Global Information Assurance Certification Paper

Novell Server Quick Security Guide for the Overworked Administrator
Tony Flowers
Version 2.1 Administrivia
Version 1.3 GSEC Practical Assignment

Introduction

In today's fast pace and need it now world, administrators are just barely able to keep up with current user problems and ongoing request. Because of this, most administrators have not properly secured their Novell NetWare servers. There is always some computer problem that affects users and must be fixed immediately. Administrators are rarely given the time and resources to properly monitor and secure the servers under their care. Most often when a new server is brought up, there is a deadline for implementing or putting the server into production. Even when new services are added to production servers, there is little time to worry about securing them; if it is up and running great then don't break what isn't broken. This document goes into some of the basic steps all administrators of NetWare servers should take to secure their servers.

Abstract

In the first section, older versions of NetWare are discussed. The bindery is security risk in older versions and many hackers will seek holes in the server through the bindery. Also, Novell uses an older protocol called IPX that is not routed on the Internet and cannot be secured or encrypted like other protocols. Afterwards, maintenance needs to be addressed, administrators need time to properly maintain a server and apply patches that are required. Monitoring the server for problems is a task taking another slice of time. There are several tools that an administrator can use to help with these tasks. Next is the Virus threat and how administrators should spend time guarding against it, where to go for updated information, and what software to have running on the server and the workstation. And then a quick discussion on updating or patching machines with new virus information follows. After viruses, an administrator must be concerned with what users have access to what resources and if a user might have too much access. An administrator has certain tools that can help in the search for user security. Then an administrator must correctly assign and monitor what other administrators do on the server. Novell offers tools to help the administrator monitor the server for changes. Intruders need to be tracked and log files need to be monitored, there are programs that can perform this function and reduce time need by the administrator. Backups are always needed and log files are there for the asking; both help the administrator in the fight for survival. Hackers listen in to traffic but what is an administrator to do? Physical location and protection are important and can be overlooked. Firewalls protect but are they enough? You are running a filer server but is it a web server too? Certificates helps with authentication but does it really help?

NetWare 2.x, 3.x, 4.x

A quick and easy security step is to upgrade older versions of NetWare. One of the strongest arguments for NetWare is its stability. NetWare tends to give administrators less headaches and problems then other network operating systems (NOS). Because of this 'feature', upgrades to the current version of NetWare take a back seat until it is a requirement to run some new service or program. This in itself is a security concern. Novell takes care to update current versions of NetWare, but cannot keep older versions up to date with new patches and security fixes. A big security problem with NetWare is the old bindery. There are several tools to hack into the bindery and take usernames and passwords. This security risk disappears when an administrator moves to a current version of NetWare and uses Novell Directory Services (NDS). Novell has moved the current version of NetWare to Internet Protocol (IP). This is the protocol that computers use to communicate on the Internet with each other and between multiple OSs'. This allows NetWare to compete with any other NOS and to support users through sharing information with any OS. Administrators should upgrade servers as soon as possible to reap the benefits and new features of newer NOS.

Down the server

It is important for administrators to schedule down time for their servers. During this down time patches can be applied to servers, changes can be made to hardware, and configuration files can be modified. This can be part of a security policy for a site. RFC 1244 (1) is a handbook that goes into some detail explaining just how to start setting up a good security policy. An often forgotten security piece is the policy of what to do and not to do. Check Novell's minimum patch list (2), this is the first step in securing a server. There are important updates that should be applied and are often overlooked. Also, peruse Novell's free tool kit (3); there are several tools that can reduce time needed for monitoring, maintaining, and securing a server. On-Site (4) is a good tool for testing the security of your NetWare server. It allows an administrator to scan the NetWare Directory Services (NDS) and gather information about the NDS structure. All administrators should become familiar with these tools to help them understand what tools hackers use to gain access to servers.

Virus Running Amok

A server needs to be updated all the time. Administrators spend a good amount of their precious time doing just that. So, updating the anti-virus software should be the next step in securing your server. Make sure the latest updates are applied to your server; subscribe to newsletters (5) about new threats, and alert users when major viruses hit the Internet. An easy way to reduce the time needed to manage a server is to set up the automatic updates that most anti-virus software has built in. This will save an administrator time in

downloading the latest changes that an email notification suggests. Notifying users about the latest virus can save several helpdesk calls, it not only helps the administrator but also puts the users on notice and the users know that their administrator is looking out for them. The administrator should have an anti-virus package installed on all workstations. These must be updated on a regular schedule and patches applied often. An administrator should require all users who take work home to have the approved anti-virus software installed on all machines that will access data from the servers or from a disk brought to and from the home. These machines should also be updated with patches on a regular schedule.

Am I an Admin?

When servers are first brought up, security is not the first thing on an administrator's mind, but getting the server to work is the foremost thought. Security should be looked at before the server goes into production. Novell offers a program called **Security.exe** that runs against the bindery to determine what security holes are open on older versions of NetWare. In newer versions of NetWare, the only way to run this same 'program' is to create a batch file with the proper commands to query the server for this information. In Novell's knowledge base, technical information document (TID) 10024879 (6) discusses how to create a batch file to gather all this information. The batch file uses the powerful command **Nlist** (7) to gather detailed information and can be modified to gather other information specified in a security policy. This will allow an administrator to further secure the server. Remember the more increased security the less usability the server will have in the eyes of the users. Users tend to want full functionality and full security but administrators cannot give them both. An administrator must carefully weigh security requirements with the needs of the users to determine what level of paranoia is required to keep the server secure. The administrator should follow a good password policy. This policy should not allow any null passwords or easy to guess passwords. It should require a certain length and not allow use of old passwords. If there would be standard usernames, as 'backup' or 'printer', that are used on certain workstations; then set up limits on which workstations that these users can login to from. In NDS, a username can be further secured by assigning an IP address or MAC (Media Access Control) address allowing only those system accesses. MAC addresses are hardware addresses that are assigned to the network card. To add even more security to user accounts, limit the number of connections a user can use. An administrator can set how many workstations a user can login from simultaneously. Time limits can help with security. An administrator can set a time limit to keep users off the system during night hours or other time tables set up by the administrator. The user 'backup' might only need access to the server from 11:00pm to 2:00 am. Another problem facing administrators is finding hidden Organization Units (OU) (23). An OU is a grouping of users, workstations, and resources that belong together. A favorite tactic of hackers is to create a hidden OU and place a user with admin privileges in the tree. The hacker takes the browse right away from everyone and then no one can 'see' the OU. This allows hackers to login into the server. Novell

offers a NLM called **Hobjloc.nlm** (26) that can help locate these hidden OU. If a hidden OU is found then the server most likely has been compromised.

Admin I Am!

An administrator not only must verify who has admin rights and access, but should also be concerned about which administrators have access to what on the server. The lead administrator can give certain users administration rights to an OU. Most of the time administrators group OU's by department, location, or some other logical grouping. This allows a local administrator to control the information in one part of the company without having access to others. The local administrator would have the ability to manage users and local resources including printers.

When more then one administrator physically operates or modifies a server, logs and records must be kept. Without this information, changes to the server cannot be tracked. A server logbook should always be kept. As an example, one administrator makes a change and logs the change for future reference in the server log. If a problem arises from the change, another administrator would know what modifications had been applied on the server. Even when only one administrator is providing support, a logbook can help. When a change is made to the system record the date, time and action. When a problem comes up later, the logbook will help to track down the problem. Also, Novell offers a service to track changes that administrators make on the server. This service is called Auditcon (9). This service allows auditors to monitor NDS events and other server events. There is a side effect to this service; it will monitor what a hacker might do to the server also. Reviewing this information might allow an administrator to protect the server before a hacker breaks in too far or help to secure it after an attack.

Intruder Alert

A hacker hopes that the administrator has not turned on Intruder Detection (10) . Without this option turned on, a hacker can try to attack a user account by guessing the password. NetWare will just keep telling him to try again. But, with this option turned on, the hackers will lockup the account for the time that the administrator has set. Intruder Lockout is set on each OU. These intruder detection alerts will temporary stop the hacker from guessing the password. If more then one alert happens and the user is not the cause of the problem, then the administrator has evidence of foul play and should take further actions to secure the server. Always have another user set up as an admin equivalent. If the admin account is locked out, then the system can still be accessed by the second account. Another good practice is to rename the admin account to something else. Then create an admin account that has no rights to the server. On the true admin account set the password to a length of at least seventeen characters. This practice helps to defeat hacking tools from discover the password. Some hackers look for the account admin or administrator to hack. Renaming the account first, adds one more step to a hacker's attack

procedure. If it becomes too much trouble then the hacker might move on to an easier target. Honeypots (22) are servers' set up to look good to a hacker and allow the administrator to watch what the hacker is doing. Most administrators do not have the time to set one up and maintain it properly. There are too many real problems and security issues for an administrator to worry about then to create and properly maintain a decoy. And then there are always those pesky user problems to deal with.

Call for Backup

Sometimes administrators overlook the need for backups. Backups are the only way to insure complete protection from hackers and other disasters. When a hacker gets into a system, the administrator must bring down the system and format it if the depth of penetration is not known. Backups then become critical for the survival of the administrator and possibly the company. With adequate and verified backups, an administrator can restore a system to functionality quickly. There are several third-party backup utilities (11)to choose from. The most important part of the backup is to do it. The next step is to verify the backups.
One very good procedure to place in the backup policy is to have off-site servers. These servers do not need to have the horsepower but only the storage capacity to equal the main servers. Take the full backups and restore them onto the off-site servers. Also, this backup policy works with the disaster recovery policy, which should call for off-site data storage. Not only are the backup tapes tested and verified as a good restore, there is an off-site working copy of the data. In case of a major disaster, an administrator could get the data to users quickly. If the main server must be formatted, then the backup server can be brought in to temporarily replace the main server until it is back online. This limits the down time for users and adds more weight to both the backup and disaster recovery policies.

Logs, Console, & The Mighty Batch File

Log files (12) can help the administrator control and secure the server. Administrators should spend some of their time monitoring these log files. Logs files pass information to the administrator letting them know what the server is up to and what is happening to the server. Another log file to look at is **Console.log** in the **Sys:etc** directory. ePlace the '**load Conlog'** command in the **Autoexec.ncf** file to have it preloaded. (13) This NetWare Loadable Module (NLM) writes console messages to this file. This will allow the administrator to look at what has happened to troubleshoot a problem or hacker activity. Here is where a batch file can be a mighty powerful tool. An administrator can set up a batch file to automatically run from a workstation and copy the **Console.log** file to the workstation or another server. Then there is a copy of the file. This can be set up to occur as often as the administrator would like. When the administrator is following a hacker's trail in their system, they can look at the copied log files to help. Most hackers will try to cover their tracks and delete or turn off the log files.

Flood of Packets

A server sends packets of information to a client. The client then responds. The server and client 'talk' back and forth sending information that a hacker might want to 'listen' in to. A hacker could intercept an existing conversion and change the information in that conversion. Novell has included in NetWare the ability to stop hackers from listening in or seizing the session. Packet Signature (14) is a Novell service that uses the NetWare Core Protocol (NCP). This signature allows the administrator to secure the packets or communication traveling between the server and the client. There are several options including setting the server to not accept packets that are not signed. One thing to note, some software will not work correctly when using Packet Signature. One example would be some uninterruptible power supply (ups) remote monitoring software, which cannot communicate to other machines when enhanced security is turned on. In order to use Packet Signature and the monitoring software an administrator would have to set the ups remote monitoring software to use a lower signature level then the server default. Most NLMs can have their signature level set lower or higher then the server default. The client and server can be set to disabled, request, preferred, or required. This allows the administrator the ability of increasing security to some workstations over others if the server must be set at a lower level. Workstation that administrators will use should be set to the highest level of security.

Now Where's That Server Located?

Administrators sometimes forget the simple security measure that includes the location of the server. Some sites have been know to have the server sitting in the hall were everyone can see it. Others place it in a meeting room or in a closet. All of these locations are not secure. Cleaning crews can come in and unplug the server to use the outlet for the vacuum cleaner. A server does not respond well to being unplugged nightly, especially when the backups most likely have not yet run. Servers should be **locked** in a controlled room. Access to this room should be controlled also. Whenever an administrator leaves the company, the lock codes need to be changed. If possible, have the air-conditioning system controls located in the room and on a separate unit for the servers. Servers should have one ups on each machine whenever possible. Part of the ups system should include monitoring software that allows the administrator the ability to monitor the status of the ups battery and voltage. This monitoring software should allow easy access to this information from remote locations.

Novell has a command that can lock down a file server. The command **Secure Console** (15) allows the administrator to increase security for the file server. It does not improve physical security but locks the location from where NLMs can be executed. Secure console also stops the data and time from being altered. This could be used to cover a hacker's tracks. On the other hand, **SCRSAVER** (16) is designed to put the physical

server into a more secure state. A password prompt is required to access the server using NDS authentication. One final step is to remove the keyboard and mouse from the physical machine. An administrator would then need to manage the server using remote control software built into Novell. Some security experts suggest having a 'power on' password. This can be helpful in a 24-hour supported site. If a site has ups software that will boot the machine when power is restored then the administrator would need to type in a password to bring up the server. But, in a site where administrators are not available around the clock then the server would sit at the password prompt. Take careful consideration on which route to take. If the servers are physical secure then opting for no BIOS or CMOS password could help the administrator.

Firewall, mine's made out of a brick wall

Firewalls, who needs them! We all need them. An administrator must deal with the fact that no operating system is hack proof. The server must be secured in some fashion. Most companies have a border firewall in place to restrict unchecked snooping from the network. But not all companies have a well thought out firewall. An administrator must protect the servers. The firewall or security group is often not in the same group as the administrators. To protect a Novell server, Novell has released a product called BorderManager. (17) This is a firewall application designed for NetWare. It allows an administrator to configure what information comes and goes on the server. The administrator can lock down whether the web page can be accessed from the Intranet or the Internet.

The administrator can use this server as the single access point for Remote Authentication Dial-In User Service (RADIUS). This is the service that users dial into for access to the network, servers, printers, and other resources or to surf the Internet. BorderManager allows the administrator to control what goes on during these connections, how long they last, what is the access time limit, which user can dial in and several other options. Another piece of BorderManager is it includes a Virtual Private Network (VPN) service. This creates a secure tunnel that is encrypted between the server and the client. This allows secure access to sensitive data. When users are connecting using broadband or high-speed connections, then a VPN greatly increases the security of the network and fills in one more hole in the fence.
The administrator must still worry about a hacker gaining access to the workstation before the VPN. A workstation-based firewall is a great protection for these users. An application firewall inspects all traffic coming and going from the workstation. It will ask the user if application xxx can access the Internet. These options can be pre-configured. ZoneAlarm from Zonelabs (18) is a free firewall (24) for personal use. There are many other choices in firewalls. An administrator must check out all options and choose which best meets the requirements of the company (19).

A Portal to the Server

NetWare allows administrators the ability to access the servers from any web browser. Try typing in http:\\server-ip:8008 and now be very afraid. Some Novell servers will have a default web page running. But all is not lost. NetWare Management Portal (NMP) (20) can greatly enhance an administrator's ability to keep tabs on the servers. There is a wealth of information available for everyone to see. That is the problem. Please, all administrators should follow the links provided with this section to close off the information provided by their servers to anyone that types in the server's IP. NMP is a great tool, it does save time and allow the administrator to remote control and manage the server, down and restart it. The main page can be customized to include other information that is needed by the administrator. The administrator should change the default page port from 80 to another port number. If a hacker types in the server's IP address, then the server will bring up the NMP by default. The port 8008 used by the NMP should also be changed.

Certificate Server

An administrator could be called upon to find a way to verify email. A user might request that the administrator verify that the email that the user received is from the real sender as stated in the email. No small task short of calling the sender. But, Novell has provided the ability to issue certificates using Certificate Server (21) on NetWare servers. This allows the administrator to issue a certificate, which is a digital attachment that guarantees that the sender is real and a reply could be encoded for even more security. This is currently a free product. This product is designed to increase security by using Secure Sockets Layer (SSL) (22) for communications on the server and for secure email (S/MIME). SSL certificates can be purchased for more security on web servers' etc. from several companies (25).

DHCP

Dynamic Host Control Protocol allows computers to get an assigned IP address from a server. When a workstation boots up it broadcasts or shouts 'is there a DHCP server around that can give me an IP address'. This at first sounds great. If a network has more computers then IP address, then DHCP will help to manage them allowing two or more computers to share an IP address. A part-time user can use the IP address and then when the user leaves and stops using their computer, another user can be assigned the same IP address. This allows one IP address to be shared. This works great in a pool of workstation composed of laptops and part-time employees. But DHCP can be a security risk. It allows any machine to connect and start looking around. To properly manage DHCP, you can assign MAC address to an IP on the DHCP server. If a hacker can gain access to the network with an IP from within the network then security is general less inside then out. Conference rooms can be dangerous and empty offices poise a threat to

security of the servers and other workstations. Within the local network, Microsoft Networking can be used or NETBOIS to view other Windows based machines. All entry points to the network should be guarded with access assign where needed. Unused access points should be disconnected or turned off using managed hubs. If possible, map the ports on the managed hubs to offices. An administrator should have a physical map of network ports to offices. When a new user is brought on board the office that the user will use should be connected and the port map updated. A copy of this map should be posted in the server room and network closets.

References, Links, & Downloads

1. Holbrook, P. & Reynolds, J. Site "Security Handbook RFC 1244." July 1991. http://www.faqs.org/rfcs/rfc1244.html

2. Novell. "Minimum Patch list." March 25 2002. http://support.novell.com/misc/patlst.htm

3. Novell. "New Free Tools." http://www.novell.com/coolsolutions/collector/freetools.html

4. Novell. "On-Site program." http://ftp.dataconstruction.se/ftp/Novell/ or http://www.google.com/search?q=cache:UCHnrrRmZLYC:ftp.dataconstruction.se/ftp/Novell/+onsite.zip&hl=en

5. Virus email alerts. http://nct1.symantecstore.com/virusalert/ or http://www.mcafee.com/ or http://www.cert.org/contact_cert/certmaillist.html or http://housecall.antivirus.com/

6. "SECURITY.EXE equivalent information in." Novell TID 10024879. 11 Nov. 2000. http://support.novell.com/cgi-bin/search/searchtid.cgi?/10024879.htm

7. Novell. "Nlist Utilities Reference." http://www.novell.com/documentation/lg/nw4/docui/index.html#../utlrfenu/data/hgvz42hx.html

8. 3Com. "Knowing Your Network's Configuration." Log books and Troubleshooting guidelines. http://support.3com.com/infodeli/tools/netmgt/tncsunix/product/091500/c3manna3.htm

9. Novell. "Auditcon." http://www.novell.com/documentation/lg/nw42/index.html?utlrfenu/data/hwrmvij9.html

10. Novell. "Activating Intruder Detection."

http://www.novell.com/documentation/lg/ndsee/index.html?ndseeenu/data/fbbcfaga.html

11. Backups Packages
http://www.veritas.com/products/category/ProductDetail.jhtml?productId=benw or
http://www.network-backup.com/datasheets/nnet8_ds.html or
http://www3.ca.com/Solutions/Product.asp?id=3371

12. Log Files
Novell. "Working with Log Files"
http://www.novell.com/documentation/lg/nw51/index.html?esvgdenu/data/a2fet9f.html

Novell. "What's the purpose of sys$log.err file?" TID 10061211. 6 April 2001.
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10061211.htm

Novell. "Working with the Log Analyzer." 4 Jan. 2001.
http://www.novell.com/documentation/lg/nw6p/index.html?adminenu/data/a2fetak.html

13. Novell. "When placing CONLOG.NLM at the top of the autoexec.ncf." TID 10059502.
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10059502.htm

14. Novell. "How does Novell's Packet Signature?" TID 10024712. 9 Jan. 2001.
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10024712.htm

Novell. "NCP Packet Security"
http://www.novell.com/documentation/lg/nw5/docui/index.html#../usserver/ssec_enu/data/hc66y4qi.html

15. Novell. "Secure The Server Console."
http://www.novell.com/documentation/lg/nw51/index.html?ssec_enu/data/hpmfqfmr.html

Novell. "Secure Console."
http://www.novell.com/documentation/lg/nw51/index.html?utlrfenu/data/hm9phvjr.html

16. Novell. "Scrsaver."
http://www.novell.com/documentation/lg/nw51/index.html?utlrfenu/data/hrs18jbe.html

17. Novell. "BorderManager 3.7."
http://www.novell.com/products/bordermanager/

18. Zonelabs
http://www.zonelabs.com/

19. Firewall Information
Gibson, Steve. "Shields Up." 26 Feb. 2002
http://grc.com/su-firewalls.htm

Bahadur, Gary. "Personal Firewalls" Personal Firewalls Under Fire. Information Security. July 2001.
http://www.infosecuritymag.com/articles/july01/cover.shtml

Graven, Matthew P. "Personal Firewalls." PC Magazine. January 2001.
http://www.zdnet.com/products/stories/reviews/0,4161,2669359,00.html

McWilliams, Brian. "Personal Firewalls Fail the Leak Test" Enterprise News. December 7, 2000.
http://www.internetnews.com/ent-news/article/0,,7_529661,00.html

http://www.pcworld.com/hereshow/article/0,aid,17012,00.asp

Dalton, Curtis. "Getting Personal With Firewalls." NetworkMagazine.com. Jan. 2001.
http://www.networkmagazine.com/article/NMG20010103S0010

20. Novell. "Using NetWare Management Portal."
http://www.novell.com/documentation/lg/nw51/index.html?admnsenu/data/a2zzmpg.html
Novell. "Using Netware Management Portal." More.
http://www.novell.com/documentation/lg/nw51/index.html?port_enu/data/a27vgr6.html

Novell. "How to increase security of the NetWare Management Portal." TID 10026783. 9 Aug. 2000.
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10026783.htm

Novell. "**How do I configure NetWare Management Portal to hide all Server info before?**" 20 April 2001.
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10061893.htm

21. Novell. "Novell Certificate Server Questions." TID 10059197. 6 Dec. 2001.
http://support.novell.com/cgi-bin/search/searchtid.cgi?/10059197.htm

Novell. "Server Certificate Object Tasks."
http://www.novell.com/documentation/lg/crtsrv20/index.html?crtadmin/data/a2ebopb.html

Novell. "Novell Certificate Server." FAQ.
http://www.novell.com/products/certserver/faq.html

22 SSL
Webopedia.
http://www.webopedia.com/TERM/S/SSL.html

Netscape. "Introduction to SSL." 1998.
http://developer.netscape.com/docs/manuals/security/sslin/contents.htm

Verisign. "SSL Basics." 2000.
http://www.verisign.com/site/ssl.html

RSA. "SSL Basics for Internet Users." 2002
http://www.rsasecurity.com/standards/ssl/basics.html

22. Honeypots
Delio, Michelle. "Honeypots: Bait for the Cracker." INC. 7 March 2001.
http://www.wired.com/news/culture/0,1284,42233,00.html

Klug, David. "Honey Pots and Intrusion Detection." Sans Institute. 13 Sept. 2000.
http://rr.sans.org/intrusion/honeypots.php

Schwartz, Mathew. "Networks use 'honeypots' to catch an online thief." Computerworld. April 2001.
http://www.cnn.com/2001/TECH/internet/04/04/trap.a.thief.idg/

Sans Institute. "Honeypots: Tracking Hackers." April 2002.
http://www.sans.org/SANS2002/honeypot.php

23 Novell. "Organizational Unit (OU)."
http://www.novell.com/documentation/lg/nds73/index.html?basicenu/data/h0000024.html

Novell. "Organizational Unit (OU)." More.
http://www.novell.com/documentation/lg/nw5/docui/index.html#../usnds/basicenu/data/h0000024.html

24 Free Firewalls
Anomaly, Inc. "Windows Free Firewall Software for download." 2001.
http://www.free-firewall.org/

Anomaly, Inc. "Download Free Personal Firewall Software" 2001.
http://www.homenethelp.com/web/howto/free-firewall.asp

LintLinks2000. "Three Angles Freeware: Firewall:" 2002.
http://www.lightlinks2000.com/Firewall.htm

25 SSL Certificates
SSL.
http://www.ssl.com/

Verisign.
http://www.verisign.com/

SecureLook.
http://securelook.com/

GlobalSign.
http://www.globalsign.net/

Media3 Technologies.
http://www.media3.net/ecommerce/sslcert.htm

26. Novell. “Hidden Object Locator.” TID 2922091. Jun 2000.
http://support.novell.com/cgi-bin/search/searchtid.cgi?/2922091.htm

Last Updated: September 22nd, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
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
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
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
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 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 Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive