PLANO DE ENSINO: Segurança em Rede de Computadores

Carga Horária Total: 66 h

EMENTA

Explora técnicas de detecção e prevenção de intrusão em redes locais ou redes do padrão WAN, com o auxílio de ferramentas e tecnologias de código aberto ou código proprietário. Também aborda os padrões éticos no uso de conhecimentos especializados em segurança, frente a necessidade de se proteger a informação.

COMPETÊNCIAS

I – ANALISAR E RESOLVER PROBLEMAS
XIX - GESTÃO DE REDES DE COMPUTADORES - Gerir redes de computadores e datacenter garantindo o seu funcionamento, controlando o acesso dos usuários e otimizando seus recursos.
XVIII- SEGURANÇA DE REDES DE COMPUTADORES - Projetar, implementar e configurar soluções de segurança em redes.

OBJETIVOS DE APRENDIZAGEM

- Analisar o funcionamento da Segurança da Informação;
- Apontar ameaças que impactam a segurança da informação;
- Classificar ativos de acordo com sua criticidade;
- Aplicar ferramentas de monitoramento, controle e auditoria de sistemas;
- Elaborar um plano de contingência organizacional;
- Implementar ferramentas que proteja a confidencialidade, integridade e disponibilidade;
- Criar uma matriz de risco;
- Avaliar uma matriz de risco.

CRONOGRAMA DE AULA

Unidade 1

1.1 Fundamentos de segurança da informação
- ✓ Princípios da SI
- ✓ Confidencialidade, integridade e disponibilidade

1.2 GERENCIAMENTO DE SEGURANÇA DE TI E AVALIAÇÃO DE RISCOS
- ✓ Políticas de Segurança
- ✓ Análise e avaliação de Riscos de Segurança

1.3 Politica, Controles, Planos e Procedimento de SI
- ✓ Plano de Segurança em TI
- ✓ Implementação de Gerenciamento de SI

1.4 Controle de Acesso
- ✓ Políticas de Autorização e diretrizes de identificação
- ✓ Modelos Formais de Controle de Acesso

Objetivos de Aprendizagem

- ✓ Identificar os princípios da Segurança da Informação.
- ✓ Descrever confidencialidade, integridade e disponibilidade.
- ✓ Aplicar os princípios básicos da Segurança da Informação.
- ✓ Examinar o processo de Gerenciamento de Segurança de TI;
- ✓ Detalhar abordagens alternativas para a avaliação de riscos no contexto de segurança de TI;
- ✓ Caracterizar ameaças e consequências identificadas para determinar riscos;
- ✓ Listar as várias categorias e Tipos de Controles Disponíveis;
- ✓ Descrever um plano de implementação para enfrentar riscos identificados;
- ✓ Aplicar a implementação continuada da segurança;
- ✓ Identificar os principais objetivos do Controle de Acesso.
- ✓ Descrever Controle de Acesso Físico e Lógico.
- ✓ Aplicar os modelos Formais de Controle de Acesso.

Estratégias de Ensino

Utilização de material referencial em diferentes formatos: vídeos, textos de referência conceitual, atividades de pesquisa, estudos de caso, infografias interativas, entre outros.

Sequência sugerida:
- ✓ Explorar a seção "**Inspire-se**" que contextualiza o tema da unidade e traz informações de tendências e inovações na respectiva área de conhecimento, aplicação prática ou estudos de caso, depoimentos ou entrevistas com profissionais qualificados do mercado de trabalho.
- ✓ Conhecer e entender os conceitos básicos da unidade apresentados na seção **"Explore"**. Neste material são apresentados os aspectos teóricos, exemplos práticos e conteúdos complementares que ampliam o conhecimento sobre as temáticas da unidade. Explorar os vídeos e infografias interativas.

