Session 6
Mid-term CTF

Security Summer School
July 10th 2014

ACS/Ixia/Hexcellents

Capture The Flag

- Information Security contests
- Test your hacking skills legally
- Or learn new stuff
- Gamification

Knowledge required

- Reverse engineering
- Binary analysis
- Cryptography
- Digital forensics
- Web application exploitation
- Misc (math, algorithms, speed coding, esoteric languages, physical layer exploitation)

Knowledge required

- Reverse engineering
- Binary analysis
- Cryptography
- Digital forensics
- Web application exploitation
- Misc (math, algorithms, speed coding, esoteric languages, physical layer exploitation)

It really boils down to understanding the full stack of technologies that power Information Technology.

Team play

- Hard for one single person to nail all categories
- Having a team of people with different backgrounds helps a lot
- Bounce ideas off team mates
- Tasks require time anyway so doing them in parallel is key

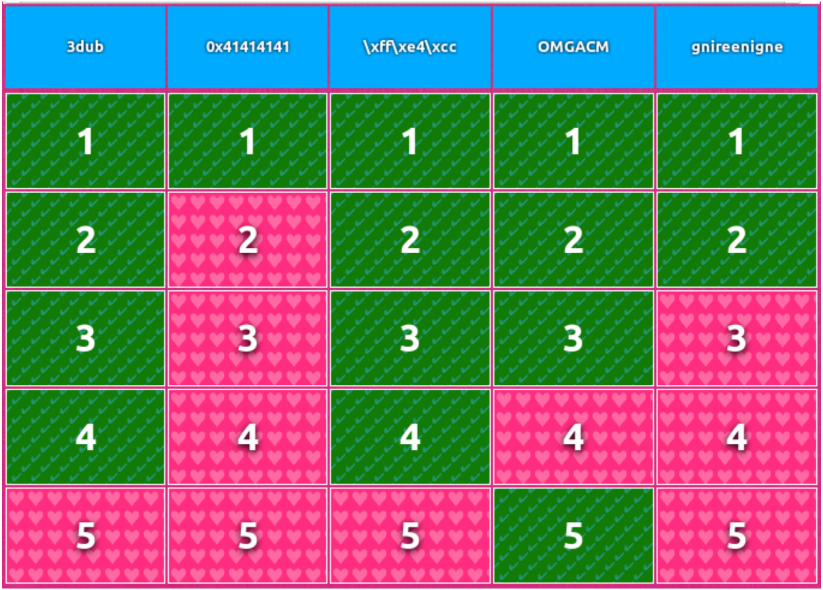
The ‘FLAG’

- The whole idea is to find weaknesses in a system
- Having found security holes you get access to restricted areas
- To prove you obtained that access the organizers place `flags`
- Submitting flags on the scoreboard validates your work

Scoring

- Problems of varying difficulty
- Usually awarded with points (100p, 200p, 500p, etc)
- Sometimes the first three teams to solve a task get `breakthrough` points (3p, 2p, 1p)

Jeopardy style CTF: Defcon CTF 2013



3dub	0x41414141	\xff\xe4\xcc	OMGACM	gnireenigne
1 ✓	1 ✓	1 ✓	1 ✓	1 ✓
2 ✓	2 ♥	2 ✓	2 ✓	2 ✓
3 ✓	3 ♥	3 ✓	3 ✓	3 ♥
4 ✓	4 ♥	4 ✓	4 ♥	4 ♥
5 ♥	5 ♥	5 ♥	5 ✓	5 ♥

Who organizes CTFs?

- Information security conferences
  - DEF CON (USA)
  - Hack In The Box (NL)
  - Codegate (KR)
  - Positive Hack Days (RU)
  - Ghost in the Shellcode
  - much much more
- Universities
  - CSAW CTF (New York University)
  - iCTF (University of California, Santa Barbara)
  - Volga CTF (RU)
  - rwth CTF (RWTH Aachen University)
  - Sharif University CTF (Iran)
  - etc
- Various groups or security companies
  - Plaid CTF
  - OWASP AppSec
  - Most security training seminars hold CTFs to illustrate skills acquired

How to practice?

- Find a team
- Find a CTF
- PLAY!

How to practice?

- Find a team
- Find a CTF
- PLAY!
- Don't get discouraged, the learning curve is very steep

How to practice?

- Find a team
- Find a CTF
- PLAY!
- Don't get discouraged, the learning curve is very steep
- Alternatively, practice by:
    - Reading writeups to previous CTF challenges
    - Playing wargames (permanently online challenges)

Resources

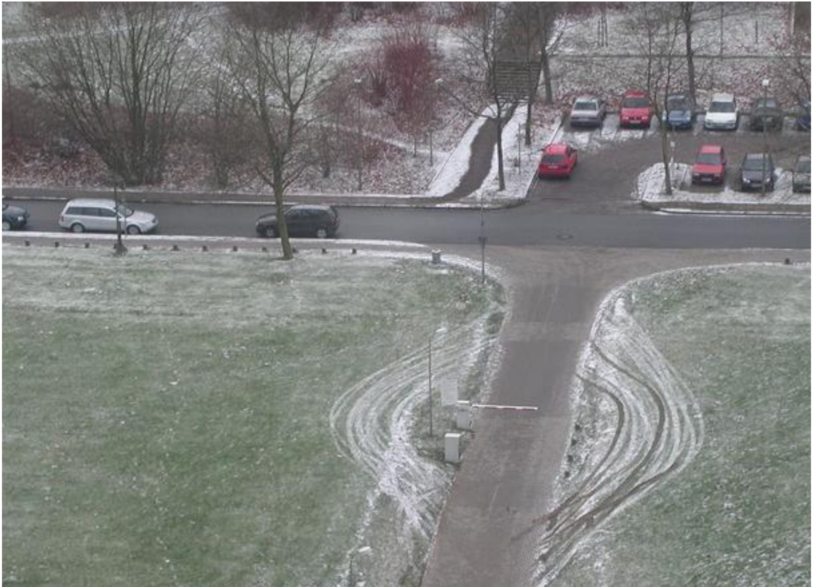
1. CTF schedule aggregation: `ctftime.org`
2. Some of our writeups: `security.cs.pub.ro/hexcellents`
3. Wargames:
   - `io.smashthestack.org`
   - `overthewire.org/wargames`
   - `www.exploit-exercises.com`

Stop! It's CTF time

Let's play

The usual suspects

Security bypass



The usual suspects

Out of the box thinking

The usual suspects

Buffer overflows