Metlstorm

SSH-Jack Redux

...and 'jack0rs for all

November 17th at Kiwicon 2k7

\m/

Intro

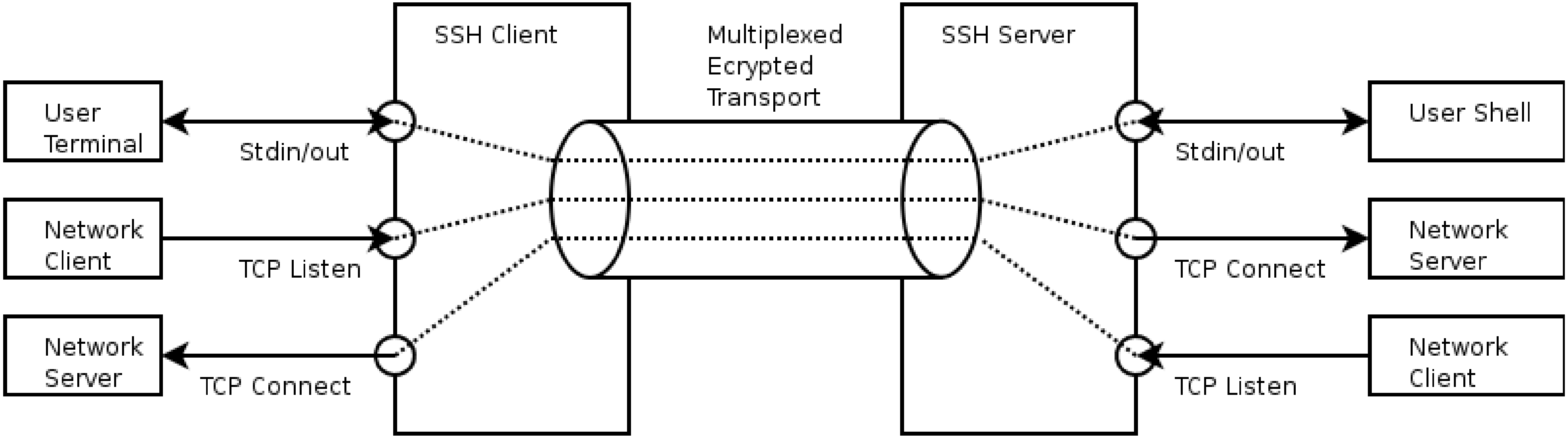
- I'm Metlstorm / Adam
- Previously:
  - an ISP network guy, ISP security guy
  - unix systems coder
  - security consultant at Security-Assessment.com
  - now work for Dave Aitel at Immunity Inc where I hack on CANVAS.
- You might remember me from Ruxcon a coupla times
- “Marketingstorm” for Kiwicon :(

SSH-Jack

- Released “ssh-jack” at BH/Defcon 2k5
- a post-intrusion ssh hijacker
- compromise a linux box, spot an existing ssh connection, gets you a shell out the other end
- transparently

Rich Protocols: SSH

- Goal: Hijack session while in active use without detection
- Virtual Channel infrastructure makes it seamless



Old Jack0r

- Found the channel set up code
  - patched it to connect a new channel to a socket
  - connected the socket to your netcat
  - pwnd
- Worked against OpenSSH v3.x

It's a Feature

- It's not a bug, it's a feature
  - but no interface to actually use it?
- Not any more!
  - OpenSSH v4.x introduces “master mode”
  - Built in SSH-Jackor!
  - Lets you share one tcp ssh session, multiple shells
  - ControlMaster, ControlPath config options
  - Off by default

Master Mode

Demo

...and jack0rs for all

- You don't need SSH-Jack any more!
  - it's built in!
  - I told you it was a feature
  - And the OpenSSH guys agreed
- My work here is done!
  - sweet. To the bar!

Buuuut, Off By Default :(

- Yeah, what are the chances that someone's gonna turn it on?
  - most people don't even know it exists
  - (I didn't until after I started porting ssh-jack to OpenSSH v4.x!)
  - And specially not on a juicy shell-bounce bastion to a global corp ^_^

Moar Demoz

Demo

For your haxxing pleasure...

SSH-Jack II: The Masterjacker

(requires OpenSSH 4.x, python, gdb)

The Masterjacker

- Turns out, way easier than SSH-Jack 1
- Main problem is GCC4 optimization
  - Crazy
  - Pain in the ass to reverse as a non-human
  - Most of the complexity in SSH-Jack II
- Word on the street is that the OpenSSH crüe are gonna escalate this into an anti-debugging arms-race.
  - bring it on :D

SSH-Jack II

- Official release today!
- Get it from http://www.storm.net.nz
- Let me know if it doesn't work for you

```
ssh-jack2$ ./test
SSH-Jack2 Test Suite              [+] sshes/mandriva2008.0-ssh
[+] sshes/centos5-ssh             [+] sshes/mandriva2008.0-ssh
[+] sshes/etch-ssh                [+] sshes/opensuse10.2-ssh
[+] sshes/fedora6-ssh             [+] sshes/opensuse10.3-ssh
[+] sshes/fedora7-ssh             [+] sshes/rhel5-ssh
[+] sshes/fiesty-ssh              [+] sshes/sid-ssh
[+] sshes/gentoo-ssh              [+] sshes/slackware10.2-ssh
[+] sshes/gutsy-ssh               [+] sshes/slackware11.0-ssh
[+] sshes/mandriva2007.1-ssh      [+] sshes/slackware12.0-ssh
```

Q&A

- Wotchya got?

Spam me

- metlstorm@storm.net.nz
- http://www.storm.net.nz

\m/ Kiwicon, motherfuckers \m/