Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

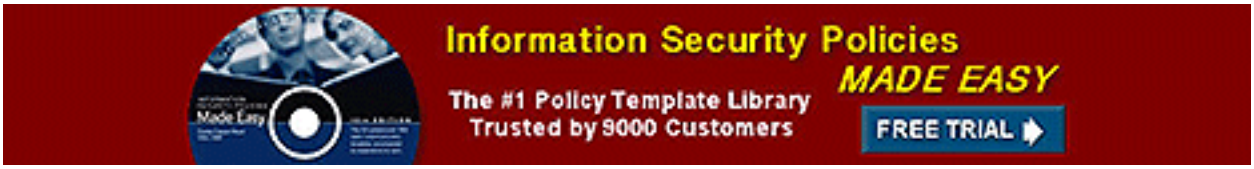
This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Investigating an Internal Case of Internet Abuse

I was recently required to investigate an incident of Internet abuse that led to the discovery that one of our own administrators was a security risk. Though this investigation was triggered by an incidence of "Internet abuse", the tools used and lessons learned are relevant for many types of security incident that require an internal investigation to discover the offender. This essay describes the detection, investigation and various tools used to collect the evidence. Lessons learned from the investigation are includ...

Copyright SANS Institute
Author Retains Full Rights

AD



Investigating an Internal Case of Internet Abuse

Mal Wright
Assignment Version 1.2e

Introduction

I was recently required to investigate an incident of Internet abuse that led to the discovery that one of our own administrators was a security risk. Though this investigation was triggered by an incidence of "Internet abuse", the tools used and lessons learned are relevant for many types of security incident that require an internal investigation to discover the offender. This essay describes the detection, investigation and various tools used to collect the evidence. Lessons learned from the investigation are included, as well as some useful resources for security investigators so they can be more prepared when they deal with internal computer security incidents.

Discovery

I would like to say that we uncovered the Internet abuse and subsequent security concerns through a proactive program, but like many discoveries, it all began with an accident. One night a senior manager discovered one of the employees viewing pornography on the Internet. In many companies and countries this is not acceptable. Our company operates in several locations throughout the Asia-Pacific region including Niugini (Papua New Guinea, where this incident occurred). In Niugini pornography is illegal and our company has a legal obligation to ensure that such material is not imported into the country. As such the discovery that someone was able to view the material was of great concern to our management. The next day our IT Manager received instructions to determine how the material could be viewed (given we use SmartFilter filtering technology) and determine if this was an isolated case or more prevalent.

As the volunteer security coordinator for our company it fell to me to investigate further. I determined that our SmartFilter was working, however from a review of our logs it became clear that the SmartFilter, running on our Microsoft Internet Proxy Server, was not preventing access to restricted sites when a user was utilizing the Winsock proxy client. I found that by using the Winsock proxy client we were able to bypass the SmartFilter blocks and still use the proxy server to access the Internet. Our company requires users to authenticate with the proxy server to obtain Internet access. Though I found that the SmartFilter did log the access to restricted material, the user was logged as "anonymous" and the log entry only provided the IP address of the offending machine. I had now discovered how users were able to access the restricted material and identified the need to review the SmartFilter configuration.

Another issue raised by the use of the Winsock proxy client is that, by allowing its use, we are also allowing our staffs access to any port on any machine on the Internet. Potentially an internal user could then use our company as a base for probing Internet sites and executing hacking attempts. As a result of this finding, we now have plans to restrict the use of the Winsock proxy client.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

It was decided that I run some reports using the Cyfin Reporter Professional product (http://www.cyfin.com/products/crp/) to analyze our SmartFilter logs. Wavecrest Computing's web site describes Cyfin products as tools to "… monitor computer users' visits to Web sites on Intranets, Extranets, or the Internet. Their reports indicate which users visited which Web sites, when they did so, how many times they did so, and the types of content they were seeking. " After running the reports we were pleased to find that there wasn't a large number of visits to "Sex" classified sites. The visits to "Sex" sites amounted to less than 1% of all sites visited and totaled just over seven hours of access in the past week. After further reporting I found that an anonymous user of one particular machine had logged most of the traffic. After a review of these findings, management requested that I investigate the machine further to determine the identity of the person accessing the restricted sites. For the purposes of this essay, I'll call him "Mr X".

