ATIVIDADES PRÁTICAS SUPERVISIONADAS

CST em Redes de Computadores

5ª. Série

Segurança de Redes

A Atividade Prática Supervisionada (ATPS) é um procedimento metodológico de ensino-aprendizagem desenvolvido por meio de etapas, acompanhadas pelo professor, e que tem por objetivos:

- ✓ Favorecer a autoaprendizagem do aluno.
- ✓ Estimular a corresponsabilidade do aluno pelo seu aprendizado.
- ✓ Promover o estudo, a convivência e o trabalho em grupo.
- ✓ Auxiliar no desenvolvimento das competências requeridas para o exercício profissional.
- ✓ Promover a aplicação da teoria na solução de situações que simulam a realidade.
- ✓ Oferecer diferenciados ambientes de aprendizagem

Para atingir estes objetivos, a ATPS propõe um desafio e indica os passos a serem percorridos ao longo do semestre para a sua solução.

Aproveite esta oportunidade de estudar e aprender com desafios da vida profissional.

AUTORIA:

Renato Cividini Matthiesen

Faculdade Anhanguera de Limeira

COMPETÊNCIAS E HABILIDADES

Ao concluir as etapas propostas neste desafio, você terá desenvolvido as competências e habilidades que constam, nas Diretrizes Curriculares Nacionais, descritas a seguir.

- ✓ Abranger ações de concepção, desenvolvimento, implantação, operação, avaliação e manutenção de sistemas e tecnologias relacionadas à informática e telecomunicações.
- ✓ Desenvolver sistemas informatizados desde a especificação de requisitos até os testes de implantação, bem como as tecnologias de comutação, transmissão, recepção de dados, podem constituir-se em especificidades desse eixo.
- ✓ Elaborar, implantar, gerenciar e manter projetos lógicos e físicos de redes de computadores locais e de longa distância.
- ✓ Promover conectividade entre sistemas heterogêneos, diagnóstico e solução de problemas relacionados à comunicação de dados, segurança de redes, avaliação de desempenho, configuração de serviços de rede e de sistema de comunicação de dados são áreas de desempenho desse profissional.

Produção Acadêmica

Relatórios parciais referentes às pesquisas e atividades desenvolvidas nas etapas:

1. Relatório 01: Conceito sobre Segurança em Redes de Computadores.
2. Relatório 02: Principais Tipos de Ataques em Sistemas em Rede.
3. Relatório 03: Mecanismos de Defesa em Redes de Computadores.
4. Relatório 04: Configurações de Segurança do Sistema de Redes de Computadores.

Participação

Para a elaboração dessa atividade, os alunos deverão previamente organizar-se em equipes com um número de participantes definida pelo professor e entregar seus nomes, RAs e e-mails ao professor da disciplina. Essas equipes serão mantidas durante todas as etapas.

DESAFIO

A cada ano que passa, os sistemas informatizados nas empresas dependem cada vez mais de sistemas distribuídos (fracamente acoplados), suportados na maioria das vezes por redes de computadores. Estes sistemas tornaram possível acessar informações em qualquer local do planeta e têm como interface de acesso a Internet. Isto gera uma melhoria significativa no gerenciamento e na operação dos sistemas, mais também traz um risco muito grande de segurança para os sistemas de informação. Estes sistemas podem ser invadidos, clonados e ter seus dados furtados entre outros problemas. Sempre que se cria uma nova técnica ou ferramenta de segurança para garantir a correta funcionalidade destes sistemas, novas técnicas e ferramentas de invasão também surgem. Torna-se fundamental para toda empresa, conhecer as técnicas de segurança, implantá-las e manter seus sistemas seguros, mobilizando todos seus colaboradores sobre a importância dos sistemas de segurança.

Este desafio propõe que a equipe de tecnologia da informação da empresa (representada por um grupo de alunos) elabore um Manual de Segurança de Redes de Computadores. A primeira parte do manual (Relatório 01 e Relatório 02) destina-se aos colaboradores da empresa, para que eles tenham conhecimento de conceitos básicos de

segurança em redes de computadores e ataques em sistemas de rede. A segunda parte do manual (Relatório 03 e Relatório 04) destina-se ao departamento técnico de Tecnologia da Informação e visa formalizar as técnicas e as ferramentas utilizadas na empresa para prover segurança de seus sistemas. O manual deve conter os seguintes documentos:

1. Relatório 01: Conceito sobre Segurança em Redes de Computadores.
2. Relatório 02: Principais Tipos de Ataques em Sistemas em Rede.
3. Relatório 03: Mecanismos de Defesa em Redes de Computadores.
4. Relatório 04: Configurações de Segurança do Sistema de Redes de Computadores.

Objetivo do Desafio

Elaboração de um Manual de Segurança de Redes de Computadores para disseminação de conhecimentos básicos para funcionários de uma empresa e também com informações técnicas para funcionários especializados na área de tecnologia da empresa.

