Título: SIC-063 - Segurança em Infraestrutura Computacional

Ativa: Sim

Carga Horária: 52 **Crédito:** 5

Responsável: Anderson Aparecido Alves da Silva

Observações:

Objetivo: Propiciar ao aluno capacitação acadêmica, técnica e profissional de segurança da informação que são aplicáveis em ambientes de infraestrutura computacional no que se refere à: detecção, prevenção e previsão de intrusão; proteção de perímetro em redes de computadores; gestão de identidades e acesso em ambientes distribuídos, de computação móvel e de computação em nuvem.

Justificativa: Devido ao novo contexto das tecnologias de rede, tornou-se necessário adequar o conteúdo acadêmico e técnico desta disciplina com tópicos de interesse mais alinhados ao mercado profissional que atendam profissionais de nível senior ou com responsabilidades gerenciais e estratégicas. Considerando a infraestrutura computacional de redes, esta adequação ainda é mais crítica pelo fato de que dados precisam continuar sendo manipulados em ambientes organizacionais de forma segura por todas estas inovações hoje existentes nas redes de computadores: nuvem, mobilidade, BYOD, novas aplicações, taxas de transmissão maiores, novos protocolos, novos mecanismos de segurança, novos serviços, ambientes virtuais, processamento centralizado etc.
Concomitantemente às novidades e com o tempo, outros artefatos maliciosos causam ameaças e vulnerabilidades que aumentam os riscos da infraestrutura computacional que hoje, pensada de uma maneira centralizada, necessita estar organizada como um centro de defesa cibernética adequado para a proteção e para gerar respostas que sejam eficientes e precisas no diagnóstico de uma rede e suas novas funcionalidades, sendo isso de fundamental importância nas tomadas de decisões relativas aos ativos de informação.
Para se adaptar a todo este contexto, gerando pesquisas acadêmicas e tecnológicas, novos dispositivos e aplicações, esta disciplina evolui para tratar em seu escopo a segurança da informação aplicada em infraestrutura computacional por meio da proteção de perímetro, detecção de intrusão, mobilidade segura e mecanismos de segurança em que atuem nos níveis operacional, estratégico e de tomada de decisão.

Ementa: Introdução ao TCP/IP para detecção de intrusão em redes de computadores; Comportamentos normais e anômalos dos protocolos TCP/IP (captura e observação de pacotes, spoofing e fragmentação); Modelo requisição/resposta para análise de detecção de intrusão (ICMP, UDP e TCP); Varreduras; Negação de serviço (DoS e DDoS); Sistemas de detecção de intrusão (Intrusion Detection Systems - IDS / NIDS e HIDS); Introdução aos sistemas de proteção de perímetro; Topologias e tecnologias de firewall; Segurança e privacidade em computação móvel e computação em nuvem; Riscos e ameaças; Introdução ao BYOD (Bring Your Own Device).

Forma de Avaliação: Formas de avaliação possíveis: prova escrita e elaboração de artigo técnico.

Material Utilizado:

Metodologia:

Conhecimentos Prévio:

Bibliografia Básica:

NORTHCUTT, S.; NOVAK, J.. **Network Intrusion Detection**. Third edition, ISBN-10: 0735712654, ISBN-13: 978-0735712652, New Riders, 2002.
NORTHCUTT, S.; ZELTSER, L.; WINTERS, S.; KENT, K.; and RITCHEY, R. W. **Inside Network Perimeter Security**. Second edition, ISBN-10: 0672327376, ISBN-13: 978-0672327377, 2005.
Pathan, A. K. **The State of the Art in Intrusion Prevention and Detection**. ISBN-10: 1482203510, ISBN-13: 978-1482203516, 2014.
SCARFONE, K.; SOUPPAYA, M. **NIST Special Publication 800-153 - Guidelines for Securing Wireless Local Area Networks (WLANs).** Computer Security Division, Information Technology Laboratory, NIST, MD, USA, 2012, p. 24.
JANSEN, W.; GRANCE, T. **NIST Special Publication 800-144 - Guidelines on Security and Privacy in Public Cloud Computing.** Computer Security Division, Information Technology Laboratory, NIST, MD, USA, 2011, p. 80.
MELL, P.; KENT, K.; NUSBAUM, J. **NIST Special Publication 800-83 - Guide to Malware Incident Prevention and Handling.** Computer Security Division, Information Technology Laboratory, NIST, MD, USA, 2005, p. 110.
SCARFONE, K.; MELL, P. **NIST Special Publication 800-94 - Guide to Intrusion Detection and Prevention Systems (IDPS).** Computer Security Division, Information Technology Laboratory, NIST, MD, USA, 2007, p. 127.
Mather, T.; Kumaraswamy, S.; and Latif, S. **Cloud Security and Privacy: An Enterprise Perspective on Risks and Compliance (Theory in Practice).** First Edition, ISBN-10: 0596802765, ISBN-13: 978-0596802769, O""Reilly Media, 2009.
Winkler, V. (J.R.). **Securing the Cloud: Cloud Computer Security Techniques and Tactics.** First Edition,
ISBN-10: 1597495921, ISBN-13: 978-1597495929, Syngress, 2011.
Madden, J. **Enterprise Mobility Management: Everything you need to know about MDM, MAM, and BYOD**. 2014 Edition, Jack Madden, 2013.
http://www.netfilter.org
http://www.snort.org
Material de aula disponível e indicado pelo professor

Bibliografia Complementar:

Programa da Oferecimento:

AULA 1º Introdução ao TCP/IP para detecção de intrusão em redes de computadores;
AULA 2º Comportamentos normais e anômalos dos protocolos TCP/IP (fragmentação e sniffing).
AULA 3º Modelo requisição/resposta para análise de detecção de intrusão (ICMP, UDP TCP, UDP).
AULA 4º Modelo requisição/resposta para análise de detecção de intrusão (TCP); DoS e DDoS.
AULA 5º Varredura e Spoofing.
AULA 6º Sistemas de detecção de intrusão (Intrusion Detection Systems - IDS / NIDS e HIDS).
AULA 7º Avaliação 1.
AULA 8º IDS e Introdução aos sistemas de proteção de perímetro.
AULA 9º Topologias e tecnologias de firewall.
AULA 10º Topologias e tecnologias de firewall; Segurança e privacidade em computação móvel e computação em nuvem.
AULA 11º Segurança e privacidade em computação móvel e computação em nuvem.
AULA 12º Riscos e ameaças; Introdução ao BYOD (Bring Your Own Device).
AULA 13º - Avaliação Final – Apresentação de artigo técnico.