	Atividade
	Atividade não pontuada disponível na seção "**Pratique e Compartilhe**". ✓ Estudos de caso, resoluções, proposta de pesquisa ou produção criativa que integram atividades práticas aos conceitos teóricos básicos da unidade. ✓ As respostas e resultados da atividade proposta devem ser postados no fórum disponível na sessão **"Compartilhe"**. ✓ Após a postagem será disponibilizado feedback com modelo de resposta).
	Avaliação Formativa
	Realizar a "Atividade Avaliativa" que constitui o recurso de avaliação pontuada da unidade. A pontuação desta atividade fará parte da nota final na N1 (ver item "Avaliação" deste plano").
Unidade 2 2.1 Operações e administração de Segurança ✓ Conformidade e Classificação de Dados Gerenciamento de mudança 2.2 Auditoria, Testes e Monitoramento ✓ Análise de Segurança ✓ Monitoramento e testes de Sistemas de Segurança 2.3 Software Malicioso ✓ Ataques, ameaças e Vulnerabilidades ✓ Engenharia Social 2.4 Criptografia e Algoritmos criptográficos ✓ Padrões de Cifração de Dados ✓ Funções Hash seguras	**Objetivos de Aprendizagem**
	✓ Definir conformidade em Segurança da Informação; ✓ Demonstrar como é feito o professo de classificação de dados; ✓ Avaliar o gerenciamento de mudanças; ✓ Definir Auditoria, Testes e Monitoramento em Segurança da Informação; ✓ Demonstrar como é feito o monitoramento e análise de Segurança; ✓ Formular testes de Sistemas de Segurança; ✓ Descrever os mecanismos que os malwares usam para se propagar; ✓ Demonstrar funcionamento e categorias de ameaças (Phinshing, bots, spyware, rootkits e Ransomware); ✓ Investigar elementos usados na Engenharia Social; ✓ Explicar os princípios básicos de Criptografia; ✓ Descrever a estrutura e a função do DES e AES ; ✓ Apreciar Funções de Hash e algoritmos RSA e Diffie -Hellaman;
	Estratégias de Ensino
	Utilização de material referencial em diferentes formatos: vídeos, textos de referência conceitual, atividades de pesquisa, estudos de caso, infografias interativas, entre outros. Sequência sugerida: ✓ Explorar a seção "**Inspire-se**" que contextualiza o tema da unidade e traz informações de tendências e inovações na respectiva área de conhecimento, aplicação prática ou estudos de caso, depoimentos ou entrevistas com profissionais qualificados do mercado de trabalho. ✓ Conhecer e entender os conceitos básicos da unidade apresentados na seção **"Explore"**. Neste material são apresentados os aspectos teóricos, exemplos práticos e conteúdos complementares que ampliam o conhecimento sobre as temáticas da unidade. Explorar os vídeos e infografias interativas.
	Atividade
	Atividade não pontuada disponível na seção "**Pratique e Compartilhe**". ✓ Estudos de caso, resoluções, proposta de pesquisa ou produção criativa que integram atividades práticas aos conceitos teóricos básicos da unidade. ✓ As respostas e resultados da atividade proposta devem ser postados no fórum disponível na sessão **"Compartilhe"**. ✓ Após a postagem será disponibilizado feedback com modelo de resposta.
	Avaliação Formativa
	Realizar a "Atividade Avaliativa" que constitui o recurso de avaliação pontuada da unidade. A pontuação desta atividade fará parte da nota final na N1 (ver item "Avaliação" deste plano").
Unidade 3 3.1 Controle de acesso à rede e segurança na nuvem	**Objetivos de Aprendizagem**
	✓ Apresentar uma visão geral dos elementos de Controle de acesso à rede;