Livro Texto da Disciplina

A produção desta ATPS é fundamentada no livro-texto da disciplina, que deverá ser utilizado para solução do desafio:

MORAES, Alexandre de. ***Segurança em Redes - Fundamentos***. 1ª ed. São Paulo: Érica, 2010.

ETAPA1 (tempo para realização: 5 horas)

- ✓ **Aula tema: Conceitos de Segurança.**

Esta atividade é importante para que você conheça livros e conceitos básicos e conceitos fundamentais de segurança em redes de computadores.

Para realizá-la é importante seguir os passos descritos.

PASSOS

Passo 1 (Aluno)

Ler atentamente o capítulo do livro texto ou de um livro complementar que faz uma introdução aos conceitos de segurança em redes de computadores.

Passo 2 (Equipe)

Acessar e conhecer o *site* da empresa **Mitnick security Consulting LLC**. Disponível em: <http://mitnicksecurity.com>. Acesso em: 11 ago. 2011.

Passo 3 (Equipe)

Elaborar o Relatório 01: Conceitos sobre Segurança em Redes de Computadores do Manual de Segurança em Redes de Computadores. Este relatório deve conter os seguintes tópicos:

1.1 Introdução à Segurança em Redes de Computadores: escrever um texto que apresente de forma objetiva os fatores que levam as empresas a investirem em sistemas de segurança em redes de computadores de forma contínua.

1.2 Exemplos de Problemas de Segurança em Redes: fazer uma pesquisa na Internet ou em livros/revistas e apresente pelo menos dois casos de problemas ocorridos em sistemas de segurança em rede e suas consequências para as empresas.

1.3 Riscos e Considerações quanto à Segurança em Redes: apresentar e fazer considerações de pelo menos 10 riscos existentes quando uma rede de computadores passa a constituir parte do sistema de informação de uma empresa.

1.4 Histórico de Kevin Mitnick: escrever um pequeno histórico sobre o *hacker* Kevin Mitnick, suas atividades no passado e no presente (1 página).

ETAPA2 (tempo para realização: 5 horas)

✓ **Aula-tema: Principais Tipos de Ataques. Vulnerabilidades dos Protocolos TCP/IP.**

Esta atividade é importante para que você conheça os principais tipos de ataques nos sistemas de informação em uma rede de computadores e as vulnerabilidades apresentadas pelos sistemas que utilizam os protocolos TCP/IP.

Para realizá-la é importante seguir os passos descritos.

PASSOS

Passo 1 (Aluno)

Ler atentamente o capítulo do livro texto ou complementar que apresenta informações a respeito de riscos em sistemas de informação nas organizações.

Passo 2 (Equipe)

Elaborar o Relatório 02: Principais Tipos de Ataques em Sistemas em Rede do Manual de Segurança em Redes de Computadores. Este relatório deve conter os tópicos:

2.1 Potenciais Atacantes: fazer uma descrição sobre os principais tipos de atacantes em sistemas de redes de computadores: *Script Kiddies*, *Cyberpunks*, *Insiders*, *Coders*, *White Hat*, *Black Hat* e *Gray Hat*.

2.2 Terminologia de Segurança: fazer uma descrição dosseguintes termos de segurança em redes de computadores: *Carding, EasterEgg, Media Whore, Phreaking, Suit, Tentacles, Trojan Horse, Virus, Worm, War Dialer* e *Warez*.

2.3 Ataques para Obtenção de Informações: fazer uma descrição dos seguintes tipos de ataques para obtenção de informações em redes de computadores: *Dumpster Diving (Trashing)*, Engenharia Social, Ataque Físico, *Packet Sniffing, Post Scanning*, *Vulnerability Sanning*, *Firewalking* e *IP Spoofing*.

2.4 Ataques de Negação de Serviço: fazer uma descrição das seguintes técnicas de ataques de negação de serviço em redes de computadores: *Bugs* em Serviços, Aplicativos e Sistemas Operacionais, *SYN Flooding*, Fragmentação de Pacotes IP, *Smurfand Fraggle*, *Teardropand Land*.

2.5 Ataque Ativo contra TCP: fazer uma descrição das seguintes técnicas de ataques de ativo contra TCP: Sequestro de Conexões, Prognóstico de Número de Sequência do TCP, Ataque de Mitnick e *Source Routing*.

2.6 Ataques no Nível de Aplicação: fazer uma descrição das seguintes técnicas de ataques no nível de aplicação: *Buffer Overflow*, Ataques na *Web*, Problemas com o SNMP, Vírus, *Worms* e Cavalos de Tróia e *War Dialing*.

ETAPA3 (tempo para realização: 5 horas)

- ✓ **Aula tema: Principais Mecanismos de Defesa. Criptografia. Algoritmos de Chave Pública e Privada. Segurança de Roteadores.**

Esta atividade é importante para que você conheça os principais mecanismos de defesa, técnicas de criptografia e algoritmos de chave pública e privada, realize a configuração em roteadores wireless e de um sistema de firewall em uma rede de computadores.

