# DefCon 12

Scott McFall, IT Commander
Terry Pell, Network Admin
Jeb Barger, NeLEIS Admin


www.skrattnet.com foto: Magnus Andersson


DODGE


NO SMOKING
STOP ENGINE
STOP


D3 9

# What are we going to discuss?

- What exactly is DefCon ?
- Interesting Topics at DefCon
  - Wireless Security
    - HackerBot, AirSnort, Sniper Yagi, 802.11i
  - Google Hacking
  - Exploring Terminal Services and Citrix
  - Morph and Tor
  - Active Network Defense
  - Games that Hacker’s Play

# What Exactly is DefCon?

- “The Largest underground hacking event in the world.”
- Contests, Security Lectures, and Mingling
- 6,000 + Attendees from all over the world
- 75 Lectures, 3 tracks covering all aspects of Security
- All over three days

# Wireless Security

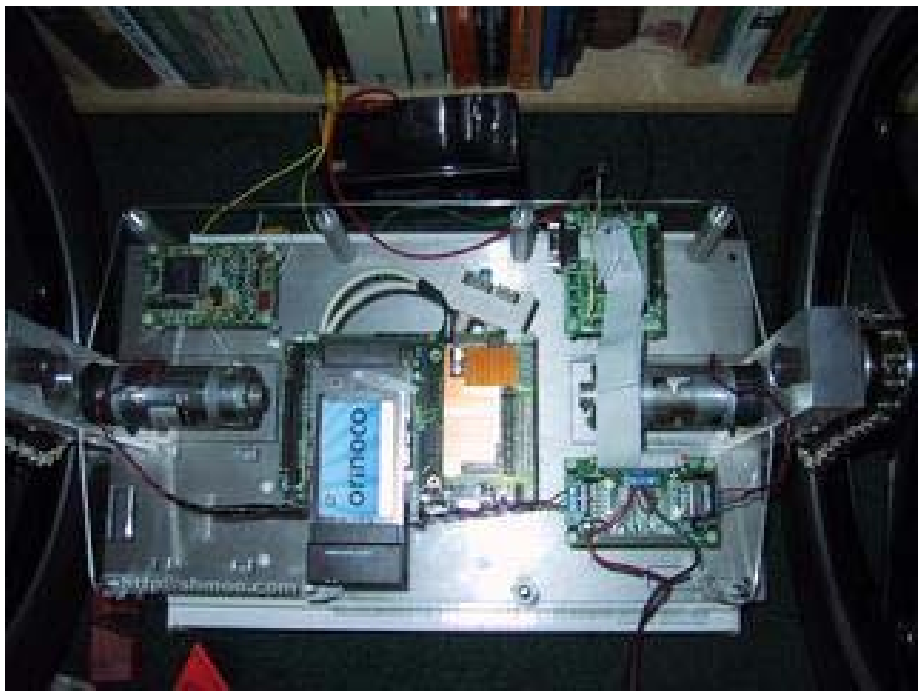

- Presentation by the Shmoo Group
  - www.shmoo.com
  - Shmoo Group is an expert in wireless technologies.
  - Known for AirSnort
    - AirSnort is a tool which recovers encryption keys from wireless networks.

