SANS Institute
InfoSec Reading Room

iPhone Backup Files. A Penetration Tester's Treasure

In a penetration test it is usually impossible to acquire permission to attack the CEO's cell phone. But what if the CEO's workstation is in scope and the CEO has an iPhone synced with a workstation? What if the CEO's iPhone backup files are resident on this workstation? Would that be in scope? The answer is probably yes. The information that can be gleaned from an iPhone backup file is amazing and extremely useful to a penetration tester. We will discuss how to hunt for possible targets with iPhone backup files using ...

IPhone backup files. A penetration tester's treasure trove?

GIAC (GPEN) Gold Certification

Author: Darren Manners, darrenmanners@manntechcomputersinc.com
Advisor: Rodney Caudle

Abstract

In a penetration test it is usually impossible to acquire permission to attack the CEO's cell phone. But what if the CEO's workstation is in scope and the CEO has an iPhone synced with a workstation? What if the CEO's iPhone backup files are resident on this workstation? Would that be in scope? The answer is probably yes. The information that can be gleaned from an iPhone backup file is amazing and extremely useful to a penetration tester. We will discuss how to hunt for possible targets with iPhone backup files using Wireshark, Tcpdump and Metasploit. This paper will show how to view the contents of the IOS 5 backup file and extract useful information for the penetration test. We will discuss various mitigation techniques and the new IOS5 iCloud initiative and what this means for the future.

1. Introduction

One of the noticeable changes in recent technology history is the emergence of the smart phone. Technological advances in these fields have created devices that have almost the equivalent power and functionality of desktop computers. Apple Computing has become one of the leaders in this field, overtaking Microsoft to become the largest technology business in the world, with a near religious like following. (Huffman, 2010)

Two products that have propelled Apple's fortunes have been the iPad and the iPhone. Both of these devices have the same operating systems (OS). IOS 5.0 is the latest OS from Apple. These devices have been rapidly adopted by business with little regard to the security implications. This paper will concentrate on the iPhone.

The new frontier of smart phones and tablets offer a new and exciting avenue for exploitation. The rapid adoption, lack of corporate policy and open security make the iPhone a promising target. The ease at which iPhone's can connect up to a wireless network or cell network is part of the attraction for end users. Fitting easily into a pocket, the iPhone can be easily concealed in a corporate environment.

Hackers are writing new code to exploit this device. (Goodin, 2011)

Security firms are scrambling to create antivirus/antimalware programs to combat this growing menace. It is just a matter of time before the sophisticated attacks seen against desktops will be launched against iPhones.

Examining how this technology functions gives a penetration tester an edge in exploiting organizations. This paper will examine, in detail, the iPhone backup file. It will examine what files, within the structure of the backup file, would be of interest to the penetration tester. It will look at what tools a penetration tester can use to extract this information from the backup file and how it can be used in a penetration test. The implications of Apple's move from local to cloud backups will be discussed.

Author Name, email@address@manntechcomputersinc.com

2. IPhone background information

Apple's iPhone has always been a source of conversation within the technology community. From the business model Apple enforces to the functionality and style they are rarely out of the news.

2.1. Brief History

The iPhone was first made available to the US on June 27th 2007. (Pogue, 2007) Steve Jobs, the late former CEO of Apple, initially tied the iPhone to AT&T. Subsequent releases contractually allowed Verizon and Sprint users to obtain the iPhone for their networks. Other vendors are used around the world, but this paper will concentrate on the US only.

The initial iPhone was simply called the iPhone and came in 4 GB and 8 GB sizes. Later models were the 3G, 3Gs, 4G and the now latest model, the 4Gs. The 4Gs can now hold a maximum 64 GB of data. ("iPhone 4s," 2011)

For this paper the 16 GB 4G running IOS 5.0 will be used.

Figure 2-1 iPhone 4G

Author Name, email@address@manntechcomputersinc.com

2.2. Jailbreaking

The term jailbreaking refers to the removal of tying the iPhone to a particular cell phone carrier and/or removing restrictions placed on the device. The initial demand for new iPhones was huge. Unless the user had a contract with a cell phone carrier that had an iPhone available, the user was out of luck. The user would have to purchase a new contract with a different carrier. The user could also not install software unless it was obtained through the App store.

Jailbreaking was born of frustration. Jailbreaking allowed users to use the iPhone on different networks and install software not approved by Apple. This was achieved by running a special piece of code on the actual device (Tether free) or running the code on a PC/Mac that is connected to an iPhone. (Tethered) In July 26th 2010 the Library of congress ruled that jailbreaking was exempt from DMCA rules and was not illegal. (Goldman, 2010)

Although Apple has attempted to make this process illegal, so far they have failed to do so. Jailbreaking will void the warranty on the iPhone as it breaks the end user license agreement, but it is not illegal. (Ionescu, 2010)

Jailbreaking software such as Jailbreakme, Cydia or Seas0npass enables the iPhone to be jailbroken. (Omar, 2011) There are a lot of sites that will offer to jailbreak phones. Unfortunately some of these sites are often infected or will download malicious software to the iPhone. (They will not be mentioned in this paper, as I cannot guarantee they will not install malicious software) Usually the end users, believing their actions were illegal in the first place, are reluctant to inform their IT department of any problems. IT departments should have a sound policy in place with regards jailbreaking iPhones.

The other security implication is that users may jailbreak their phone and install software that may contain malicious intent or damage the phone. (Battery drain, unable to do an update and device instability) ("Unauthorized modification of," 2011)

Author Name, email@address@manntechcomputersinc.com

2.3. The App Store

The App store is Apples service side of the iPhone technology. Users can access the App store to obtain software, called Apps, for the iPhone. Apple controls very strictly what applications are available for the iPhone. Developers submit applications for Apple to review and once approved, those applications are available for users to download. Apple maintains strict control over this process to ensure that users get secure and stable applications. Unlike the Android OS, Apple has suffered less from malicious software using this strict model. Some would argue though, that it forces users to jailbreak their phones to use software that was rejected by Apple. ("Publishing an app," 2011)

2.4. ITunes

ITunes 1.0 was originally released in January 9th 2001. Originally called SoundJam MP, it was acquired by Apple in 2000. It is a software program that can be installed on a windows or mac machine. The current version is 10.5. Originally an iPhone end user had to install iTunes to initialize a device. In the new 5.0 IOS, devices no longer have to be connected to a PC, with iTunes installed. End users can now do this directly from the iPhone itself. ("IOS features," 2011)

The iTunes software allows end users to purchase and manage audio/video files. When used with an iPhone it can initialize the device, transfer audio/video and back the device up. It is the backup data that this paper will focus on.

Author Name, email@address@manntechcomputersinc.com

3. How the iPhone backup works

Apple created a very simple way to restore and backup an iPhone. Originally the end user would connect the device to a PC/MAC. If set for automatic backup, each time the device connected it would back up. What data it backed up was dependent upon what the user had selected. The modern iTunes backs up in a very similar way with a few extra options. The new iPhone devices can also backup to Apples iCloud service. This paper will examine both methods and discuss the implications.

3.1.   Local backup

The test phone is my personal iPhone. It has been upgraded from 4.1 OS to the latest 5.0 OS. It is an iPhone 4G. It has been in use for approximately one year, so it should be a good example of a working phone. The iPhone 4G running IOS 5.0 was attached to an Apple Macbook Pro running 10.6.8 OS with iTunes 10.5. (Fig 3-1) It begins to transfer file and data to backup files.
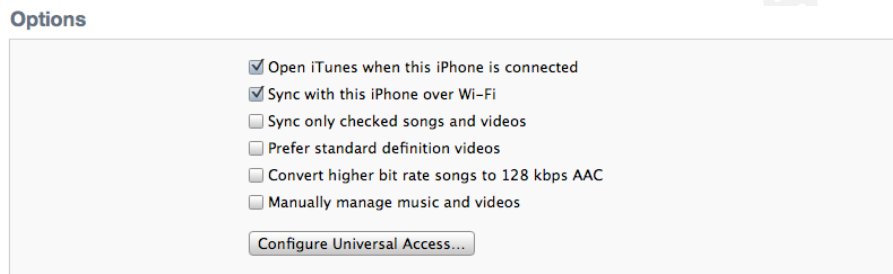

Figure 3-1 Starting the backup

Author Name, email@address@manntechcomputersinc.com

By default the iPhone will backup to the desktop unencrypted. Encryption is an option as shown in Figure 3.
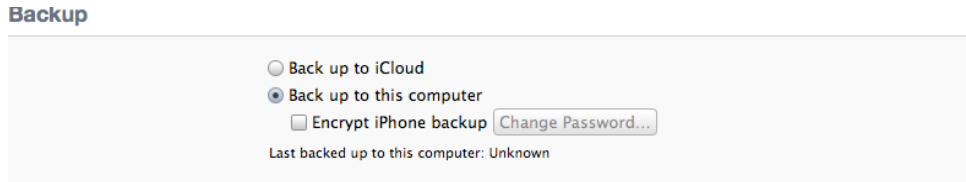
Figure 3-2 Backup encryption option

Other options are to sync the iPhone over WI-FI (Fig 3-3)

Figure 3-3 WI-FI Sync

When selected, WI-FI will sync content every time sync is pressed on the iPhone. (Fig 3-4) The Apple Macbook Pro must be on and iTunes open. A backup is not synced on every press of the sync button. The iPhone device seems to back up to iTunes on the initial connection only. Subsequent connections will backup content only. Once iTunes is shutdown and reopened then a new backup is created again. (Landau, 2011)

Figure 3-5 Sync now option

Author Name, email@address@manntechcomputersinc.com

3.2. The setup for iCloud backup

One of the new features that Apple IOS 5.0 introduces is the ability to back data up to Apple's iCloud Service. This new functionality will avoid the penetration tester's ability to recover data from the iPhone backup file, as no data is stored on the local machine. From an information security perspective possibly sending the companies sensitive information to a third party vendor may breach security policy and be more problematic than storing data locally.

The data is backed up over WI-FI to the iCloud service when the iPhone is on and connected to a power source. According to Apple's website iCloud backs up purchased music, TV shows, Apps, Books, Photos and video's, Device settings, App data, Home screen and app organization, SMS, MMS, iMessage and ringtones. ICloud is selected under settings. Move the slider to the on position. (Fig 3-7)

Figure 3-7 iCloud backup

Author Name, email@address@manntechcomputersinc.com

4. The data structure of the iPhone/iPad Backup file

As with most backups there is a particular file structure to be adhered to. Apple is no exception.

4.1. Location

The iPhone backup file is located on an Apple computer in ("Iphone backup location,")

~/Users/<username>/Library/Application Support/MobileSync/Backup

On a Microsoft Windows XP machine the location is:

Documents & Settings\<username>\Application Data\Apple Computer\MobileSync\Backup

On a Microsoft Windows Vista/Windows 7 the location is:

Users\<username>\AppData\Roaming\Apple Computer\MobileSync\Backup

This paper will use a Macbook Pro.

The folder name for the test device in the backup folder is 52e08276128ad4ed32ee13fa81b476f569df459e on the test machine. This number represents the device Unique Device Identifier (UDID). The UDID is created when the device is first connected to iTunes. On a Microsoft Windows OS the UDID can also be found as a sub-key in the hardware registry file system. The folder is not created when iTunes is installed but is created when the first backup is run.

4.2. File Structure

The file structure is the same on both a Microsoft Windows OS and an Apple OS. The file types consist of .PLIST, .DB, .SQLITE, .DAT, .JPG, .ASIDE, .ITHMB, and .PNG files. Certain files within the data structure will be of more interest to a penetration tester.

Author Name, email@address@manntechcomputersinc.com

The tool being used for analysis is called iBackupbot version 3.1.2. This is a commercial tool, but can be used in evaluation mode with a purchase niggle box. The left hand column shows the apps that have been installed. By clicking on the main folder more files are shown in the right hand panel. (Fig 4-1)
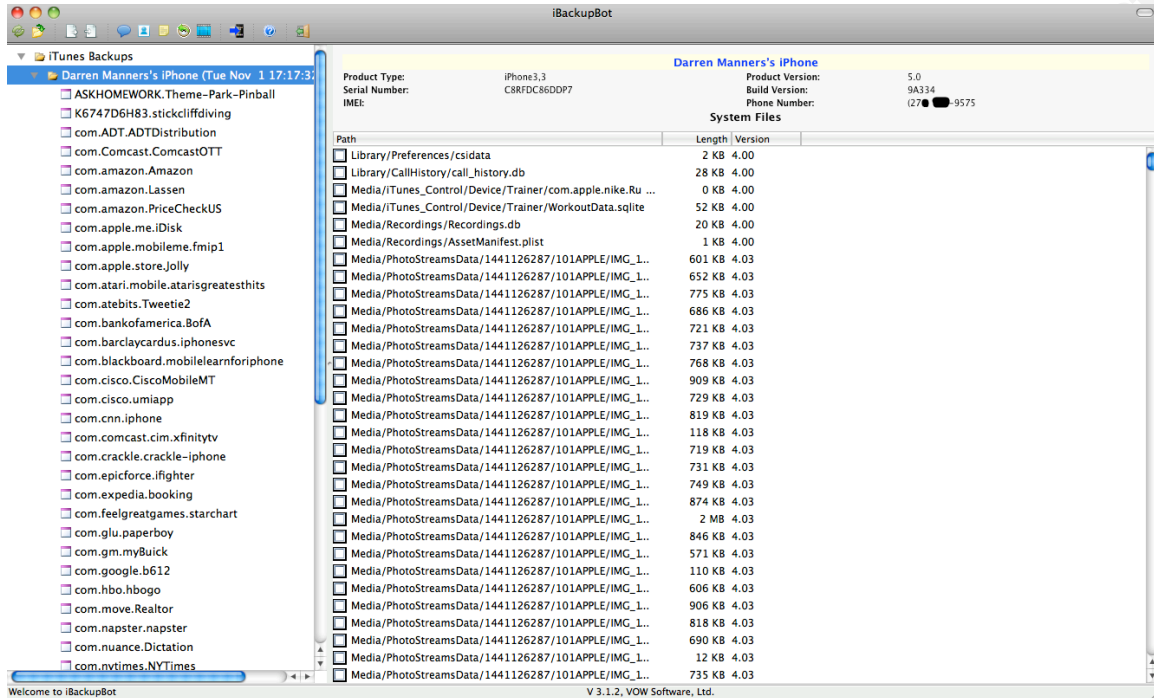

Figure 4-1 IBackupbot

4.2.1. Image Files

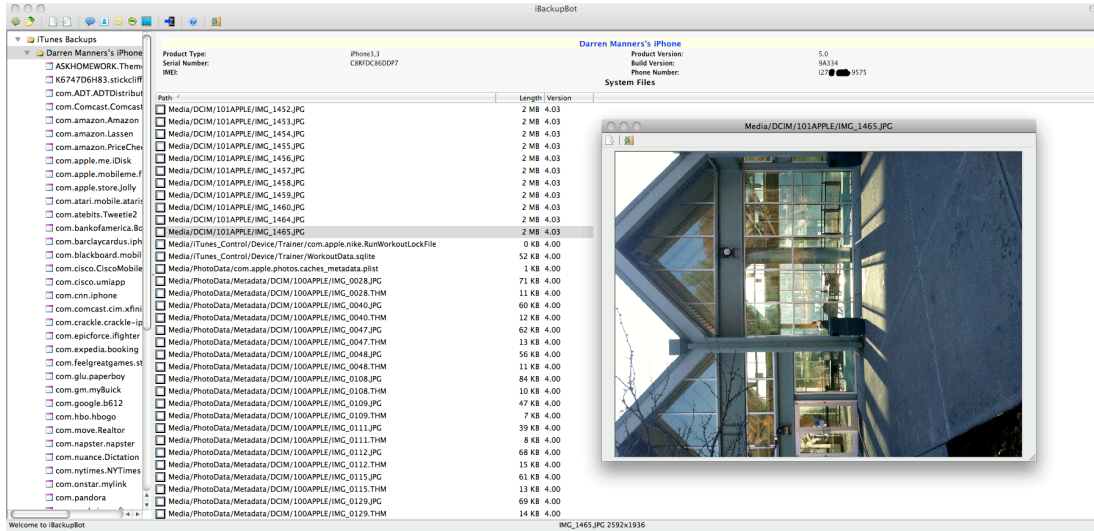Image files contained within the backup folder are normally .JPG or .MOV files. Selecting and double clicking the file name the image is displayed. (Fig 4-2)

Author Name, email@address@manntechcomputersinc.com

Figure 4-2 Standard image file

By examining image IMG_1465.JPG we can start to look at other files that may give more information about this image. If Photostream is enabled it will also create another image, in this case IMG_1062.IMG. (Fig 4-3) Note that the names are different.
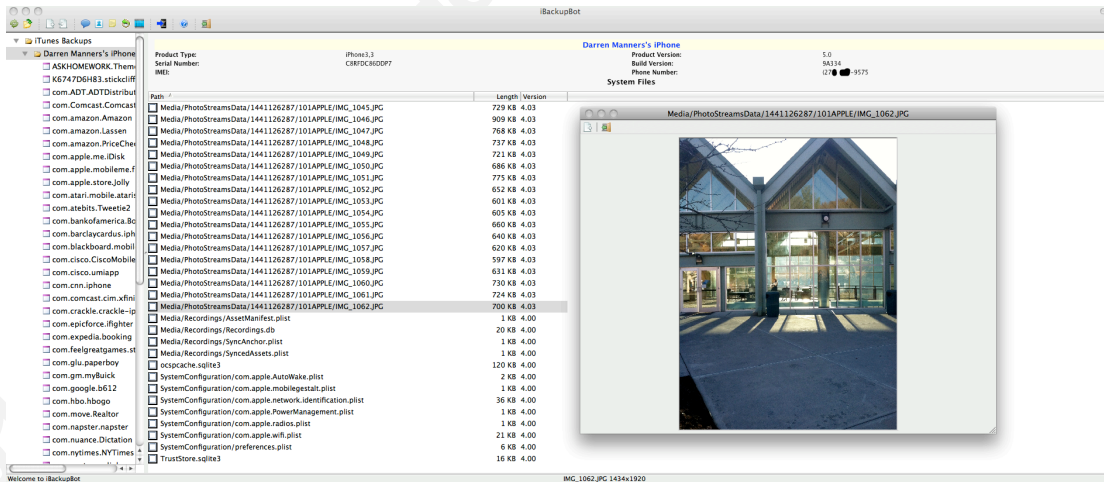
Figure 4-3 Photostream file

Another file for IMG_1062.JPG is created. This is called 101APPLE-IMG_1062.JPG. This contains metadata concerning the Photostream service. (Fig 4-4)

Author Name, email@address@manntechcomputersinc.com
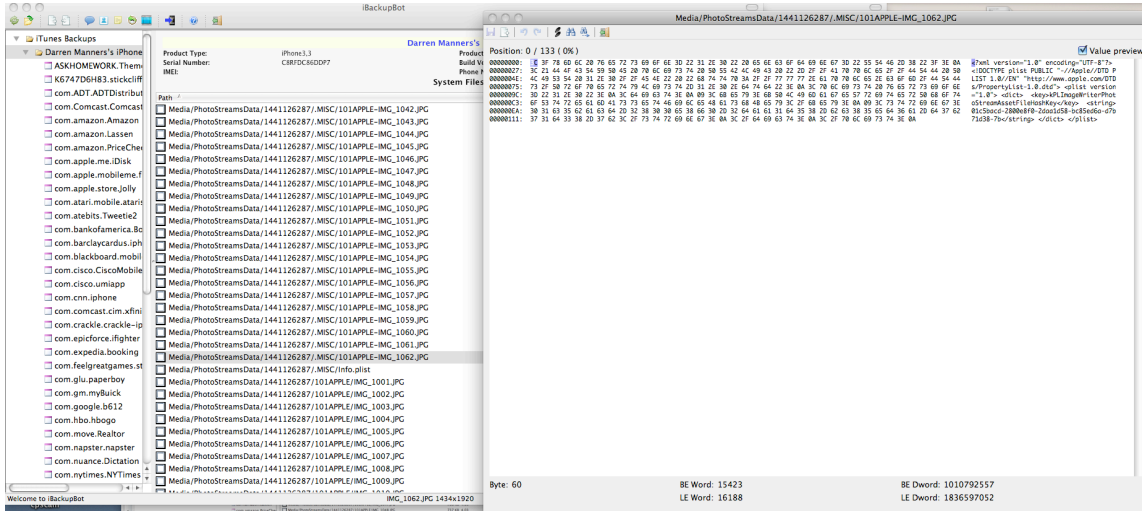
Figure 4-4 Image metadata

To find the GPS locational data information, assuming the end user had GPS enabled, save the image to the desktop. Open the image using Preview and press Command +I to bring up Inspector. The latitude and longitude and be viewed. This can be opened into Google maps for more detail by pressing the locate button. In this case the photo was taken at Mountain Empire Community College located in Southwest Virginia, USA. (Fig 4-5)

Figure 4-5 Command +i

Author Name, email@address@manntechcomputersinc.com
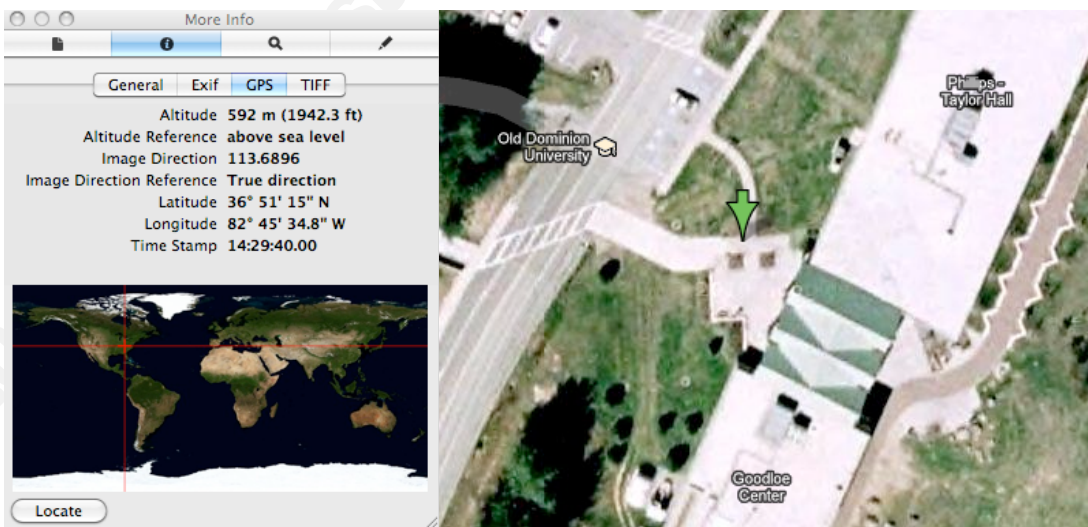
Other information about the picture is also available. Using a similar technique similar to that used in Figure 4-6 can see the date and time. In this case we can see it was taken on November 2nd 2011 at 09:02:53.
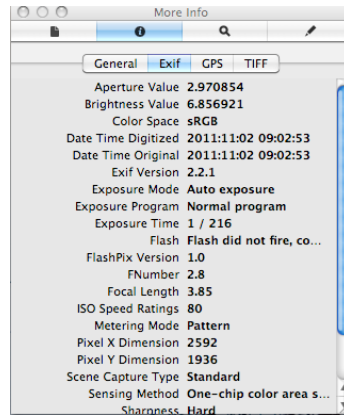
Figure 4-6 Dates of GPS data

4.2.2. Text Files

Files within the data structure can contain an amazing amount of information. Users may be totally unaware that this information is stored on the desktop. One interesting file is the dynamic-text.dat file. (Fig 4-6) It is located in Library/Keyboard/. This file is used to autocomplete predictive common words the user tends to use that are not in its built in dictionary. (Sadun, 2009)

It is the user's personal dictionary. It keeps a list of approximately 600 words. It appears that it does not store passwords typed into password fields in forms. However, if the user typed a password into an email or web search it may appear in this file. Not all the iPhone apps will add text to the personal dictionary. The easiest way to add new words to this is to open up mobile Safari and enter the words into the search field.

The words appear jumbled and do not follow the text that was actually typed. In fact at times, words typed into an email/text message did not appear. This may be due to the existence of the word already in the build in dictionary. It does create some interesting sentences at times if you forget that it is randomized.
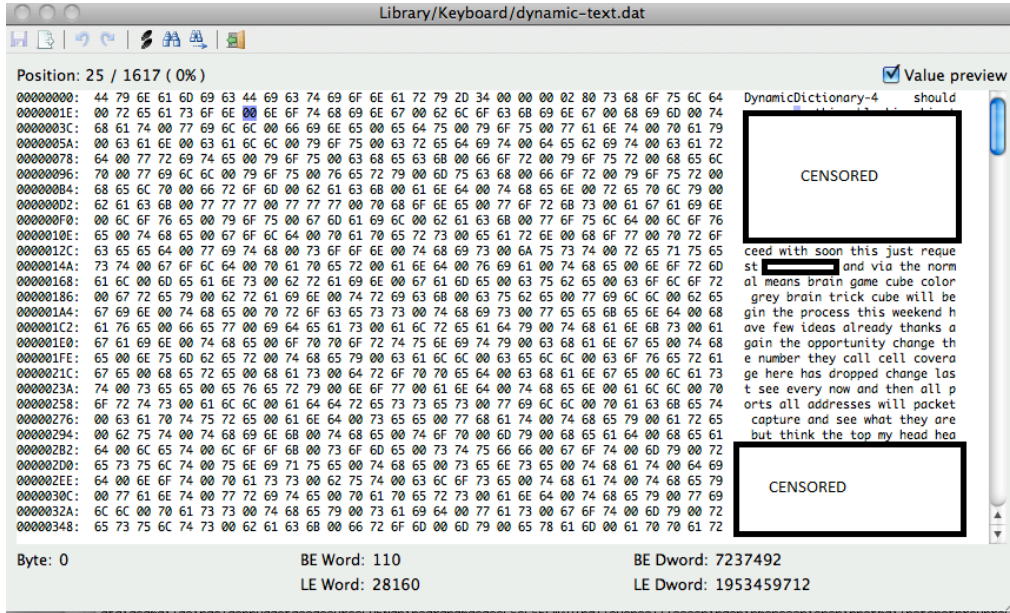
Author Name, email@address@manntechcomputersinc.com

Figure 4-6 Dynamic-text.dat

Note: I even had to censor my own data as it contained personal identifiable information.

4.2.3. Text Message Files

Text messages can be found in the Library/SMS/ section. The main database is the sms.db file. Pictures that are sent are also stored in the Library/SMS/ section. Current iBackupbot version for Apple Mac crashed when opening this file. This screenshot was taken from the Microsoft Windows version as this seemed to work fine. (Fig 4-7)
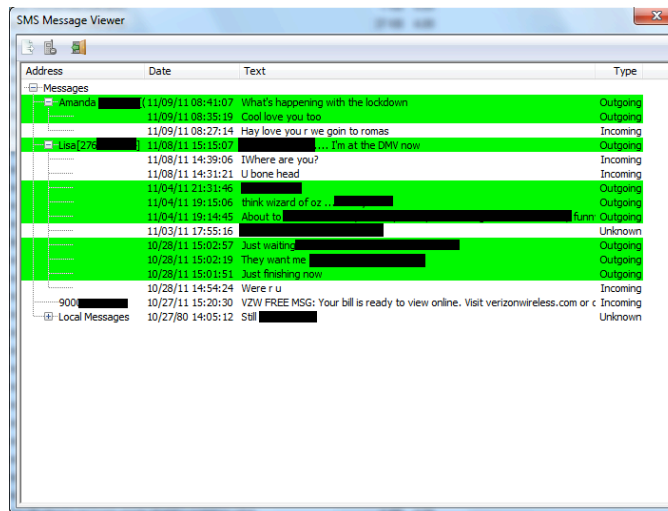

Figure 4-7 SMS database

Author Name, email@address@manntechcomputersinc.com

4.2.4. Address Book Files

The address book files will contain information contained in the users address books. This is under the Library/AddressBook/ area. It will contain phone numbers and email addresses. (Fig 4-8) This is useful for creating email phishing lists.

Figure 4-8 Call list

4.2.5. Calendar Files

Calendar items are located in Library/Calendar/Calendar.sqlitedb. Working down the list it is possible to identify upcoming and previous engagements. (Fig 4-9)

The time format used by iPhone backups is the Unix Timestamp format and the Absolute Time format. This format uses the Unix Epoch start date of Midnight GMT January 1st 1970. It then counts the seconds lapsed from this value. An example would be the current date of 7th November 2011, 08:41:32. In the Unix Timestamp format this would equate to 1320655292. There are many sites that can convert the Unix Timestamp format to a normal readable format. http://www.onlineconversion.com/unix_time.htm is one of them. On a Unix system you can type date +%s to find the current Unix time.

Absolute time measures the number of seconds from one point in time to another point in time. (Mona & Baggili, 2010)

Author Name, email@address@manntechcomputersinc.com

Figure 4-9 Calendar data

4.2.6. Notes Files

Notes files are located under Library/AddressBook/AddressBook.sqlitedb.
This database will contain information contained in the notes app. (Figure 4-10)
This would be useful as possible passwords or personal identifiable information
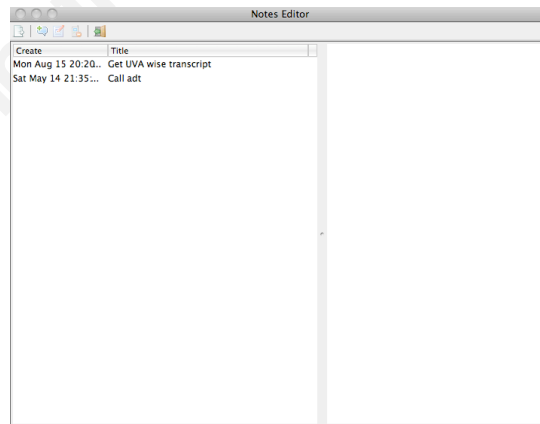may be found here. (Bader, and Baggili 1-15)

Figure 4-10 Notes

4.2.7. Call history

Located under Library/CallHistory/call_history.db. (Fig 4-11) This file will
show the incoming and outgoing information of the cell data. It will also show any
Facetime connections. This may be useful for phishing phone calls.

Author Name, email@address@manntechcomputersinc.com

Figure 4-11 Call list

4.2.8. Voicemails

Voicemails are located under Library/Voicemail. (Fig 4-12) They are .AMR files extensions. Exporting them to the desktop allows voicemails to be played back using Apple Quicktime software. This is extremely useful as lots of information may be leaked in voicemails.
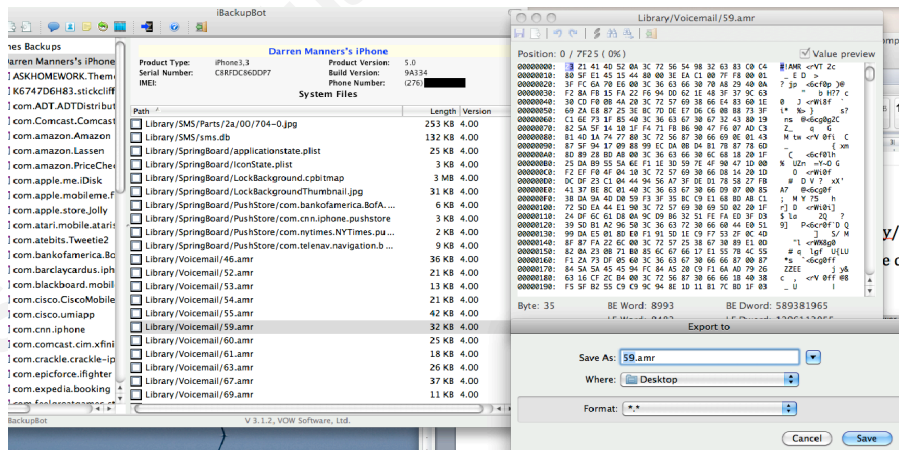

Figure 4-12 Voicemail

4.2.9. Email

The number and types of email files are dependent upon how many email accounts the end user is connecting to. The majority of email messages are stored as

Author Name, email@address@manntechcomputersinc.com

local files, but the iPhone being tested was only connecting up to a corporate Microsoft Exchange 2010 email system, so no local web caching was evident.

The iPhone keeps the Microsoft Exchange email databases on the local device. So unless the penetration tester has the actual device, the email data being extracted is going to be limited. More data may be exposed if the user is connecting to personal webmail accounts. (Be warned, personal email may be out of scope or even illegal!) This may be partly due to the fact that the iPhone syncs with the accounts and therefore any restore process would just sync the iPhone email accounts again.

The Library/Preferences/com.apple.accountsettings.plist (Fig 4-13) contains lots of information about corporate email. It will show the IP address of the SMTP server and username. It also shows that it is an exchange account.
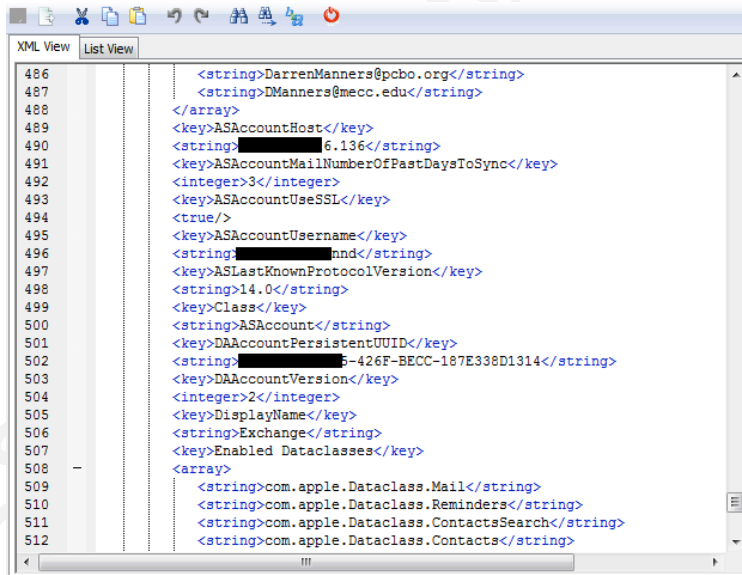

Figure 4-13 Email account settings

4.2.10. General user information

The backup file contains some other interesting files that are worthy of attention as they contain preference information that can be used. One such file is the preferences.plist located in SystemConfiguration/preferences.plist. Upon review it

Author Name, email@address@manntechcomputersinc.com

contained the IP address and group name for a VPN setup. It also contained WI-FI

SSID's that the iPhone had connected up to. (Fig 4-14)
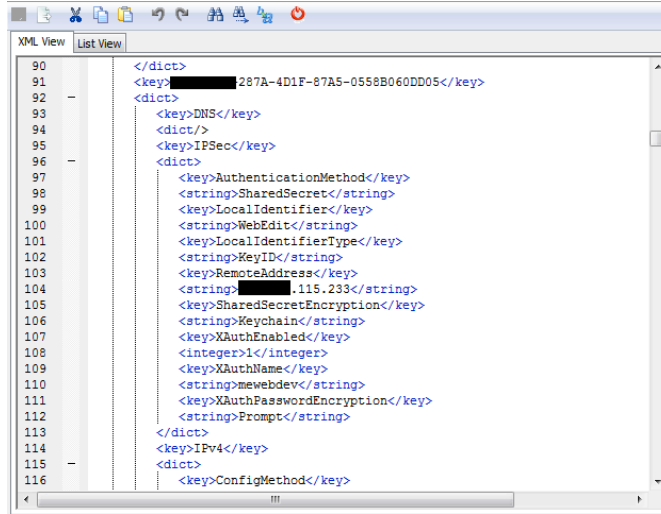
Figure 4-14 Preferences

4.2.11. Safari

Safari is the installed browser that comes with the iPhone. Users can install other

browsers so attention must be paid other apps may store the data elsewhere. The file

History.plist contains the Safari history list. (Fig 4-15) This is located in

Library/Safari/History.plist. This may give information about what the user is interested

in.

Figure 4-15 Safari history

Author Name, email@address@manntechcomputersinc.com

The cookis.binarycookies located under Library/Cookies/ also will give clues about the interests of the user. From Fig 4-16 it seems the end user was visiting Williamsburg, VA.
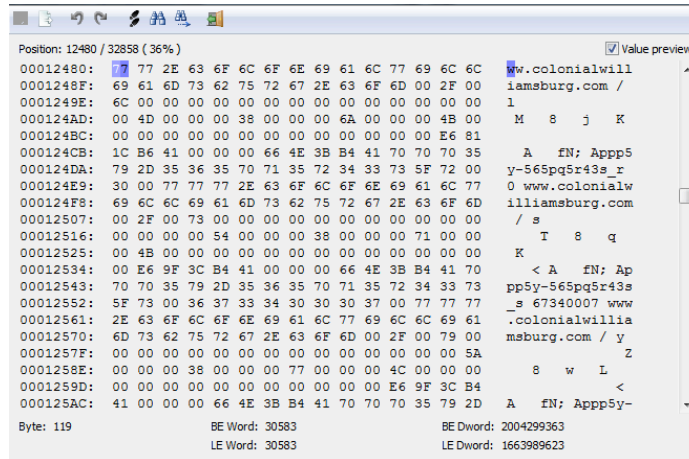
Figure 4-16

5. Hunting down backup files in a network

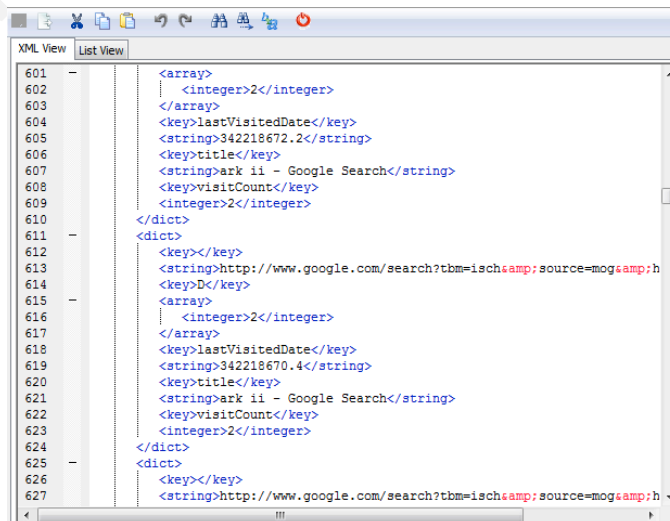ITunes was needed in the older generation of iPhones. As of iPhone 4Gs that is no longer the case. Still a large proportion of users will still have iTunes and will use it to transfer audio/video to their iPhone and create backups. Once the backup file is obtained a great deal of information, as has been shown, can be recovered from it.

Backup files may be identified by simply looking at the default directory on a workstation or sniffing network traffic to identify the existence of iTunes. ITunes traffic could possibly point to the existence of a backup file on a workstation, but as mentioned before, the latest IOS does not need to be tethered to a workstation.

Author Name, email@address@manntechcomputersinc.com

5.1. Traffic analysis

Examining a packet capture using very simple filtering tools, such as Wireshark, can identify iTunes traffic. The HTTP request header user agent field will contain the word "iTunes". An example of the user agent for iTunes 10.5 is

iTunes/10.5 (Windows; Microsoft Windows XP Home Edition Service Pack 3 (Build 2600)) AppleWebKit/534.51.22

The user agent will not only tell us the version of iTunes, but also the Operating system that it is running on. In this case it is a Microsoft Windows XP Home Edition Service Pack 3. It is also running the AppleWebkit version 534.51.22, an open source Internet browser engine. This information is very useful, as it will allow penetration testers to narrow the exploits being tested to only Microsoft Windows XP home SP3. The filter used to hunt for iTunes user agents is

http.user_agent contains iTunes

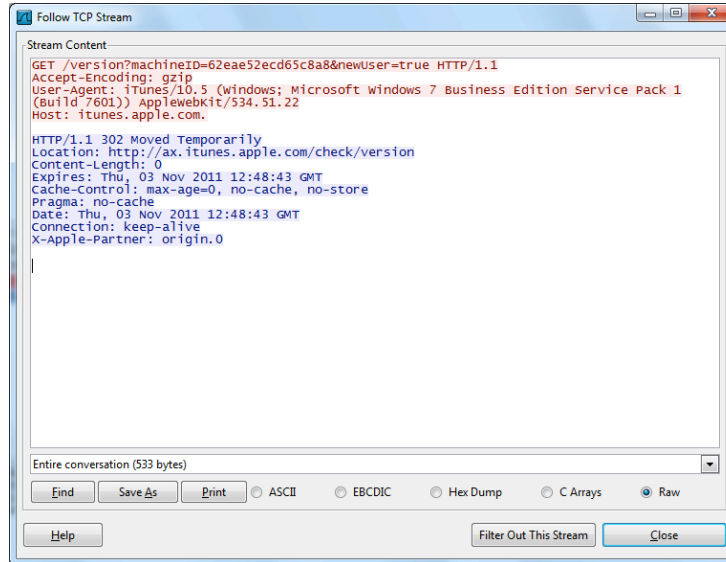Using the follow TCP streams option in Wireshark, the user agent can be viewed.

Author Name, email@address@manntechcomputersinc.com

Figure 5-1 User agent

Figure 5-1 shows that a Microsoft Windows 7 Business edition service pack 1 operating system is running iTunes 10.5. A pentester could then concentrate on this particular box for possible backup files.

5.2. Manual Desktop Search

Physically traversing the directories of a compromised machine may yield iPhone backup files. Since the folder name is based upon the UDID it will be hard to search for a folder name, as it may not be known. The end users tend not to change the default location of the backup folder. If the operating system is known, look in the default locations for backup files.

Author Name, email@address@manntechcomputersinc.com

6. Metasploit

Metasploit framework is a common tool used by penetration testers worldwide. It allows exploitation code to be created and run within a common framework. This framework facilitates the creation of exploits by the community for the community. The following will use Backtrack 5 from Offensive Security, running Metasploit framework 4.0

6.1. Setup

A Windows XP SP2 box has been exploited using the ms08_067_ netapi exploit in Metasploit 4.0. The payload used was a reverse Meterpreter TCP payload..
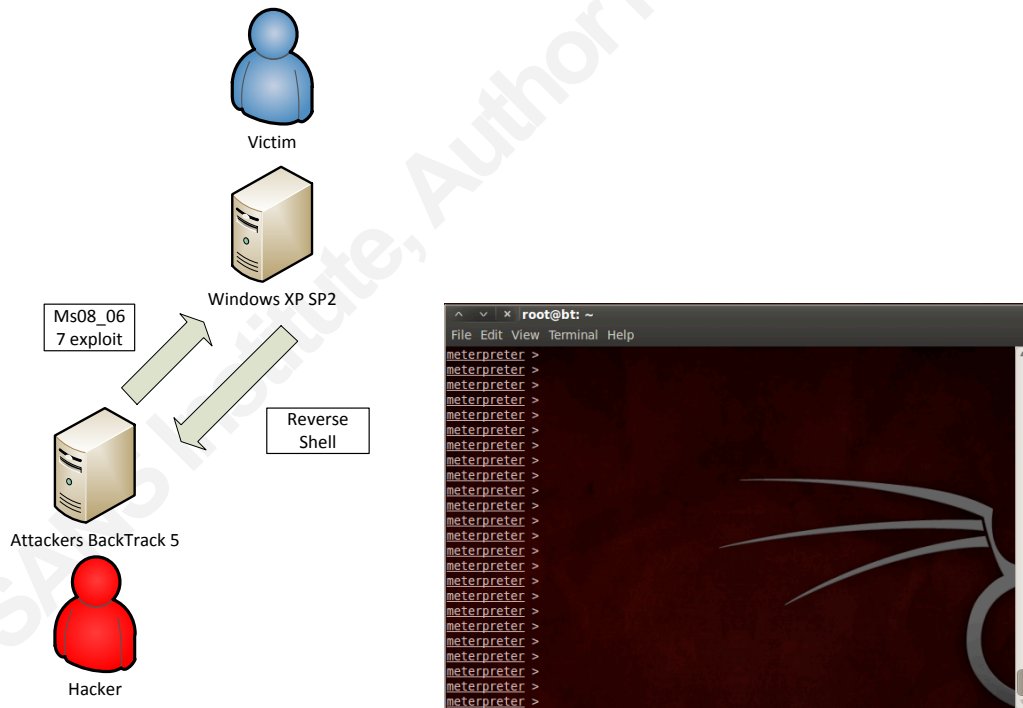

Figure 6-2 Meterpreter shell

Currently the attacker's system box is sitting at the Meterpreter shell having successfully exploited the victim's box.

Author Name, email@address@manntechcomputersinc.com

6.2. Finding the backup file

Dropping into a command shell inside the Meterpreter session, via the "shell" command, will allow directory traversal. Figure 6-2 shows a backup file located at the default location. Remember when traversing directories to put any folder with a space in its name inside quotation marks.

Figure 6-2 Shell

The Meterpreter prompt can also be navigated to find the backup files. (Fig 6-3) Using basic Unix commands like "cd", "ls" and "pwd" navigate the directory structure to the default location.

Figure 6-3 Meterpreter shell

The "download" command can be used to transfer the file from the compromised machine to the local machine. (Fig 6-4) The file can be a big file, depending upon what data is store on the iPhone. If it is too big, download it one section at a time, it is time consuming but the information is worth it.

Figure 6-4 Download

Once downloaded, the file can be transferred to another computer for further analysis. This may not be the case if the attacking computer also contains

Author Name, email@address@manntechcomputersinc.com

iBackupbot. In this scenario the system was compromised using Metasploit, the file was downloaded from the victim's machine to the attacker's machine. The attacking machine then offloaded the backup file to an Apple Macbook Pro. Further analysis was then conducted.

Author Name, email@address@manntechcomputersinc.com

7. Penetration tester's use of the iPhone/iPad backup file

Examining the information is only the beginning of the attack. The newly found information will give a penetration tester multiple avenues to think about. This section will examine social engineering using the backup file information. The penetration tester is only limited by the imagination.

7.1. Social engineering

As the perimeter is becoming hard to crack, social engineering is escalating. Recent attacks have been concentrating on the end user. Although the technical ability of the end user is sometimes questionable, current mass phishing emails are often discarded. An example of this type is the Nigerian 419 scam. ("Nigerian Letter or "419" Fraud") These emails are often littered with bad grammar and are designed for a generic audience. With the information gathered from the iPhone backup file, the penetration tester can craft a very specific social attack. An example would be to send an email to the CEO of the company with a picture already gathered from the backup file.

Hi <Name from contact list>

We talked on Tuesday, Noticed that a lot of your pictures are on the web!! <insert picture> I've enclosed some that I found, but it seems someone has added more explicit ones of you here!!!!

<link to evil server>

Thanks

<Name from contact list>

This type of attack will probably have a higher success rate than standard phishing attempts.

The information can be used in all sorts of evil ways, from phone conversations to get more information, to blackmail. Some of these out of band

Author Name, email@address@manntechcomputersinc.com

communications may contain sensitive information that the organization was never aware of. (Remember this when conducting data loss prevention exercises).

7.2. Social Engineering and Exploitation

This is a simple scenario that may be used to conduct further exploitation using the information gathered from the iPhone backup file. The tool being used is the Social Engineering Toolkit (SET) from www.social-engineer.org . This tool is installed by default in Backtrack 5.

Figure 7-1 Menu SET

Launch the SET. The menu (Figure 7-1) shows a number of possible social engineering vectors for attack. Select number 4 "Create a payload and listener". Selection 1 could also have been used. I just find 4 easier to create and use. If we were mass emailing this then selection 1 "Spear-Phishing attack Vectors" would probably be better, but it depends upon the type of attack being exploited.

Author Name, email@address@manntechcomputersinc.com

Figure 7-2 Payload

Select the Payload for the attack. (Fig 7-2) In this case a reverse TCP Meterpreter shell was selected. This is best as the machine may be behind a firewall.
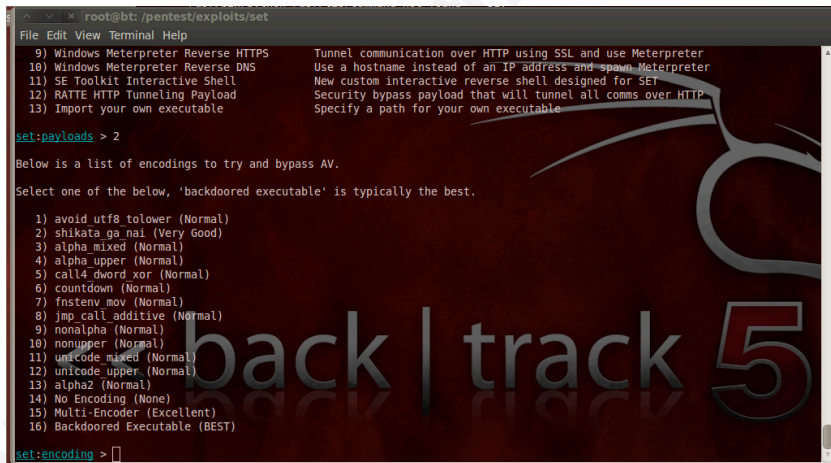
Figure 7-3 Encoding

Select the encoder 16 "Backdoor Executable" exe file. (Fig 7-3) Now this is for test purposes, but some mail systems will not allow .exe extensions through. It may be a process of trial and error. Another solution is to email a link to the exe or another form of exploitation. This way the victim can download the exe or another exploit regardless of the email policy, as links are generally not blocked. Both attack vectors will be used to help ensure delivery of payload.

Author Name, email@address@manntechcomputersinc.com
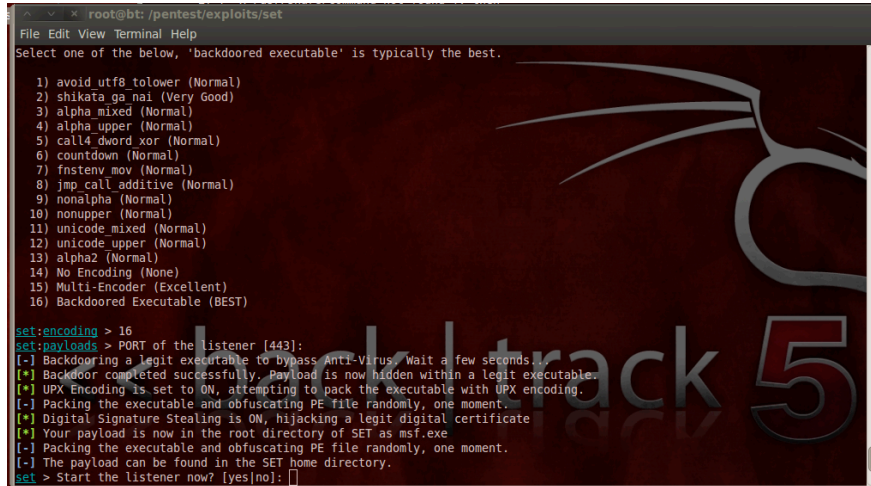
Figure 7-4 Listener

Select the port that the reverse shell will connect back to. (Fig 7-4) Select port 443 or 80 as they are normally allowed back out of an organization if it is using a firewall. Once the exe has been created, a listener can be started to capture the reverse shell back. Now wait for the victim to open the exe that is attached in the email. (Fig 7-5) The attached file is called msf.exe. This can be renamed if required.

Figure 7-5 Email Spoof

Author Name, email@address@manntechcomputersinc.com
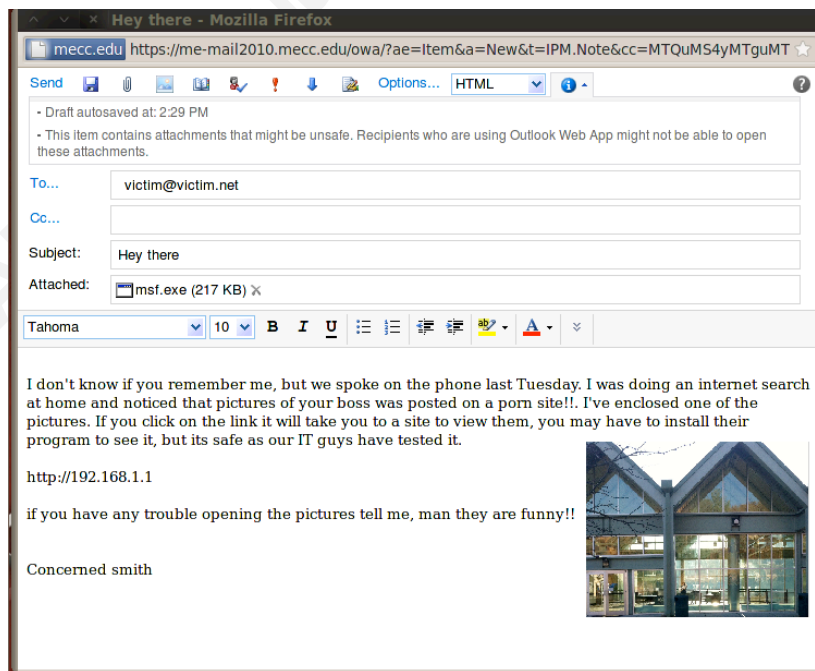
The listener is now running and waiting for the victim to connect back. (Fig 7-6)
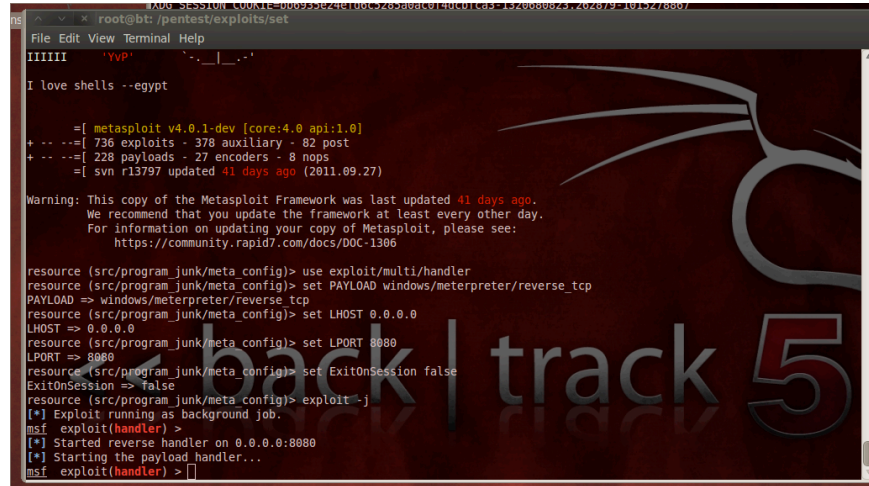
Figure 7-6 Payload handler

Since it is unsure that the exe will go through, another attack vector can be added to the same email. This is a link that when clicked on will pop up a java update. The popular Facebook template was used, but a site can be cloned or another template selected. Since we already have a listener on port 443 we can add a new one on port 444. Another better alternative is to import the already created executable into the fake website for a java attack. This means that one multi handler can be used for both attack vectors. Select 1 "Java Applet Attack Method" (Fig 7-7)

Figure 7-7 Java attack

Author Name, email@address@manntechcomputersinc.com
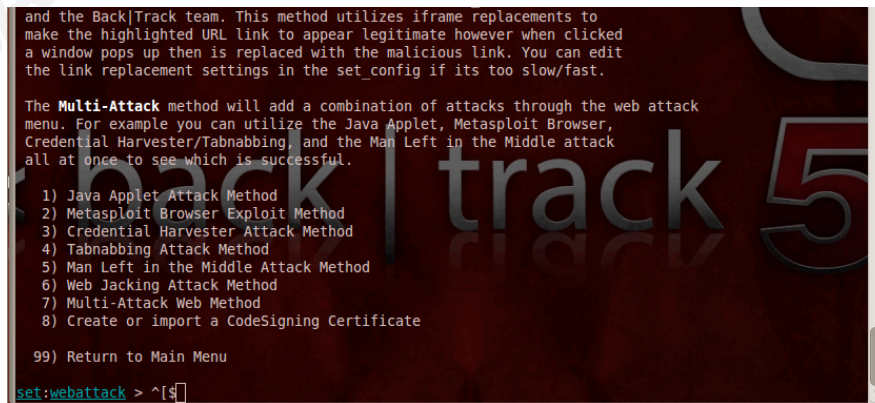
We are going to use a website template. (Fig 7-8)

Figure 7-8 Functionality

Now select the Facebook template. (Fig 7-9)

Figure 7-9 Facebook template selection

Import the executable created earlier. Select 13 "Import your own executable" (Fig 7-10)

Author Name, email@address@manntechcomputersinc.com
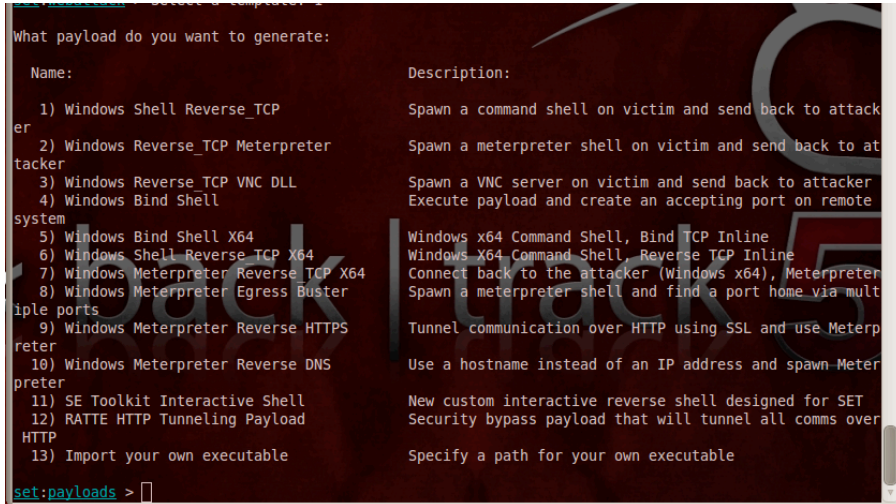
Figure 7-10 Payload generator

Enter the path for the executable to be imported. You can add a link into the email that points to the webserver of the attacking machine. In this example the IP address of the attacking machine was 192.168.1.1. In the email add a link to point to this IP address. The template is then run and the attacker's machine is ready and waiting for connection. (Fig 7-11)
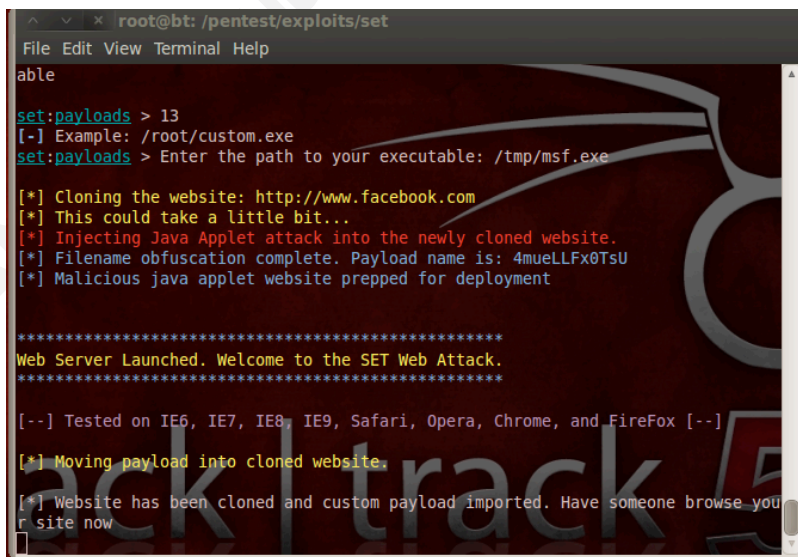
Figure 7-11 SET web attack

As you can see the link and the attachment are ready to send. We now send this to our victim. (Fig 7-12)

Author Name, email@address@manntechcomputersinc.com
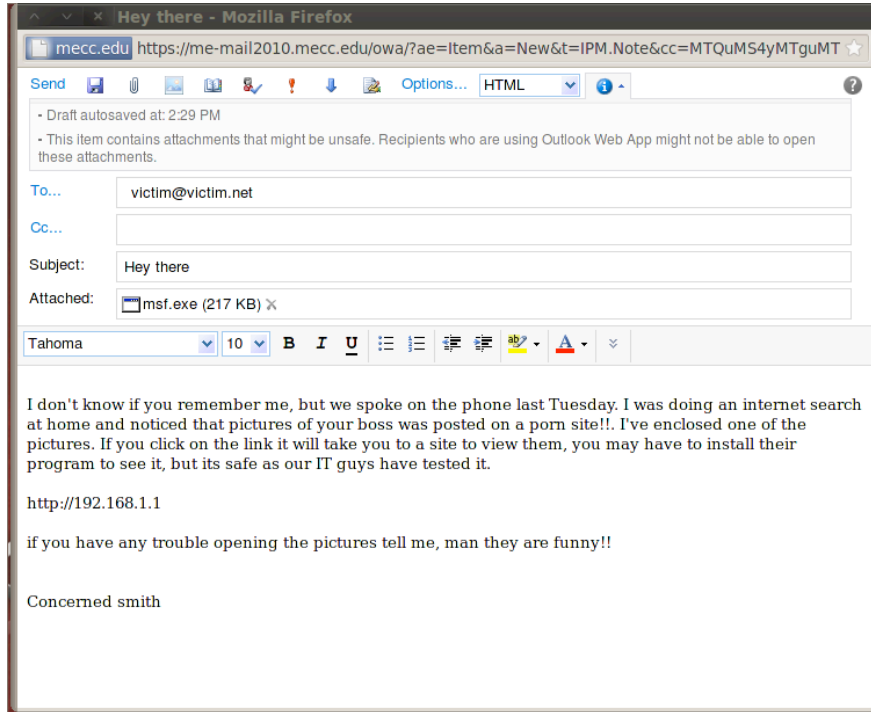
Figure 7-12 Phishing email

On the victim's machine, the email is opened. As suspected, the exe was blocked. (Fig 7-13) But if the victim clicks on the link it takes them to the fake Facebook account.
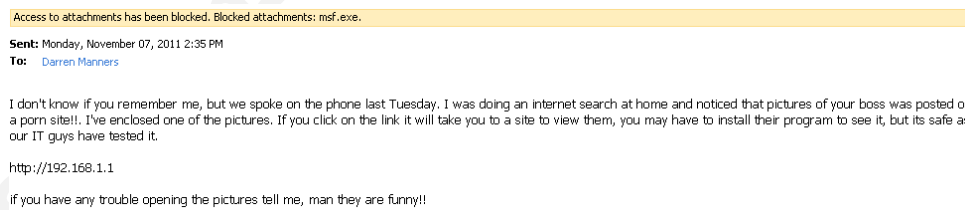
Figure 7-13 Attachment blocked

Here we see the java pop up on the victim's machine. (Fig 7-14) The victim then clicks on the java run box and the exploit begins.

Author Name, email@address@manntechcomputersinc.com

Figure 7-14 Java attack

Now on the attacker's machine, the payload exploit is run. (Fig 7-15)
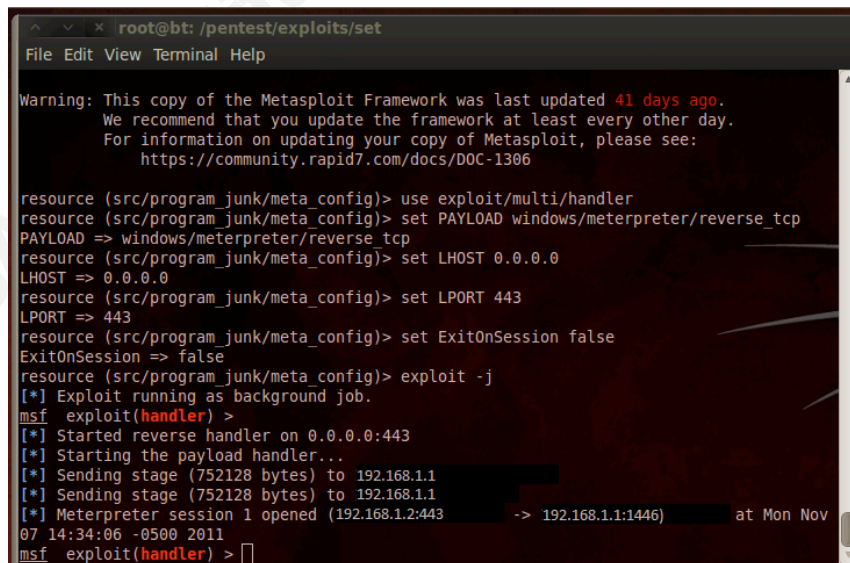
Figure 7-15 Successful exploitation

After a short time, the payload is executed and we now have control over our victim's machine.

Author Name, email@address@manntechcomputersinc.com

7.3. Restoring Backups

Another use of the backup file is to misuse the restore function. By restoring an encrypted backup file to a separate physical iPhone, the Photostream service, as well as other services that are password encrypted, can be manipulated. The penetration tester can take a photo with the cloned device and let the Photostream service copy it to all other devices. (If the Photostream service was enabled that is). Imagine if the photo was pornographic or other types of nefarious pictures. The only defense mechanism against this type of attack is the password for both the iCloud (as you can upload directly to the iCloud) and the encrypted backups password. When restoring an unencrypted backup file to a different physical iPhone, the username is restored across, but the password is not restored, so the attacker will still have to grab the password to these services from elsewhere.

This is not true if the backup file is encrypted. If the victim is using the encrypted backup option in iTunes, restoring the device to a different physical iPhone will restore the password as well. There is software available that claims to have cracked the encrypted file password mechanism. (Although it is a brute force attack, so the more secure the password used in encrypting the backup the longer it will take to crack).

Author Name, email@address@manntechcomputersinc.com

2) Restored iPhone does not contain Passwords

New Device Clone A

3) Attacker now has access to Photostream/email of Victim and can upload photo's that will appear on Original Device B if Photostream is turned on

Attacker

New Device Clone B

PhotoStream/Email etc

2) Cracked Password is used to restore iPhone device effectively creating a clone

1) Attacker steals non encrypted backup from desktop

1) Attacker steals encrypted backup from desktop

Non Encrypted Backup

Encrypted Backup

Original Device A

Original Device B

Figure 7-16

The organization in question states that Apple has "confirmed" that if the backup is encrypted, the keychain is generated from the iTunes backup password, then transferred and stored on the new device. Unencrypted backups use a keychain that is encrypted using hardware keys stored on the device itself.

The Apple ID, for iCloud access, will be disabled if numerous incorrect attempts are made to guess it. Attacking the iCloud password directly would prove difficult due to the lock out mechanism. The password can be reset online via Apple's reset feature, if you know the users security answers. (Sometimes the questions may be easy to guess)

In this example a penetration tester can use an encrypted backup file to restore a "cloned" copy of the victim's iPhone. Since Photostream uses WIFI, the fact that the Cell settings/data will be different is irrelevant. (Strangely on this test an encrypted backup file the Facetime and iMessage passwords did not carry over.)

Author Name, email@address@manntechcomputersinc.com

Once a cloned iPhone is ready, the penetration tester could take a photo and it will upload to the Photostream service. (Again the Photostream service has to be enabled). Once uploaded, it will then be distributed to the original victim's device, as well as other devices, if the victim had other devices that are subscribed to the Photostream service. An example would be a victim that has an iPad as well as an iPhone. The penetration tester can now also view the victim's emails in real time.

For this test two iPhones were used. (Apple iPad's could have also been used) One device, iPhone 'A', was used to create the initial unencrypted backup residing on an Apple MacBook Pro. When the unencrypted backup file created by iPhone 'A' was used to restore iPhone 'B', no passwords were restored. iPhone 'A' was then wiped using the reset "Erase All Content and Settings". An encrypted backup was taken off of iPhone A. When the backup file was restored to iPhone 'B' the Photostream and email passwords were restored also. This allowed the penetration tester to upload a photo on the cloned iPhone 'B' and see it appear on the original iPhone 'A'.

One must remember that attacking the encrypted password may be out of scope. The paper does not mention companies by name that claim to be able to crack the encryption nor was their software claims tested.

Author Name, email@address@manntechcomputersinc.com

8. Conclusion

Users are blissfully unaware of the security implications that new technology brings. The iPhones rich feature set, aimed at making life easier for the end user, and has contributed to security issues facing IT departments. Even Apple had to take a step backwards with regards to the data it collects from the iPhone is end users. (This was the case with GPS data)

The Photostream service raises a concern of mine. The idea is that if a photo is taken on an iPhone, then it will appear on other devices, like an iPad if they are subscribed to the same Photostream. Now imagine that a single vulnerability was found that allowed an attacker to upload a pornographic image to the Photostream service. The vulnerability bypassed authentication and authorization checks. The attackers image would be sent to all the end users subscribed devices.

The Photostream service also has a Microsoft desktop and Mac OS X agent that syncs to the mobile devices. By bypassing authentication an attacker can upload pornographic images and then perhaps contact the authorities, attempting to get the end user arrested. It might be a case of encrypting the backup files may actually decrease the security.

The penetration tester has to be ingenious and explore all avenues of potential exploitation. This means paying special attention to new technology. Apple has shown how a company can have a large impact on business technology with a must have consumer item. As information security professionals, there are times that the business model moves so fast it is almost impossible for security to keep pace. Endeavoring to use security policy to slow rapid adoption down, so that further security analysis can be done, sometimes is impossible in the face of upper management needs. The iPhone was a tool that embedded itself into business before even security realized it. Its ease of use leads to its rapid adoption, a testament perhaps, to the late Steve Jobs.

Hunting down the backup files is not easy, but it is made easier if the phone is tethered to a PC. Simple packet capturing/filtering can expose machines running Apple's iTunes software, which may contain a backup file. By default this is

Author Name, email@address@manntechcomputersinc.com

unencrypted. One recommendation is to encrypt this file and perhaps backup it up on a central secure server. If the iCloud is used, this opens up another whole security risk to an organization. The actual data stored is at the mercy of the provider. Having what the end user is searching for may provide lucrative marketing data that Apple cannot ignore.

The iCloud account information also appears to be stored in Library/Preferences/com.apple.accountsettings.plist.

Figure 9-1 Account settings

The user name is stored in plaintext, so half the information needed to compromise this account has already been found. The ID is called the AppleID. This is used for all Apple related services. One such service is the MobileMe service. This is used to locate your iPhone should you lose it. Now we have a single password not only for uploading images, purchasing Apps/Music/Video's but also to locate real time whereabouts of the end user. With this simple username and password, a hacker can log on to icloud.com and locate the end user, remote lock the system or erase it. Imagine if this username and password was compromised. To mitigate this type of problem the iPhone should not be linked to cloud services and the "find my iPhone" in the iPhones settings should be switched off.

Author Name, email@address@manntechcomputersinc.com

Figure 9-2 iCloud.com

The information that is stored in the iPhone backup file is quite incredible. Designed to make an easier restore for the end user if the phone fails, it has created a potential goldmine for the penetrations tester and malicious attackers. Penetration testers can use the information contained in the backup file for reports or social engineering. Nothing helps a penetration report more than showing the CEO's SMS messages for the last year.

Companies have mostly wised up to, and adopted, basic security practices. They understand that patching; firewalling and adding monitoring devices protect the majority of systems.

This makes it increasingly difficult for a penetration tester to get a foothold on a system. From experience, many companies are still soft when it comes to in depth security. So once a foothold is gained inside a network, moving from system to system becomes easier. Social engineering is a great way to get that foothold, and the iPhone backup file gives plenty of information to help with this.

Many companies do not have a policy with regards to backup files from iPhones. The fact is many companies do not fully understand what is contained in the backup files or they most certainly would have a policy. This is really the role of the penetration tester. To successfully exploit vectors of attack that the client would not think possible. Make the client aware of how the hacker is thinking.

Author Name, email@address@manntechcomputersinc.com

Some penetration tests are purely compliance requirements with no real teeth for the penetration test. The engagement is extremely limited in both time and scope. This is sometimes by design, as the IT department wants no surprises from the engagement of a penetration tester. A good penetration tester has to think outside the scope and have multiple ways to achieve the same goal. In effect this will aid the IT department. It may give the IT department the necessary information to build a strong policy and this paper was designed to give the penetration tester another attack vector. By attacking residual backup data, the penetration tester may show that hackers could seem to be holding the CEO's phone in their hand. Now wouldn't that be handy in convincing business to take a more proactive role in security and validate the necessity of thorough penetration testing which does not fail to look extensively at new technologies as they are adopted.

Author Name, email@address@manntechcomputersinc.com

9. References

Goldman, D. (2010, July 26). *Jailbreaking iphone apps is now legal*. Retrieved from http://money.cnn.com/2010/07/26/technology/iphone_jailbreaking/index.htm

Goodin, D. (2011, November 08). *Apple expels serial hacker for publishing iphone exploit*. Retrieved from http://www.theregister.co.uk/2011/11/08/apple_excommunicates_charlie_miller

Huffman, K. (2010, May 31). *Apple overtakes microsoft as industry leader*. Retrieved from http://www.headlinesnews.net/4997/apple-overtakes-microsoft-as-industry-leader

Ionescu, D. (2010, July 27). *Never mind legality, iphone jailbreaking voids your*. Retrieved from http://www.pcworld.com/article/201968/never_mind_legality_iphone_jailbreaking_voids_your_warranty.html

Ios features. (2011, November 08). Retrieved from http://www.apple.com/ios/features.html

Iphone backup location. (n.d.). Retrieved from http://www.iphonebackuplocation.com

iphone 4s. (2011, November 08). Retrieved from http://www.apple.com/iphone/specs.html

Landau, T. (2011, October 27). *itunes wi-fi sync & back up: Fail (& workaround)*. Retrieved from http://www.macobserver.com/tmo/article/itunes_wi-fi_sync_and_back_up_fail_and_workaround

Mona, B., & Baggili, I. (2010, November 8). *iphone 3gs forensics: Logical analysis using* . Retrieved from http://ssddfj.org/papers/SSDDFJ_V4_1_Bader_Bagilli.pdf

Nigerian letter or "419" fraud.. (n.d.). Retrieved from http://www.fbi.gov/scams-safety/fraud/fraud

Author Name, email@address@manntechcomputersinc.com

Omar, A. (2011, October 2011). *ios 5 untethered jailbreak is already covered by hackers*. Retrieved from http://cydiahelp.com/ios-5-untethered-jailbreak-is-already-covered-by-hackers

Pogue, D. (2007, June 27). *The iphone matches most of its hype*. Retrieved from http://www.nytimes.com/2007/06/27/technology/circuits/27pogue.html?pagewanted=all

Publishing an app in the app store. (2011, October 12). Retrieved from http://developer.apple.com/library/ios/

Sadun, E. (2009, January). *What the duck? train your iphone to (truly) learn new words*. Retrieved from http://arstechnica.com/apple/news/2009/01/what-the-duck-train-your-iphone-to-truly-learn-new-words.ars

Unauthorized modification of ios has been a major source of instability,. (2011, November 08). Retrieved from http://support.apple.com/kb/ht3743

Author Name, email@address@manntechcomputersinc.com

Last Updated: October 1st, 2012

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

SANS CyberCon 2012	**Online, VAUS**	**Oct 08, 2012 - Oct 13, 2012**	**Live Event**
SEC 579: Virtualization and Private Cloud Security @ Bangalore	**Bangalore, IN**	**Oct 08, 2012 - Oct 13, 2012**	**Live Event**
SOS: SANS October Singapore 2012	**Singapore, SG**	**Oct 08, 2012 - Oct 20, 2012**	**Live Event**
SANS Gulf Region 2012	**Dubai, AE**	**Oct 13, 2012 - Oct 25, 2012**	**Live Event**
SANS Seattle 2012	**Seattle, WAUS**	**Oct 14, 2012 - Oct 19, 2012**	**Live Event**
SANS Baltimore 2012	**Baltimore, MDUS**	**Oct 15, 2012 - Oct 20, 2012**	**Live Event**
SANS@ Grid Security Conference 2012	**San Diego, CAUS**	**Oct 16, 2012 - Oct 16, 2012**	**Live Event**
SANS South Africa 2012 - Cape Town	**Cape Town, ZA**	**Oct 26, 2012 - Oct 27, 2012**	**Live Event**
SANS Chicago 2012	**Chicago, ILUS**	**Oct 27, 2012 - Nov 05, 2012**	**Live Event**
SANS South Africa 2012	**Johannesburg, ZA**	**Oct 29, 2012 - Nov 06, 2012**	**Live Event**
SANS Bangalore 2012	**Bangalore, IN**	**Oct 29, 2012 - Nov 03, 2012**	**Live Event**
FOR526 Beta	**Denver, COUS**	**Nov 05, 2012 - Nov 09, 2012**	**Live Event**
SANS Korea 2012	**Seoul, KR**	**Nov 05, 2012 - Nov 13, 2012**	**Live Event**
SANS Tokyo Autumn 2012	**Tokyo, JP**	**Nov 05, 2012 - Nov 10, 2012**	**Live Event**
SANS San Diego 2012	**San Diego, CAUS**	**Nov 12, 2012 - Nov 17, 2012**	**Live Event**
SANS Sydney 2012	**Sydney, AU**	**Nov 12, 2012 - Nov 20, 2012**	**Live Event**
SANS London 2012	**London, GB**	**Nov 26, 2012 - Dec 03, 2012**	**Live Event**
SANS San Antonio 2012	**San Antonio, TXUS**	**Nov 27, 2012 - Dec 02, 2012**	**Live Event**
European SCADA and Process Control System Security Summit 2012	**Barcelona, ES**	**Dec 05, 2012 - Dec 11, 2012**	**Live Event**
SANS Cyber Defense Initiative 2012	**Washington, DCUS**	**Dec 07, 2012 - Dec 16, 2012**	**Live Event**
SANS Egypt 2012	**Cairo, EG**	**Dec 08, 2012 - Dec 20, 2012**	**Live Event**
SANS Forensics Prague 2012	**OnlineCZ**	**Oct 07, 2012 - Oct 13, 2012**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**