

introduction

hacking from the restroom

YOU SHOT THE SHERIFF 3.0 - SÃO PAULO/SP

BRUNO GONÇALVES DE OLIVEIRA

BRUNO.AT.BSDMAIL.COM



\$ whoami?

- computer engineer
- hold some certs
- security analyst / independent researcher
- pentester {comp/network/webapp}
- speaker at security cons {H2HC IV/
ToorCon X/YSTS 2.0}

Schedule

- Motivations !
- Our goal !
- Why cellphones?
- How ?
 - What do we already have ?
 - Some Demos!
- Concerns and Challenges
- Conclusions

Motivations



Goal



Why cellphones?



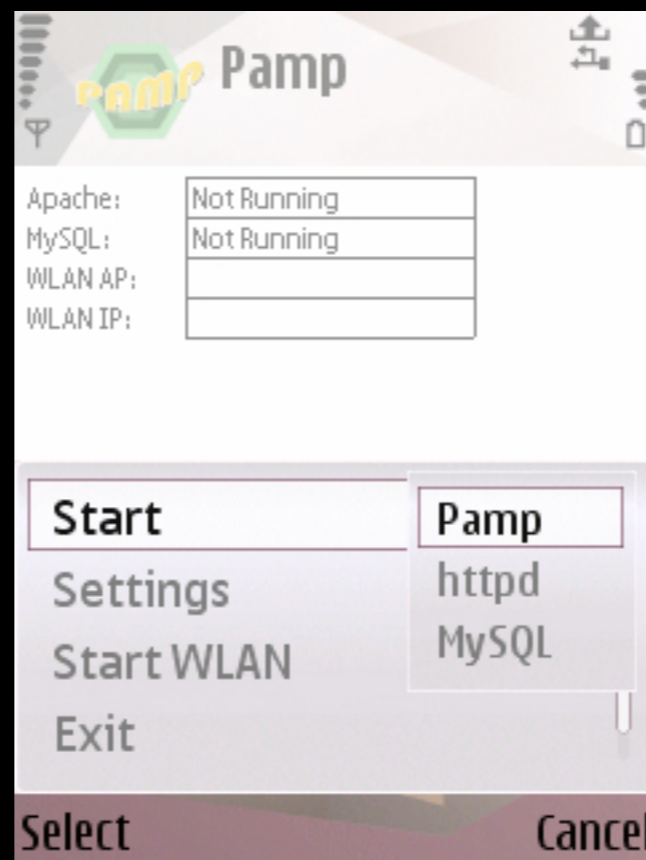
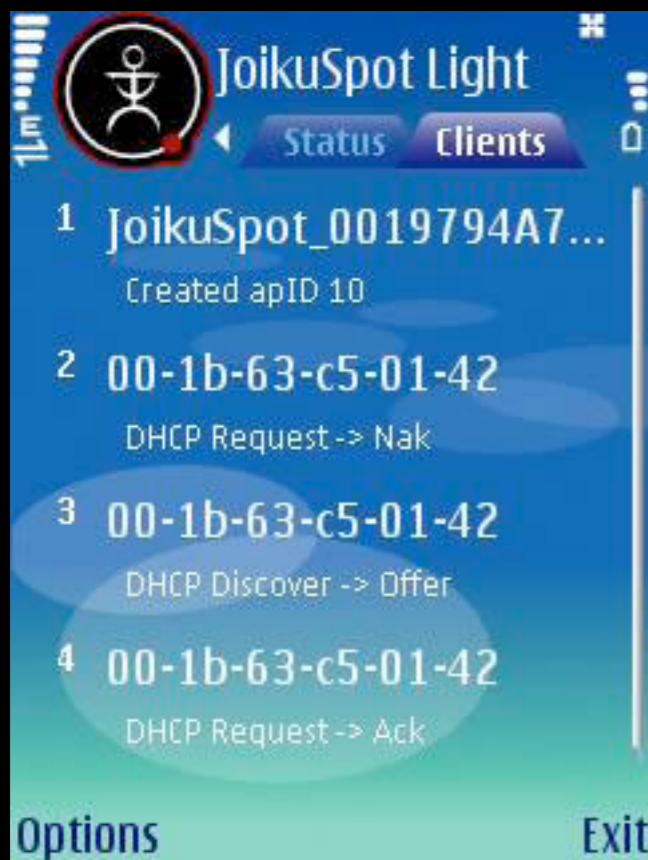
How?



How > Softwares for sharing and selling (ordinaries)

- JoikuSpot => Sharing connection through the wi-fi for Symbian
- PAMP => Portable Apache + MySQL + PHP: Need more?
- Almost ALL Clients (HTTP, FTP, VNC, RDP, SSH, SOCKET) to Almost ALL mobile OSs

Screenshots



How > Softwares for sharing and selling (h4ck1n)

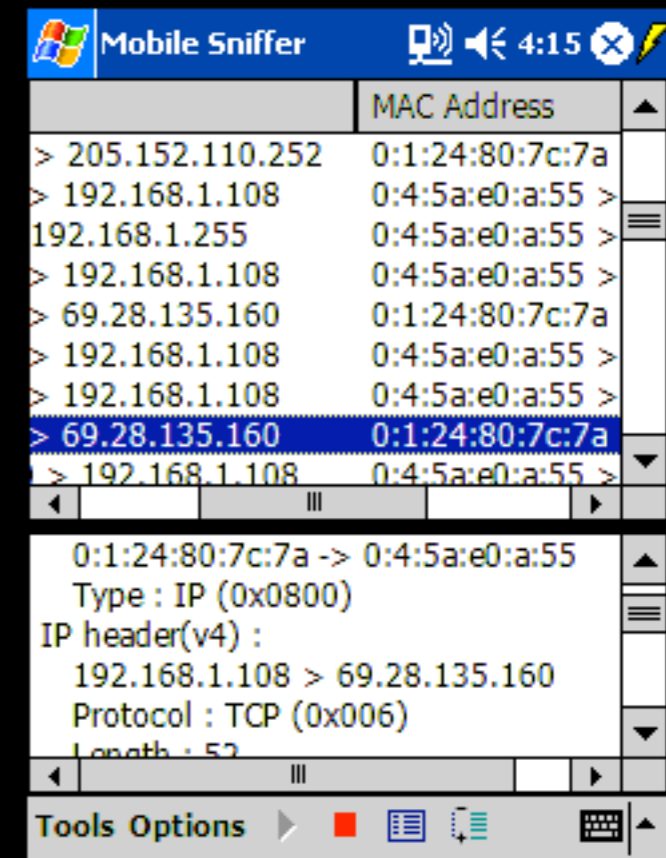
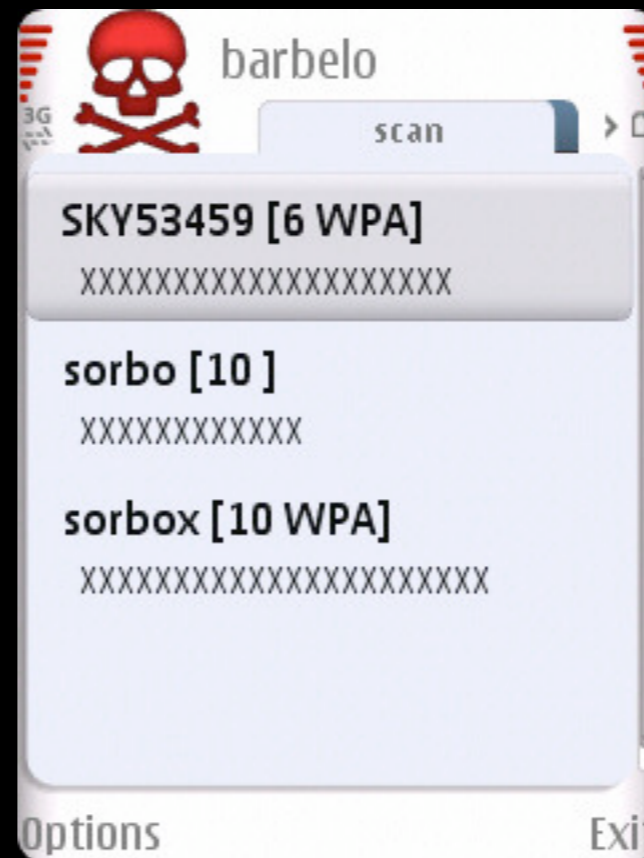
- Metasploit Framework
- Pirni Arp Spoofer & Packet Sniffer
- Nmap
- NeoPWN (have you ever seen this? => www.neopwn.com)
- Silica & SilicaQ => www.immunitysec.com/products-silica.shtml
- Barbelo Wi-Fi Scanner for Symbian

Screenshots

```
AT&T 8:13 PM
ok_extractiptc.rb
A modules/exploits/windows/browser/ibmlot
usdomino_dwa_uploadmodule.rb
U modules/payloads/singles/osx/armle/vibr
ate.rb
A modules/payloads/singles/osx/x86/exec.r
b
U modules
U documentation/users_guide.pdf
U documentation/users_guide.tex
A data/msfweb/patches
A data/msfweb/patches/filehandler.rb
U data/msfweb/config/environment.rb
U msfcli
Updated to revision 5546.
muts:~/framework-3.1 mobile$
```



A virtual keyboard overlay is positioned at the bottom of the terminal window, featuring a standard QWERTY layout with keys for letters, numbers, space, and return.



How > Develop

- SDKs for ALL!
 - Windows Mobile => <http://msdn.microsoft.com/en-us/windowsmobile/default.aspx>
 - Symbian => <http://forum.nokia.com/>
 - **Android => <http://developer.android.com/>**
 - iPhone OS => <http://developer.apple.com/iPhone/program/>
 - BlackBerry => <http://na.blackberry.com/eng/developers/>
 - **OpenMoko => http://wiki.openmoko.org/wiki/Openmoko_developer_guide**
- Python for ALL as well!

My Little Toys

Nokia E65

Symbian S60 9.1



iPod Touch 2G

Mac OS X



Demo(1)

- What: Client-Side Attack
- Tools: PAMP + Telnet Client
- Vuln: IE7 Uninitialized Memory Corruption
- Payload: Bind Port
- Toy: Nokia E65

Demo (2)

- What: MITM
- Tools: Pirni
- Toy: iPod Touch

Demo(3)

- What: Reverse Shell
- Tools: SSH Client and Daemon
- Toy: iPod Touch

Concerns and Challenges

- Attacks just (somewhere) inside the target perimeter, really?
- Faster and better;
- QWERTY always welcome, virtual kbd of iPod Touch rox;
- Even with *jailbroken* phones, we can't play in kernel land; Android and OpenMoko may rule!

Conclusions

- Ah! Do your best!

\$ locate me

- Contact: bruno@bsdmail.com
- LinkedIn: <http://linkedin.com/in/brunogoliveira>
- Blog: <http://g0thacked.wordpress.com/>

Thank you ALL! ;)