UNIVERSIDADE FEDERAL DE UBERLÂNDIA
Faculdade de Computação
Av. João Naves de Ávila, nº 2121, Bloco 1A - Bairro Santa Mônica, Uberlândia-MG, CEP 38400-902
Telefone: (34) 3239-4144 - http://www.portal.facom.ufu.br/ facom@ufu.br

PLANO DE ENSINO

1. IDENTIFICAÇÃO

Componente Curricular:	Tópicos Especiais em Segurança da Informação - Laboratório de Segurança de Redes - Ataques e Mecanismos de Defesa							
Unidade Ofertante:	FACOM							
Código:	GBC235		Período/Série:		7º	Turma:	S	
Carga Horária:						Natureza:		
Teórica:	30	Prática:	30	Total:	60	Obrigatória:	()	Optativa: (X)
Professor(A):	Rodrigo Sanches Miani					Ano/Semestre:	2021-2	
Observações:								

2. EMENTA

Princípios de Segurança da Informação, Análise de Ciberataques, Segurança em Aplicações, Segurança de Rede e Mecanismos Clássicos de Defesa.

3. JUSTIFICATIVA

Segurança da informação é a atividade de assegurar a proteção de informação em termos de confidencialidade, integridade e disponibilidade. Atualmente, o uso de sistemas e conceitos de segurança da informação é amplamente difundido para uma grande gama de aplicações, variando desde a segurança em computadores pessoais até em grandes infraestruturas como a Internet. O Bacharelado em Ciência da Computação possui uma disciplina que trata de conceitos de segurança da informação (GBC083). Contudo, o foco de tal disciplina está no estudo de algoritmos criptográficos. Conceitos relacionados a outros tópicos da área de segurança da informação como segurança de software, segurança de redes e aspectos humanos em ciberataques são essenciais para diversificar e complementar a formação dos alunos.

4. OBJETIVO

Objetivo Geral:

Ao final do curso o aluno conhecerá, de forma prática, os principais ciberataques e os respectivos mecanismos de defesa contra eles. O aluno também irá adquirir a capacidade de identificar vulnerabilidades de segurança em diferentes tipos de sistemas. Adicionalmente, o aluno desenvolverá senso crítico sobre os riscos e ameaças de segurança presentes nos sistemas computacionais.

5. PROGRAMA

1. Conceitos Básicos de Segurança da Informação - Confidencialidade, Integridade e Disponibilidade.
2. Conceitos Básicos de Segurança da Informação - Riscos e considerações sobre Segurança;
3. Introdução a Segurança de Redes – Conceitos básicos de Linux e Bash Script;
4. Introdução a Segurança de Redes - Potenciais atacantes;
5. Introdução a Segurança de Redes - Pontos explorados;
6. Introdução a Segurança de Redes - Planejamento de ataques (Wireshark, Google Directives, Nmap, Nslookup, Whois entre outras);
7. Exemplos de ataques - Ataques de Negação de Serviço (DoS);
8. Exemplos de ataques - Códigos maliciosos;
9. Exemplos de ataques – Exploração de vulnerabilidades de segurança;
11. Aplicações de Segurança de Redes - Firewalls e Sistemas de Detecção de Intrusão;
12. Atividades práticas (laboratórios usando máquinas virtuais) sobre cada um dos itens vistos acimas.

6. METODOLOGIA

A disciplina será organizada no formato semanal com auxílio do sistema Microsoft Teams. Notas de aula, códigos-fonte, exercícios e materiais complementares serão disponibilizados em uma equipe, previamente criada, no Microsoft

Teams. Máquinas virtuais fornecidas pelo projeto SEED Labs (https://seedsecuritylabs.org/labsetup.html) serão utilizadas para conduzir a parte prática da disciplina.

As aulas presenciais acontecem às terças de 14h50min às 18h30min.

O cronograma a seguir detalha as atividades a serem realizadas em cada aula.

