Projeto em Segurança – Técnicas de Intrusão

Os testes de intrusão são constituídos por um conjunto de técnicas que permitem identificar métodos de contornar as medidas de segurança de uma Aplicação, Sistema e/ou Rede.
A finalidade de um teste de intrusão é:

- Medir a reação e a tolerância do sistema, a padrões de ataque;
- Aferir o nível de sofisticação necessário a um atacante, para comprometer o sistema;
- Identificar as contramedidas adicionais necessárias, para evitar ataques ao sistema;
- Avaliar a capacidade atual para detetar e responder adequadamente a ataques.

Na disciplina de Engenharia de Segurança, o *focus* é colocado nas medidas de segurança, trabalhando-se os conceitos de segurança que o developer deverá conhecer ao desenvolver software.
Nessa perspetiva, este projeto permite que o aluno obtenha também conhecimento de quais as técnicas de intrusão utilizadas, permitindo-lhe perceber ainda melhor a necessidade das medidas de segurança no desenvolvimento de software.

Os grupos que optarem por este projeto têm de:

- Seguir o PTES (*Penetration Testing Execution Standard*[1]) nas suas fases de *Pre-Engagement*, *Intelligence Gathering*, *Threat Modeling*, *Vulnerability Analyis* e *Reporting*;
- Efectuar as fases de *Exploitation* e *Post Exploitation* do PTES, apenas após a concordância explícita do titular dos sistemas/aplicações/redes a serem alvo dessas fases.

Como bibliografia auxiliar poderão utilizar o NIST SP 800-115[2] (*Technical Guide to Information Security Testing and Assessment*), ISSAF (*Information System Security Assessment Framework*) e OWASP *Testing Guide*[3].

Este projeto pode ser desenvolvido por até dois grupos, que trabalharão autonomamente e, cada um deles irá seguir o PTES para efetuar testes de intrusão às empresas MediaSis e Modula C.

[1] http://www.pentest-standard.org
[2] https://csrc.nist.gov/publications/detail/sp/800-115/final
[3] https://www.owasp.org/index.php/OWASP_Testing_Project