# GTS 7
# Wireless Intrusion Detection/ Protection Systems

ARUBA™
The Mobile Edge Company

Luiz Eduardo Dos Santos
CISSP, CEH, CWSP, CWAP, CWNA
Lead Systems & Security Engineer
Latin America & Caribbean

# Agenda

- Introduction to Wireless IDS/IPS
- Limitations & challenges
- Bypassing WIDS Systems
- Rogue AP
- WIPS Systems
- The "Tools"
- How to protect yourself
- Conclusion

# Introduction to WIDS

- Not too different from any wired IDS system, but in a new medium
- No wires, but channels
- Different medium different challenges
- But, why?

# Limitations & Challenges

- Some vendors walked (or are still walking) the same path the wired IDS people did (sometimes doing the same mistakes)
- High number of False-positives
- Poor logging capabilities
- Signatures don't help much because of passive tools
- In most cases, unless you have an IDS behind every AP, it won't see everything

# Bypassing WIDS Systems

- Just like wired IDS
- Protocol Fragmentation
- Hacking open-source drivers to change the "standard" behavior
- Protocol fuzzers
- Play with management fragments
- (X) All of the above
- Or... The easy way...

# Rogue Access Points

- Unauthorized & unsecure AP in your network
- It doesn't matter you have the best firewall "protecting" your network from the outside
- It doesn't matter you have the best encryption in your APs
- Search & destroy AND, if possible, FIND it
- ...

# Wireless IPS Systems

- What do they do? Well, protect... Well II, not that much
- Types of defense, show me your IPS-foo
- False-positives, BAAAAD (specially when it's setup to "protect")

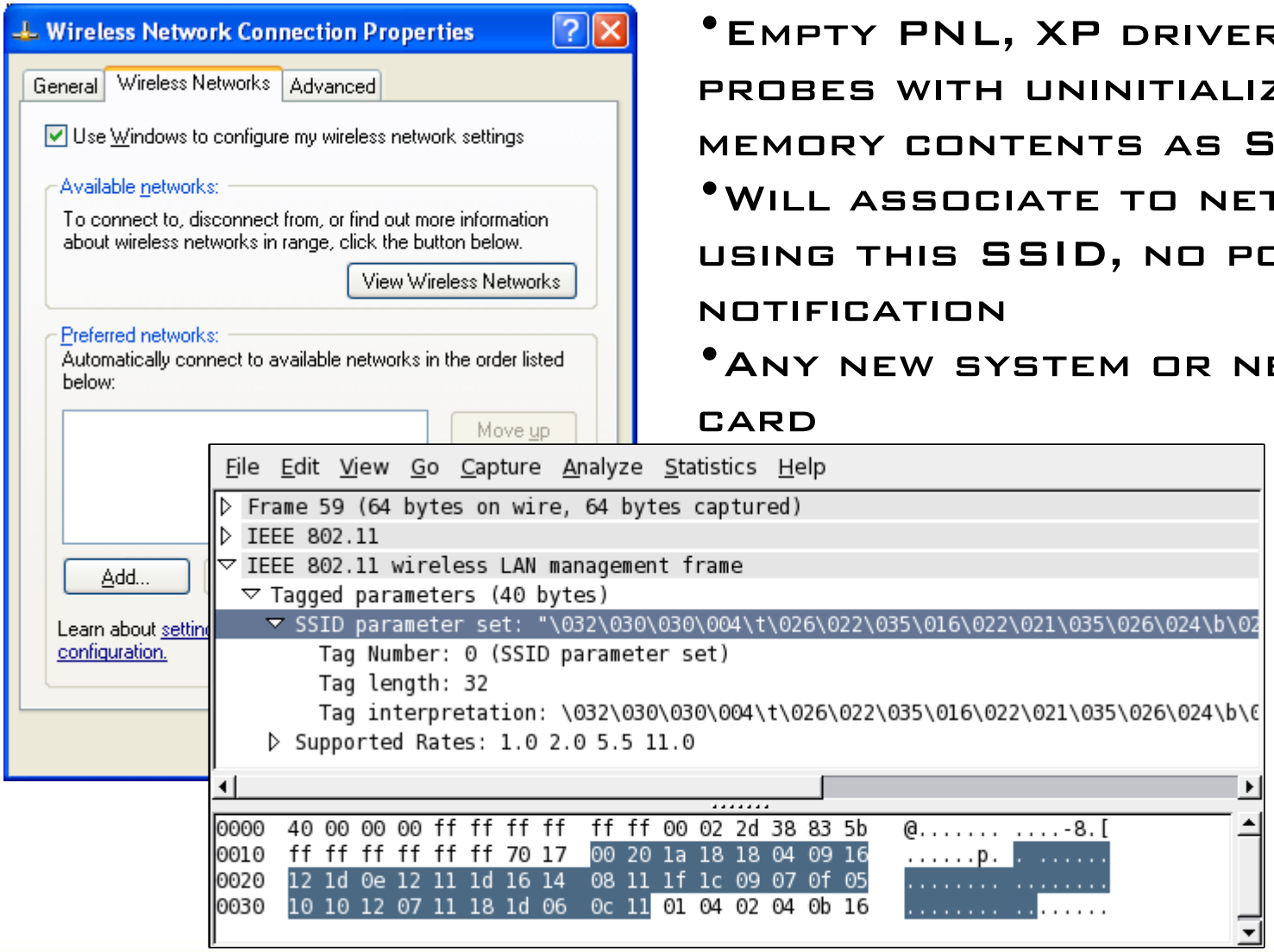
# The "Tools"

