Global Information Assurance Certification Paper

Increasing VPN Security On A Limited Budget – A Case Study

GSEC Practical Assignment 1.4b

September 2003

Abstract

Acme Widget's has a small network for its North American Corporate office consisting of 7 servers and 30 clients. Acme has a Windows 2000 VPN to support its mobile users. A recent security assessment of the subject company determined that the overall security of the network was good, however, several issues were noted during the review. The most important issue was the security of the VPN solution utilized by the subject company.

This case study describes my efforts to change the VPN solution to provide for more security on a limited budget. It discusses the vulnerabilities with the current solution, possible solutions, and the steps and challenges required to implement the solution.

Before

The Acme International Widgets North American headquarters was set up in 2001 as a result of their growing presence in North America. The mission of the office is to provide support to the Italian Headquarters office and to the Divisions of Acme's North American operations. This includes providing financial, legal, tax planning, and treasury operations.

A corporate staff of 30 was hired. Business circumstances required moving into office space before it was completely renovated. The renovation to the space continued at night and on weekends but it was still going to require that the office be closed for at least 1 week to accommodate the construction. The CFO tasked the IT department to quickly deploy a solution to enable the staff to work from home. They would need access to email and departmental files as well as their home drive on the file and print server.

The network had a RAS server with 4 available 800 lines for dial up access. This would not be enough to accommodate 30 users and would incur high phone bills. All of the employees already had dial up access or high-speed internet access at home. It was decided that a VPN solution would be the best. Because of the immediate need, a Windows 2000 VPN was deployed on the existing RAS server. 25 PPTP ports were set up on the RAS server. A combination of hardware and software based firewalls were deployed at each users home to tighten VPN security. Complex passwords were enabled via group policy to more fully secure the network and the VPN. While not as secure as L2TP\Ipsec, PPTP was chosen because it could be set up with minimal configuration. The termination of the tunnel behind the firewall was also a known security risk but it was an acceptable risk in order to accomplish the business need of getting it up quickly at

a low cost. The assumption was that as soon as the renovation was over, the VPN would be discontinued until a more secure solution could be budgeted for and implemented.

The executive staff works from home frequently and travels a lot. Once the renovation was over they did not want to give up this high-speed access. They were allowed to keep using it while another solution was being researched. Many other IT projects were being implemented and this project was put on the backburner.

Acme is a large International Corporation however it is very decentralized in nature. The IT departments at most entities are completely independent of one another. The only exception is IT purchasing which is negotiated globally. Because of this independence I am essentially the only IT person responsible for this network. The network was set up on a very short timetable by 4 different consultants. When I was hired as the Network Administrator I went over the network very carefully to see how securely the network was set up. I had my hands full. The network had numerous serious security issues. Default passwords were not changed, unneeded services were running, hundreds of patches were missing, and the mail server was open for relay to name just a few. After several weeks of hard work I was confident that our network was secure, however, I thought that an independent review was important to verify that I was not overlooking anything.

I had an established relationship with a local security consulting company and contracted with them to perform an assessment. The security review was done from the perspective of the Internet. The potential of an attack to an organization does not solely originate from the Internet. A larger threat may exist from inside the network, however, that was not the purpose of this review. The assessment consisted of a 1-day site visit with follow up penetration testing from the consultant's security operations center. The report was delivered several weeks later and was quite comprehensive. It strongly reinforced what I already knew: The VPN issue that had been on the backburner had to be addressed.

