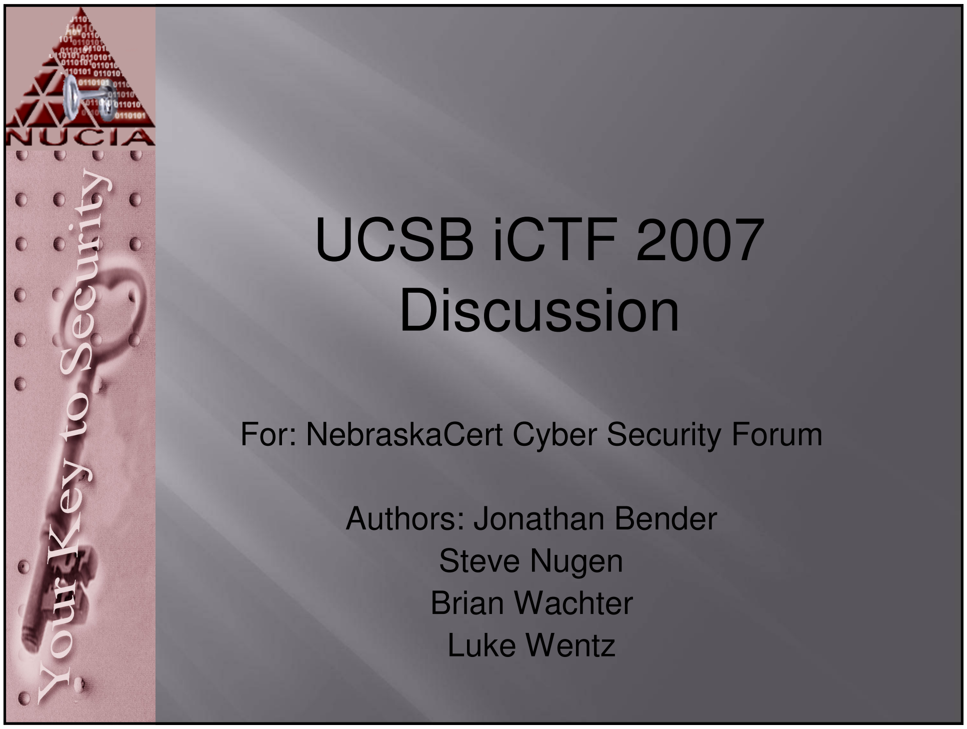
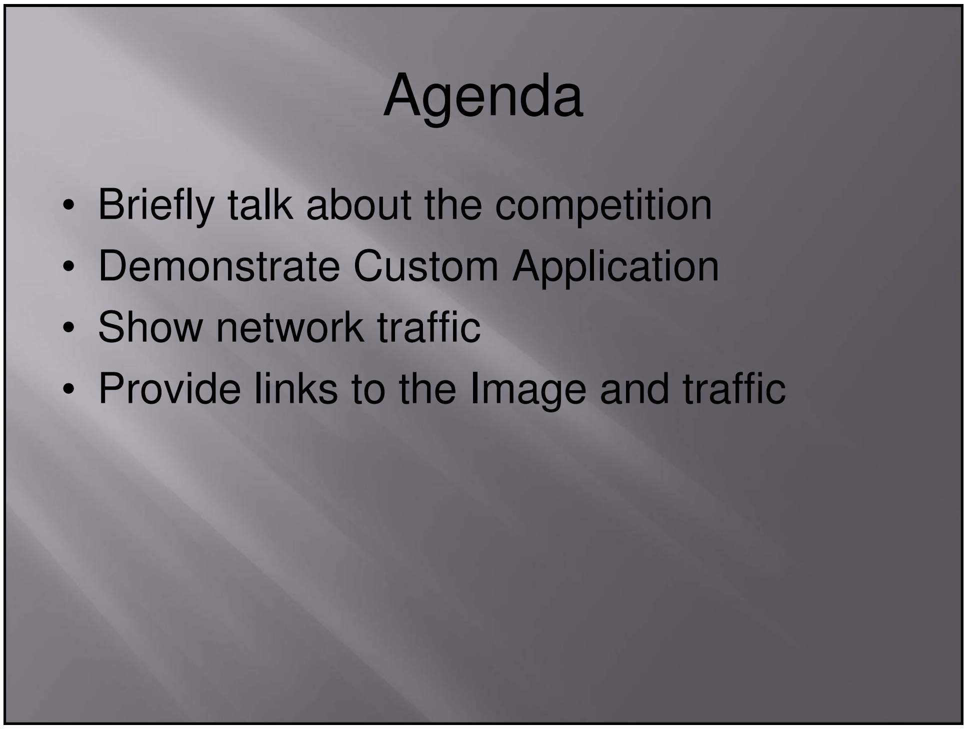


UCSB iCTF 2007 Discussion

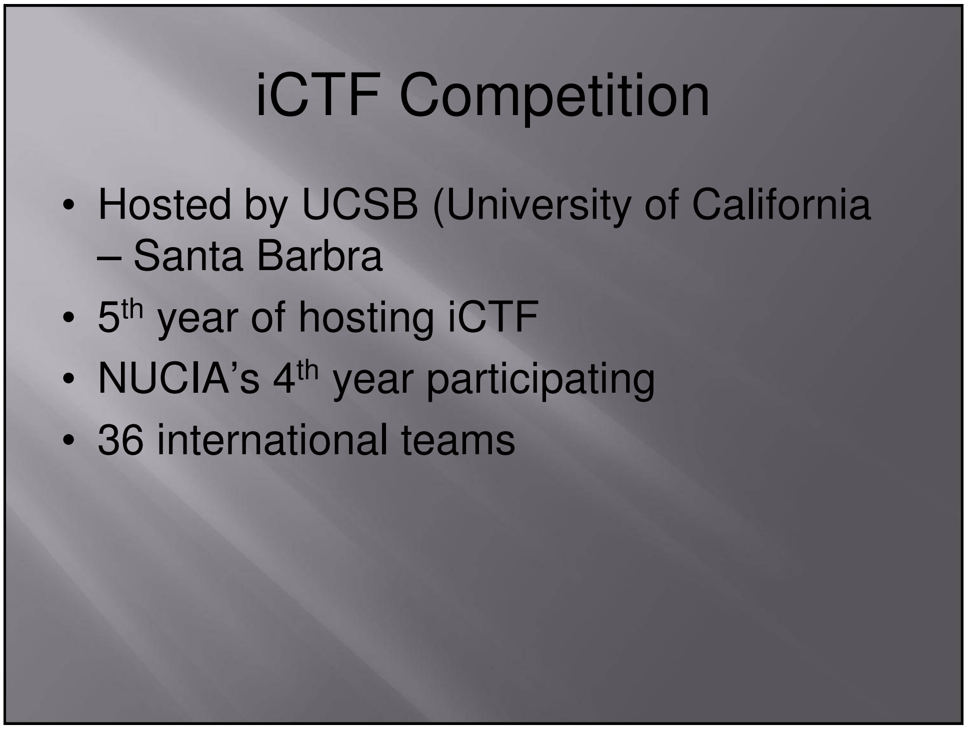
For: NebraskaCert Cyber Security Forum

Authors: Jonathan Bender
Steve Nugen
Brian Wachter
Luke Wentz



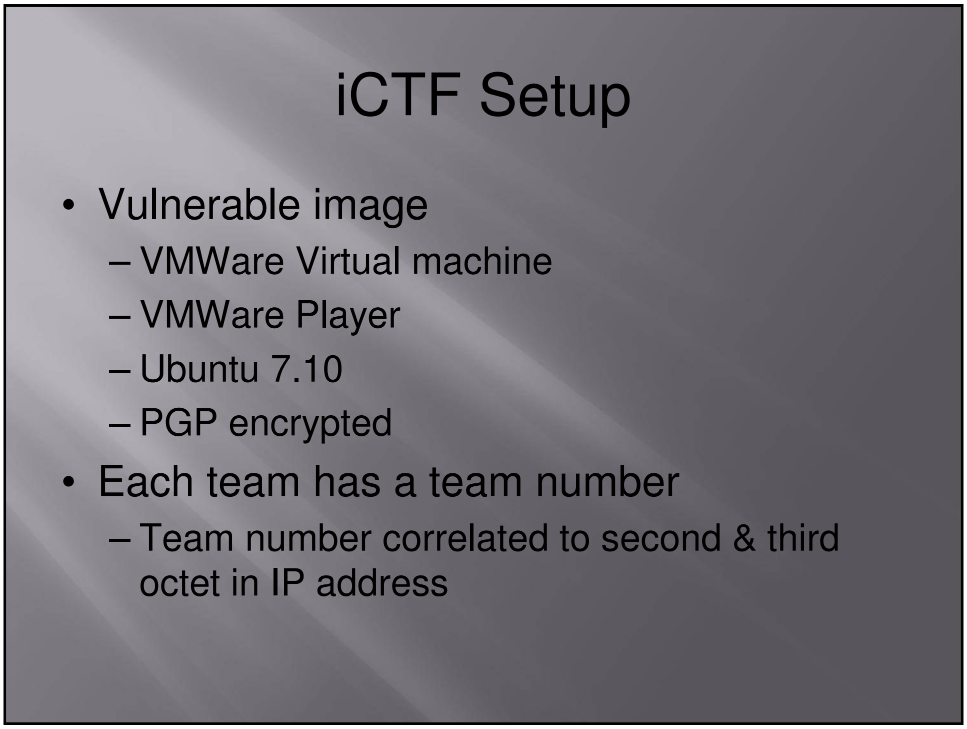
Agenda

- Briefly talk about the competition
- Demonstrate Custom Application
- Show network traffic
- Provide links to the Image and traffic



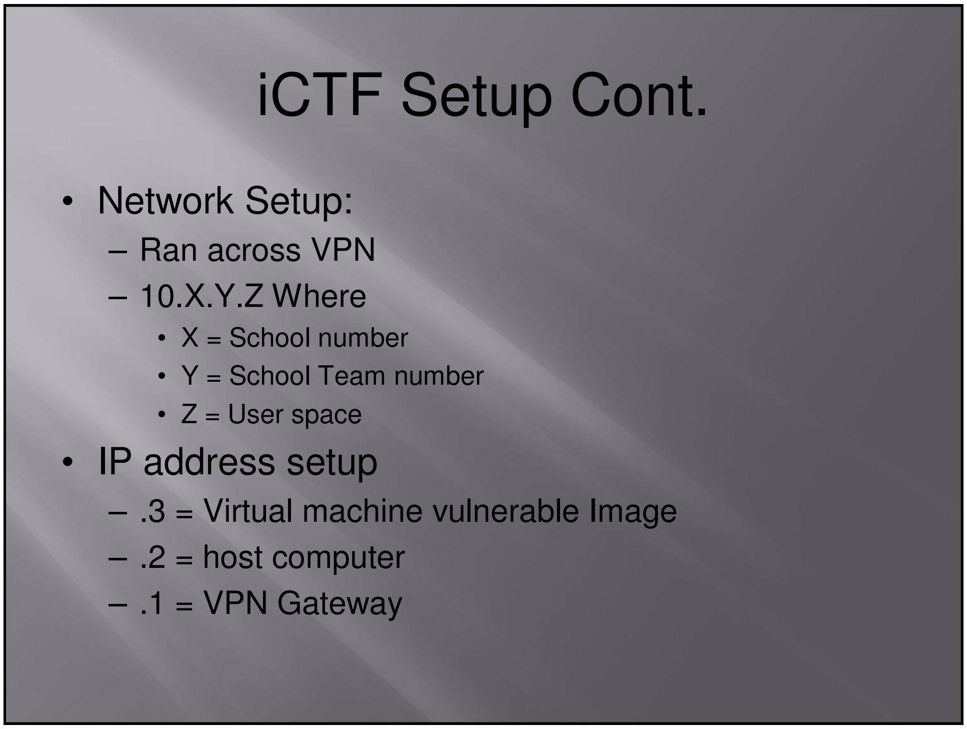
iCTF Competition

- Hosted by UCSB (University of California – Santa Barbra
- 5th year of hosting iCTF
- NUCIA's 4th year participating
- 36 international teams



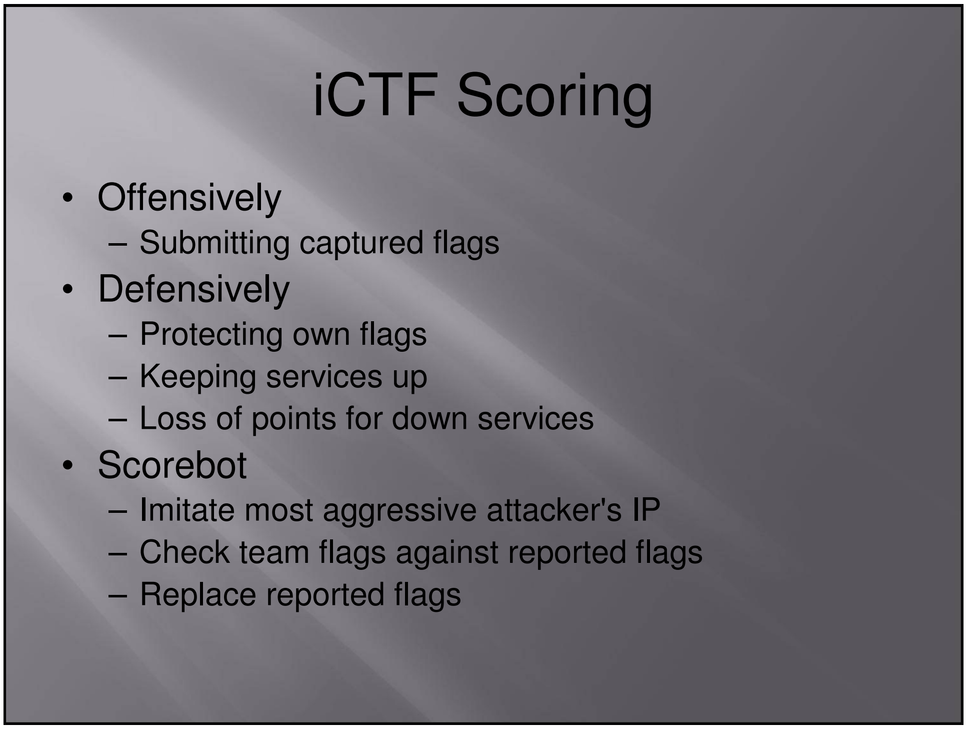
iCTF Setup

- Vulnerable image
  - VMWare Virtual machine
  - VMWare Player
  - Ubuntu 7.10
  - PGP encrypted
- Each team has a team number
  - Team number correlated to second & third octet in IP address



iCTF Setup Cont.

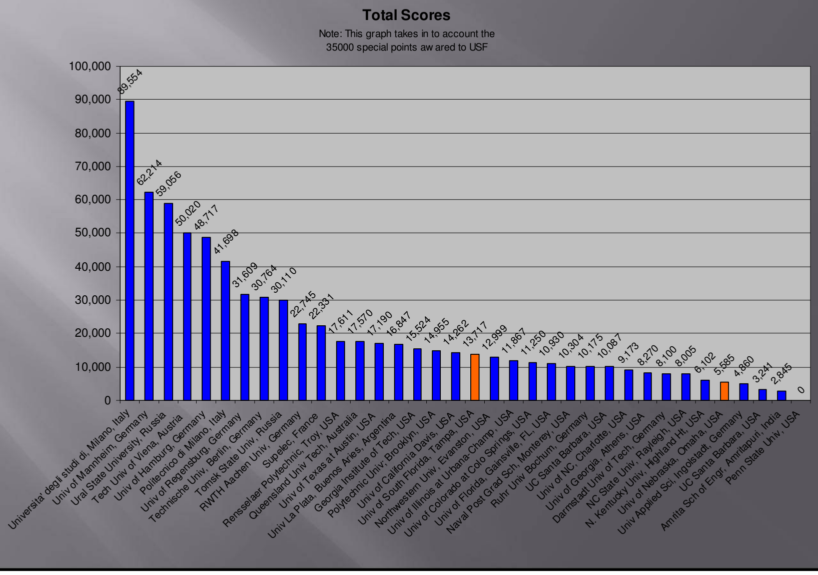
- Network Setup:
  - Ran across VPN
  - 10.X.Y.Z Where
    - X = School number
    - Y = School Team number
    - Z = User space
- IP address setup
  - .3 = Virtual machine vulnerable Image
  - .2 = host computer
  - .1 = VPN Gateway



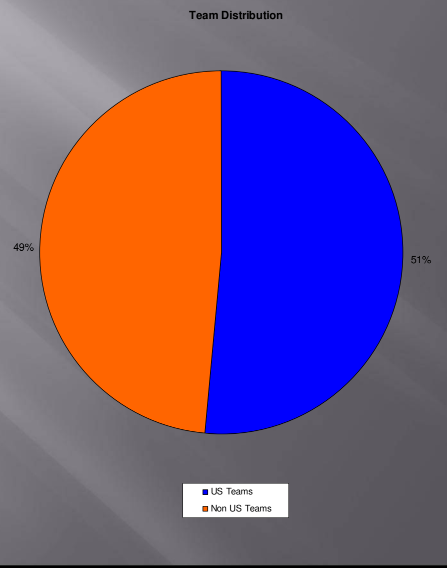
iCTF Scoring

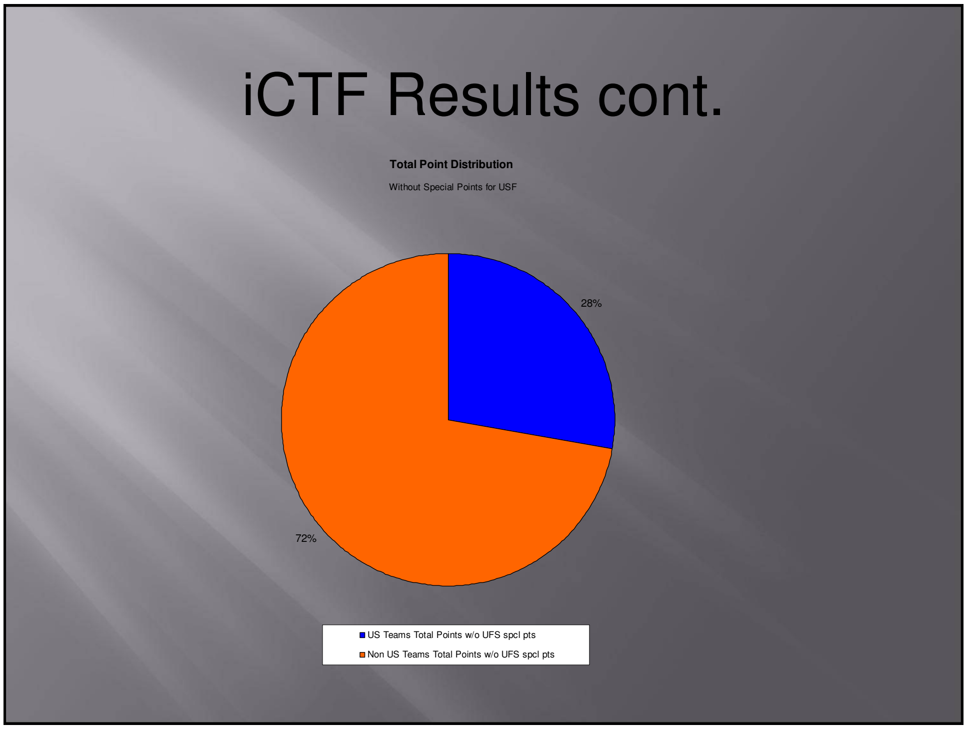
- Offensively
  - Submitting captured flags
- Defensively
  - Protecting own flags
  - Keeping services up
  - Loss of points for down services
- Scorebot
  - Imitate most aggressive attacker's IP
  - Check team flags against reported flags
  - Replace reported flags

iCTF results



iCTF Results cont.

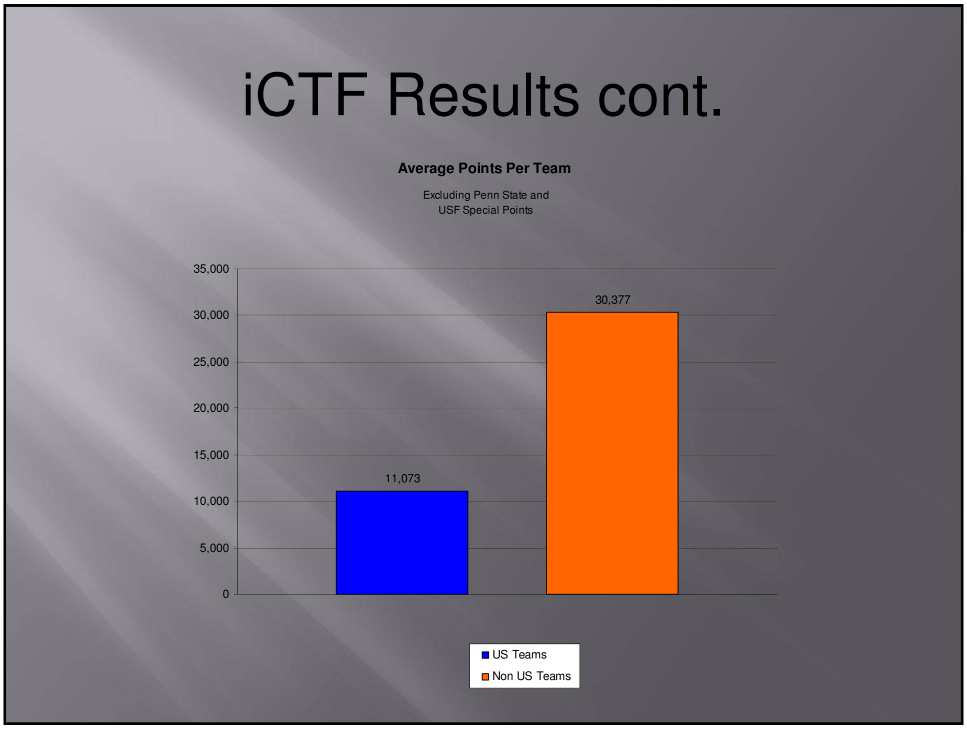




iCTF Results cont.

Total Point Distribution

Without Special Points for USF



iCTF Results cont.

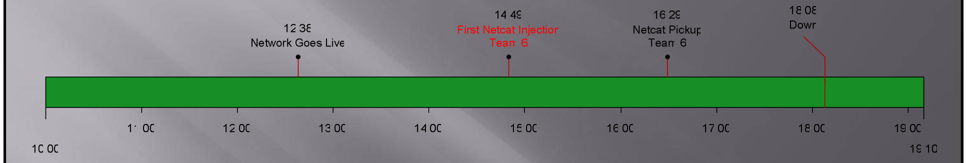
Average Points Per Team

Excluding Penn State and
USF Special Points

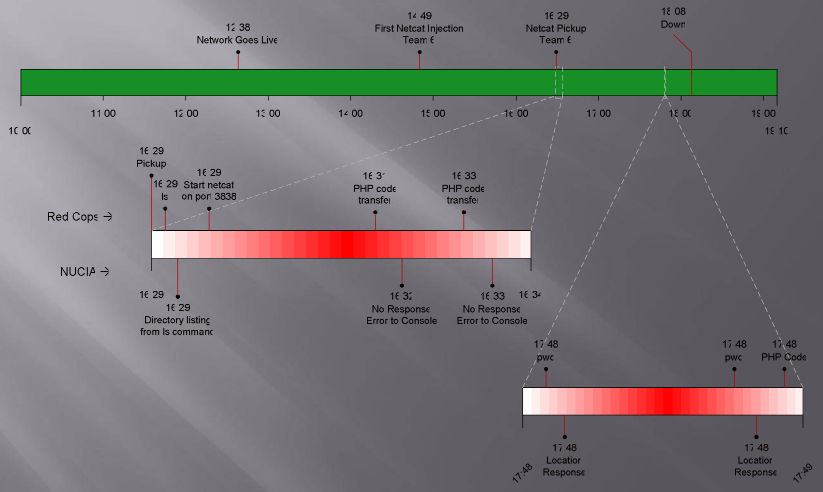
Network Traffic

- Tools used to analyze traffic
  - WireShark (Ethereal)
  - Ngrep

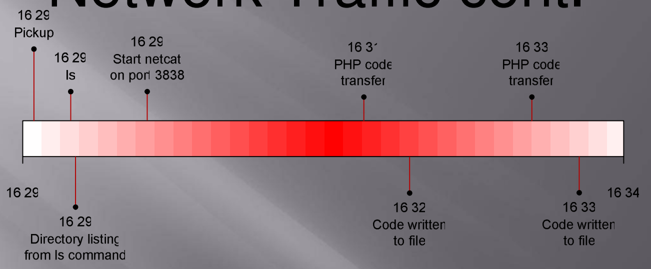
Network Traffic



Network Traffic cont.



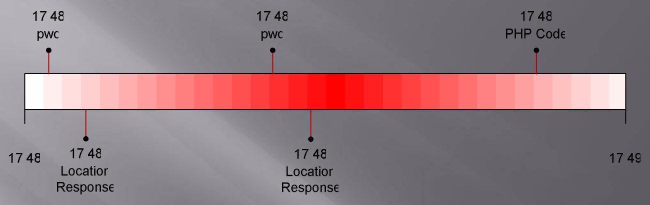
Network Traffic cont.



NUCIA

RED COPS

Network Traffic cont.



17 48
pwc

17 48
pwc

17 48
PHP Code

17 48

17 48
Locatior
Response

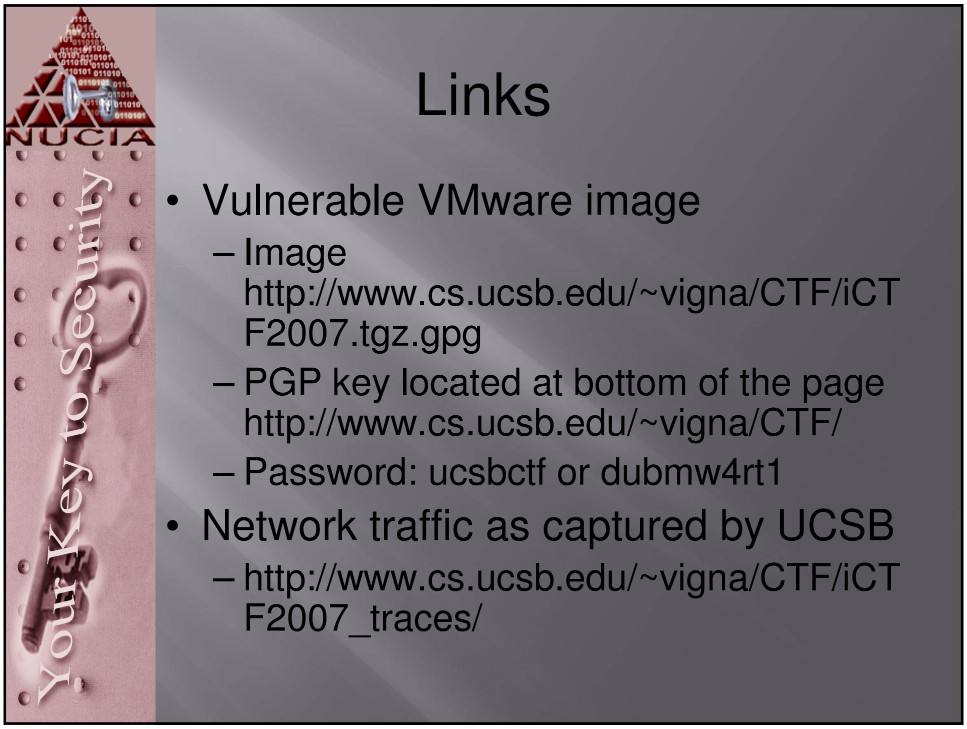
17 48
Locatior
Response

17 49

NUCIA

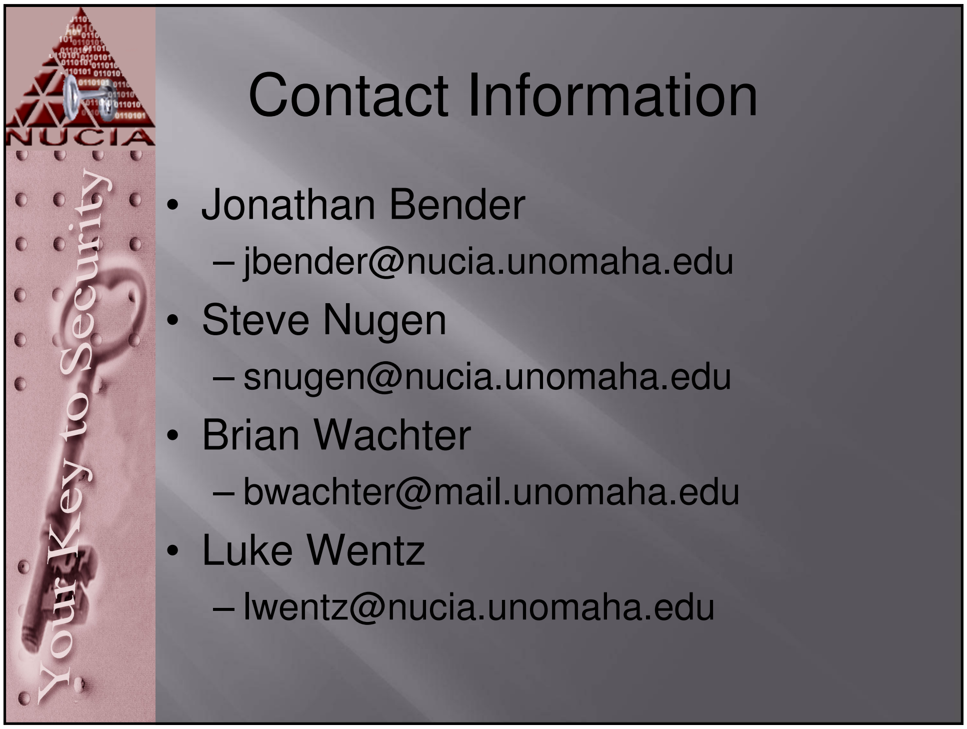
RED COPS

NetCat Demo



Links

- Vulnerable VMware image
  - Image http://www.cs.ucsb.edu/~vigna/CTF/iCTF2007.tgz.gpg
  - PGP key located at bottom of the page http://www.cs.ucsb.edu/~vigna/CTF/
  - Password: ucsbctf or dubmw4rt1
- Network traffic as captured by UCSB
  - http://www.cs.ucsb.edu/~vigna/CTF/iCTF2007_traces/



Contact Information

- Jonathan Bender
  - jbender@nucia.unomaha.edu
- Steve Nugen
  - snugen@nucia.unomaha.edu
- Brian Wachter
  - bwachter@mail.unomaha.edu
- Luke Wentz
  - lwentz@nucia.unomaha.edu