<table>
<tr>
<td>
✓ Controle de acesso à rede
✓ Segurança relacionada a computação em nuvem
3.2 Segurança na camada de transporte
✓ Considerações de segurança na web
✓ SECURE SHELL
3.2 Segurança IP
✓ Política de segurança IP
✓ Encapsulando o payload de segurança
3.3 Protocolos de Autenticação na internet (das coisas)
✓ Sockets
✓ Segurança no IPV6 e IPV4
</td>
<td>
✓ Comparar diferentes abordagens, riscos e contramedidas de segurança na nuvem;
✓ Avaliar questões de segurança relacionada a computação em nuvem;
✓ Apresentar uma visão geral do Secure Shell (SSH).;
✓ Resumir as ameaças à segurança da rede e os métodos de segurança do tráfego na Web.;
✓ Avaliar medidas necessárias para manter a segurança na camada de transporte;
✓ Apresentar uma visão geral da segurança IP (IPsec);
✓ Explicar a diferença entre o modo de transporte e o modo túnel;
✓ Explicar a diferença entre o banco de dados de associação de segurança e o banco de dados de política de segurança.;
✓ Apresentar uma visão geral dos elementos de segurança SSL e TLS;
✓ Comparara segurança no IPV6 e IPV4;
✓ Avaliar questões de segurança relacionada a conexão HTTPS;

Estratégias de Ensino

Utilização de material referencial em diferentes formatos: vídeos, textos de referência conceitual, atividades de pesquisa, estudos de caso, infografias interativas, entre outros.

Sequência sugerida:
✓ Explorar a seção “Inspire-se” que contextualiza o tema da unidade e traz informações de tendências e inovações na respectiva área de conhecimento, aplicação prática ou estudos de caso, depoimentos ou entrevistas com profissionais qualificados do mercado de trabalho.
✓ Conhecer e entender os conceitos básicos da unidade apresentados na seção “Explore”. Neste material são apresentados os aspectos teóricos, exemplos práticos e conteúdos complementares que ampliam o conhecimento sobre as temáticas da unidade. Explorar os vídeos e infografias interativas.

Atividade

Atividade não pontuada disponível na seção “Pratique e Compartilhe”.
✓ Estudos de caso, resoluções, proposta de pesquisa ou produção criativa que integram atividades práticas aos conceitos teóricos básicos da unidade.
✓ As respostas e resultados da atividade proposta devem ser postados no fórum disponível na sessão “Compartilhe”.
✓ Após a postagem será disponibilizado feedback com modelo de resposta.

Avaliação Formativa

Realizar a “Atividade Avaliativa” que constitui o recurso de avaliação pontuada da unidade. A pontuação desta atividade fará parte da nota final na N1 (ver item “Avaliação” deste plano”)
</td>
</tr>
<tr>
<td>
Unidade 4

4.1 Segurança em Redes Sem Fio
✓ Componentes e arquitetura
4.2 Código e atividade maliciosa
✓ Técnicas de Prevenção de Ataques
✓ Técnicas de Detecção de Ataques
4.3 Aspectos Legais e éticos da SI
</td>
<td>
Objetivos de Aprendizagem

✓ Definir os tipos de ameaças relevantes no contexto das redes sem fio e citar contramedidas;
✓ Analisar os elementos essenciais do padrão LAN sem fio IEEE 802.11;
✓ Avaliar os vários componentes da Arquitetura da Segurança da LAN sem fio;
✓ Definir o que é uma atividade Maliciosa;
✓ Demonstrar como feira a prevenção de um ataque;
✓ Formular como feira a detecção de um ataque;
✓ Discutir uma visão geral dos diferentes tipos de cyber crimes e crimes de computador;
✓ Comparar os tipos de propriedades intelectual;
✓ Avaliar questões éticas do Profissional Security Office;
</td>
</tr>
</table>

<table>
<tr>
<td>✓ Cyber Crime e Crime de Computador
✓ Privacidade e questões Éticas
4.4 Educação e Certificação em Segurança da Informação
✓ Treinamentos em SI
✓ Formação e certificações em SI</td>
<td>✓ Discutir uma visão geral dos diferentes tipos de treinamentos em Segurança da Informação;
✓ Comparar os programas de educação continuada em Segurança da Informação;
✓ Avaliar as certificações profissionais e Profissional Security Office;

Estratégias de Ensino

Utilização de material referencial em diferentes formatos: vídeos, textos de referência conceitual, atividades de pesquisa, estudos de caso, infografias interativas, entre outros.

