Wireless Security on the Philippine Setting

Introduction:

- **WHOAMI**
- **What's this all about?**

The Philippine Wee-fee setting

- **2004 German hacker finds open Wi-Fi networks in Manila**

  Sept 2004: Van Hauser discovered that only 15 out of the 66 wireless APs were encrypted

- **More Wifi networks on Homes and small businesses**

  - Unaware and indifferent
  - Low or no security (due to cost and convenience)
  - More direct targets

Wireless Security History

- **Open Wireless**
- **WEP**
  - Use of Streaming Algorithm
  - Per packet master key re-use
  - Group use and sharing of the same PSK
  - Lack of Authentication from network to client
  - Confidentiality vulnerabilities with header
  - Integrity vulnerability and replay attacks
- **WPA**
- **WPA2**

Top Wireless Tools

1. Kismet
2. NetStumbler
3. Aircrack
4. Airsnort
5. Kismac

* Pyrit

DEMO

Click Me!

How to Secure?

-Change the defaults
-Long key with wide characters set
- MAC Address filtering
-Limit connections
-Disable DHCP
-Hide SSID or a creative SSID
-Change your key
-Tools
-Active security

"The only truly secure system is one that is powered off, cast in a block of concrete and sealed in a lead-lined room with armed guards."

- Gene Spafford

Credits:

- SecurityUncorcked.com
- InfosecPhils.wordpress.com
- **PGHO (Nogie and Aphro)**