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

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

Carga Horária: Total: 60 horas/aula Semanal: 04 aulas Créditos: 04
Modalidade: Teórica
Classificação do Conteúdo pelas DCN: Optativa

Ementa:

Introdução aos conceitos e principais práticas relativas a testes de invasão: ética, carreira, certificações, CTFs e metodologias. Procedimentos para varreduras de redes e sistemas, descoberta de vulnerabilidades e uso de ferramentas. Principais ataques contra aplicações Web (OWASP Top 10) e possíveis proteções ou contra medidas. Principais ataques de corrupção da memória e 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	
Laboratório de Segurança Ofensiva de Software	

Objetivos: *A disciplina devera possibilitar ao estudante*	
1	Conhecer os procedimentos para a execução de um teste de invasão.
2	Saber relatar com clareza e ética as falhas encontradas em um teste de invasão, bem como eventuais correções.
3	Saber encontrar e explorar as principais vulnerabilidades em sistemas computacionais.
4	Saber propor soluções de proteção ou contra medidas para mitigar as vulnerabilidades encontradas.

Unidades de ensino		Carga-horária Horas/aula
1	**Introdução aos testes de invasão** • Ética na execução de testes de invasão (*pentest*). • Carreira de *pentester*. • Certificações. • Competições "*Capture the flag*". • Fases e metodologias de *pentest*. • Elaboração de relatórios. • Conceitos gerais: vulnerabilidade, *exploit*, *shellcode*, *payload*. • Serviços úteis: TFTP, FTP, SSH (scp), Apache.	4
2	**Varreduras, descoberta de vulnerabilidades e ferramentas** • Varreduras de rede (nmap, netcat, wireshark). • Coleta de informações (*Google Hacking*, whois, recursos web). • Reconhecimento de serviços (DNS, SNMP, SMTP, Netbios). • Ataques a tráfegos de rede (*ARP Spoofing*, *DNS Spoofing*, *Man in the Middle*, Evasão de firewall). • Redirecionamento de portas e tunelamentos. • Ataques de força bruta (hydra, John the ripper, rainbow tables). • Descobrindo vulnerabilidades via método *Fuzzing* (Spike). • Ataques por acesso físico a dispositivos (*resetting*). • Ofuscadores (*rootkits*) e portas de entrada (*backdor*) em sistemas. • Escalada de privilégios. • Metasploit.	18
3	**Ataques contra aplicações Web** • Ofuscação de caracteres. • *Cross site scripting*. • *Cross site request forgery*. • Inclusão de arquivos locais e remotos. • Injeção via SQL. • *Proxies* Web.	14
4	**Proteções para ataques contra aplicações Web** • Filtros de dados. • Assinaturas (IDS, IPS). • *Firewalls*. • Ofuscação de dados.	4

5	**Ataques de corrupção da memória** • Ofuscação de código. • Estouro de *buffer* na pilha. • Estouro de *buffer* no *heap*. • *Return after free*. • Falhas de formatação de strings. • Sobrescrita de Tratadores de Exceção Estruturados (SEH). • Egg hunting. • Heap Spraying. • Programação Orientada a Retornos (ROP). • Porta de entrada (*backdor*) em binários • Superação de antivírus.	14
6	**Proteções para ataques de corrupção da memória** • Pilha não-executável (nx-stack). • Canários / *Cookies*. • SafeSEH e SEHOP. • Espaço aleatório de endereços (ASLR). • Prevenção de Execução de Dados (DEP). • Integridade do Fluxo de Execução (CFI, CET). • Anti-vírus.	6
	Total	60

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.