Para realizá-la é importante seguir os passos descritos.

PASSOS

Passo 1 (Aluno)

Ler atentamente o capítulo do livro texto ou complementar que traz informações referentes às técnicas e mecanismos de defesa em redes de computadores.

Passo 2 (Equipe)

Elaborar o Relatório 03: Mecanismos de Defesa em Redes de Computadoresdo Manual de Segurança em Redes. Os serviços de segurança implementam políticas (diretrizes) de segurança e são implementados por mecanismos de segurança. Este relatório deve conter os seguintes tópicos:

3.1 Serviços de Segurança: apresentar a definição dos seguintes serviços de segurança: Autenticação, Controle de Acesso, Confidencialidade, Integridade, Irretratabilidade e Disponibilidade.

3.2 Mecanismos de Segurança: apresentar a definição e pelo menos um exemplo dos seguintes mecanismos de segurança: Criptografia, Assinatura Digital, Controle de Acesso, Integridade de Dados, Troca de Informações de Autenticação, Preenchimento de Tráfego, Controle de Roteamento e Certificação.

3.3 Segurança em Roteador *Wireless*: fazer e documentar as principais configurações de segurança em um roteador *wireless* de uma rede de computadores local.

3.4 Sistema de *Firewall*: fazer a instalação de um *software* (*Firewall*) ou a configuração de um serviço de *firewall* (o grupo pode definir o *software* ou o sistema). Documentar as etapas de instalação, configuração e as características da rede em relação à proteção oferecida pelo sistema instalado/configurado.

ETAPA4 (tempo para realização: 5 horas)

- ✓ **Aula tema: Redes Privadas Virtuais (VPN). Política de Segurança.**

Esta atividade é importante para que você entenda e pratique as configurações de segurança em roteadores, conheça e elabore uma rede privada virtual e escreva uma política de segurança para uma empresa.

Para realizá-la é importante seguir os passos descritos.

PASSOS

Passo 1 (Aluno)

Ler atentamente o capítulo do livro texto ou complementar que traz informações referentes a redes privadas virtuais (VPN – *Virtual Private Network*), *firewall* e política de segurança em redes de computadores.

Passo 2 (Equipe)

Acessar e conhecer o *site* da ***Computer Crime Research Center***. Disponível em: <http://www.crime-research.org>.Acesso em:23ago. 2011. Acesse e leia o artigo: *Crimes in cyber space* de Jane Schmitt. O artigo também se encontra disponível em: <https://docs.google.com/leaf?id=0B5zZAtiBwoEXOTJiYTViNTUtNjI4NC00ZWZmLTk4YTUtY2VlZTM5Nzk0OTUw&hl=en>. Acesso em: 23 ago. 2011.

Passo 3 (Equipe)

Elaborar o Relatório 04: Configurações de Segurança do Sistema de Redes de Computadores do Manual. Este relatório deve conter os seguintes tópicos:

4.1 Rede Privada Virtual: utilizando a ferramenta de *software Microsoft Visio*, elaborar um esboço (desenho) para a implantação de uma VPN ou Rede Privada Virtual. Apresentar, além do esboço, os aspectos de segurança do acesso remoto pela VPN.

4.2 Política de Segurança: elaborar um documento com a política de segurança para uma empresa. Utilizar como modelo o Exemplo de Estrutura de Política de Segurança apresentado no livro Segurança de Redes em Ambientes Cooperativos (NAKAMURA, 2007, pag. 216).

4.3Cyber Seguro: elaborar uma resenha (1 página) sobre o artigo *Crimes in cyber space*.

Referências Bibliográficas

NAKAMURA, Emilio T.; GEUS, Paulo L.. ***Segurança de Redes em Ambientes Cooperativos***. 1ª ed. São Paulo: Novatec, 2007, v.1.

Padronização

O material escrito solicitado nesta atividade deve ser produzido de acordo com as normas da ABNT, com o seguinte padrão (exceto para produções finais não textuais):

- em papel branco, formato A4;
- com margens esquerda e superior de 3cm, direita e inferior de 2cm;
- fonte *Times New Roman* tamanho 12, cor preta;
- espaçamento de 1,5 entre linhas;
- se houver citações com mais de três linhas, devem ser em fonte tamanho 10, com um recuo de 4cm da margem esquerda e espaçamento simples entre linhas;
- com capa, contendo:
  - nome de sua Unidade de Ensino, Curso e Disciplina;
  - nome e RA de cada participante;
  - título da atividade;
  - nome do professor da disciplina;
  - cidade e data da entrega, apresentação ou publicação.

Para consulta completa das normas ABNT, acesse a Normalização de Trabalhos Acadêmicos Anhanguera. Disponível em: <http://issuu.com/normalizacao/docs/normaliza__o_para_trabalhos_acad_micos?e=8070144/2211159>. Acesso em: 18 mar. 2014.