GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Investigating Unidentified Network Traffic

Marc Duggan
GSEC practical

Overview

One of the most important job functions of any good security administrator is to know what kind of traffic you have in your networked environment. If you know what kind of traffic is normal then you should be able to recognize traffic that is abnormal. Investigating unidentified traffic can at times be very difficult and time consuming if you do not know what you're doing. Where should I start? What sort of response is needed? Is someone hacking my environment? These are common questions asked by security administrators when unidentified traffic is noticed. The goal of this paper is to answer some of these questions and hopefully offer a process to investigate unidentified network traffic.

I plan to describe the investigation process in three different sections: Identification, Information Gathering and Response. The Identification stage discusses locating and identifying the traffic, the Information Gathering stage describes some methods for finding out more about the traffic and the Response stage deals with what to do about the traffic once it has been identified.

Identification

The first step in investigating unidentified Network traffic is to actually identify which traffic is normal to your environment and which network traffic is abnormal to your environment. Identifying network traffic is not always as easy as it seems. It requires filtering through a ton of information to try and locate what you are looking for. It can be like looking for a needle in a haystack at times, but if you use the right tools it can make your job a lot easier. In this section I plan to discuss some tools and techniques that should make this task easier.

1) Logs

   Logs are probably the best source of information you will have. There are all sorts of network logs you might have. Router logs, firewall logs and syslog are but a few of the different types of logs you should be using. If you do not have logging enabled on your networked systems you should definitely turn them on. Without logging you will have almost no information to go on. I will only discuss Network and Host Based Firewall Logs in this paper but the principle is the same for router logs and UNIX systems. The main focus here is to make sure you log as much information as possible and find a really good filtering tool to view those

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

logs. Most routers and UNIX systems use proprietary systems, so you may have to search a bit for a good filtering tool that will work with your system.

- Network Based Firewall Logs

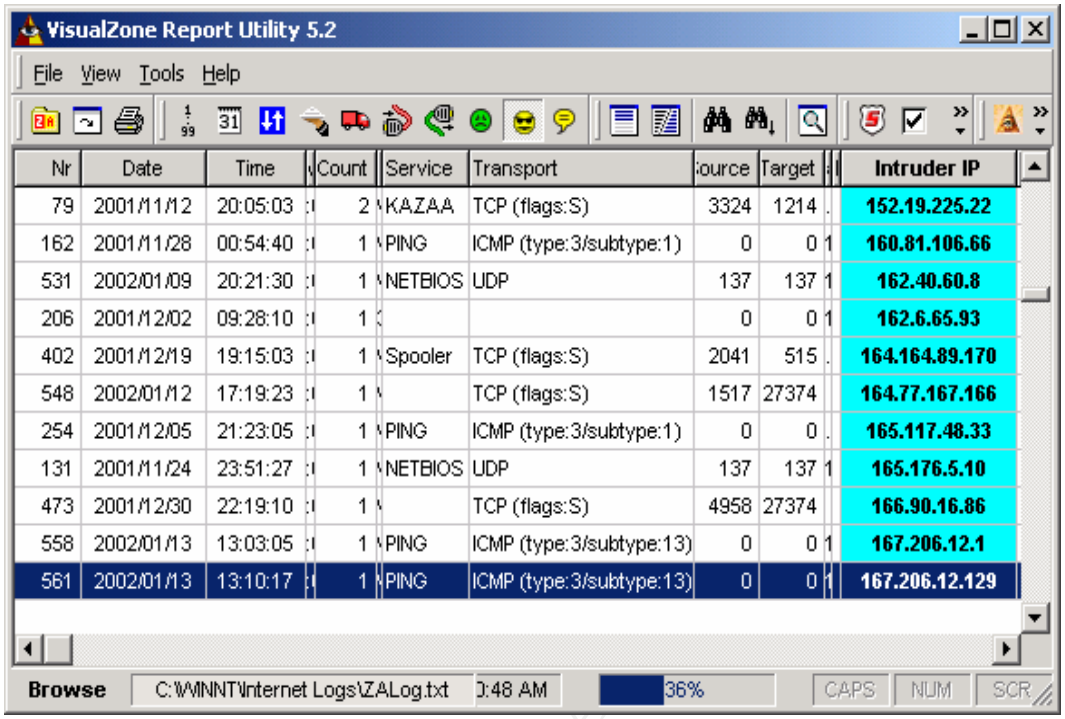
  I find the most useful logs for investigating unidentified network traffic are network firewall logs because they log your network perimeter traffic. Your firewall is the entry and exit point to your network so it would be nice to know what is trying to get in or out through that point. Just because your firewall is already configured with policies that should be filtering the traffic for you doesn't mean that some malicious traffic hasn't found its way around your existing policies. It's a good idea to go through your network firewall logs every once and a while to make sure that your firewall policy is doing its job. This can also be a good network security auditing procedure if done monthly.

  Any good network firewall product out there these days usually has extensive logging and filtering capabilities that should be sufficient for your search. I like to filter using IP source and target, port number and type of service when filtering my firewall logs. I look for any suspicious IP's or services that I don't recognize and look for the time and frequency of that traffic then move on to investigating further as described in the "Information Gathering" section of this paper listed below. Try and find IP's that are pinging your network or trying to connect using a port that your network doesn't allow. Remember, this traffic could be coming from inside you network as well. There may be something or someone inside your network trying to get out using a service you don't want leaving your environment. The main thing to keep in mind here is that you're not only looking for external traffic trying to penetrate your internal network but also traffic from inside that may be trying to get out.

- Host Based Firewall Logs

  If you are using a host based firewall it's a good idea to turn on logging. There are many host based firewall products on the market such as ZoneAlarm™ by Zone Labs [1] and BlackICE Guard™ by Network Ice [2]. These are two of the most popular host based firewalls out there right now. I use ZoneAlarm but it's all personal preference, the two programs are basically the same. ZoneAlarm comes with logging capabilities but doesn't provide a very good log viewer. So, I use a freeware tool called VisualZone™ Report Utility [3] by Visualize Software. VisualZone™ allows you to filter your logs in many different ways including some attack details. The screenshot on the next page shows some normal traffic and some suspect traffic using VisualZone™.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.



VisualZone Report Utility 5.2

File View Tools Help

Nr	Date	Time	Count	Service	Transport	Source	Target	Intruder IP
79	2001/11/12	20:05:03	2	KAZAA	TCP (flags:S)	3324	1214	152.19.225.22
162	2001/11/28	00:54:40	1	PING	ICMP (type:3/subtype:1)	0	0	160.81.106.66
531	2002/01/09	20:21:30	1	NETBIOS	UDP	137	137	162.40.60.8
206	2001/12/02	09:28:10	1			0	0	162.6.65.93
402	2001/12/19	19:15:03	1	Spooler	TCP (flags:S)	2041	515	164.164.89.170
548	2002/01/12	17:19:23	1		TCP (flags:S)	1517	27374	164.77.167.166
254	2001/12/05	21:23:05	1	PING	ICMP (type:3/subtype:1)	0	0	165.117.48.33
131	2001/11/24	23:51:27	1	NETBIOS	UDP	137	137	165.176.5.10
473	2001/12/30	22:19:10	1		TCP (flags:S)	4958	27374	166.90.16.86
558	2002/01/13	13:03:05	1	PING	ICMP (type:3/subtype:13)	0	0	167.206.12.1
561	2002/01/13	13:10:17	1	PING	ICMP (type:3/subtype:13)	0	0	167.206.12.129

Browse C:\WINNT\Internet Logs\ZALog.txt 0:48 AM 36% CAPS NUM SCR

You can see that the IP 167.206.12.129 is pinging my network on 2002/01/13. It may be nothing but it could be someone port scanning my firewall for open ports. It might be a good idea to filter the above log by Intruder IP and see how often it has been attempting to hit my firewall. These types of things are hard to notice at first, but as you filter through the logs you'll start to see what's really going on. Spend some time filtering the logs by different categories. It pays to experiment with different filters and pattern matching, look for trends, good and bad. Write some of this information down, as it will come in handy later during the Information Gathering stage later on.

2) Network Monitors and Intrusion Detection Systems

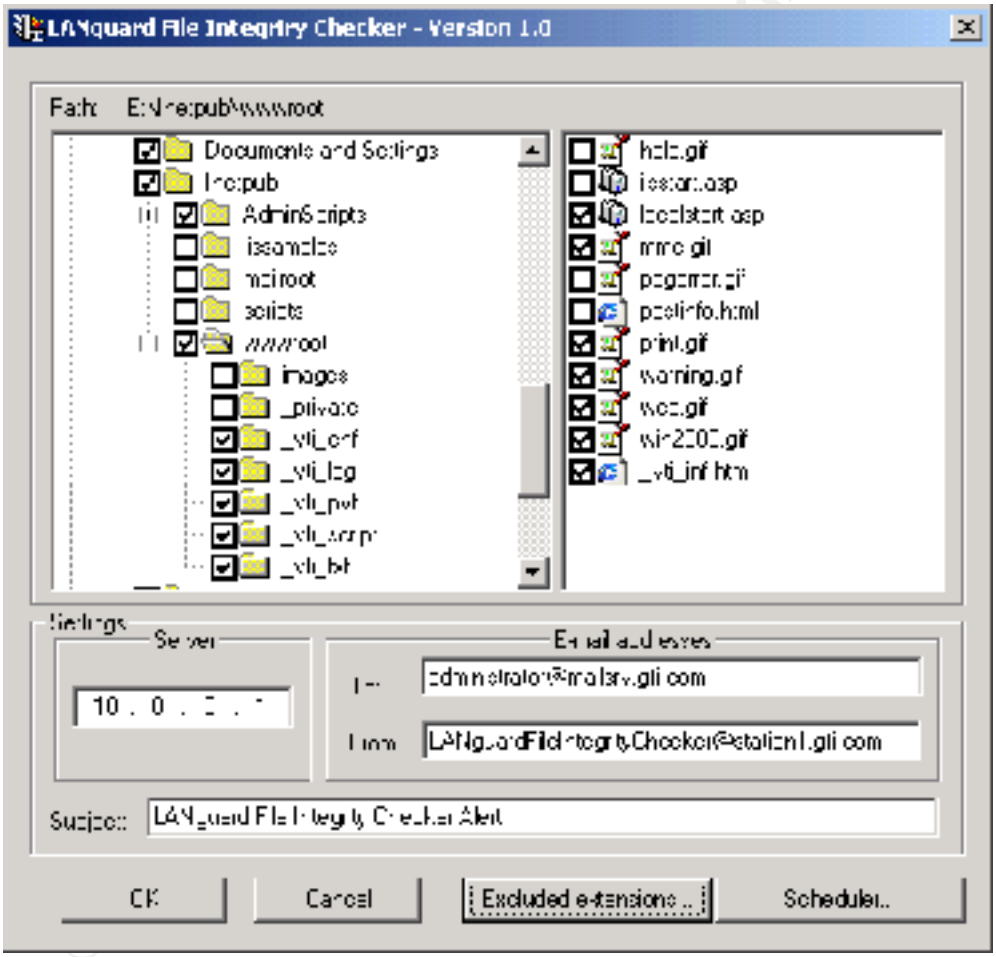
Network Monitors and Intrusion Detection Systems can include everything from tools that perform basic heartbeat functions to tools that can perform very sophisticated Intrusion Detection functions. These systems can notify you if a potential intrusion has taken place on your network. The big disadvantage of a lot of these systems is that they will simply notify you once the event has taken place. Some of them however are starting to be able to block intrusions known attacks and log information about the attacks. The ability to do this is relatively new technology and can still be limited by the vendor's known intrusions database file.

There are many network monitoring software packages on the market. Most of them perform heartbeat functions and have extensive notification, logging and filtering capabilities. They can notify you of problems with your network in a graphical form that will allow you to analyze your network traffic flow. There are also many network monitoring tools available as freeware.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Intrusion detection systems almost always have extensive logging capabilities and it's good to utilize them to the fullest. They can give you information like where the attack is coming from and what type of attack it may be. In some cases your IDS may block these attacks for you, in others you may have to take action yourself. Keep on top of these logs as they can give you invaluable information about what kind of traffic you have on your network.

LanGuard™ File Integrity Checker is a freeware tools by GFI. It's an IDS tool that will notify you if the contents of a folder or a file has changed and send you an email to notify you. The screenshot below shows LanGuard™ File Integrity Checker's configuration options.



When the above settings are enabled the program will start scanning for any changes made to the folders and files that are checked and send an email to the address indicated in the E-mail addresses field. I find this tool particularly useful on my web servers when dealing with website defacement threats. If any of my web files change the application notifies me immediately. This is also a good tool to notify you of changes made to you system files. The application's scheduling functions also allows you to set monitoring times and dates, which can be quite useful for some application traffic.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Many other enterprise level intrusion detection software will allow you to run this sort of application network-wide so that you could monitor your files on the entire network all from one location. Intrusion detection systems are a valuable resource for tracking down information but unfortunately, most of them will only notice the problem once the damage is already done. Once you get notified of the change you can gather more information as described in the Information Gathering section of this paper to further your investigation.

3) Honey Pots

Honey Pots are basically decoy systems that you set up in a test environment far away from your production network to study external network attacks. They can give you a wealth of information about IP address that you should probably take action to avoid and ports you should probably close. The most extensive research done on Honey Pots is by the HoneyNet Project (project.honeynet.org) [4]. This group of security experts does extensive work with Honey Pots and probably knows more than anyone about this subject. You can learn a lot about an attacker by studying them on a decoy or sacrificial network or machine. Make sure you keep them far away from your network in a lab environment as they could easily compromise your production network environment and cause a disaster.

All of the Identification techniques described above will help you gather more information about the unidentified traffic and give you a better understanding of how to respond once you've identified them. There are many other identification techniques that are also very useful. Use whatever tools you can find, experiment and remember to log as much information as you can. We'll use these logs in the Information Gathering section to start probing deeper into the information we have gathered so far.

Information Gathering

Information gathering is probably the most exciting part of trying to investigate unidentified network traffic. You'll likely start to develop and extensive toolbox of network utilities and sniffers tracking down suspicious information. When performing information gathering functions it is important to know what you're looking for. Listed below are a few key pieces of information I always like to have.

- Contents of the Packet – High-Level

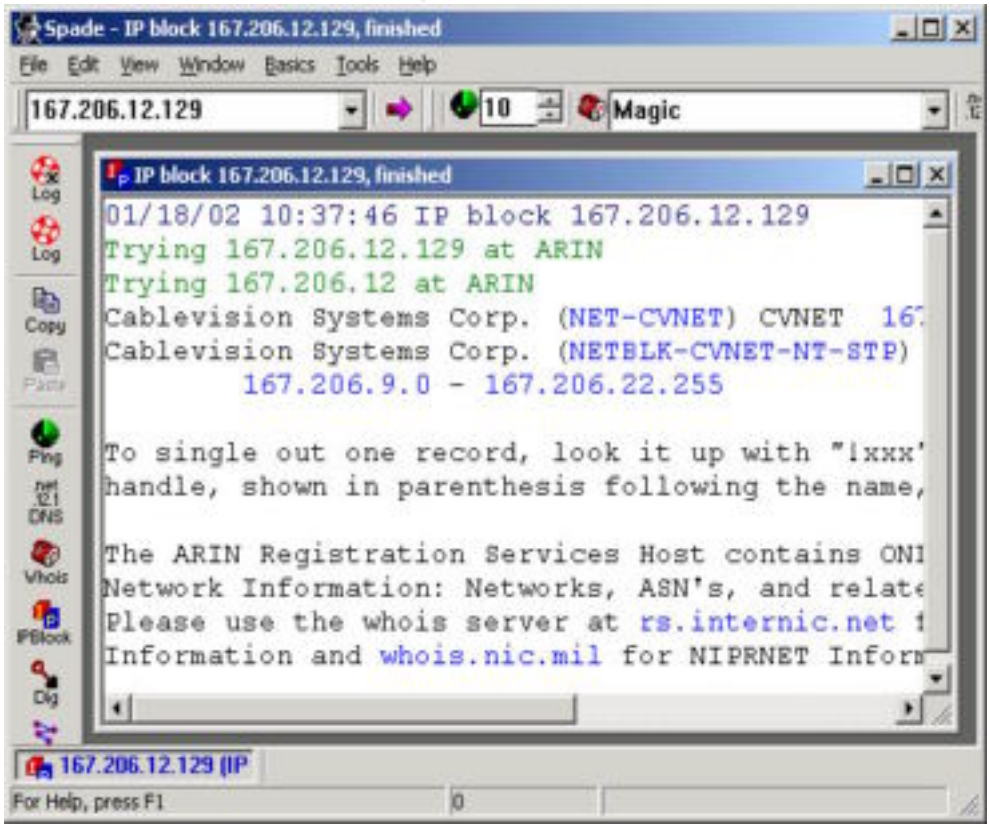
  The high level contents of a packet are fairly easy to find as most firewalls log this automatically. You should be looking for the port numbers, the data type, text, etc. Look for unusual port numbers, unfamiliar IP's and strange data types. This kind of information can give you a good idea of what the traffic is trying to accomplish.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

In most firewall logs viewing applications there will be plenty of high-level packet information available to you. A great resource for well-known port numbers is www.iana.org [5]. Look up the port the traffic is using and compare it to a list of well-known attacks that use that particular port. Maybe the traffic is associated with a certain application. Perhaps the traffic is coming from a machine inside your network running a service or application that is generating that traffic. It's really important to get as much information as you can about the high level information of the packets. You'll probably use this information more than any other due to the fact that most traffic generated on or through your network will be from your network applications or services and most of your external traffic will be caused by sources outside of your networked environment. Web server and firewall requests from external sources can cause a ton of traffic in cases of DDOS attacks and network scanning. You'll probably notice that there is a lot more network scanning happening to your network than you thought.

- Source and Destination

  To find the source and destination of these packets you can use many tools. There are all sorts of lookup utilities available on the internet. Whois, Sam Spade™ [6] and LanGuard™ [7] Network Scanner are but a few of the free tools that you could use to accomplish this task. The screenshot below shows an example of the output from a whois command using Sam Spade™.



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The output from Sam Spade™ tells me where the traffic is coming from and I can trace route the IP to see what path it is taking to get to me. This is all good information to have when trying to track down the source of this traffic. Remember, the source of this traffic maybe completely unaware of the fact that they are sending traffic you way (this being the case with zombie or trojan attacks). Be careful not to probe someone else's network though, you merely want to identify the source of the traffic and what type of traffic it is. You don't want to find out anything about the traffic sources internal network.

Sam Spade™ is also capable of performing all sorts of inquires such as pings, fingers, trace routes and many others. There are tons of tools that will do virtually the same thing. You will likely find your favourites and stick with them.

- Contents of Packet – Low-Level (Packet Sniffers, Netmon, TCPDump)

  Low level packet content is not always necessary information to have when investigating unidentified network traffic, but it's nice to have and in some circumstances very valuable information. Tools like packet sniffers, netmon and tcpdump can give you quite a bit of detailed information about the packet. Ethereal by Gerald Combs [9] is a great open source packet-sniffing tool. It works on Windows and UNIX and it allows you to examine data from a live network or from a capture file on disk. You can browse the capture data interactively, viewing summary and detailed information about each packet. Ethereal also has many powerful features, including the ability to view the reconstructed stream of a TCP session and a rich display filter language. It really pays to find a good packet sniffer. You may not need to use it that often but when you do you'll find the information invaluable.

Information gathering takes a lot of time and patience but the information you gain will give you a good understanding of what your network traffic looks like. It's a very important part of investigating unidentified network traffic and you should take your time doing it. It's important to do your research carefully without disturbing other networks integrities. You'll likely start to develop an eye for oddities or abnormal behaviours, the process will become easier for you as you spend time doing your research. Now that you've done your information gathering it is time to respond to this unidentified network traffic.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Response

There are two different ways you can react to the information you have just gathered and analyzed. Either you care about the traffic or you don't care about the traffic. Either way, some kind of response is required. Even if you decide you don't care about the traffic or the traffic is normal, a response is still required. Listed below are the steps you should take after you have finished analyzing the information you have just gathered.

- "I care about the traffic because it is abnormal traffic for my network"

  If you are concerned that the traffic you have identified may be malicious, or is abnormal traffic for your network, you should definitely investigate further. Once you are sure that the traffic identified is traffic that you do not want on your network you should start to think about filtering that traffic.

  Filter this traffic by port number or IP number. Make the necessary changes to your firewall policies, your IDS's and your routers or whatever device lies between you and the traffic source. Restricting time and date on certain services is always a good idea. Keep in mind though there may be nothing you can do about the traffic short of shutting you network down. Particular DDOS attacks can render your web servers useless if it's coming from multiple sources or "zombie" machines.

  Another good response is to filter at the log level of these devices. You can use your logs or monitoring tools to alert you when a certain IP is hit with a port you have flagged or notify you if a directory has been changed. This type of filtering will take a lot of time and care to get it right, but if you spend time on this it will definitely make your network traffic cleaner for the future.

  Make sure you monitor the filters you have put in place. You'll probably find they require a lot of fine tuning at first, they run for a while, then down the road at some point the filter is of no use anymore and you didn't even realize it. These filters can then cause havoc with your systems. It is very important to monitor the filters you have in place. Do an inventory of them every month or so to make sure they are still relevant.

  Document everything you've done concerning the traffic you've been investigating and all of the filters and monitors you have put in place on your network. Documentation is the last but probably the most important step when investigating unidentified network traffic. If you've documented everything you possibly can about your investigations you can refer back to that information later if needed and find relevant information that may help you with similar events in the future.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The main focus of here is to Identify, Gather, Analyze, Filter, Monitor and Document as much information about the "suspect" traffic as possible. Thresholds should be set with alert mechanisms so that you can get to the information has soon as possible. Proactively applying filters in this stage is important for preventing further traffic. These steps, performed over and over again will help you to run an efficient, clean network.

- "I don't care about the traffic, it's normal to my network"

  If you've come to the conclusion that the traffic you've been investigating is normal to your network you should still respond in some way, shape or form. Most importantly you should document this traffic as being normal. This will help you create a baseline for normal traffic to which you can filter against.

  Setting a baseline for normal traffic is extremely important and should be documented thoroughly. Record the time and date, the type of traffic, the source and destination. This type of information is very important because you want to make sure that none of your new filters block or interfere with the normal traffic on your network. Create a database with all of the applications your network considers normal traffic and try and isolate your normal traffic flows. The baseline database should be audited monthly and modified as needed.

  Remember, just because this traffic is normal network traffic doesn't mean your job is done. You should document this traffic as normal and baseline your network accordingly.

Summary

After completing the above steps you should be able to know what kind of traffic is normal and what type of traffic is abnormal. Remember, one of the most important job functions of any good security administrator is to know what kind of traffic you have in your networked environment. The best defence you have against malicious network behaviour is your understanding of your network baselines. You should be able to recognize traffic that is abnormal to your network and respond accordingly. Having the right tools, setting baselines for normal traffic and documenting everything should help you greatly when performing these job functions. Investigating unidentified traffic is a tedious task at times but can be quite rewarding when it solves a major problem you've been having on you network.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

[1] Zone Labs
http://www.zonelabs.com/products/za/index.html

[2] Network Ice
http://www.networkice.com/products/soho_solutions.html

[3] VisualZone
http://www.visualizesoftware.com/visualzone/visualzone.htm

[4] Honeynet Project
http://project.honeynet.org

[5] www.iana.org
http://www.iana.org/assignments/port-numbers

[6] Sam Spade
http://samspade.org

[7] LanGuard by GFI
http://www.gfi.com/languard/lantools.htm

[8] tcpdump.org
http://www.tcpdump.org

[9] Ethereal by Gerald Combs
http://www.ethereal.com/download.html

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Last Updated: May 1st, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 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 Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 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 Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
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
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
SANS Munich Summer 2017	Munich, Germany	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
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 Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS