Global Information Assurance Certification Paper

10 Simple Rules for Dating my Exchange Antivirus Gateway

Chris Green
GSEC Practical Assignment v1.4
Option 1 – Research on Topics in Information Security

Abstract

Defense in Depth teaches us that all gates must have a keeper. CD ROMs, diskettes, network shares, FTP, and E-mail are all gates upon which a user's computer can become infected by viruses. As we are responsible for – at a minimum – the availability of our users computers, it is our responsibility to set up the keeper at each gate to protect against issues such as viruses.

This paper will review four Antivirus gateways for Microsoft Exchange 5.5 Groupware platform. It will provide setup commonality to ensure independence and fairness, standard test practices to ensure features are equally tested, and unbiased results.

With the information provided in this document, you should see that there is a product that will service your needs, and possibly introduce you to needs you might not have thought of. In addition, it will show you there is really no reason for you to not have one of these products protecting your Exchange server from viruses and unwanted file types.

Introduction

Antivirus is a critical aspect of enterprise security. There was however a misconception that because Antivirus was installed on users workstations, the job was done. While this does protect against contaminated files accessed by the workstation, it marginally protects against files received via E-mail.

To follow the Defense in Depth strategy, organizations are now employing Antivirus software at the groupware or E-mail level. Most importantly they scan incoming file attachments for viruses. And being good Internet neighbors, it provides the ability to scan file attachments on their way to the Internet.

This is import to Defense in Depth because Antivirus software is not 100% and is also susceptible to user error. If Antivirus software on a workstation becomes corrupt and stops working, or the network administrators forgot to install Antivirus on a particular computer, then they are now open to virus attacks.

And to take it a step further, most software now allows you to create a list of file types that you would like blocked. VBS script files are a common mechanism of

distributing viruses. Through file blocking, you can now disallow all .vbs files from entering your network through E-mail. This is especially important for protecting against viruses that have not been discovered by your Antivirus software provider.

Threat Vectors

The obvious threat vector when discussing Antivirus software is Attack from Malicious Code. However it can be argued that Antivirus actually embodies other vectors as well. This section will review the threat vectors that Antivirus software on your Exchange server protects against.

Outsider Attack from Network
Trojans are typically transmitted via E-mail. Trojan payloads can include remote system control software and keystroke logging. As this directly attacks a computer from the outside network, Exchange Antivirus software protects against this threat vector.

Insider Attack from Local System
Once a Trojan or virus has been introduced into your system, is can start to attack other workstations in your network, web servers, and file servers. Preventing infections from occurring and/or spreading protects against insider attack from local system.

Attack from Malicious Code
As we said earlier, the obvious threat vector for E-mail gateway based viruses is attack from malicious code.

Lab Setup

The following section discusses how the systems were set up, and what the configuration of each system was. The most important aspect of the setup was to ensure the network was isolated, self sufficient (aside from the Internet connection), and fair to all vendors.

Having an isolated network required that two servers be used. This allowed the network to be self-sufficient while still providing SMTP mail exchange.

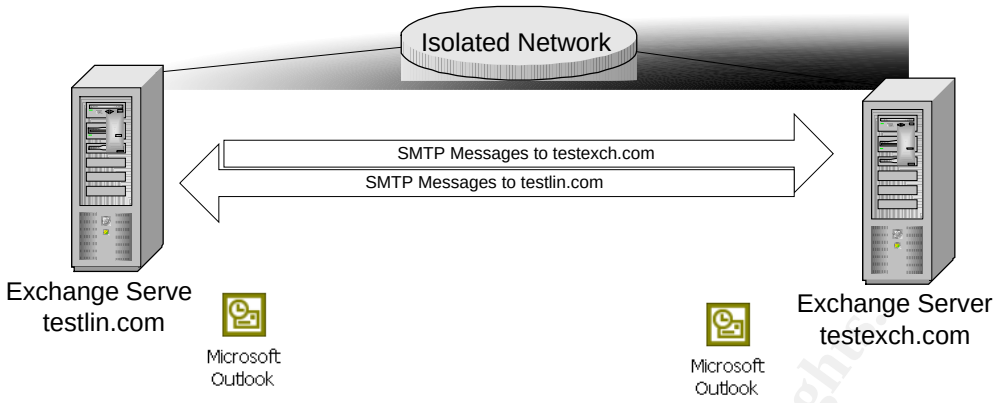


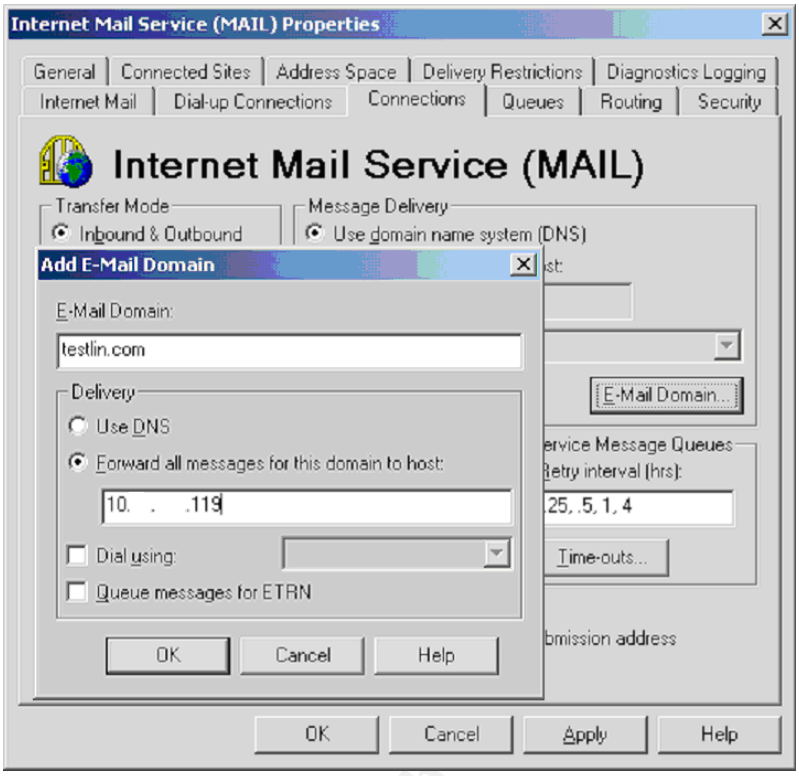
Figure 1 System Connection and Communication

For simplicity, two Windows 2000 servers were used, both running Exchange Server 5.5 service pack 4. Each server belonged to its own domain so that E-mail sent between the two systems would be sent via SMTP. This would test the Internet Mail Connector in Exchange, which provides the sending and receiving of SMTP E-mail.

The testexch.com server was designated as the "guinea pig" host and would have the gateway Antivirus products installed on it one at a time. When testing for a specific product is completed, the software is removed and the computer is rebooted. Without doing this, the individual products may interfere with each other tainting the testing process.

Both servers have Microsoft Outlook installed and configured to use mailboxes locally to their Exchange installation. This removes the requirement to have a desktop PC and because we are using MAPI from Outlook to the Exchange server, it emulates a real Exchange environment.

The servers are configured so that in the Internet Mail Connector configuration, any E-mail initiated on testexch.com destined to testlin.com, is sent directly to the IP address of the testlin.com server. Likewise, any E-mail generated on testlin.com destined to testexch.com is sent directly to the IP address of testexch.com. This can also be done with DNS, but this is the easiest method in an unchanging, static lab environment. The following illustration shows how this is done.



The hardware configuration was important as four products were being reviewed and slow servers would unnecessarily drag the comparison process. The hardware configuration is as follows:

Testexch.com

Dell Optiplex GX260
P4 2.0 Ghz
20GB IDE HDD
256MB RAM
Integrated NIC
Windows 2000 Server with Active Directory Enabled
Service Pack 3
Exchange Server Enterprise 5.5 with Service Pack 4
SMTP Inbound/Outbound configured for testexch.com domain

Testlin.com

Dell Optiplex GX400
P4 1.6Ghz
60GB IDE HDD
256MB RDRAM
Integrated NIC
Windows 2000 Server with Active Directory Enabled
Service Pack 3

Exchange Server Enterprise 5.5 with Service Pack 4
SMTP Inbound/Outbound configured for testlin.com domain

Testing Practices

In order to fairly compare each software application, it is important to have identical tests performed for each product. The following table describes the action performed in each test and what the results will indicate. Wherever possible, these tests will be performed for each product. If a test was unable to be performed it will be noted in the Test Results section.

In order to protect against lab contamination, real viruses were not used. Instead, the EICAR Standard Anti-Virus Test File is used. This is a relatively small file that most Anti-Virus providers treat as a real virus but has no damaging payload. In order to facilitate the discovery the EICAR file as a virus, .COM files are not blocked. If .COM files were blocked, then the eicar.com file would not be recognized as a virus but rather a violator of the file blocking setup.

Test Number	Test Performed	Indication
1	Create E-mail with the following attachments .vbs, .pif, .exe., .eml, .nws, .dll, .bat, .shs and send from Testlin.com to Testexch.com.	Checks effectiveness of file blocking across different file types.
2	Rename all the above extensions to "allowed" extensions and send from Testlin.com to Testexch.com.	Checks to see if renaming the extension can circumvent file blocking. If files are still blocked, then it is not file blocking but actually content blocking.
3	E-mail the EICAR E-mail attachment from Testlin.com to Testexch.com	Checks Inbound SMTP real-time scanning.
4	On Testexch.com, E-mail the EICAR file to a recipient on the same server.	Checks real time Information Store scanning.
5	Create a message with an infected attachment and close the message so that it gets stored in the drafts folder of Outlook.	Once again, checks real time Information Store scanning.
6	Turn off any real time Information Store scanning and MAPI send an infected E-mail attachment to testlin.com.	Tests the Outbound SMTP scanning engine.

7	Turn off any real time Information Store scanning that is performed. Drag and drop infected file directly into Inbox and Drafts folder. Perform scheduled scan.	Validates the effectiveness of scheduled scan jobs on private mailboxes.
8	Drag and drop an infected file to the Exchange Public Folder system.	Tests the Public Folder Information Store real time protection.
9	Turn off real time Information Store scanning and drag and drop a file to the Public Folders. Perform a scheduled scan of the Public Folders.	Confirms that scheduled scans find viruses in Public Folders as well.
10	SMTP E-mail a Zip file with a virus two levels deep.	Checks that nested Zip files are scanned several layers deep for viruses.

Standardized Setup

Vendor fairness requires that all the products be configured in a standardized manner. For example, seven file attachments were sent in the first test, it would not be fair to configure Trend Micro Scan Mail to block all seven attachments and Sybari Antigen to only block six. The following criteria were used when setting up the E-mail Gateway Antivirus products.

Product Knowledge

In order to ensure that the following were actually implemented properly in each test, the product manual was consulted for each product. Where it is available online, a link is included in the References section.

File Blocking

Where applicable, files with the extensions .vbs, .pif, .exe, .eml, .dll, .bat, and .shs were blocked. While this does not encompass all possible files that can transmit viruses, it does provide wide range of file. For example, .vbs and .bat files are text, .exe and .dll files are machine code, and .eml and .shs are files that may have malicious content embedded in it.

For products that had a default set of files to block, the .com filter was removed from the list. In most instances, file blocking occurs before virus checking which consumes more CPU. If .com files were blocked, then the virus checking capabilities would never be tested.

When to Scan

Based upon the tests, inbound, outbound, and internal E-mail should be set up to be scanned by the Antivirus software. In some cases, there are separate services that scan the Internet based E-mail, and the real-time access to E-mail

in user's Inboxes or Public Folders. Either way, all possible scanning was turned on to provide fair test results.

Cleansing
Because we are using the EICAR file, it is not possible to clean it. Therefore, if a virus file cannot be cleaned, then it is to be deleted. That is the true test of the software is that infected files are deleted. For tests such as dragging and dropping the EICAR file into a Public Folder, if the software deletes the file we know it to have found the virus and dealt with it properly.

Just to be sure that we are not susceptible to user error, the software was configured to notify when a virus is found. This can be done by either replacing the file with a text file indicating the infection, or an E-mail sent to an administrator and/or user who submitted the file. Software that did not allow this feature, the test was run twice to ensure accuracy.

Compressed File Scanning
A common feature is to be able to scan Zip or compressed files multiple levels deep. In some instances, you can Zip a Zip file that contains a virus or other content that you want to get past a filter. This feature was turned on when available. In addition, the EICAR site provided the EICAR file in a two level deep Zip file, which was used for the testing.

Best Practices

While this paper provides some ideas as to best practices, it in no way provides the "definitive guide for best practices when protecting your Microsoft Exchange Groupware." However, I did spend quite a bit of time trying to find the ultimate guide to what files can contain viruses, and what your Groupware Antivirus software should block.

The following list of files are copied directly from Microsoft Technical Network Q Article 262631. From this list, you can derive your list of files that should be blocked at your location. In a completely secure setting, all of these files should be filtered by your Groupware Antivirus software.

File extension	File type
.ade	Microsoft Access project extension
.adp	Microsoft Access project
.bas	Microsoft Visual Basic class module
.bat	Batch file
.chm	Compiled HTML Help file
.cmd	Microsoft Windows NT Command script
.com	Microsoft MS-DOS program
.cpl	Control Panel extension
.crt	Security certificate

.exe	Program
.hlp	Help file
.hta	HTML program
.inf	Setup Information
.ins	Internet Naming Service
.isp	Internet Communication settings
.js	JScript file
.jse	Jscript Encoded Script file
.lnk	Shortcut
.mdb	Microsoft Access program
.mde	Microsoft Access MDE database
.msc	Microsoft Common Console document
.msi	Microsoft Windows Installer package
.msp	Microsoft Windows Installer patch
.mst	Microsoft Visual Test source files
.pcd	Photo CD image, Microsoft Visual compiled script
.pif	Shortcut to MS-DOS program
.reg	Registration entries
.scr	Screen saver
.sct	Windows Script Component
.shb	Shell Scrap object
.shs	Shell Scrap object
.url	Internet shortcut
.vb	VBScript file
.vbe	VBScript Encoded script file
.vbs	VBScript file
.wsc	Windows Script Component
.wsf	Windows Script file
.wsh	Windows Script Host Settings file
.app	Visual FoxPro Application
.fxp	Visual FoxPro Compiled Program
.prg	Visual FoxPro Program
.mdw	Microsoft Access Workgroup Information
.mdt	Microsoft Access Workgroup Information
.ops	Office XP settings
.ksh	Unix shell extension
.csh	Unix shell extension
.app	Visual FoxPro Application
.fxp	Visual FoxPro Compiled Program
.prg	Visual FoxPro Program
.mdw	Microsoft Access Workgroup Information
.mdt	Microsoft Access Workgroup Information
.ops	Office XP settings
.ksh	Unix shell extension
.csh	Unix shell extension
	(http://support.microsoft.com/default.aspx?scid=kb;en-us;262631)

Vendors Used

A vendor list was extracted by doing searches on http://www.google.com and entering in the search phrase "Microsoft Exchange Antivirus". Once a vendor was identified as having a Microsoft Exchange Antivirus Product, an evaluation was downloaded. The following is a list of four vendors and links to the information on their web site for the product used.

