Global Information Assurance Certification Paper

Case Study: Adventures in Securing Mom and Pop
Ken Davidson
August 11, 2002
GSEC Practical Version 1.4 – Option 2

ABSTRACT

A recent commercial for one of the high-speed Internet providers depicts a couple of American tourists, somewhere in rural Europe, amazed by the quality of the small shop's wares. The tourists are in a corner whispering to each other about how they could import the shop's goods to America, and make a fortune. The wiley shop owner, who can of course overhear the discussion, informs the tourists about his website and his amazing American import business. The shop owner, of course, made this possible by technology and the Internet. The message to mom and pop shops everywhere is that the ease of use and the relatively low price of tech nology can propel your business from just a small town shop to a 21st century global market company.

Small businesses everywhere are getting this message, and flocking into the technology quagmire in droves. By May of 2000 it was estimated that "84 percent of small businesses have PCs, 57 percent have Internet access, 21 percent have web sites, and 18 percent have high-speed access". ("Reid, screen 1) The Small Business Administration predicted that, by 2002, 85% of small business would utilize the Internet for business purposes. (Reid)

Although technology has been made simpler and computers are a small investment, the understanding of how important information security is to these business owners does not become apparent to them until they suffer a loss of information. They quickly find how much these losses can cost and that they need a professional to help them understand what they need to do to protect themselves against future losses. Some of the losses reported so for in 2002 are in excess of 450 million dollars. (CSI)

OVERVIEW

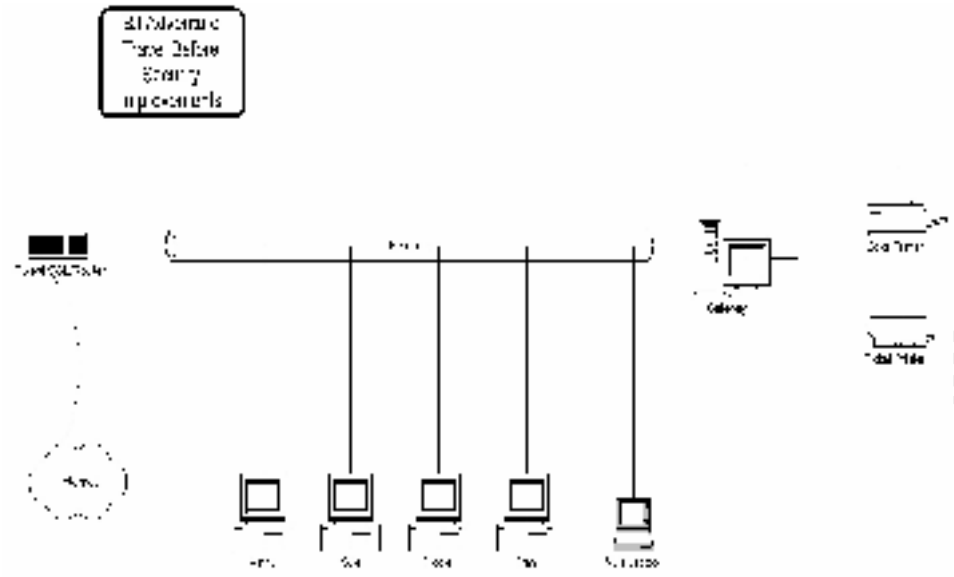
Bobby Joe's Adventure Travel Company quickly figured out that with their specialty, adventure travel to remote countries, they would greatly benefit from a presence on the Internet. Their adventures in technology began slowly with a couple of computers, a web site hosted at another location, then dial up access to collect the email that their web site generated. In the beginning, the Internet provided BJ Adventure Travel with a very small percentage of their business, while the majority of their customers were those who walked through the door or called and booked their trips. The tour operators and resort owners communicated mainly by phone and fax although this resulted in strange hours for Bobby Joe, since she had to talk with them during their business hours in various time zones.

