Unix System Administration

Chris Schenk
Lecture 04 – Thursday Jan 24

CSCI 4113, Spring 2008

SSH Brute Force Attacks

- They happen all the time, everywhere
  - Type and amount varies, but they are all similar
- Taken from machine `ihavecandygetinvan`:
  - Jan 22 17:29:40 ihavecandygetinvan kernel Inspecting /boot/System.map-2.6.17-10-server
    - First log message generated
  - Jan 23 00:06:44 ihavecandygetinvan sshd[11267]: Failed password for t1na from 69.16.228.184 port 51333 ssh2
- First attempt to login about ~4.5 hrs later
  - But the brute force didn't start here!

SSH Brute Force Attacks (cont)

- All servers are scanned first for open port 22
  - Port 22 is the standard port for SSH
    - /etc/services lists port names/numbers from the IANA
- A simple telnet test will do
  - `% telnet trunkmonkey 22`
  - Jan 23 22:39:41 localhost sshd[4245]: Did not receive identification string from 127.0.0.1
- This is a good sign that an attack is coming
  - Unfortunately, many times the scanning machine is not the one that will brute-force you!