Título: SEG-017 - Segurança de Sistemas

Ativa: Sim

Carga Horária: 60 **Crédito:** 6

Responsável: Anderson Aparecido Alves da Silva

Observações:

Objetivo: Apresentar, de forma abrangente, conhecimentos acadêmicos e técnicos de segurança da informação e cibersegurança, com foco tanto na área de redes quanto na de software.

Justificativa: Infraestrutura de rede: 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). Sistemas: requisitos básicos de segurança em sistemas de informação, ameaças e ataques de segurança, segurança lógica e física. Gerenciamento e análise de risco Auditoria e vulnerabilidades em softwares maliciosos, noções de programação segura e segurança Web.

Ementa: Infraestrutura de rede: 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). Sistemas: requisitos básicos de segurança em sistemas de informação, ameaças e ataques de segurança, segurança lógica e física. Gerenciamento e análise de risco Auditoria e vulnerabilidades em softwares maliciosos, noções de programação segura e segurança Web.

Forma de Avaliação: 30% (Trabalho) + 35% (1ª Prova/Avaliação individual) + 35% (2ª Prova/Avaliação individual)

Material Utilizado: Slides para apresentação e discussão do conteúdo teórico, e ferramentas computacionais para desenvolvimento de atividades práticas, sala de aula com quadro branco e projetor, laboratório de informática e ambiente Moodle.

Metodologia: Aulas teóricas expositivas acompanhadas de atividades práticas.

Conhecimentos Prévio: Conhecimentos equivalentes a disciplina Redes de Computadores (REC-013), e lógica de programação de computadores.

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.

Bibliografia Complementar:

STALLINGS, W.; BROWN, L. Computer Security: Principles and Practice. 2nd Edition. Pearson Education: Prentice Hall, 2011. GOODRICH, M.; TAMASSIA, R. Introduction to Computer Security. 1st Edition. Pearson Education: Addison-Wesley, 2011. BENANTAR, Messaoud. Access Control Systems: Security, Identity Management and Trust Models. Springer. 2006. HOWARD, Michael; LEBLANC, David. Escrevendo Código Seguro: Estratégias e Técnicas Práticas Para Codificação Segura de Aplicativos em um Mundo de Rede. 2a Edição. Artmed. 2005. HOGLUND, Greg; MCGRAW, Gary. Como Quebrar Códigos: A Arte de Explorar (e Proteger) Software. Makron Books. 2005.

Programa da Oferecimento: 15 aulas

Aula 1: Conceitos fundamentais de segurança da informação e cibersegurança
Aula 2: Normas e padrões de segurança, NBR ISO 27001 e NBR ISO 27002
Aula 3: Sistemas criptográficos – Algoritmos e protocolos
Aula 4: Mecanismos de autenticação em sistemas
Aula 5: Mecanismos de autorização – DAC, MAC e RBAC
Aula 6: Comunicação segura – Principais protocolos de segurança (TLS/SSL, IPSec)
Aula 7: 1ª Prova/Avaliação individual
Aula 8: Análise de tráfego, scan de vulnerabilidades e ataques (Spoofing, DoS e DDoS)
Aula 9: Sistemas de detecção e prevenção de intrusão – IDS e IPS (Snort)
Aula 10: Sistemas de firewalls e proteção de perímetro
Aula 11: Programação segura – Buffer overflow
Aula 12: Softwares maliciosos (malwares) e segurança de aplicações web
Aula 13: Mecanismos de segurança em computação em nuvem
Aula 14: Apresentação de trabalho
Aula 15: 2ª Prova/Avaliação individual