Organizing Large Scale Hacking Competitions

Nicholas Childers  Giovanni Vigna
Ludovico Cavedon
Manuel Egele  Lorenzo Cavallaro
Bryce Boe  Marco Cova
Outline

• Hacking Competitions Overview
• UCSB’s iCTF
  – History
  – 2003-2007 Competitions
  – 2008 Competition
  – 2009 Competition
  – Lessons Learned
• Final Remarks
HACKING COMPETITIONS
OVERVIEW
Why a hacking competition?

• Time constrained
• Provides hands-on security experience
• Mimics real-world scenarios
• It’s fun
  – Engaging
  – Motivates students to go beyond the call of duty
  – Promotes participation
Types of hacking competitions

• Challenge based
  – DEFCON Quals, Codegate

• Capture the flag
  – DEFCON, iCTF 2003-2007, CIPHER, RuCTF
2003-2007 iCTF example
2003-2007 iCTF example

TEAM A
TEAM B
TEAM C

VPN server

scoring system

UC Santa Barbara
Types of hacking competitions

• Challenge based
  – DEFCON Quals, Codegate

• Capture the flag
  – DEFCON, iCTF 2003-2007, CIPHER, RuCTF

• Attack based
  – Pwn2Own, iCTF 2008-2009

• Defense based
  – Cyber Defense Exercise (CDX)
  – NSF Security Grand Challenge
Hosting a hacking competition

• Design
  – Challenging but not frustrating
  – Cater to various abilities
  – Be objectively scored

• Development
  – Allocate ample time

• Execution
  – Maintain and monitor network
  – Support remote teams
  – Limited timeframe
UCSB’S INTERNATIONAL CAPTURE THE FLAG COMPETITION
iCTF History

- 2003: 14 US university teams
- 2004: Addition of European teams
- 2005: Addition of more international teams
- 2006: 25 teams
- 2007: 36 teams
- 2008: 39 teams
- 2009: 56 teams
2003-2007 Competitions

- Traditional CTF format with side challenges
- Limited to universities
- Addition of remote teams
- Introduced traffic blending technique

Limitations

- Favored experienced teams
- No longer unique
2008 iCTF

• Attack-based with side challenges
• Mimics a “save the world” scenario
• Goal: Defuse bomb by breaking into the softerror.com network
2008 Simulated Network

Softerror.com

Internet

Web

Financial

Password cracking

Directory traversal command injection

Binary reversing & patching

Format string vulnerability

Development

Bomb

Bryce Boe @ UCSB -- DIMVA 2010
2008 Physical Network

Teams

openVZ Web

VPN server

iptables firewall

openVZ Financial

openVZ Development

openVZ Bomb

Bryce Boe @ UCSB -- DIMVA 2010
2008 Dataset

- Snort Alerts (by team)
  - Mean: 8482
  - Max: 43254

- Pcap files
  - 5.5 GB data (3 GB compressed)
  - 34 million packets

- Useful for attack correlation research
2009 iCTF

- Also attack based with side challenges
- Mimics a “botnet creation” scenario
- Goal: Deliver *profitable* drive-by-downloads to simulated web users
2009 Game Play

Team Website

Team Websites
2009 Game Play

PayPerNews → periodic indexing → Team Website

optional publishing $$$ → Goollable

UC Santa Barbara
2009 Game Play

PayPerNews

Numerous Simulated Users

Browsers

User

Goollable

periodic indexing

optional publishing $$$

Team Website

UC Santa Barbara

Bryce Boe @ UCSB -- DIMVA 2010
2009 Game Play

User

Step 1: Robabank

Step 2: PayPerNews

Step 3: Goellaneous result

Step 4: Team Website

Optional publishing $$$

Periodic indexing

UC Santa Barbara
2009 Game Play

User

step 1

transfer

Robabank

step 2

PayPerNews

optional publishing $$$

UC Santa Barbara

Goollable

periodic indexing

step 3

Team Website

Mothership

step 4

"C&C"
Lessons Learned

• KISS principle
• Budget sufficient time and resources
• Stress test competition components
• Scoring
  – Fully automated
  – Rollback and repeatable
• Attack only competitions level the playing field
Final Remarks

• Hacking Competitions
  – Fun and Challenging
  – Engaging

• Datasets and source from UCSB’s iCTF available at http://ictf.cs.ucsb.edu
Questions?