Global Information Assurance Certification Paper

Windows 2000 and Network Security

Travis Abrams
June 26th, 2001
Version 1.2e

This paper will focus on basic network security procedures and the new features of Windows 2000. Although we will be focusing on Windows 2000 there are certain topics that will be discussed that pertain to network security in general and cannot be overlooked. The topics in this paper will focus on Security Policies, Anti-Virus, Active Directory and Group Policy.

Security Policies are the foundation of any security plan and cannot be ignored. These policies will help to define the responsibilities of the end-users and administrators. They will also assist in defining what an organization is trying to protect and how security will fit into their business model. There may be the need to define multiple policies depending on the model of the company. Some of these may be based upon location, department, or business function. For example, the accounting department may need different policies than general staff. The difference in laws between countries would cause policies in Brazil to be different than the United States. There also may be a need for separate policies for Remote Access, email, acceptable use, etc. The policies should be easy to read for all staff and should not be more than a few pages long. The policy should not try to anticipate every possible problem but should help guide business and security goals. The policies will then define the standards and procedures for the organization. For example, a policy may say "We will prevent unauthorized access to the internal network". A firewall would then be implemented as a standard to reach the goal of the policy. Procedures would then be created to configure settings on the firewall to attain the goals of the policy. Creating policies from scratch can be time consuming and difficult to implement. The following is a link to a set of templates that can be used and changed as needed (http://www.sans.org/newlook/resources/policies/policies.htm).

Anti-virus (AV) software is a must and should be loaded on all computers. Despite what the vendors may say no single product is 100% effective against viruses and different products should be used on different services. For example, email servers should run a different vendors anti-virus than the desktops and file servers. This allows for maximum protection but it is important to remember that all anti-virus software is reactive not proactive. It must have the updated definitions in order to detect the virus. Viruses such as the "I love you" virus spread so rapid that many organizations were infected long before the definitions were released by the AV vendors. Only authorized files should be allowed to enter the gateway. Files such as .vbs and .wsh should not be allowed to enter at all. The updating of virus signatures should be automated whenever possible and procedures to deal with virus outbreaks should be in place before an outbreak occurs. Organizations such as Avien (www.avien.org) can provide

an early warning system that can allow an organization to be notified of potential viruses before an outbreak occurs.

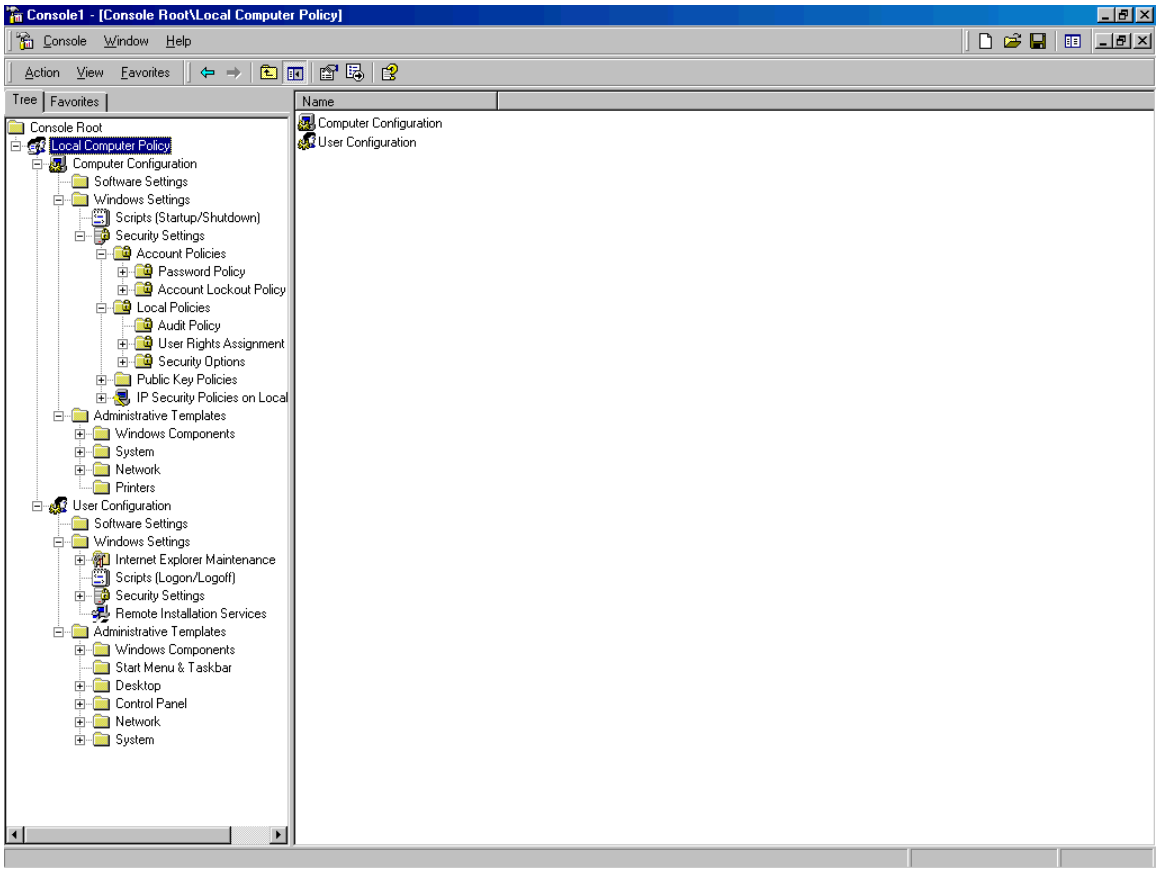
Windows 2000 has a lot of new features that allow for greater security and control and a general understanding is essential to securing it. These features include Active Directory (AD) service, Kerberos authentication protocol, public key infrastructure, Encrypting File System (EFS), Group Policy and support for Internet Protocol security (IPSec). AD provides central storage of information on users, computers and data and allows for centralized management and single sign on to resources. AD stores information in a logical hierarchy using domains, OU's and objects. A domain creates a logical security boundary and allows multiple domains to be managed by separate administrators, which can be useful in large enterprises. Multiple domains should be created to partition parts of the AD that require different security policies. The domain can be further divided by using OU's. An OU is used to organize objects into administrative groups within a domain. Administrative control can then be applied to the OU's allowing delegation to other administrators. An object contains attributes or information about a user, computer, or file. Grouping information using these methods allows for security configuration of groups, computers and users.

