Introduction Project

Neline van Ginkel
Neline.vanGinkel@cs.kuleuven.be
Development of Secure Software

Outline

- Why?
- What?
- How? – demo
- Practicalities

Why?

- “In theory, theory and practice are the same. In practice, they are not.” – Albert Einstein
- Get experience
- Understand how low-level attacks work
- Think like a hacker

Outline

- Why?
- What?
- How? – demo
- Practicalities

What?

- Casper wargame
- Binary exploitation
  - Stack-based overflow
  - Heap-based overflow
  - Return to libc
  - Data-only vulnerabilities
- 12 base-levels
  - 4 introduction levels
  - 8 (4x2) actual levels
  - For first 6 actual levels: 3 advanced challenges

Outline

- Why?
- What?
- How? – demo
- Practicalities

How?

- Virtual machine with all levels
- Reachable via ssh
- Credentials for ssh on Toledo (at 15:00)

How?

- Levels are stored in /casper/
- Binaries have corresponding source code
- Passwords are stored in /etc/casper_pass/
- More information (and hints) about levels on the website

How?

- Demo time!
  - ssh -p 8080 casper0@casper.haxx.be
    hv0Epdze23IybTQzIhb9X2xMgLp2IbAf

Outline

- Why?
- What?
- How? – demo
- Practicalities

Practicalities

- Read the rules!
- Assignment on Toledo for all details
- Exploit one level of each category
  - For the first three categories: exploit one advanced level per category
- Write a report (example on website)

Practicalities

- Shellcode should execute **/bin/xh**
  - Normal shellcode executes /bin/sh, change it!
- /bin/xh displays a banner with username & password
- /bin/xh is used for automatic exploit verification!

Practicalities

- Send in a tarball (.tar.gz) and report
- Requirements tarball:
  - Makefile in toplevel directory
  - One target per exploit (exploit4, exploit6, ...)
  - No binary files!
  - Example available at website: exploits.tar.gz
- Verify your tarball with **casper_verify_tarball.py**
  - Only send in after verifying!

Practicalities

- Send in a tarball (.tar.gz) and report (.pdf)
- Requirements report:
  - Summary of solved levels
  - Explain what the vulnerability is
  - Explain how you exploited it
  - Explain how to fix the program
- Details in assignment

Practicalities

- You can work in /tmp (non-browsable)
- Back up your work locally!
- Detailed system information on the website

Practicalities

- Lab session in a few weeks (23/24 November)
  - Work on the assignment
  - Ask questions

- Prerequisites for the assignment
  - Read the background paper about low-level attacks (you can skip section 3)
  - Make sure you have an ssh client
  - Learn about gdb

Practicalities

- Questions
  - Ask on lab session
  - Ask on Toledo forum

- Emergencies (e.g. server down/unreachable)
  - Send me an email
    Neline.vanGinkel@cs.kuleuven.be

Practicalities

- Good luck & have fun!