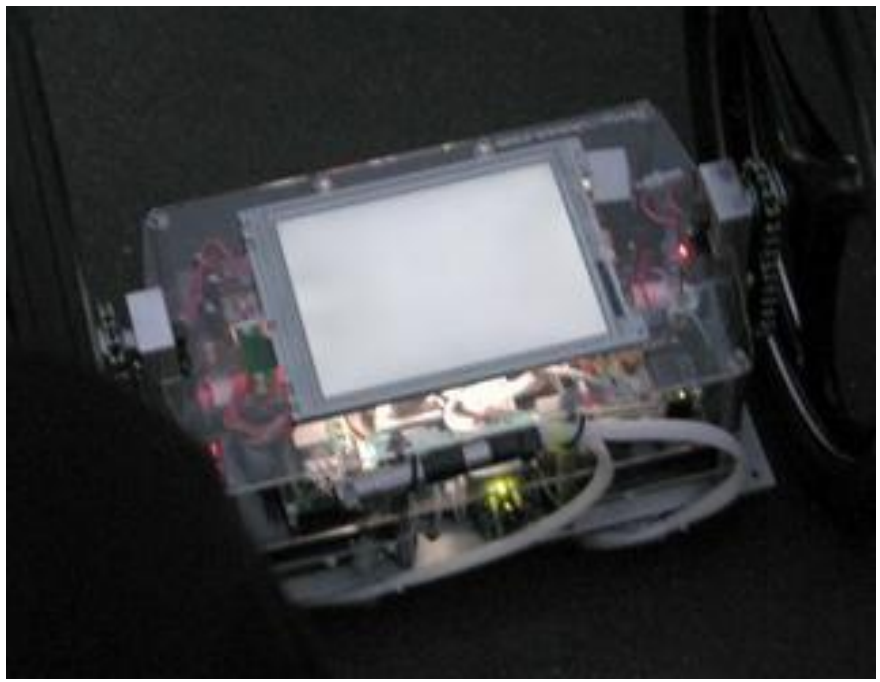
# Wireless Security

- HackerBot
  - A robot designed to move toward a wireless signal, crack the WEP key, and display the WEP key along with other passwords (Email, SSH, etc) back to the user.

THE HACKERBOT, CREATED BY PAUL HOLMAN (LEFT) AND ERIC JOHANSON, IS DESIGNED TO ROAM AROUND AND DETECT INSECURE TRANSMISSIONS IN WIRELESS NETWORKS.

# Wireless Security HackerBot





# Wireless Security


- Super Yagi
  - Created a Yagi resembling a sniper rifle
  - Range of a few miles
  - DON’T STAND BEHIND IT

# Wireless Security


- 802.11i
  - Good Attempt, however, new “Michael Mick” rogue AP can cause problems.
  - Current Encryption Technologies

# Google Hacking

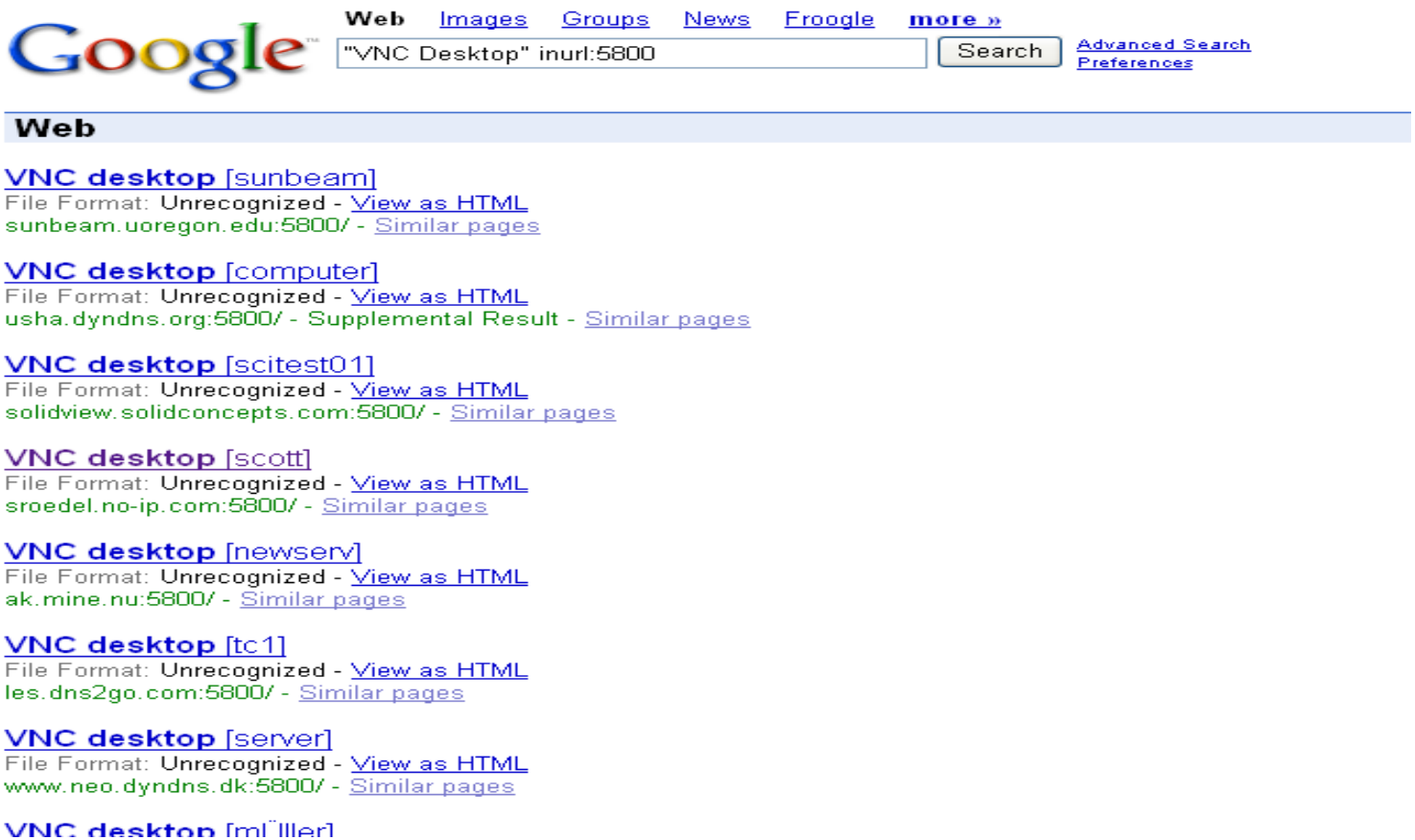
- From Johnny Long's Presentation
  - johnny.ihackstuff.com
- Examples
  - FrontPage Site Passwords
  - VNC Servers
  - Terminal Services
  - Printers
  - Other Stuff