Sequência sugerida:
✓ Explorar a seção “Inspire-se” que contextualiza o tema da unidade e traz informações de tendências e inovações na respectiva área de conhecimento, aplicação prática ou estudos de caso, depoimentos ou entrevistas com profissionais qualificados do mercado de trabalho.
✓ Conhecer e entender os conceitos básicos da unidade apresentados na seção “Explore”. Neste material são apresentados os aspectos teóricos, exemplos práticos e conteúdos complementares que ampliam o conhecimento sobre as temáticas da unidade. Explorar os vídeos e infografias interativas.

Atividade

Atividade não pontuada disponível na seção “Pratique e Compartilhe”.
✓ Estudos de caso, resoluções, proposta de pesquisa ou produção criativa que integram atividades práticas aos conceitos teóricos básicos da unidade.
✓ As respostas e resultados da atividade proposta devem ser postados no fórum disponível na sessão “Compartilhe”.
✓ Após a postagem será disponibilizado feedback com modelo de resposta.

Avaliação Formativa

Realizar a “Atividade Avaliativa” que constitui o recurso de avaliação pontuada da unidade. A pontuação desta atividade fará parte da nota final na N1 (ver item “Avaliação” deste plano”).</td>
</tr>
<tr>
<td>N2 - Prova Presencial</td>
<td>Avaliação em formato de prova presencial constituída de atividades múltipla escolha contemplando as quatro unidades da disciplina (ver item “Avaliação” deste plano”).</td>
</tr>
</table>

AVALIAÇÃO

A Nota Final (NF) da disciplina considera os seguintes elementos e valores:

NOTA N1				NOTA N2
UNIDADE 1	**UNIDADE 2**	**UNIDADE 3**	**UNIDADE 4**	**PROVA PRESENCIAL A5**
Atividade Avaliativa A1 Avaliação Individual com nota de 0 a 10	Atividade Avaliativa A2 Avaliação Individual com nota de 0 a 10	Atividade Avaliativa A3 Avaliação Individual com nota de 0 a 10	Atividade Avaliativa A4 Avaliação Individual com nota de 0 a 10	Contendo Questões Objetivas e/ou Dissertativas, individual.

Média Final (MF) é calculada com a seguinte média ponderada das duas notas, N1 e N2 e pesos, respectivamente, de 40% e 60%, resultante da seguinte equação:

$$MF = (N1*0,4) + (N2*0,6)$$

Para aprovação, a Nota Final da disciplina deverá ser igual ou superior a 6,0 (seis), além da necessária frequência mínima de 75%, que corresponde a realização de, no mínimo, três das quatro Atividades Avaliativas da N1

O estudante que não atingir a média final 6,0 (seis), poderá realizar uma Prova Substitutiva (A6), cuja nota substituirá a nota da N2 (A5) obtida, caso seja maior.

BIBLIOGRAFIA BÁSICA

KOLBE JÚNIOR, Armando. Sistemas de segurança da informação na era do conhecimento.Editora Intersaberes. ISBN: 9788559723038 [Biblioteca Virtual]
Galvão, Michele da Costa. Fundamentos em Segurança da Informação. Pearson. ISBN: 9788543009452. [Biblioteca Virtual]
William Stallings. Criptografia e segurança de redes: princípios e práticas – 4. ed. – São Paulo: Pearson Education do Brasil, 2015. ISBN: 9788576051190 [Biblioteca Virtual]

BIBLIOGRAFIA COMPLEMENTAR

Ford, Jerry Lee. Manual Completo de Firewalls Pessoais: tudo o que você precisa saber para proteger o seu computador. Pearson ISBN: 9788534614641 [Biblioteca Virtual]
Kurose, James F.; Ross, Keith W. Redes de Computadores e a Internet: uma abordagem top-down - 3ª edição. Pearson. ISBN: 9788588639188. [Biblioteca Virtual]
Tanenbaum, Andrew S. Sistemas Operacionais Modernos - 2ª edição. Pearson. ISBN: 9788587918574. [Biblioteca Virtual]
Nemeth, Evi; Snyder, Garth; Hein, Trent R. Manual Completo do Linux: guia do administrador. Pearson. ISBN: 9788534614863. [Biblioteca Virtual]