The main vulnerability in the design for VPN services is the fact that the VPN terminates ***behind*** the firewall. Any encrypted tunnel should be established and authenticated at the "edge", of the network (or the Internet, in this case), prior to permitting the traffic into the protected network. Firewall policies exist for a reason. When you allow an encrypted tunnel THRU your firewall and terminate it at an internal server, you are effectively allowing all traffic thru that tunnel to completely bypass your firewall rules. Network engineer Jose Muniz gives a good example: "If the security policy on your network does not allow Telnet, then you probably drop TCP 23 at the firewall. However, if someone uses Telnet over the VPN tunnel, they are violating your security policy and, what's worse, you will not have any accounting or logs of the problem."[1] This violates 2 of the rules that the SANS course taught me:

1) *"Defense in Depth."*[2] If someone does not need to access a resource then they should be denied access. Access should only be provided to the resources that they need to get their job done and nothing else. (Principle of least privilege) Blocking them at the firewall accomplishes this task. If the resource has the right permissions assigned

then you could allow them through the firewall, however, a proper defense in depth strategy would block them at both the firewall and the resource in case there was a misconfiguration or they were able to subvert one of the defenses. "Protections need to be layered". [2]

2) *"Prevention is ideal- Detection is a must."*[3] Also, any kind of Intrusion Detection capability you may have in place will be completely blind to the traffic in the PPTP tunnel, as it cannot decrypt the packets. Another of the security principles that I learned at the SANS Security Essentials course was not being practiced: If it is encrypted, you cannot detect suspect activity.

The assessment pointed out several other issues that I had never thought about: In addition to terminating inside the firewall, it was terminating on a domain controller. From a security standpoint this server holds the most sensitive information on the network – the user accounts. Because this is a small network, this server also runs several other critical services. It is the Global Catalog Server for the domain. It provides internal DNS name resolution, DHCP, Veritas Backup Exec Server and is the main file and print server. Finally, the firewall currently permits TCP 1723 and protocol 47 (GRE) to this server. These ports/protocols are required for PPTP-based VPNs. "PPTP provides simple-to-use, lower-cost VPN security for companys who do not require the sophistication of IPsec, who do not want to deploy PKI, or who require a NAT-capable VPN protocol. But most security experts consider PPTP weak".[4] When the VPN was established, it was being used for email and file access. Many financial software programs have been installed on the network since that time and users are accessing them over the VPN. This type of data is much more critical and higher security than PPTP is a must. Ipsec is a framework of open standards developed by the Internet engineering Task Force and should be considered a necessary part of the solution for the following reasons.

- IPsec provides per-packet data origin authentication (proof that the data was sent by the authorized user.
- Data integrity (proof that the data was not modified in transit)
- Replay protection (prevention from resending a stream of captured packets)
- Data confidentiality (prevention from interpreting captured packets without the encryption key). By contrast, PPTP provides only per-packet data confidentiality.
- IPsec connections provide stronger authentication by requiring both computer-level authentication and user-level authentication.
- It is slowly replacing proprietary VPN protocols and becoming the industry standard. [5]

I needed to implement a new VPN solution that terminates at the edge of the network and Utilizes Ipsec.

There are hundreds of solutions on the market that solve these problems, unfortunately, they all cost money. Sometimes a great deal of it. The Widget industry is currently in its largest downturn in 30 years. As a result the Acme IT budget has been frozen. Only small cost effective purchases were being approved. I had to find a solution that addressed these issues at the lowest possible cost.

During

It was obvious that a managed VPN was out of the question because of cost. What other options did I have? My first thought was that if I could find a low cost hardware based VPN appliance solution, I could justify the cost to management. I researched a lot of different products and was impressed by the Netscreen 25 It had a lot of functionality at a reasonable price. At $5300.00 including installation and configuration, I thought I had a 50/50 chance of fighting for it and having it approved. What I thought would be a very tough fight suddenly became impossible when bad quarterly results prompted the layoffs at the headquarters and a renewed emphasis by management to cut costs wherever possible. Layers 8 & 9 of the OSI model (Finance & Politics) had struck again.

Next I considered moving the VPN server outside the firewall and using Microsoft L2TP/Ipsec. I could do this 2 different ways. I could put it between the router and the firewall, also known as inline. The 2 main problems with this would be that the VPN would not be protected by the firewall and Internet connectivity would now depend on the VPN gateway. The second method would be to put the box outside the firewall on an external network. In this scenario, Internet connectivity no longer depends on the VPN however the VPN gateway is still not protected by the firewall and special routing information is needed in the firewall. [6] Another problem with both of these solutions is that because the VPN server also performs other functions, a new server would have to be utilized. Money would be needed for hardware and software licensing. It will also have to be installed and configured. Microsoft's Article, Layer Two Tunneling Protocol in Windows 2000, point out 2 disadvantages to L2TP

> Because L2TP/IPSec requires the high security features of IPsec:

- L2TP/IPSec requires a certificate infrastructure for issuing computer certificates to the VPN server computer and all VPN client computers. Computer certificates are needed to negotiate the IPsec security association. By contrast, PPTP can use password-based authentication protocols and does not require an installed certificate.

- Windows 2000 and Windows XP VPN clients cannot be placed behind a network address translator (NAT) unless an update is installed on the client. By contrast, PPTP traffic is supported by most NATs. IPSec NAT Traversal (NAT-T) is a new set of standards for sending IPSec traffic across a NAT and is supported by

Microsoft L2TP/IPSec VPN Client, the Windows Server 2003 family, and L2TP/IPSec NAT-T Update for Windows XP and Windows 2000. [7]

For all of these reasons, this solution was disregarded.

I started to consider purchasing a new PIX 506. At around $1000.00 it would be less expensive than the Netscreen 25 or a new VPN server outside the firewall. The current hardware is over 3 years old and both the IOS and PDM software are outdated. The updated software includes enhancements to the configuration as well as patches for the software. The newest PDM version 3.0.1 supports VPN configuration via a wizard type interface. This appealed to me because while I knew that the VPN could be configured via the command line, I knew that the wizard would make it faster, easier and less prone to errors. The PIX also supports PIX to client VPN's utilizing Ipsec without having to use certificates.

The final alternative was to deploy a Cisco VPN using the existing PIX 506 Firewall. The PIX 506 software was version 6.1.1 and needed to be upgraded to 6.3.1. I would need to download the latest IOS PDM and PIX Client software. To do this you must have a current maintenance agreement from Cisco. We did not have a current maintenance agreement so we would have to sign up for a 1 year smart net subscription. Through our global purchasing agreement with a large reseller I was able to purchase the Smartnet for $189. We also had to purchase a new 3DES key, which was an additional $26. This solution terminated the VPN at the edge. This solution would utilize Ipsec and would be the simplest to implement and was $800 less than a new PIX. For these reasons, this is the solution that I chose.

As I do with any upgrade or change to the network, I put together a step-by-step plan to follow.

My plan was to:

1) Acquire the correct firmware
2) Do a test of the upgrade in a lab environment
3) Upgrade the PIX during off hours
4) Install an IAS Server
5) Testing via various clients
6) Deploy clients
7) Educate users
8) Turn off W2k VPN
9) Document

I ordered the Smartnet Subscription through our reseller. To place the order, you need to send in the serial number to the PIX. I used the show version command for the serial number and sent it in. 2 days later I received an email informing me that the serial number was not valid. After a few phone calls, I learned that the serial number in the show version is for the software, not the hardware. A quick trip to the server room and I

had the serial number off of the unit and sent it along to our reseller. He forwarded it to Cisco and 5 days later I received an email informing me that I had another bad serial number. The network was originally set up by 2 different consulting companies and after several days of telephone tag, it was determined that the current PIX replaced a defective one. The old PIX was located in a storage room and the serial number was again forwarded along. This was the one that Cisco had and they updated their records.

The bright side to the problems acquiring the Smartnet subscription was that I now had an extra PIX to test the upgrade. Apparently the reason that it was replaced was due to a faulty power connection. The unit worked fine except that once every few days the power cord would work loose.

First I made a copy of the configuration from our production PIX. Then I set up a lab that was separate from our production environment, and copied the configuration to the test PIX. Next I set up a tftp server in the lab and downloaded the IOS – PDM and PIX client. I upgraded the IOS with no problems. The upgrade of the PDM was smooth as well. I set up an IAS server in the lab to authenticate user accounts. I ran the VPN wizard and set up a VPN. I set up a VPN client and connected to the PIX with no problems. I felt comfortable that the upgrade on the production box would go smoothly.

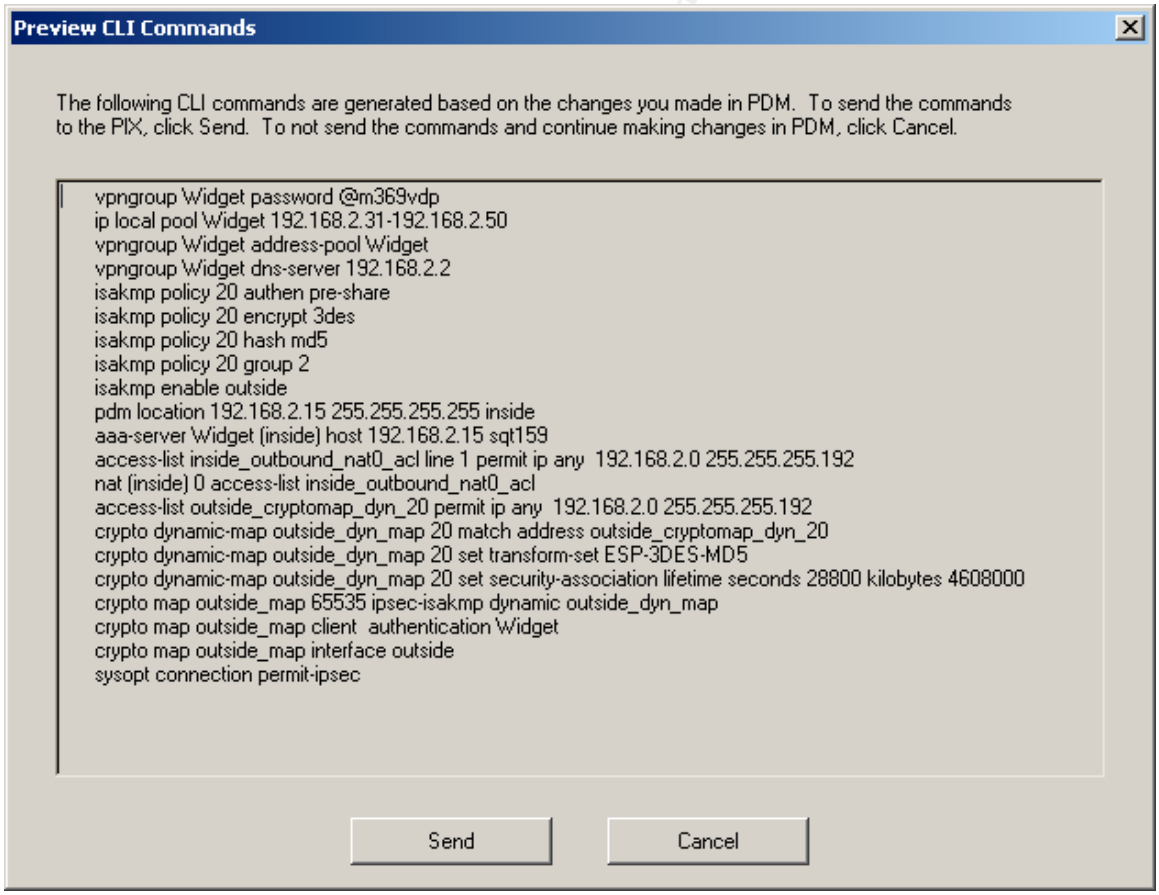
A lot of our employees stay late, so I scheduled the upgrade for 9 pm on a Wednesday night. I allowed ½ an hour for the upgrade and ½ an hour for testing the firewall to make sure everything was running smoothly. I also allowed 2 hours extra to contact Cisco if I encountered any problems. I thought that in a worst-case scenario, I would be done around midnight.

I performed the upgrades and was done in 35 minutes. I went to my desk to run some checks and was surprised to find that the firewall was passing no traffic. After running a few tests, I decided to call Cisco. I could get from anywhere on my network to the firewall and the Cisco technician could get to our edge router, but no traffic would pass between the 2. After 4 hours of testing and mailing configs back and forth, it was decided that we should wipe out the configuration and rebuild it line by line. This process led us to determine that an IPsec crypto statement in the configuration was causing the problem. This statement had been used to connect to one of the North American companies and was no longer being used. It was deleted from the configuration and the firewall was operating normally again. The big lesson learned here was that the firewall that was upgraded in the lab environment never actually passed any traffic. Before I started to upgrade the production PIX, I should have replaced it with PIX from the lab and test it's functionality.

Know that the tunnel no longer terminated on a domain controller, I needed to find another way to authenticate users. I needed a Remote Authentication Dial-in User Service (RADIUS) server. There are many 3rd party Radius servers available. Microsoft Windows 2000 Internet Authentication Service (IAS) is the Microsoft implementation of RADIUS. This is the solution that I chose because it is free with the OS. IAS performs centralized connection authentication, authorization, and accounting for dial-up and

virtual private network (VPN) remote access and for router-to-router connections. IAS enables the use of a single- or multiple-vendor network of remote access or VPN equipment. The install of the IAS server for the PIX to authenticate users was smooth and required about 15 minutes. I installed it on an existing member server. I added the PIX as a client and chose a shared key.

I then continued the deployment by running the VPN wizard on the PIX. The Wizard is very straightforward. You choose a group name and group password, which is a pre shared key to be used for IKE authentication. While using a shared key does not scale well in a larger environment, it was fine for our purposes.You then enter the AAA server and protocol. I used RADIUS. You then create a local pool of IP addresses to be used as well as a DNS server. Next you select the encryption algorithm and authentication algorithm for IKE security and then the encryption and authentication methods for the tunnel. Finally I enabled split tunneling to allow the remote users encrypted access to local resources and unencrypted access to the Internet. After you click Finish, the PDM VPN Wizard displays your configuration in CLI format as shown below
The names and Ip addresses in the diagram have been changed for security.



It is easy to see by the above configuration that using the VPN wizard saves time and prevents errors.

As mentioned earlier, several financial applications were now being run over the VPN. I was concerned that the processor on the PIX might not be able to handle the increased burden that the VPN would place on it. I installed the software on 3 test machines and ran the software over the VPN for a week with no problems. I was getting ready to deploy the clients until I discovered an issue. I was offsite connected to the VPN and needed to check on a server. I used terminal server in administrative mode to connect to the server. A day later it hit me: The firewall blocks access to that server from the Internet, so why were the firewall rules being ignored? A little digging and I discovered that the VPN wizard sets Ipsec authenticated/cipher inbound sessions to always be permitted through the PIX (I.E. without a check of the conduits or access-lists statements) Deselecting this option under VPN system properties solved this problem. Further testing revealed that the firewall rules were being enforced. Now I had to add some rules to allow only VPN users access to the resources that they needed. Adding some statements permitting the source addresses from the DHCP Pool access to various ports and servers accomplished this. Seeing the granular control that I now have over the VPN, I set up groups for each department instead of the one large group for all VPN users. Now that I had the ability to control access more tightly, I met with the various department heads to finely tune what resources should be available over the VPN. We now block some confidential resources that use to be available via the old VPN.

The lesson learned here was that while I tested for performance, I never tested for security. With this is mind, I connected to the VPN and accessed various resources. I then opened the log from the syslog server to ensure that I was indeed able to see the traffic via the logs. The previous solution did not permit this.

The next 2 steps were to deploy the clients and instruct the users in its use. A few of the initial users of the W2K VPN were using their home PC's. Fortunately all of the users of the VPN now have laptops. This makes the rollout much easier. The Widget headquarters staff is comprised of mostly vice presidents and above. For this reason most training is based on their schedule and is almost always one on one. I scheduled appointments with each of them over the course of a week. I had a CD with the PIX client on it and would quickly install it on their laptop as I discussed the security reasons behind the new software. Once it was installed I quickly configured it. I then guided them thru the process of how to log on properly.

Once all users had the client installed and were knowledgeable in its use, I monitored the W2K RAS server daily and sure enough users were still connecting to it. I would call them and instruct them to log off and use the Cisco VPN. After a few days, no one was using the W2K VPN. I set the Ports available for PPTP on the RAS server to 0 so that no one could VPN in without using the Cisco VPN.

The final step that I always follow is to document all configurations and add them to the network operations manual. Update the network diagram. What changes were made? What is the IP of the IAS server? Where are the shared secrets for the various VPN groups stored? What are the settings on the VPN clients? Etc. Etc. Know thy system.

After

The vulnerabilities that were identified with our current VPN solution were negated. The one negative that I have found with the new VPN is that with the Windows RAS server you could open up a management console and see immediately who was connected. This could be valuable when trying to troubleshoot remote user issues. There are other Radius server products that could solve this issue, however cost containment was one of the prerequisites. The positives far outweigh this little annoyance. Now the tunnel now can block traffic to our most sensitive data at the firewall. The VPN traffic can be monitored. Various VPN users have access to a more limited set of resources via groups. Computer-level authentication is now performed as well as user-level authentication. This limits a vulnerability that had always concerned me. While I had enabled complex passwords to make them harder to guess, I know that sometimes employees give out or write down their password. My concern was that if an employee was terminated and their access was revoked, they might try to connect to the VPN with someone else's user name and password. This additional computer level authentication now prevents that. The Ipsec implementation is more secure than the previous PPTP VPN and the tunnel no longer terminates on a domain controller. The VPN was made more secure on a limited budget.

References:

1) Dejesus, Edmund. "VPNS Handle with Care" Information Security July 2000 URL: http://infosecuritymag.techtarget.com/articles/july00/features1.shtml (6 October 2003)

2) Cole, Eric., Jason Fossen, Stephen Northcutt, Hal Pomeranz. SANS Security Essentials with CISSP CBK Volume 1 USA: SANS Press, 2003 292 – 294

3) Cole, Eric. "How to Secure Your Company" Computerworld June 26th 2003 URL: http://www.computerworld.com/securitytopics/security/holes/story/0,10801,82515,00.html (6 October 2003)

4) Phifer, Lisa. Windows 2000's VPN-Related Security Issues URL: http://www.isp-planet.com/technology/vpn_windows2000b.html (6 October 2003)

5) Corrent Corporation. What kinds of Internet security are there? URL: http://www.corrent.com/KnowBase/Kinds_Of_Security.htm (6 October 2003)

6) Clavister Corporation Why VPN in Firewalls? URL: http://www.clavister.com/manuals/ver8.1x/manual/vpn/why_vpn_in_firewalls.htm (6 October 2003)

7) Microsoft Corporation. Layer Two Tunneling Protocol in Windows 2000 August 2001 URL: http://www.microsoft.com/technet/treeview/default.asp?url=/technet/columns/cableguy/cg0801.asp (6 October 2003)

Other Resources:

The Internet Society. Security Architecture for the Internet Protocol URL: http://www.ietf.org/rfc/rfc2401.txt (6 October 2003)

Cisco Systems. SAFE VPN IPSEC Virtual Private Networks in Depth URL: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns128/c654/cdccont_0900aecd800b05ad.pdf (6 October 2003)

Hines, Eric. Virtual Private Networks: A Broken Dream? URL: http://www.securityfocus.com/infocus/1461 (6 October 2003)

Last Updated: May 23rd, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 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 San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
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 Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 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 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
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event