Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Discretionary Access Control Knowledge, a Practical System

This paper offers a new solution for administrators to reduce abuse of access controls and simplify permissions management. The end-user's abuse of access controls is a threat to network resources. The poorly configured permissions by the administrator produce a vulnerability. The countermeasure is knowledge and efficient techniques. If the concepts of "THE SNAIL" and the best practices are followed, administrators will be able to reduce the confusion of calculating the effective cumulative permissions. Using THE GRID ...

Copyright SANS Institute

Author Retains Full Rights

AD

Discretionary Access Control Knowledge, a Practical System

© SANS Institute 2003, Author retains full rights.

GIAC Security Essentials Certification (GSEC)
Practical Version 1.4b, Option 1
July 7th, 2003

Dean Bushmiller, CISSP

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract 3
Introduction 3
Who needs to know more about permissions? 3
What are the current systems of group organization? 4
THE SNAIL 4
How can we organize groups and permissions to reduce confusion? 5
Local groups 5
Global groups 5
Nesting Global groups 5
Universal groups 5
Summary of Groups and use 6
Naming conventions 6
Is there a system to decipher existing permissions? 6
THE GRID 7
Steps to populate THE GRID with data 7
THE FIVE RULES for NT 4.0 7
Permission types 10
THE FIVE RULES for Windows 2000 11
Permission types 14
What are best practices for permissions? 14
Conclusion 14
List of Sources 15

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

This paper offers a new solution for administrators to reduce abuse of access controls and simplify permissions management. The end-user's abuse of access controls is a threat to network resources. The poorly configured permissions by the administrator produce a vulnerability. The countermeasure is knowledge and efficient techniques. If the concepts of "THE SNAIL" and the best practices are followed, administrators will be able to reduce the confusion of calculating the effective cumulative permissions. Using THE GRID and THE FIVE RULES allow administrators to quickly identify and reduce vulnerabilities. By understanding permissions, you increase the security of file servers and your network.

Introduction

The popular operating systems today are Microsoft NT 4.0 and Windows 2000. These operating systems offer a great deal of control over resources to end-users in the form of discretionary access control. Typically, corporate documents are stored on these operating systems in an insecure manner. Our highest threat to our data is our users, as supported by a 2001 Information Security Magazine survey. 58 percent of the 2545 IT managers cited abuse of access controls as an internal breach.[1] Further, SANS lists "Unprotected Windows Networking Shares" as one of the top twenty vulnerabilities.[2] Discretionary access control for the Microsoft operating systems needs to be better understood.

This paper answers the questions:

- Who needs to know more about permissions?
- What are the current systems of group organization?
- How can we organize groups and permissions to reduce confusion?
- What is a system to decipher existing permissions?
- What are best practices for permissions?

Who needs to know more about permissions?

Users, Administrators and Auditors need to clearly understand permissions. More than half of users abuse access control. Users need to be aware of the impact of their abuse on the business processes. Most administrators do not take the time to manage permissions correctly. As security professionals, we should go after the low hanging fruit of systematically tightening permissions.

[1] Briney, Information Security October 2001, 40

[2] SANS, SANS / FBI The Twenty Most Critical Internet Security Vulnerabilities, 1

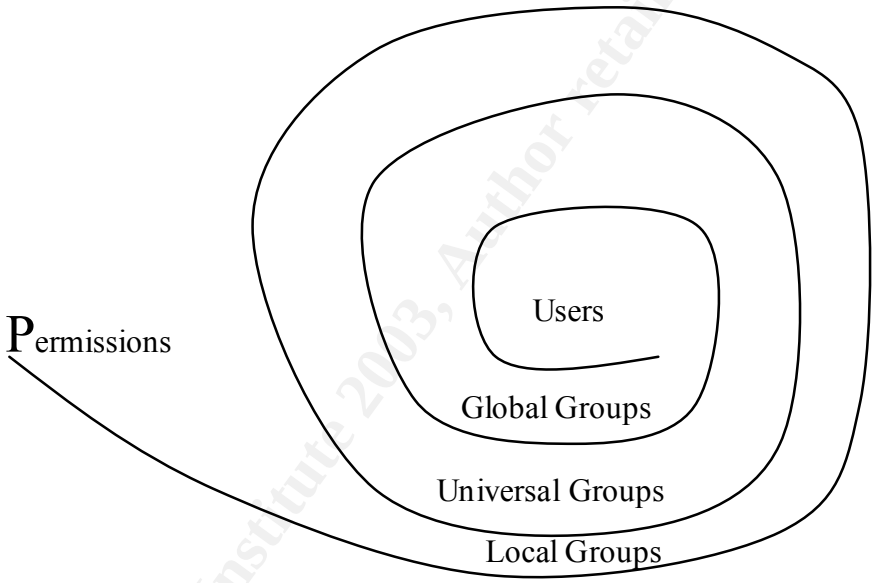
© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Audits have become a hot issue due to corporate scandals. But auditors rarely check the effectiveness of permissions; they only check the access events in the reporting functions.

