= Security Summer School =

From „Voodoo“ to „You Do“ via hex and fun.

Proudly brought to you by ACS, Ixia and Hexcellents.

Period

23rd of June - 10th of August 2014

Links

* Wiki * Facebook page * Google Plus page * E-mail contact address

Summary

The first edition of a new Security Summer School focused on Practical Software Exploitation will take

place between June 23rd and August 10th 2014, at the Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest. Students will go through an in-depth tour of what it means to discover, successfully exploit and patch a software vulnerability and develop the necessary skills and insights needed to embark on such an endeavor.

Activities will take place during two intensive training sessions per week as well as two Capture the Flag (CTF) contests that will be held mid-term and at the end of the summer school. The final CTF contest will be the highlight of the summer school and students will be able to showcase the skills they have learned and be awarded prizes offered by Ixia.

Application

We welcome students to apply via Stagii pe Bune. Choose „Security Summer School“ under the „Summer Schools“ heading, for the company „Facultatea de Automatica si Calculatoare, UPB“.

Apart from filling out your CV, we want to see your h4x0r sk111z by solving a set of three challenges. Please download the challenge tasks, go through the README and then submit your solution on this Google form; you may edit your submission if you forget something during the first try. The deadline for submitting your answers is Sunday, May 25th.

After May 25th we will organize a set of interviews to decide who will take place in the Security Summer School.

Requirements

We expect good programming skills and a fair knowledge of the C programming language. Python and shell scripting skills are welcome.

More than anything we expect a proactive attitude, a love for challenges and „tinkering“ and an interest in security and hacking.

Location & Schedule

The Security Summer School will take place in Faculty of Automatic Control and Computers, University POLITEHNICA of Bucharest, room EG106 (Ixia lab), first floor, EG wing.

Activities will take place twice a week:

- Monday, 4pm-8pm
- Thursday, 9am-1pm

Each session will be highly practical: a presentation of a set of basic concepts on slides followed by hands-on activities (tutorials and tasks).

The 9th-10th of August week-end is reserved for the final CTF contest and awards ceremony.

Syllabus

1. Introduction into the World of Security
    1. 23rd of June: OS (pmap, strace, ltrace, file descriptors, lsof, ldd), Linux dinamic analysis
    2. 26th of June: assembly intro: registers, mnemonics, the stack, gdb (step instruction/read-only)
2. Binary Formats
    1. 30th of June: writing assembly, executable code analysis (IDA)
    2. 3rd of July: from ELF to a process, PLT, PIC → gdb / IDA
3. Vulnerability Assessment
    1. 7th of July: overwrite data in GDB, overflow of all kinds: function pointers, vtable, local variables, format string, use after free
    2. 10th of July: CTF Demo (4 challenge tasks)
4. Vulnerability Discovery
    1. 14th of July: stateless fuzzing (on files), fuzzer + gdb
    2. 17th of July: stateful fuzzing (on protocol)
5. Weaponizing the vulnerability
    1. 21st of July: shellcode + stack, null character, call trampoline
    2. 24th of July: DEP, ASLR
6. Weaponizing the vulnerability II
    1. 28th of July: information leak, canary value, format strings
    2. 31st of July: ROP, remote + socket reuse
7. Preventing vulnerabilities in your own code + Windows
    1. 4th of August: secure programming techniques (sanitizing, system())
    2. 7th of August: Windows: shell code exploit on windows (Immunity, WinDbg)

Team

* Adrian Șendroiu * Dan Gioga * Dragoș Comăneci * Radu Caragea * Răzvan Crainea * Răzvan Deaconescu * Silviu Popescu * Tudor Azoiței

Supporting members

* Irina Preșa * Lucian Cojocar * Vlad Dumitrescu

In case of any inquiries please send us an e-mail.