# Global Information Assurance Certification Paper

# SECURING WIRELESS NETWORKING WITHIN THE COLLEGE DISTRICT CASE STUDY

Practical Assignment Presented to the
SANS Institute
GIAC: Global Information Assurance Certification

In partial fulfillment of the requirements for
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b - Option 2

By

Gregory Evilsizer

December 31, 2002

TABLE OF CONTENTS

***Abstract***

Wireless networks ease of deployment and low startup costs has made this technology very popular in the private and pubic business sectors. Wireless technology also brings a great deal of vulnerability to computer networks. The vulnerabilities inherent with wireless networking need to be understood and additional security measures need to be taken in order to secure sensitive data on computer networks.

This paper will discuss the challenges the College District has faced in deploying secure systems, the steps taken to understand and identify the vulnerabilities of wireless networking, and the solutions proposed by the newly formed Wireless Committee to secure sensitive student data. Also discussed are the technologies that were used to secure the network infrastructure and the results that were achieved by implementing secure wireless solutions.

## Chapter I – Description of the Problem

*Section 1 – Statement of Purpose*

Technical support at the College District must understand, manage and secure the wired and wireless infrastructure in order to protect sensitive student data from security threats. During technical staff meetings it was discovered that wireless networks had been deployed with little to no consideration to securing the network and there was a need to define best practices for wireless networks. To that end the College District has formed a Wireless Committee composed of technical support from each campus. The author has volunteered his time to serve as chairman of the Wireless Committee and to organize committee activities.

The task of the Wireless Committee is to define management and security policies for wireless networks, and propose these solutions to management. One intended goal of the Wireless Committee is to share competencies between campuses as new wireless technologies present themselves to the marketplace, and to keep a vigilant eye on standards that develop in securing wireless networks.

The purpose of this paper is to look at the 802.11 protocol standard as it relates to wireless networking with laptop and desktop computers. PDA's, cell phones, pagers and Bluetooth enabled devices will not be covered in this paper.

*Section 2 – Setting of the Problem*

The College District faces many challenges to properly secure the network resources, budget being one of the most notable issues. Wireless networking may be easy and inexpensive to deploy. However, what is often overlooked is

the high cost of properly trained technical support, perimeter firewalls, switches and routers that must be properly configured prior to securing a wireless network. Because we are a publicly funded entity having the required funds to setup the necessary infrastructure has always been an issue. Add to that the fact that we reside in a state that has been faced with huge budget deficits; education is always a prime candidate for budget cuts.

Another factor that has hindered security has come from the educational institution and the idea of academic freedom. Those who support this freedom campaign for open access and do not want to be hindered with the complexities of secure network access to the systems that are used for education.

Systems that are installed without any help from the college technical support staff have also played a role in undermining security. There have been instances that have come to the attention of the college technical support where grant monies have been approved, equipment has been purchased, and installations have taken place without any consultation from the technical support staff. These activities can greatly undermine network security and compromise data integrity if left unchecked. One can imagine the consequences of a rogue wireless access point that was improperly configured with no security and that allowed open access to the District network infrastructure. Writing on security issues with wireless LAN's (WLAN), Maria Caravaggio (2002) outlines the ease of deploying a wireless access point with only the vendors' default Service Set Identifier (SSID) and management password. With little effort a hacker could gain access to the network resources and this is a threat that must be addressed to secure those resources.

The very students who are educated in computer sciences at the College District have at times posed a threat to security. What better place to practice hacking techniques, hide software that captures data, and launch Denial of Service (DOS) attacks, than in a working computer network that is open to public access. We have discovered cases of abuse to shared network resources that have been perpetrated by crafty students bent on abusing public resources for personal gain and/or gratification.

The Internet poses our biggest threat, and the College District must recognize and secure the network infrastructure from this ominous threat. There are those who use the Internet with malice intent to break into systems, steal data, and use stolen information for personal gain. Data such as credit card numbers, social security numbers, names and addresses can be used for ill-gotten gain. Not to be overlooked are enemy's of the state who are bent on toppling the United States data infrastructure. We have discovered abuses from the Internet who have used our bandwidth and processing power for their own benefit, launched DOS and brute force attacks against our systems, and who continually probe our systems for information.

*Section 3 – History and Background of Security Issues*

The author arrived at the College District at a time when these threats were being recognized and needed equipment to secure the network infrastructure were just beginning to be looked at and deployed. Network security had come to the forefront of infrastructure upgrades, and staff was being trained on securing these data networks.

The College District had no perimeter firewalls in place, and public IP addressing was deployed throughout the network. There were some host based firewalls in place, but these were deployed in what seemed to be a direct result of previous system attacks from outside forces and could be labeled little more than patch work fixes. Router Access Control Lists (ACL's) had been deployed at a few campuses, protecting select systems from the Internet threat. However, managing large lists of ACL's slows the routers performance and is at best a temporary stop gap measure until perimeter firewalls can be put in place.

For the most part the student and administrative networks had been separated by physical barriers such as distinctly separated networks, and this offered some bandwidth protection and little more.

The author was responsible for the deployment of wireless access at the District Office. District Office technical staff had been sent to SANS training, and on returning from SANS the authors wireless project was placed on hold until the proper infrastructure could be put in place to secure the network and then secure the wireless network.

Management recognized the need to send the author to SANS training, and the topics covered in the SANS Security Essentials curriculum opened his eyes to the threat posed by wireless networks. Those threats are the same threats posed to wired networks, only compounded by the use of airwaves for the broadcast media and the mobility and the risk of theft inherent with laptop computers.

These security issues posed by an insecure network infrastructure are only compounded by the addition of wireless networks and the security gaps discovered in wireless networks. These weaknesses in the wireless technology must be looked at and fully understood in order to protect the District's data networks.

*Section 4 – Threats Posed to District Wireless Networks*

The wireless infrastructure had already been deployed at most of the campuses, and 128bit Wired Equivalency Privacy (WEP) with Media Access Control (MAC) address filtering is the only deployed means of security. According to researchers at the University of California at Berkeley, many flaws can be found

in the WEP algorithm that relies on the RC4 cryptographic algorithm. Borisov, Goldberg and Wagner (2001) detail the weaknesses and vulnerabilities that can be found in the way that the WEP algorithm was deployed in the 802.11 protocol standard, and WEP cannot be considered a secure solution for wireless networking.

Passive attacks include eavesdropping and traffic analysis, whereby the attacker simply monitors WLAN packet data and/or captures WLAN data for later analysis. Active attacks perpetrated by an attacker actually modify the data packets. This type of attack can be divided into four subcategories, masquerading, replay, message modification and DOS attacks. Masquerading as the name implies, is where an attacker impersonates a valid user to gain their network privileges. A replay is where the attacker who is listening to captured user data replays the data of the valid user. Message modification is when the attacker actually modifies the data by adding, deleting, or in some way tweaking the data. The DOS attack is where the attacker blocks or prevents use of the network resources (Karygiannis & Owens, p. 3-13).

Because data is broadcast over the airwaves, confidentiality of data is of concern (Karygiannis & Owens, 3-13). The College District administrative and faculty staff continually accesses student data and providing access to this sensitive data over wireless networks is of great concern.

Access points are typically configured to broadcast the SSID, and there are tools such as Netstumbler, by Marius Milner, available to aid the discovery of the SSID. By discovering the SSID, the attacker can join the network (Cole, et al. 6-34, 6-39).

One well documented threat to wireless networking is exploiting the vulnerabilities of the WEP encryption mechanism. Tools such as AirSnort are used to recover WEP encryption keys and are freely available from the Internet. By passively capturing data packets broadcast over the air waves, the WEP password can be cracked (The Schmoo Group). Because this is a passive attack, detecting such activity is next to impossible. Therefore WEP encryption will only deter the casual hacker, and an attacker with a determination to break into a network will not be thwarted by WEP encryption.

MAC address filtering offers yet another level of protection from the casual hacker. Most access points deployed on the district WLAN were capable of allowing only selected MAC addresses access to the WLAN resource. However, with the ability to change the MAC address, MAC address spoofing is a possibility for the determined hacker. We learned from the SANS curriculum that the MAC address is broadcast in clear text even with WEP enabled. The hacker can passively capture data and use the MAC address information to modify his own network card that would then be recognized as a valid MAC address to the access point. Therefore, MAC address filtering is not a viable

solution for securing wireless networks (Cole, et al. 6-34).

## Chapter II – Analyzing WLAN Technologies

*Section 1 – The Wireless Committee*

Urged by the Vice-Chancellor of Information Technology (IT) to find a solution to the security holes posed by wireless networks, technical staff from six-campus locations formed the Wireless Committee. We were asked to come up with a recommended solution for wireless networks that would secure sensitive student data.

In subsequent meetings the Wireless Committee drafted a wireless networking policy that defined minimum and recommended security standards for wireless LAN's. It was important to draft a policy that would address the current installed WLAN at the campus locations, and also address the future of wireless networking as budget, equipment, and technology became available to further secure the WLAN.

It was a consensus among to technical staff to design a standard for wireless networking that would allow the full potential of wireless networking to be used by faculty and staff who may at times travel between campuses. It was also important to define a policy that would allow limited student and vendor access where required. The committee agreed that student and vendor access should be tightly controlled, segmented and secured to protect the network.

It was also a requirement that the committee would focus on standards based security technologies. Propriety based security solutions offered by select vendors would only be a interim security solution until such time as a secure standard that was not propriety based could be implemented by the entire district.

*Section 2 – Challenges and Issues*

During our meetings it was obvious that the security requirements for the campus location differed greatly than those security requirements needed at the District Office. The District Office is where the all student data is processed, and all access to student data is made via client/server communication with the District Office; the central database of students' records is hosted on UNIX systems at the District Office. It was agreed by the membership of the Wireless Committee that this was the one foremost system that required protection from all fronts, and WLAN technologies posed the greatest threat to this systems security. The campus viewpoint of security was that there were few systems that were of a critical nature to secure, and that segmentation of student systems and administrative systems was the foremost issue for each campus.

Another challenge to securing systems within the entire district stems from the fact that the technology departments at all the campuses operate independent from one another, and there is no centralized entity governing technology. This decentralization of technology presents unique challenges to security as a whole.

Add to that the mix of technical expertise found at each campus, and the obvious differences of opinion on security related issues, and we have a hot bed of controversy that must be overcome. The authors' opinion on this matter is that communication is the key variable to overcome these challenges, and that the Wireless Committee was a positive step to bring all these issues together and gain a consensus on security.

*Section 3 –Defining the Problem*

All members of the Wireless committee agreed that the currently installed WLAN technologies at our college campuses lacked the desired security that could be realized by adding the proper infrastructure, but there was some disagreement on what was an acceptable security standard. The issues with using WEP to secure the WLAN resources were well understood, and we were able to share research on the problems with the WEP algorithm. It was also brought up by a member of the committee that MAC address filtering was not tamperproof, and that some network cards allowed the MAC address to be changed via software, and this was not a sound secure solution.

We spent some time researching existing technologies that would provide a more secure solution than that offered through WEP and MAC address filtering. We met with two different vendors to discuss their solutions to WLAN security. And we discussed methods of securing our existing infrastructure with the technologies we had in place, knowing that hardware upgrades were required to further strengthen security.

We looked at our vulnerabilities and agreed that wireless access to the UNIX server that maintains all student records was our largest vulnerability, and that this system was the most important system to secure. It was agreed that we would work on drafting policies that would protect this system from the security holes posed by wireless networking. We are currently drafting a recommended standard for wireless networking and have completed a minimum standard to support the transition from our current WLAN technologies to future, more secure WLAN technologies.

*Section 4 – Securing the District Office Network*

One of the first measures the District Office looked at was the need to upgrade our existing Wide Area Network (WAN) routers and incorporate perimeter firewalls at the District Office. The author was involved with the deployment of

the routers and firewalls at the District Office. The wireless network at the District Office would be placed on hold and not deployed until the perimeter firewalls were in place.

The installation of redundant Cisco PIX 515 firewalls was installed on two WAN's. One WAN supported connections to six campus networks and the other WAN supports connections to our K12 schools that need access to our IBM mainframe.

This firewall installation was soon followed by upgrades to the Districts WAN routers and the deployment of layer 3 stitches. These technologies were needed in order to support the ability to use VLAN technologies. The District Office is currently moving to private IP addressing and utilizing Network Address Translation (NAT) for the internal network. These technologies will be used to secure the District Office wireless network.

*Section 5 – Securing the Campus Network*

The District management met with the technology management at the campuses and discussed the need for them to also acquire and deploy perimeter firewalls at the campus locations. District management had decided to go with Cisco solutions based on the fact that the Campuses taught the Cisco curriculum and that most campuses would standardize on the Cisco PIX firewall solution.

Several campuses have already deployed perimeter firewalls on their networks. These campuses are also implementing VLAN and VPN solutions to further secure their WLAN. All campus location are currently moving to private IP addressing utilizing NAT for the internal network.

*Section 6 – Steps to Secure the WLAN*

The Wireless Committee drafted the following required policies for wireless networking.

1. All wireless implementations must go through the technology departments at each respective campus before installation on the network.
2. Only IT support personnel at each respective campus will have management access to their wireless access points.
3. In an effort to secure student confidential data, access to the UNIX server will not be permitted via a wireless device. Client installations allowing access to the UNIX server will only be installed on wired computers.

The Wireless Committee drafted MINIMUM standards for wireless LAN's, these minimum standards were drafted to support the existing installed base of WLAN

technologies. Existing wireless networks must meet and/or exceed these minimum standards.

Propriety based solutions can be implemented to provide more secure solutions than what is currently offered with WEP and MAC address filtering. However, it was agreed that an eye toward open standards should be the direction of the colleges WLAN implementations.

The minimum standard for administrative wireless LAN's must include the following;

1. MAC address filtering.
2. 128bit WEP.
3. Changing the default management password.
4. Changing the default SSID for access points. It was also recommended that if the access point supported turning off the broadcast of the SSID, that feature should be implemented also.
5. The implementation of Virtual Local Area Network (VLAN) technology has been discussed as a future minimum standard when the equipment required to VLAN a network is in place.

The minimum standard for student/vendor access to wireless LAN's must include the following. This standard is intended to give the student and/or vendor access to the Internet only without requiring WEP or MAC address filtering. Isolation technologies will be implemented to separate this type of access from the administrative network. The idea with including this type of WLAN technology is to offer a tiered wireless architecture by beefing up security on the administrative network while allowing open access to students and vendors needing access to the Internet on the separate student network.

1. Changing the default management password.
2. Isolate the student/vendor wireless LAN using VLAN and DMZ technologies.

The Wireless Committee is currently developing RECOMMENDED standards for wireless networking, and will add these recommended standards as the technology matures, and upgrades to existing systems are implemented. The technologies that we are looking at, and currently testing include the following;

1. Implementing the 802.1x protocol standard using the Extensible Authentication Protocol (EAP) to securely authenticate the wireless user. The 802.1x protocol offers an effective mechanism for authenticating and passing authenticated traffic through the access point, and works in conjunction with either Extensible Authentication Protocol - Transport Layer Security (EAP-TLS) or Extensible Authentication Protocol - Tunneled Transport Layer Security (EAP-TTLS). This is significantly

better than WEP in that the encryption key is dynamic and can be changed on a varying basis before an attacker can hack the encryption key (Geier, 2002).
2. Virtual Private Network (VPN) technologies utilizing IP Security (IPSEC) to provide secure encryption for WLAN users.
3. Tiered security architectures providing levels of security for student, vendor, and faculty/staff access to WLAN resources.

*Section 7- Installing the District Office WLAN*

Once the District Office perimeter firewall was in place, and our routers and switches had been upgraded, work on deploying the Wireless LAN began. Our goal was to implement access to Internet resources only via the WLAN at the District Office, and not allowing any access to internal resources that were not already available via the Internet.

We had discussed several methods of deploying a WLAN that would allow Internet access only to WLAN clients, those options included:

1. Using a VLAN on a firewall DMZ to segment the WLAN from the internal network, and using WEP and MAC filtering to secure this access.
2. Adding a wireless VLAN to the firewall DMZ to segment the WLAN from the internal network, and tunnel IPSEC through a VPN connection to gain Internet access.

It was decided to go with the higher level IPSEC tunneling and VPN connection to encrypt this data. Our desire to be good Internet neighbors helped foster this decision. The training at SANS definitely formed our opinion on using VPN and IPSEC, even though we are limiting access to the Internet only. According to the SANS GSEC curriculum, to protect the 802.11 network one should use end-to-end encryption at the higher protocol layers and provide a secure authentication scheme (Cole, et al. 6-35). If we chose option one there was the possibility that a hacker could crack our WEP, gain access to the wireless network and launch an attack on someone else's Internet site.

We have deployed two Cisco Aironet 340 Series Direct Sequence Spread Spectrum (DSSS) bridges set up as access points. The first access point was setup on the third floor of our building and the second access point was setup on the sixth floor. The access points' signal on our third floor also covers the first through fourth floor of our building, with very few dead spots. Our access points' signal on the sixth floor provides acceptable coverage for the fourth through sixth floors. We placed our access points in the central point of our building as the signal radiates in a circular fashion and we wanted to limit signal bleed to the outside parking lot. The signal from our access point can be detected up to 200 feet on the perimeter of our building.

These two access points have been placed in their own VLAN that hang off the firewall DMZ designated for WLAN access only. We have setup a VPN access on our PIX firewall that uses IPSEC to tunnel traffic that will access only the Internet. Any user requiring WLAN access will need to pass their equipment through the IT department for setup to access the WLAN resources. The following steps were used to configure the WLAN at the District Office;

1. Establish a private IP addressing scheme for the WLAN.
2. Configure the switch ports required to the WLAN VLAN.
3. Connect the Ethernet interface on the PIX firewall to the switch port designated to the WLAN VLAN.
4. Configure the Cisco access point.
5. Use the Cisco PIX Device Manager (PDM) to configure the VPN access with IPSEC tunneling on the PIX firewall.
6. Test access with and without the VPN client.

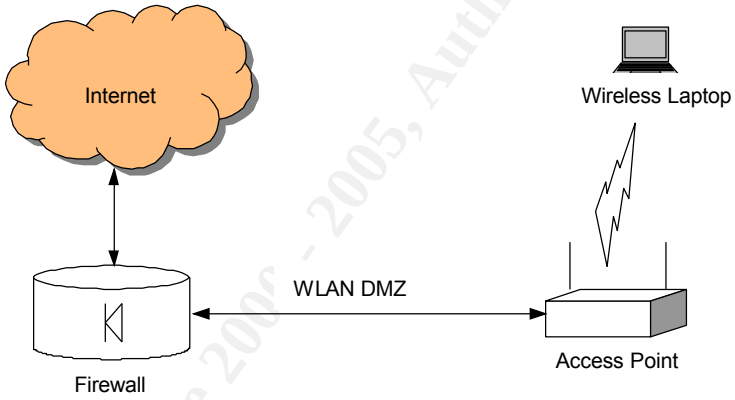


Figure 1-1 District Office WLAN – Internet Access Only

*Section 8 – PIX Firewall Code*

We utilized the Cisco PDM to setup the VPN using IPSEC, and then worked from the PIX command line interface to generate our firewall ACL for our wireless network. Below is sample code from our PIX firewall. Please note that the content has been sanitized with generic IP addressing indicated by an IP octet containing "x" and generic group naming. This is sample code intended to aid the reader with configuring the PIX firewall interface. Remarks have been added to ease the readers understanding for the following code. Code for DHCP has been added to the firewall, but not implemented at this time. Usage of the WLAN resources needs to be metered before arriving at a decision to implement DHCP on the wireless network. At this time all wireless usage is coming from dedicated systems used for a mobile training facility.

*Firewall ACL
access-list WLAN permit icmp any any
access-list WLAN deny ip any 192.x.x.x 255.255.255.0
access-list WLAN deny ip any 192.x.x.x 255.255.255.0
access-list WLAN deny ip any 192.x.x.x 255.255.255.0
access-list WLAN deny ip any 192.x.x.x 255.255.255.0
access-list WLAN deny ip any 10.0.0.0 255.0.0.0
access-list WLAN permit ip 10.x.x.x 255.255.255.x any
access-list WLAN_cryptomap_dyn_xxx permit ip any 10.x.x.x 255.255.255.x

*IP definition for the WLAN
ip address WLAN 10.x.x.x 255.255.255.0

*IP address pool for DHCP
ip local pool WLAN 10.x.x.x-10.x.x.x

*Redundant PIX firewall
failover ip address WLAN 10.x.x.x

*Definition for outside route
global (outside) xxx 192.x.x.x netmask 255.255.255.255

*NAT definition for WLAN
nat (WLAN) xxx 10.x.x.x 255.255.255.0 x x

*IPSEC Cryptography
crypto ipsec transform-set xxx-xxx-xxx xxx-xxx xxx-xxx-xxx
crypto dynamic-map WLAN_dyn_map xxx set transform-set xxx-xxx-xxx
crypto map WLAN_map xxxxx ipsec-xxxxxx dynamic WLAN_dyn_map
crypto map WLAN_map interface WLAN
isakmp enable WLAN
isakmp policy xxx authentication xxxx-xxxxxx
isakmp policy xxx encryption xxxxxx
isakmp policy xxx hash xxxxxx
isakmp policy xxx group xxx
isakmp policy xxx lifetime xxxxxxx

*VPN definitions
vpngroup xxxxxxxxx address-pool WLAN
vpngroup xxxxxxxxx dns-server 192.xxx.xxx.xxx 192.xxx.xxx.xxx
vpngroup xxxxxxxxx default-domain xxx.xxx
vpngroup xxxxxxxxx idle-time xxxxxx

## Chapter III – State of Enhanced Security on District WLAN

*Section 1 – Enhanced Security on District Network*

The implementation of the perimeter firewall has secured our network from the outside, specifically the Internet. That coupled by the use of NAT to utilize private addressing on our internal network has beefed up our perimeter defenses and goes a long way in supporting what we learned at SANS to provide defense in depth.

The engineers I work with have attended the SANS courses on firewalls, routers and UNIX systems and have used the knowledge gained in these courses to access the risk and vulnerability posed by having no perimeter defenses, and secure our systems following recommendation made by the SANS instructors. The author attended Track-1 SANS Security Essentials and has used knowledge gained at SANS to harden servers and workstations, and deploy the WLAN at the District Office with success.

With the technology in place to support VLANS and VPN connections, segmentation has been realized and remote access has been hardened. Our network has come a long way in a short period of time concerning security, and the elimination of brute force attacks and DOS attacks from our network is testimony of these efforts to secure our network.

*Section 2 – Improvements Associated with the Wireless Committee*

The author feels the greatest benefit realized by forming the Wireless Committee is the depth and breadth of knowledge that has been shared, and the communication that has helped bridge gaps in security. We have a great deal of technical talent in our group and the ability to bounce ideas concerning WLAN implementations, share the results of tests of new WLAN technologies, and share equipment to test ideas and troubleshoot WLAN issues has been a resounding benefit to the technology staff. Communication about future directions concerning WLAN security and forming a cohesive security strategy has helped the district as a whole work together to secure WLAN resources.

*Section 3 – Conclusion; Enhanced WLAN Security*

One issue the Author feels has been of great benefit to his security understanding has been the enlightenment learned at SANS to the security threat of WLAN networks. The author can state without reservation that he was somewhat concerned about WLAN security before attending SANS, and he is now extremely concerned about WLAN security after attending SANS. Learning that the threat is more than just exaggerated as some writers would lead you to believe, and obtaining first hand information on tactics used by hackers from both the SANS curriculum and from your peers in the class, one benefits greatly

on the topic of security.

Having the WLAN project stalled until technology could be put in place to secure the network is without a doubt one of the wisest directives the author has had to follow. The author shudders when he thinks about our initial plans to deploy the WLAN with nothing more than WEP and MAC address filtering. The author is most grateful to his peers who helped him understand the risk associated with our initial plans, and it was the SANS training that helped his peers form their opinion with such fervor.

We have now placed the WLAN on the network and know that an attacker will not benefit from attempting to hack our WLAN resources. We have tested access to the network assuming the attacker could guess our private IP addressing, and have verified that access to the Internet is not possible without a properly configured VPN client. Because we have blocked all access to our internal network from the wireless DMZ, no access is possible to internal systems even if you had a properly configured VPN client, the only access available with a properly configured VPN client is access to the Internet.

We are comfortable with the IPSEC and Triple DES encryption protocol used by our IPSEC tunnel, and know that this form of encryption is secure. The SANS curriculum clearly articulates the differences between the two modes of IPSEC, Tunnel Mode and Transport mode, and it was this knowledge that help form our preferences (Cole, et al. 3-11). We desired an encryption model that encrypted no only the data packet, but also encrypted the IP header. That desire was fulfilled using the IPSEC Tunnel.

The overall condition of our WLAN at the District Office has been deployed with the desired level of security and privacy required by the security staff. We will continue to refine our security efforts concerning the WLAN infrastructure as technologies mature and funds are made available and we will continue to harden our networks from knowledge gained by attending the SANS seminars.

***References***

Borisov, Nikita, Ian Goldberg, and David Wagner. "Security of the WEP algorithm." January 2001. URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (December 27, 2002).

Caravaggio, Maria. "Understanding Security Issues with Wireless LANs." October 2002. URL: http://www.giac.org/GSEC_2300.php (December 11, 2002).

Cole, E.' et al. "SANS Security Essentials IV: Encryption and Exploits." April 17, 2002.

Geier, Jim. "802.1x Offers Authentication and Key Management." May 7, 2002 URL: http://www.80211-planet.com/tutorials/article.php/1041171 (December 30, 2002).

Karygiannis, Tom, and Les Owens. "Wireless Network Security." URL: http://csrc.nist.gov/publications/drafts/draft-sp800-48.pdf (December 27, 2002).

Macaulay, Tyson. "Hardening IEEE 802.11 wireless networks." February 18 2002. URL: http://www.ewa-canada.com/Papers/Hardening_802.11.pdf (December 22, 2002).

Milner, Marius. NetStumbler. Computer software. NetStumbler.com, Downloaded from URL: http://www.netstumbler.org

The Shmoo Group. AirSnort. Computer software. AirSnort Homepage, Downloaded from URL: http://airsnort.shmoo.com

Walker, Jesse R. "Unsafe at any size; An analysis of the WEP encapsulation." October 27, 2000. URL: http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip (December 27, 2002).

Last Updated: May 28th, 2017

# Upcoming Training


| | | | |
|---|---|---|---|
| SANS Stockholm 2017 | Stockholm, Sweden | May 29, 2017 - Jun 03, 2017 | Live Event |
| SANS San Francisco Summer 2017 | San Francisco, CA | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Security Operations Center Summit & Training | Washington, DC | Jun 05, 2017 - Jun 12, 2017 | Live Event |
| SANS Houston 2017 | Houston, TX | Jun 05, 2017 - Jun 10, 2017 | Live Event |
| Community SANS Ottawa SEC401 | Ottawa, ON | Jun 05, 2017 - Jun 10, 2017 | Community SANS |
| SANS Charlotte 2017 | Charlotte, NC | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | vLive |
| Community SANS Portland SEC401 | Portland, OR | Jun 12, 2017 - Jun 17, 2017 | Community SANS |
| SANS Secure Europe 2017 | Amsterdam, Netherlands | Jun 12, 2017 - Jun 20, 2017 | Live Event |
| SANS Rocky Mountain 2017 | Denver, CO | Jun 12, 2017 - Jun 17, 2017 | Live Event |
| SANS Minneapolis 2017 | Minneapolis, MN | Jun 19, 2017 - Jun 24, 2017 | Live Event |
| SANS Columbia, MD 2017 | Columbia, MD | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS Cyber Defence Canberra 2017 | Canberra, Australia | Jun 26, 2017 - Jul 08, 2017 | Live Event |
| SANS Paris 2017 | Paris, France | Jun 26, 2017 - Jul 01, 2017 | Live Event |
| SANS London July 2017 | London, United Kingdom | Jul 03, 2017 - Jul 08, 2017 | Live Event |
| Cyber Defence Japan 2017 | Tokyo, Japan | Jul 05, 2017 - Jul 15, 2017 | Live Event |
| SANS Cyber Defence Singapore 2017 | Singapore, Singapore | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Minneapolis SEC401 | Minneapolis, MN | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Los Angeles - Long Beach 2017 | Long Beach, CA | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Community SANS Phoenix SEC401 | Phoenix, AZ | Jul 10, 2017 - Jul 15, 2017 | Community SANS |
| SANS Munich Summer 2017 | Munich, Germany | Jul 10, 2017 - Jul 15, 2017 | Live Event |
| Mentor Session - SEC401 | Ventura, CA | Jul 12, 2017 - Sep 13, 2017 | Mentor |
| Mentor Session - SEC401 | Macon, GA | Jul 12, 2017 - Aug 23, 2017 | Mentor |
| Community SANS Atlanta SEC401 | Atlanta, GA | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| Community SANS Colorado Springs SEC401 | Colorado Springs, CO | Jul 17, 2017 - Jul 22, 2017 | Community SANS |
| SANSFIRE 2017 | Washington, DC | Jul 22, 2017 - Jul 29, 2017 | Live Event |
| SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style | Washington, DC | Jul 24, 2017 - Jul 29, 2017 | vLive |
| Community SANS Charleston SEC401 | Charleston, SC | Jul 24, 2017 - Jul 29, 2017 | Community SANS |
| Community SANS Fort Lauderdale SEC401 | Fort Lauderdale, FL | Jul 31, 2017 - Aug 05, 2017 | Community SANS |
| SANS San Antonio 2017 | San Antonio, TX | Aug 06, 2017 - Aug 11, 2017 | Live Event |
| SANS Prague 2017 | Prague, Czech Republic | Aug 07, 2017 - Aug 12, 2017 | Live Event |