Trend Micro ScanMail for Microsoft Exchange 5.5
http://www.trendmicro.com/en/products/email/smex/evaluate/overview.htm

Network Associates McAfee Groupshield 5.0SP1 for Exchange 5.5
http://www.mcafeeb2b.com/products/groupshield-exchange/default.asp

Reliable Antivirus 8.2.3.3 for Microsoft Exchange Server 5.5
http://www.ravantivirus.com/pages/showproduct.php?p=56

Sybari Antigen 7.0
http://www.sybari.com/products/antigen_exchange.asp

There was an effort for the following three products to be included in this testing however their web sites did not offer evaluation products for Microsoft Exchange 5.5. These companies are reputable in the Antivirus market and therefore links to their websites are included;

Symantec Antivirus/Filtering 3.0 for Microsoft Exchange
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=66

F-Secure Antivirus for Microsoft Exchange 6.10
http://www.f-secure.com/products/anti-virus/ms-exchange/

Sophos MailMonitor for Exchange 2000
http://www.sophos.com/products/software/mailmonitor/mmexchange.html

Test Results

The following chart represents the results of testing the four vendors. The test number in this chart references the test number in the Testing Practices section. Following this table is a list of notes regarding the tests and can describe why a test was not applicable, or substantiate the results. A ✓ indicates that the test passed, a × indicates that the test failed, and a #/7 indicates how many attachments were caught by the filter if they were not all caught (this applies only to tests 1 and 2).

Test	Trend			

Number	Micro	NAI	RAV	Sybari
1	4/7	✓	×	✓
2	2/7	×	×	×
3	✓	✓	✓	✓
4	✓	✓	✓	✓
5	✓	✓	×	✓
6	N/A	N/A	N/A	✓
7	✓	✓	✓	✓
8	✓	✓	×	✓
9	✓	✓	×	✓
10	✓	✓	×	✓

Notes

1. In test number 1 for Trend Micro, the software only blocked 4 out of 7 attachments. Trend allowed .vbs, .bat, and .shs through to the end user. I double-checked my configuration and E-mailed screen scrapes of my setup to the Trend Micro support department. Their response was that they filter based upon the document type stored in the header of the file and not by extension. Therefore, .vbs and .bat were allowed through because the true type is .txt or text document. They offered a solution to this problem which was to note each filter as *.vbs; instead of vbs;, which I did for all file types. This ended up allowing all types through. By the time I received another response to my inquiry with technical support, I had to move on to another product, and therefore uninstalled Trend Micro's product.
2. In test number 2 for Trend Micro, two file types were detected after the renaming, the .dll file and .exe file. This validates what the support department said in their E-mail relating to test number 1 where they review the header and not just the file extension.
3. In test number 6 for Trend Micro, the test is not applicable as the scanning engine for the Internet Mail Connector and the real time scanning is not separate. Therefore, you cannot turn off real time scanning to test the Internet Mail Connector scanning. This is also the case for NAI McAfee and RAV Antivirus. However, if this test is performed without turning any scanning off, the virus is found on all Antivirus products, which tests that infection attempts from inside to outside will be thwarted by these products.
4. In test number 7 and 9 for Trend and NAI, the entire Antivirus application was shut down in order to prevent the real time scanning from cleaning the virus. Once the virus was placed in the destination folder, the Antivirus software was started and a schedule was created. Because the file already existed, it was not scanned for contamination until it was

accessed. So the effectiveness of the scheduled scan could still be tested by not accessing the file in any way.

5. In test number 7 for RAV Antivirus, the Antivirus software was not turned off because test 5 failed to detect the presence of a virus when it was placed in the Inbox. Therefore, we could place the EICAR file where it needed to be for test 7 and test 9, and the Antivirus software did not detect it. It did however find the virus when the scheduled task ran on the mailbox, but not on the Public Folders.

Observations

The following sections describe observations made of each product that was reviewed. Where possible, these are quantitative observations as this is a non-biased report.