DNS is used in AD to provide name resolution, access to services and establishes the domain namespace. AD uses integrated zones to control who has permission to update DNS, provide fault tolerance and more reliable replication. DNS in AD provides support for dynamic updates which are replicated using a multi-master model; this eliminates the DNS master server as the single point of failure. Administrators can specify which servers can participate in zone transfers and can enable secure updates causing all information to be encrypted as it travels over the network. There is also a DNS log in the event viewer that allows auditing and troubleshooting of DNS. Administrators can be placed in the DnsAdmins group to control who has access to the DNS configuration pages.

Group Policy is a mechanism for controlling user and computer settings in a Windows 2000 domain. Group Policy Objects (GPO) allows administrators to apply policies to a large number of computers in an organized manner. These policies can be used to manage security settings such as file and registry permissions, audit settings, and control software installation and desktop settings. You can apply policies at the site, domain and ou level. Administrators can define global settings at the domain level, such as password policies, account policies, etc. Finer, more detailed policies could then be applied at the OU level. For example, the Marketing OU could be allowed to install software where as the Accounting OU would not.

Group Policy can be configured using the Group Policy snap-in, which can be loaded into the MMC or by using the Active Directory Users and Computers or Active Directory Sites and Services and specifying a new policy for the appropriate container. It is divided into two areas, Computer Configuration, which can be used to configure desktop and operating system behavior, security settings, startup and shutdown scripts and application

settings. These settings are applied when the computer starts and are refreshed periodically. The next area is User Configuration and configures the same settings as above but they are applied when the user logs on.