- The usual stuff...
- Network discovery tools
  kismet/ netstumbler
- wep-cracking tools
  wpa-cracking tools
  rainbow tables/ sw or hw based
  mac/IP spoofing
  management frames mayhem
  MitM attacks (nah, too old school, you gotta **BE** the MitM providing services and sniffing passwords)
- KARMA
- LORCON
- Packet injection (file2air)
- And more

# KARMA

- Replies to all probe requests it sees
- Provides network level services on demand
- Victim believes they are connected to a valid network/ services
- May be found on Backtrack & Auditor knoppix distros

# Windows XP PNL Weakness




- Empty PNL, XP driver still probes with uninitialized memory contents as SSID
- Will associate to networks using this SSID, no popup notification
- Any new system or network card

# LORCON

- Stands for Loss of Radio Connectivity
- Created to resolve the tool/ driver dependency problem
- In the case of an upgrade, you need to upgrade LORCON and not re-write the application

# How to protect yourself?

- HotSpot defense kit from TSG
- (as usual) apply the security patches for your favorite OS, otherwise something like hacking the friendly skies can hit you
- Do not connect to the **EVIL** network
- WAVEsec (open-source tool for creating IPSec tunnels on WLANs)
- Rogue Scanner by Network Chemistry
- The project from the France Telecom guys

And the old/usual stuff...

- Protect your network (duh!?)
- Change the defaults passwords

# After the commercials...

- Bluetooth could do the same damage
- Other wireless technologies
- Check out wirelessve.org

# Conclusion

- Test it!
- Choose the right system for your needs
- If you have a policy against WLANs, you need to make sure you don't have a WLAN in your company
- Just like a good wired IDS system, pick one that works 24x7
- Take a baseline **BEFORE** you turn on IPS
- WIDS/WIPS might be not enough, your WLAN system should provide secure access
- Keep your eyes opened for the future, people sometimes are VERY creative

# Resources

- http://www.wirelessve.org
- http://www.cwnp.com/forums
- http://www.wifipedia.org
- http://www.shmoo.com/PROJECT
- http://www.networkchemistry.com/products/roguescanner.php
- http://www.arubanetworks.com/support/training/

# Obrigado

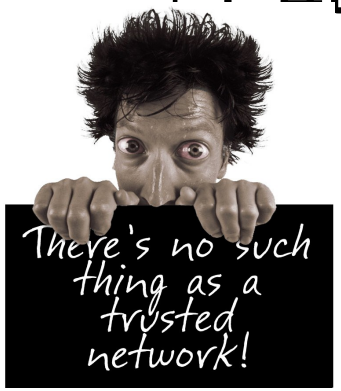
## Comments/ questions/ flames?


