OS Security

Summary

Radboud University, Nijmegen, The Netherlands

Winter 2016/2017

Assignment 6

- Deadline - 11 January 2017 (23:59 CET) (EXTENDED)
- Submit via Blackboard (as usual)

Assignment 6

- Deadline - 11 January 2017 (23:59 CET) (EXTENDED)
- Submit via Blackboard (as usual)
- Expect to receive marked assignments back by Wednesday, January 18

Assignment 6

- Deadline - 11 January 2017 (23:59 CET) (EXTENDED)
- Submit via Blackboard (as usual)
- Expect to receive marked assignments back by Wednesday, January 18
- No werkcollege on Friday, January 13

Exam

- Monday, 23 January from 12:30-15:30 in LIN 1
- For students who requested extra time - 12:30-16:00 in HG01.028, same day

Exam

- Monday, 23 January from 12:30-15:30 in LIN 1
- For students who requested extra time - 12:30-16:00 in HG01.028, same day
- Closed book exam, i.e no books, notes or calculator allowed
- You may answer in English or Dutch

Exam

- Monday, 23 January from 12:30-15:30 in LIN 1
- For students who requested extra time - 12:30-16:00 in HG01.028, same day
- Closed book exam, i.e no books, notes or calculator allowed
- You may answer in English or Dutch
- Please use a **blue** pen and proper handwriting!!

How to prepare for the exam?

- Review the lecture materials (slides and recorded lectures)
- Go over the assignments (very strongly recommended!!)
- Complete last year's exam (can be found on the course website, http://www.cs.ru.nl/~vmoonsamy/os-security-2016.html)

Topics covered in this course

- Authentication
- Authorization
- Memory
- Malware
- Mandatory Access Control
- Virtualization
- Mobile Sandboxing and Linux Containers
- (Note: the content of the guest lecture will not be on the exam)

Authentication

- Classical UNIX/Linux authentication
- Password hashing algorithms
- Pluggable authentication modules (PAM) - see assignment as well!
- PAM activities
- PAM configuration syntax

Authorization

- Protection rings in Linux
- Understanding system calls and `strace`
- Kernel modules
- File-related `syscalls`
- Symbolic links and pipes
- Access matrix
- UNIX/Linux protection model
- The setuid bit

Memory

- Virtual/Shared memory
- Memory management unit (MMU)
- Buffer-overflow attack
- Return to libc, ROP, ASLR
- Race conditions

Malware

- Types of malware (both on desktops and smartphones)
- Malware detection: signature- and behavior-based detection
- Intrusion detection system: host- and network-based
- SNORT

Mandatory Access Control

- Bell-LaPadula
- Biba model
- Linux Security modules
- SELinux
- Type enforcement

Virtualization

- Protection rings
- Kernel and user mode
- Types of virtualization
- VM vulnerabilities

Mobile Sandboxing and Linux Containers

- Android software stack: (i) application, (ii) middleware and (iii) kernel layer
- Linux Containers (LXC)
- Namespaces and cgroups