Over time, as the popularity worldwide of the Internet grew, her reliance on the Internet and technology became much more important to the viability of her business. Now tour operator s and resort owners were on the Internet and began booking tours and making reservations utilizing email as their primary mode of communication. Utilizing software that she bought from Ticket Explorer she could make plane reservations over the Internet and print airline tickets from her office. Also, the majority of her cliental booked their trips through her web page. Over 75 percent of her customers came from the Internet, and even the walk-ins were utilizing email to keep up with their arrangements.

To meet the demand of her growing business, she called her local DSL provider, Qwest, and connected her burgeoning network of four computers to the Internet full time behind the Qwest-provided DSL modem. Bobby Joe's adventure travel was off and running ful l time on the Internet, and it was secure behind the preinstalled firewall that came free with her DSL modem. Secure that is, until disaster struck in the form of a virus that crippled her entire network and kept the company from functioning.

THE PROBLEM

As Bobby Joe hired people, she put new computers into place. As a result her network had various computers running several different versions of Windows9x at many different patch levels with the Microsoft standard base install. She had not upgraded h er company computers to Windows 2000 because initially the Ticket Explorer software that was vital to her business did not run on Windows 2000. She also felt her business was secure since it was operating behind the firewall running on her DSL modem.



Each travel agent required his or her own computer. Each computer had a pretty standard install that included Netscape, Eudora for email, Ticket Explorer for ticketing, Adobe for producing graphic brochures, and an ftp client to upload the content for the web page to the ISP that houses the web page. Their most immediate need was to stop viruses from infecting their computers in the first place. However, if a computer did become infected, they needed to determine this quickly so the infected computer could be removed from the network immediately, and a professional called to clean the affected computer if needed. They also required that if a computer was beyond repair that they could get it back up and running quickly so that no one agent was prevented from working.

In addition to the agents' individual computers, BJ Adventure Travel has another system, "gateway1" that they used for various but very important purposes. Gateway1 is not only a print and central file server but is necessary to the proper functioning of the Ticket Explorer software. This computer needed to be made safe yet accessible.

The computer infrastructure for Bobby Joe's travel company was not ready for the Internet. While she had installed an anti virus software package it was rarely updated. She had not decided on even the simplest of security policies. For example, most current active passwords where simple words from the dictionary which where very easy to crack. All computers in the office shared their entire hard drives as unprotected windows shares. The firewall they thought they had installed on the DSL router had been wide open in order to allow easy setup of the ticketing software. The last straw was that some of Bobby Joe's employees

were running Peer-to-Peer file sharing software on their business machines in the office.

THE SOLUTION

All of BJ Adventure Travel's problems needed to be fixed with a strict budget in mind, as they are a very small company with not much to spend. The solutions also needed to be easy to maintain by people who were not computer professionals. This situation screamed for a Security in Depth solution.

OS PATCHING

The first step was to patch the systems so that they were all running the same version of the OS. This would also insure that all the latest security patches were installed. Included in this step was the installation of Microsoft Update notification software. After training the users to recognize the update icons they could make sure that they easily maintained a patched and somewhat secure OS.

PASSWORD POLICY

Like many small businesses that felt that nobody would want to break into their systems, BJ Adventure Travel had a very insecure password policy. All employees logged in to each system using one password. This password had been in place for the last 3 years and had never been changed even though several agents had left the company. The first step was to teach the users what was a good password policy. In the document by Cert "Configuring Computers for Authentication" recommends that a good password should:

1) Have a minimum length of 8 characters
2) Contain both upper and lower case letters as well as at least on non-alphabetic character
3) Password aging be implemented on the systems
4) Passwords not be reused

Once Bobby Joe understood what could happen to her vital business information if a disgruntled ex-employee or any other non-authorized user gained access to her systems, she quickly implemented a new password policy. All users were required to follow the above guidelines when choosing a new password.

VIRUSES

In the 4th quarter of 2000 there were more than 71,402 virus attacks detected around the world according to Internet Security Systems. (Information Security) Sophos reports that over 3,200 new computer viruses were detected in the first half of 2002 alone. In 2000, 99.67% of companies surveyed

encountered at least one virus and 51% claimed they had what they considered a disaster due to a virus in the past year. (Virus)

Bobby Joe had experienced the des tructive nature of viruses first hand. Systems had to be rebuilt several times over the last few years due to an infected computer. After many hours of down time and lost data, she needed no persuading in purchasing a good virus detection package.

Bobby Joe Adventure Travel had to conduct business with other travel agencies and businesses worldwide. Most of these partners were not computer savvy, and used their systems directly out of the box, which meant they didn't follow any policies to stop viruses from entering their systems. Thus, they passed the viruses to Bobby Joe's computers with regularity.

The Computer Virus FAQ for New Users recommends the following steps be taken to avoid viruses:

1. Install anti-virus software from a reputable company.

   In an effort to find viruses on the systems McAfee version 6 Virus Scan was put onto all systems.

2. Update it regularly

   After running the virus scan software for a few weeks, a virus infected a computer and rendered it useless, and the operating system had to be reloaded. Why a computer ran for days infected on the network became apparent when Bobby Joe discovered that none of the systems were updating the software nor were they regularly running scans on their systems. A strict policy for updating and running virus scans was put into place. Every Thursday all systems were left running when the employees went home for the day. McAfee was configured to go and retrieve the updated virus definition file. After this file was installed on the system, a virus scan was preformed. On Friday when the employees came in, the results of the scan were displayed on their screens for their immediate attention.

3. Scan any new files or code.

   All email as well as files received by vendors were submitted to a scan by McAfee before use.

4. Anti-virus software isn't very good at detecting "Trojan Horse" programs.

The users were educated to be careful on which documents they could open. The ability to automatically execute Java Script or Word Macros was disabled. (FAQ. org)

Since Bobby Joe seemed to be exposed to just about every virus that was making the rounds, it was decided to scan all types of files and to use the heuristic feature of the virus scan software. It was hoped that the heuristic scanning feature would catch even the unknown viruses. Heuristic scanning is designed to look at files for activity that is virus -like in nature. This type of behavior is typically found in Microsoft Word Macros and in executable programs. Heuristic scanning examines these ty pes of files for known viruses and virus -like actions. These types of actions could include a known Trojan payload, a replication method like a virus, or a propagation scheme like a worm. Typically, this sort of analysis is done by the virus scan softwar e using a rules-based system. However, the first heuristic scanner used a weight -based system but it was soon discovered that this resulted in a lot of false positives. These false positives where a product of not having any real contextual analysis buil t into the product. It was believed that with this setup every file downloaded to a machine from the Internet was now being scanned no matter if it came in email, the web, or from ftp. (Heuristic)

UNPROTECTED WINDOWS SHARES

A few weeks after this polic y was put in place, Bobby Joe found a virus on her system. She removed it from her system. The following day, she found the same virus on her system, and again she removed it. For the next couple of days she would find the same virus on her system after rerunning the virus scan software. It was even stranger that no matter how many times the files were removed, they came back and they had the same date stamp. Since she was never alerted when she downloaded her email to the presence of a virus, the virus was not found in her mail folders on her system, and since she never ran a program that came through to her via email, she was pretty sure that she hadn't received this reoccurring virus from email.

McAfee was reporting the present Downloader.A virus. Going to the McAfee site and searching on Downloader.A produced no results, but a file rdvs.exe was reported by McAfee to contain the virus Downloader.A. Additionally, since this was not a known virus in the McAfee virus definitions file, it could not be cleaned from the system using the McAfee Virus Scan software. This appeared to be a virus that the heuristic scanner in McAfee had found. McAfee did not know what to call it and had giving it a temporary name based on the heuristic analysis. This fil e was verified not to be a standard file on BJ Adventure Travel's computers by checking other machines in the office with the same OS and applications installed on it. An attempt was made to just remove the file from the machine, however this gave a file sharing error message. Since

this program was running on the machine already, and had the file open, it was determined that the best way to remove the file from this Windows 98 machine was to deleted file from DOS mode. Once the file was removed, the mac hine was scanned and found to be clean. The machine was left running all night, but was not used for any purpose by the employees of Bobby Joe's Adventure Travel. The following morning before any work was done on the machine it was rescanned and found to again be infected with the virus. At this point the machine was physically disconnected from the company's network.

