DISCIPLINA: Tópicos Especiais em Computação e Algoritmos: Laboratório de Segurança Ofensiva de Software	**CÓDIGO**:

VALIDADE: Início: **01/2022** Término:

Carga Horária: Total: 30 horas/aula Semanal: 02 aulas Créditos: 02
Modalidade: Prática
Classificação do Conteúdo pelas DCN: Optativa

Ementa:

Práticas em laboratório dos temas e tópicos abordados na disciplina Segurança Ofensiva de Software:

- Praticar procedimentos para varreduras de redes e sistemas, descoberta de vulnerabilidades e uso de ferramentas.
- Exercitar a execução dos principais ataques contra aplicações Web (OWASP Top 10) e testar a eficácia das possíveis proteções ou contra medidas.
- Exercitar a execução dos principais ataques de corrupção da memória e testar a eficácia das possíveis proteções ou contra medidas.

Cursos	**Período**	**Eixo**	**Obrig.**	**Optativa**
Engenharia de Computação	7º	Fundamentos de Engenharia de Computação		X

Departamento/Coordenação: Departamento de Computação (DECOM)

INTERDISCIPLINARIDADES

Pré-requisitos	**Código**
Banco de Dados I	2ECOM.033
Redes de Computadores I	2ECOM.044
Sistemas Operacionais	2ECOM.072
Co-requisitos	
Segurança Ofensiva de Software	

Objetivos: *A disciplina deverá possibilitar ao estudante*	
1	Praticar em laboratório a execução de procedimentos comuns em um teste de invasão.
2	Praticar em laboratório a varredura de sistemas computacionais e a descoberta de vulnerabilidades em softwares.
3	Praticar em laboratório a exploração dos principais tipos de vulnerabilidades encontradas em sistemas computacionais.
4	Experimentar a eficácia dos principais mecanismos de proteção e contra medidas para mitigar vulnerabilidades em software.

Unidades de ensino		Carga-horária Horas/aula
1	Redirecionamento de portas e tunelamentos para tráfegos de rede.	2
2	Execução de ataques de força bruta contra bases de senhas e serviços (hydra, John the ripper, rainbow tables).	2
3	Descoberta de vulnerabilidades em softwares através de método *fuzzing* com a ferramenta Spike.	2
4	Uso do framework Metasploit para fazer varreduras, criar payloads e disparar ataques.	2
5	Uso de *Proxies* Web para a varredura e exploração de aplicações Web.	2
6	Envio de entradas com caracteres ofuscados para aplicações web.	2
7	Exploração de vulnerabilidades do tipo *Cross Site Scripting* (XSS).	2
8	Exploração de vulnerabilidades do tipo *Cross Site Request Forgery*.	2
9	Exploração de vulnerabilidades que permitem a inclusão de arquivos locais ou remotos em sistemas web.	2
10	Injeção de artefatos maliciosos via consultas SQL.	2
11	Inserção de porta de entrada (*backdor*) em binários.	2
12	Alteração de binários para a superação de antivírus.	2
13	Ofuscação de *payloads* e exploração de vulnerabilidades de estouro de *buffer* na pilha.	2
14	Uso da técnica de *Egg Hunting* para explorações de corrupção da memória com restrições de espaço.	2
15	Uso da técnica *Return-Oriented Programming* para explorar vulnerabilidades em sistemas com proteções $W \oplus X$ habilitadas.	2
	Total	30

Bibliografia Básica	
1	Erickson, Jon. "**Hacking: The Art of Exploitation**", 2008.
2	Stuttard, Dafydd; Pinto, Marcus. "**The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws**", 2011.

Bibliografia Complementar	
1	https://sites.google.com/site/mateustymbu/SBSeg_2012-Minicurso1.pdf
2	https://www.corelan.be/index.php/articles/
3	https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/
4	Anley C., Heasman J., Lindner F., e Richarte G. "The Shellcoder's Handbook: Discovering and Exploiting Security Holes", 2004.
5	Kennedy, David et al. "Metasploit: The Penetration Tester's Guide", 2011.