Trend Micro ScanMail for Microsoft Exchange 5.5

When I've run up against mail filters in the past and there was something that I just had to get to the other side, I would always try to rename the extension of the file and send it through. In most instances, it would get through and I thought to myself that this is a major deficiency of these types of products. Trend Micro tries to prevent this by tying in to the header of the file, and not just the file extension. They were the only vendor that had any success in test number 2 where the files were renamed to test content filtering and not just extension blocking.

However, it is also a detriment to them because they do not implement both forms of filter checking. This is evident in the fact that .vbs and .bat files were allowed through. If both forms of checking were performed, their product would no doubt have passed both tests.

Network Associates McAfee Groupshield 5.0SP1 for Exchange 5.5

NAI provided a very solid product that passed all but the extension renaming tests. The interesting part of NAI's implementation is the fact that the configuration occurs within the Microsoft Exchange Administrator's console, which is unique in the products that were tested. Everything worked as expected and time to learn the product was short. Another benefit of NAI is that they provide a full suite of Antivirus products providing you a single source for most Antivirus needs.

Reliable Antivirus 8.2.3.3 for Microsoft Exchange Server 5.5

Reliable Antivirus has less functionality compared to the other products that were tested. It does not implement file blocking and based upon the tests there was no real time scanning. RAV is better positioned to intercept viruses at the Internet Mail Connector level only. The other benefit is that because it is scaled

down, it is substantially smaller in size to download and evaluate. The size was approximately 5MB compared to the other products that were 20MB and higher.

Sybari Antigen 7.0
As a company, Sybari focuses only on Groupware virus protection and does it quite well. It is the only product that separates Internet Mail Connector scanning and real time scanning. While this provides flexibility, where you would actually need this requirement is up to you. The only feature lacking in Sybari is being able to tie into the file header to determine the true file type, and not just extension type. If this feature were added, then it would have tested better then all other products.

Conclusion

Each product reviewed is different and none of them may be perfect for you. RAV is best positioned for protecting Internet mail. Trend Micro is the first to protect against types of file not by extension, but based upon the header. NAI McAfee provides a full suite of products, which allows you to standardize on a single vendor. And Sybari focuses specifically on Groupware protection, which may be of interest to you. In the end, it all boils down to the fact that there is a variety of software available, and no valid excuse for not protecting the gate that is opened to viruses via your Microsoft Exchange E-mail server.

References

Northcutt, S. "Threat Vectors". Security Essentials Day 3 Section 10.3.2, SANS GIAC Securities Essentials Course v1.9a: Page 2-3

Northcutt, S. "Defense in Depth". Security Essentials Day 2 Section 10.2.1, SANS GIAC Securities Essential Course v1.11: Page 1-2

Mitchell, David and Staley, Natasha. "Best practice for using MailMonitor for SMTP with threat reduction". August 2002. http://www.sophos.com/virusinfo/whitepapers/threat.html (21 Dec 2002).

Sajeev, K A. "California Software Laboratories
E-mail Security White paper". December 5, 1999.
http://services.cswl.com/whiteppr/tech/emailsecurity.html (29 Nov 2002).

Little, Keith. "Scrap Files can Tear you Up". July 9, 2000.
http://www.pc-help.org/security/scrap.htm (3 Dec 2002).

Microsoft. "OL2000: Information About the Outlook E-mail Security Update Q262631". December 3, 2002.
http://support.microsoft.com/default.aspx?scid=kb;en-us;262631 (14 Dec 2002).

LaFantano, Michel. "Sybari Antigen 7.0 for Exchange User Manual". October 2002. http://www.sybari.com/download/licensed/manuals/A70ExUserManual.pdf (16 Dec 2002).

Trend Micro. "Scan Mail 3 Documentation" November 2001. http://www.trendmicro.com/ftp/documentation/guides/smex38_352.pdf (19 Dec 2002).

Ducklin, Paul. "European Institute for Anti-Virus Research Test File". http://www.eicar.org/anti_virus_test_file.htm (10 Jan 2003).

Last Updated: May 26th, 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
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
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
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 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
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 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