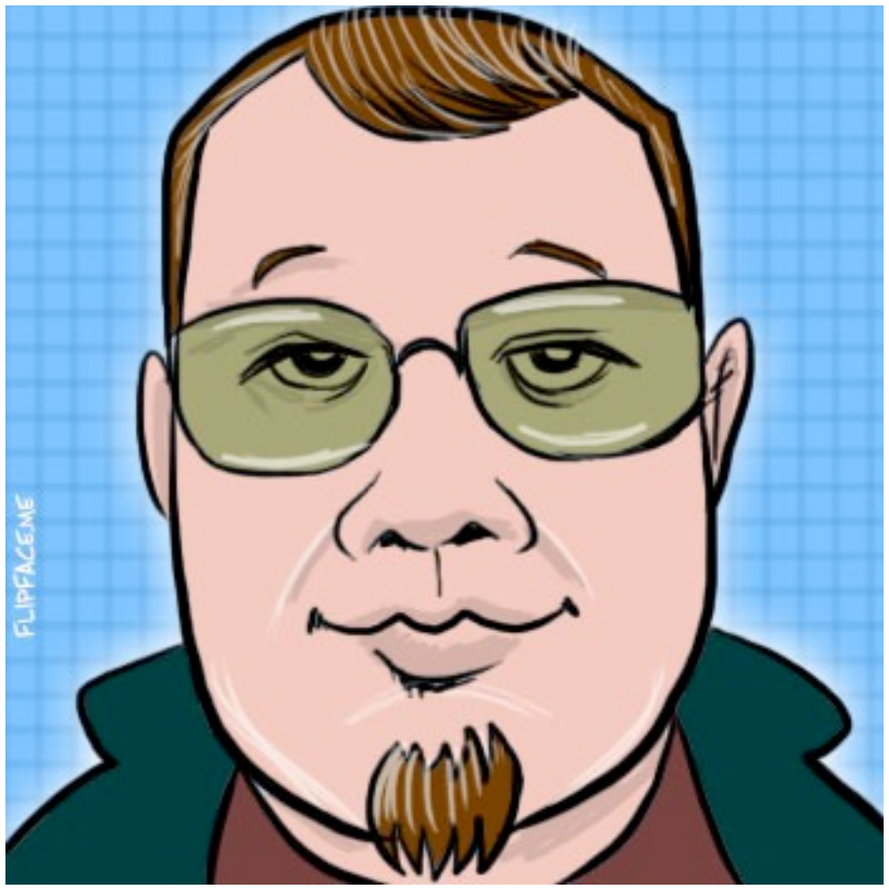
Taming ~~Stuxnet~~ Skynet

Derbycon 2012

Come with me if you want to live.

Who the hell is this guy?

- Not a security guy
- Actually, this is my first con talk
- Hi, I'm Jason Frisvold
- Senior Network Engineer, Lafayette College
- But if I'm not a "security" guy, WTF am I here for?
- Like you, I'm here to learn



friz@godshell.com
@XenoPhage

So Let's Get Started

Taming Skynet

- Catchy name, eh?
- Why Skynet?
- The “Ultimate” in cloud technology
- Out of our control, but maybe we can use it?
- Born out of Mick Douglas’ talk from Derbycon 2011 - Blue Team Is Sexy

The “Cloud”

- Seriously? The Cloud?
- Danger Will Robinson! Religious Territory!
- WTF is "The Cloud" ??
- Why the Cloud? Which cloud?
  - Public - Amazon AWS
  - Private - CloudStack

Ok, so .. The Cloud

But what are you going to do with it?

Baselining!

What is Baselining?

- Google Says
  - A minimum or starting point used for comparisons
- I like this better
  - A normalized view of the network used to detect anomalous activity

Why Baseline?

- Relatively easy way to detect misconfiguration and/or possible breach activity
- Can provide historical network data
- Intelligence on your network
- Easily automated, relatively silent unless it detects something

