Global Information Assurance Certification Paper

Wireless Security – Dispelling Myths

Eric Smith

GIAC Security Essentials Certification (GSEC)
Version 1.4b Option 1

January 27, 2004

Table of Contents

Abstract
This paper's intent is to dispel the myth that wireless security is essentially non-existent. It seems as if many people discount even the most basic security options that are packaged with wireless networking equipment because they have heard that wireless security features are worthless. These features, while not perfect by any means, are useful and can be successful as deterrents when utilized properly. When combined with each other or used as a means in connection with other implementations, these features can provide the security that is needed to protect your wireless network.

Introduction
When wireless networking technology first made its way onto the stage a few years ago, security wasn't exactly along for the ride. The technology had been put forward as merely a connection enabler, allowing for network users without access to a Cat5 Jack to access a Local Area Network (LAN) and potentially the Internet. What a great idea! I could now sit in the conference room at work with my laptop and have access to the same network I was able to access from my desktop in my office! No special requests needed, no waiting for the room to be wired…rather it was only a matter of establishing a connection between my wireless PCMCIA network card and the access point that was directly connected to the corporate LAN. I did have an uneasy feeling, however, that this might just be a little too easy.

My uneasy feeling related to the fact that I had to do nothing extra to gain access to the network. There were no additional means of authentication. No special hardware was required. There were no restrictions. The only thing I could immediately think of was distance, although that could be changed with the proper equipment. There was essentially nothing keeping someone in the building across the street from gaining the same access I had. The physical hurdle of actually needing access to an Ethernet port had been cleared without effort. The potential for disaster was exponential. Hackers, corporate spies, terrorists – nothing was keeping them at bay.

As things have progressed in the wireless world over the last few years, security mechanisms have improved. This paper will review each of the main mechanisms that are available to secure a wireless network.

Basic Security Options
Wi-Fi vendors have created an industry standard in which their equipment is shipped with simple default settings and without any security enhancements enabled.[1] While a great deal of people simply take their WLAN equipment out of the box and plug it in with no security enabled, some at least utilize the basic security options that are available. While these basic options are less than ideal

[1] Mohney, Doug. "Wi-Fi Remains a Work in Progress". URL: http://www.newsfactor.com/story.xhtml?story_title=Wi_Fi_Remains_a_Work_in_Progress&story_id=23030&category=netsecurity#story-start

for a completely secure environment, they are exponentially better than leaving your access point in a default mode that anyone can access.

Closed Mode

The first step that can and should be taken by anyone implementing a wireless network is to disable the Service Set Identifier (SSID) Broadcasts. This is often referred to as putting the Access Point (AP) into "Closed Mode".

The SSID is simply the common name that the AP has been given that acts as a means to differentiate between wireless networks. All APs come with the SSID already set to something that typically relates to the manufacturer. For instance, Linksys sets their default SSIDs to 'linksys', while D-Link sets their default SSIDs to 'default'. Many users make the mistake of never changing the SSID. On the other hand some change them, but then give them names that are too descriptive. For instance, the name of the company running the AP is often used as the SSID. Although this does not seem like a big deal, it provides someone targeting that company with critical information that they previously did not have – especially if the AP is still open to anyone with a wireless card and no further knowledge.[2]

One way to avoid a majority of the problems surrounding SSID Broadcasts is to put the AP into Closed Mode. By doing this, broadcast is disabled and a large majority of the people out there trying to detect and exploit wireless networks will not find your AP. While the network is still discoverable through more advanced exploits, someone simply looking for broadcast beacons through the use of a basic tool such as NetStumbler will not see your network. Interestingly, the ability to disable SSID broadcasts is not a requirement of the standard that WLAN equipment manufacturers must follow. It was added by nearly every manufacturer after they learned that people were actively looking for WLANs to exploit and that the broadcast beacons were the means by which they were able to discover them. Many firmware updates were distributed to solve the issue.

Simply put, disabling the SSID on an AP should be one of the very first steps taken upon setting up a wireless network. It is an easy fix, and it is the first move toward a more secure WLAN.

MAC Filtering

Another step that can be taken to protect your wireless network involves enabling MAC address filtering on the AP. This feature comes with nearly every AP on the market, and allows the administrator of the AP to add the MAC addresses of their authorized wireless users into a list on the AP that it then uses to allow or disallow users attempting to associate to or use the wireless network. MAC filtering works very well for a small network that is centrally managed and has a limited number of APs and a user base that is essentially static. However, for a

[2] Dismukes, Trey. "Wireless Security Blackpaper." URL: http://www.arstechnica.com/paedia/w/wireless/security-1.html

large network or a network that has a high turnover rate for its users, this is less than ideal due to the fact that the AP's authorized MAC address list would need to continually be updated. That problem multiplies when you factor in doing this for numerous APs that each user is authorized to use.

MAC filtering has one other problem that is well known – MAC addresses for network cards can easily be spoofed. The problem here relates to the inability of many APs to detect multiple identical and concurrently active MAC addresses. A determined attacker can easily sniff MAC addresses that are associated to a given AP even if WEP is enabled due to the fact that all of the frame headers that go through the air are in clear text. The attacker can then manipulate the MAC address of their network card to appear to be that of the authorized user. In many cases, this will go without being detected by the access point or the administrator. Furthermore, depending on the AP that is being attacked, the collision problems that occur on wired networks that disallow simultaneous MACs from existing on a network are not necessarily present. We were able to exploit this problem in our own office environment through a Linksys WAP11 AP. Both systems that were using the same MAC address were able to acquire different IP addresses and maintain access to the wireless network and the Internet without experiencing any problems. Some APs will not allow a scenario like the one explained previously. However, they most likely will allow an attacker that has captured a MAC address the ability to masquerade as that authorized user once the true authorized user has either gone home for the day or stopped using the wireless network. Unless some other means of authentication is required, this is a very simple attack.

Considering the ease with which MAC address filtering can be usurped, it is still another level of security that needs to be overcome by an attacker. Once again, you have to ask yourself how much work a bad guy is willing to do to gain access to your network. Adding multiple levels of basic security like this may be just enough to deter them.

WEP

Wired Equivalent Privacy (WEP) has been thoroughly beaten up by both security professionals and the media alike. The reason for this revolves around the inherent vulnerability that is present in its implementation. For a complete discussion concerning the problem, see the Fluhrer, Mantin, Shamir paper that details the weaknesses in the RC4 algorithm.[3] While this problem is a very serious one, it does not make WEP completely irrelevant. It is still a very useful tool that can be implemented – especially in a home or small business environment. Before we get further into the problems and implementations of WEP, let's talk a little about WEP in general.

[3] Fluhrer, Scott; Mantin, Itsik; Shamir, Adi. "Weaknesses in the Key Scheduling Algorithm of RC4." URL: http://downloads.securityfocus.com/library/rc4_ksaproc.pdf

"According to the IEEE 802.11 standard, the WEP algorithm is used to protect wireless communication from eavesdropping. A secondary function of WEP is to prevent unauthorized access to a wireless network. While this function is not an explicit goal in the 802.11 standard, it is frequently considered to be a feature of WEP."[4] The way that WEP accomplishes both is through the use of a shared key. On the AP, up to four different WEP keys can be entered at either 64 or 128 bit key lengths. Of course, only one WEP key at a time can be active. Unfortunately, the standard implementation of WEP requires that you enter the keys at each station that will be accessing the network. You must also specify which key will be used. In a utopian situation, these keys could then be frequently and easily cycled to prevent someone from easily breaking your WEP encryption. This is unfortunately not the case with WEP. To cycle the keys, you could rely on educating users so they can do it on a predetermined schedule. Even then, you must determine a means to securely distribute the WEP key to those educated users. Another option would be to do it yourself. Of course, this becomes almost as much overhead as maintaining a MAC address filtering list if you are doing it in a large environment. As was noted before, this is one of the main reasons that WEP in its most basic state is best used in a home or small office environment.

Another reason WEP is a useful tool for the small office/home office (SOHO) environment is due to the length of time and amount of traffic it takes for an attacker to successfully crack a WEP key. Contrary to many of the articles that are posted on the web, a WEP key can not be cracked in a matter of minutes on a wireless network in a real-world environment. Depending on the amount of traffic that is traversing the network, it may take days or even weeks to collect the millions of frames essential to be able to crack the WEP key. Knowing this, you then need to factor in how badly the attacker wants to get into your network. Are they trying to damage your network or steal proprietary information? In most cases, if someone is trying to crack your WEP key they are obviously targeting your network for some specific reason other than just to gain access to the Internet. If that were the case, why would they not spend the extra couple minutes it would take to find an unprotected AP that they could easily utilize? If they are specifically targeting your network, then what are the odds they will be able to maintain their position or access for the length of time that they need to gather the necessary data? Will their equipment be able to maintain power and run without crashing for this extended period of time? Will they be able to detect the physical security measures that you have in place for that amount of time? More importantly, in that time will the WEP key be cycled and cause their actions to be all for naught? In other words, there are a lot of factors that are working against the attacker considering the length of time it will take them to crack the WEP key.

[4] Borisov, Nikita; Goldberg, Ian; Wagner, David. "Security of the WEP Algorithm". URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

All of the factors mentioned above are things that absolutely need to be factored in when determining what level of security is sufficient for your WLAN. It's very possible that the combination of turning off the SSID broadcast, turning on MAC filtering, and enabling WEP will be enough to keep an intruder from even thinking about attempting to crack your wireless network. Why go through all that work when they can gain access to one of the many APs that are completely unprotected? Combining these three basic security features may be enough security in the right situation, but that will need to be determined by the company or person implementing the wireless network. In situations where this will not be enough, more advanced options will need to be explored.

Advanced Security Options

While the basic security measures that were previously mentioned are enough to sufficiently protect a SOHO environment, they will not be enough to provide a fluid yet secure environment in a larger business setting. I emphasize the fluidity of the solution due to the fact that any of the previous security implementations could be utilized but all would be extremely cumbersome.

WPA

Wi-Fi Protected Access (WPA) was developed by Wi-Fi manufacturers as an alternative solution to WEP that will remain in place until the 802.11i standard is ratified by The Institute of Electrical & Electronics Engineers (IEEE), thus providing a more secure wireless environment. Although WPA is a temporary solution and isn't recognized by IEEE, it is very similar to what 802.11i will look like once it is finalized.[5] It may seem that manufacturers could have just waited for 802.11i to be completed, however there are no definitive timeframes for IEEE standards to be finalized and the community did not want to be left in the lurch. Essentially, they took the portions of 802.11i that were ready for use and put them into WPA.

The most important things that WPA offers that pre-existing integrated wireless security options do not is an improved means of encryption as well as the ability to utilize authentication. The improved encryption comes in the form of the Temporal Key Integrity Protocol (TKIP), while authentication is accomplished by using 802.1x and the Extensible Authentication Protocol (EAP). All of this can be accomplished through a simple software or firmware upgrade while 802.11i is expected to require a hardware upgrade.

TKIP replaces WEP and is required in WPA. TKIP is able to utilize the same hardware that does WEP calculations, but does it in a stronger, far more robust manner. Encryption keys can be up to 256 bits in length, improving on WEP's 64 and 128 bit keys. TKIP also addresses all of the weaknesses that are present in WEP, and gives wireless users a more secure environment in which to operate.

[5] Posey, Brien. "WPA Wireless Security Offers Multiple Advantages over WEP." URL: http://techrepublic.com.com/5100-6265-5060773.html

802.1x and EAP provide the means of authentication within WPA. The most important thing to know about 802.1x and EAP is that they require a somewhat complicated infrastructure to implement. 802.1x and EAP will be explained in more detail later in this paper, and at that point it will be more apparent why it is a technology solution that is more appropriate for a larger business or enterprise environment. Knowing this, it seems as if WPA does not make sense for someone in a SOHO environment. Wi-Fi manufacturers thought of this, though, and added a secondary mode within WPA that can be enabled for home users. Instead of needing to implement an 802.1x environment, they can simply enable this mode. Lee Barken's book, How Secure is Your Wireless Network? : Safeguarding Your Wi-Fi LAN, provides the following explanation of how this secondary mode works:

> In this special mode, all the user has to do is enter a shared secret (called a master key) in the AP and each client. This is similar to the way WEP worked when you had to enter a WEP key in the AP and each client. However, unlike WEP, TKIP uses the master key as a starting point to mathematically derive the other encryption keys. Unlike WEP, which used the static key over and over again, TKIP changes the encryption keys to ensure that the same key is never used twice.[6]

This clearly demonstrates that TKIP is a much better solution than WEP in the SOHO environment. The ease with which WPA can be implemented in this mode also makes it an attractive solution. The only problem that remains is the existence of a shared secret and the tendency for most people to make that shared secret something overly simplistic, thus making it easier to crack.

As you can see, WPA is a much better security option for small and large networks alike. It has the flexibility that the original built-in Wi-Fi security mechanisms lacked. While it is only a temporary solution, users should not hesitate to use it on their wireless networks.

Captive Portals

The Personal Telco Project provides the following definition for captive portals: "Captive portals allow you to leverage a common browser as a secure authentication device. They also have the potential to allow you to do everything securely via SSL and IPSec and setup per user quality of service rules, and still maintain an open network."[7] Sounds like a great idea, huh? Well, it is. Numerous companies have put this idea to good use, setting up hotspots in places like airports and coffee shops all over the world in an effort to provide Internet access to anyone that is interested and is willing to part with a few dollars or at least be responsible for their actions. It has also been put to good use by corporate and casual users to maintain control of their network and keep track of users in the interest of limiting the provider's level of liability.

---

[6] Barken, p. 66.
[7] Personal Telco Project. URL: http://www.personaltelco.net/index.cgi/CaptivePortal

Basically, the way a captive portal works is quite simple. You set up a web page that unauthenticated users are initially forced to go to when they associate with an AP and open up their web browser for the first time. Once at the portal's page, they either log on with the credentials they created during a previous session, or create a new user account via the web interface that is presented. Once a user has been authenticated they are seen as a trusted user on that node and can surf to their heart's content.

Captive portals are popular with users as well as providers. Users like the fact that they do not need to install any additional software on their computer to utilize the service. The whole process is very straightforward. Providers, on the other hand, like the fact that it is a relatively easy service to set up and maintain. The cost of providing and maintaining the service is relatively minimal so it is an attractive business model as long as there are enough interested users to make it worthwhile. The business potential was apparent to one company in particular – Starbucks. They decided to provide wireless Internet access via a captive portal system during the summer of 2001 at a large number of their coffee shops nationwide. Many other companies have popped up that specialize in providing hotspots worldwide, and while many are provided specifically for recreational use, there are a large number of these hotspots that are being placed strategically in an effort to cater to traveling business users.

Another benefit of a captive portal system for a provider is the ability to track users of the service. While some may think this is an unfortunate byproduct of using this service, many realize it is a much-needed means of protection. One very unique element that wireless internet access offers that is unmatched by other types of access is the fact that users can gain access in many cases without the provider knowing or being able to find out. Whether the provider is knowingly offering access is truly the question. In many cases, APs are set up at homes or businesses without the intention of providing access to anyone other than family members or employees. The fact that the radio waves that provide the connection propagate beyond the walls of the building the AP resides in is often forgotten or not realized. In many cases it is as easy to gain access as pulling up to the curb outside of a house or parking in a parking lot outside of a company's headquarters. If no security is in place, the person looking for access can many times get access, do what they want to do, and subsequently leave without the provider even knowing they were there. This may not seem problematic, as that is what wireless access was designed for, but what if that user decides to download or distribute child porn via that AP's connection? What if the WLAN is utilized to hack a company's server? Who will be responsible for the actions that are being taken via this connection? Unfortunately, the person who owns the AP that provides the network connection will be left holding the bag because of the lack of tracking mechanisms available for WLANs. Essentially, the only proof that may exist to show a connection was made by another person is a MAC address in the logs of the AP. The likelihood of being

able to track down a single MAC address is slim to none. That's not even taking into account that MAC addresses are easily spoofed. This is why captive portals are very useful. Connections can be tracked and tied to users, thus giving the provider a means of limiting their liability. This is a very attractive feature not only for hotspots, but also for business WLANs and community networks.

One major problem that currently exists with captive portals is the potential to fall prey to someone spoofing a captive portal site. One program in particular – Airsnarf – was created to specifically target users utilizing hotspots.[8] It essentially allows a rogue access point to impersonate a legitimate hotspot and steal usernames and passwords. This is obviously an extremely serious problem if the attacker is able to successfully execute the attack. Fraud and misuse of another user's account could lead to liability problems down the road, not to mention the fact that the user could be stuck with a huge bill for activity for which they were not responsible. What can providers do about this problem? Basically they can do a better job of AP placement as well as maintaining better physical security in an effort to detect people attempting to set up these rogue APs. Beyond that, it is something that will have to be addressed with improved security solutions in the future.

802.1x

802.1x is a port-based authentication protocol that allows users to establish a secure means of communication via a wireless network. While it was originally designed to work on a wired medium, it definitely translates well to a wireless environment.

802.1x was initially developed to control access to Ethernet ports in a University campus environment. Administrators did not want to allow just any user to be able to plug into an Ethernet port and then gain access to their network as well as potentially the rest of the Internet. 802.1x gave them the ability to limit the use of the port until the user could be authenticated. In the wireless world, the idea of a port is rather abstract, but still essentially exists. Unfortunately, wireless ports can exist anywhere – to include the parking lot if the signal propagates that far.

802.1x utilizes the Extensible Authentication Protocol (EAP) to provide for the means of authentication. The genius of EAP comes in the fact that it is a flexible protocol and pretty much any means of authentication can be plugged in. Standard passwords can be used as well as certificates, Public Key Infrastructure (PKI) or Kerberos. EAP was developed so future authentication methods could be plugged in as they were developed, thus removing the need to develop a new protocol as new methods of authentication are developed. This flexibility is a huge key to 802.1x's popularity as a security solution.

To better understand how 802.1x maintains a secure environment, it is best to discuss its three basic parts. The first part is the user or client, which is referred

[8] The Shmoo Group. URL: http://airsnarf.shmoo.com/

to as the supplicant. The next part – typically the AP – is referred to as the authenticator. The authenticator's main job is to act as the middle man – blocking or allowing access based on what it is being told by the authentication server, which is the third component. The authentication server handles authentication information, and typically comes in the form of a RADIUS server. This server maintains a database of user credentials in order to determine whether or not the authenticator will provide open access to the supplicant. A good analogy that allows better visualization of the entire process is explained by an excerpt from the book How Secure is Your Wireless Network? : Safeguarding Your Wi-Fi LAN written by Lee Barken.

> Imagine you're trying to get into a swanky new downtown club or bar. The supplicant is the person trying to get inside. The authenticator is the bouncer letting people in or keeping them out. The authentication server is the VIP list of people who are allowed inside.[9]

Since many businesses already have some form of authentication server already integrated into their network, an 802.1x framework for a WLAN would not be that big of an addition. On the other hand, 802.1x does not make a whole lot of sense for a home or small office user.

Outside of an attacker doing a complicated man-in-the-middle attack in an attempt to steal a user's credentials, there are not any known vulnerabilities with the actual implementation or framework of 802.1x. Additionally, the only published vulnerability for 802.1x deals with a specific piece of Cisco hardware.[10] Limited vulnerabilities and the good track record of 802.1x in the wired arena point toward this being a very good solution for wireless networks.

802.11i

802.11i is being treated like the Holy Grail for wireless security. It will be the official replacement for WEP as of sometime during mid 2004, and will introduce improved security in a couple of different ways. The standard will address improvements to existing 802.11 equipment using the current WEP algorithm, as well as create the need for all new 802.11 equipment due to the fact that it requires the Advanced Encryption Standard (AES).[11]

As was discussed earlier in the paper within the WPA section, people with 802.11 equipment developed prior to the ratification of 802.11i will be able to do a firmware or software upgrade to allow them to utilize a more robust implementation of the hardware they already have. This portion of 802.11i will be basically the same as what has been utilized within WPA, and will mostly be used by SOHO users. This portion of the standard will come in the form of TKIP

[9] Barken, p. 70.
[10] Cisco. "Cisco Security Advisory: Catalyst 5000 Series 802.1x Vulnerability." URL: http://www.cisco.com/warp/public/707/cat5k-8021x-vuln-pub.shtml
[11] O'Hara, Bob. "Wireless Security: Wait for 802.11i?" URL: http://www.nwfusion.com/columnists/2003/1110wizards.html

and be implemented via a shared secret. Again, the security of this particular mode will only be as strong as the passphrase that is created by the users, and will be vulnerable to dictionary-style attacks.

The second portion of 802.11i will be very significant. The encryption standard utilized by 802.11i-compliant APs will be AES. AES will take the place of WEP and will provide what some refer to as "unbreakable" encryption. This, of course, is a ludicrous statement considering that all encryption can be broken given enough time, and with the advent of technology from year to year that time frame continually shrinks. However, it does make the point that AES is a huge step up from a flawed WEP implementation. The reason that new equipment will be required for 802.11i is simply due to the fact that there needs to be more processing power for the AES algorithm to work. The current processing power in APs is insufficient for an algorithm as powerful as AES, therefore firmware and software updates will do no good. In addition to the improved encryption of 802.11i, it also implements the likes of 802.1x for authentication. As was discussed in the previous section, 802.1x is a solid solution by itself. When implemented with AES, the overall standard becomes that much more secure.

Knowing all of this, why is 802.11i so much less vulnerable to hackers? Well, there are a number of specific reasons. First and foremost, there is no longer just a single key for each packet in a session. Obviously this is quite different than the WEP implementation. Also, packet ordering will be combined with security key generation, thus forcing out of order packets to be ignored. This makes hackers powerless, preventing them from sniffing, intercepting or replicating traffic. The addition of the MAC addresses of both the source and destination addresses to the generation of the key add yet another component of complexity for hackers to overcome.[12] All of the these things as well as a couple other minor implementation changes make 802.11i a huge issue for hackers to overcome.

Conclusion

Wireless networking is truly still in its infancy. New jumps in speed and options in quality of service are still being introduced to this burgeoning technology. Most importantly, the security of WLANs continues to improve even though pretty much all you hear and read is that wireless security is nonexistent. While this may have been true when wireless networking came on the scene, it is no longer the case. In a matter of approximately 4 years we have migrated from an environment in which security was an afterthought to currently being on the cusp of a security implementation that could make a huge impact in the security of wireless networks for years to come. There are still flaws that will surely be discovered over time, but at least the community is moving in the right direction in an effort to make a very positive impact on wireless users and will allow for the

[12] MacVitte, Don. "802.11i to Lock Down WLANs." URL: http://www.networkingpipeline.com/specwatch/802.11i.jhtml

continued proliferation of wireless networks into both the home and workplace environments for years to come.

References

[1] Mohney, Doug. "Wi-Fi Remains a Work in Progress." 20 Jan 2004. URL: http://www.newsfactor.com/story.xhtml?story_title=Wi_Fi_Remains_a_Work_in_Progress&story_id=23030&category=netsecurity#story-start (21 Jan 2004).

[2] Dismukes, Trey. "Wireless Security Blackpaper." 18 Jul 2002. URL: http://www.arstechnica.com/paedia/w/wireless/security-1.html (20 Jan 2004).

[3] Fluhrer, Scott; Mantin, Itsik; Shamir, Adi. "Weaknesses in the Key Scheduling Algorithm of RC4." URL: http://downloads.securityfocus.com/library/rc4_ksaproc.pdf (20 Jan 2004).

[4] Borisov, Nikita; Goldberg, Ian; Wagner, David. "Security of the WEP Algorithm." URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (21 Jan 2004).

[5] Posey, Brien. "WPA Wireless Security Offers Multiple Advantages over WEP." 10 Sep 2003. URL: http://techrepublic.com.com/5100-6265-5060773.html (23 Jan 2004).

[6] Barken, Lee. How Secure is Your Wireless Network? : Safeguarding Your Wi-Fi LAN. Upper Saddle River: Pearson Education, Inc., 2004.

[7] Personal Telco Project. 4 Jan 2004. URL: http://www.personaltelco.net/index.cgi/CaptivePortal (23 Jan 2004).

[8] The Shmoo Group. URL: http://airsnarf.shmoo.com/ (24 Jan 2004).

[9] Cisco. "Cisco Security Advisory: Catalyst 5000 Series 802.1x Vulnerability." 13 Apr 2001. URL: http://www.cisco.com/warp/public/707/cat5k-8021x-vuln-pub.shtml (26 Jan 2004)

[10] Bob O'Hara. "Wireless Security: Wait for 802.11i?" 10 Nov 2003. URL: http://www.nwfusion.com/columnists/2003/1110wizards.html (26 Jan 2004)

[11] MacVitte, Don. "802.11i to Lock Down WLANs." URL: http://www.networkingpipeline.com/specwatch/802.11i.jhtml (26 Jan 2004)

Last Updated: July 22nd, 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
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
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