HITB SECCONF 2009

MALAYSIA

5TH - 8TH OCTOBER 2009

HACKING FROM THE RESTROOM

HITB SECCONF2009
MALAYSIA
5TH - 8TH OCTOBER 2009

iBLISS

INTRODUCTION

HITB SECCONF 2009
MALAYSIA
5TH - 8TH OCTOBER 2009

$ whoami

- Intrusion Analyst at iBLISS
- Computer Engineer
- Holds some certs
- Over 10 years having fun/ studying/working with security
- Spoken at ToorCon X (USA), H2HC IV and YSTS 2.0/3.0 (Brazil)

AGENDA

- MOTIVATIONS
- GOAL
- WHY CELLPHONES?
- HOW?
- DEMOS
- ISSUES AND CONCERNS
- CONCLUSIONS

Motivations

- Pentest more than we used to do
- Just 0days?
- Unknown power in hands ha ha ha
- New market
- A lot of softwares
- Utilize ur phone!

CELLPHONE MYTHS

Discovery

HITB SECCONF2009
MALAYSIA
5TH - 8TH OCTOBER 2009

GOAL

- CELLPHONES CAN DO INTERESTING STUFFS
- PENTEST PLATFORM? NAH!
- A LOT OF RESOURCES!!

WHY CELLPHONES?

HITB SECCONF2009
MALAYSIA
5TH - 8TH OCTOBER 2009

Nokia looking for n900 hackers
Posted by l33tdawg on Tuesday, September 15, 2009 - 01:21 AM (Reads: 197)

Source: Pocket Lint

Normally most companies frown upon users hacking the software to meet their own needs, however Nokia is taking the rather different approach of actually organising an event around it.

PUSH N900 as it will be called, is a "A unique hack and mod project for designers, creatives, coders and hackers using the new Nokia N900". The event, being held in London, is calling for people to tell Nokia how they would hack and mod the N900 to connect it to something you love like a big screen TV for example.

The creations/ideas will be judged by Kari Tuutti from Nokia and Olavi Toivainen from Maemo with the best ones showcased in Nokia's flagship stores around the globe. "With its innovative open source Maemo platform, 32GB internal storage and sleek design, the Nokia N900 has a speed and raw power which will be even more powerful in the hands of the UK's best hack and mod creatives. We can't wait to see the results," said Tuutti.

Digg submit

Little Toys(1)

- Nokia E65
- Symbian S60 9.1

LITTLE TOYS(2)

- IPOD TOUCH 2G
- MAC OS X

HOW?

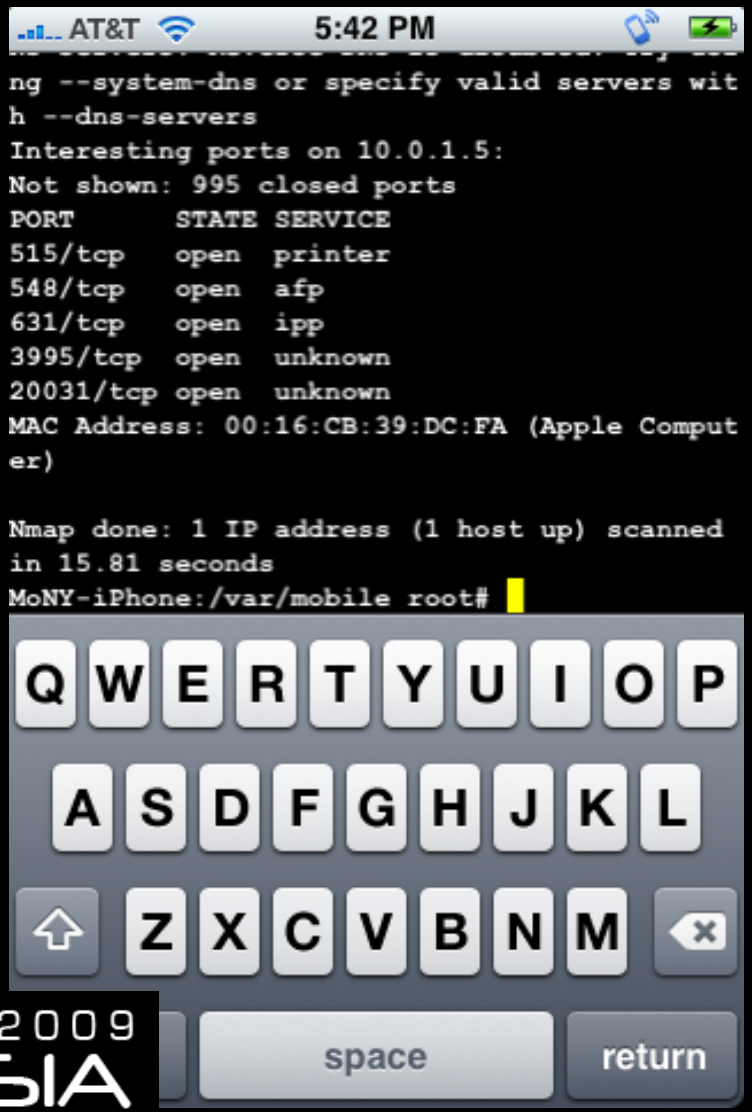
- UNIX SYSTEMS
- SDK FOR EVERYTHING!
- ORDINARY TOOLS CAN HELP
- HACKING TOOLS ALREADY DONE*
- WI-FI CONNECTION

PENTEST STEPS

INFORMATION GATHERING

- BROWSERS
- ALMOST ALL CLIENTS (RDP, TELNET, FTP, VNC, ETC)
- PORTSCANNERS
  - SIMPLY DONE IN ANY LANGUAGE
  - NMAP UP AND RUNNING!

NMAP RUNNING ON IPHONE/IPOD TOUCH



SCANNING

- NIKTO FOR WEB (SCRIPT LANGUAGES ALWAYS WORKS)

EXPLOITING

- LONG CONCEPT
- SERVER-SIDE & CLIENT-SIDE
- PRIVILEGE ESCALATION

- IN ALL WE HAVE OUR PHONES! ☺

EXPLOITING(SERVER-SIDE)

- METASPLOIT

Exploiting (client-side)

- Creativity
  - PAHP (Portable Apache + MySQL + PHP)
  - Any exploit (mainly for browsers)
  - Social engineer and/or phishing
  - Our first demo!

DEMO(1)

- WHAT: CLIENT-SIDE ATTACK
- TOOLS: PAMP + TELNET CLIENT + SOCIAL ENGINEER
- VULN: IE7 UNINITIALIZED MEMORY CORRUPTION
- PAYLOAD: BIND PORT
- TOY: NOKIA E65

PRIVILEGE ESCALATION

- BRUTE-FORCE ONLINE
  - BRUTE-FORCE OFFLINE, NECESSARY?
- ARP POISONING
- SNIFFERS
- SECOND DEMO

DEMO(2)

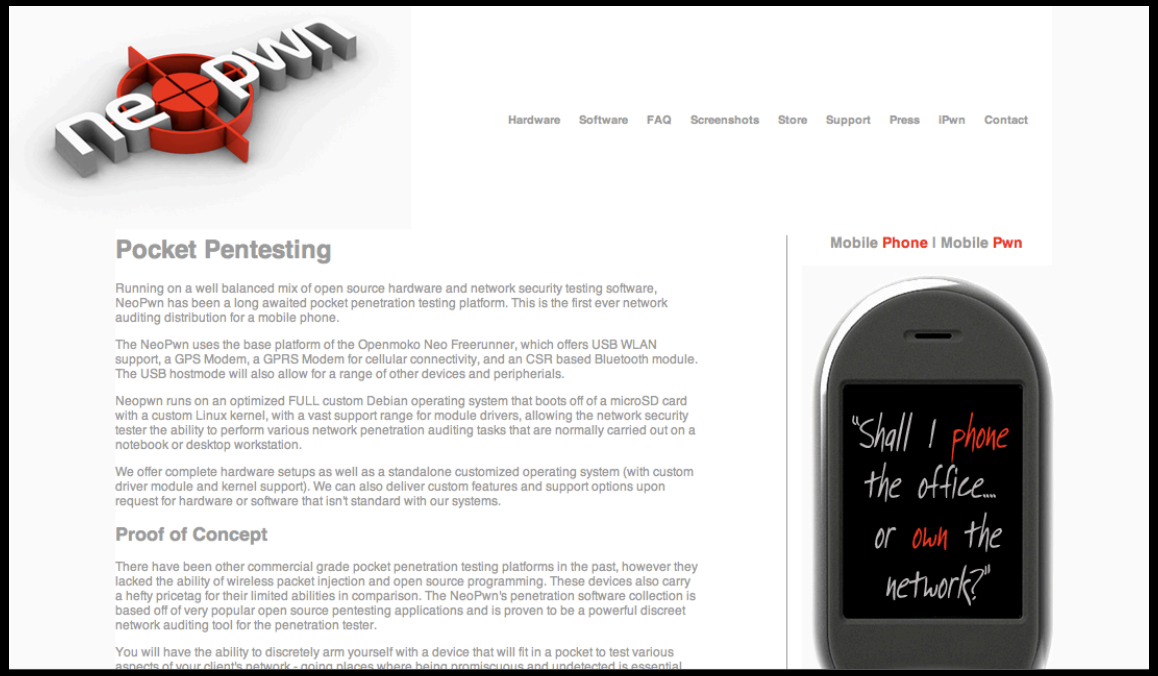
- WHAT: HITH
- TOOL: PIRNI
- TOY: IPOD TOUCH

