CI1007 - Cronograma 2026/1

- As atividades indicadas com  serão avaliadas;
- Os projetos devem ser entregues usando o Moodle.
- Leia com atenção as Regras das Atividades de Laboratório.

Regras de avaliação

A média final da disciplina é calculada com as notas das provas e dos trabalhos solicitados (entre 0 e 100), da seguinte forma:

```
Média = (P1 + P2 + T1 + T2) / 4
P1: prova do 1º bimestre (parcial)
P2: prova do 2º bimestre (parcial)
T1: média dos trabalhos do 1º bimestre
T2: média dos trabalhos do 2º bimestre
```

23/2: Aula 1

- Apresentação da disciplina
- Conceitos básicos
- Conteúdo complementar:
  - Computer security, C. Landwehr, 2001
  - Basic Concepts and Taxonomy of Dependable and Secure Computing. A. Avizienis et al, 2004
  - A Review of Information Security Principles, 1997

25/2: Aula 2

- Conceitos básicos (cont.)
-  Atividade: Base de Vulnerabilidades (prazo: aula 5)

2/3: Aula 3

- Criptografia: conceitos básicos; algoritmos simétricos
- Atividade em sala sobre cifradores simétricos

4/3: Aula 4

- Criptografia: algoritmos assimétricos
-  Atividade: O algoritmo RSA (não precisa fazer o 3.6) (prazo: aula 7)
- Conteúdo complementar:
  - Video: Acordo de chaves de Diffie-Hellman (video 1, video 2)
  - Texto: How RSA Works with Examples
  - Vídeo: o algoritmo RSA (video 1, video 2)
  - Vídeo: Elliptic Curves Cryptography

9/3: sem aula

11/3: sem aula

16/3: Aula 5

- Criptografia: resumo criptográfico; assinatura digital; certificado de chave pública; infraestrutura de chaves públicas.
- Conteúdo complementar:
  - Certificate MITM attack 1, 2011
  - Certificate MITM attack 2, 2019

18/3: Aula 6

- Autenticação: usuários e grupos; técnicas de autenticação; senhas; senhas descartáveis
- Definir Tópicos em autenticação para os seminários
- Leitura complementar:
  - The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes, IEEE Symposium on Security and Privacy, 2012.
  - Designing Password Policies for Strength and Usability, Shay et al, 2016.
  - Método Diceware
  - TOTP

23/3: Aula 7

- Atividade (Lab 12 do DINF): Certificados digitais
- Conteúdo complementar: Modelos de criptografia de chave pública alternativos. Goya et al, minicurso do SBSeg 2009.

25/3: Aula 8

- Atividade (Lab 12 do DINF): Quebra de senhas
- Leitura complementar: Password cracking

30/3: Aula 9

- Autenticação: desafio/resposta; técnicas biométricas
- Leitura complementar:
  - Introdução à Biometria. Costa et al, SBSeg 2006.

1°/4: Aula 10

- Infraestruturas de autenticação; Kerberos
- Leitura complementar:
  - Gerenciamento de Identidades Federadas. Wangham et al, SBSeg 2010.

6/4: sem aula

8/4: Aula 11

-  Atividade: seminários sobre Tópicos em autenticação

---

13/4: Aula 12

- Atividade: seminários (cont.)

15/4: Aula 13

- Atividade: seminários (cont.)

20/4: sem aula

🙂

22/4: Aula 14

- ❗ Prova 1 (conteúdo: conceitos básicos, criptografia, autenticação)

27/4: Aula 15

- Controle de acesso: políticas, modelos e mecanismos de controle de acesso; políticas discricionárias; políticas obrigatórias
- Definir Tópicos em controle de acesso para os seminários

29/4: Aula 16

- Controle de acesso: políticas baseadas em domínios; políticas baseadas em papéis; políticas baseadas em atributos.
- Controle de acesso: mecanismos de controle de acesso: infraestrutura básica, controle de acesso em UNIX, controle de acesso em Windows
- Leitura complementar:
  - RBAC: Role-Based Access Controls, 1992; Role-Based Access Control Models, 1996.
  - ABAC: Guide to Attribute Based Access Control (ABAC) Definition and Considerations, 2014.
  - UCON: The UCONabc usage control model, 2004.

—-

4/5: sem aula

🙂

6/5: Aula 17

- Controle de acesso: mudança de privilégios
- Credenciais de um processo em UNIX: credentials.c

11/5: Aula 18

Palestras convidadas:

- **Segurança ofensiva além do hacking**, por Thayse Solis.

Thayse Solis é profissional de segurança da informação. Atua como consultora de segurança ofensiva e é instrutora na Mente Binária. É engenheira de computação pela Universidade Tecnológica Federal do Paraná e mestre em Informática pela Universidade Federal do Paraná. Além disso, possui bacharelado em Música pela Universidade Estadual do Paraná. Thayse é palestrante em eventos técnicos da área de cibersegurança, tendo participado de edições do Hacking na Web Day, BxSec Security Conference, BSides VIX, Nullbyte e H2HC. Possui certificações profissionais, incluindo SCMP|A – Mobile Pentester Android pela Sec4US, PenTest+ pela CompTIA e eJPT pela INE.

- **Racing for Fun and Profit – When bugs turn into bonuses**, por Maycon Vitali.
  Maycon Vitali é especialista em segurança ofensiva, com aproximadamente duas décadas de experiência na identificação e exploração de vulnerabilidades em sistemas e aplicações. Ao longo de sua carreira, atuou em avaliações técnicas de segurança, pesquisa aplicada e desenvolvimento de ferramentas voltadas à análise de ameaças e testes de intrusão. É palestrante em conferências nacionais relevantes na área de segurança da informação, como H2HC e NullByte, além de integrar a organização de eventos técnicos, incluindo o BSides Vitória. Possui certificações profissionais reconhecidas internacionalmente, entre elas OSCE, CRTE e eMAPT, que atestam elevada proficiência prática em exploração de sistemas e ambientes complexos. É graduado em Ciência da Computação e mestre em Informática. Também é fundador do Hack N' Roll, iniciativa criada em 2008 dedicada à pesquisa e à consultoria em segurança cibernética, com foco em técnicas avançadas de avaliação ofensiva.

13/5: Aula 19

*  Atividade: seminários sobre Tópicos em controle de acesso

---

18/5: Aula 20

- Atividade: seminários (cont.)

20/5: Aula 21

Palestra convidada:

- **Segurança em Hardware**, por Newton C. Will (UTFPR).
  Graduado em Tecnologia em Sistemas de Informação pela UTFPR (2007), Mestre em Engenharia Elétrica pelo Programa de Pós-graduação em Engenharia Elétrica da UTFPR Pato Branco e Doutor em Ciência da Computação pelo Programa de Pós-Graduação em Informática da UFPR, com pesquisa na área de Segurança Computacional. Atualmente é Professor na UTFPR Campus Curitiba.

25/5: Aula 22

- Atividade: seminários (cont.)

27/5: Aula 23

- Auditoria: coleta de dados; análise de dados; auditoria preventiva
- Leitura complementar:
  - NIST Guide to Intrusion Detection and Prevention Systems (IDPS), 2007
  - Intrusion Detection Systems: A Survey and Taxonomy, 2000.
- Exemplos de NIDS: Suricata, Snort, Kismet
- Exemplos de HIDS: OSSEC, Samhain, TripWire
- Exemplo de IPS: Fail2ban

1/6: Aula 24

Palestra convidada:

- **Segurança de redes na RNP**, por Christian Lyra (RNP).
  Christian Lyra é formado em Ciência da Computação e mestre em redes de computadores pela UFPR. Atualmente é o coordenador técnico do Presença da Rede Nacional de Pesquisa (RNP) no Paraná.

3/6: Aula 25

- **Exploits e Patches: A Complexidade do Ataque e a Simplicidade da Defesa**, por Jorge Correia.
  Bugs são falhas de implementação que podem existir em software ou hardwere. A partir do momento que essa falha pode ser explorada para contornar mecanismos de segurança, o bug passa a ser uma vulnerabilidade. A criação de um exploit para abusar dessa brecha costuma ser complexa e exige bastante conhecimento técnico sobre o alvo. Mas como a complexidade de um ataque se compara à simplicidade da sua mitigação? Nesta palestra, vamos mostrar essa diferença. Olhando para o Kernel Linux, vamos comparar o funcionamento de exploits para vulnerabilidades como o Dirty Pipe (CVE-2022-0847) e udmabuf (CVE-2023-2008) com os seus patches de correção. Em seguida, sairemos do software: afinal, o que significa uma vulnerabilidade de hardware? É possível aplicar um patch em uma CPU física que já está rodando? Ao observar falhas como Spectre (CVE-2017-5753, CVE-2017-5715), Meltdown (CVE-2017-5754) e Zenbleed (CVE-2023-20593), vamos responder a essas perguntas e mostrar como a indústria conserta problemas diretamente nos nossos processadores.
  Jorge Correia é doutorando em Ciência da Computação e mestre em Informática pela Universidade Federal do Paraná (UFPR), onde também atuou como professor substituto entre 2024 e 2025. Sua pesquisa tem foco em segurança de sistemas operacionais, segurança assistida por hardware, segurança de redes, virtualização e sistemas de arquivos.

8/6: sem aula

10/6: Aula 26

-  Atividade: demonstrações de ataques (tem peso 2 na avaliação)

15/6: Aula 27

- Demonstrações de ataques (cont.)

17/6: Aula 28

- Demonstrações de ataques (cont.)

22/6: Aula 29

- Demonstrações de ataques (cont.)

24/6: Aula 30

-  Prova 2 (conteúdo: controle de acesso, auditoria)

29/6: sem aula

1°/7: Exame final