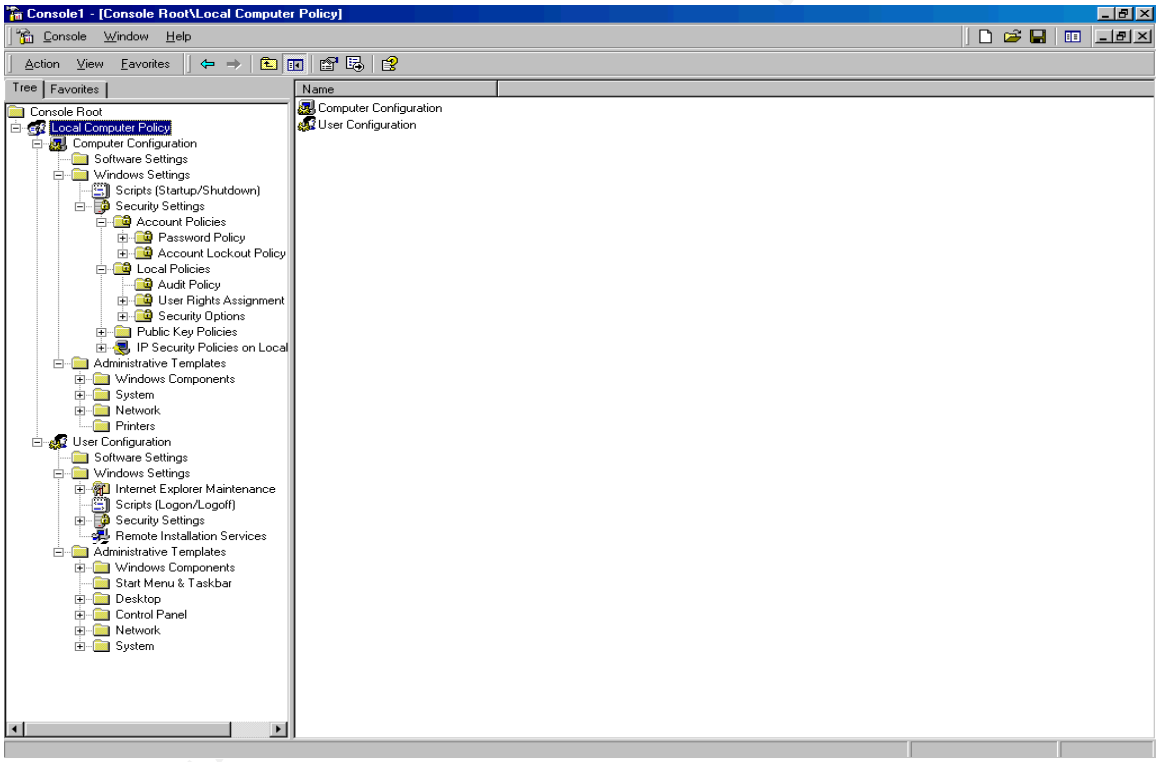
A default access control list (ACL) is applied when an object is created in Active Directory. Beyond these default permissions, management of user and object security is performed with GPOs that are applied to the site, domain or OU containers. GPO settings will flow downward from the Site to the domain to the OU containers. A single GPO can link to multiple sites, domains and OU's and causes the settings to be applied to all objects in the containers. When a GPO is created it is automatically linked to the container it is created in and none of the settings are yet defined. Only Domain Admins and Enterprise Admins can link GPOs. Members of the Group Policy Creator Owners can edit GPOs but cannot link them.

Linking a GPO to a site allows multiple domains to be configured and all users and computers will be affected regardless of their domain membership but there are possible problems that should be considered. When a GPO is linked to a site anyone with read and write permission can make changes. These changes would propagate to the entire site changing settings on users and computers in different domains. Creating a site GPO requires that it be created in the root domain of the forest. Because of possible limitations of bandwidth this could cause a problem with inter-domain replication and policy