Maintaining Access

- SSH Daemon & Client
- Netcat
- Stunnel

HAVE SOMEONE EVER SEEN THAT?

- NEOPWN
- HTTP://WWW.NEOPWN.COM/



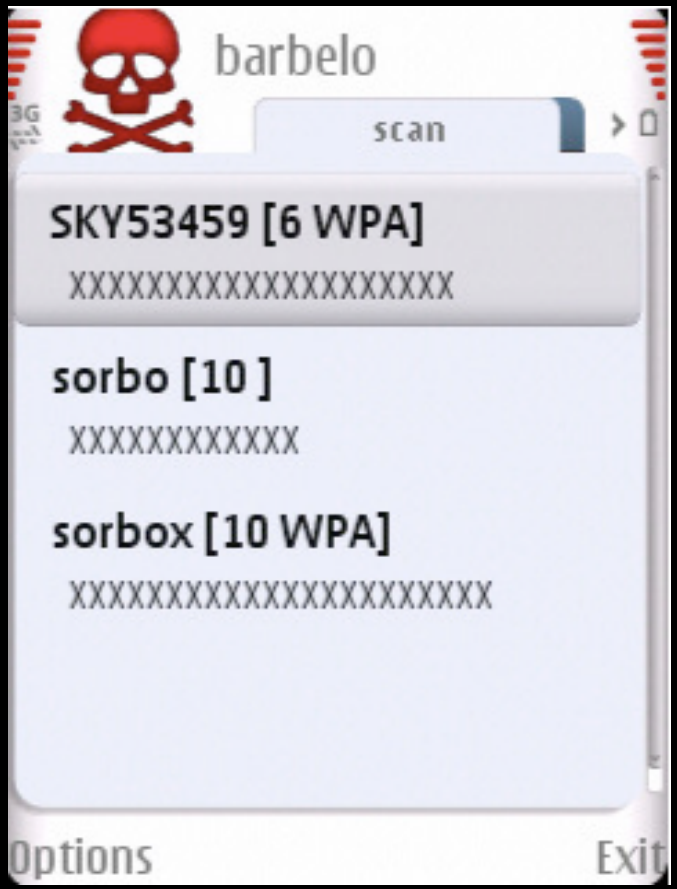
WHAT ELSE?

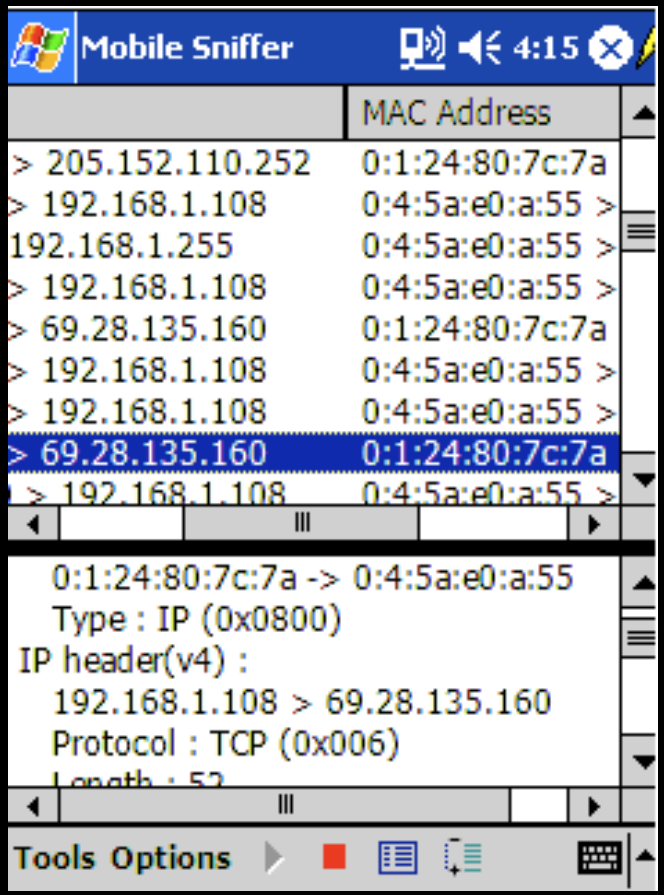
HITB SECCONF 2009
MALAYSIA
5TH - 8TH OCTOBER 2009

802.11 ATTACKS

- BARBELO (WI-FI SCANNER) FOR SYMBIAN
- MOBILE SCANNER (PROMISCUOS MODE) FOR WINDOWS MOBILE
- SILICA & SILICA Q FROM IMMUNITY (DUMPING AND CRACKING)

SCREENSHOTS





802.15 (BLUETOOTH) ATTACKS

- BLUETOOTH SCANNERS AND SOME EXPLOITS (BLUESNARF, ETC)
  - BTBROWSER & BLOOVER FOR MOBILE (MADE IN JAVA)

SCREENSHOTS

WHAT ABOUT IMAGINATION?

HITB SECCONF 2009
MALAYSIA
5TH - 8TH OCTOBER 2009

ROGUE AP

- JOIKUSPOT
  - SAME SSID, ATTACK IS READY
  - USER WILL NOT MAKE DIFFERENCE (AD-HOC CONNECTION)

SNIFFING KEYSTROKES??

- LASER ROX, I KNOW THAT – BUT CELLPHONES AS WELL !!
- CELLPHONES HAVE MICROPHONES, RIGHT?
- SOUNDS INTO WOOD TABLE?

- DANIELE AND ANDREA CAN GIVE A SHOT! :D

SMS ATTACKS

- ZANE & LUIS DID A GREAT JOB ABOUT THAT!
- MANIPULATE PDUS FROM CELLPHONE (THE ECONOMY)
- T.A.F.T. – HTTP://WWW.BLACKHAT.COM/PRESENTATIONS/BH-USA-09/LACKEY/BHUSA09-LACKEY-ATTACKINGSMS-SLIDES.PDF

MORE?

HITB SECCONF 2009
MALAYSIA
5TH - 8TH OCTOBER 2009

JUST DEVELOP!

- SDKS FOR EVERYBODY!
  - SYMBIAN, BLACKBERRY, WINDOWS MOBILE, ANDROID, OPENMOKO, IPHONE, MORE?

ISSUES AND CONCERNS

- ATTACKS JUST FROM INSIDE?
- QWERTY ALWAYS WELCOME – VIRTUAL KBD FROM IPOD ROX TOO!
- FASTER AND BETTER
- EVEN *JAILBROKEN* PHONES LIMIT US, OPENMOKO AND ANDROID MAY RULE!
- NEW GADGETS, NOT JUST PHONE: ZUNE HD

CONCLUSIONS

- LET'S THINK MORE IN WHAT WE ALREADY HAVE IN HANDS
- IMAGINATION MAKE US BETTER HACKERS! ☺
- EACH ONE MAKE YOURS ☺

$ locate me

- Contact: bruno.mphx2 *nospam* gmail.com
- Linkedin: http://linkedin.com/in/brunogoliveira
- Blog: http://g0thacked.wordpress.com/
- IRC: #securityguys@freenode.net
- Conferences around the globe (hope see you in H2HC) ☺

THANKS!

- ORGANIZERS!!!
- BRAZILIAN SECURITY FRIENDS (LEO CAVALLARI – BOSS ;), SPOOKER, BSDAEMON, ANDERSON RAMOS, COIDELOKO, FLAMBERS, MR.BILLY, LE, C4ROL, ALAN CASTRO, BOGUS, ZUCCO, ETC)

HITB SECCONF2009
MALAYSIA
5TH - 8TH OCTOBER 2009

THAT'S ALL

HITBSECCONF2009
MALAYSIA
5TH - 8TH OCTOBER 2009

TERIMA KASIH

HITB SECCONF 2009
MALAYSIA
5TH - 8TH OCTOBER 2009