MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA

CST EM REDES DE COMPUTADORES

INSTITUTO FEDERAL
Paraíba
Campus João Pessoa

PLANO DE DISCIPLINA		
IDENTIFICAÇÃO		
CURSO: **Curso Superior de Tecnologia em Redes de Computadores**		
DISCIPLINA: **Práticas de Segurança de Redes**	CÓDIGO DA DISCIPLINA: **65**	
PRÉ-REQUISITO: Segurança de Redes de Computadores e Administração de Sistemas Proprietários		
UNIDADE CURRICULAR: Obrigatória [X] Optativa [ ] Eletiva [ ]	SEMESTRE: **2018.1**	
CARGA HORÁRIA		
TEÓRICA: **20h**	PRÁTICA: **47h**	EaD[1]:
CARGA HORARIA SEMANAL: **4h**	CARGA HORÁRIA TOTAL: **67h**	
DOCENTE RESPONSÁVEL: **JOSE GOMES QUARESMA FILHO**		

EMENTA

Identificação de vulnerabilidades e ameaças em redes de computadores. Principais ataques em redes de computadores. Mecanismos de segurança em redes de computadores. Testes de penetração (*Pentest*). *Honeypots* e *Honeynets*.

OBJETIVOS

Geral: Implementar mecanismos de segurança para a proteção das redes de computadores

Específicos: Compreender o processo de identificação de vulnerabilidades e ameaças em redes de computadores. Compreender os principais ataques e anatomia de um ataque em redes de computadores. Implementar mecanismos de segurança em redes de computadores. Realizar testes de penetração em redes de computadores. Implantação de *honeypots* e *honeynets*.

CONTEÚDO PROGRAMÁTICO

Unidades	**Aulas**

[1] Para a oferta de disciplinas na modalidade à distância, integral ou parcial, desde que não ultrapasse 20% (vinte por cento) da carga horária total do curso, observar o cumprimento da Portaria MEC nº 1.134, de 10 de outubro de 2016.

Unidade 1 – Vulnerabilidades e ameaças • Histórico e definições • Processo de identificação catalogação de vulnerabilidades (https://cve.mitre.org/)	10
Unidade 2 – Ataques em redes de computadores • Ataques em camada de aplicação • Ataques em camada de transporte • Ataques em camada de rede • Ataques em camada de enlace	20
Unidade 3 – Mecanismos de segurança em redes de computadores • Firewalls • Proxies • Sistemas de detecção de intrusão • Redes privadas virtuais • Segurança de porta • Antivírus corporativo • Autenticação centralizada (Radius e TACACs)	20

Unidade 4 – Testes de penetração (PENTEST)
• Definição do escopo
  ○ *White-box*
  ○ *Black-box*
• Fases do *Pentest*
  ○ Reconhecimento
  ○ Varredura
  ○ Obtenção do acesso e exploração
  ○ Obtenção de evidências e reporte
	20

Unidade 5 – *Honeypots* e *Honeynets*
• Tipos de *honeypots*
  ○ Baixa interatividade
  ○ Alta interatividade
• Tipos de *honeynets*
  ○ Reais
  ○ Virtuais
• Implantação de *honeypots* e *honeynets*
	10

METODOLOGIA DE ENSINO

Aulas expositivas utilizando os seguintes recursos didáticos: quadro branco, pincel atômico, *software* para exibição de *slides* e software simulador de redes em computador com TV ou projetor de vídeo. Aplicação e resolução de listas de exercícios. Aulas práticas em laboratório.

RECURSOS DIDÁTICOS

[X] Quadro
[X] Projetor
[X] Vídeos/DVDs
[X] Periódicos/Livros/Revistas/Links
[X] Equipamento de Som
[X] Laboratório
[X] Softwares[2]: Nmap, Nessus, Openvas, OpenVPN, Kali Linux, GNS3, Cisco Packet Tracer

CRITÉRIOS DE AVALIAÇÃO

Será feita através de instrumentos como avaliações escritas, num total de 3 (três) a cada semestre, e possivelmente através de relatórios de atividades práticas. Além disso, será realizada uma avaliação de recuperação final.

BIBLIOGRAFIA[3]

BIBLIOGRAFIA BÁSICA

1. SCAMBRAY, Joel; McCLURE, Stuart; KURTZ, George. Hackers Expostos: Segredos e Soluções para a Segurança de Redes. 4ª edição. Editora Campus.
2. HATCH, Brian, LEE, James, KURTZ, George. Segurança contra Hackers – Linux, 2ª edição. Editora Futura.
3. NORTHCUTT, Stephen. Como Detectar Invasão em Rede - Um Guia para Analistas.

[2] Especificar
[3] Observar os mínimos de 3 (três) títulos para a bibliografia básica e 5 (cinco) para a bibliografia complementar.

Editora Ciência Moderna, 2000.

BIBLIOGRAFIA COMPLEMENTAR

1. BAUER, Michael D. Linux Server Security, 2nd Edition. O´Reilly, 2005.
2. BRAGG, Roberta. Windows Server 2003 Security: A Technical Reference. Addison-Wesley, Paperback, 2005.
3. STALLINGS, William. Criptografia e segurança de redes princípios e práticas. 4. ed. São Paulo: Pearson Prentice Hall, 2008. 492 p. ISBN 9788576051190.
4. CHESWICK, William R; BELLOVIN, Steven M; RUBIN, Aviel D. Firewalls e segurança na Internet: repelindo o hacker ardiloso. 2. ed. Porto Alegre: Bookman, 2005. 400 p. ISBN 8536304294.
5. BURNETT, Steve; PAINE, Stephen. Criptografia e segurança o guia oficial RSA. Rio de Janeiro: Campus, 2002. 367 p. il. ISBN 8535210091.