I reviewed the logs and found that Mr X's machine was accessing one restricted site on a regular basis, like clockwork.

An extract of the log is included here for reference:

Sex D-http://stats.virtuagirl.com/phps_application/stats.php3?database=vgirl&date=2001-08-08&starts=1&startsreg=1

The "stats" reference in the URL of the restricted site indicated to me that Mr X's machine was likely to be running a piece of software that was communicating with a restricted site automatically for statistics collection. This being the case, it was likely that Mr X was unaware that his machine was accessing a SmartFilter restricted site. With this in mind, it was possible Mr X was innocent of any wrong doing, however there was still the question of what the software running on Mr X's machine was, whether its use was legal in Niugini and whether its use breached company policy. The next step was to determine what the software was likely to be. I decided to visit the home page of the web site indicated by the URL (www.virtuagirl.com) and find out more about the software. It appeared that the site sells software that displays pornographic animations on the desktop. It was now time to determine if Mr X was running this software on his computer. I downloaded the "DEMO" version of the software and ran through the setup program to determine where it installed the software and then cancelled the installation. I now knew where I would be likely to find the VirtualGirl software on Mr X's computer, should it be there.

Investigation Detail

At this point I checked with the IT Manager as to whether I should proceed to review Mr X's machine itself, as I would have to log on to the computer to review files. After obtaining permission, I proceeded to the next step.

As our company uses PC workstations (that are all Windows NT 4.0 machines) and UNIX systems, I decided the next step in finding more about the machine was to open a command prompt on my Windows NT workstation and use NBTSTAT on the machine's IP address. NBTSTAT displays protocol statistics and connection information using NetBIOS over TCP/IP. NBTSTAT is a good way of quickly gaining more machine information, such as whether the machine is Windows networking based. If the machine is Windows networking based you can determine the machine's Windows NT

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

domain name (very useful because our company uses many domains), the currently logged on user and even the machine's MAC Address.

I used the "***nbtstat –A IP_Address***" command to discover this information. What follows is the output from a NBTSTAT on my machine (IP address and domain altered for privacy):

```
C:\WINNT\Profiles\USER\Personal>nbtstat -A 10.5.1.208
Host not found.
       NetBIOS Remote Machine Name Table

   Name               Type         Status
---------------------------------------------
TW002L7130     <00>  UNIQUE      Registered
NIUGINI        <00>  GROUP       Registered
TW002L7130     <03>  UNIQUE      Registered
USER           <03>  UNIQUE      Registered
TW002L7130     <20>  UNIQUE      Registered

MAC Address = 00-00-86-53-FA-74
```

As you can see from this output, from this command I have found that machine "10.5.1.208" is:

1. A Windows networking based machine (because it has NetBIOS name information registered).
2. In the domain "Niugini", which is very helpful for us as our domains relate to geographic locations and our IT support is geographically distributed. Now I know the machine is in Niugini and I know how to find the machine in the Windows network.
3. The machine's name is "TW002L7130". In our company this is also useful as we name computers using the serial number of the machine. So we know the machine's serial number. If you wished, you could determine the make and model of the hardware using this serial number.
4. The user presently logged on is "USER".
5. The machine's MAC Address is "00-00-86-53-FA-74". This is unique to the ethernet card in the machine. This ties the use of the IP address to the ethernet card and as such the physical machine.

As you can see, you are able to determine a lot of information very quickly with this command in a Windows network environment. During the investigation I was able to obtain similar information about the machine used by Mr X using the "nbtstat" command however there were two notable differences.

