Demonstrações de Ataques

Esta atividade consiste em produzir uma demonstração prática de um determinado ataque e das possíveis defesas contra o mesmo. Podem ser usados os seguintes ataques:

1. ~~stack overflow~~
2. heap overflow
3. format string
4. null pointer dereference
5. TOCTTOU (time of check to time of use)
6. local denial of service
7. remote denial of service
8. distributed denial of service
9. cross-site scripting
10. cross-site request forgery
11. directory traversal
12. SQL injection
13. hash collision
14. replay
15. ARP poisoning
16. MITM – connection hijacking
17. WEP/WPA cracking
18. Rootkits
19. Return to LibC
20. race condition attack
21. ... (sugestões são bem-vindas)

Cada aluno ou grupo será designado responsável por um ataque e deverá produzir:

- um artigo (PDF) explicando em que consiste o ataque (vulnerabilidade explorada, princípio de funcionamento, resultados), qual a infraestrutura/plataforma e ferramentas usadas para a demonstração, uma descrição passo-a-passo (sucinta) do ataque e quais as possíveis defesas contra ele.
- Uma **demonstração prática** 😮 do ataque em sala de aula:
  - aspectos conceituais do ataque
  - ataque com sucesso
  - possíveis estratégias de defesa
  - ataque sem sucesso (usando uma defesa)

O PDF produzido deverá ser enviado ao professor **antes da apresentação**.