Luiz Eduardo Dos Santos

cissp, ceh, cwsp, cwna, cwap

luiz (at) arubanetworks.com

+1 408 646 7869


No. 314159265

TO PROTECT OUR SERVERS

**Network Police Department**

**NETWORK TRAFFIC VIOLATION**

YOU ARE HEREBY CITED FOR THE FOLLOWING OFFENSE(S) AGAINST PROPER NETWORKING:
YOU MUST ANSWER TO THIS SUMMONS, FOR ALL SUSPECTS ARE GUILTY UNTIL PROVEN INNOCENT.

| FIRST NAME | LAST NAME | INITIAL |
|---|---|---|
| ADDRESS (EMAIL) | MONTH / DAY / YEAR | TIME ☐ AM ☐ PM |

OPERATING SYSTEM: ☐ WIN 3.1 ☐ WIN 95 ☐ WIN 98 ☐ WIN NT ☐ MAC OS ☐ UNIX ☐ LINUX ☐ IRIX ☐ AMIGA ☐ SOLARIS ☐ VAX ☐ DOS

ZONE: ☐ .GOV ☐ .EDU ☐ .COM ☐ .MIL ☐ OTHER

TRAFFIC: ☐ NONE ☐ LIGHT ☐ MEDIUM ☐ HEAVY ☐ SATURATED

VISIBILITY: ☐ CLEAR ☐ FLOOD ☐ STORM ☐ SLEET ☐ FOG

THE DESCRIBED DID THEN AND THERE COMMIT THE FOLLOWING OFFENSE(S)
FOR AN EXCESSIVE AMOUNT OF OFFENSES, PLEASE CONSIDER THE GALLOWS POLE.

- ☐ Running an insecure web server.
- ☐ Running pirated software.
- ☐ Running unsupported software.
- ☐ Running a name server with bad or missing PTR records.
- ☐ Running an SNMP scan against a foreign net.
- ☐ Strobing a foreign net.
- ☐ Emitting SMB traffic.
- ☐ Posting make.money.fast ad.
- ☐ Emitting rwho packets.
- ☐ Installing a firewall with an "accept all" policy.
- ☐ Failure to install vendor provided security patch.
- ☐ Allowing 3rd party SMTP relaying / spamming.
- ☐ Bad "postmaster" mail box.
- ☐ SATAN scanning.
- ☐ Open NNTP server for external posting.
- ☐ Picking a random TCP/IP address.
- ☐ Posting to a public list to get your homework.
- ☐ Including too much text in a posting.
- ☐ Sending an "unsubscribe" message to mailing list.
- ☐ Replying "me too" to a "me too" email message.
- ☐ Replying to mail which was Bcc'd.
- ☐ Signature using binary unreadable format
- ☐ Signature more than four lines.
- ☐ Having a guessable password.
- ☐ Having NO password.
- ☐ **Reckless cluelessness.**
- ☐ **Clueless recklessness.**

FAILURE TO RESPOND TO THE VIOLATION AS CHARGED SHALL BE CONSIDERED AN ADMISSION OF LIABILITY AND MANY JUDGEMENTS MAY BE MADE AGAINST YOU IN THE NAME OF BAD TASTE.

| CITING OFFICER | BADGE NUMBER |
|---|---|
| TOTAL POINTS | TOTAL FINE |

TO PLEAD NOT GUILTY FOLLOW INSTRUCTIONS ON REVERSE SIDE

COMMENTS OR NOTES:

NFR

Send questions or comments to:
NFR DEPARTMENT OF FINANCE PARKING VIOLATIONS
http://www.nfr.net