What are the current systems of group organization?

A proprietary system in Microsoft Official Curriculum will teach you what kinds of permissions exist, what type of groups are possible, and their best practice of using "AGDLP". [3] Microsoft offers two different designs for group nesting. Microsoft differentiates between domain local groups and local groups, which is confusing. No information is discussed regarding built-in groups. Further complexity is added by the nesting of global groups in global groups, which can only be achieved in "native mode". Administratively this can cause increased overhead and confusion.

THE SNAIL



Another way to define the order of group and user nesting is THE SNAIL: Users go in Global groups, Global groups go in Universal groups, Universal groups go in Local Groups, and Local groups are assigned permissions.

When drawn, THE SNAIL model remains consistent in a single domain, multi-domain and 2K forest. If you do not have one of the group types, it still holds true. For example, if you do not have Universal groups because you are not in Windows 2000 Native mode, then Global groups go in Local groups. THE SNAIL is also easy to remember either by visualization or simple verbal repetition.

[3] Green, AGDLP documentation sample, 1

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

How can we organize groups and permissions to reduce confusion?

Before we organize groups we need to understand the purpose of each group type.

Local groups

Local groups were originally used for small local area networks to organize users based upon resource needs or permissions. These small networks consisted of a single server and a few clients. Organization of resources was simple.

Global groups

As local area networks grew to include separate security boundaries, administrators found it necessary to control multiple resources concurrently. Global groups solved the issue of traversing domain boundaries.

Nesting Global groups

Why nest global groups in local groups? A single domain can organize users under local groups for permissions. If we add a second domain, the Local group cannot be assigned permissions in the second domain. We now need Global groups and a trust to cross the domain boundary. It is possible to use global groups exclusively, but they do not exist on stand-alone servers.

Universal groups

Under NT 4.0 there were no Universal groups but there were large multi-domain structures with the need for groups of users to access the same type of resources across domain boundaries. Taking each domain-bound group of users and placing them in a local group with permission to the resource allowed groups of users to manage resources across domains. This management technique needed to be done for every new domain that was trusted. The number of administrative points was calculated by the equation: Administrative Points = Local Groups * Global Groups.

Universal groups do away with the multiplicative increase of administrative burden by allowing a single group in the forest to span all domains. Now we place the universal group in the local group of each domain and place each Global group in the Universal group. The equation now becomes: Administrative Points = Local Groups + Global Groups + 1 (Universal group)

Use of Universal groups only becomes necessary when we have more than 3 domains in a forest that require access to each other's resources.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Summary of Groups and use

We should follow THE SNAIL model because:

- The Universal group is used to reduce administrative overhead and confusion.
- Nesting Global groups in Local groups allows us to cross domain boundaries in a multi-domain scenario with multiple file servers.
- Naming conventions are less confusing if we simplify the number and type of groups discussed.

Naming conventions

Organization is very difficult when mixed groups are used. In an enterprise environment, we run into mixing of groups, as proven by the before and after excel spread sheet from Fair Haven International.[4] If we follow the model of THE SNAIL, permissions are set on the Local group only. We need a clear naming convention for the association of user functions to global groups and of permissions with the share. Our convention is as follows: Local groups are named Lg(Sharename)(Permission). Global groups are named Gg(GroupDepartment/Function). Universal groups are named Ug(GroupDepartment/Function)

Examples:
LgHomeFC
LgHomeM
LgAccountingDataRX
LgStuffNA

GgAccounting
GgAccountingMgrs
GgAuditors

UgHumanResources

Typically we will see 2 or 3 groups for each share: RX Read/Execute, M Change (modify), FC Full Control, NA No Access (Deny) Other special permissions can be noted by S.

Is there a system to decipher existing permissions?
Until now, no. THE GRID & THE FIVE RULES is penicillin for permissions.

How many times have you heard, " I can't get to the file"? The standard approach is to give full control over the folder or document to the individual. Sometimes this does not work, so we rip out the permissions and start over. These blunt instruments cause a great deal of pain, not to mention opening the network resources to the possible abuse of privilege by the user.

[4] Green, AGDLP documentation sample, 1-2

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

There are many articles on permissions but none of them discuss the way to calculate permissions in a real world environment. THE GRID & THE 5 RULES is simple to use and can be proven against the traditional explanations of access control entries and access control list. The system proposed here will work for both NT 4.0 and Windows 2K.

