



# DefCon 12

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



[www.skrattnet.com](http://www.skrattnet.com) foto: Magnus Andersson











# 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](http://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.

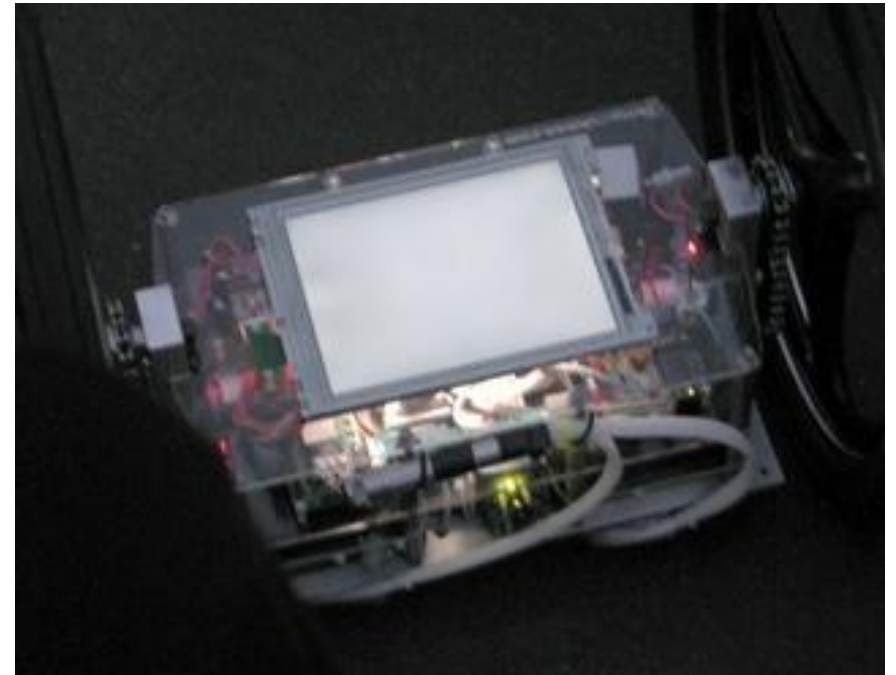
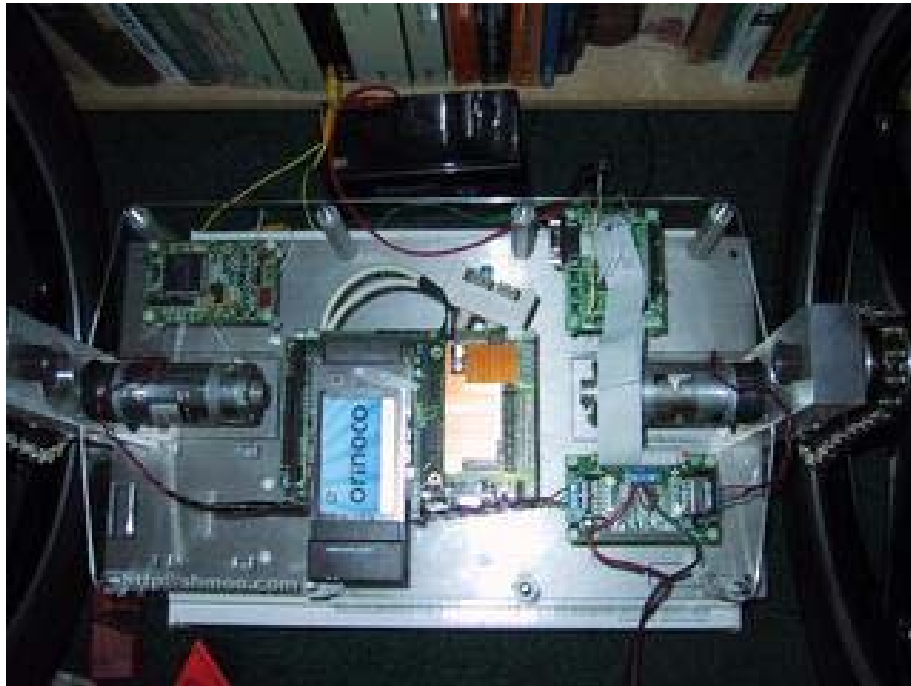
# Wireless Security

## ■ 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.



# 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



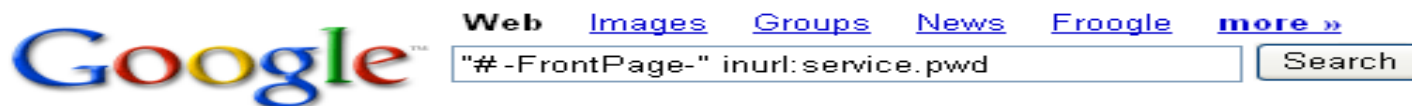
- 802.11i
  - Good Attempt, however, new “Michael Mick” rogue AP can cause problems.
  - Current Encryption Technologies

# Google Hacking

- From Johnny Long's Presentation
  - [johnny.ihackstuff.com](http://johnny.ihackstuff.com)
- Examples
  - FrontPage Site Passwords
  - VNC Servers
  - Terminal Services
  - Printers
  - Other Stuff

# Google Hacking

## ■ FrontPage Site Passwords



### Web

**FrontPage-** [admin:YbV1JnafKRmnQ](#)

# -**FrontPage-** [admin:YbV1JnafKRmnQ](#)

[library.thinkquest.org/C007492F/\\_vti\\_pvt/service.pwd](#) - 1k - [Cached](#) - [Similar pages](#)

**FrontPage-** [ekendall:bYId1Sr73NLKo](#) [louisa:5zm94d7cdDFiQ](#)

# -**FrontPage-** [ekendall:bYId1Sr73NLKo](#) [louisa:5zm94d7cdDFiQ](#)

[www.heyerlist.org/garderobe/\\_vti\\_pvt/service.pwd](#) - 1k - [Cached](#) - [Similar pages](#)

**FrontPage-** [hmchou:TeCdIT2BEIkM6](#)

# -**FrontPage-** [hmchou:TeCdIT2BEIkM6](#)

[www.hint.org.tw/family/\\_vti\\_pvt/service.pwd](#) - 1k - [Cached](#) - [Similar pages](#)

**FrontPage-** [landcruiser:ddA3bHQ3j1sUo](#)

# -**FrontPage-** [landcruiser:ddA3bHQ3j1sUo](#)

[home.off-road.com/~landcruiser/\\_vti\\_pvt/service.pwd](#) - 1k - [Cached](#) - [Similar pages](#)

**FrontPage-** [fpadmin:glV41mLw6l6kg](#) [kherad:GRxN4Aja1rOfY](#)

# -**FrontPage-** [fpadmin:glV41mLw6l6kg](#) [kherad:GRxN4Aja1rOfY](#)

[www.schoolnet.ir/~kherad/\\_vti\\_pvt/service.pwd](#) - 1k - [Cached](#) - [Similar pages](#)

# Google Hacking

## ■ VNC Web Server





# Google Hacking

## ■ Terminal Services Remote Desktop Web



Web [Images](#) [Groups](#) [News](#) [Froogle](#) [more »](#)

[Advanced Search](#)  
[Preferences](#)

Web

Results 21 - 30 of about 564 for intitle:"Remo

### [Remote Desktop Web Connection](#)

... User Name: Password: Remember me. Viewing: Dev Shed Forums > System Administration > Networking > **Remote Desktop Web Connection**. ... **Remote Desktop Web Connection**. ...  
[forums.devshed.com/showthread.php?t=128895&goto=nextoldest](#) - 52k - Supplemental Result - [Cached](#) - [Similar pages](#)

### [Remote Desktop Web Connection](#)

Raytex Travis **Remote Desktop Web Connection**. If server box is empty, type 66.234.227.233 and then click Connect. . Server: Size: ...  
[66.234.227.233:61356/tsweb/](#) - 22k - [Cached](#) - [Similar pages](#)

### [Remote access issues - XP Remote Desktop Web Connection does not ...](#)

... XP **Remote Desktop Web Connection** does not work. thread595-781576. ...  
[www.tek-tips.com/viewthread.cfm?qid=781576](#) - 37k - [Cached](#) - [Similar pages](#)

### [Connectivity Remote Desktop Web Connection](#)

**Remote Desktop Web Connection**. ...  
[www.windowsforumz.com/Connectivity-Remote-Desktop-Web-Connection-ftopic139150.html](#) - 35k - [Cached](#) - [Similar pages](#)

### [Remote Desktop Web Connection](#)

[http://members.dslextre.me.com/users/joshlee/tsweb/default.htm](#). **Remote Desktop Web Connection**. ...  
[jltsweb.cjb.net/](#) - 2k - [Cached](#) - [Similar pages](#)

### [JSI Tip 6104. Windows XP Remote Desktop Connection Web Connection ...](#)

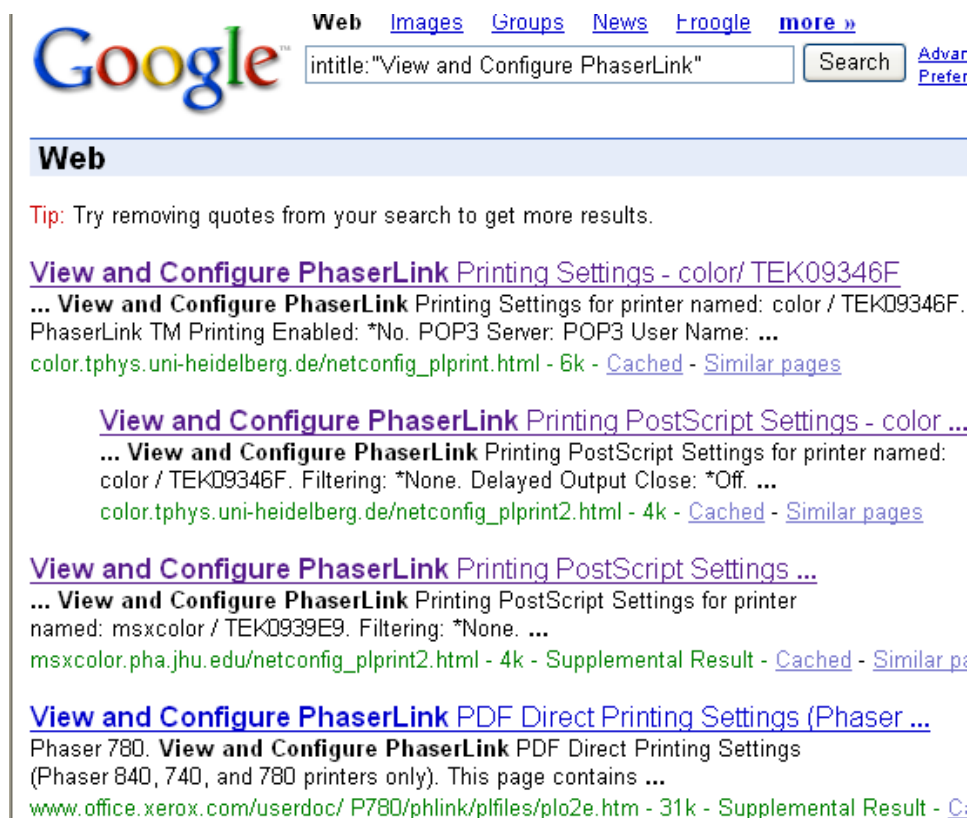
... The **Remote Desktop Web Connection** ActiveX control allows you to access your computer, via the Internet, from another computer using Internet Explorer. ...  
[www.jsiinc.com/SUBM/tip6100/rh6104.htm](#) - 9k - [Cached](#) - [Similar pages](#)

### [Desktop Publishing: Remote Desktop - remote desktop web connection](#)

Internet Directory >> Desktop Publishing >> Remote Desktop >> **remote desktop web connection**. GotoMyPC: Free Download Securely access ...  
[www.silentwords.net/directory/Desktop-Publishing/Remote-Desktop/remote-desktop-web-](#)

# Google Hacking

## ■ Printers



The screenshot shows a Google search interface. At the top left is the Google logo. To its right are navigation links: Web, Images, Groups, News, Froogle, and more ». Below these is a search input field containing the text "intitle:View and Configure PhaserLink". To the right of the input field is a "Search" button and two links: "Advar" and "Prefer". Below the search bar is a "Web" section header. Underneath, there is a tip: "Tip: Try removing quotes from your search to get more results." The search results are listed below, each starting with a link to a document titled "View and Configure PhaserLink" followed by a brief description of the document's content and a link to the full document.

Web [Images](#) [Groups](#) [News](#) [Froogle](#) [more »](#)

Google   [Advar](#) [Prefer](#)

---

**Web**

Tip: Try removing quotes from your search to get more results.

[View and Configure PhaserLink Printing Settings - color/ TEK09346F](#)  
... **View and Configure PhaserLink** Printing Settings for printer named: color / TEK09346F. PhaserLink TM Printing Enabled: \*No. POP3 Server: POP3 User Name: ...  
[color.tphys.uni-heidelberg.de/netconfig\\_plprint.html - 6k - Cached - Similar pages](#)

[View and Configure PhaserLink Printing PostScript Settings - color ...](#)  
... **View and Configure PhaserLink** Printing PostScript Settings for printer named: color / TEK09346F. Filtering: \*None. Delayed Output Close: \*Off. ...  
[color.tphys.uni-heidelberg.de/netconfig\\_plprint2.html - 4k - Cached - Similar pages](#)

[View and Configure PhaserLink Printing PostScript Settings ...](#)  
... **View and Configure PhaserLink** Printing PostScript Settings for printer named: msxcolor / TEK0939E9. Filtering: \*None. ...  
[msxcolor.pha.jhu.edu/netconfig\\_plprint2.html - 4k - Supplemental Result - Cached - Similar pages](#)

[View and Configure PhaserLink PDF Direct Printing Settings \(Phaser ...](#)  
Phaser 780. **View and Configure PhaserLink** PDF Direct Printing Settings (Phaser 840, 740, and 780 printers only). This page contains ...  
[www.office.xerox.com/userdoc/ P780/phlink/plfiles/plo2e.htm - 31k - Supplemental Result - C:](#)

# 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](http://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

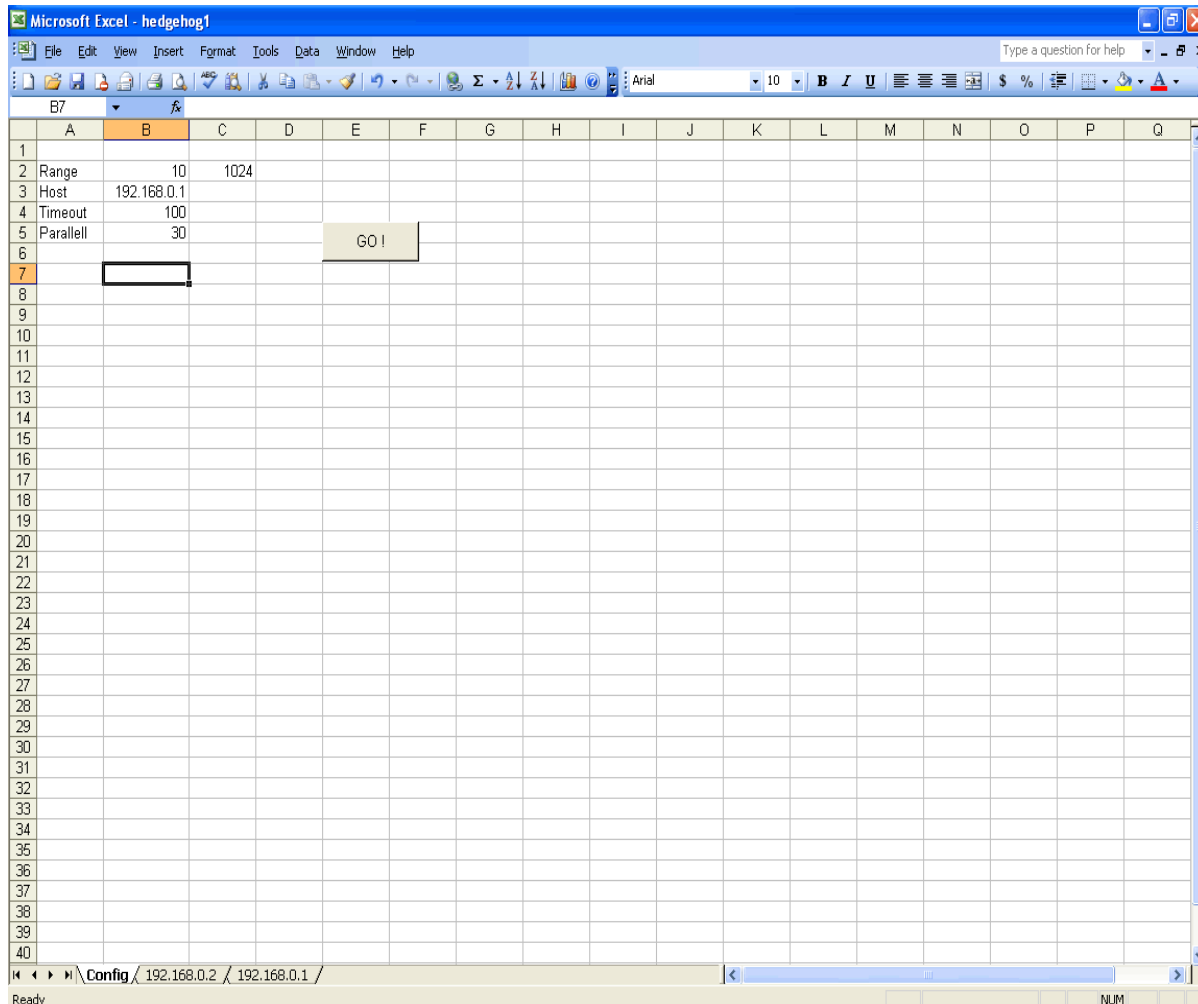
- Net Command (Net Use, Net User, Net View)
- Neststat -na
- FTP and Telnet

### □ Excel Port Scanner

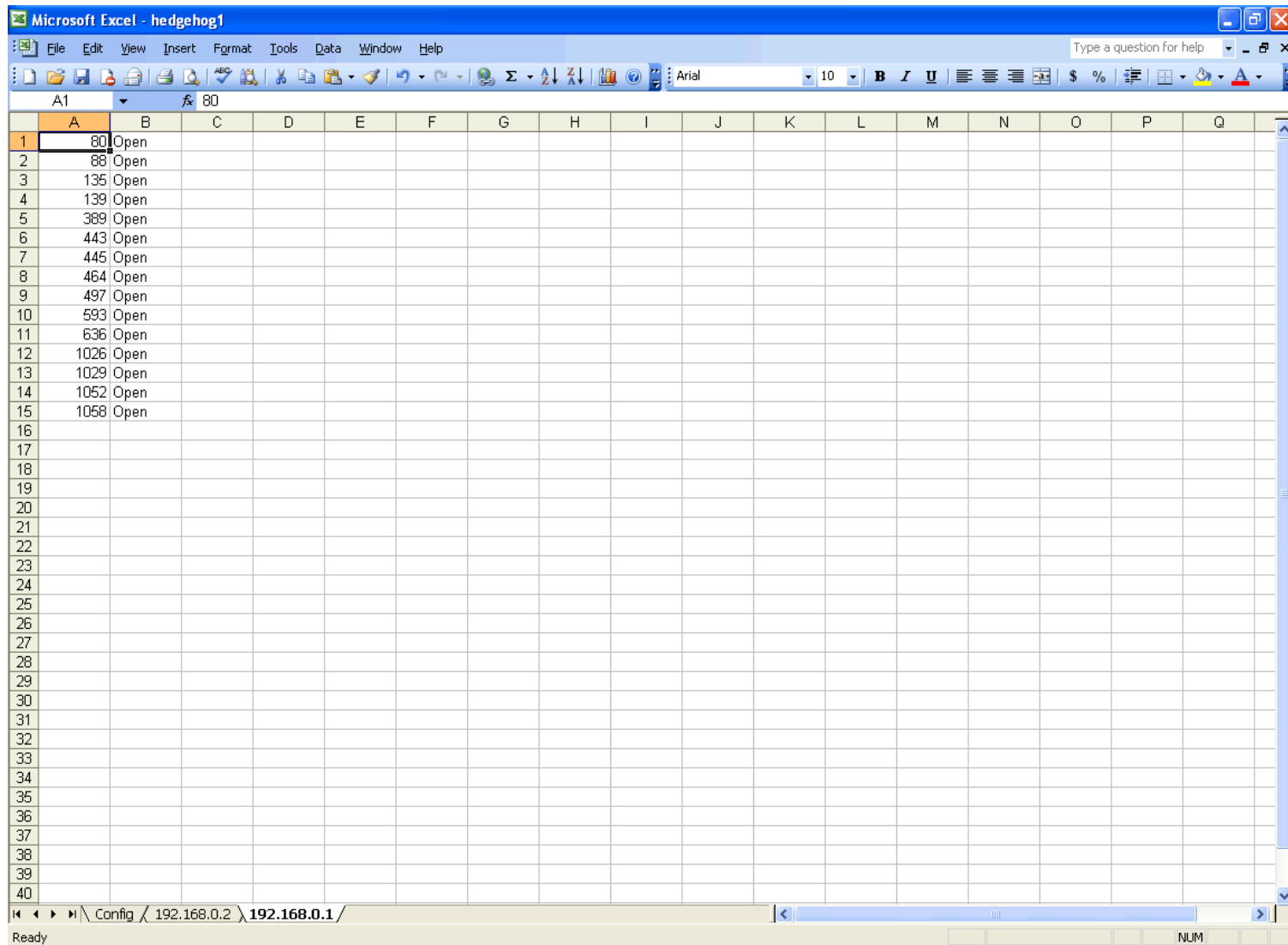
- Named Hedgehog
- Luckily, VBS security set on high will not let it run
- Example of Hedgehog

# Terminal Services and Citrix

- Hedgehog, an MS Excel Port Scanner



# Terminal Services and Citrix



The screenshot shows a Microsoft Excel spreadsheet with the following data in column B:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
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															
16																	
17																	
18																	
19																	
20																	
21																	
22																	
23																	
24																	
25																	
26																	
27																	
28																	
29																	
30																	
31																	
32																	
33																	
34																	
35																	
36																	
37																	
38																	
39																	
40																	

The status bar at the bottom shows the path: Config \ 192.168.0.2 \ 192.168.0.1 /

# 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 cquire
      - 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](http://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](http://www.rstack.org)
  - [www.sensepost.com](http://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 distributions 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](http://www.defcon.org)
- Contact Information:
- Scott McFall – [SMcFall@nsp.state.ne.us](mailto:SMcFall@nsp.state.ne.us)
- Terry Pell – [TPell@nsp.state.ne.us](mailto:TPell@nsp.state.ne.us)
- Jeb Barger – [JBarger@nsp.state.ne.us](mailto:JBarger@nsp.state.ne.us)