1. The machine name was "HPVLI8-A", indicating that the operating system was not built using our procedures and that the machine was likely to be a Hewlett Packard VL 8I machine.
2. There was no user information, so the user was not presently registered with NetBIOS.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

I was eager to determine who was using the machine, but also whether the machine had the VirtualGirl software installed and if it was indeed pornographic in nature. I thought, "Maybe it is a sanitized version of VirtualGirl and though inappropriate, not illegal?". At all stages I tried to approach the task with an "innocent-until-proven-guilty" mindset and as such was constantly trying to come up with "innocent possibilities". I decided that I would map to the hidden administrative share "\\hpvli8-a\c$" on Mr X's computer and look at the directory structures to find out more. I was able to do this by using my Windows NT domain administration privileges to map the share. I mapped the share successfully and it was obvious from the directory structure that an operating system was not installed on the "C" drive. As all of our systems are configured with a Windows NT standard operating environment on drive C, it was clear this system was out of the ordinary.

It was at this point that I realized two things. Firstly, that I should be keeping a written log of what I am doing. By keeping a written log I could ensure that I am logically progressing through the investigation and would also be able to create a report for management of what I did when requested. Secondly, I realized that I should take screen captures as evidence of my findings as I investigated and that these screen captures should be of the whole screen, not just the area of interest. This is important as all the clocks on computers in our company use time synchronization, so by using a whole screen capture I was capturing an accurate time-stamp as well.

As there was no operating system installed on this disk, I proceeded to successfully map the hidden administrative shares "\\hpvli8-a\d$", "\\hpvli8-a\e$" and "\\hpvli8-a\f$" until no more shares would map. I reviewed each share's directory structure, to determine who has logged into this machine in the past by viewing the user profiles in the \\WINNT\Profiles directory I found. Upon viewing the Profiles directory, I was able to determine that only two people had ever logged onto Mr X's Windows NT machine. The usernames identified in the profile directory told me who the users were and I confirmed one of the users was now in another country on holiday, which left only one person who could be using the machine. The likely identity of Mr X had been revealed. Mr X was likely one of our system administrators in Niugini!

It was now time to confirm that the VirtualGirl software was on Mr X's computer system. A review of the "Program Files" directory on one of the drives revealed the VirtualGirl software. From the filenames it certainly seemed the software was pornographic in nature, but of far more concern was the fact that several cracking tools were installed on Mr X's machine, from Word password crackers to port scanners. Using these tools was not part of this administrator's job description.

It was time to confirm my results so I could be sure of my findings. I confirmed the IP address belonged to Mr X's machine using the DHCP manager and also confirmed that the MAC address matched the findings of NBTSTAT.

Using HYENA (http://www.systemtools.com/hyena/) I was able to determine that Mr X was currently logged onto the computer, so his identity was confirmed. Also using HYENA I was able to determine that the machine was currently running with Windows 2000 (NT5) and not our standard operating environment (SOE), though our SOE did appear to be installed. I "pinged" hpvli8-a to again confirm that this machine had the IP address in question, which it did. There were also other shares identified, and a review of the directory names revealed the installation of copyrighted software and music files.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

I also found a sms.ini file on the Windows NT (SOE) disk. I viewed this file to determine that the system name referred to in this file was the serial number of the computer (as per our standard) when running Windows NT, and HPVLI8-A when running Windows 2000. I confirmed that the system was running Windows 2000 by using regedt32 on my Windows NT workstation to remotely open the registry of HPVLI8-A and reviewing the key HKEY_LOCAL_MACHINE->Software->Microsoft->Windows NT->Current Version. The version of the operating system was shown to be Windows NT Version 5. This was documented along with my other findings with full screen captures.

The IT Manager after reviewing the findings decided to contact the company head for which our Mr X worked and his supervisor to determine how they wanted to proceed, if at all. We decided that the best course of action was to isolate the machine so that we could review it in detail and ensure the system could not be tampered with. Mr X's supervisor also confronted Mr X with our findings to date and asked if there was an innocent explanation. Mr X said that he had not used any such software, other than what was on the Windows NT SOE, but he did have a CD with various tools and software which may have been accidentally construed by us as being suspect. The machine was collected, secured in a locked room and connected to the network for further investigation. I then changed Mr X's password so we could log in as Mr X when required to view his desktop and so he could not use his administrative privileges. In hindsight, I believe I should have done this as early as when I first discovered the identity of Mr X and determined he was a domain administrator. The system was offline for about an hour. As we were investigating remotely, Mr X's supervisor became our "eyes" for this part of the investigation. When the machine was started, all we found was a standard Windows NT SOE, with no evidence of the hacking tools, VirtualGirl or the music files.

Our first thought was that the wrong machine had been secured. However, the system's name was now the serial number of the machine, as per our company standards, and the machine's name was now the name identified in the sms.ini file we had found on HPVLI8-A. This made us believe something had probably changed, but to make sure we had the correct machine we used the Windows NT "IP Configuration" tool to display the machine's MAC address. The MAC address of this machine did indeed match the MAC address of HPVLI8-A. We had the right hardware, but not the right operating system.

We searched for any evidence of a dual boot configuration, but found none. It was at this point we decided to ship the machine to another nearby location were we had other system administrators who could investigate further. However, our administrators were still unable to find any evidence of a dual boot configuration. Windows NT disk administrator and the system BIOS confirmed one hard disk installed with two partitions. A review of the root directory structures of both partitions showed that they matched the directory structures of two of the partitions we found on HPVLI8-A, however the drive letters had changed. Furthermore, both disks still had the "System Volume Information" directories that indicated that Windows 2000 had been used to access these partitions recently. Something had changed, and I believed a hard disk was probably removed in the time between when we asked to secure the machine and when it was brought back online. We decided to open the case to determine if there was any physical evidence of a second hard disk in the machine. The machine had one hard disk only, however the hard disk cable had been positioned such that when the case was off, a second hard

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

disk could be run on top of the machine. I had an administrator take photographs of the cable position.

I was now certain that another hard disk had been used with the machine, however we could not investigate further if we could not find the additional hard disk. I had enough evidence of the second hard disk's existence to confront Mr X with the new information. Though he did admit to having a second hard drive running in the machine, he indicated he had removed it in the afternoon, before we had been reviewing it. I have not been able to resolve this discrepancy and it leaves a question mark about what happened in the hour the machine was being secured. Mr X agreed to supply us with the second disk for our review and we were then able to review the system to confirm our findings. We took full screen captures of the VirtualGirl software as confirmation that the software was running.

The last step in my investigation was to summarize my findings in written form and report these findings to my management.

Lessons Learned

At the time, I felt that I adequately investigated the occurrence of Internet abuse, successfully identifying the user and even discovering the attempted cover-up. However, I later felt that there were a number of things I should have done, or could have done better. As such I decided to do research to determine what additional security practices I could have utilized during this investigation, should the need arise in the future. What I found was that there were some problems with my ad-hoc approach and that I was overconfident in my investigation.

According to Moira West-Brown "Experience shows that most organizations don't think about how to respond to a computer security incident until after they have experienced a significant one." It was certainly true in my case that I had never thought how I would deal with an incident until after this one had occurred. This exposed me to some possible pitfalls that I would have been able to avoid if I had been more prepared, or had taken more time to plan my approach.

Using the benefits of hindsight and my research into security incident handling, I have created the following list of positive aspects of my investigation that could be used by other investigators to improve their investigations:

- *Double check facts using different tools* – this made me confident enough about the data that I could challenge the explanations of Mr X if required.

- *Use an innocent until proven guilty attitude <u>and</u> approach* – one of the most difficult things during the investigation was ensuring I remained objective. I found that I became suspicious and cynical. It is the reality that many people involved in investigation work are often accused of being cynical and suspicious. It took significant effort and pauses for "reality checks" to ensure I was being reasonable, and these worked well to keep me objective. More than an attitude though, the approach was to find evidence of innocence as much as guilt. It is important to remember that our job is to collect all of the available evidence, not just the evidence that would support a reprimand or prosecution.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- *Get approvals for further investigation and involve management* – At all stages I ensured that my management approved before proceeding to the next stage of investigation. This ensured that the next steps were agreed necessary by others and that human resources, local supervision and legal staff could be involved as appropriate.

- *Remotely link evidence to a specific piece of hardware early on* – If I hadn't matched the IP address of Mr X's computer system to a MAC address from two sources early on, the investigation would have been significantly hampered when the Windows 2000 hard disk was removed. I almost thought that we had secured the wrong system until we confirmed the machine had the same MAC address!

- *Keep a written log* – Keeping a written log helped me to ensure that the investigation followed logical steps and that I would be able to write up an accurate incident report later.

- *Use full screen captures* – By performing full screen captures of my machine during the remote investigation, I was able to keep a very accurate record of the data I was collecting with a timestamp thanks to the clock (which is synchronized with other clocks) in the corner of the screen.

- *Backup the evidence* - I mailed the data to myself so there was an additional copy of the data if necessary. Had my system, or the e-mail server, experienced data loss from any cause there would still have been a record of all the evidence collected.

- *Collect as much evidence as possible remotely before involving local investigators* – By collecting all the evidence I could remotely, I was able to continue the investigation even after the second hard disk was removed from the system. If we had proceeded to secure the machine early on to benefit from local evidence collection too early, there would have been no evidence to collect!

Though the investigation had some good aspects, there are several improvements to the investigation I would have made given my increased knowledge of security incident handling.

- *Preserve the Evidence* – At no stage did I obtain backup images of the disks in Mr X's computer system. Though I could not do this remotely (our WAN link speed to Niugini is only 256k), we could have done this using a local investigator. This can be very important because the system being investigated could have been configured with cleanup routines to remove evidence. Furthermore, by opening files I was changing the last accessed date on them. Had the last access date become important to my investigation, I would have destroyed the evidence.

- *The approach to the investigation needs to be formalized* - Without a formalized approach it is difficult to ensure you are using a consistent and logical approach to the investigation and that you have collected all of the evidence required. Security incident investigation is often performed in a crisis situation and as such there is no guarantee that you will be able to remember everything you need to do in a crisis. Identification of these lessons learned is another example of the need for a formalized approach.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

- *Train staff for incident response* – With all of the different factors to consider when dealing with a security incident, it is important that the staff dealing with a security incident are properly trained in computer security incident handling. Though an administrator may have the technical skills to perform an investigation, there are legal, privacy and investigative best practices to consider that are just as critical to the investigation. Without trained staff, the likelihood that your evidence will be inconclusive, incomplete or even altered unintentionally increases dramatically.

- *The administrator's account should have been locked as early as practical* - The user's password was not changed until we needed it to log in as the user. This delay created a window of opportunity for Mr X to cover his tracks.

- *Document the chain of custody* - We don't know how the user was able to remove the disk before we could secure the system, given we were logged onto the system up to minutes before its collection. Proper chain of custody documentation would have improved this situation, such that we could have determined what had taken place.

- *Follow appropriate investigative shutdown procedure* – According to Computer Incident and Computer Forensics Overview by Scott Grace, we should have taken photos of the system if possible and shut the power off from the wall when dealing with a Windows NT system. This is done to prevent the execution of any cleanup scripts set up on the machine to remove evidence. Mr X is technically skilled enough to have created such scripts if he wished.

- *Handling and transportation of evidence should be done carefully* - No backup was taken, and a vehicle transported the machine over rough terrain, the computer could have been damaged, destroying the evidence.

- *Proactive approach to reviewing log data* – We should have been reviewing log data on a regular basis to determine if there was any illegal activity. We had the tools to do this, we just needed to use them on a regular basis.

Conclusion

As David Morrow states "Just as you would not want to begin a long journey into unfamiliar territory without a good road map, you should never begin an investigation without giving careful thought to an investigative plan." The best lesson I learned from this experience is the need for such a plan. Fortunately, I was able to learn these lessons before a more serious crisis had occurred.