Aula	Semana	Data	Modalidade	Conteúdo/Descrição	Carga Horária (hora-aula)	Formato
1	1	03/05/2022	Presencial	Conceitos Básicos de Segurança da Informação - Lab 1: Máquinas virtuais	4	Expositiva/Prática
2	2	10/05/2022	Presencial	Introdução a Segurança de Redes - Parte 1 - Lab 2: Conceitos básicos de Linux e Bash Script	4	Expositiva/Prática
3	3	17/05/2022	Presencial	Introdução a Segurança de Redes - Parte 2 - Lab 3: Primeiras atividades de reconhecimento	4	Expositiva/Prática
4	4	24/05/2022	Presencial	Introdução a Segurança de Redes - Parte 3 - Lab 4: Reconhecimento passivo	4	Expositiva/Prática
5	5	31/05/2022	Presencial	Introdução a Segurança de Redes - Parte 4 - Lab 5: Varredura de portas (Port scanning)	4	Expositiva/Prática
6	6	07/06/2022	Presencial	Introdução a Segurança de Redes - Parte 5 - Lab 6: Varredura em múltiplos alvos	4	Expositiva/Prática
7	7	14/06/2022	Presencial	Introdução a Segurança de Redes - Parte 6 - Lab 7: Obtenção de informações livres	4	Expositiva/Prática
8	8	21/06/2022	Presencial	Exemplos de ataques - Parte 1 - Lab 8: Ataques de Negação de Serviço (DoS)	4	Expositiva/Prática
9	9	28/06/2022	Presencial	Exemplos de ataques - Parte 2 - Lab 9: Análise estática de códigos maliciosos	4	Expositiva/Prática
10	10	05/07/2022	Presencial	Exemplos de ataques - Parte 3 - Lab 10: Análise dinâmica de códigos maliciosos	4	Expositiva/Prática
11	11	12/07/2022	Presencial	Exemplos de ataques - Parte 4 - Lab 11: Explorar vulnerabilidades de segurança em um sistema Web	4	Expositiva/Prática
12	12	19/07/2022	Presencial	Mecanismos de defesa - Parte 1 - Filtro de pacotes (Firewall) - Lab 12	4	Expositiva/Prática
13	13	26/07/2022	Presencial	Mecanismos de defesa - Parte 2 - Sistemas de detecção de intrusão - Snort - Lab 13	4	Expositiva/Prática
14	14	02/08/2022	Presencial	Mecanismos de defesa - Parte 3 - Sistemas de detecção de intrusão baseados em anomalia - Lab 14	4	Expositiva/Prática
15	14		Assíncrona	Mecanismos de defesa - Parte 3 - Sistemas de detecção de intrusão baseados em anomalia	4	Prática
16	15		Assíncrona	Mecanismos de defesa - Parte 3 - Sistemas de detecção de intrusão baseados em anomalia	4	Prática
17	15	09/08/2022	Presencial	Mecanismos de defesa - Parte 3 - Sistemas de detecção de intrusão baseados em anomalia - Lab 14	4	Expositiva/Prática
18	16	16/08/2022	Presencial	Dúvidas sobre o laboratório 14 e encerramento da disciplina	4	Expositiva/Prática
				Carga horária Presencial - Total	64	
				Carga horária Assíncrona - Total	8	
				Carga Horária - Total	72	

7. ATENDIMENTO

O atendimento aos alunos ocorrerá nas quintas-feiras, entre 16h e 18h na sala 1B148, campus Santa Mônica. A comunicação com a turma ocorrerá por meio de mensagens no grupo da disciplina, no sistema Microsoft Teams.

8. AVALIAÇÃO

Trabalhos: os trabalhos consistirão na entrega (via Microsoft Teams) de relatórios referentes à diferentes tipos de atividades práticas relacionadas simulação de ataques e desenvolvimento de mecanismos de defesas sobre segurança de redes. Serão solicitados 14 trabalhos (um por aula, de acordo com o cronograma detalhado em "Metodologia"), totalizando 100 pontos.

Recuperação: para os alunos com frequência mínima de 75% (setenta e cinco por cento) na disciplina e que não atingiram a pontuação necessária para a aprovação, será oferecido ao aluno(a) a oportunidade de refazer até três atividades (menores notas).

9. **BIBLIOGRAFIA**

Básica

NAKAMURA, E. M., and GEUS, P.L. Segurança de redes em ambientes cooperativos. Novatec. (2007).

STALLINGS, William, and Lawrie BROWN. Segurança de computadores: princípios e práticas. (2014).

DU, Wenliang. Computer Security: A Hands-on Approach. (2018).

ENGEBRETSON, Patrick. The basics of hacking and penetration testing: ethical hacking and penetration testing made easy. Elsevier, (2013).

Complementar

STALLINGS, W. Criptografia e segurança de redes: princípios e práticas. Pearson Prentice Hall, 2008.

Hack Attack Systems. How to Conduct your own security audit. Chirilo. John. Wiley Publishing

BELLOVIN, Steven M. **Thinking Security: Stopping Next Year's Hackers**. Addison-Wesley Professional, 2015.

10. **APROVAÇÃO**

Aprovado em reunião do Colegiado realizada em: ____/____/_____

Coordenação do Curso de Graduação: _____