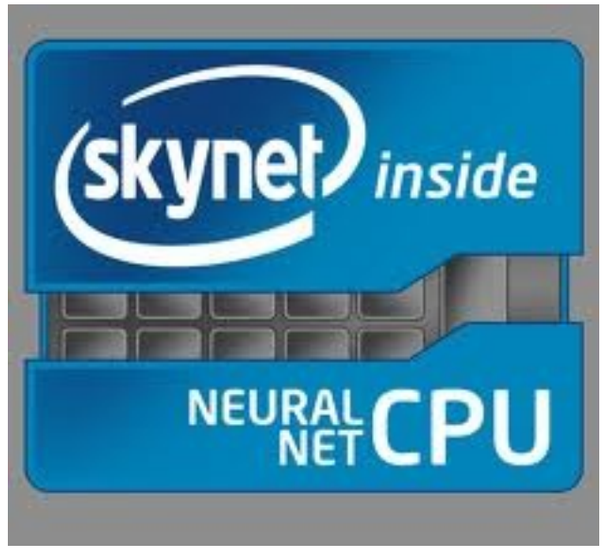
In vs Out

- In-Network Scanning
  - Not a “public” view
  - May be difficult depending on network design
- Out-of-Network Scanning
  - Where the kiddies live

What am I proposing?

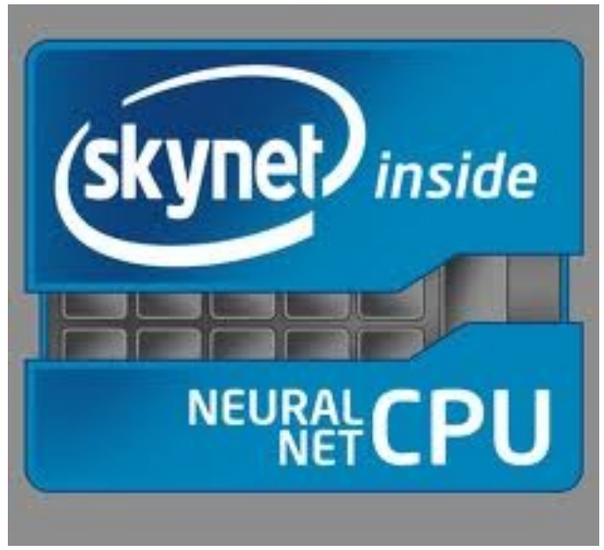
Skynet's New Firmware

- The Cloud Component
  - NMAP
  - Local spawning daemon
  - Scans encrypted on completion
- The Control System
  - Set scan times and options
  - Send/Retrieve data from/to remote systems



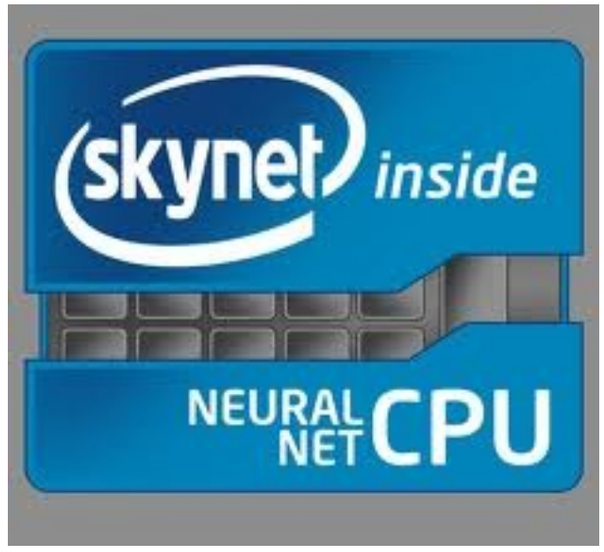
Skynet's New Firmware

- The Visualization System
  - Web-based GUI
  - View past reports
  - Pretty Pictures!
    - # of hosts per scan
    - # of ports per scan



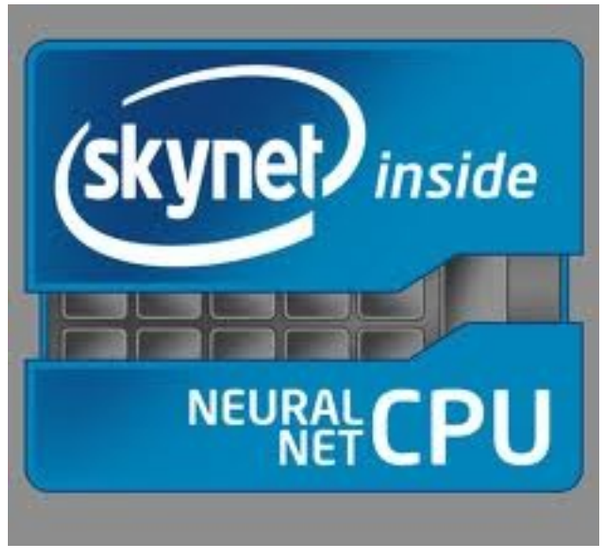
Skynet's New Firmware

- The Reporting System
  - Pre-defined Reports
  - Custom Reports
  - Automated
  - No changes, no report



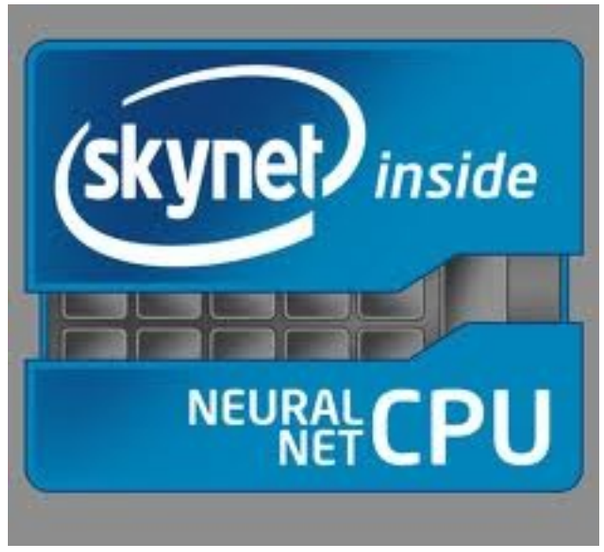
Skynet's New Firmware

- CLI
  - Same capabilities as the GUI
  - Well, except graphs
  - Easily scriptable



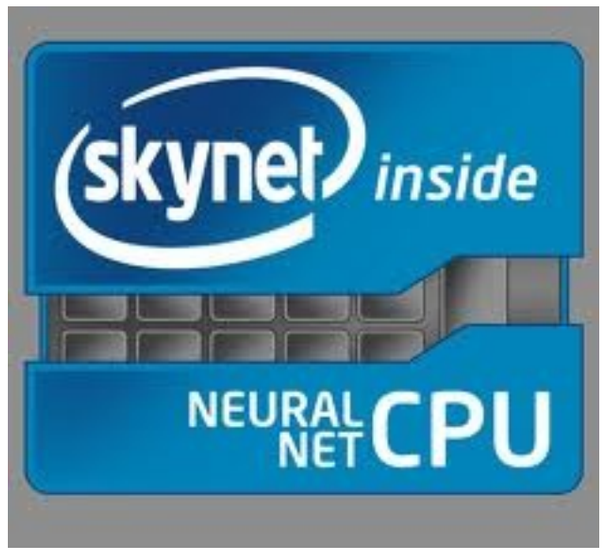
Skynet's New Firmware

- Security!
  - Encrypted Scan Results
  - SSH/SCP
  - Data Scrubbing
  - What am I missing?



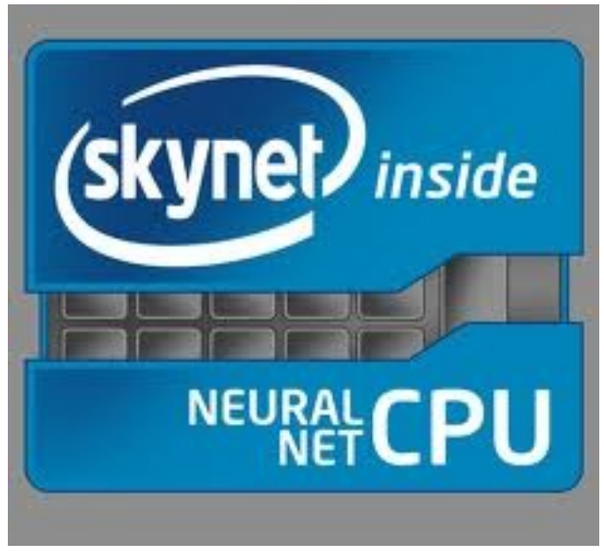
Skynet's New Firmware

- The Back End
  - Python
    - CLI Tools
    - Control Daemons
  - PHP
    - GUI Front End



Skynet's New Firmware

- Data Storage
  - MySQL
    - Metadata Storage
- Git ?
  - NMAP XML Data



So show me already!

Where's the demo?

< Insert Excuses Here >

Current Work

- Design Document (and this talk)
  - http://www.godshell.com/presentations
- ETA on a Beta?
  - Hopefully by January 1
- How can you help?
  - Email : friz@godshell.com
  - Twitter : @XenoPhage

Questions?

Listen, and understand. That terminator is out there. It can't be bargained with. It can't be reasoned with. It doesn't feel pity, or remorse, or fear. And it absolutely will not stop, ever, until you are dead.