# Google Hacking

- FrontPage Site Passwords

# Google Hacking

- VNC Web Server

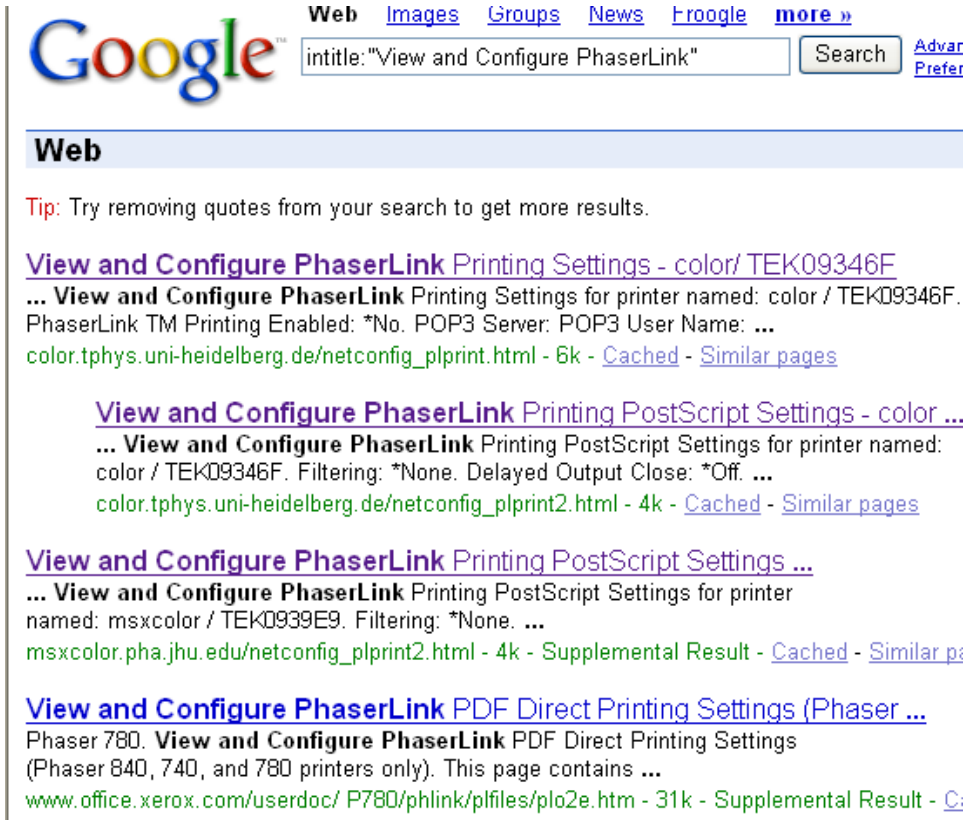


# Google Hacking

- Terminal Services Remote Desktop Web

# Google Hacking

- Printers



# Google Hacking

- Other Stuff
  - Web Cams
  - New Web Server Installations
  - Anything that has a web page
- What can you do about it?
  - Firewall is configured correctly
  - Follow vendors white pages

# Terminal Services and Citrix

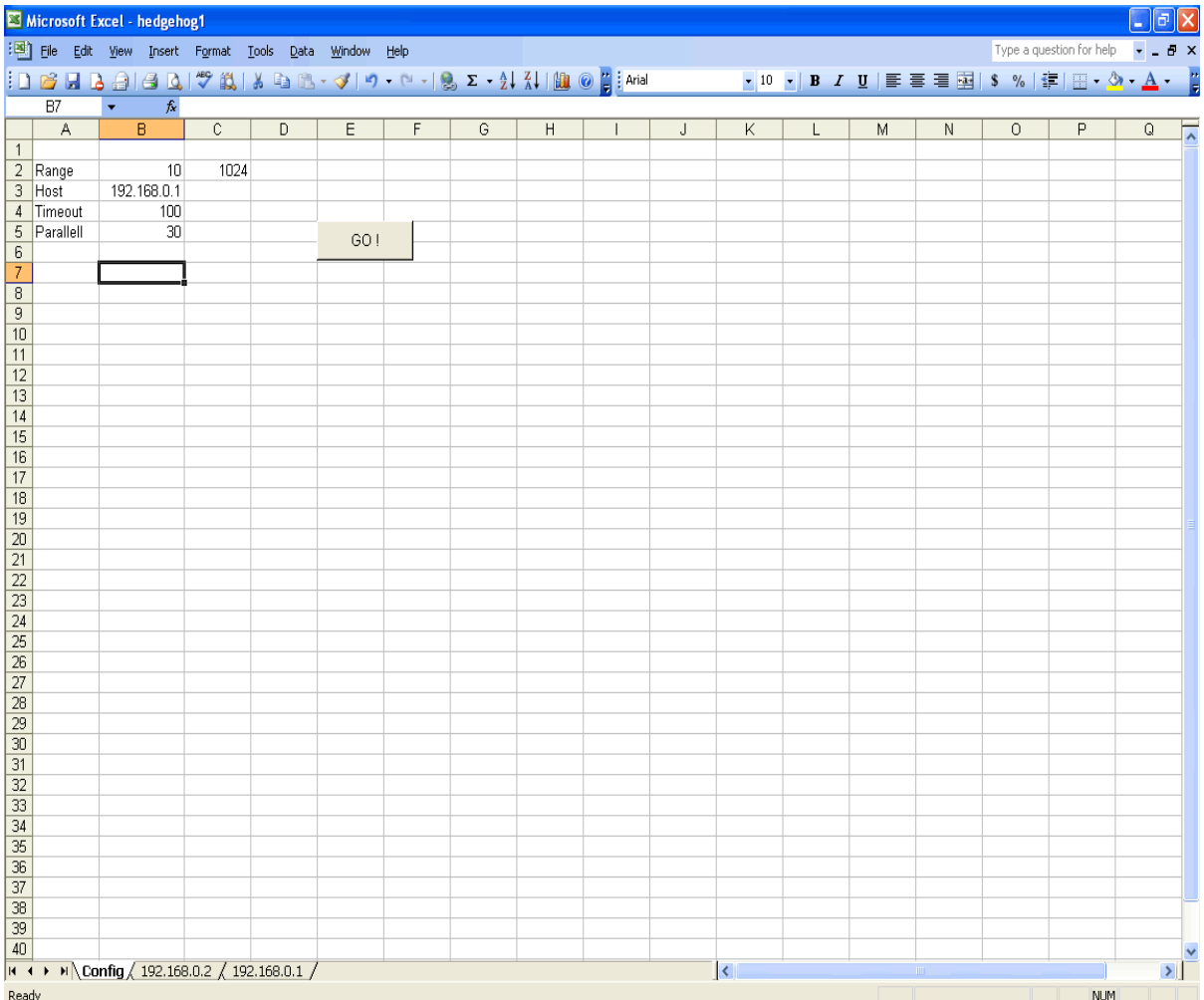
- Presentation given by Ian Vitek and Patrik Karlsson
- www.cqure.net/itools02.html
- Topics Covered
  - Exploring
  - Uploading Files
  - Gaining System
  - Controlling Users and their local network
  - Protection

# Terminal Services and Citrix

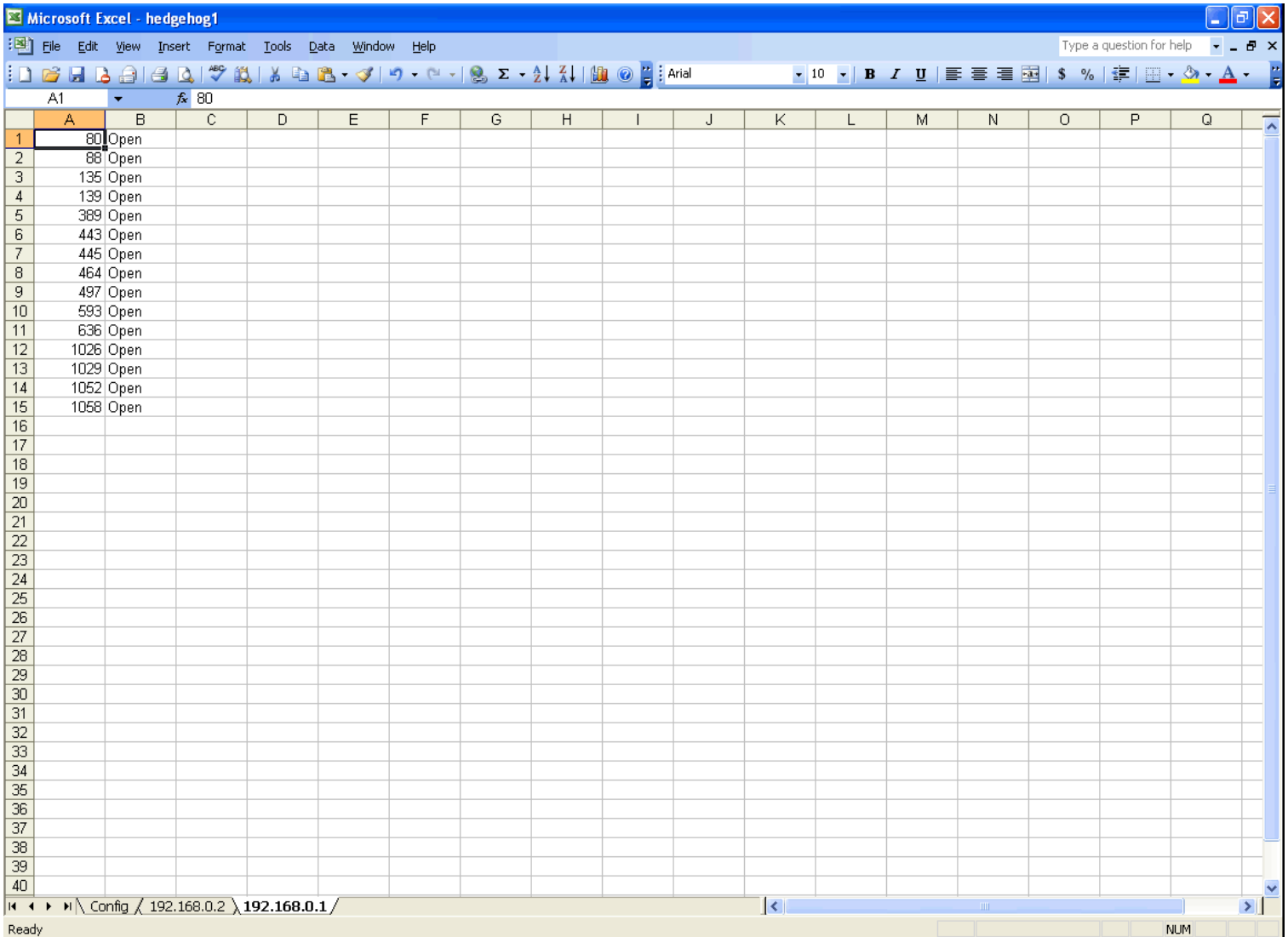
- Exploring
  - The Normal Stuff
    - Net Command (Net Use, Net User, Net View)
    - Neststat –na
    - FTP and Telnet
  - Excel Port Scanner
    - Named Hedgehog
    - Luckily, VBS security set on high will not let it run
    - Example of Hedgehog

# Terminal Services and Citrix

- Hedgehog, an MS Excel Port Scanner



# Terminal Services and Citrix




| | A | B |
|---|---|---|
| 1 | 80 | Open |
| 2 | 88 | Open |
| 3 | 135 | Open |
| 4 | 139 | Open |
| 5 | 389 | Open |
| 6 | 443 | Open |
| 7 | 445 | Open |
| 8 | 464 | Open |
| 9 | 497 | Open |
| 10 | 593 | Open |
| 11 | 636 | Open |
| 12 | 1026 | Open |
| 13 | 1029 | Open |
| 14 | 1052 | Open |
| 15 | 1058 | Open |

# Terminal Services and Citrix

- Uploading Files
  - Normal
    - Client Map
    - HTTP or FTP Transfer
  - Sneaky Way
    - Convert BIN to text (Netsend)
    - Convert Text to BIN (Muud.com)
  - If All Else Fails
    - Upload the files with a keyboard (copywk.pl)

# Terminal Services and Citrix

- Gaining System
  - Trojan Printer Driver
    - Not Released
  - Windows Help Files
    - Yes, let me locate one (cmd.exe)
    - Perl Program to send F1 to any program, including drivers
    - Will give you a command line with System Privileges

# Terminal Services and Citrix

- Controlling Users and their network
  - Steal Citrix Users Disks
    - Winobj from Sysinternals
    - Administrators and System can access all DosDevices
    - Easy to Enumerate drives
      - Citrixmap.exe from cqure
      - Mount Drives
        - Net use * \\client\c$ (Citrix)
        - Net use * \\tsclient\c (Terminal Services)

# Terminal Services and Citrix

- Protection
  - Uploading Files
    - Normal TS / Citrix protection
    - Disable 16-Bit Application Support
  - Programs (Not Tested)
    - Sanctuary
    - CIS
    - Apiguard

# Morph and Tor

- Morph
  - http://www.synacklabs.net/projects/morph
  - Morph is a tool that allows the user to select an Operating System to emulate
    - OpenBSD 3.3 looks like Windows 2000 SP4
    - Fools most OS Scanners
      - QueSO, Nmap, Xprobe, p0f
  - Linux Only for now

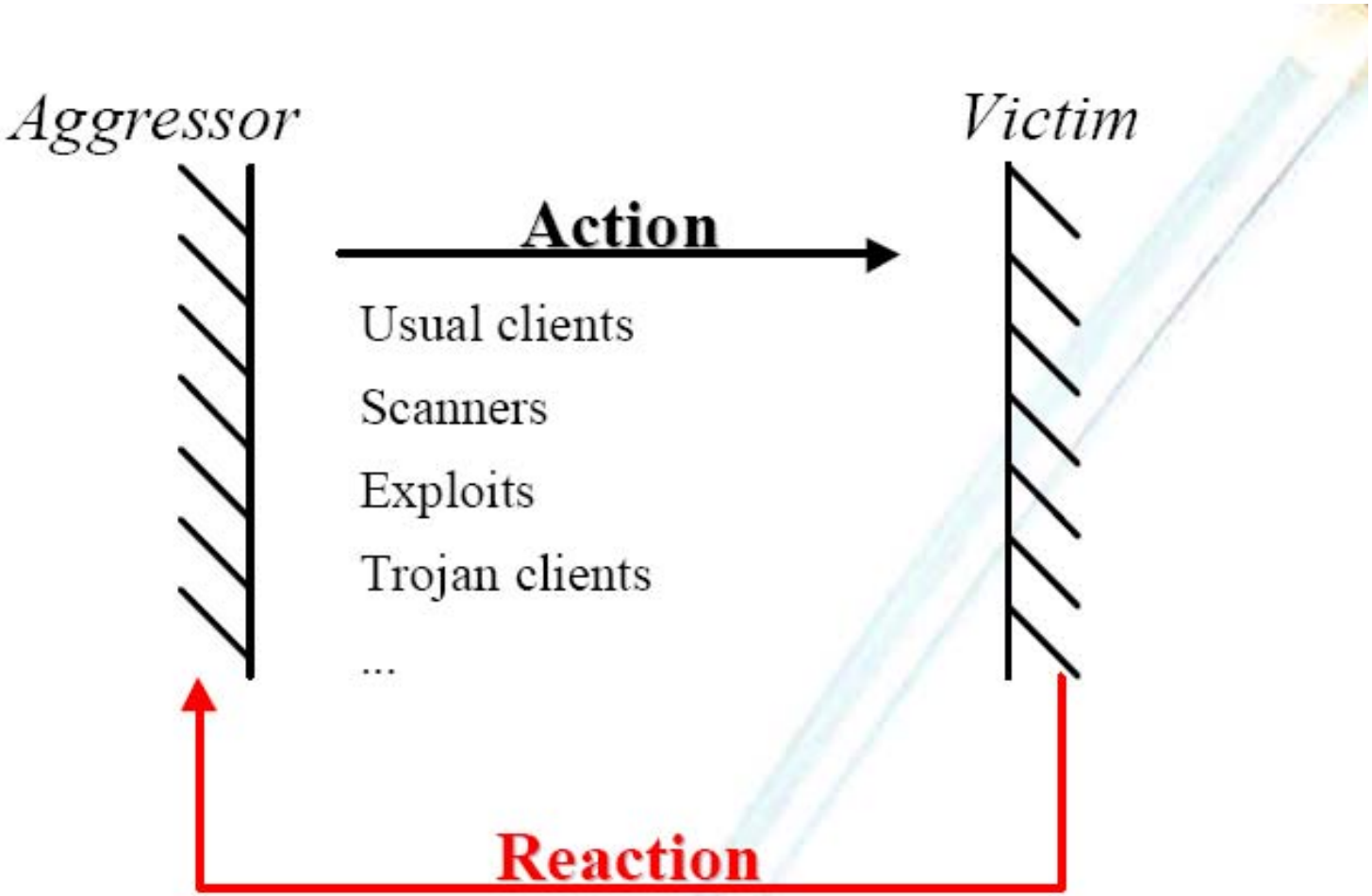
# Morph and Tor

- Tor
  - www.freehaven.net/tor
    - Web site was down
  - Distributed network to anonymize network applications such as web browsing, secure shell, and instant messaging.
  - Encrypted traffic with circuit only knowing its predecessor and successor
  - Bypass all surf controls

# Digital Active Self Defense


- Laurent Oudot
  - www.rstack.org
  - www.sensepost.com
- More Aggressive Network Defense Method
- May or may not be legal

# Digital Active Self Defense

# Digital Active Self Defense


- Examples
  - Cleaning a client that attacked your network with MS Blaster
  - Denial of Servicing (DOS) a computer that is trying to denial of service that is DOSing a computer on your network.
  - Placing your favorite html into your dns when someone tries to use reporting software to view your network

# Games:  Root Fu

- Root FU?  What is that?
  - A game of capture the using computers
  - Teams are given identical Linux x86 distrubutions to host.
  - Each team must defend the host and keep it running
  - Teams can choose to port, upgrade or replace services

# Games: Spot the Fed

- Who is that person next to you at the conference?
  - Wearing Khakis and Clean Cut → FED!
  - Wearing mostly black and scuffy → normal attendee
  - Played in between speakers
  - The “Spotted Fed” goes on the stage and the crowd and MC grill them with questions.
  - If the Fed is real, the spotter gets a t-shirt, “I spotted the fed”.
  - Note to Federal Agencies planning on attending, don’t send the business unit manager, send your agencies geek!

# Games: Others

- Lockpick Contest
- Scavenger Hunt – “Running Man”
- WarDrive
  - Winner had 80,000+ AP
- Wi-Fi Shootout
  - Land Record – 55.1 mile unamplified
  - Ran out of road
  - 19 Year Old’s using 30mw Orinoco Gold USB

# Games: Others

Team P.A.D, from Ohio, left to right: Greg Rigling (Justin's father), Andy Meng, Justin Rigling, and Ben Corrado. For their inventive efforts, the winning team received uber-hacker badges, giving them lifetime admission to DefCon for free.

# Questions ?!?!?

- More Information: www.defcon.org
- Contact Information:
- Scott McFall – SMcFall@nsp.state.ne.us
- Terry Pell – TPell@nsp.state.ne.us
- Jeb Barger – JBarger@nsp.state.ne.us