

Fundamentos de Segurança Informática (FSI)

2021/2022 - LEIC

Manuel Barbosa
mbb@fc.up.pt

Aula 0

Apresentação

Porquê FSI na LEIC?

**Harvard
Business
Review**

[Diversity](#) [Latest](#) [Magazine](#) [Ascend](#) [Topics](#) [Podcasts](#) [Video](#) [Store](#)

Security & Privacy

Every Computer Science Degree Should Require a Course in Cybersecurity

by Jack Cable

August 27, 2019

**A segurança informática faz parte
das competências fundamentais de
um programador/informático**

Competências fundamentais

- Compreender a necessidade de considerar sempre aspetos de segurança
- Contribuir para a redução/deteção de erros e potenciais vulnerabilidades
- Saber comunicar com equipas especializadas em segurança informática
- Perceber o que significa trabalhar em segurança informática
 - Identificar sub-áreas e níveis tecnológicos associados
 - (Decisão informada sobre uma carreira nesta área)

Tópicos

- Princípios da segurança informática e posicionamento de segurança
- Princípios da construção de sistemas seguros
- Conceitos básicos de criptografia
- Controlo de acessos e autenticação
- Introdução à programação defensiva
- Tópicos de segurança de redes
- Segurança Web

Inspiração/Acknowledgement

Inspiração para conteúdos, forma de apresentação e estruturação dos slides teóricos.

- CSE 127: Computer Security, University of California, San Diego,
 - Nadia Heninger, (<http://cseweb.ucsd.edu/classes/wi21/cse127-a/>)
 - Stefan Savage, (<http://cseweb.ucsd.edu/classes/fa18/cse127-a/index.html>)
- CS155 : Computer and network security, Stanford,
 - Dan Boneh and Zakir Durumeric, (<https://cs155.stanford.edu>)
- CS261, Computer Security, Berkeley,
 - David Wagner, (<https://people.eecs.berkeley.edu/~daw/teaching/cs261-s21/>)
- CS343: Computer & Information Security, Oberlin College,
 - Steven Checkoway, (<https://checkoway.net/teaching/cs343/2020-fall/>)

Os slides contêm imagens retiradas de referências Web, nomeadamente da Wikipedia (caso default quando a origem de uma imagem não é explicitamente referenciada).

Ética

- Muitas dos ataques de que falamos nas aulas **são crime**
- Nunca fazer hacking sem permissão: **pedir permissão e não desculpa**
- Praticar sempre **responsible disclosure**
- Ser um ethical (ou não) hacker reputado (e livre) exige
 - (muito) trabalho e competência
 - consistência e paciência
 - discrição

Logística de FSI

Aulas teóricas

- Duas aulas de 1 hora por semana x2 turmas! 🥲
- Duração de aproximadamente 45 minutos (gravadas)
 - 5/10 minutos finais para perguntas (não gravadas)
- Videos das aulas T serão colocadas no Moodle
 - objetivo => auxilio no estudo para testes
 - exigem edição => não estarão necessariamente disponíveis antes da aula TP relevante
 - **IMPORTANTE: videos não substituem participação nas aulas teóricas**
 - **as atividades das aulas TP baseiam-se nas aulas Teóricas!**

Aulas Teórico-Práticas

- Atividades propostas semanalmente
 - Grupos de 3 alunos **do mesmo turno (sem exceções)** => inscrições no Moodle
- Dois tipos de atividades:
 - resolução de tutoriais nas aulas TP
 - resolução de pequenos desafios tipo CTF propostos online
- Todas as atividades devem estar documentadas em **log book**
 - **log book** = repositório git do grupo ao qual docente TP tem acesso

Avaliação

- Teste intercalar em Novembro (1a metade da matéria, nota mínima 6/20) => 30%
- Exame final na época normal (2a metade da matéria, nota mínima 6/20) => 30%
- Atividades propostas para aulas TP (nota mínima 10/20) => 20%
- Desafios CTF (nota mínima 10/20) => 20%
- Avaliação TP/CTF:
 - acompanhamento semanal pelo docente TP
 - com base no log book mantido pelo grupo
 - nota atribuída no final do semestre

Comunicação

- Informação estática no sigarra (Ficha de UC)
- Videos, slides, enunciados, etc => ver Moodle
- Interação com os docentes => canal Slack (ver Moodle)
- **Próximos passos:**
 - **Consultar Moodle => tudo o que têm de fazer está lá**
 - **Participar nas aulas**
 - **Dúvidas: falar com professores nas aulas ou usar Slack**

Bibliografia

- Bibliografia obrigatória:
 - Slides e videos das aulas teóricas
 - Material das aulas TP
- Bibliografia complementar:
 - Michael Goodrich and Roberto Tamassia, Introduction to Computer Security, ISBN: 978-0321512949, Pearson, 2014