thinks that a hacker doesn't know they are doing something illegal unless they are told. This is your chance.)
Message title for users attempting to log on	Check with your legal representative (you need to warn a hacker that he is trespassing. The court thinks that a hacker doesn't know they are doing something illegal unless they are told. This is your chance.)
Number of previous logons to cache (in case domain controller is not available)	0 logons
Permissible exit routines	Not defined
Permit administrator automatic logon	Disabled
Prevent creation of 8.3 file names	Not defined
Prevent system maintenance of computer account password	Disabled
Prevent the dial-up password from being saved	Enabled
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	Something other than administrator or any name that will hint to this being the administrator account.
Rename guest account	Something other than guest.
Restrict CD-ROM access to locally logged-on user only	Enabled
Restrict floppy access to locally logged-on user only	Enabled
Secure channel: Digitally encrypt or sign secure channel data (always)	Disabled
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	Disabled

Policy	Local Settings
Send unencrypted password to connect to third-party SMB servers	Disabled
Shut down system immediately if unable to log security audits	Enabled
Smart card removal behavior	Lock Workstation
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Enabled
Unsigned driver installation behavior	Warn but allow installation
Unsigned non-driver installation behavior	Warn but allow installation

I am going to briefly cover the most critical settings above:

- Additional restrictions for anonymous connections should be set to: No access without explicit anonymous permissions. This will keep anyone (unless the user has explicit permissions) from accessing a ton of information from you computer. There are tools that hackers use to gather information from remote computers and to be successful in using these tools they have to have anonymous access.
- Allow system to be shut down without having to log on should be set to: Disabled. Disabling this option will force a user to log on before he or she can shut down the system.
- Clear virtual memory pagefile when system shuts down should be set to: Enabled. This will keep information stored in the pagefile from being viewed by unauthorized individuals.
- Disable CTRL + ALT + DEL requirement for logon: This should be set to disabled. Disabling this will require someone to physically press these three keys to log into a system.
- Do not display last user name in logon screen should be set to: Enabled. This should be enabled to ensure that someone cannot collect data from machines in your enterprise by walking up to a machine and seeing who was logged in last. Once a hacker gathers usernames he can use this to his advantage. This is also called "Social Engineering". Social Engineering is defined as, "the technique of using persuasion and/or deception to gain access to information systems.) [4].
- LAN Manager Authentication Level should be set to: Send NTLMv2 responses only\refuse LM & NTLM. LanManager (LM) is very insecure and NT LanManager (NTLM) is a little more secure than LM. NTLMv2 is the latest and greatest version and should be used when the systems communicate.
- Message text and Message title for users attempting to log on are something many people overlook. Make sure you obtain the correct message from your legal office. The message should tell the person trying to gain access to your system that if they are not authorized to access the system that they will be held legally responsible.
- Number of previous logons to cache (in case domain controller is not available) should be set to: 0 logons. This is to ensure unauthorized individuals cannot see cached information.

- Permit administrator automatic logon should be set to: Disabled. If you wish to have the administrator account log on automatically, you must store the users name and password in the registry in clear text. Anyone who has access to the registry can view the administrator's password. This is not a good thing.
- Rename administrator account should be set to: Anything but administrator or a name that will hint to this account being an administrator account.
- Rename guest account should be set to: Anything but guest. Hopefully you have given the guest account a very difficult password and disabled the account already.
- Shut down system immediately if unable to log security audits should be set to: Enabled. Be cautious enabling this option. It could result in disabling quite a few systems on the network if you don't have your security auditing properties set correctly.

After you have configured your security settings, right-click on the **Security Configuration and Analysis** node and select save. Next, right-click on **Security configuration and Analysis** again and choose Export Template. You will need to type in a name for your template. In this example we are going to call it TEST.inf. **See Figure 2.**

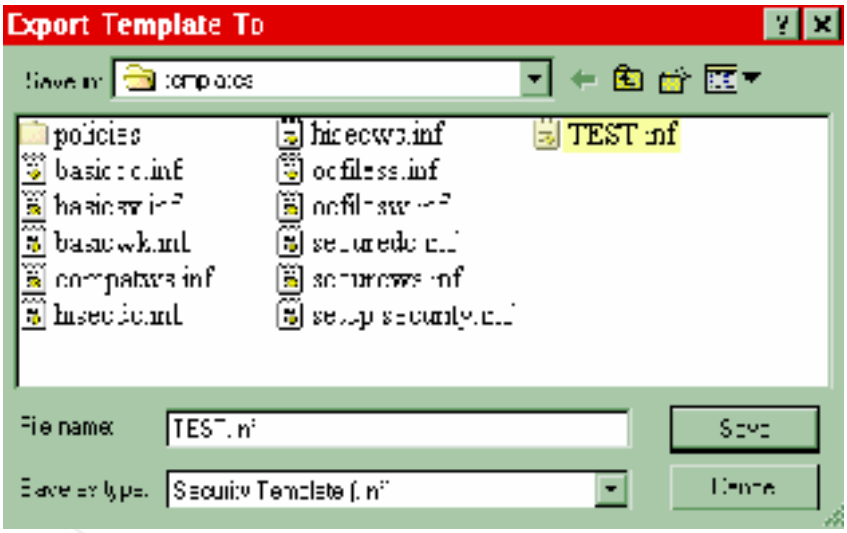

Figure 2

Next, click on Console at the top of the **MMC** and choose save then exit. After you exit the **Security Configuration and Analysis MMC**, you will need to apply the security template you just modified. Click on **Start → Program Files → Administrative Tools** and choose **Local Security Settings**. Under the tab "Tree", right-click on Security Settings and choose Import Policy… A box will pop up asking which policy to Import. **See Figure 3.**

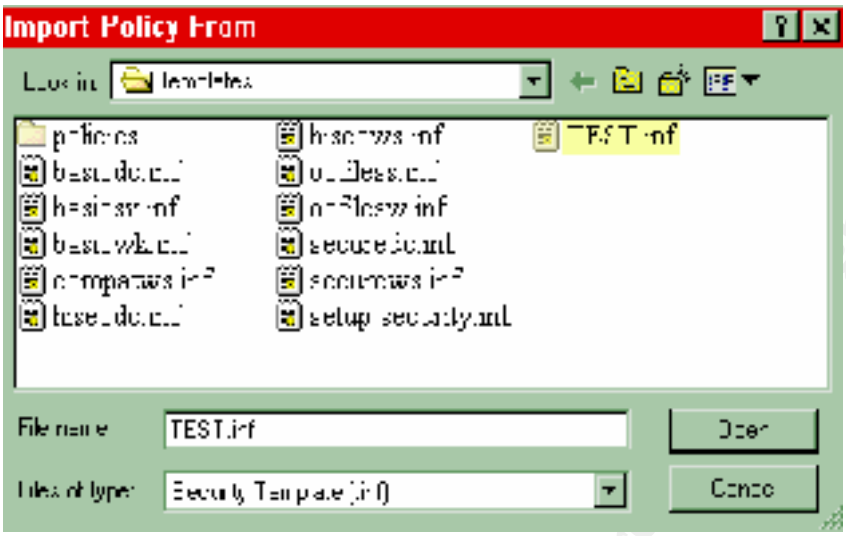

Figure 3

Choose the TEST.inf Template that you configured above then click on Open. This will apply the security policy to the local computer. Re-boot and you are good to go.

As you see above, Microsoft ships templates of different levels of security policies with Windows 2000. If you happen to configure a policy that is too stringent you can always reapply a "Basic" policy [5]. As I mentioned above, these are **recommended** guides. The Local Security configuration above is a configuration that I have personally used in the past and it worked well enough for the networks I managed. Every security configuration will be different depending on what types of applications are running on the systems, the physical location of the systems on the network (e.g. systems that are not connected to the internet need less security configuration), and the types of systems (e.g. Windows 2000 Server or Workstation). There are more in-depth security configurations that you can perform on your systems in order to make them even more secure.

Conclusion

We have covered the "basics" when it comes to securing Windows 2000 locally. Not every functional network or computer is "Hack" proof. No matter what you do to your network or how far you go to harden a specific system, there will always be someone out there that will get in. When giving an individual or group's rights or permissions, make sure you only give the minimum permissions needed for the employee to complete their job. Never give administrator privileges to someone unless it is absolutely necessary. Taking the extra time building a system and configuring the local security policy correctly can keep the majority of the hackers out.

References:

[1] Brush, Colleen. "Cyberinsurance", Information Security Magazine, TruSecure Publication, November 2001. p. 56

[2] Indiana University Knowledge Base, In the Microsoft Management Console, how do I add a snap-in?, URL: http://kb.indiana.edu/data/ajlv.html?cust=3596, 1997-2001.

[3] @stake Web site, L0pht Crack Software, URL: http://www.atstake.com/research/lc3/index.html

[4] Scambray, Joel, "Hacking Exposed", Network Security Secrets & Solutions, Second Edition, McGraw Hill, 2001, p. 561.

[5] Admin Tip #74: Windows 2000 Default Security Policy Templates, http://is-it-true.org/nt/nt2000/atips/atips74.shtml.

Last Updated: July 21st, 2017

Upcoming Training

SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
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 Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 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
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 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
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 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