We will start with a blank Grid and step thru the Rules.

THE GRID

THE GRID offers a simple format for documenting the current permissions structure. The rows of the grid represent the many possible assigned permissions and one subtotal row. The three columns in THE GRID represent the three types of permissions: Share, NTFS folder, and NTFS file. The goal is to correctly determine the Effective Cumulative Permissions (ECP) based on any scenario.

	Share	NTFS folder	NTFS file	
User				
Group 1				
Group 2				E.C.P.
Subtotal				

Steps to populate THE GRID with data

All of the information needed for documentation can be ascertained by sitting at the computer with the file share. Use the windows explorer to navigate to the folder, right click on the shared folder, and then choose properties. In the Sharing sheet tab, click the permissions button to see the sharing permissions. On the Security sheet tab click the permissions button to see the NTFS folder permissions. After navigating to the file in the windows explorer, right click and choose properties, on the security sheet tab click the permissions button to see the NTFS file permissions. Write the permissions in the grid.

THE FIVE RULES for NT 4.0

The rules of THE RULES

- You must step thru the rules in order.
- You must test for every rule.

THE RULES:

1. Local or Remote? If local, share column is crossed out
2. If UNC & file name are known, File permissions win *
3. No Access = No Access

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4. In each column, combine the permissions downward for the least restrictive permission
5. In the subtotal row, combine the permissions for the most restrictive permission

Explanation of the rules:
Rule # 1 has some very limited applications. If you are sitting on the file server you must ask yourself the question: What are *your* share permissions as opposed to someone across the network? Since you don't see the share permissions locally, they do not count. Consequently, you must cross off the entire share column in THE GRID if you are sitting at the server that contains the shared resource. This case occurs when two people are in the same groups and one is testing permissions locally (they can get in) versus you testing permissions remotely (you cannot get in).

	Share	NTFS folder	NTFS file	
User				
Group 1				
Group 2				E.C.P.
Subtotal				

Rule # 2 is more rare than #1. The default installation of NT4.0 is POSIX compliant[5]; this has known security vulnerability[6], so most systems administrators turn POSIX compliance off. The POSIX subsystem requires a user with direct permissions set on the file to have access to the file regardless of the permissions set at a higher level. (This is why when you give away FC to the user on the file, they can get access.) Again, this is rare but possible.

	Share	NTFS folder	NTFS file	
User				
Group 1				
Group 2				E.C.P.
Subtotal				

Rule # 3: If the No Access permission is found anywhere in a column, all other permissions are ignored in that column. So the subtotal of any column with No Access is No Access and you move on to the next column; no other assessment in that column is necessary. NOTE: Not specified is not the same as No Access. You ignore Not Specified.

[5] Microsoft, Microsoft Windows NT, the Foundation: Design Goals, System Architecture, 1
[6] Courington, A Step-by-Step Guide to Securing Windows 2000 for Use as an Internet Server, 13

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Execute Rule # 3 for each of the three columns, Share, NTFS folder, and NTFS File.

	Share	NTFS folder	NTFS file	
User	Full Control	Read		
Group 1	No Access		Read	
Group 2	Read	No Access		E.C.P.
Subtotal	No Access	No Access		

Rule # 4: Examine all of the permissions in the column and determine which is the least restrictive; this becomes your subtotal permission for each column. If the permissions are not mutually exclusive, combine them, as in the case of List and Read or Read and Write.

	Share	NTFS folder	NTFS file	
User	Full Control	Read	Write	
Group 1		List	Read	
Group 2	Read			E.C.P.
Subtotal	Full Control	Read & List	Write & Read	

You now have three permissions in the subtotal row at the bottom of THE GRID.

Rule # 5: Examine all of the permissions in the subtotal row only. Find the most restrictive. This most restrictive permission becomes your Effective Cumulative Permission.

	Share	NTFS folder	NTFS file	
User	Full Control	Read	Write	
Group 1		List	Read	
Group 2	Read			E.C.P.
Subtotal	Full Control	Read & List	Write & Read	Read & List

In the example below there are 5 rows, which correspond to a user and 4 groups; however, this can be extended to accommodate as many groups as the situation requires. Special built-in groups should be investigated if this is a foreign system. The built-in groups are "pseudo-groups automatically defined by Windows NT (*Everyone*, referring to any user; *Interactive*, which applies to any currently logged-in user; *Network*, for permissions that apply to remote access of

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

a file/directory; and *Authenticated Users*, limited to users that have been authenticated by presenting a valid username and password)."[7]

Permission types

NT 4.0 has share permissions of Read, Change, Full Control, and No Access.

NT 4.0 has NTFS permissions of Read, Write, Execute, Delete, Change Permissions & Take ownership. These are combined together to give us standard permissions of: Full Control, No Access, List, Read, Add, Add & Read, Change, Special Directory and Special file.

For the example below we will not follow any user or group management of permissions, such as THE SNAIL. As in the real world, the example below addresses the messiest most convoluted permissions possible. We will use Example 1 to prove each of the FIVE RULES.

Example: A remote user belongs to Group #1, Group #2, Domain Users and Everyone. The POSIX compliance is turned OFF. The permissions are as follows:

User has
- Share permissions of Full Control
- NTFS Folder permissions of List
- NTFS File permissions of Read

Group #1 has
- Share permissions of Change,
- NTFS Folder permissions of NOT Specified
- NTFS File permissions of NOT Specified

Group #2 has
- Share permissions of Full Control,
- NTFS Folder permissions of NO Access
- NTFS File permissions of NOT Specified

Domain Users has
- Share permissions of NOT Specified
- NTFS Folder permissions of List
- NTFS File permissions of Change

Everyone has
- Share permissions of Full Control
- NTFS Folder permissions of NOT Specified
- NTFS File permissions of NOT Specified

[7] Frisch, Understanding ACLs, 38

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Rule #1 & 2 Do not Apply.

Rule #3

	Share	NTFS folder	NTFS file	
User	Full Control	List	Read	
Group 1	Change		Read	
Group 2	Full Control	No Access	Write	
Domain Users		List	Change	
Everyone	Full Control			E.C.P.
Subtotal		No Access		

Rule #4

	Share	NTFS folder	NTFS file	
User	Full Control	List	Read	
Group 1	Change		Read	
Group 2	Full Control	No Access	Write	
Domain Users		List	Change	
Everyone	Full Control			E.C.P.
Subtotal	Full Control	No Access	Change	

Rule #5

	Share	NTFS folder	NTFS file	
User	Full Control	List	Read	
Group 1	Change		Read	
Group 2	Full Control	No Access	Write	
Domain Users		List	Change	
Everyone	Full Control			E.C.P.
Subtotal	Full Control	No Access	Change	No Access

THE FIVE RULES for Windows 2000

The rules of THE RULES

- You must step thru the rules in order.
- You must test for every rule.

THE RULES:

1. Local or Remote? If local, share column is crossed out
2. If UNC & file name are known, File permissions win
3. Expand combination permissions where deny is checked and deny those permissions
4. In each column, combine the permissions downward for the least restrictive permission
5. In the subtotal row, combine the permissions for the most restrictive permission

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Window 2000 has a more granular permission structure. Please note: No Access has been replaced by a two-column system. 'Allow' and 'Deny' can be applied to each possible permission. Applying Rule #3 in the same fashion will yield incorrect results. So let's adjust the rules.

Rule # 1 has some very limited applications. If you are sitting on the file server you must ask yourself the question: What are *your* share permissions as opposed to someone across the network? Since you don't see the share permissions locally, they do not count. Consequently, you must cross off the entire share column in THE GRID if you are sitting at the server that contains the shared resource. This case occurs when two people are in the same groups and one is testing permissions locally (they can get in) versus you testing permissions remotely (you cannot get in). Rule # 1 in Windows 2000 is identical to Rule # 1 in NT4.0.

	Share	NTFS folder	NTFS file	
User				
Group 1				
Group 2				E.C.P.
Subtotal				

Rule # 2 is more rare than #1. The default installation of Windows 2000 is POSIX compliant; however, it is not turned on. This is not to say that the POSIX subsystem is not installed.[8] This is the opposite of NT4.0. The POSIX subsystem requires a user with direct permissions set on the file to have access to the file regardless of the permissions set at a higher level. (This is why when you give away FC to the user on the file, users can get access.) Rule # 2 is typically ignored in Windows 2000 default installations.

	Share	NTFS folder	NTFS file	
User				
Group 1				
Group 2				E.C.P.
Subtotal				

Rule #3 under Windows 2000 requires two steps. Step A. Expand any combination permissions where deny is involved. Step B. For every 'Deny' permission, eliminate the corresponding 'Allow' for the entire column.

[8] LABMICE.net, Windows 2000 Security Checklist, 1

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Execute Rule # 3 for each of the three columns, Share, NTFS folder, and NTFS File. In most cases a full expansion is not necessary. Please note: It is important to know what is specifically denied to derive the Effective Cumulative Permissions.

