Interested in learning more about security?

SANS Institute InfoSec Reading Room

Penetration Testing on 802.11b Networks

The Institute of Electrical and Electronics Engineers (IEEE) created the 802.11b Standard to provide a secure architecture for communicating with networking devices over an air medium but the standard has fallen short in providing a secure criterion. The 802.11b Standard has left many doors open for hackers to exploit these shortcomings and the goal of this document is to surface these issues while illustrating how to prevent them. A technique of attacking wireless networks that hackers have dubbed as "WarDriving" is b...

SANS GSEC Practical Assignment

Penetration Testing On 802.11b Networks

Worldwide Services
The knowledge behind the network

Lucent Technologies
Bell Labs Innovations

Prepared By:	Benjamin S. Huey
Assignment Version:	GSEC Practical Assignment (v.1.3)
Assignment Title	Penetration Testing On 802.11b Networks
Assignment Date:	February 6, 2003

TABLE OF CONTENTS

1.0 Executive Summary

The Institute of Electrical and Electronics Engineers (IEEE) created the 802.11b Standard to provide a secure architecture for communicating with networking devices over an air medium but the standard has fallen short in providing a secure criterion. The 802.11b Standard has left many doors open for hackers to exploit these shortcomings and the goal of this document is to surface these issues while illustrating how to prevent them.

A technique of attacking wireless networks that hackers have dubbed as "WarDriving" is becoming an everyday buzzword in the security industry. This document will cover the fundamentals on how to deter a WarDriving attack by performing controlled penetration tests on a wireless network. These fundamentals will consist of an overview of 802.11b security, how to exploit its vulnerabilities and will conclude with how to thwart attackers from gaining access to the wired network.

2.0 Wireless 802.11b Security

The IEEE tried to devise a security model for the 802.11b Standard that would allow for mobile clients to securely authenticate & associate to an Access Point (AP) and provide a way to maintain data confidentiality.

2.1 Security Defense Mechanisms

Many hardware vendors have devised proprietary solutions to handle the deficiencies of the 802.11b Standard but they are out of the scope of this document and will not be discussed. The 802.11b Standard has two basic security defense mechanisms. These two mechanisms are:

- SSID
- WEP

2.1.1 SSID – Network Name

A Service Set Identification (SSID) is basically the network name of a Wireless LAN (WLAN) segment and it is supposed to logically segment the users and APs. Theoretically, the client's wireless Network Interface Card (NIC) should be configured with the same SSID as the AP in order to join the network.

2.1.1 Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) was designed by the IEEE to bring WLAN security to a level comparable to a wired networking environment such as a Local Area Network (LAN). WEP uses a security feature widely used throughout the security industry known as encryption.

WEP's encryption process uses a symmetric key and a mathematical algorithm to convert data into an unreadable format called cipher-text. In cryptography, a symmetric key is a variable length value used to encrypt or decrypt a block of data. Any device desiring to participate in the symmetric encryption process must possess the same key. WEP keys are configured by the WLAN administrator and the larger the key, the harder it will be to break the encryption cipher.

RC4 is the encryption algorithm used by WEP and it needs the assistance of an Initialization Vector (IV). An IV is a pseudo-random binary string used to jump-start the encryption process for algorithms that depend on a previous sequence of cipher-text blocks. A smaller IV in conjunction with keys that do not frequently change will increase the changes that encrypted data packets with duplicate the IV.

WEP consists of up to four variable length symmetric keys based on the RC4 stream cipher. All keys are static in nature and are common to all devices on the WLAN. This means that the WEP keys are manually configured on the WLAN devices and will not change until the administrator configures different keys. Most 802.11b equipment comes with two key sizes. The two key sizes are shown below.

- 64-bit 40-bit Key and a 24-bit Initialization Vector
- 128-bit 104-bit Key and a 24-bit Initialization Vector

Nonetheless, the static nature of the WEP keys and the small initialization vector combine to create a massive problem in both scalability and security. These are all IEEE standards problems but as stated earlier, many hardware vendors have created proprietary solutions. There are two main purposes of WEP and they can be seen below.

1) Deny WLAN Access
2) Prevent Replay Attacks

An AP will use WEP to prevent WLAN access by sending a text challenge to an end user client. The client is supposed to encrypt the challenge with their WEP key and return it back to the AP. If the results are identical, the user is granted access.

WEP also prevents replay attacks. This is where an attacker will try to decode sniffed data packets. If the intruding WLAN user manages to capture WEP encrypted 802.11b frames out of the air, the attacker will not be able to decode the packets unless they possess the proper WEP key to decrypt the data.

2.2 Authentication and Association

In order for a wireless client to have access to a WLAN, the 802.11b Standard indicates that the client must go through two processes. These two processes are known as the:

- Authentication Process
- Association Process

Once the wireless client has successfully completed the authentication and association processes, the end user will be given access to the WLAN.

2.2.1 Authentication Process

A wireless client that desires access to a WLAN must first undergo the authentication process. This authentication process validates information about the client and is the initial step in connecting with the wireless AP. The authentication process consists of two types of authentication:

- Open System Authentication
- Shared Key Authentication

With Open System Authentication (OSA), all negotiation is done in clear text and it will allow a client to associate to the AP without possessing the proper WEP key. The only thing that is needed is the proper SSID. Some APs will even accept a null SSID. An AP can be configured for OSA but still be configured for WEP data encryption. So if a client does properly associate to the AP, the client will be unable to encrypt or decrypt data it receives from the AP.

In contrast to OSA, Shared Key Authentication (SKA) forces the AP to send a challenge text packet to the wireless client. The client in turn, will encrypt the challenge text with its WEP key and send it back to the AP. The AP will then decrypt the challenge and compare it to the original text sent. If the two match, the AP will allow the client to associate with it.

2.2.2 Association Process

The Association Process is the course of action in which a wireless client pursues a connection with an AP. The Association Process is the final step in connecting to a wireless AP.

2.2.3 Authenticated and Associated

The 802.11b Standard indicates that the client must first authenticate to the AP and then it must associate to the AP. The standard also specifies that these two aforementioned processes will make up one of three states in the sequence joining a WLAN through an AP. The three states are:

- State 1: Unauthenticated and Unassociated
- State 2: Authenticated and Unassociated
- State 3: Authenticated and Associated

Unauthenticated and unassociated is the initial state of an AP and a client. Once a client has completed the authentication process but has yet to complete the association process, the client is considered to be in the second stage known as authenticated and unassociated. After the client successfully associates to an AP, the client has completed the final state and is considered to be authenticated and associated. The client must be authenticated and associated with an AP before access to a WLAN is granted. There are three phases in the development of a client becoming authenticated and associated to an AP. The three phases that make up this state are:

- Probing Phase
- Authentication Phase
- Association Phase

Probing Phase

A wireless client will send a probe request packet out on all channels and any AP that is in range of the client will respond with a probe response packet. These AP probe response packets contain information that the client will use in the association process.

Authentication Phase

As stated earlier, the authentication phase can use either OSA or SKA. The configuration of the AP will dictate which type of authentication is used. For the most secure WLAN environment, it is highly recommended to go with SKA authentication.

In the OSA scheme, a client will send an authentication request packet to the AP. The AP will analyze the authentication request packet and send an authentication response packet back to the client stating whether it is allowed to move onto the association phase.

In the SKA scheme, a client goes through the same process as with OSA but the AP sends a challenge text to the client. As stated earlier, the client will take this challenge and use its static WEP key to encrypt the text. Once the client sends it back to the AP, the AP will then decrypt the challenge with its static WEP key and compare it to the original text sent. The AP will allow the client to move on to the association phase if the text was properly decrypted but if the AP found the text to be contradictory, it will prevent the client from accessing the WLAN.

Association Phase

In the association phase, the client will send an association request packet to the AP. The AP will send an association response packet back to the client stating whether the client will be allowed to have access to the WLAN. The "Authenticated and Associated" state is the final negotiation step between an AP and a wireless client. If there are no other security mechanisms (RADIUS, EAP, or 802.1X) in place, the client will have access to the WLAN.

3.0 Preparing for Penetration Testing

There is not a lot to do to prepare for penetrating a WLAN. All network sniffing and penetration testing documented in this report was conducted with the following hardware set up:

- Dell Latitude CPH 850 MHz Laptop with 256 MB RAM
- Microsoft Windows XP Professional Operating System
- Lucent Technologies WI-FI Orinoco Gold 11 Mbps NIC

In order to conduct a penetration test on a WLAN; all necessary materials must be collected, installed and configured. Preparing for a wireless penetration testing consists of two steps and can be seen listed below:

- Installing the Orinoco Gold NIC
- Setting Up Wireless 802.11b Sniffers

3.1 Installing the Wireless NIC

Installing the wireless NIC is an particularly important stage. A wireless NIC that is not correctly installed and configured will not be capable of taking advantage of all WarDriving tricks documented throughout the body of this report. A properly installed Orinoco Gold NIC has two major features that a normal Orinoco Gold NIC doesn't. These two features are:

1) Promiscuous network sniffing
2) Ability to change the MAC address

The NIC should be inserted into the Laptop's PCMCIA slot and Windows XP will install its own drivers for the adapter. As a best practice, the PC should be rebooted after installing each driver. The default drivers that Windows XP installs are inadequate for the purposes of WarDriving and need to be hacked with special versions of software & firmware. This process must be carried out in a precise sequence.

First, an older version of drivers and firmware (R6.4winter2001) [i] must be installed from the OrinocoWireless.com or WaveLan.com FTP sites. This is what will allow the NIC to have its Media Access Control (MAC) address manually configured to a custom setting. The drivers will update the firmware and software to:

- Orinoco Station Functions firmware Variant 1, Version 6.16
- NDIS 5 Miniport driver Variant 1, Version 6.28
- Orinoco Client Manager Variant 1, Version 1.58

Once the firmware and software have been updated, a final patch can be applied to the Orinoco NIC. A WildPackets AiroPeek [ii] driver is a hacked version of the Orinoco Gold NIC driver that will allows the NIC to sniff promiscuously. Once this driver is properly loaded, the NIC is fully operational for WarDriving.

3.2 Setting up Wireless 802.11b Sniffers

There are several 802.11b Sniffers [iii] that can sniff 802.11b frames out of the air. This document only addresses free solutions, as opposed to expensive commercial products. The two sniffers used in this exercise are WinDump and Ethereal.

WinDump and Ethereal were originally UNIX utilities that relied on libpcap, but they have been ported to Win32. In order for the Win32 ports to work, WinPCap [iv] must be loaded before the

sniffers can pick up traffic. WinPCap is a Win32 version of the libpcap UNIX utility. As of the writing of this document, WinPCap 2.2 does not work with Windows XP; therefore it is necessary to run the beta 2.3 version of WinPCap. After WinPCap has been loaded, WinDump and Ethereal are ready to install.

WinDump is a simple application that is run from a command prompt. Once WinDump has been downloaded, it should be copied to the < %SystemRoot%\system32 > directory so that it can be run from any command prompt. WinDump is good for generating raw packets.

As for Ethereal, it has a GUI that is far more advanced than WinDump. Install Ethereal into a directory of you choice and it is ready to go. Ethereal is good for looking at packets in a decoded mode and is much easier to view packets.

3.3 Sniffers for Cracking WEP

The aforementioned sniffers are only good for sniffing when the client is associated to the AP and for 802.11b frames that are not encrypted with WEP. In a situation where an AP is using a WEP key to cipher its data, it will be necessary to use a different type of sniffer.

AirSnort, [v] a UNIX utility, is a special type of sniffer that will crack the APs WEP key. AirSnort must be run long enough to collect between 500 Megabytes to 1 Gigabyte of traffic in order to retrieve the key. This can take a few hours or significantly longer, based upon network traffic. AirSnort exploiting the undersized 24-bit IV, so it makes no difference if the WEP key is 64-bit or 128-bit.

WEPcrack [vi] is a script that can be run against a raw capture file created by Ethereal and it too must also be run on a UNIX system. Ethereal packet captures can be exported to a file and WEPcrack can be used to devise the static WEP key.

The fact that this document is utilizing Windows XP for the penetration test, it is presumed that another laptop running Linux and compiled with either AirSnort or WEPcrack has already cracked the WEP key. Once the WEP key is known, an AP can be treated as any other.

4.0 WarDriving for WLANs

In order to penetrate a WLAN, an AP must be located. APs are devices that use Radio Frequency (RF) transceivers in the 2.4 GHz range to connect end users in the same RF range. APs bridge wireless end users to the wired network, and are often located BEHIND the firewall. Cheap APs or improperly configured APs broadcast frames that contain information about the WLAN and hackers have built utilities to exploit this information. One such hacker utility is called NetStumbler. [vii] A laptop armed with NetStumbler will allow intruders to sniff the air for 802.11b frames with the convenience of driving around in their car.

4.1 Locating an Access Point with NetStumbler

NetStumbler will log information when it passes within the range of an AP, which is approximately 1-350 feet. NetStumbler is supposed to alarm when it sees an AP, but it was not created with XP in mind. However, NetStumbler can be made to annunciate an alarm in Windows XP by taking any desired < .wav > file and renaming it to < ir_begin.wav >, then placing the file in the Windows XP < %SystemRoot%\Media > directory. If the root directory does not contain a subdirectory named media, just create one and place the < ir_begin.wav > file there.

Once NetStumbler is executed, it starts sending out broadcast probes at a rate of once per second. If any APs respond to the probe, NetStumbler will alarm and report information extracted out of the 802.11b frames such as SSID, MAC address, channel, signal strength and whether WEP is on. NetStumbler can also be configured to use a GPS to locate the global position of an AP. This is very convenient for pinpointing a certain AP when NetStumbler has discovered many APs in a general area. A typical NetStumbler session can be seen below in Figure 1.

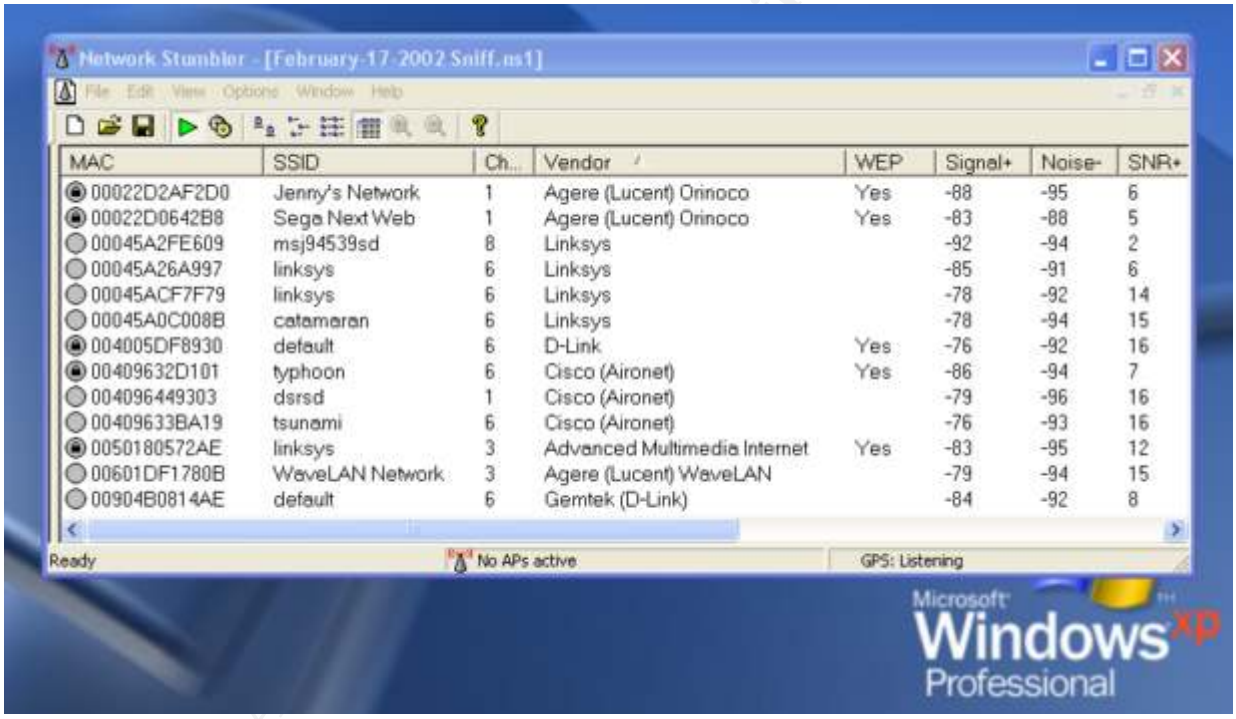

Figure 1: NetStumbler Locating Access Points

NetStumbler is only effective if the AP is responding to broadcast probes and can be made obsolete if the AP is configured to not broadcast the SSID. Many hardware vendors have solutions that can resolve broadcasting issues ranging from shutting off the broadcast to negotiating a broadcast encryption key. It is highly recommended to prevent an AP from broadcasting unless it is encrypted.

5.0 Penetrating the WLAN

Now that an AP has been located, it is time to gather information to see if the AP is vulnerable and welcomes hackers into the LAN. This is where "Penetration Testing" comes into effect on a WLAN segment.

5.1 Scoping Out the IP Scheme

Some WLAN administrators will set up a DHCP server for the WLAN segment that will assign a wireless NIC an IP address and gateway. If this is the case, an attacker has already successfully gained access to the network. There is nothing more for an attacker to do than begin scanning the network.

If the laptop and wireless NIC are *Associated* to the AP (Layer 2) but do not have an assigned IP address (Layer 3) for the local WLAN segment, they cannot participate on the TCP-IP WLAN. In order to have routing privileges or Internet connectivity, the wireless NIC needs a layer 3 IP address and default gateway. Gaining an IP address can be accomplished with Ethereal or WinDump by sniffing the air medium for packets containing the vital IP information.

5.2 Gaining Layer 3 Network Access

The Ethereal GUI can be used to import packets picked up by the Orinoco Gold NIC and decode them for easy viewing. WinDump can be used for the same purpose but it works in a command prompt and visually shows all packets received by the Orinoco Gold NIC as they enter the interface. This will reveal source and destination IP addresses of devices on the WLAN segment.

WinDump can be made to use a specific adapter interface and even dump output to a file. The interface that WinDump is to sniff must be represented by the registry string settings for the desired NIC interface. These wireless NIC registry settings can be conveniently found in Ethereal by hitting "Ctrl – K" and copying the text in the "Interface" box for the desired NIC. Here is an example command which allows WinDump to sniff an interface and dump its output to a file called WarDrive.txt.

```
C:\ > windump -i \Device\Packet_{BAC2F63F-45D5-4AC3-9C3C-73E0ADAE054D} >> WarDrive.txt
```

After the necessary IP information has been uncover by WinDump or Ethereal, it can be easily applied to the wireless NIC. This fully arms the laptop with a connection to the WLAN and an IP stack to route on the WLAN segment. As can be imagined, this will cause all kinds of problems for an administrator.

Once there is an *Association* with the AP and a proper IP address & subnet mask assigned to the wireless NIC, an attacker can start to probe the network for further layer 3 information. In order to move from the local WLAN segment to other parts of the network, it is necessary to find the nearest gateway router. This can be done with a quick ping scan of the local segment.

Rhino9 Pinger v1.0 [viii] is an application that can ping an entire subnet, ping a specific range of IP addresses, and locate all ICMP enabled devices on the WLAN segment. This utility will also

resolve the hostnames of the pinged devices. This is very beneficial when it comes to locating the gateway router. If it is not evident which device is the gateway router, just begin to try various IP addresses for the laptops gateway.

A better way to detect the gateway is to scan the newly discovered IP addresses with Nmap [ix] and selecting Operating System (OS) detection. Once a router IOS shows up, try the device IP as the laptop gateway. After the gateway router is found and the laptop is configured, verify the IP stack is correct by entering < ipconfig /all > in a command prompt.

If the gateway router has a connection to the Internet, then the laptop also has WWW access. This, of course, is only true if there are no firewalls behind the router or a router Access Control List (ACL) to prevent egress to the Internet or other parts of the network. An intruder that has access to the Internet can use the WLAN to download other hacking tools and perform attacks on the local network. The intruder can also attack other networks on the Internet disguising their conduct as the penetrated WLAN.

5.3 Problems WLAN Hackers Cause

Now that there is full access to the LAN and Internet, an attacker is free to exploit the network for any vulnerabilities or misconfigurations. Nmap is also a terrific port scanner for verifying what ports are open on the discovered IP addresses. This will tell the attacker what type of OS is running, what services are running and what exploits should be conducted next.

For example; let's say the attacker has discovered that the LAN consists of NT Servers. Unless properly configured, the NT machines will allow "Null Sessions" with their IPC$ shares. By establishing a null session with an NT machine, an intruder can extract extremely critical information from the NT network. Such information can include the Domain name, PDC & BDC info, share names and user accounts. A null session can be achieved by issuing a "Net Use" command with an empty password in an ordinary command prompt. Here is an example:

C:\>net use \\192.168.0.1\IPC$ "" /u:""

Once a Null Session has been executed successfully, an attacker can use hacking tools like NetBIOS Auditing Tool (NAT) [x] to find remote name tables and even crack passwords. NAT allows an intruder to extract various user account information from an NT Server and perform password attacks. This is done by using the extracted usernames to devise username and password dictionary files. If an account is set up with a weak password or no password at all, NAT could possibly compromise a user account or even an administrator's account. This is an extremely common situation and has very serious repercussions. An example of a typical null session being executed in conjunction with a NAT attack on a Windows NT server can be seen below in Figure 2.

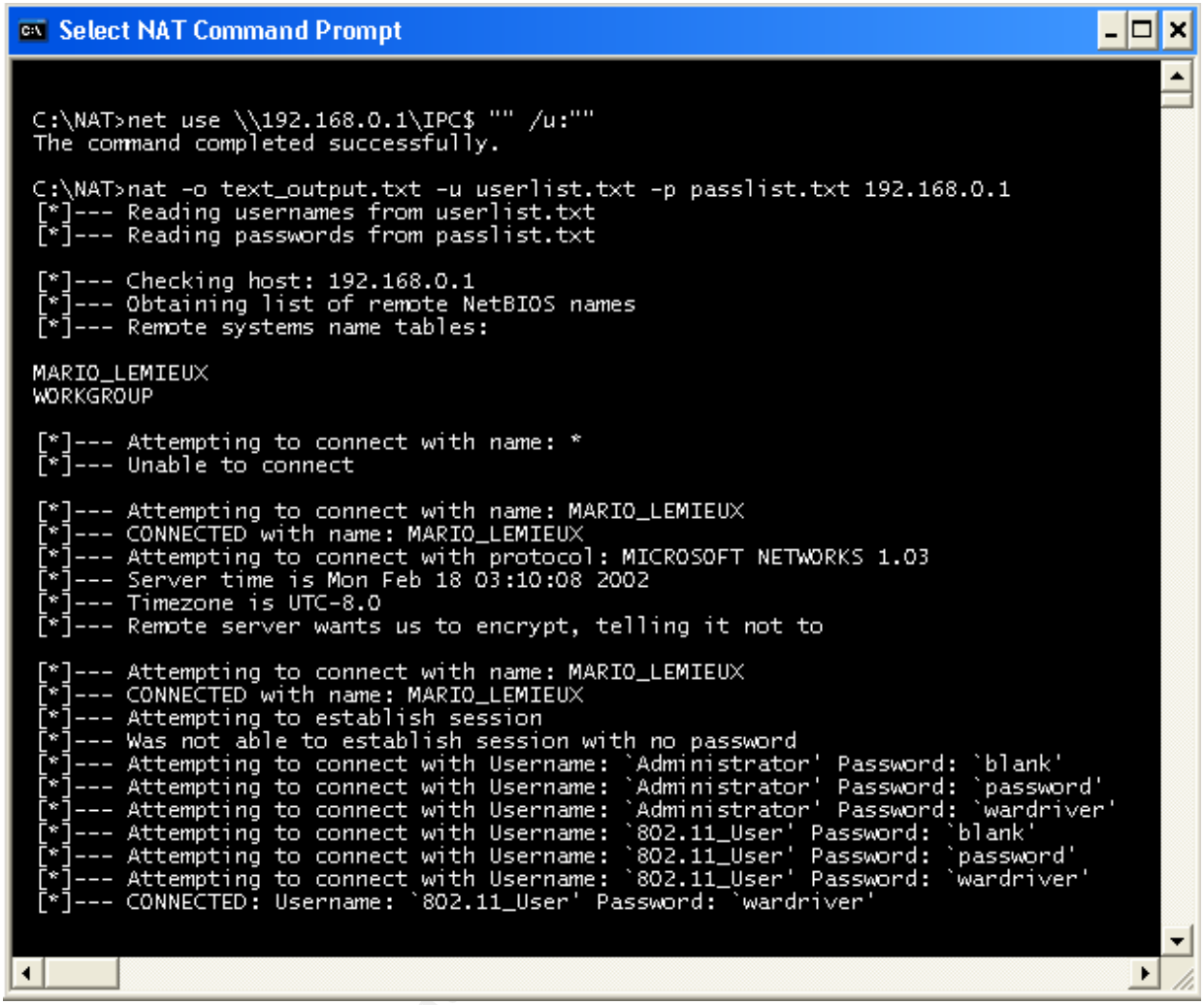

Figure 2: Executing a Null Session and NAT on an NT machine

There is a fair chance that NAT will be able to exploit an administrator's password, which will grant the attacker administrative rights for the NT domain. Administrative rights on a domain, in turn, give the hacker the ability to attach to any Microsoft Window machine on the domain or any trusted domain. This includes a range of abilities from deleting Windows NT user accounts to taking a domain controller off line. In short, the attacker is now the networks new and unethical administrator.

L0phtCrack 3.0 (LC3) [xi] is a utility that will crack encrypted Windows NT passwords. With the newly acquired administrative rights, a hacker will be able to connect to the PDC with LC3 and withdrawal ALL users accounts and crack ALL passwords on the NT Domain. LC3 is a favorite among hackers and is one of the best password cracking utilities available today. As can easily be seen, once a hacker has compromised the PCD Security Account Manager (SAM), the NT domain is at the will of the intruder. An example of LC3 is depicted in Figure 3 below.

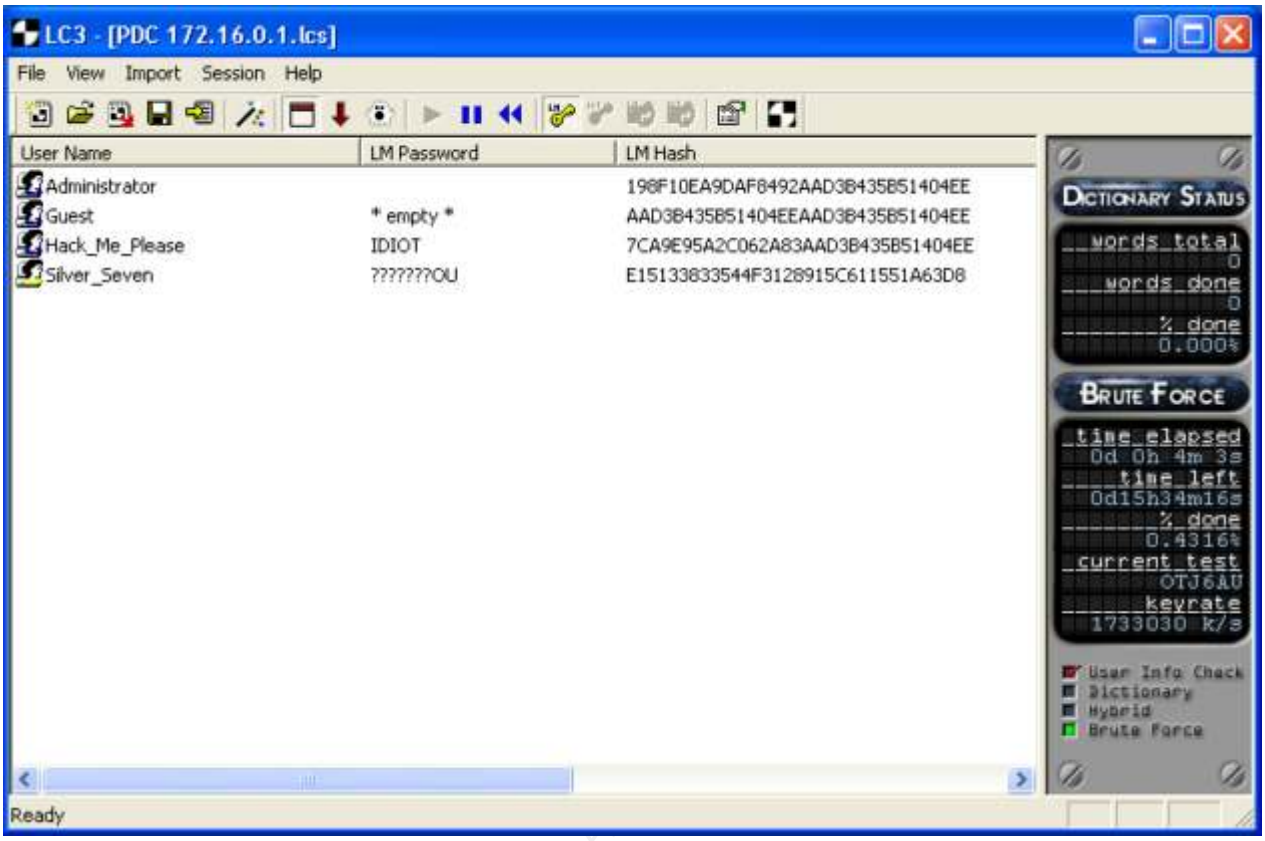

Figure 3: LC3 Cracking PDC Users Accounts

6.0 Security Recommendation

The best way to prevent the issues covered in this document is to have security on the mind when designing and implementing the network. Once the network is properly designed and implemented, it is necessary to have policies in place so it remains secure. The two types of security concerns that have been addressed in this document are:

- WLAN Security
- Wired Network Security

6.1 WLAN Security

As for security on the wireless segment, the WLAN should be regarded as the public Internet and all traffic should be treated as subject. A list of security recommendations to help prevent several vulnerabilities discussed in this document can be found on the next page.

1) Purchase WLAN products that have proprietary security mechanism to overcome the shortcomings of the 802.11b security standards. Many hardware vendors are creating APs that utilize per user and per session WEP keying along with per packet authentication.

2) Install RADIUS servers on the wired LAN to aid in the authentication process of WLAN users. Extensible Authentication Protocol (EAP) can be used in conjunction with 802.1X to block traffic to the wired LAN until the RADIUS server has authenticated the WLAN user.

3) Place a firewall in front of the AP so all traffic to the wired LAN can be filtered and screen for malicious activities. All services not being utilized should be disabled and logging should dump to a SysLog Host located in a Demilitarized Zone (DMZ). The SysLog Host will log all incoming traffic and act as a first line of defense in detecting attacks aimed at the router & firewall interfaces. It is also recommended to implement an Intrusion Detection System (IDS).

4) Utilize VPN technologies to ensure proper confidentiality, authentication, integrity and non-repudiation of all WLAN usage. This type of environment can incorporate both hardware and software solutions that provide a minimum-security standard of:

- IKE – 3DES, SHA-HMAC, DH Group 2 and preshared key
- IPSec – 3DES, SHA-HMAC, no PFS and tunnel mode.

6.2 Wired Network Security

Wired network security consists of the same "good old-fashion" policies that should be followed every day. It is a best practice to lock down everything, check all IDS logs and keep a constant eye on any up and coming exploits. Located below is a brief list of recommendations to help prevent issues that were outlined in this document.

1) All Domain Controllers should make use of the S/Key [xii] utility located in Windows NT Service Packs 3 and greater. This utility prevents attackers from remotely retrieving usernames & passwords from domain controllers with LC3.

2) Microsoft has created several Security Checklists [xiii] on how to tighten up and lockdown a Windows NT Domain along with all of it Workstation and Servers. They consist of several stringent documents and it is highly recommended to complete these Checklists on all the NT nodes in the domain.

3) It is a best practice to insure all machines have the latest HotFixes applied. To assist in the mass deployment of HotFixes on all the Windows NT machines in the domain, QChain [xiv] can be used. QChain is an application that allows multiple HotFixes to be executed on a computer without multiple reboots.

4) Microsoft Windows NT accounts with no passwords, passwords that are the same as the username and generally weak passwords should be prevented. This can be done by loading the Windows NT User Manager and changing the password to something more secure such

as a combination of letters, numbers and alphanumerical characters. Consider implementing a password filter such as passfilt.dll [xv] to enhance password security.

5) A switch or router with no password or even a weak password will give an attacker freedom into the network. A weak password can be cracked in a matter of seconds by many different software applications or scripts such as Cisco Auditing Tool.[xvi] Once an attacker gains access to the password, they can configure the network to route or switch traffic at will. The administrator should change the password to something very difficult such as a random combination of letters, numbers and alphanumerical characters.

6) The perimeter routers should be configured with very strict granular ACLs that will disable all unnecessary services and put anti-spoofing measures in place. This is absolutely crucial to the security of a network. All routers should also be configured with a banner warning hackers to stay out of the network. This is important for legal reasons because it will act as an official warning. Too many hackers get off by playing stupid.

7.0 Appendix A – Wireless Resources

A.1 Cisco Wireless Technology and Security

Securing the Wireless LAN

< http://www.cisco.com/warp/public/784/packet/jul01/p74-cover.html >
< http://www.cisco.com/warp/public/784/packet/jul01/pdfs/p74-cover.pdf >

Cisco Wireless Technical Tips and Product Literature

< http://www.cisco.com/warp/public/102/ >
< http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/ >

Overview Wireless LAN Security

< http://www.cisco.com/warp/public/102/wlan/nextgen.html >
< http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm >

Comments on Recent Security Paper from Universities of Berkeley, Maryland and Rice

< http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1281_pp.htm > Berkeley

< http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1327_pp.htm > Maryland
< http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515_pp.htm > Rice

Configuring Wired Equivalent Privacy (WEP)

< http://www.cisco.com/warp/public/102/wlan/confwep.html >

Cisco TAC's Top Wireless Issues

< http://www.cisco.com/warp/public/102/ >
<http://www.cisco.com/warp/public/102/top_issues/wireless_lan/top_issues_wireless_lan.shtml>

A.2 Wireless Security Research Sites

< http://www.cs.umd.edu/~waa/wireless.html >
< http://www.drizzle.com/~aboba/IEEE/ >

A.3 WEP Vulnerabilities

Jesse Walker created a document on WEP vulnerabilities called "Unsafe at any key size; An Analysis of the WEP encapsulation" and it can be located at:

< http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip >

Maryland University

Scott Fluhrer, Itsik Mantin, and Adi Shamir cracked the RC4 key setup algorithm which results lead to discovery of the WEP key. The document explaining their findings can be found at:

< http://www.cs.umd.edu/~waa/wireless.pdf >
< http://www.cs.umd.edu/~waa/class-pubs/rc4_ksaproc.ps >

Cisco Comments on Recent WLAN Security Paper from University of Maryland

< http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1327_pp.htm >

UC Berkeley

University of California at Berkeley researchers released a document describing WEP problems. This document can be located in the following locations:

< http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf >

< http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html >

Cisco Comments on Recent WLAN Security Paper from University of Berkeley

< http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1281_pp.htm >

Rice University

The FMS attack can uncover a WEP key in approximately 500 MB to 1 GB worth of data. This is the weakness that AirSnort exploits. The document can be viewed at the following location:

< http://www.cs.rice.edu/~astubble/wep/ >

Cisco Comments on Recent WLAN Security Paper from University of Berkeley

< http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1515_pp.htm >

8.0 Document References

[i] Orinoco Gold R6.4winter2001 NIC Drivers

The proper drivers to load and install the Orinoco Gold wireless NIC as described in this document can be found in the following FTP locations. Download and store on a local machines as these sites continually go down and change address locations.

< ftp://ftp.orinocowireless.com/pub/software/ORiNOCO/PC_Card/win_2000/R6.4winter2001 >
< ftp://ftp.wavelan.com/pub/software/ORiNOCO/PC_Card/win_2000/R6.4winter2001 >

[ii] WildPackets AiroPeek Orinoco Gold NIC Driver

The WildPackets driver is a hacked version of the Orinoco Gold NIC driver that was created to allow the card to sniff in a promiscuous setting for AiroPeek. The WildPackets AiroPeek Orinoco Gold NIC Driver can be downloaded from:

< http://www.wildpackets.com/support/hardware/ap_lucent_driver/lucent6.28driver.exe >

[iii] 802.11b Network Sniffers

The sniffers located below can be used to sniff and decode 802.11b packets picked up by the Orinoco Gold wireless NIC. Sniffer Wireless and AiroPeek can be used to sniff the management 802.11b frames put out by the AP. Ethereal and WinDump will sniff the traffic generated by the AP after a successful association with the AP. The utilities can be downloaded from:

WinDump	< http://netgroup-serv.polito.it/windump >
Ethereal	< http://www.ethereal.com/distribution/win32 >
AiroPeek	< http://www.wildpackets.com/products/airopeek >
Sniffer Wireless	< http://www.sniffer.com/products/wireless/default.asp >

[iv] WinPCap For Ethereal and WinDump

WinPCap is a Win32 version of the libpcap UNIX utility. It is need by programs such as Ethereal or WinDump to allow them to run on a Windows OS. WinPCap can be downloaded from:

< http://netgroup-serv.polito.it/winpcap >

[v] AirSnort For Cracking WEP

AirSnort is a Linux utility that will promiscuously sniff 802.11b frames and exploit vulnerability in WEP to retrieve the key. AirSnort must sniff approximately 500 Megabytes to 1 Gigabyte of data to extract the WEP key. AirSnort can be downloaded from the following location:

< http://airsnort.sourceforge.net >

[vi] WEPcrack

WEPcrack, like AirSnort, can be used to crack the weak WEP security mechanisms of the 802.11b standard and derive the static AP's WEP key. WEPcrack is a script that can be executed against an Ethereal export. WEPcrack can be downloaded at the following location:

< http://wepcrack.sourceforge.net >

[vii] WarDriving with NetStumbler

NetStumbler is the ultimate Win32 utility that will detect 802.11b APs by sending probe requests to the AP. It will alarm and log various data about the AP such as WEP, SSID, signal strength and MAC address. NetStumbler works with WLAN adapters that have the Hermes chipset, so it will work fine with the Orinoco Gold NIC. NetStumbler is located at:

< http://www.netstumbler.com >

[viii] Ping Scanning with Rhino9 Pinger v1.0

Rhino9 Pinger is a hacking tool used to located pingable devices located on a given subnet. Not only does Rhino9 Pinger locate the devices but it also resolves the hostname for a given device. Rhino9 Pinger can be downloaded from:

< http://packetstorm.widexs.nl/groups/rhino9/pinger.zip >

[ix] Port Scanning with Nmap

Nmap is the ultimate port scanner for device OS detection and open ports running services. Nmap can also be run in stealth mode by using faked decoy addresses. Nmap can be downloaded at the following location:

< http://download.insecure.org/nmap/dist/nmap-2.54BETA30-win32.zip >

[x] NetBIOS Auditing Tool (NAT)

NAT is a command line utility that can be used to find remote name tables and even crack passwords. NAT can be downloaded from sites such as:

< http://www.ussrback.com/NT/scanners/nat10bin.zip >

[xi] L0phtCrack 3.0 (LC3)

LC3, sold by Foundstone, can grab usernames and passwords in numerous ways ranging from the Microsoft NT SAM file to SMB sniffing on the network media. LC3 can be downloaded from the following location:

< http://www.atstake.com/research/lc3/application/lc3setup02.exe >

[xii] Microsoft S/Key Utility

S/Key is a utility located in the Microsoft NT Service Pack 3.0 and greater. It can be used to ward off LC3 attacks. S/Key is explained in greater detail in the Service Pack documentation and can be downloaded from:

< http://support.microsoft.com/support/servicepacks/WinNT/4.0/SP6a.asp >

[xiii] Microsoft Security Checklists

Microsoft has created several Security Check-Off Lists to tighten up NT product line. Microsoft has made these Security Check-Off lists available to the public in the following locations:

Windows NT 4.0 Server Checklists

< http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/nt4svrcl.asp >

< http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/mbrsrvcl.asp >

Windows NT 4.0 Workstation Checklists

< http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/security/tools/nt4wscl.asp >
< http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/wrkstchk.asp >

Windows Domain Controller Checklist

< http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/dccklst.asp >

NT 4.0 IIS Security Checklist

< http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/tools/iischk.asp >

Microsoft has also implemented a tool called the Microsoft IIS Lock-Down Tool. This tool will lock down the IIS box and give a manageable interface for security on all Web Servers. The Microsoft IIS Lock-Down Tool can be located at the following Internet locating:

< http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32362 >

[xiv] QChain for Microsoft HotFixes

QChain will mass deploy Microsoft Windows NT HotFixes. QChain is explained in further detail and can be downloaded from the following location:

< http://support.microsoft.com/support/kb/articles/Q296/8/61.asp >

[xv] Strong Microsoft Windows NT Passwords

Password randomness enforcer like passfilt.dll will force strong password policies. See details on how to install a password filter DLL at:

< http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/pswd_about_9xm4.asp >

Listed below are a couple more sites that explain how to implement and enforce strong password policies on a Microsoft Windows NT domain.

< http://support.microsoft.com/support/kb/articles/Q161/9/90.asp >
< http://www.microsoft.com/TechNet/prodtechnol/winntas/tips/platinum/ptespass.asp >

[xvi] Cisco Auditing Tool

Cisco Auditing Tool allows an intruder to run a script against a Cisco device and crack weak passwords. This script can be downloaded at the following location:

< http://packetstormsecurity.org/cisco/CiscoAuditingTool-v1.tar.gz >

Last Updated: September 21st, 2017

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Rocky Mountain Fall 2017	**Denver, COUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Baltimore Fall 2017	**Baltimore, MDUS**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
Data Breach Summit & Training	**Chicago, ILUS**	**Sep 25, 2017 - Oct 02, 2017**	**Live Event**
SANS Copenhagen 2017	**Copenhagen, DK**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS London September 2017	**London, GB**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS Oslo Autumn 2017	**Oslo, NO**	**Oct 02, 2017 - Oct 07, 2017**	**Live Event**
SANS DFIR Prague Summit & Training 2017	**Prague, CZ**	**Oct 02, 2017 - Oct 08, 2017**	**Live Event**
SANS Phoenix-Mesa 2017	**Mesa, AZUS**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS October Singapore 2017	**Singapore, SG**	**Oct 09, 2017 - Oct 28, 2017**	**Live Event**
Secure DevOps Summit & Training	**Denver, COUS**	**Oct 10, 2017 - Oct 17, 2017**	**Live Event**
SANS Tysons Corner Fall 2017	**McLean, VAUS**	**Oct 14, 2017 - Oct 21, 2017**	**Live Event**
SANS Brussels Autumn 2017	**Brussels, BE**	**Oct 16, 2017 - Oct 21, 2017**	**Live Event**
SANS Tokyo Autumn 2017	**Tokyo, JP**	**Oct 16, 2017 - Oct 28, 2017**	**Live Event**
SANS Berlin 2017	**Berlin, DE**	**Oct 23, 2017 - Oct 28, 2017**	**Live Event**
SANS Seattle 2017	**Seattle, WAUS**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
SANS San Diego 2017	**San Diego, CAUS**	**Oct 30, 2017 - Nov 04, 2017**	**Live Event**
SANS Gulf Region 2017	**Dubai, AE**	**Nov 04, 2017 - Nov 16, 2017**	**Live Event**
SANS Miami 2017	**Miami, FLUS**	**Nov 06, 2017 - Nov 11, 2017**	**Live Event**
SANS Milan November 2017	**Milan, IT**	**Nov 06, 2017 - Nov 11, 2017**	**Live Event**
SANS Amsterdam 2017	**Amsterdam, NL**	**Nov 06, 2017 - Nov 11, 2017**	**Live Event**
SANS Paris November 2017	**Paris, FR**	**Nov 13, 2017 - Nov 18, 2017**	**Live Event**
Pen Test Hackfest Summit & Training 2017	**Bethesda, MDUS**	**Nov 13, 2017 - Nov 20, 2017**	**Live Event**
SANS Sydney 2017	**Sydney, AU**	**Nov 13, 2017 - Nov 25, 2017**	**Live Event**
SANS London November 2017	**London, GB**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SANS San Francisco Winter 2017	**San Francisco, CAUS**	**Nov 27, 2017 - Dec 02, 2017**	**Live Event**
SIEM & Tactical Analytics Summit & Training	**Scottsdale, AZUS**	**Nov 28, 2017 - Dec 05, 2017**	**Live Event**
SANS Khobar 2017	**Khobar, SA**	**Dec 02, 2017 - Dec 07, 2017**	**Live Event**
SANS Munich December 2017	**Munich, DE**	**Dec 04, 2017 - Dec 09, 2017**	**Live Event**
European Security Awareness Summit & Training 2017	**London, GB**	**Dec 04, 2017 - Dec 07, 2017**	**Live Event**
SANS Austin Winter 2017	**Austin, TXUS**	**Dec 04, 2017 - Dec 09, 2017**	**Live Event**
SANS Frankfurt 2017	**Frankfurt, DE**	**Dec 11, 2017 - Dec 16, 2017**	**Live Event**
SANS Bangalore 2017	**Bangalore, IN**	**Dec 11, 2017 - Dec 16, 2017**	**Live Event**
SANS SEC504 at Cyber Security Week 2017	**OnlineNL**	**Sep 25, 2017 - Sep 30, 2017**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**