Global Information Assurance Certification Paper

Enforcing the "Least Privilege" Principle through Active Directory, OUs, GPOs, and Group Policy Filtering.

By

Ricardo Rodriguez
GSEC Practical – V1.2f

January 7, 2002

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

II. Introduction

Microsoft Windows 2000 includes a set of new features. Some of these features give administrators better control over servers, workstations and users. The addition of Active Directory (AD) and Group Policy Objects (GPO) significantly decreases the amount of overhead associated with administering and maintaining a properly secured environment. The enhancements lead to a consistent look and feel, better distribution of resources, proper user rights assignments, etc… This is evident by the granular control exhibited by objects, which include users, groups, and workstations among others.

This document presents an approach to further enforce the "Least Privilege" principle by combining Active Directory, GPOs, and Group Policy filtering techniques. This principle states that users should be given the minimum amount of privileges to perform their job. A simple scenario follows to emphasize the concepts and processes required to properly accomplish this task. Basic understanding of Active Directory and GPOs is assumed.

III. Scenario

A Windows 2000 environment has been implemented. It includes different types of services provided by file, print, web, and exchange servers among others. These services are available to end-users using Windows 2000 professional.

The initial steps to provide some level of security have been taken. Things such as separating administrators from the rest of the users, installing the latest patches, creating and applying a group policy object at the domain level to enforce account policy, and to configure recommended computer and user configuration settings, and others have already been performed.

There is just one problem. All servers and workstations have the same group policy settings. In the case of the users, although they were grouped and assigned specific rights, they all have the same security settings, and same software available. Since there are different roles that can be defined by the career level of the users and their current project, it is essential to classify and group both machines and users. This will help enforce the "Least Privilege" principle.

IV. Organizational Units (OUs) and GPOs

When planning and designing a Windows 2000 environment using Active Directory, the first obvious categories that can be used to group all machines are servers and workstations. Figure 1 illustrates a simplistic view of an Active Directory structure where the two main OUs are servers

and workstations.

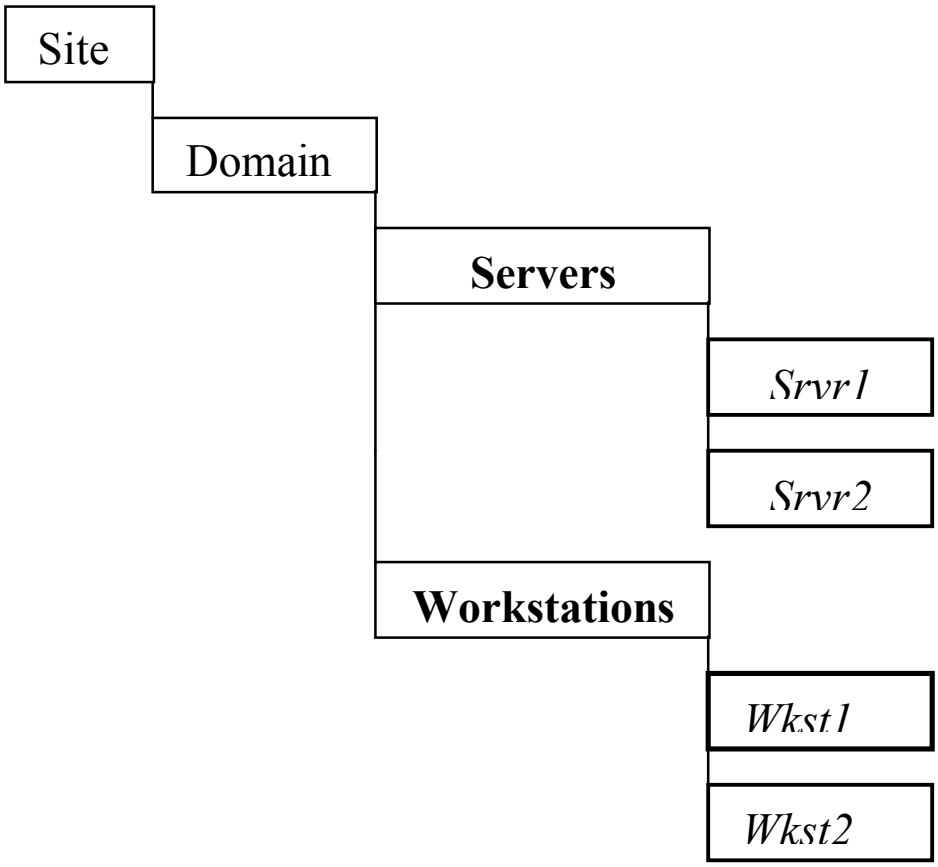

Figure 1. Simple AD Structure

In this case, two OUs were created containing two members each. A "**Servers**" OU with two servers (Srvr1, Srvr2), and a "**Workstations**" OU with two workstations (Wkst1, Wkst2).

In this simple structure, a GPO defining the account policy can be applied at the domain level. A second GPO defining common server settings, including security options, can be applied at the server level while a third GPO defining common workstation settings and security options can be applied at the workstation level.

Before going any further, it is essential to understand how GPOs are processed. When a workstation is initially built, it contains what is called local security settings. When it joins a domain, these settings are overridden, if configured, by GPO-defined values specified at different OU levels. The order in which GPOs are processed are as follows:

1. Local

2. Site
3. Domain
4. OU

The short notation LSDOU can be used to memorize the order of processing. In the case of OU, this can be further broken down as follows:

1. OU1
2. OU2
3. OU3
   .
   .
   .
n. OUn

OU1 is the OU created at the first level, and n is the lowest existing level.

This order of processing determines the effective value for any given setting. Table 1 illustrates how the effective value of a setting is determined.

Setting	Local Policy	Site GPO	Domain GPO	OU GPO	Effective Value
Setting 1	Configured	Not Configured	Not Configured	Not Configured	Local
Setting 2	Configured	Not Configured	Not Configured	Configured	OU
Setting 3	Configured	Not Configured	Configured	Not Configured	Domain
Setting 4	Configured	Configured	Configured	Configured	OU
Setting 5	Not Configured	Not Configured	Configured	Not Configured	Domain

Table 1. GPO Processing (LSDOU) and Effective Values

In this case, a unique GPO is created and applied at the site level, domain level, and first level OU. If setting 1 represents a configurable item that is defined locally and not configured in any GPO at the different levels, the local setting is the effective setting.

In the case of setting 2, it is configured locally and at the OU level. Based on the order of processing (LSDOU), the value selected at the OU level prevails and becomes the effective setting.

Going back to figure 1, the structure shown can be redesigned as shown in figure 2 on the next page.

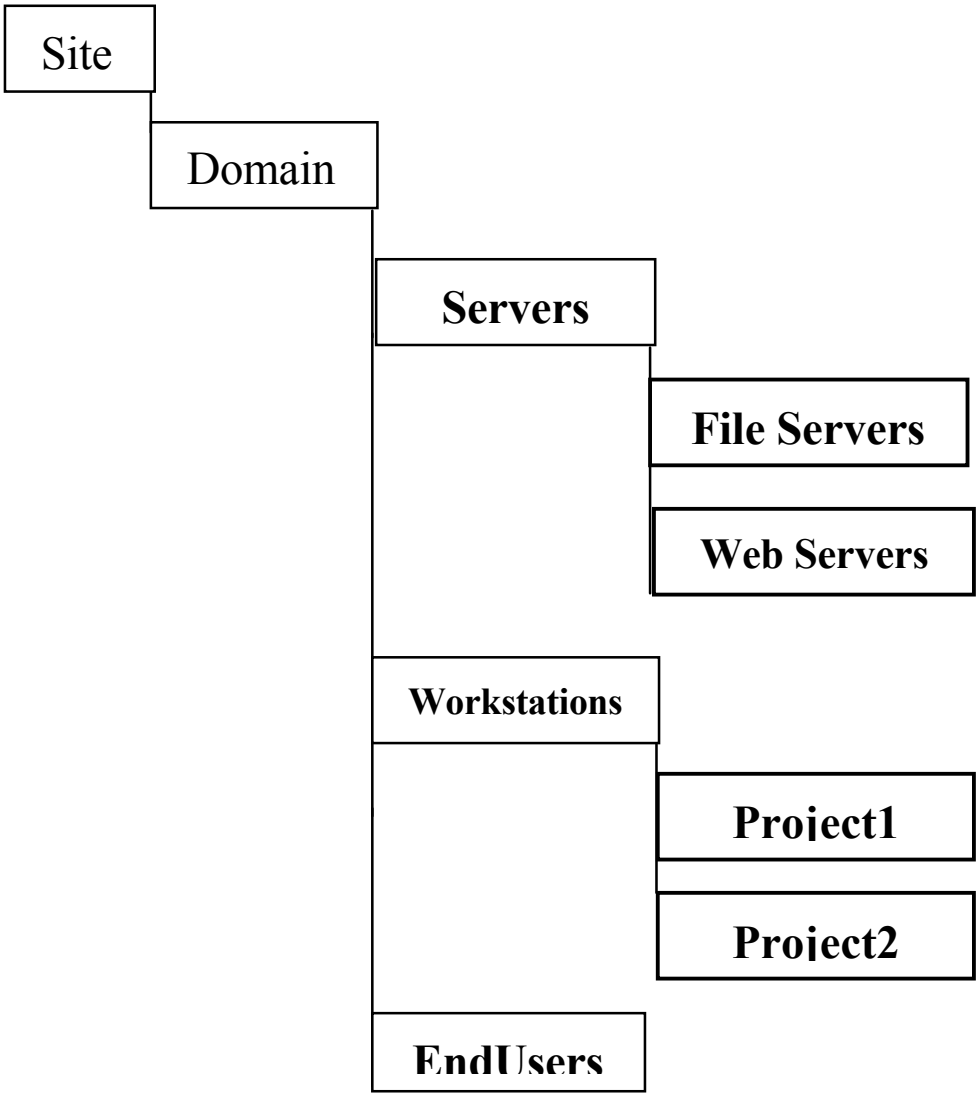

Figure 2. AD Structure with Sub-level OUs

With this new structure, additional GPOs can be created and applied. For instance, at the Servers OU level, computer configuration settings common to all servers can be configured in a GPO and applied at that level. At the sublevel OUs, GPOs defining computer configuration settings specific to the type of server can be created and applied. The same is true for workstations. In the case of

the EndUsers OU, a GPO defining the user configuration settings can be created and applied.

II. Computer Configuration Settings

Computer configuration settings can be considered static settings since once a machine joins a domain, the resulting effective settings can only be overridden by similar settings available in the User Configuration portion of a GPO or by changing the value in the prevailing GPO. It is essential to note that Computer Configuration settings are applied during the boot-up process whereas User Configuration settings are applied at log-on.

Figure 3 shows an OU structure where machines have been grouped and moved to their respective OUs. It also shows users members of the EndUsers OU.

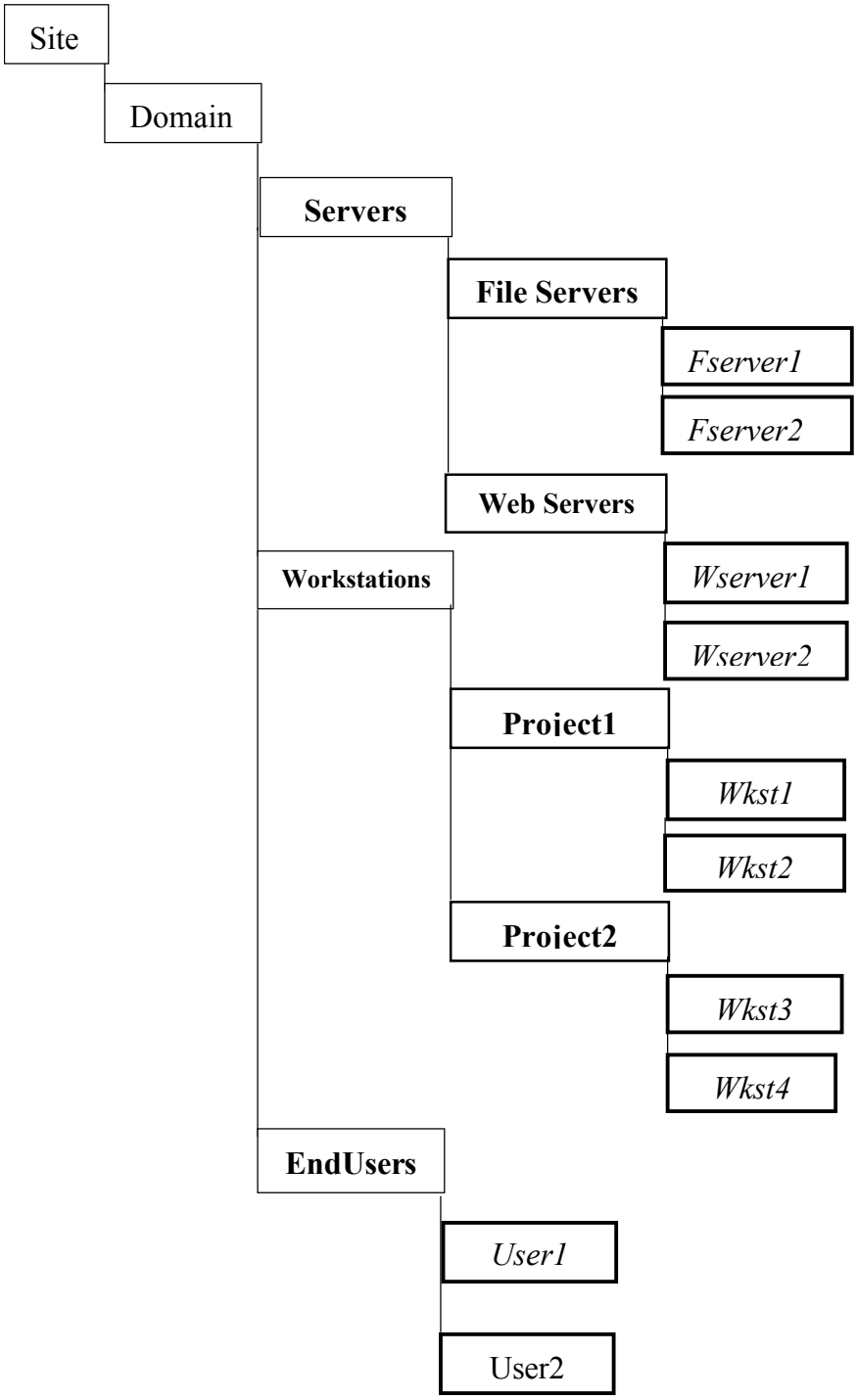

Figure 3. AD Structure with Sub-level OUs and Grouped Members

Each project OU has a different GPO with computer configuration settings defined. The settings of each GPO can be configured based on the particular circumstances of the project. A third GPO defining common settings across projects can be created and applied at the Workstation level.

III. User Configuration and Role-based Permission Groups

The User Configuration section of a GPO defines system behavior, desktop settings, security settings, assigned applications, and published applications. The fact that these settings are applied at log-on makes possible the use of group policy filtering to augment the granularity of the system administration process, thus enhancing security. It also helps minimize the complexity of the AD structure by keeping users together under the same OU.

Table 2 shows possible roles that can be used to create different groups (analysts, consultant, etc…). In this case, any given user will belong to only one group.

Projects	Roles			
	Analyst	Consultant	Manager	Partner
Project 1	20	5	2	1
Project 2	15	3	1	1
Project 3	50	15	3	2

Table 2. Users per Project and their Career Level.

The next step is to define what settings are going to apply to each group. Since the main difference is the software packages required to perform their jobs, the user configuration portion of the GPO can be used to specify which software package will be available to each user. Table 3 depicts this.

Role	Office Tools	Development Tools	Financial Tools	Videoconference/Sharing Tools
Analyst	**X**	**X**		
Consultant	**X**	**X**		
Manager	**X**	**X**	**X**	**X**
Partner	**X**	**X**	**X**	**X**

Table 3. Software Requirements per Career Level.