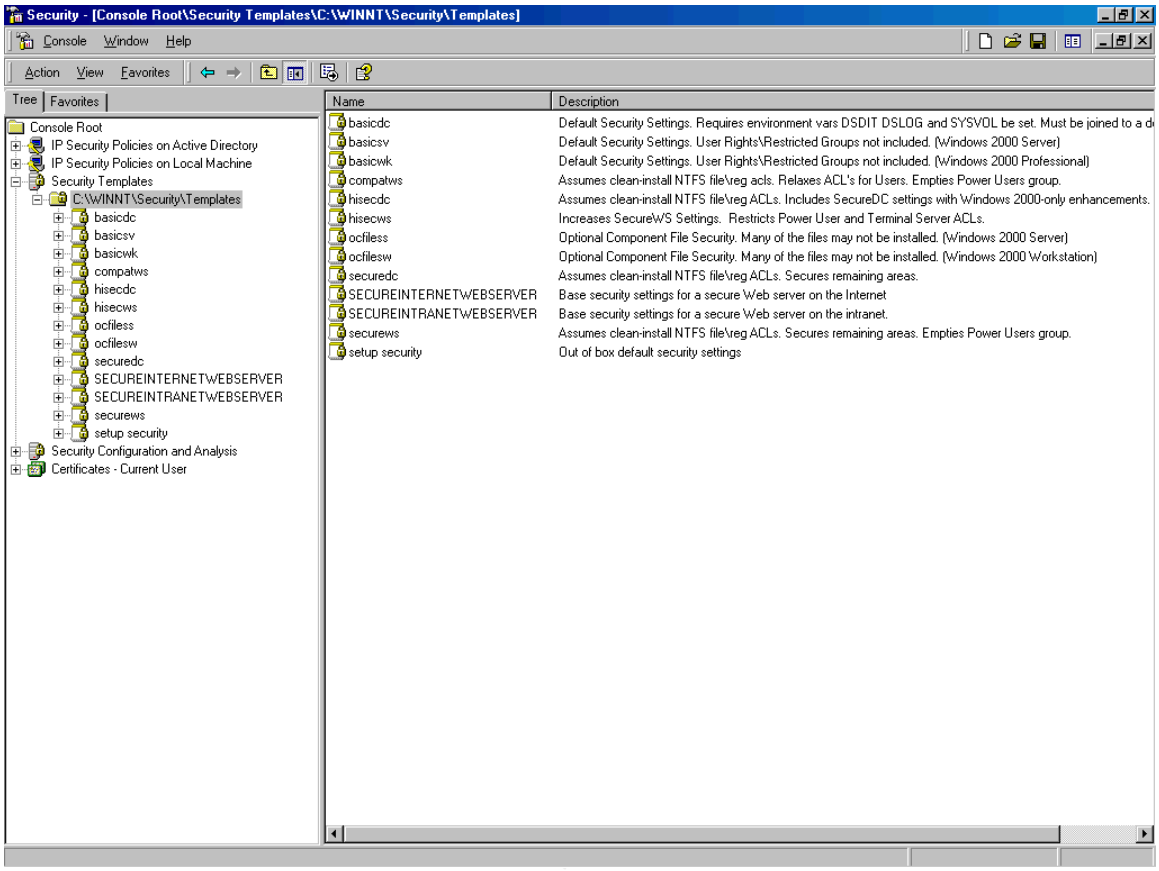
refresh. By default policies are refreshed every 90 minutes on computers running Windows 2000 professional and member servers running Windows 2000 server, domain controller policies are refreshed every 5 minutes. Because of these issues, it is recommended that GPOs not be linked to sites.

Linking a GPO to a domain allows settings to be applied to all computers and users in the domain. The only catch is that a GPO applied to a parent domain does not apply to any child domains while a GPO linked to an OU applies to all users and computers and all child OU's.

The most important part of Group Policy, as far as we are concerned, is the Security Settings extension. These settings allow consolidation of many security related settings into a single interface. Security settings are computer and user specific. A number of settings can be configured including Account policies, local polices, event log settings, groups, services, registry and file system, public key polices and IP security policies.

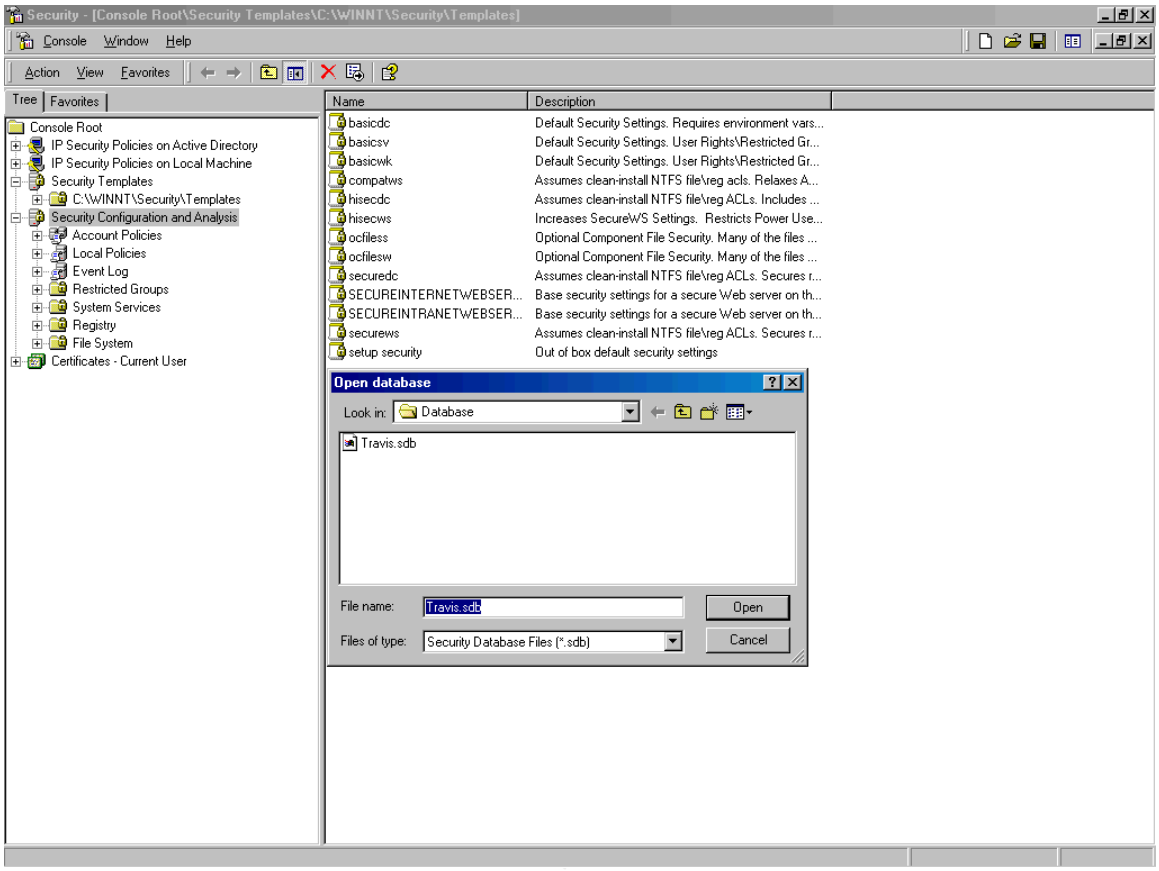


All security settings, except for Public key policies and IP security polices, can be configured initially by using the Security Templates snap-in. This snap-in allows administrators to create custom security settings that can be saved as templates or INF files. There is a number of default security templates provided with Windows 2000.



These include templates for workstations, member servers, domain controllers and internet servers. They can be imported into a GPO by using the Group Policy snap-in and then be applied to a domain or OU. All computers within the domain should be grouped into OUs based on their role. This allows individualized security settings to be applied to each type of computer. For example, domain controllers should stay in the default Domain Controllers OU so that a higher level of security can be applied to these computers, where as, workstations would be in a separate OU where different security settings would be applied.

Once the templates have been created and applied through Group Policy, the Security Configuration and Analysis tool can audit the systems to make sure the policy hasn't changed. The tool can also be used to configure security polices locally. This can be useful on laptops since they are not always connected to the network and not affected by the domain or OU policy. This is accomplished by creating a new security database on the local computer and importing the appropriate template. The computer can then be configured and periodically checked for continued compliance to the policy. The local policies will apply when the users are off the network but they will be overwritten when connected to the network. This configuration should be used only as needed because it can become confusing trying to troubleshoot different policies.



As we have seen Windows 2000 includes many powerful security configuration options but like all systems it takes a lot of work to ensure reliability and security. Service Packs and hot fixes should be applied as they become available to help maintain security at the OS level. Administrators should use non-privileged accounts for normal activities. When Admin access is required the Run As command should be used. This command can be accessed by holding down the shift key + right clicking the object you wish to launch and then entering the appropriate username and password. Use Group Policy to control settings on users and computers. Below are some recommended practices for Windows 2000 and a link to known Windows 2000 vulnerabilities.

- Develop security policies
- Use antivirus software and update it frequently
- Require Administrators to use non-privileged accounts for day to day functions. When administrative access is required the Run As command should be used to login with an Admin account.
- Use Active Directory integrated DNS zones
- Enable secure dynamic updates for the zone
- Create a DNS audit policy
- Create separate domains to partition parts of Active Directory that

require different security settings
- Physically secure domain controllers
- Membership in the Domain Admins group should remain small and controlled
- Do not link GPOs to sites
- Group computers performing different roles into separate OUs. Then apply computer settings based on computer type
- Apply strong local Group Policy to computers that are not a member of a domain.
- Maintain Service Packs and hot fixes

http://www.labmice.net/articles/win2000securityholes.htm .

References

Windows 2000 Security Technical Overview
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/sectech.asp

Windows 2000 Distributed Security Features
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/evaluate/secover.asp

Step-by-step Guide to Configuring Enterprise Security Policies
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/entsec.asp

Microsoft Technet , *Windows 2000 Security Technical Overview*

Sanderson, Mark, *Guide to Securing Microsoft Windows 2000 Active Directory version* 1.0, National Security Agency, December 2000

Haney, Julie, *Guide to Securing Microsoft Windows 2000 Group Policy version* 1.0, National Security Agency, January 2001

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event