This machine was kept off the network while research was done on the virus that she never seemed to be able permanently get rid of or t ruly identify. At the end of the week McAfee reported a new virus, W32/Ultimax, a worm that exactly described the little pest that BJ Adventure Travel had been dealing with for over a week at this point. This worm would try to download a PornDailer program from another website that was named dailer123.exe. While the dialer123.exe program appears to have no worm abilities, rdvs.exe did try to copy itself to a random IP address in available, unprotected windows shares that are possible startup locations. Then, when the computer was rebooted, and rdvs.exe was run, it would create a registry entry so it was capable of running itself. The virus definition at McAfee pointed out that Bobby Joe was most likely running an unprotected windows share, and this was the way this worm was spread. Although it is not known how the virus got past the McAfee System scan function that is resident in memory and should have caught the file copy on to the box. (McAfeeHelp) From auditing her systems it was found that her com puter was the only system with an unprotected share. This share had been setup to allow a couple of the agents to share files on a quick one -time basis. It was explained to the users that unprotected windows shares would allow anyone on the Internet acce ss to their files. This was quickly remedied and a new policy was put into place – no unprotected window shares. (Virus Profile)

PERSONAL FIREWALLS

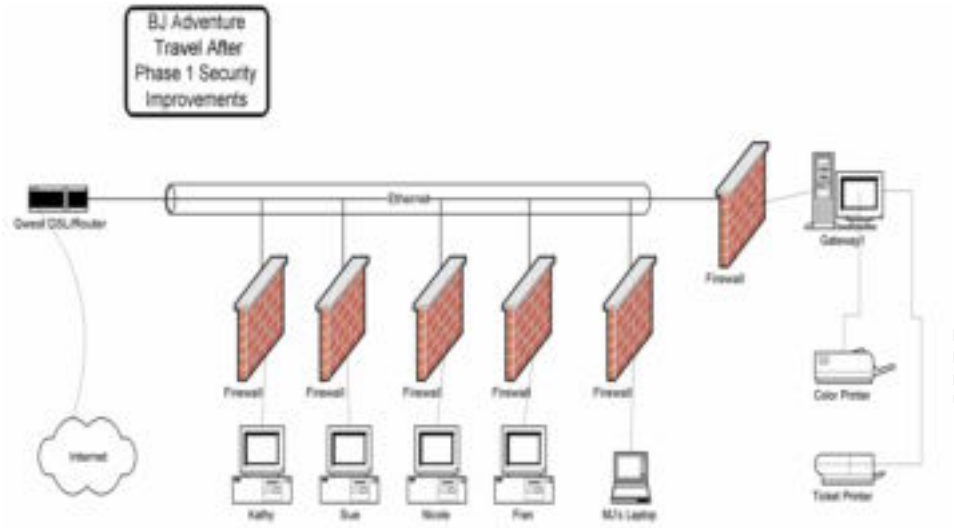
The firewall that was provided with the Qwest DSL router had been totally disabled by the installer of th e Ticket Explorer ticketing software so that Bobby Joe's Adventure Travel could use their software to produce tickets and travel itineraries. When this software was originally installed Ticket Explorer required static IP addresses on all the machines in B obby Joe's network so that a hole could be punched into their firewall to allow the Travel Company access. At the time of the installation, the Ticket Explorer software seemed to require that BJ not run any firewall so that it could function. The need fo r a quick and dirty solution overtook the hopes for security. While this did provide the Travel Company the ability to use the Ticket Explorer software, their network was now open for any hacker to attack. Ticket Explorer felt that they were safe since t hey used a VPN to connect BJ Travel to their ticketing system.

The firewall that came with the router was not very sophisticated. To provide better protection to the travel agents, Zone Alarm Pro Personal Firewall was installed on every computer in the network. It was initially configured by shutting off all incoming and out going connections. Slowly, each program that was necessary to the functioning of the business was started and the firewall was configured to allow that application to the Internet . As each program was started Zone Alarm Pro asked if it should be allowed access to the Internet, and the affirmative was checked.

The firewall also had to be configured to allow communication between Ticket Explorer and Bobby Joe's computer system. The communication between the two companies was initiated from Bobby Joe's computers. The firewall logs were watched for the incoming communication from Ticket Explorer central servers. Since the Ticket Explorer software needed to communicate with the Gateway1 computer to print tickets and itineraries and to the individual machines for the traveler research each system needed have the a set of very specific protocols and ports opened in their firewall to allow communication to the Ticket Explorer central servers. It was found that Ticket Explorer only utilized two IP addresses for these functions. Because of this, the rule could be made very specific which decrease the security risk. Additionally all communication with the Ticket Explorer software was m ade only via VPN network link.

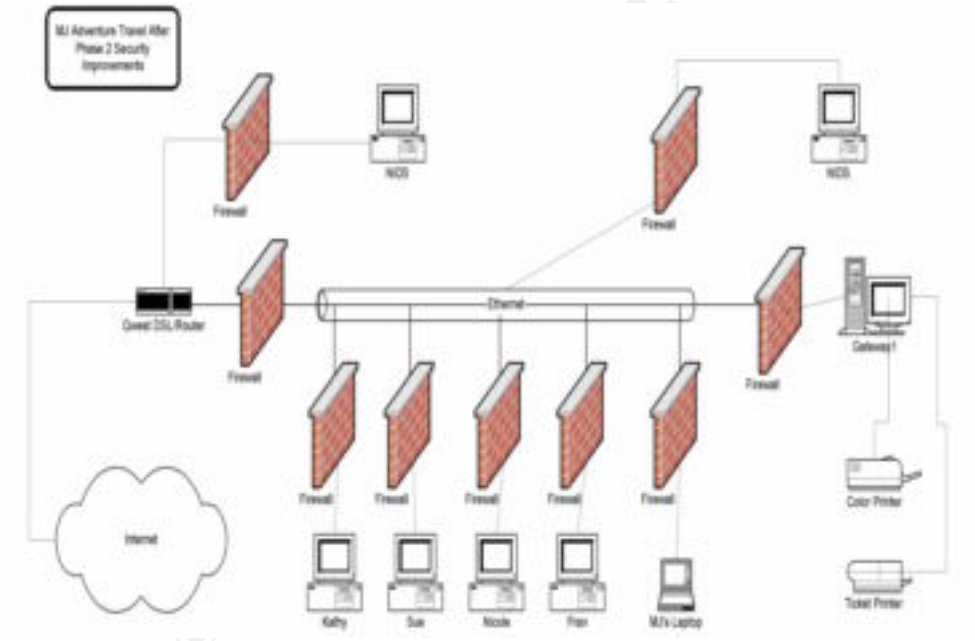
During this process machines were rebooted and several computers were found to be running several programs that do peer -to-peer file sharing. These programs were uninstalled and the employees that were running these progra ms were educated on the dangers these programs.

Additionally, the BJ Adventure Travel users were shown how to look into the log files for hacker's access attempts to their machines. They where shown how to add IP's and networks to the list of Blocked Zo nes. This setting should allow BJ Adventure Travel to block hackers from continuing to attack from one location on the net. While this procedure is not a foolproof solution to the hacking activity directed towards BJ Adventure Travel, it should make it somewhat more difficult for the hackers to succeed.



PLANS FOR THE FUTURE

This initial security improvement and lock down was done without breaking the budget. Some software was purchased, but the majority of the work was done with policies that were i mplemented, procedures that were put into place and training of the employees. However, to truly secure Bobby Joe's Adventure Travel Company's systems many more things could be put into place.



Bobby Joe Adventure Travel does seem to get several very destructive viruses every year. These viruses do so much damage to her systems that they need to be rebuilt. While these systems are being rebuilt, the machine usually leaves the place of business to visit the computer shop, and the travel agent is not able to work or needs to share another agents systems for a couple of days. This is detrimental to the running of the business. The new procedure for safeguarding their computers should greatly reduce the risk to a virus damaging their systems. However, the use of ghosting software would be a great addition as a Disaster/Recovery solution in the event that another virus should damage a computer beyond the ability of easy repair. Additionally, updating Qwest firewall in such a way as to not break the tic keting functionality would provide another level of security, and decrease the risk that some malicious software could infect BJ Adventure Travel Company. Finally, if in the future, cost will allow the addition of a Network Intrusion Detection system insi de and outside the Qwest firewall in the office an even greater sense of confidence could be maintained about the computer system integrity.

CONCLUSION

The lessons learned here are that no one security measure is enough to stop loss of productivity br ought on by virus and other hacking attempts even at a small "mom and pop" shop. The concept of Security in Depth is seen in action in this kind of case study. Even small operation can be victims of attacks, and in fact because they generally deal with a lot of other small companies who are not very savvy about computer security, they are subject to attacks via these vendors as well. Also, just a little bit of security training, a set of well documented and understood policies, and supporting procedures can significantly reduce the exposure for such an operation. It should be noted that the greatly improved security for BJ Adventure Travel did not break the budget of this small business. The perceived large budget and complexity of setting up a secure e nvironment has many small business skipping the effort and hoping that they will be safe enough because they are small and "Who would want to attack them anyway." After a lot of down time and expense for BJ Travel, it became obvious that they could no longer skip this step in their business plan. They also discovered that the cost and complexity of the security setup was not as bad as they first thought, and now they are relieved to have taken the step to protect themselves. Every day when they download email and McAfee warns them about a new virus imbedded in some piece of email, (lately that has been a great many variation of the Klez virus), they can feel much more confident that they will not have a major outage in the office if they follow the new pr ocedure, and stay a little paranoid.

Works Cited

"Computer Virus FAQ for New Users" 16 Aug 2002. URL:
http://www.faqs.org/faqs/computer-virus/new-users/ (16 Aug 2002)

"Cyber crime bleeds U.S. corporations" CSI April 7, 2002
URL: http://www.gocsi.com/press/20020407.html (15 August 2002)

"Configure computers for user authentication." Copyright 1999, 2000, 2001, 2002 Carnegie Mellon University.
URL: http://www.cert.org/security-improvement/practices/p028.html (5 Aug 2002)

"Heuristic Techniques in AV Solutions: An Overview"
by Markus Schmall February 4, 2002
URL: http://online.securityfocus.com/infocus/1542 (19 August 2002)

"Information Security. Departments" May 2001. URL:
http://www.infosecuritymag.com/articles/may01/departments_news.shtml#numbers
(2 Aug 2002)

"McAfeeHelp" McAfee August 15, 2002. URL
http://www.mcafeehelp.com/ (15, August 2002)

Reid, Lucile, & Lonier, Terri "Small Business Facts" Copyright 1999 -2002 URL:
http://www.bigstep.com/company/small_business_facts.jhtml (1 Aug 2002).

"Virus Profile" McAfee 11 July 2002. URL:
http://vil.mcafee.com/dispVirus.asp?virus_k=99580#characteristics (25 July 2002)

"Virus Related Statistitcs" 3 October 2001. URL:
http://www.securitystats.com/virusstats.asp (2 Aug 2002)

Last Updated: September 26th, 2017

Upcoming Training

Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor