Global Information Assurance Certification Paper

Effective vulnerability/patch management in the large corporations

Fabrice Besson
July 9, 2002
GSEC 1.3

Abstract

The purpose of this paper is to highlight the real challenge and issues to manage a new security hole and its potential workaround/patch for the large companies. Particular emphasis will be put on to understanding the patch management framework. This whitepaper will also try to present the architecture and products to manage this.

Introduction

Bruce Schneier from Counterpane wrote "*The press regularly writes the story like this: First, vulnerability discovered and we're all in danger. Then, vulnerability patched and we're all safe again. What they forget is that patches don't work unless they're patched. And more and more often people don't install patches. I predict that years from now, Web sites will still be broken into because of this vulnerability*". [1]

Hackers say: "*if you want to protect your assets against attack, first patch your systems*". A large percentage of intrusions and defacements may be caused by a failure of the organizations to identify and deploy vendor software patches in a timely manner. The patch management with the host-hardening step is really a key activity to prevent intrusions in a proactive security model. With the apparition of the famous CodeRed, the market has been tremendously increasing the product list that handles the vulnerability assessment, patch management and/or deployment for a year. Even if some products such as Nessus or ISS Internet scanner had been released prior to the birth of this famous worm, the increasing number of vulnerabilities re-enforces the basic questions for each Security professional:

Which systems are vulnerable to this new security hole?
Is the appropriate patch installed on these systems?

The patch/vulnerability management is not only a matter of products and resources; it is above all a complex process. Even this process was triggered by a new security bulletin coming from one of the major security information providers, there are numerous ways to deal with it and the complexity remain proportional to the size of the enterprise.

1. What is the vulnerability management?

Managing vulnerabilities and patches requires a high degree of security awareness from all the people involved in this activity, from the Security professionals to the system engineers including the Business Account managers and the customer. The main

complexity remains in the process itself, we will see that a lot of products can help and ease the decision cycle, the deployment; but none of them covers all activities. In a large Corporation the security processes are deeply correlated and linked to the IT model.

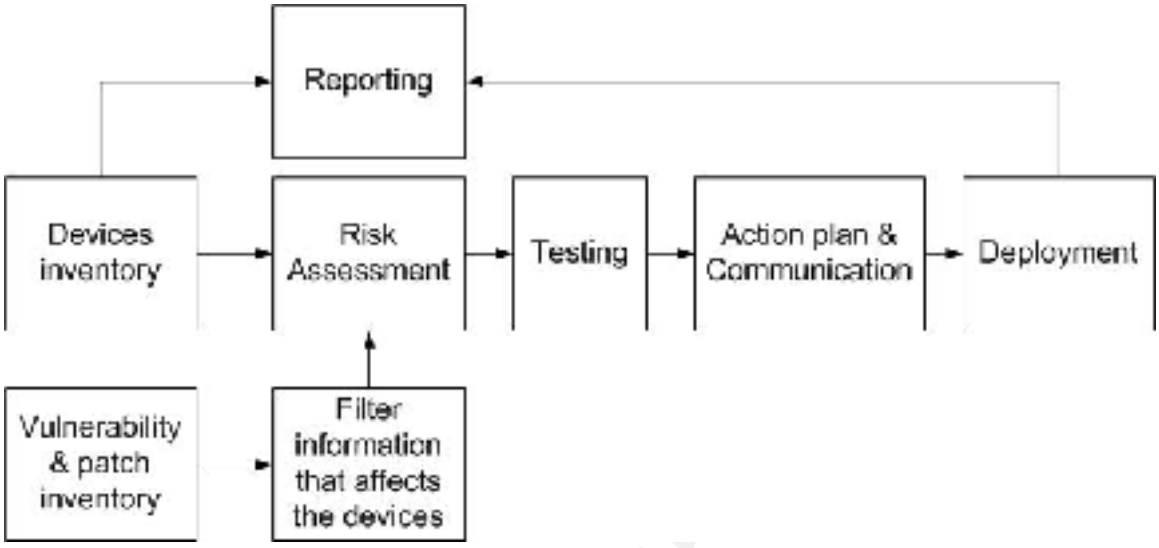

Figure1: Vulnerability management scheme

2. INVENTORY STEP

2.1. Security data:

Large corporations need a strong ongoing process to monitor the web sites and the mailing lists of the security information providers as well as the software providers. It is not difficult to find security advisories through your favorite search engine but it's harder to find data structured in a timely manner. Keep in mind that in the security warfare, Time is a key differentiator. The sooner you are informed, the faster you re-act.

Regardless of the number of resources, managing the security information is in itself a major difficulty for a large organization. Such activity is a full time job for a dedicated team. These professionals should be recognized as the Authoritative Knowledge source for all employees. It is still an issue to avoid massive mailing from employees who want to increase the global security awareness, but overflow and hide critical information.

Various channels are available to remain up to date informed, from the mailing list (free or not) to the support subscription. The fee-based services often offer a better level of structure, customization, filtering and response time.

Source information providers (non exhaustive list):

Reference	Free/Fee	Main Activity	Data access
SecurityFocus www.securityfocus.com	Both	Managed Security Services Provider (MSSP)	ML/WWW/DB (*)
SecurityTeam www.securiteam.com	Free	Consulting	ML/WWW
CERT www.cert.org	Free	Training	ML/WWW
Vigilin'x www.vigilinx.com	Free	MSSP	ML
ICAT Metabase icat.nist.gov	Free	Government	WWW
Neohapsis http://www.neohapsis.com/	Free	Consulting	WWW
SecurityTracker www.securitytracker.com	Both	Information reseller	ML/WWW
SecuritySearch www.securitysearch.net	Both	Information reseller	ML/WWW/DB

(*)
ML: Daily or weekly Mailing list
WWW: Web interface to query the vulnerabilities database.
DB: Direct database access

2.2. Devices inventory:

Another important aspect is the detailed inventory of the systems. Far from the security management, it is critical to understand which type of platform IT is managing. Remember, "You can only manage what you can measure".

If vulnerability appears, the security professionals need to know as quickly as possible which platform is potentially vulnerable. According to the architecture chosen, the inventory granularity can be very different.

A few samples of what could be necessary to consider

Hardware Information:

- Mother card reference
- CPU type
- Network card reference
- Disk space metrics
- Other HW card reference
- Firmware version

Software information:

- O/S version
- Service Pack version
- Product version
- Patch list

Beyond this bulk inventory, it is necessary to introduce some classification concepts based on technical or business criteria:

- Platform type (Windows, Unix)
- Potential Risk (internet facing, legacy, Business critical)
- Service level (Premium, Standard)
- Business

Basically, the role of the configuration database is to store all this information. Even for a small Company, building and managing a good inventory is still a problem, but imagining thousands and thousands of systems would be a nightmare.

What is the expectation of a large company?

- Information should be stored and managed CENTRALLY.
- Device information should be gathered on a REGULAR basis (daily if possible).
- Information should be collected AUTOMATICALLY.
- Information should be CONSISTENT throughout the platform.

Obviously the market has understood this problem and offers a myriad of products often based on an agent concept. A small piece of code is installed on each system you want to monitor. On a regular basis, the agent sends a picture of the system to a central

repository, which aggregates all the data. The central server retrieves the data from each client. Even if the method is similar from a product to another, the price per host can vary a lot. That's definitely another parameter to consider!

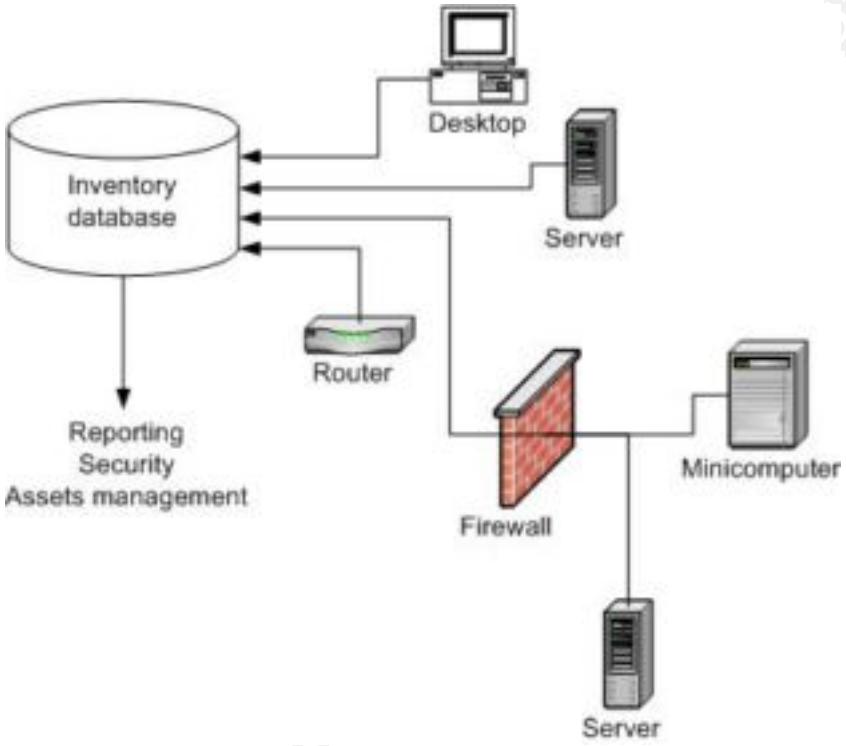

Figure2: Inventory database architecture

Some Configuration Management solutions (non exhaustive list):

Focus on Server level:

Marimba: www.marimba.com

HP OpenView: http://www.openview.hp.com/

Tivoli inventory: www.tivoli.com

Focus on Desktop level:

LANAuditor: www.landitor.com

IT VantagePoint: http://www.mwired.com/

PC-Duo Enterprise: inventory management: http://www.vector-networks.com/

Focus on Network level:

Nortel Network inventory management application: http://www.nortelnetworks.com/

Visionael network inventory: www.visionael.com

Network Management System: http://www.cisco.com/

3. VULNERABILITY ASSESSMENT

This topic is articulated around two types of models. This paragraph will detail these approaches and list existing products available on the market. For convenience, we will name these models External Probing and Internal Probing.[12]

3.1. External probing

This architecture is based on the vulnerability scanning technology. The main function of a vulnerability scanner (VC) is to probe hosts located on a network and report potential exposure according to a collection of 'well-known' vulnerabilities. The process is pretty similar to a black box testing. The security professional should evaluate a component but does not have the internal and/or external architectures specifications. Understand how a system is vulnerable allows him/her to determine the level of patch it is necessary to install.

Criteria and questions to choose a VC:

Criteria	Questions
Automatic feature to update the signature database	- How to update the database with the latest vulnerabilities? - Is the update process compatible with the corporate network security policy?
Scan host and network vulnerability	- Does the same product allow to probe system and network devices?
Product vendor viability/reactivity	Should I trust this vendor? (Technical, financial and partnership aspects).
Command-line automation	- Can I run this product in a batch mode to preserve network during the business hours?
Open standard reporting	- Is there any pre-defined template to report the scan result? - How to automatically export the data to another system such as a database? - Is there any programmatic gateway to

	exchange the data between heterogeneous application?
Consistency with CVE references	- What is the consistency with CVE referral ?
Capacity management/ performance	- Is it possible to run multiple scan in parallel?
SDK/Language	Is it possible to develop custom check for a new vulnerability?
Open Source	What is the strategy of the software provider in term of source code licencing?
Product portfolio	- Am I using a product that is not covered by this scanner? - What is the risk of not evaluating the security level? - Can I do it in another way?
Costing model	- What is the ratio: price per host or network devices?
Result accuracy	- What is the rate of false positives? False positives imply lost time for the security professional and solution discredit.

Some references of the market extracted from an internal evaluation and interesting reading (non exhaustive list). [2][3]

Nessus Security Scanner 1.1.12:

Open Source project built on a client/server model. The master is only available on *nix platform. The product/vulnerability coverage is quite exhaustive with accurate results (few false positives). A scripting language called NASL (Nessus Attack Scripting Language) is available to develop specific check. The reporting feature supports a lot of different formats including XML for automatic processing like database integration.

Internet Security Systems – Internet scanner 6.2.1:

This product is part of ISS Vulnerability scanner Suite (Internet, Database, Firewall, Network). It comes with a useful set of pre-defined policies. GUI is rather intuitive especially the policy editor. Moreover, a lot of templates for the reporting are available. One important drawback is that it is not convenient to integrate and manage the scan result in the global security infrastructure if you do not work with ISS RealSecure

solution for the monitoring. The results are not always accurate as you could expect from this type of product. The false positives are numerous (for instance, *nix vulnerabilities on NT platform). Nevertheless, the support is reactive to provide the signature of the latest vulnerabilities for the common products.

Network Associates – CyberCop scanner 5.5(*):

This is a very complete product in term of features (GUI, Reporting, Auto update, Scripting language). The false positive treatment is accurate but the drawback is that some "well-known" vulnerabilities are not reported. [2].

(*) Product not tested

NetIQ – Security Analyzer 4.0:

NetIQ is very similar to the ISS scanner with a reporting feature based on WebTrends engine. There is no convenient gateway available to export the result if NetIQ portal is not used. The product provides a SDK for custom development. The coverage is very good for M$ platform but poor for *nix (No support for IBM, HP products and Apache Web Server).

Let's summarize what the vulnerability scanning technology brings to the patch/vulnerability management

ADVANTAGE

- Cross platform: Most of the VC is able to probe several types of platforms, operating systems and products.
- Deployment: Easy to implement even for distributed vulnerability scanner.
- Scalability: Easy to adapt the architecture when the infrastructure evolves.

DISADVANTAGE

- Reactive:

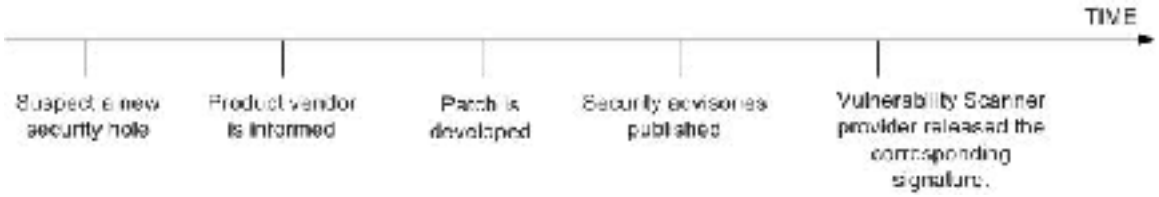

Figure 3: scenario for a new vulnerability
(For clarity purpose, the figure shows regular intervals between events, but it does not mean equal period in the reality)

In a general case, the VC vendors are informed or react after the major product vendor, which implies that the patch is often available before the attack signature. From a pure security standpoint, it is better to invest time to patch a system than wait for the new signature.

- Products portfolio: In a large corporate, the inventory of supported or installed products is huge and no scanner cover the entire portfolio.
- Dynamic approach: As it is an external probing, the VC can only check what is running in term of services, daemons.
- False positive management and result accuracy
- Testing vulnerability may cause damage, and thus cannot be executed on live equipment.

Best Practices: Try to deploy at least two different products to mitigate part of the disadvantage listed above.

3.2. Internal probing

This architecture is built on a configuration checker approach. The strategy is not to probe the host and evaluate the vulnerability exposure but to evaluate the discrepancies between the real inventory of a system and an ideal picture. In fact, if a new vulnerability is published and a patch is available, it will be possible to evaluate which system needs to be patched assuming that a detailed configuration inventory is available and up-to-date. Within this approach, two architectures are mainly implemented:

Distributed - Each platform runs a local program which:

- Retrieves the reference list of patch from an Authoritative repository.
- Makes an inventory of the patch/program installed on the platform
- Compares both sources via a dedicated algorithm
- Reports discrepancies between the real and the ideal pictures.

Central - A central server polls each platform:

- Fetch patch/product information throughout the network.
- Compares with ideal current picture
- Reports discrepancies
- The reference update is done separately

Optional: help the patch deployment:

- Retrieving missing data
- Deployment
- Installation (schedule or live)
- Reporting installation phase

The term ‘patch’ includes a procedure, workaround, code, new product release or service pack to fix vulnerability.

The major software or O/S providers like HP, IBM, Microsoft and SUN dominates this market but none of them provides cross products coverage as the VC does. The security professionals have to deal with different and incompatible products to manage the entire portfolio.[13]

Some references sorted by software vendor.

MICROSOFT

SHAVLIK Technologies – HFNETCHK

(http://www.shavlik.com/security/prod_hf.asp)

”*HFNETCHK* is a command-line tool that enables an administrator to check the patch status of all the machines in a network from a central location. The tool does this by referring to an XML database that's constantly updated by Microsoft. HFNetChk can be run on Windows NT 4.0 or Windows 2000 systems, and will scan either the local system or remote ones for patches available for the following products: Windows NT 4.0, Windows 2000, All system services, including Internet Information Server 4.0 and 5.0, SQL Server 7.0 and 2000 (including Microsoft Data Engine), Internet Explorer 5.01 and later “[5]

Based on this engine, various products have been developed with additional reporting, GUI, centralized storage features. This tool does not cover the entire MS catalogue but it is free.

SUN: Solaris

IST – *CheckPatches* & *GetApplyPatch* (http://ist.uwaterloo.ca/security/howto/2000-12-04/)

CheckPatches script downloads the patch reference on an anonymous SUNSOLVE FTP site, compares with existing installed base and reports the missing patches listed by category: Security, Recommended, Y2k.

GetApplyPatch script assists the system administrator to retrieve and install SUN patches.

SUNSOLVE (http://patchpro.sun.com/)

- PatchManager Base 1.0 for Solaris 2.6 through Solaris 8 (based on *smpatch* command)

- Patch PRO 2.1 for Solaris 9 with *smpatch*

”The system command analyzes patch requirements and downloads signed or non-signed patches on the local system only. Apply one or more signed patches in JAR format, which also authenticates the patch or patches to be added. Remove one or more patches, which checks patch dependencies before removing the patch or patches.” [6]

IBM: AIX.[7]

For AIX 4.x & Aix 3.x

Fixdist is a user interface tool designed to enable customers to select and download the missing fixes.

HP: HP-UX.[8]

For HP-UX 11.x

security_patch_check is equivalent to SUNSOLVE or IBM scripts to evaluate the gap between the inventory of a lambda system and the reference.

However, it requires installation of the PERL scripting language, HP-UX 10.x is not supported. Moreover, the script does not allow to retrieve the necessary fixes for the implementation.

Linux

RPM model

RedHat Network provides an enterprise network service to manage all fixes released by RedHat. Static reports are available per release but it is also possible to register each system in this portal. RedHat Network retrieves the configuration of these systems and reports the gap analysis for security, bug fixes and enhancements. This portal is based on the ‘Errata’ section of the RedHat web site. [9]

AutoRPM. [10]

“*AutoRPM* is a Perl program that automates RPM installation. It is designed to be run from cron nightly and to run interactively. By default, every night, it will check for official Red Hat updates for your system. However, you can modify the configuration file to do much more, i.e. automatically install the same RPMs on a cluster of machines.”[7]

AutoRPM is not exactly a product to manage the security fixes but rather a RPM manager. After the comparison step, the report does not make the difference between a security fix and an enhancement.

APT model. [11]

As for the RPM distribution model, only '*apt-get update*' command allows to evaluate this gap using the 'sources.list' entries. However distinction between security and bugs fixes is not explicit for an automate process.

Configuration checker solution debriefing:

ADVANTAGE

- Speed to react/proactive: The software vendors are often more reactive than the vulnerability scanner provider.
- False positive/Result accuracy: As the process is based on a simple comparison between two system status (pattern matching), the result is more accurate than the external probing approach, especially for the false positive aspect.
- Static approach: In most cases, these applications are based on what is installed on the platform and not on what is running. Patching a product if it is not running is a definitely proactive approach. Moreover, it avoids security problems if someone runs the application by mistake.

DISADVANTAGE

- Many products to check various configurations: For large corporations, which manage heterogeneous systems, the security professionals should be able to deal with many different products.
- Difficult to implement: Increasing the number of products to assess the hosts, increases the deployment complexity.

Other considerations:

In a managed services context, the IT delivery not only provides to the business the monitoring and operations activities, but also security advice and information. However in particular corporation model, the business remains the decision maker for patch deployment and s/he can refuse this implementation for various reasons.

Dealing with large corporations often means working with different languages. The impact of the localization aspect for software/patch is not minor when talking about thousands and thousands of systems.

IT complexity could be also another issue. Large corporations have a lot of difficulties to centralize their system management activities. The side effects are numerous to implement a vulnerability management strategy.

4. Conclusions

Although there are several good products for the patch management or the vulnerability assessment, none of them covers the entire portfolio of a large corporation. As it is often the case, the ideal solution is a mix between various tools and technologies and the

technical challenge remains in the aggregation of this information to build a consistent patch management framework.

References

[1]: Bruce Schneier. "Crypto-Gram". Counterpane Security, Inc , May 15,2001.

URL: http://www.counterpane.com/crypto-gram-0105.html#5

[2] Jeff Forristal and Greg Shipley. "Vulnerability Assessment Scanners". NetworkComputing . January 8,2001

URL: http://www.networkcomputing.com/1201/1201f1b2.html

[3] VA Test Group," Vulnerability Assessment second edition". NSS Group. December 2001

URL: http://www.nss.co.uk/va/va_edition_2.htm#Table

[5] Microsoft. «Microsoft Network Security Hotfix Checker"

URL: http://support.microsoft.com/default.aspx?scid=kb;EN-US;q303215#1

[6] On line documentation/references

URL : http://patchpro.sun.com/servlet/com.sun.patchpro.servlet.PatchProServlet

[7] IBM *FixDist* man page

URL: http://www-1.ibm.com/support/manager.wss?rs=0&rt=0&org=aix&doc=BD402C9D0B48245B852568160069FFC3

[8] HP Security product catalog

URL:http://www.software.hp.com/cgi-bin/swdepot_parser.cgi/cgi/displayProductInfo.pl?productNumber=B6834AA

[9] RedHat network services

URL: https://rhn.redhat.com

[10] AutoRPM Man page

URL : http://www.autorpm.org/

[11] Debian security model

URL: http://www.debian.org/security

[12] Richard Steinberger . “Proactive vs. Reactive Security”. Vigilante.

URL: http://www.vigilante.com/inetsecurity/commentary/proactive_vs_reactive.htm

[13] John Fontana. **“**New tools available for managing patches“

URL: http://www.nwfusion.com/news/2002/132904_05-27-2002.html

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event