

Forum:[Hack Forums](#)

Thread: [\[Android/iOS\] Mobile Hacking Overview | How to hack from a cellphone](#)

Linux™ - July 16, 2016, 12:24 pm

Remember to drop a comment to keep this thread alive, else you're just being cancer.

DEFCON had published a guide based on converting an iPod touch into a "mobile pentesting lab" by adding modules to a jailbroken device, tools such as nikto, metasploit, nmap, and sqlmap, and much more are covered, it can be found "I'll update after ten posts" or just google "DEFCON hacking with an ipod" on google

Web-Based tools: Web Based Booters

Websites that provide information for things such as doxing Online bins for posting/dumping raw data

Online text/email spoofer Anonymous emails

Free PPTP VPN's can give your device proper anonymity.

Useful Apps: RDP Apps

SSH Apps Photoshop Mobile (Used for forging photos)

PDF Editors(Used for Social Engineering) SIP Trunk/Telephony Apps EG(Skype, textnow, textfree, textplus.)

IRC Client Apps

[+] Subsection Index:

1. RDP Uses
2. SSH
3. IRC, and Botnets on the go.
4. [Android Exclusive] zANTI MITM Attacks
5. [iOS Exclusive] Blocking skype resolvers
6. Social Engineering on the go, and phone phreaking.

1. RDP (Remote Desktop protocol) or simply applied to as an "RDP" is a virtualized workstation much like a virtual server, but with a GUI interface, a windows 7 RDP can be rented out fairly cheap, some practical uses may be using windows based pentesting/hacking programs from a virtualized place, be wary as a providers aup could lead to suspension or worse, but this may be ideal for RAT's, etc. Or used to host web servers, and much much more.

2. SSH (Secure SHell) Secure shell is a command-line based login protocol for remote computer management, usually associated with servers or nix based systems, you have the power of the entire command line at your disposal, lets just for a moment pretend we have a debian 7 VPS with decent specs, what can we do? You can set up an IRC daemon, and host a botnet, install mtasploit, nmap, nikto, sqlmap, you name it the full power of a linux machine at your fingertips is a very amazing experience. This closely relates to RDP's but is more on the "cheaper" and lightweight side. Want a deal, you can get an OpenVZ server from interserver with the coupon code "1cent" for the first month for a penny, if you know your way around you can easily exploit this ;)

3. IRC Botnets (Internet Relay Chat Bot Network) is a type of botnet that is powered by internet relay chat an old, yet flexible form of instant messaging platform that's been around since the 1980's. For example AndroIRC is a free Android IRC client with a wide range of customizable settings, regardless of the exploit used lightaidra, webdav, pma, telnet, etc. If you have a botnet at your disposal you have a wide range of options from DDoS attacks, to email spam, to downloading

and running other forms of malware. Imagine using a keylogger, and having email hooked up to your phone, passwords sent by the hundreds right to your cellular device. Spreading using your botnet to use a self-replicating worm.

4. zANTI MITM Attacks, and Rooted android. zANTI is a pentesting application developed via android SDK, it is a local-network based application for many things, but includes functions such as SSL stripping, and MITM attacks which can be used to harvest credentials. Thinking of this has me excited for the release of the cicret android bracelet which is still under development, but imagine pulling out your phone after ordering your morning starbucks coffee, you look over and see some poor sap looking at movie ratings, and decides to log into his netflix account, well you're in luck fire that baby up, and wait for him, or someone to log into netflix, use their account for your own viewing pleasure, of course you can do much more than this practical example.

5. Blocking Skype resolvers on iOS, now this method is fairly easy. All you do once logged into skype is go to settings>advanced> "Allow direct connections to contacts only" close the app, and kill the running process, or just reboot your phone, and you're done.

6. Social Engineering, and phone phreaking. Now this will be cut short a bit, but we'll mainly focus on phone phreaking, now lets discuss voicemail/answering machines, usually there's a service code, or action performed when the phonenumber is transferred to "voicemail" on mobile networks sometimes you can hit the * key, and it'll ask you for a password, or to enter "the ten digit phone number" the number will be the phone line you just called common examples to try are as follow the last four digits of the phone number. "0000" "1234" "9999" or something like "1111" but for numbers 1-9, sometimes you can get a "call spoofing" app or spoof the caller ID, and "make the number call itself" sometimes this will let you directly in, if they haven't setup their voicemail this is perfect. Now lets discuss some social engineering tactics, lets say you have some kmart in the middle of bumfucked nowhere, you google another location, ask for the following, the managers name, the store number, and then get the address off of google, next call your kmart and pretend to be a manager at the establishment you just called, and ask for someones help, something along the lines of forgetting the "intercom extension", just drag the conversation out, and then thank them, wait a bit and redial, pose as someone from corporate, and ask for a transfer to the extension without telling them the intercom, then once it goes through you should be live on the intercom.

I should have posted this some time ago. Never the less, now you guys have it, and yes I am the original author.

iKinky - July 21, 2016, 11:55 pm

Only real cool thing is zAnti. Didn't they merge recently, though?

Ace Of Jesus - July 21, 2016, 11:57 pm

Please link, I want to do this with my ipod bro

iKinky - July 22, 2016, 12:08 am

Btw you need root for zAnti. It's pretty dope, I replaced all the images on my network with stupid pics for like a week.

Monostable555 - July 22, 2016, 12:13 am

I remember doing this many years ago, I thought it was so cool that you could run MSF and other "PC" apps on your phone. Now I just have a lightweight laptop with me running Kali.

Thanks for the tutorial!

Linux™ - July 22, 2016, 10:10 am

(Jul 21, 2016 11:55 PM)iKinky Wrote: [\[CITE\]](#) Only real cool thing is zAnti. Didn't they merge recently,

though?

This layout is months old, I'd cypypasta'd an old thread of mine on a different forum.

XADX - *July 25, 2016, 1:15 pm*

Anyone have a link for this :)