In this scenario, only two software package combinations are needed. The first GPO will contain office and development tools whereas the second one will contain office tools, development tools, financial tools, and videoconference/sharing tools. In summary:

GPO A = {Office Tools, Development Tools}
GPO B = {Office Tools, Development Tools, Financial Tools, Videoconference/Sharing Tools}

Once the proper settings of each GPO have been configured, the next step is to apply both GPOs at the EndUsers OU level and perform group policy filtering.

IV. Group Policy Filtering

Once the two GPOs are created they have to be applied at the EndUsers OU level. Figure 4 shows the two GPOs available at the EndUsers OU level.

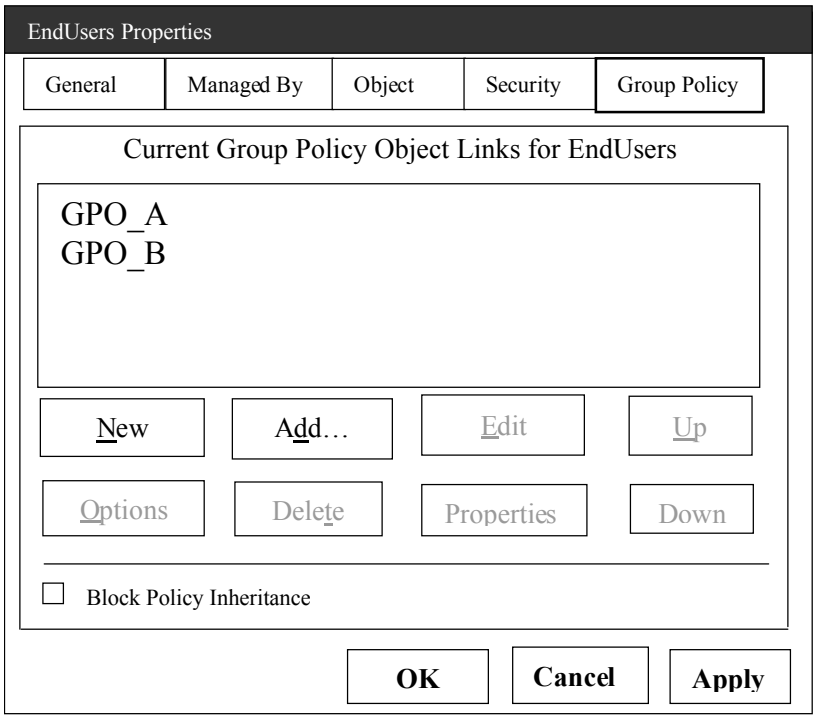

Figure 4. Representation of the EndUsers OU - Properties (Group Policy Tab) Window.

The following steps are required to filter GPOs using role-based permission groups:

1. *Right-click* **GPO_A**
2. *Choose* **Properties**
3. *Click* the **Security Tab**. Figure 5 shows the available groups and permissions.
4. *Select* the **Authenticated Users** group and clear **Allow Apply Group Policy**.
5. *Click* **Add**. Either select the **analysts** group and the **consultants** group from the list or enter their names directly using a semicolon to separate them. *Close* window when finished.
6. *Select* the analyst group and mark **Allow Apply Group Policy**. **Allow Read** should be marked by default. Do the same with the **Consultants** group.
7. Repeat steps 1 through 6 using GPO_B, which has to be applied to the **Managers** and **Partner** groups only.

.

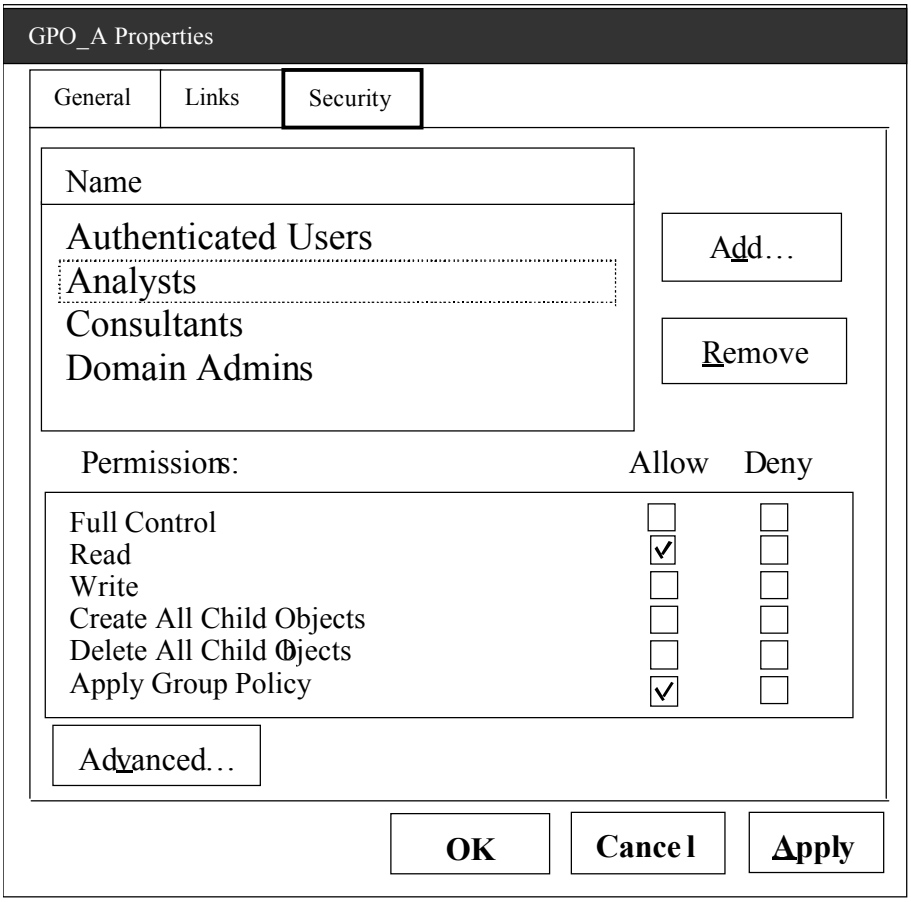

Figure 5. Representation of the GPO_A – Properties (Security Tab) Window

By performing the previous steps, the following is accomplished:

1. Every user has the potential to belong to the Authenticated Users group. Denying Apply Group Policy ensures that all users except those included in the desired groups will not get the GPO.
2. Explicitly allowing Apply Group Policy to desired groups ensures that only users belonging to these groups will get the settings from the GPO. In the case of GPO_A, only users belonging to the Analysts and Consultants groups get the settings from the policy. GPO_B is only applied to users belonging to the Managers and Partner groups.

3. Once these steps are performed, any user belonging to the defined groups will have available the corresponding software.

VII. Conclusion

Active Directory, Group Policy Objects, Organizational Units, and the ability to filter GPOs are new features that provide system administrators a better and more efficient mechanism to administer and maintain Windows 2000 environments. There is an increased overhead associated with the planning and designing of the environment. But once implemented, the amount of time required to perform common administrative tasks is significantly reduced while providing a more granular control over objects and their permissions. The end result is an increased level of security by taking the "Least Privilege" principle a step further.

II. References

Carter, Alan R. Windows 2000 MCSE Study System. Foster City: IDG Books Worldwide, 2000.

Jennings, Roger. Admin 911 : Windows 2000 Group Policy. Berkley: Osborne/McGraw-Hill, 2001.

Lowe-Norris, Alistair G. "Windows 2000 Active Directory: Chapter 8 – Profiles and Group Policy Primer. January 2000. URL: http://www.oreilly.com/catalog/win2000ads/chapter/ch08.html (November 20th, 2001).

Lane, Brent (Oakridge Consulting Group). "Best Practices for System Policies in Windows 2000 Networks." URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/tcevents/itevents/network/tnq10107.asp (November 24th, 2001).

Microsoft. "Windows 2000 Distributed Security Features Security Services." URL: http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/evaluate/featfunc/secover.asp (November 24th, 2001).

Last Updated: June 25th, 2017

Upcoming Training

SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	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 Phoenix SEC401	Phoenix, AZ	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
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
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 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 Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	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 Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Community SANS San Diego SEC401	San Diego, CA	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
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