Global Information Assurance Certification Paper

Assessing And Exploiting The Internal Security Of An Organisation
Tony Stephanou
13 March 2001

Introduction

> *"It is easy to run a secure computer system. You merely have to disconnect all dial-up connections and permit only direct-wired terminals, put the machines and its terminals in a shielded room, and post a guard at the door."*
>
> *-F.T. Grampp and R.H. Morris*

The purpose of this paper is to provide a guideline on how to go about performing an internal penetration exercise. First, internal threats facing an organisation will be introduced. Thereafter, a simple and practical "how to" guide for assessing the internal security posture of an organisation will be presented.

Threats ? What Threats ?

The Computer Security Institute (CSI), announcing the results of its sixth annual "2001 Computer Crime and Security Survey" found that 85% of respondents detected computer security breaches within the last twelve months. This includes attacks from the Internet and from within an organisation's network perimeter. The respondents (which consisted mainly of large organisations, government agencies and other institutions) reported that their most serious financial loss occurred due to theft of proprietary information (34 respondents reported a loss of $151,230,100).

The threat of insiders to computer security and the subsequent financial losses cannot be underestimated. A study by the FBI and the Computer Security Institute on Cybercrime, released in 2000 found that disgruntled employees (or insiders) are a major source of computer security breaches. The survey released in 2000 found that 71% of security breaches were carried out by insiders. The FBI expects this trend to continue and for threats to become more serious.
This is supported by the realisation that persons with high technical skill and organisational process knowledge for example, employees or contractors, pose the greatest threat to an organisation. This coupled with inadequate internal network level controls within an organisation, means that persons with access to an internal network point could potentially disrupt or corrupt vital services as well as gain access to confidential information.

A study by the CSI and FBI released in 1999 shows that among the types of security breaches reported by organisations, unauthorised access by employees presents the largest impact to an organisation in terms of financial losses (see Figure 1 below).

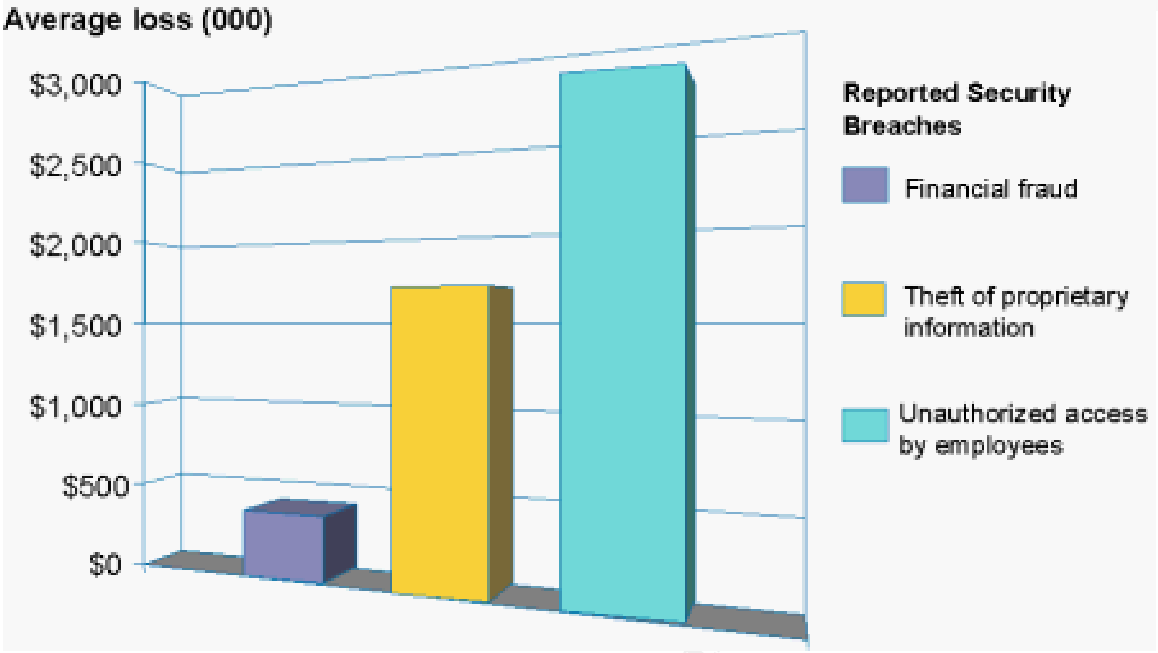

Figure 1: The cost of Security breaches (Source: 1998 CSI/FBI Computer Crime and Security Survey)

A security survey by KES/Utimaco found that the threats facing an organisation are not only due to sinister motives but can also be as a result of human negligence (see Figure 2):

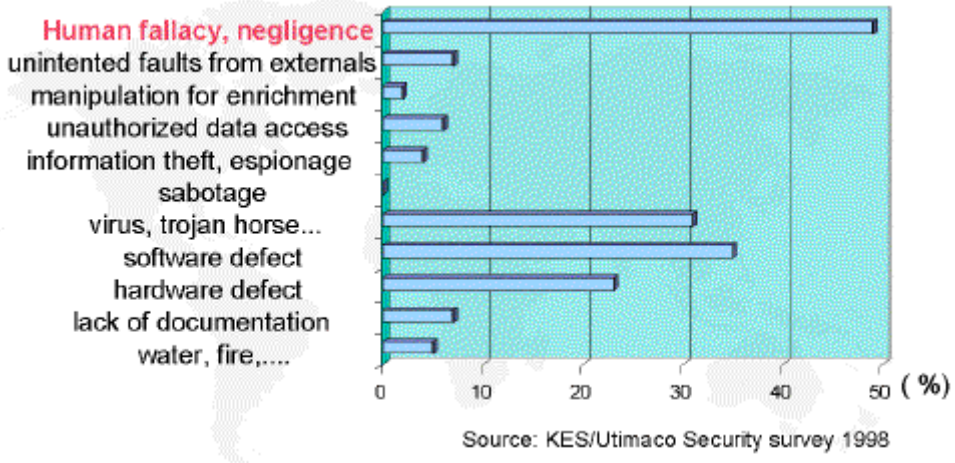

Figure 2: Security Threats to organisations.

From the CSI press release, "Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar", Patrice Rapalus, the CSI Director provides some insight: "Organizations that want to survive in the coming years need to develop a comprehensive approach to information security, embracing both the human and technical dimensions".

Internal Penetration Testing

In recent years, organisations have been testing their network security by simulating hacker-like attacks. This is known as penetration testing. Organisations could either use automated network vulnerability analysis tools themselves or contract third-party information security consultants to carry out such testing. Internal Penetration testing requires the analyst to have physical access to the target organisation's network, as opposed to external penetration testing which is carried out from the Internet. Internal Penetration testing is used to demonstrate how a potential intruder or unauthorised employee could gain unauthorised access. Once, vulnerabilities are found on a network, the analyst performing the test will try to exploit these vulnerabilities. Thus, the purpose of a penetration exercise is to determine and organise the technical vulnerabilities found on a target organisation's network and to try and exploit them.

It is important to make a distinction between Penetration testing and Network security assessments. As mentioned above, Penetration testing includes an attempt to exploit discovered vulnerabilities, whereas Network security assessments using commercially available tools may be useful to a degree, but do not always reflect the extent to which hackers will go to exploit a vulnerability.
The issue of what type of business impact and exposure the vulnerabilities found will have on the organisation is not covered by an internal penetration test.

The are a number of reasons why organisations would want to carry out an internal penetration test. Firstly, a large organisation may want to take stock of how many vulnerable systems are present in their organisation thereby measuring trends in their network security position.
Others may want to provide assurance to their customers or business partners that their sensitive information is secure. Finally, other organisations may use the results of penetration testing to persuade management to invest more in information security technology.

Before carrying out any testing, it is always important for the analyst to obtain written permission from the systems administrator of the organisation to be tested. Due to the possibility of sensitive information being exposed, the systems administrator may require the analyst to sign an NDA.

There are a wide variety of tools that one could use for internal penetration testing. These tools typically map out a network environment and the services available on the network. The services found on the network are then compared to a vulnerability database and the tool will report on vulnerabilities found. The two most common commercial tools used

for penetration testing are ISS Scanner (produced by produced by Internet Security Systems) and Cybercop (produced by produced by Network Associates). The tools that will be used in this paper are:

- Cerberus Internet Scanner (CIS) written and maintained by Cerberus Information Security, Ltd.
- nmap (by Fyodor)
- Nessus (by Renaud Deraison)
- L0phtcrack by L0pht Heavy industries, Inc.
- Sqldict (by Arne Vidstrom)
- DumpAcl (by SomarSoft Utilities)

The process described below is meant to be a guideline for those wanting to conduct an Internal Penetration test. It is difficult to describe an Internal Penetration exercise in a step-by-step manner because penetration testing may lead the analyst down many different paths. In addition, what is tested and how it is tested or exploited depends on the scope of the testing, the size of the organisation, the type of networks and operating systems being tested, the type of services and vulnerabilities found, the type of tools at your disposal and so on.
For this paper, it is assumed that the test will be conducted on an IP-based, Windows NT domain environment.

For our purposes, Internal Penetration testing can be broken down into four broad phases:

- Footprinting: Activities within this phase include determining the subnets and specific hosts within the organisation that will be targeted. Are you going to footprint an entire organisation or are you going to limit your activities to certain hosts? The analyst may want to discuss the IP ranges that will be targeted with the systems administrator.
- Host Enumeration: Once the range of hosts have been identified it will be necessary to enumerate hosts that are live and listening on the network.
- Network Scanning: This phase will determine the specific services that are available on the hosts identified in the previous phase.
- Vulnerability assessment and exploitation: This phase includes running (automated) vulnerability/exploitation tools against selected hosts in order to identify possible vulnerabilities that may be exploitable.

Footprinting

Firstly, the analyst should try and get a network diagram and a list of machine names or IP addresses to test from the systems administrator. This will help to determine the scope of the testing and the time it will take to complete all the scanning. The systems administrator will be able to assist with identifying which are the critical business applications. He or she may also want the analyst to keep away from certain machines. It is important to sit down with the systems administrator and explain to him or her exactly what is going to be tested and the possible consequences. The analyst should try

and estimate how long the testing will take, given the information at hand. If critical business applications will be involved in the testing then some systems administrators may prefer to conduct the testing after hours or when the systems are less busy.
Simple preparation beforehand will ensure that the systems administrator is prepared in the event of something going wrong, like critical applications or hardware failing. It is also a good idea to have the systems administrator or an elected representative, present when performing the testing in case something goes wrong or if you need to query an IP address, the purpose of a machine and so on.

- Host Enumeration

Before running **any** tools it is vital that you understand exactly what you are doing, i.e. understand how to use the tool fully and understand the implications of running such a tool against a specific system. For example, some tools have denial-of-service exploits built into them.
First, you should ensure that your computer is connected to the network and that a valid IP address and default gateway is configured. Pinging the default gateway will determine whether there you have a network connection. It is best to start the test without any domain access. This way you can see how far you can penetrate the hosts on the network with limited privileges. If you need to a run tool against a specific system that requires administrator privileges you can always ask the systems administrator for that. Once you have obtained an IP range to test from the systems administrator it is time to check which hosts are up. One way of doing this is to use nmap to perform an ICMP ping-sweep to identify live accessible hosts in the network range:

```
$ nmap -sP -v -oN nmap-ping.txt 192.168.7.1-48
```

nmap, is a popular UNIX-based portscanner, which is very useful for scanning large networks. nmap supports scanning multiple protocols such as UDP, TCP and ICMP. It also supports a very large number of scanning techniques such as TCP connect, TCP FIN, TCP SYN and so on. Some other features include detecting remote operating systems and decoy scanning, to name but a few.
The nmap command above will perform a ping-sweep on the IP range 192.168.7.1-48 and place the results of all live hosts in the range in a file called nmap-ping.txt. This file will act as your target list and so you now have a list of hosts that you can probe.

- Network Scanning

The contents from the nmap-ping.txt file above may look something like this:

```
.
Host  (192.168.7.2) appears to be up.
Host  (192.168.7.10) appears to be up.
Host  (192.168.7.11) appears to be up
.
.

# Nmap run completed at . . .
```

In order to use the contents of this file effectively we will need to edit it so that just a list of IP addresses remains and nothing else. One way of doing this is to edit this file manually, however this can may be quite time consuming if there are large number of IP addresses. Another way is to write a short Perl script to cut out all the unwanted text. The edited file should then be saved under a different name, for example, targets.txt.

We can now use the use the results in the target.txt file with nmap to perform a comprehensive port scan on the systems we know are up:

```
$ nmap -sT -vv –p 1-65535 –oN nmap-tcp.txt -iL targets.txt
```

This command will run a TCP port scan on all 65535 ports on all machines identified in the targets.txt file. The output of the scan will be written to a file called nmap-tcp.txt. This scan is extensive and thus may be very time consuming if there are a large amount of hosts to scan. Depending on the circumstances, you may want to reduce the number of ports to be scanned. You may also want to run a UDP port scan to probe any UDP ports that are open. The contents of the output file should look something like this:

```
.
.
Interesting ports on 192.168.7.10:
(The 1055 ports scanned but not shown below are in state:
closed)
Port       State       Service
80/tcp     open        http
135/tcp    open        loc-srv
139/tcp    open        netbios-ssn
1433/tcp   open        ms-sql-s
```

The purpose of the port scan is to identify what services the target hosts are offering. Once this is established you can decide which hosts should be tested for vulnerabilities.

- Vulnerability assessment and exploitation

The steps that will be carried out in this phase will depend to a large degree on what the results of the previous port scan were. Based on the results of this port scan the analyst will now need to determine whether any of the services that were found open are vulnerable to any exploits. Also, the analyst needs to determine which hosts should be tested for vulnerabilities. Once vulnerabilities have been found the analyst should attempt to exploit these vulnerabilities. Ultimately, the analyst should attempt to gain administrative access to the target hosts.
One tool that can be used for such an activity is Nessus. Nessus is a free security scanner that will test a network for known vulnerabilities. Nessus consists of a client and a server portion. The server portion performs the scanning, while the client acts as the front-end. It consists of a "plug-in architecture", which allows separate security tests to be written

and added as external plug-ins. According to the author of Nessus, Renaud Deraison, Nessus not only checks for vulnerabilities but also attempts to exploit them. Nessus provides exportable reports in a number of formats, including ASCII text and HTML (with pies and graphs).

It is easy to run Nessus just point it at the target list and start the scan. Before running Nessus though, the analyst should ensure that all dangerous plug-ins are disabled (denial-of-service attacks). The Nessus report gives a description of the vulnerability and a rating of the severity of the vulnerability. The reports usually provide a link to other web sites where more information can be obtained about the vulnerability and how to go about exploiting it. With a little research on the Internet and some luck the analyst may be able to exploit the vulnerability and gain access to the target host. It mostly depends on the type of vulnerability found.

Another vulnerability scanner that can be used is CIS. This is a free scanner, run on Windows NT and 2000 platforms that performs around 300 checks. CIS is designed in a modular fashion. All checks are divided up into modules, which are implemented as separate DLL's. CIS vulnerability tests include : WWW tests, SQL tests, FTP tests, various NT tests, SMTP tests, POP3 tests, DNS tests, Finger tests and others.
CIS reports are generated as HTML pages and include links to more information about vulnerabilities found.

The analyst may want to run CIS against those hosts that have http (port 80) and NetBIOS session service (port 139) open. With NetBIOS checks, CIS attempts to establish a NULL session with the target host. If successful CIS enumerates the following information:

- Accounts name
- Account type
- File Shares
- Last password change
- Logon Count
- Account Status

The information gathered here might be dangerous as it could allow an intruder or unauthorised employee to begin to plan an attack. Note, this information can be obtained without having any domain access.
Another handy NetBIOS check performed by CIS is a simple password check. It checks whether passwords on the target host are equal to the account name, or whether they are blank. This is probably the easiest way to gain (administrative) access to the target host.

A recently discovered vulnerability is the "Extended UNICODE Directory Traversal Vulnerability". This vulnerability affects Microsoft IIS 4.0 and 5.0 web servers. This is a serious vulnerability. If exploited successfully it could allow a user to execute commands on the affected target and upload programs to the target and execute them. Commands executed by the user would be processed under the IUSR_machinename account.

Microsoft Security Bulletin (MS00-078) gives the following description of the vulnerability:

> Due to a canonicalization error in IIS 4.0 and 5.0, a particular type of malformed URL could be used to access files and folders that lie anywhere on the logical drive that contains the web folders. This would potentially enable a malicious user who visited the web site to gain additional privileges on the machine – specifically, it could be used to gain privileges commensurate with those of a locally logged-on user. Gaining these permissions would enable the malicious user to add, change or delete data, run code already on the server, or upload new code to the server and run it.

See: http://www.microsoft.com/technet/Security/Bulletin/ms00-078.asp

The analyst should test whether all hosts with the http service open (port 80) are vulnerable to the "Extended UNICODE Directory Traversal Vulnerability", and whether they are exploitable. There are a number of exploits that test this vulnerability. To find them visit: http://www.securityfocus.com.
If the analyst is successful with the exploit, he or she could copy the sam._ file of the target host from the c:\winnt\repair directory to the c:\inetpub\wwwroot directory. The analyst would then visit the target web site with their browser and request the sam._ file like so: `http://IP_address/sam._` The sam file will then be downloaded to the analyst's system. From there the analyst could use the L0phtcrack tool to crack the administrator password offline and gain administrative access to the machine. If the sam file of the organisation's domain controller is obtained then the analyst should crack all the passwords in the file in order to determine the strength of the passwords used by the domain users. Before any sam file is downloaded and cracked it is important to first ask permission from the systems administrator whether it is acceptable to do so.
Depending on the purpose of the machine, the analyst could also upload tools to the target host in order to probe or scan other hosts that are not accessible from the analyst's system.

Another way of obtaining access to a system is by using the SMB Packet capture feature shipped with L0phtCrack. L0phtCrack is an NT password cracking tool. It is easy to use and can crack password rapidly. If the target organisation is not using a switched network it may be possible to capture (sniff) domain login sessions. This passive attack would allow the analyst to crack the captured password hashes offline and eventually gain access to the target host. It is however possible to capture traffic in a switched environment by attacking the switches.

Sqldict is an SQL dictionary attack tool that allows one to test the strength of passwords used by SQL accounts. The tool supports, Windows 9X, Windows NT and Windows 2000. The tool is easy to use and allows the user to select and customise the dictionary to be used. The analyst should use this tool to test the 'SA' account of all hosts that have the sql service open (port 1433), identified in the Network Scanning phase.

Finally, DumpAcl should be run against selected hosts (such as domain controllers) in order to obtain configuration settings. DumpAcl is a security auditing program for Windows NT. It is a useful tool that extracts a wide range of permissions and security settings including information on audit settings, file permissions, user information, share information and so on. For example, the analyst could dump the policy settings of the domain controller in order to assess the adequacy and effectiveness of the user account and password settings. These settings can be dumped remotely.

Conclusion

This paper presented some of the research that has been carried out regarding threats to an organisation's internal security. A simplified demonstration on how to go about assessing the technical vulnerability of an organisation to such threats, and some of the tools used in the process were also presented.
Internal Penetration testing is not a panacea to mitigate the threats mentioned above. It provides a snapshot of the systems at the time of testing. New vulnerabilities in products such as Internet Information Server (IIS) are continually being released and, in practice, it is almost impossible for an administrator to remain up to date on the latest security issues. A strong security process is required to manage this on an ongoing basis, and so some organisations use the services of security consultants to address some of these issues.
The core problem is that the system administrator has to close every single hole, while the attacker only needs to find a single exposure.

References

1. CSI. "Financial losses due to Internet intrusions, trade secret theft and other cyber crimes soar". 12 March 2001. URL: http://www.gocsi.com/prelea_000321.htm (14 Mar 01).
1. FBI Press Room. "Cybercrime". 21 April 2000. URL: http://www.fbi.gov/pressrm/congress/congress00/gonza042100.htm (14 Mar 01).
2. Utimaco Safeware. "Sec Risks". URL: http://www.reycon.com/utimaco/info/secrisk/secrisk.htm#_Toc478469137 (15 Mar 01)
3. The MIS corporate Defence Solutions Ltd., Network Security Team. "An overview of Network Security Analysis and Penetration Testing". 1 August 2000. URL: http://www.mis-cds.com (15 Mar 01).
4. Fyodor. "NMAP – The Network Mapper". 10 March 2001. URL: http://www.insecure.org/nmap/index.html (14 Mar 01).
5. Deraison, Renaud. "The Nessus Project: Introduction". 8 March 2001. URL: http://www.nessus.org/intro.html (14 Mar 01).

6. Cerberus Information Security, Ltd. "Cerberus Information Security, Ltd". URL: http://www.cerberus-infosec.co.uk/cis.shtml (14 Mar 01).
7. Microsoft TechNet. Microsoft Security Bulletin (MS00-078). 17 October 2000. URL: http://www.microsoft.com/technet/Security/Bulletin/ms00-078.asp (12 Mar 01).
8. SANS Institute. "L0phtCrack". SANS GIAC Level One. 2000.
9. Vidstrom, Arne. "SQLdict". URL: http://ntsecurity.nu/toolbox/sqldict/ (14 Mar 01).
10. Somarsoft. "Somarsoft Utilities". URL: http://www.somarsoft.com (15 Mar 01).

Last Updated: July 25th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
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
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
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
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
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
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
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
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
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
Community SANS Sacramento SEC401	Sacramento, CA	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