



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 permitted 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>

Security Implications of Virtual Private Networks

Tony Samsom

In order to understand Virtual Private Networks (or VPN's) better I built one using the Internet Security Protocol (or IPSec) VPN support that ships with Windows 2000. Based on the Microsoft experience, I will describe what an IPSec VPN is. I will also explore some of the security implications of using Virtual Private Networks (or VPN's).

What is a VPN?

A simple VPN is a "virtual" tunnel between two machines. All network traffic between these machines passes through this "virtual" tunnel. Because encryption is done at the Network layer, VPN support must be provided in the network stack. I used Microsoft Windows 2000 to construct an IPSec VPN. See Appendix B for an example of an IPSec VPN packet built by Windows 2000. Notice that the packet is not TCP or UDP and there is no indication what the packet may originally have started as.

Wide Area Network vendors market VPN services. With these services I have to trust the vendor to keep my data safe. The vendor may or may not use cryptographic methods to do this. This is not the VPN discussed in this paper.

Current Web browsers support encrypted conversations (HTTPS). This is not a VPN. It is application layer encryption. This kind application layer encrypted packet (SSL) is of type TCP, (with destination port 443 for HTTPS) and only the application payload is encrypted.

How is it built?

Windows 2000, Checkpoint 2000 and Cisco Routers can use the IKE protocol to construct an IPSec VPN. See references [1,2] for a detailed description of the process.

When the tunnel is first created, both machines must authenticate each other. Windows 2000 provides 3 choices of authentication method: shared secret, certificate, and Kerberos. Kerberos authentication is not useful over the Internet. I used a shared secret for my testing but certificates are the best choice to ensure the authenticity of each machine in the VPN.

After authentication the machines negotiate what encryption algorithm to use, what secret to use with the encryption algorithm, what data integrity algorithm to use, what network traffic to pass through the tunnel etc.

After successful negotiation network traffic between the machines will flow through the constructed VPN.

Why is it useful?

VPN's are typically used to provide secure communication between systems across the Internet. Company to company or branch-office to head-office secured communications are common examples. VPN technology is becoming more inexpensive and high speed

Internet access is also becoming both more prevalent and inexpensive. This contributes to VPN's becoming a cost-effective alternative to private networks and also an effective way to provide high speed network access from home to the office.

A VPN can be used to ensure the identity of the participating machines (authentication and non-repudiation). It effectively prevents data modification and session hijacking. The VPN can prevent eavesdropping if the data is encrypted. Unlike application level network encryption like SSL a VPN is not application specific. All data between machines participating in a VPN can be protected.

It is not generally possible to guarantee that a particular security technique or tool is 100% foolproof. There is no guarantee that there isn't a way to circumvent or crack an IPSec VPN. However, a lot of effort has gone into the IPSec design and most security compromises will not be a result of a direct attack on the VPN.

What are the security implications of using VPN's?

VPN's do not remove the requirement for proper security practices. When we connect company A to company B using VPN technology the systems at company B can access systems at company A. If company B has compromised systems the VPN can allow free access to company A resources. This is not a new exposure. When companies connect their networks together through a private line, most if not all of the same exposures exist. With inexpensive VPN technology however, we have the capability of building many more exposures. Microsoft Windows 2000 can be configured to talk over a VPN to some machines and to talk in the clear to others. This is a typical home office situation. Unwanted parasites like Back Orifice [6,7] can allow a hacker real-time unrestricted access to the corporate network. We can limit the possible attack points to machines participating in the VPN if all the machines only accept VPN network traffic. In practice this is not practical.

VPN's do not provide fine-grained access control mechanisms. A major VPN strength is that it can provide all the same services as the local LAN. Applications cannot usually tell if the user is VPN based or not. A VPN can be configured so that only certain networks segments are accessible or only certain protocols flow over the VPN. Network controls usually cannot restrict access to resources by user. Application proxies like the iPlanet application server can but they cannot provide access to all applications.

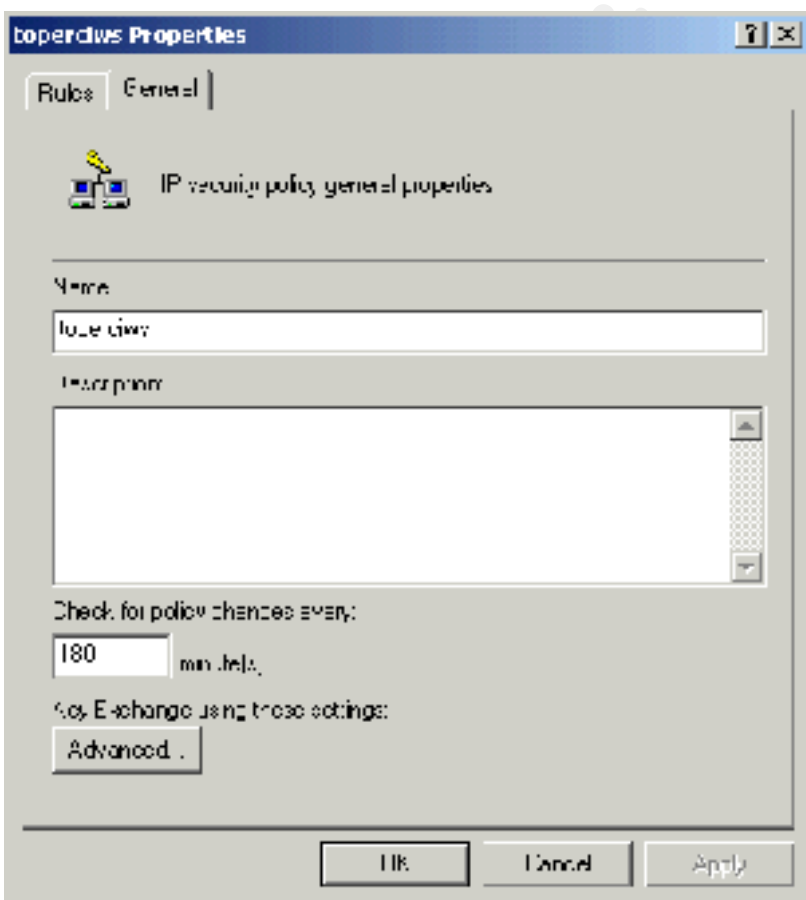
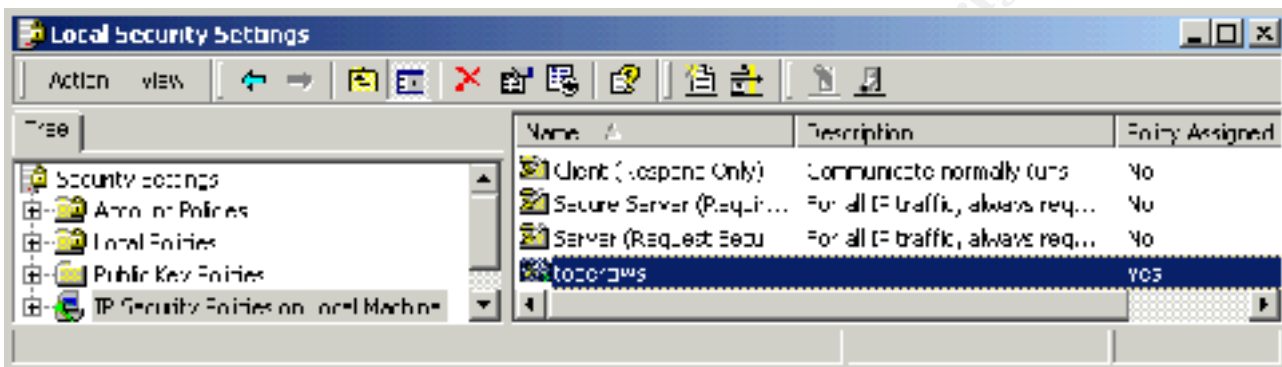
Conclusion

VPN's are an effective way to create secure communication channels across the Internet or between sensitive systems within a company's internal network. With the inclusion of VPN support in Microsoft 2000, Cisco routers, Checkpoint 2000, and a host of other systems, the deployment of VPN's is going to become more commonplace. Without proper security design, these VPN's could add many more unwanted entrances to corporate networks. Use VPN's where appropriate but ensure security issues including machine configuration, policy and user security awareness have been considered.

Appendix A: Setting up a Windows 2000 VPN

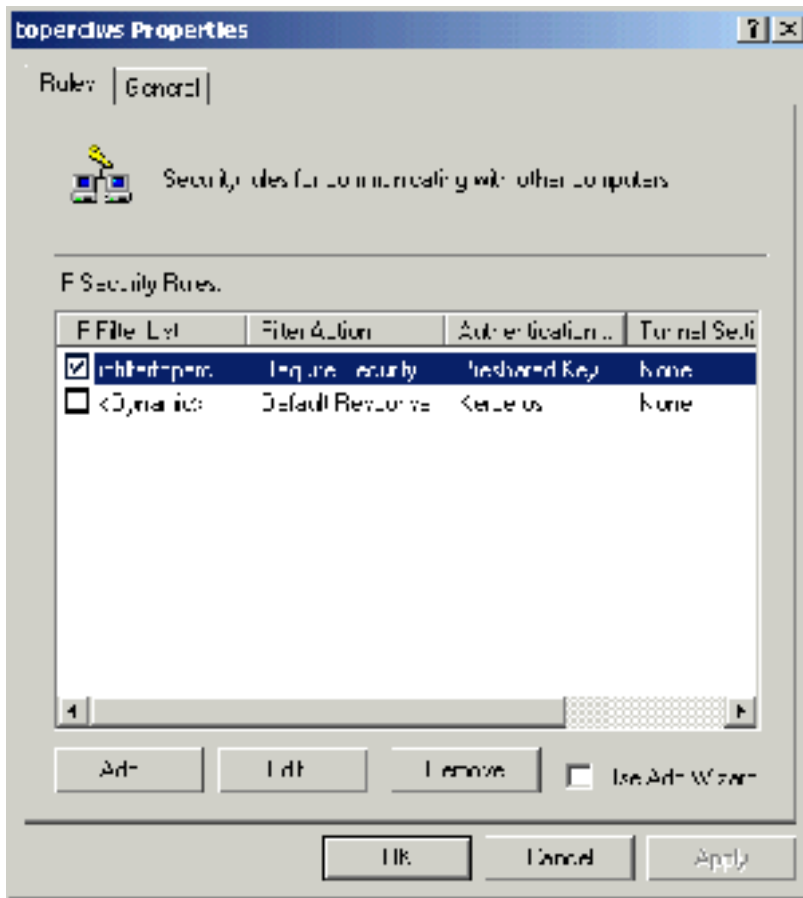
The following is a quick introduction to setting up a VPN on Windows 2000. See [5] for more detailed instructions and a description of the various Windows 2000 VPN debugging tools.

The administrative tool used on Windows 2000 to create and edit IPSec security policies can be accessed by “file -> run -> secpol.msc”.

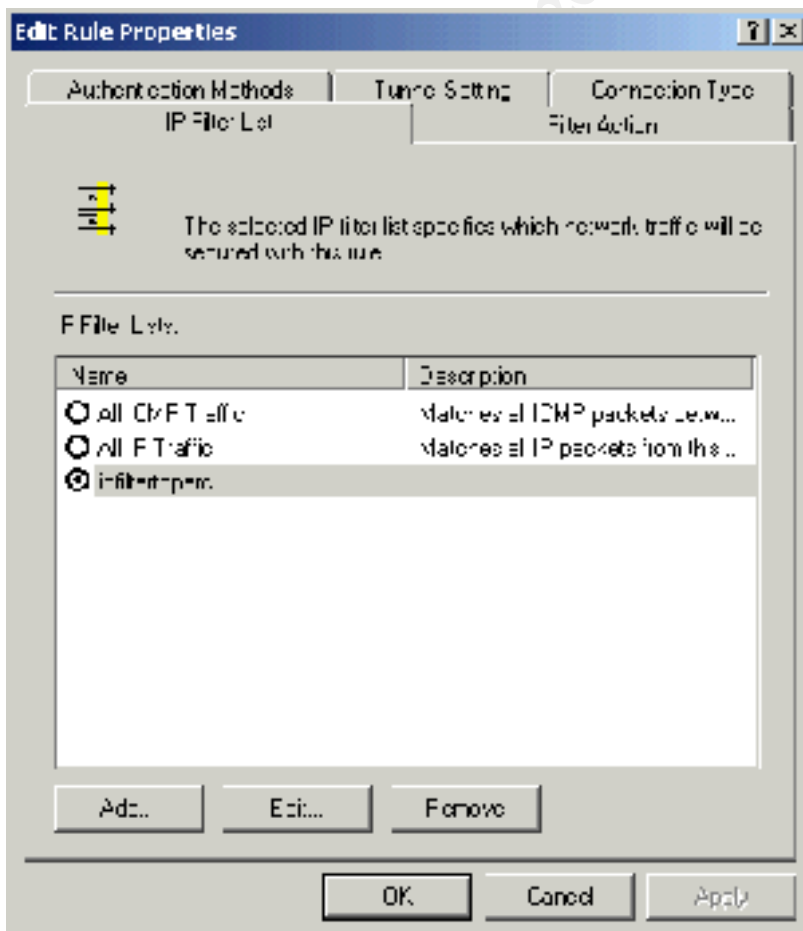


Right click on the security policy on the window above to assign and un-assign the policy. The policy is only active when assigned.

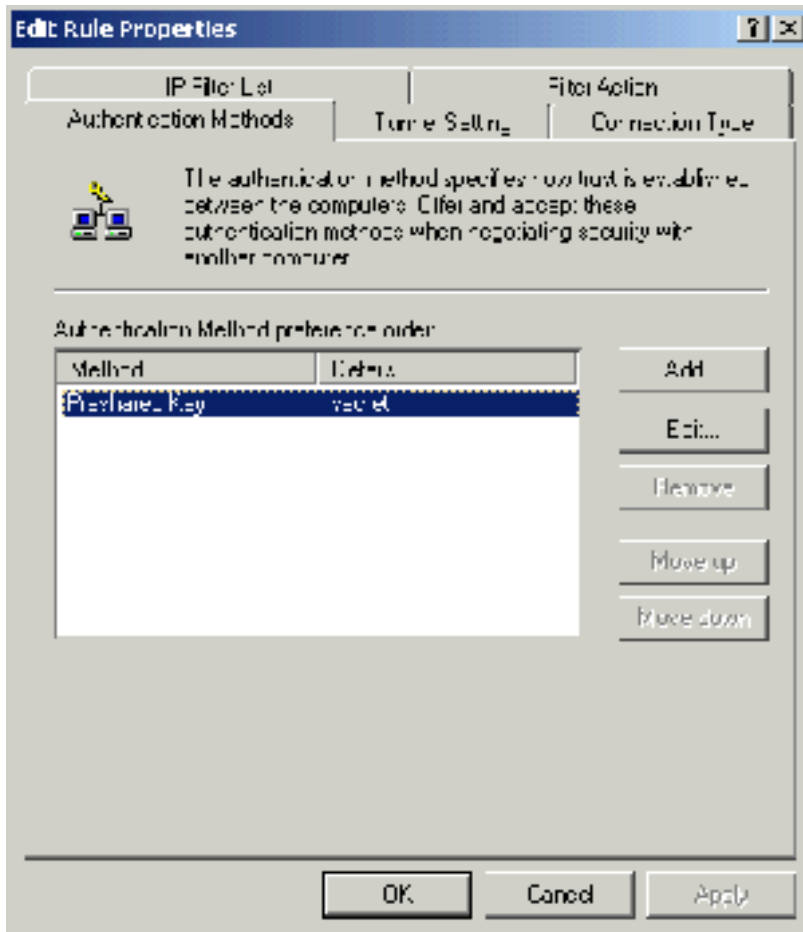
Double Click on the security policy to obtain the “properties” window for the “toperciws” security policy as seen on the left.



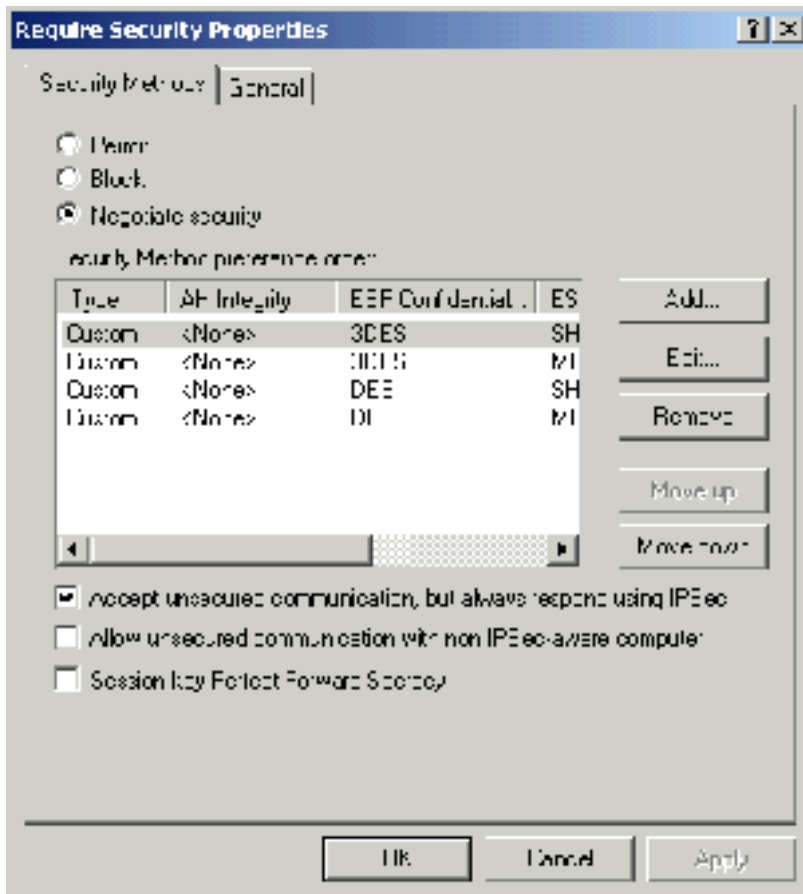
The “rules” tab of the security policy shows which “IP Filter Lists” is in effect. Double Click on a filter list to view or change it.



The “IP Filter List” tab shows the active filter. This filter specifies which networks define the encryption domain or VPN.



The “Authentication method” tab describes how a VPN is constructed. I used the shared key method (with a poor password) for testing. Kerberos and Certificates are also available methods.



The “Filter Action” tab drills down to the following “Security Properties” window. IPsec negotiation parameters are set here.

Appendix B: VPN Trace

The Following is a Network General sniffer trace of a single encrypted IPSec transport mode (Not Tunneled) packet generated via the setup described in Appendix A. As can be seen, VPN traffic is not TCP or UDP traffic. The VPN settings described above are really in effect.

```
DLC: ----- DLC Header -----
DLC:
DLC: Frame 7734 arrived at 07:46:52.0743; frame size is 110 (006E hex) bytes.
DLC: Destination = Station 00C04F97E6A6
DLC: Source       = Station 00C04F92F6F3
DLC: Ethertype    = 0800 (IP)
DLC:
IP: ----- IP Header -----
IP:
IP: Version = 4, header length = 20 bytes
IP: Type of service = 00
IP:    000. .... = routine
IP:    ...0 .... = normal delay
IP:    .... 0... = normal throughput
IP:    .... .0.. = normal reliability
IP: Total length   = 96 bytes
IP: Identification = 20416
IP: Flags          = 0X
IP:    .0.. .... = may fragment
IP:    ..0. .... = last fragment
IP: Fragment offset = 0 bytes
IP: Time to live   = 128 seconds/hops
IP: Protocol       = 50 (SIPP-ESP)
IP: Header checksum = 02B3 (correct)
IP: Source address  = [10.49.100.24], 4F92F6F3
IP: Destination address = [10.49.111.127], WDCM4C
IP: No options
IP:
ESP: ----- IPv6 ESP -----
ESP:
ESP: Security Association Identifier = 2641496210
ESP: Opaque Transform Data          =
00000001F2F7B41A6B7DD81A211487A56E4B96633FDF5A7652310178B9F6218436CF3921614F88F
E6539D143AC69...
```

ADDR	HEX	ASCII
0000	00 C0 4F 97 E6 A6 00 C0 4F 92 F6 F3 08 00 45 00	..O.....O.....E.
0010	00 60 4F C0 00 00 80 32 02 B3 0A 31 64 18 0A 31	.`O....2....1d..1
0020	6F 7F 9D 72 08 92 00 00 00 01 F2 F7 B4 1A 6B 7D	o..r.....k}
0030	D8 1A 21 14 87 A5 6E 4B 96 63 3F DF 5A 76 52 31	..!...nK.c?.ZvR1
0040	01 78 B9 F6 21 84 36 CF 39 21 61 4F 88 FE 65 39	.x...!.6.9!aO...e9
0050	D1 43 AC 69 5D CC 15 FE 53 3C AA 5A 84 27 B6 D9	.C.i]...S<.Z.'...
0060	DD 46 E6 4A 45 9F AD 24 0C 11 F8 A8 EF 2F	.F.JE..\$....../

References

- [1] "IETF Internet Security Protocol Standard". 01 Mar 2000. URL: <http://www.ietf.org/html.charters/ipsec-charter.html>
- [2] Checkpoint Software Technologies Ltd. "Checkpoint Virtual Private Networks" January 2000
- [3] Sun-Netscape Alliance. "iPlanet Home Page" URL: <http://www.iPlanet.com>
- [4] Reference Q252735. "How to configure IPSec Tunneling in Windows 2000". 25 Feb 2000. URL: <http://support.microsoft.com/support/kb/articles/Q252/7/35.ASP?LN=EN-US&SD=gn&FR=0>
- [5] "Step-by-Step Guide to Internet Protocol Security (IPSec)". 17 Feb 2000. URL: <http://www.microsoft.com/WINDOWS2000/library/planning/security/ipsecsteps.asp>

- [6] <http://www.cyberarmy.com>.
- [7] <http://www.rootshell.com>

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

Upcoming Training

Click Here to
{Get CERTIFIED!}



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
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 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 Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 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
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 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
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 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