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

Total Scores
Note: This graph takes into account the 35000 special points awarded to USF.

iCTF Results cont.

Team Distribution
iCTF Results cont.

Total Point Distribution
Without Special Points for USF

US Teams Total Points w/o UFS spcl pts
Non US Teams Total Points w/o UFS spcl pts

Average Points Per Team
Excluding Penn State and USF Special Points

US Teams
Non US Teams
Network Traffic

- Tools used to analyze traffic
  - WireShark (Ethereal)
  - Ngrep
Network Traffic cont.

Network Traffic cont.

NUCIA

RED COPS
Network Traffic cont.

NetCat Demo
Links

• Vulnerable VMware image
  – Image
  – 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

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