

Internet Security 2

(aka Advanced InetSec)

Christian Platzer

cplatzer@seclab.tuwien.ac.at

Gilbert Wondracek

gilbert@seclab.tuwien.ac.at

Markus Kammerstetter

mk@seclab.tuwien.ac.at

Edgar Weippl

edgar.weippl@tuwien.ac.at

Administrative Issues

*Int. Secure Systems Lab
Vienna University of Technology*

- Mode
 - weekly lectures, held in English
 - regular programming assignments
 - written final exam (end of January)
- When and Where
 - Thursday 11:15 am. – 13:15 pm. (s.t.)
 - FH HS3
 - Lectures (are planned to) end before Christmas
- Slides and News (please visit regularly)
 - <http://www.seclab.tuwien.ac.at/inetsec2/>
 - TISS

Lecture - Topics

*Int. Secure Systems Lab
Vienna University of Technology*

- Unix security
- Windows security
- Race Conditions
- Buffer overflows (Stack, Heap, Format String)
- Web security (XSRF, session stealing)
- Reverse engineering and binary analysis
- Viruses and worms
- Guest lecture topics: DRM / Adv. Web Security

Who should do InetSec 2

*Int. Secure Systems Lab
Vienna University of Technology*

- People who would like become “security gurus”
 - we usually take part in a Capture the Flag hacking contest against other universities. → <http://ictf.cs.ucsb.edu/>
 - lots of fun: many top 5 positions over the last years, won some time ago
- People who are technically oriented
 - you should be somewhat familiar with C and Linux
 - Java-purists will have some catching up to do ;-)
- 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 or trojan
 - reverse engineering applications

Who should do InetSec 2

Int. Secure Systems Lab
Vienna University of Technology

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 Kadenschmiede 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 „Hack-academy“, die in Paris, Belgien, der Schweiz, Algerien

Your Roadmap to Enlightenment

*Int. Secure Systems Lab
Vienna University of Technology*

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

Lab

*Int. Secure Systems Lab
Vienna University of Technology*

- Assignments
 - 6 challenges, mostly following the lecture content
 - lab starts with the lectures on the October 13th (i.e., challenge 1)
 - registration open until October 19th (via lecture homepage)
 - you cannot turn in challenge solutions later
 - **enrolling via TISS is not enough!**
- Environment
 - assignments should be mostly solved at home
 - small test network, which is remotely accessible via ssh (Linux)
 - accounts are created automatically with the registration
 - check homepage for details

Lab

Int. Secure Systems Lab
Vienna University of Technology

- Challenge topic (*tentative*)
 - Unix vulnerabilities
 - Remote stack buffer overflow
 - Windows Security
 - Program analysis and Patching (“Cracking”)
 - Advanced stack buffer overflow
 - Malware (Worm, Virus)

Grading

Int. Secure Systems Lab
Vienna University of Technology

- How you get your grade
 - written exam + challenges determine your grade
 - 5 regular challenges, 20 points each
 - 1 optional challenge, 10 points
 - written exam is worth up to 50 points
 - you have to have >25 points on the exam and >50 points on the challenges
 - => **required to correctly solve 3 assignments to take the exam**
 - solving all challenges helps as exam preparation
- Turning in challenge solutions
 - through the lab environment (remember `/usr/local/bin/submit;-)`)
 - hard deadlines (with sufficient time)
 - automatic checking with immediate feedback
 - **no points for partially solved challenges!**

What's more

*Int. Secure Systems Lab
Vienna University of Technology*

Capture the Flag (CTF) Exercise

- security exercise involving universities around the world
- we can send a team if there are enough people interested
- teams have to hack into other machines while simultaneously defending their own systems

- probably rather time consuming
- but very rewarding and interesting (and there will be free pizza ;-)
- more information on <http://ictf.cs.ucsb.edu/> and lecture homepage

Spam

*Int. Secure Systems Lab
Vienna University of Technology*

- Praktika, Bachelor thesis, Diploma theses, Ph.D.
 - We always look for students who want to work on security projects, a *very* incomplete list is on <http://www.seclab.tuwien.ac.at/praktikaandtheses.html>
 - Please do not hesitate to write us your own proposals:
inetsec@seclab.tuwien.ac.at

Conclusion

*Int. Secure Systems Lab
Vienna University of Technology*

Hope you are interested and
we'll see you next week!