Many a "good roadmap" needed for successful incident handling is available on the Internet. One such "good roadmap" is the SANS Institute's" Computer Security Incident Handling: Step-by-Step". This guide is especially useful for its "Emergency Action Card", which is a quick reference on how to deal with a security incident for the unprepared. Simply by using the "Emergency Action Card" I could have formalized my investigative approach with little extra effort.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

SANS Institue's, "Computer Security Incident Handling: Step-by-Step", has detailed information on preparing to deal with, and for responding to incidents. It breaks incident handling up into six phases (preparation, identification, containment, eradication, recovery and follow-up) with ninety step-by-step instructions to guide you through the incident handling process.

With this step by step guide and the lessons learned from my investigation; I will be better prepared in future. Though it would not always be critical that you perform every step in an investigation, every step should be considered to ensure a thorough investigation.

I hope my review of this internal investigation gave others some helpful insights into useful investigative tools, such as "nbtstat", "regedt32", Hyena and Cyfin, when you are investigating an internal source of a security threat on a Windows network. However, these tools may not be useful for every situation, or for non-Windows based environments. More importantly I hope others can learn lessons from this experience, before they have an investigative experience of their own. As a final review, the lessons learned in summary were:

- *Double check facts using different tools*.
- *Use an innocent until proven guilty attitude and approach*.
- *Get approvals for further investigation and involve management*.
- *Remotely link evidence to a specific piece of hardware early on*.
- *Keep a written log*.
- *Use full screen captures*.
- *Backup the evidence*.
- *Collect as much evidence as possible remotely before involving local investigators*.
- *Preserve the evidence*.
- *The approach to the investigation needs to be formalized*.
- *Train staff for incident response*.
- *The administrator's account should have been locked as early as practical*.
- *Document the chain of custody*.
- *Follow appropriate investigative shutdown procedure*.
- *Handling and transportation of evidence should be done carefully*.
- *Use a proactive approach to reviewing logs*.

Finally, I encourage all IT security staff who perform investigations to review and document lessons learned from each experience. Step-by-step guides are very helpful, but there is no substitute for learning from experience.

REFERENCES

The SANS Institute. Computer Security Incident Handling Step by Step, Version 1.5. The SANS Institute, 1998.

The SANS Institute. "Computer Security Incident Handling: Step-by-Step." URL: http://www.sans.org/newlook/publications/incident_handling.htm (2 Sept. 2001).

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

West-Brown, Moira J et. al. "Handbook for Computer Security Incident Response Teams (CSIRTs)." December 1998. URL: http://www.sei.cmu.edu/pub/documents/98.reports/pdf/98hb001.pdf (2 Sept. 2001).

West-Brown, Moira. "Avoiding the Trial-by-Fire Approach to Security Incidents." Security Matters. March 1999. URL: http://interactive.sei.cmu.edu/news@sei/columns/security_matters/1999/mar/security_matters.htm (2 Sept. 2001)

Grace, Scott. "Computer Incident Response and Forensics Overview." 6 Mar. 2001. URL: http://www.sans.org/infosecFAQ/incident/IRCF.htm (2 Sept. 2001).

Fraser, B. "Request for Comments: 2196, Site Security Handbook." Sept. 1997. URL: http://www.ietf.org/rfc/rfc2196.txt (2 Sept. 2001)

McMillan, Jim. "Importance of a Standard Methodology in Computer Forensics." 2 May 200. URL: http://www.sans.org/infosecFAQ/incident/methodology.htm (2 Sept. 2001)

Morrow, David. "The IT Security Professional as Investigator." Computer Security Alert. March 1999. URL: http://www.gocsi.com/sec.pro.htm (2 Sept. 2001)

PRODUCT LINKS

URL: http://www.systemtools.com/hyena/ (2 Sept. 2001)

URL: http://www.cyfin.com/products/ (2 Sept. 2001)

URL: http://www.securecomputing.com/index.cfm?skey=85 (2 Sept. 2001)

© SANS Institute 2001, Author retains full rights.

Last Updated: September 2nd, 2015

Upcoming SANS Training

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

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