
Advanced Internet Security (also known as InetSec 2 ;))

Clemens Kolbitsch

ck@iseclab.org

Christian Platzer

cplatzer@iseclab.org

Paolo Milani

pmilani@iseclab.org

Thorsten Holz

tho@iseclab.org

Administrative Issues

- Mode
 - lectures
 - regular programming assignments
 - written final (end of January)
- When and Where
 - Monday 3:00 pm. – 4:30 pm.
 - Radinger Hoersaal, Getreidemarkt 2
- Slides and News (please visit regularly)
 - <http://www.iseclab.org/InetSec2/>
- Mailing List
 - TUWIS

Lecture

Topics

- Unix Security
- Windows Security
- Buffer Overflows (Stack, Heap, Format String)
- Web Security (XSRF, Session Stealing)
- Reverse Engineering and Binary Analysis
- Fuzzing
- Viruses and Worms
- General Topics of Interest (Program Shepherding, Trusted Computing, Underground Economy)

InetSec 1 and InetSec 2

	InetSec 1	InetSec 2
• Unix Security	x	✓
• Windows Security	x	✓
• Buffer Overflows	✓	✓
• Internet Application Security	✓	x
• Cryptography	✓	x
• Fuzzing	x	✓
• Reverse Engineering	x	✓
• Viruses and Worms	x	✓
• Testing	✓	x

Who should do InetSec 2

- People who would like become “security gurus”.
 - we usually take part in a Capture the Flag hacking contest against other universities. This year, we need to see...
 - lots of fun: 3rd place last year, 1st place the year before that
- People who are hard-core technical
 - C and Linux should not be a problem for you
- You should be interested in solving technical problems
 - Even if it might cost you some time
- People who have time
 - you get the chance to solve security challenges such as writing a worm, reverse engineering applications, writing a Trojan

Who should do InetSec 2

Hacker im Universitäts - Computer - Netzwerk...

es keine größeren Attacken, doch will man nicht „zu großspurig“ darüber reden.

„Wir glauben, dass wir unter Attacke stehen, die von außen kommt und nicht nur Flux und Tollerei ist“, berichtet Hermann Maier, ZID-Direktor der Uni Klagenfurt. Man versuche durch E-Mail-Fallen Passwörter zu stehlen. „Technologisch ist das überhaupt keine Herausforderung“, erklärt Fabian, doch Cracker denken nicht in kreativen Sphären, sie sind auf den eigenen Vorteil bedacht.

Um präventiv dagegen vorzugehen, zeigt die Vorlesung „Internet-Security 2“ der TU Wien, wie Sicherheitslücken erkannt und vermieden werden. Eine Kaderschmiede für zukünftige Cracker? „Wenn man nicht weiß, wie man ins System einbricht, dann kann man sich auch nicht verteidigen“, unterstreicht Uni-Assistent Christian Platzer.

Salonfähige Hacker

Dieselbe Philosophie verfolgt die französische „Hackacademy“, die in Paris, Belgien, der Schweiz, Algerien

Your Roadmap to Enlightenment

Challenges Solved	Rating
0	Script Kiddie Nobody+ Nobody++ Nobody Junior Nobody Senior Nobody Professional InetSec1
1	
2	
3	
4	
5	
6	Apprentice Stackmaster Apprentice+ Apprentice++ Apprentice Junior Apprentice Senior Apprentice Professional Stackmaster expl0it Warlock Guru / Master Guru (CtF required) InetSec2
7	
8	
9	
10	
11	
12	
13	
14	

Lab

- Assignments
 - 8 challenges, no immediate credit assigned
 - **you are required to correctly solve 6 assignments to take the exam!**
 - lab starts with the lectures on the 12th of October (i.e., Challenge 1)
 - registration between 12th and 26th of October
- Environment
 - assignments should be mostly solved at home
 - small test network, which is remotely accessible via ssh (Linux)
 - accounts can be obtained next week
 - check home page for details
- Turning in
 - hard deadlines (with sufficient time)
 - automatic checking with immediate feedback

Lab

Assignments (tentative)

- Unix Vulnerabilities (Input Validation)
- Stack Buffer Overflow
- Advanced Buffer Overflow (e.g., Heap, Format String Vulnerability)
- Windows Security
- Forensics
- Fuzzing
- Program Analysis and Patching (“Cracking”)
- Malware (Worm, Virus, something simple)

Lab

- Capture the Flag (CtF) Exercise
 - security exercise involving universities around the world
 - TU can send a team if there is interest
 - we need to see about this year
 - half of the lab is in France/California this year

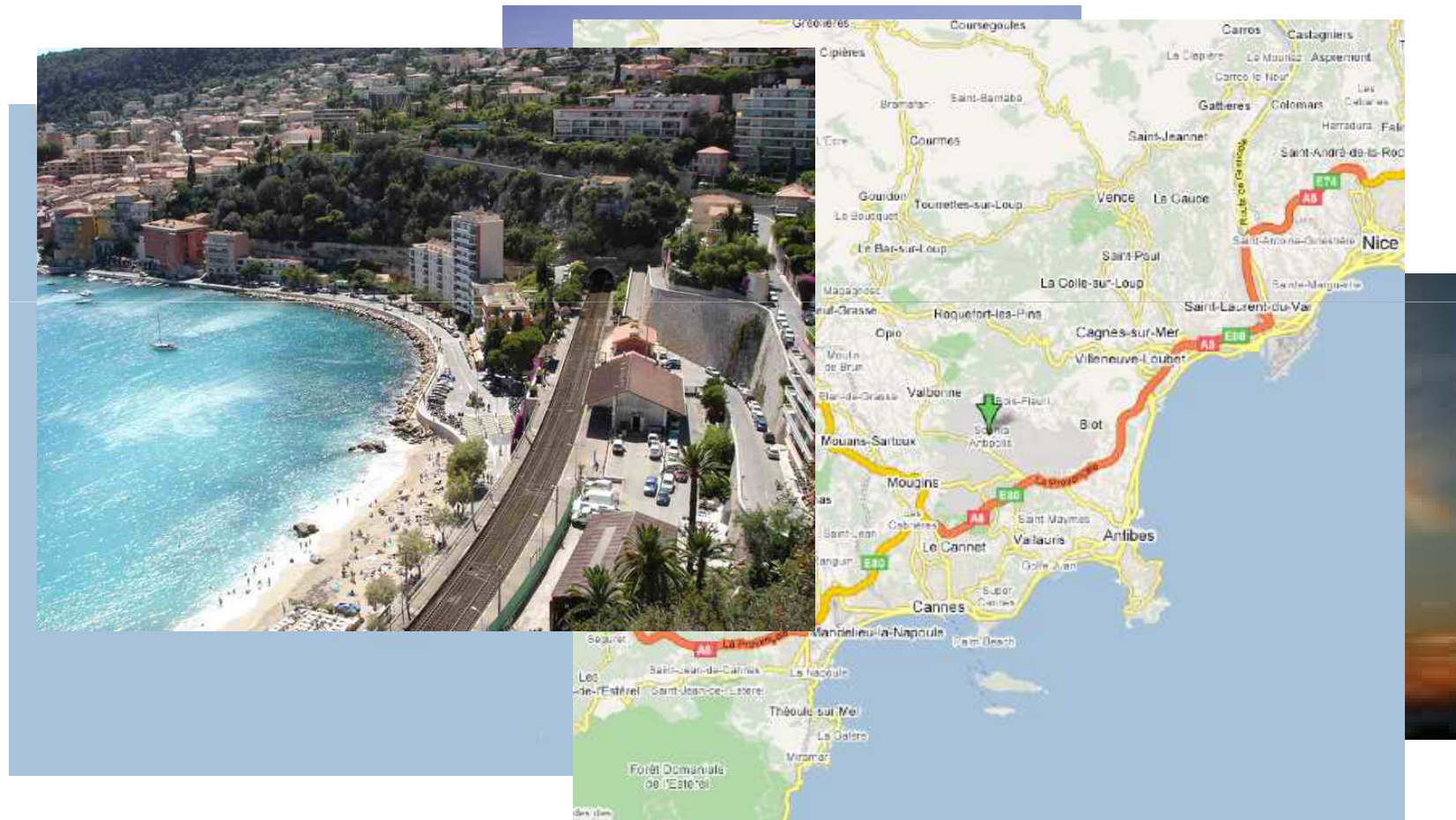
 - teams have to hack into other machines while simultaneously defending their own systems

 - probably rather involved and time consuming
 - but very rewarding and interesting
 - more information under <http://ictf.cs.ucsb.edu/>

Internships

- Secure Systems Lab has become international
 - possibility for very good students to do internship projects abroad
 - take from three months to half a year
 - participate in our research projects
 - if you are good (technically AND academically) then we like you 😊

Locations besides Vienna



Time for tradition and the infamous
DARPA video

If you think the video is realistic,
please leave the class ;-)
