

Running head: A JAILBROKEN IPHONE CAN BE A VERY POWERFUL WEAPON
IN THE HANDS OF AN ATTACKER

Smart Phones can become an Attackers most Camoflashed Weapon

Alejandro Chavez

Abstract

Apple's iPhone is smart phone that can easily be used by attacker to attack a network and not seem to attacking the network at all. A small phone is not consider to be a possible threat to a network infrastructure, rather the person checking his email on his or her notebook. Even someone how had an Asus' Eee pc would get stop by security because it is a computer that is known to be used in attacks.

Since the 90s, the cell phone market has been developing phones that do more than just make and receive phone calls. They started offering customers access to the internet and ability to check their email. These phones were called smart phones because they could do more than the average phone. On June 29, 2007 Apple released the iPhone which is a touch screen cell phone and much more. The iPhone a multimedia device that is also a camera, iPod, visual voicemail, e-mail, web browsing, a Quad-band GSM process, and has a wireless card built-in. With these advancements, in technology, carrying a computer is now able to fit in anyone's pocket. Since the iPhone is a computer running OS X with phone capabilities, then what is to stop someone to put tools that would attack a network? When released there was a four gigabyte version which in September of 2007 was discontinued, an eight gigabyte version, and most recently a sixteen gigabyte version. When the four gigabyte iPhone was discontinued Apple also announced a price drop of the eight gigabyte iPhone and surprisingly offered a \$100 gift card, to the apple store, to anyone who bought the iPhone before the price drop. Apple also offers firmware upgrades through iTunes, and in June of 2008. Apple announced at a conference that they are scheduled to release iPhone firmware 1.2.0 which will make the iPhone more useable in the corporate world. This will bring features such as Active Sync with Microsoft Exchange, Cisco IPsec VPN, WPA2/ 802.1x support and more. Soon after the iPhone's release, software was developed to unlock the restrictions that Apple placed on the iPhone, such as adding third-party software. Unlocking the iPhone became known as Jail breaking which unfortunately also voids the warranty Apple provides their customers with when buying an iPhone. In the beginning, jailbreaks were done to the firmware, which increased the possibility of bricking the iPhone. Soon after a

vulnerability was discovered through Safari which in turn made unlocking the iPhone much easier and safer. With iPhone firmware 1.1.1 it was as simple as being connected to a wifi network and launch Safari, go to www.jailbreakme.com and scroll down to the bottom and tap on Install AppSnapp as shown in figure 1-1.

When jailbreaking the iPhone using the Safari exploit, the jailbreak would unlock the phone and place a blue icon called Installer on the home page of the iPhone and when finished would also patch the Safari exploit. Bricking became a term when after a firmware update, from either third-party software or Apple, would cause the phone to no longer respond at any key-combination or connection request through iTunes, the phone became a paper weight or a brick. It has been said that after firmware 1.1.3 the iPhone could not be bricked as simply as before.

Later a man in Italy spent three months developing ZiPhone, which is available for download at www.ziphone.org and is available for both Windows and Mac users.

ZiPhone is a graphical user interface that neatly and seamlessly unlock and jailbreak iPhones or iPod touch. ZiPhone is very simple to use, even young children are on YouTube showing people how to jailbreak your iPhone using ZiPhone, an example of ZiPhone working on an iPhone firmware 1.1.4 shown in figure 1-2. ZiPhone version 2.6b will jailbreak all firmware up to 1.1.4.

With a jailbroken, iPhone attackers can use this to find out information about a network using just a phone. Gathering information or footprinting is important to have when wanting to attack a secure network. According to Stuart McClure, Joel Scambray, and George Kurtz (1999), “systematic footprinting of an organization will allow attackers to create a complete profile of an organization’s security posture”(p. 5). They go on to say

“Footprinting is necessary to systematically and methodically ensure that all pieces of information related to the aforementioned technologies are identified”(Kurtz et al., 1999, p6). Footprinting can involve scanning tools such as Metasploit, Nmap, Whois, tcpdump and others.

Cydia is an alternative to Installer and can be installed through the Installer after being jailbroken. Cydia will install Metasploit, Nmap, Whois, tcpdump, a terminal, Wifi Stumbler, and other useful tools onto the iPhone, which can be used to retrieve information about a network. At www.hackthatphone.com/114/iphone_cydia there is a nice tutorial on how to install Cydia through the Installer and they screen shots of every step. First after jailbreaking the iPhone launch the Installer and run any update that is for the Installer if it appears (note: when installing update or packages it is best to do so while connected to a wireless network rather than using the Edge network). Then tap on Sources on the bottom as shown in figure 1-3. Next tap on the Edit button located at the top, then note the change from the Refresh button, which will then change to Add. Tap the Add button and enter the following (not the quotes): “<http://aptapp.saurik.com>” then tap OK. After the iPhone updates its sources note the new Source at the bottom called Saurik’s Coding Toolbox as shown in figure 1-4. Next tap Install located at the bottom of the screen. Then tap on All Packages and scroll down to Cydia Packager. On the next page, it will give a description of the Package, the Version, the Size, Contact, a brief description, and a More Info slot, which may give more information about the package or send the user to a web page about the Package as shown in figure 1-5.

Next tap on Install at the top but make sure you are connected through a wireless network since the package is 13.7 MB and would take a significant amount of time through

AT&T's Edge network. After the download when the iPhone installs Cydia it is know to install very slowly and although it may seem to have stop responding that is not the case. Also do not allow the iPhone to timeout or lock for this will cause the install to muddle. After the install, a warning will appear about the BSD Subsystem only because it has not yet been installed. Then after the install tap on install again and tap on System. Locate Fake BSD Subsystem and install the package. When finished click the home button and the iPhone will then restart and after you slide to unlock the Cydia package manager will be on the home page of the iPhone. Next tap on Cydia and when it first runs there may need to be some updates that may need to happen. Cydia is very similar to Installer with some changes and also a Search feature. Tap on install, then scroll down to Networking and not Network which has different packages. Under Networking is where one can install Metasploit, Nmap, Whois, tcpdump, wifi stumbler, ftp client, netcat, remotely access windows machines with rdesktop, and other packages as shown in figure 1-6, 1-7, and 1-8.

Stumbler is an application that stumbles upon wireless networks, even networks that are hidden. Stumbler can be find under the Networking section of Cydia. Stumbler provides such information as: SSID, BSSID, the channel the access point is running on, the AP mode, where it is running WPA or WEP, signal strength, if it is a hidden network, and Beacon Interval. An example of what Stumbler displays is shown in figure 1-9 and 1-10 for wireless network "Alex".

A must for running some of these packages is a terminal, which is not installed by default. Just tap Search and type in terminal and a listing of shell terminals will appear for install. When lunning the terminal and attempting to use some application such as

nmap, require the user to be root and it did not take long to crack the default root password on the iPhone, which is alpine. To be root type in su and tap enter next just type the root password of alpine as shown in figure 1-11. Nmap is a useful command when wanting to discover devices on the network. According to Stuart McClure, Joel Scambray, and George Kurtz (2001), Nmap, “provides basic TCP and UDP scanning capabilities as well as incorporating” (p.48). Nmap on the iPhone can be used to discover different devices, TCP/IP fingerprint, open ports and will do a best guess operating system. Under networking, in Cydia, Nmap is available for installation. Launch the terminal and type in su then alpine for the password. Then to use Nmap type in `nmap -Ss -O -e en0 network address/subnet` as shown in figure 1-12 and TCP/IP fingerprint in figure 1-13.

With having such application that appear on the home page of the iPhone, others would know if examining the phone that it is jailbroken and has tools that are know to be used by attackers. Luckily, for attackers there is another application that can hide applications behind a calculator. This application is called HidePod and was originally written so that one may hide there porn behind a calculator. Along with hiding video and photos, one may hide applications such as stumbler, terminal, APlogger, Cydia, and other tools. HidePod functions just like the calculator on the iPhone and can replace the iPhone calculator but when entering the secret password HidePod launches and gives the user access to there hidden material as shown in figure 1-14. The down side to HidePod is that HidePod is not free and every key purchased, is registered to the purchasing iPhone’s serial number. HidePod is available through a pay pal purchase of \$9.99.

With all these techniques, gathering information from a wireless network has gone from carrying a laptop to using the device that one mostly already has, smart phones. Peter Grabosky and Russell G. Smith say, “In 1995, 250,000 smart phones were sold in the United States” (p.6). Two-hundred and fifty thousands smart phones were sold in 1995 and today who many young adults do not want an mp3 player with build-in wireless card that can be used to run attacks against networks because they saw it on You Tube. You Tube is providing people with the knowledge to unlock there smart phone and use it for there own good well or terrorize someone else’s job.

References

Grabosky, P., & Smith, R. (1998) *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*. New Jersey: Transaction Publishers

Kurtz, G., McClure, S., & Scambray, J. (1999). *Hacking Exposed: Network Security Secrets and Solutions*. Berkeley: Computing Mcgraw-Hill

Kurtz, G., McClure, S., & Scambray, J. (2001). *Hacking Exposed: Network Security Secrets and Solutions*. (2nd ed.) Berkeley: Computing Mcgraw-Hill

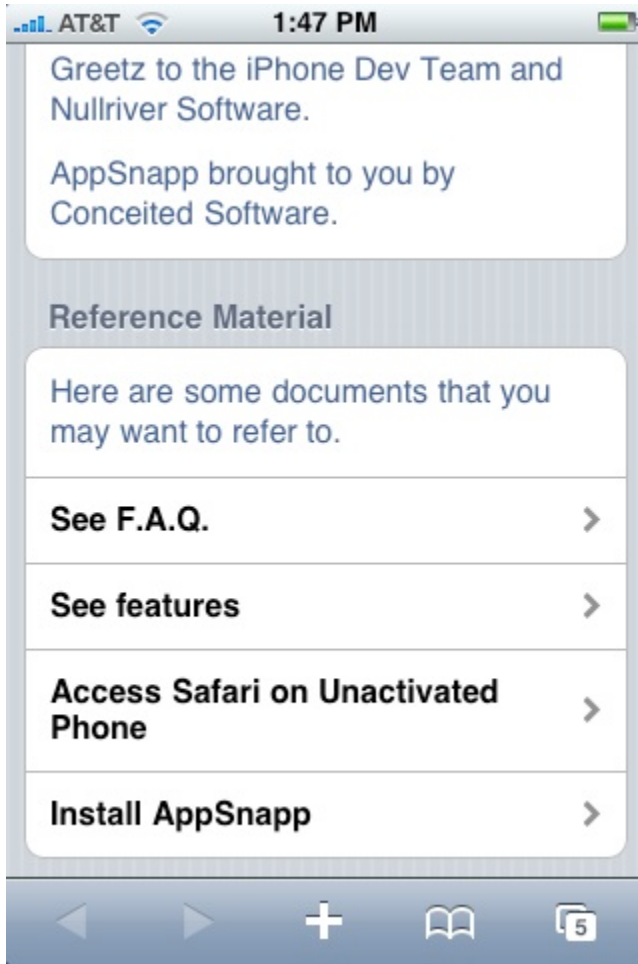


Figure 1-1 Installing AppSnapp for iPhone Firmware 1.1.1

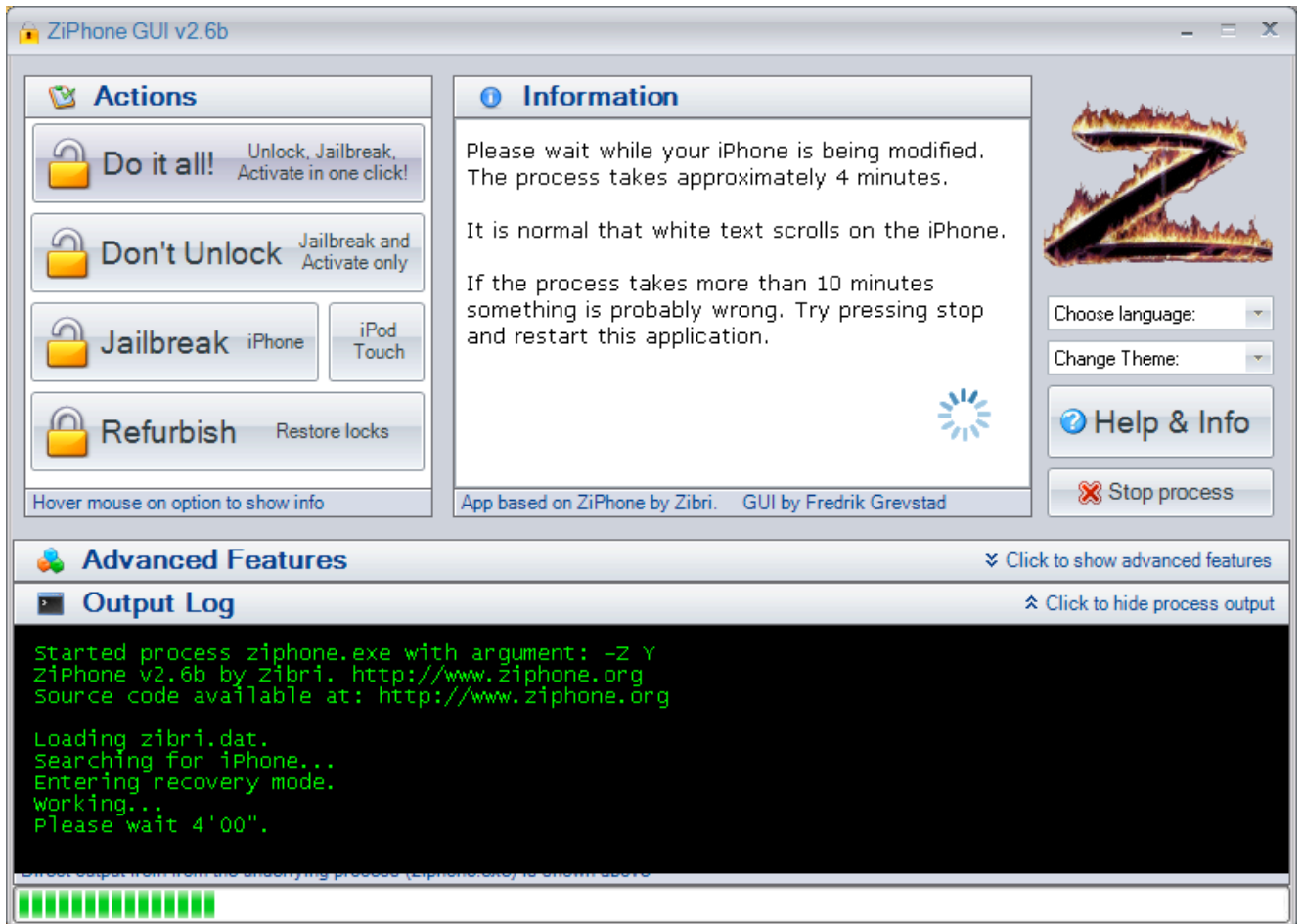


Figure 1-2 ZiPhone GUI V2.6b is Jailbreaking an iPhone Firmware 1.1.4

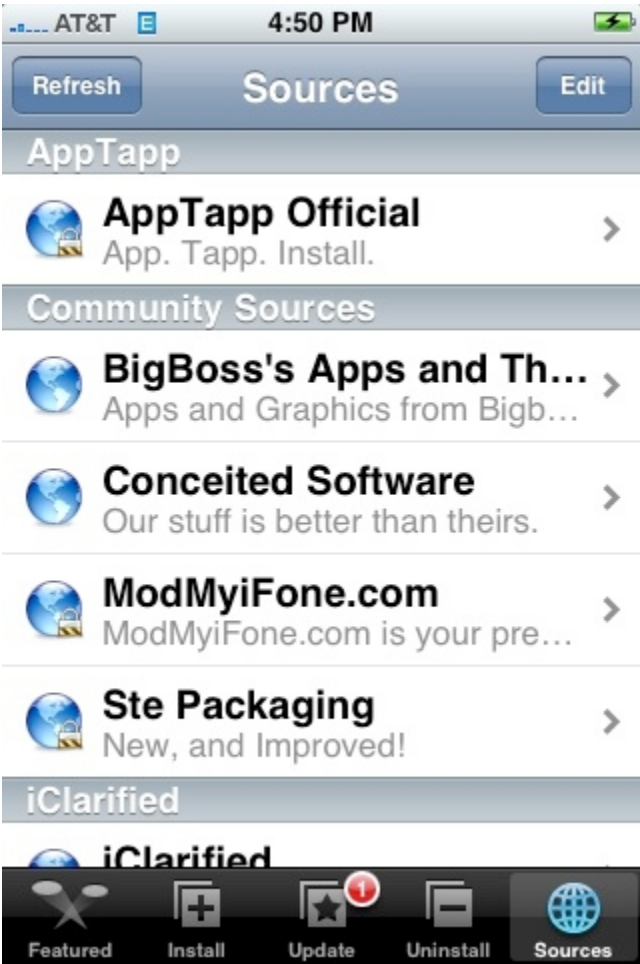


Figure 1-3 iPhone firmware 1.1.4 Installer Sources

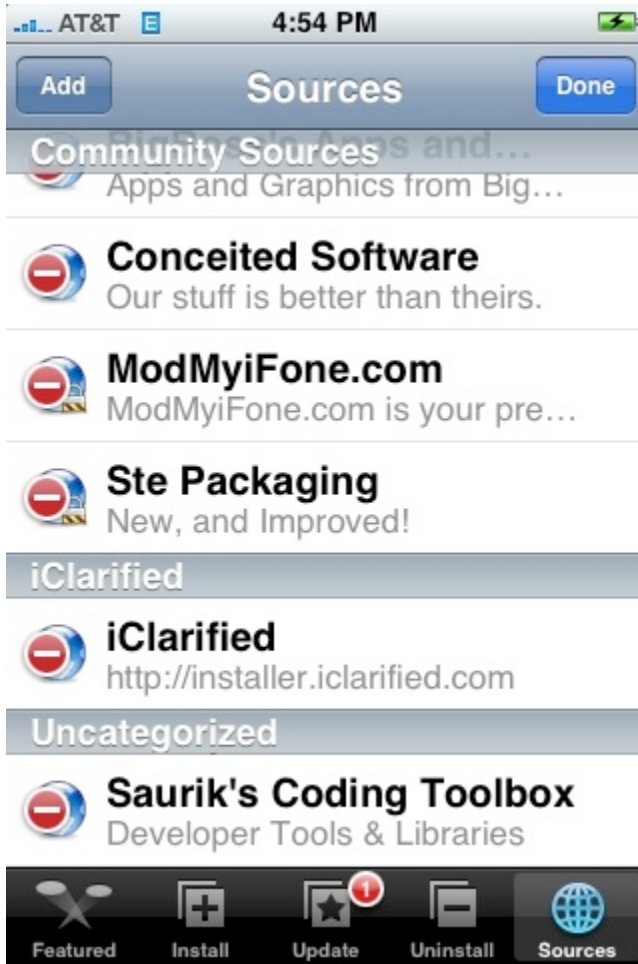


Figure 1-4 Added New Source for installing Cydia on a Jailbroken iPhone



Figure 1-5 Cydia Packer Install for the iPhone, which is to replace Installer



Figure 1-6 Packages Starting N under Networking in Cydia such as netcat which is a simple socket manipulation tool



Figure 1-7 rdesktop which offers a way to remotely connect to a windows machine



Figure 1-8 Shows the package for tcpdump which stores network traffic

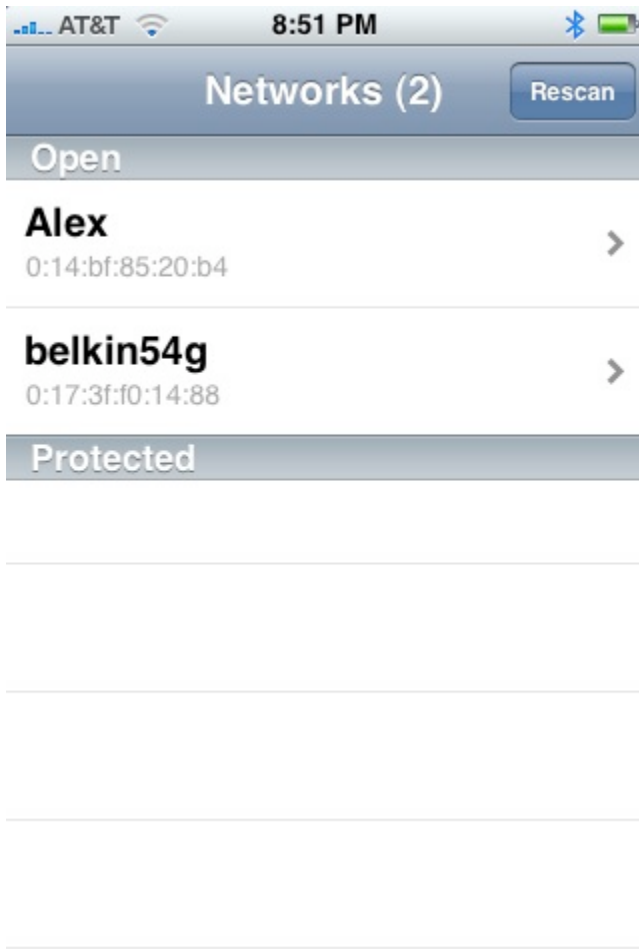


Figure 1-9 Stumbling upon two different wireless networks

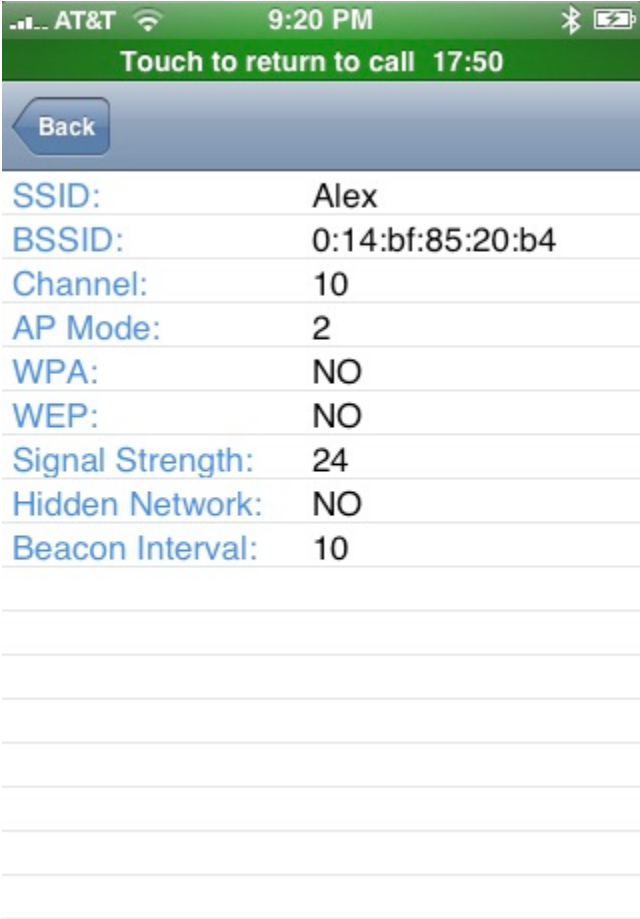


Figure 1-10 Using Stumbler to discover information about wireless network “Alex”

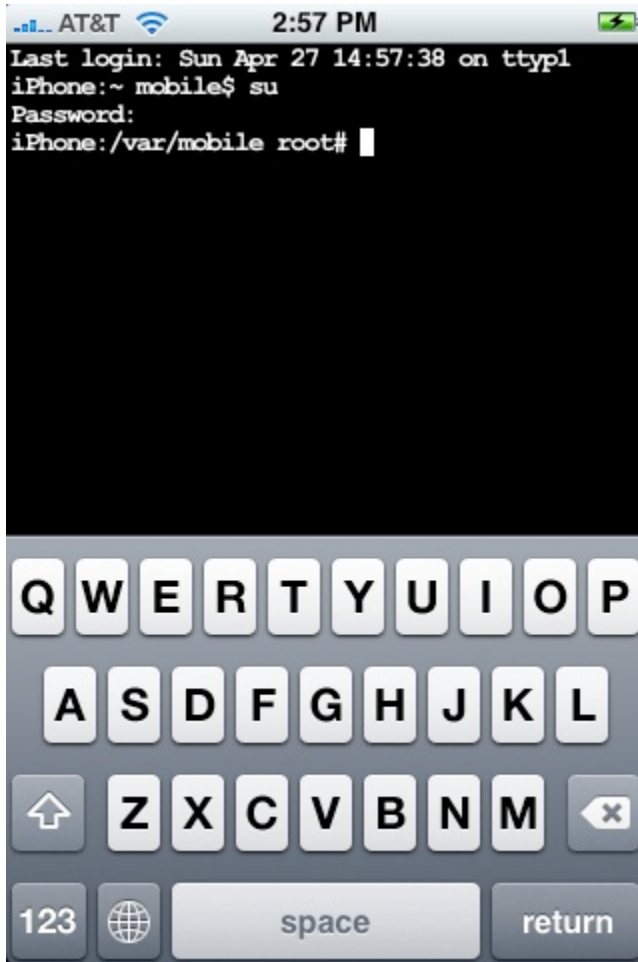
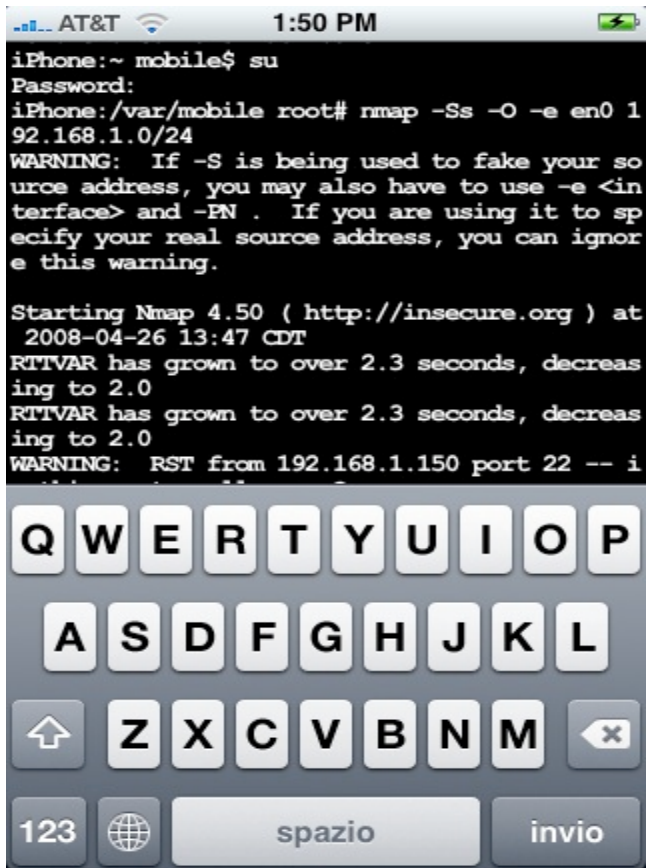


Figure 1-11 Becoming root on the iPhone

A screenshot of an iPhone's terminal application. The status bar at the top shows 'AT&T' as the carrier, signal strength bars, a Wi-Fi icon, the time '1:50 PM', and a battery icon. The terminal text shows a user switching to root with 'su', then running 'nmap -Ss -O -e en0 192.168.1.0/24'. The output includes a warning about the -S flag, the Nmap version (4.50), the start time (2008-04-26 13:47 CDT), and RTT statistics. A keyboard is visible at the bottom of the screen.

```
iPhone:~ mobile$ su
Password:
iPhone:/var/mobile root# nmap -Ss -O -e en0 192.168.1.0/24
WARNING: If -S is being used to fake your source address, you may also have to use -e <interface> and -PN . If you are using it to specify your real source address, you can ignore this warning.

Starting Nmap 4.50 ( http://insecure.org ) at 2008-04-26 13:47 CDT
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
WARNING: RST from 192.168.1.150 port 22 -- i
```

Figure 1-12 Port scanning using Nmap on the iPhone

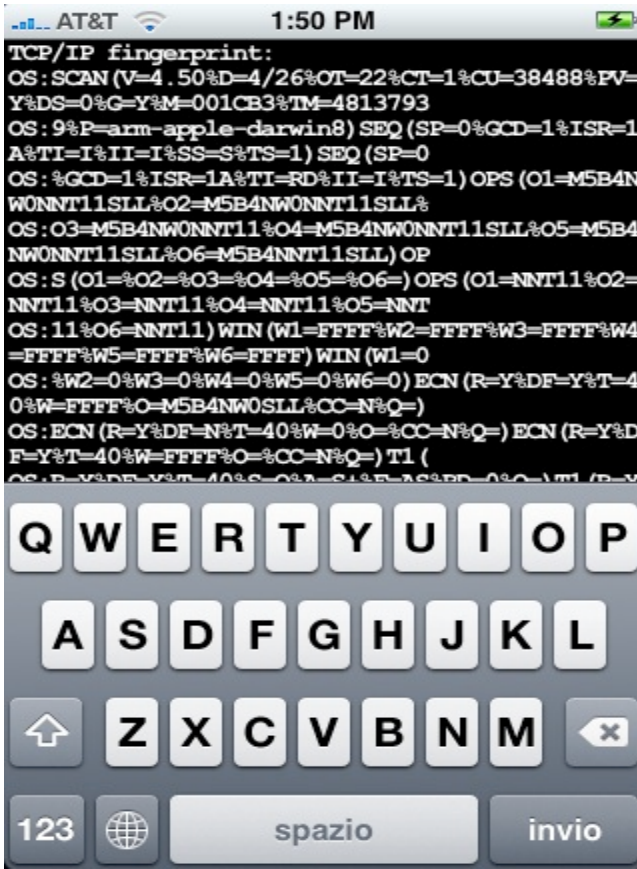


Figure 1-13 TCP/IP fingerprint using Nmap from iPhone



Figure 1-14 HidePod, where users may hide there porn or applications