|  |  |
| --- | --- |
| **ELEMENT** | **CONTENT** |
| DEPARTMENT | CIS |
| AUTHOR (S) | Jack Skoda |
| COURSE NUMBER | **CIS 4040** |
| COURSE TITLE | **Computer Security** |
| SHORT TITLE | Comp Security |
| COURSE LEVEL | 4000 |
| DATE CREATED |  |
| CHECKED/CHANGED | 2/10/2017 |
| PREREQUISITES | CIS 2151, 2230; C- or better in CIS 2025 or 2262 or 2271 |
| COREQUISITES |  |
| RESTRICTIONS |  |
| SPECIAL FEES | No |
| CREDITS | 3 |
| HOURS | 3 hours of lecture per week |
| SEMESTER | Fall |
| COURSE DESCRIPTION | This course focuses on security issues associated with computers and computer networks and begins by covering cryptographic topics such as symmetric and public key cryptography, digital signatures, secure hashes, random number generation, and message authentication codes. Network security topics are also covered including secure protocols (SSL/TLS, IPsec), network attack methods, network authentication protocols (Kerberos), and firewalls. Finally, the course covers host security matters such as building secure software, auditing, and intrusion detection. |
| SUGGESTED TEXTS | *Essential Cybersecurity Science*; Josiah Dykstra |
| OPTIONAL TEXTS |  |
| COURSE OUTCOMES | The successful student will be able to:   1. Understand cryptographic technology well enough to recommend appropriate use of the technology and to deploy the technology both in the context of system administration and software development. 2. Appreciate the mathematical basis of encryption technology without the need to formally verify the strength or correctness of cryptographic algorithms 3. Understand the details of at least one security protocol and implement at least some aspects of it at either the administrative or software developmental capacity 4. Describe how various network related attacks are performed as well as appropriate counter measures 5. Explain situational awareness challenges related to processing security log information 6. Explain the purpose and limitations of firewalls 7. Explain the Kerberos authentication protocol 8. Use appropriate methods to build secure software that avoid buffer overflows 9. Use language security features 10. Interact with security support libraries 11. Explain the role of intrusion detection (at both the network and host levels), auditing, and similar technologies 12. Explain various methods for analyzing potentially malicious software 13. Interact with other administrators to evaluate security risks, potential attacks, and appropriate countermeasures |
| COURSE CONTENT | 1. Block encryption algorithms: DES and AES 2. Encryption modes and cryptographic random number generation 3. Public key encryption systems 4. Secure hashes 5. Security protocols 6. Network attack methods and countermeasures 7. Firewalls 8. Kerberos authentication protocol 9. Building secure software    1. Buffer overflows    2. Language specific security features    3. Interacting with security libraries 10. Host security mechanisms 11. Capabilities     1. Access control lists     2. Discretionary access control     3. Mandatory access control 12. Malware analysis 13. Security policy and risk assessment |
| LAB/STUDIO OUTCOMES |  |
| LAB/STUDIO CONTENT |  |
| LECTURE CAPACITY | 32 |
| LAB CAPACITY |  |
| GRADED OR P/NP | Graded |
| EVALUATION | Participation, quizzes, exams, homework |
| DELIVERY METHOD | LEC or HYB |
| ROOM REQUIREMENTS |  |
| AUTHOR’S NOTES |  |