	Share	NTFS folder	NTFS file	
User	Full Control	Read	Modify = ~~Read~~/ Write/ Exec/ Del	
Group 1			DENY Read	
Group 2	Read			E.C.P.
Subtotal			Write/ Exec/ Del	

Rule # 4: Examine all of the permissions in the column and determine which is the least restrictive; this becomes your subtotal permission for each column. If the permissions are not mutually exclusive, combine them, as in the case of List and Read or Read and Write. Rule # 4 in Windows 2000 is identical to Rule # 4 in NT4.0.

	Share	NTFS folder	NTFS file	
User	Full Control	Read	Modify = ~~Read~~/ Write/ Exec/ Del	
Group 1			DENY Read	
Group 2	Read			E.C.P.
Subtotal	Full Control	Read	Write/ Exec/ Del	

You now have three permissions in the subtotal row at the bottom of THE GRID.

Rule # 5: Examine all of the permissions in the subtotal row only. Find the most restrictive. This most restrictive permission becomes your Effective Cumulative Permission. Rule # 5 in Windows 2000 is identical to Rule # 5 in NT4.0.

	Share	NTFS folder	NTFS file	
User	Full Control	Read	Modify = ~~Read~~/ Write/ Exec/ Del	
Group 1			DENY Read	
Group 2	Read			E.C.P.
Subtotal	Full Control	Read	Write/ Exec/ Del	Read

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Permission types

Windows 2000 has share permissions of Read, Change and Full Control. Each permission can be modified with deny or allow, for a total of 6 permissions.

Windows 2000 has NTFS permissions of the following: Traverse Folder/ Execute File, List Folder, Read Attributes, Read Extended Attributes, Create Files / Write data, Create Folders/Append Data, Write Attributes, Write Extended Attributes, Delete Subfolders and Files, Delete, Read Permissions, Change Permissions, Take Ownership. Each permission can be modified with deny or allow, for a total of 26 permissions.

What are best practices for permissions?

- At the share level:
  - Disable sharing wherever it is not required.[9]
  - Remove the Everyone group permissions.
  - At a maximum, apply the change permissions to Authenticated Users.
  - Apply Full Control to Administrators , only when necessary.
- Apply permissions at the NTFS Folder level.
- Apply permissions only to Local Groups.
- Do not specify permissions instead of denying permissions.

Conclusion

Microsoft is not to blame for discretionary access control threats, administrators are. Knowledge is a requirement to reduce these threats. If you know the key concepts of group and permission management you can protect your network resources better.

With THE SNAIL, THE GRID, & THE FIVE RULES as tools for demystifying groups and permissions we can reduce poor design of access control thereby decreasing the possible threats to our data.

[9] SANS, SANS / FBI The Twenty Most Critical Internet Security Vulnerabilities, 1

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

List of Sources

Briney, Andy."2001 Industry Survey." Information Security Magazine. October 2001. http://www.infosecuritymag.com/articles/october01/images/survey.pdf. (7/17/2003)

Briney, Andy & Prince, Frank. "2002 Industry Survey." Information Security Magazine. September 2002 http://www.infosecuritymag.com/2002/sep/2002survey.pdf. (7/17/2003)

Courington, David, A Step-by-Step Guide to Securing Windows 2000 for Use as an Internet Server. 3/29/2001. http://www.sans.org/rr/papers/66/181.pdf. (7/17/2003)

Frisch,Æleen. Understanding ACLs. SW Expert. April 2000. http://swexpert.com/C5/SE.C5.APR.00.pdf. (7/17/2003)

Green,Kevin .AGDLP documentation sample,9/18/2001, http://www.fairhavenintl.com/Samples/AGDLP.xls (7/17/2003)

LABMICE.net.Windows 2000 Security Checklist. 6/1/2003. http://www.labmice.net/articles/securingwin2000.htm. (7/17/2003)

Microsoft. "Microsoft Windows NT. the Foundation: Design Goals. System Architecture". 3/28/2002. http://www.microsoft.com/ntserver/techresources/foundation/1_introduction.asp. (7/17/2003)

Microsoft. "Subordinate Explicit Grant Overrides Inherited Denial. Microsoft Knowledge Base Article – 233419". 5/14/2003 http://support.microsoft.com/default.aspx?scid=kb%3ben-us%3b233419 (7/17/2003)

Russell, Deborah and Gangemi, G.T, Computer Security Basics. Cambridge, MA.: O'Reilly, 1992.

The SANS Institute.SANS / FBI The Twenty Most Critical Internet Security Vulnerabilities. v3.23. 5/29/2003 http://www.sans.org/top20/ (7/17/2003)

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: September 5th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced