COMPUTER INFORMATION SYSTEMS: SECURITY (CISS)

CISS 11 Practical Computer Security
2 Units (Degree Applicable)
Lecture: 27 Lab: 27
Advisory: *CISB 11*

Computer security for all computer users. Provides awareness for computer users to protect user accounts and computer systems from attacks. Projects illustrate security software and hardware configuration.

CISS 13 Principles of Information Systems Security
4 Units (Degree Applicable)
Lecture: 72
Advisory: *CISB 11 and CISS 11*

Systems Security Certified Practitioner (SSCP) course preparation including practical technical skills for operational information technology (IT) roles.

CISS 15 Operating Systems Security
3 Units (Degree Applicable)
Lecture: 54
Advisory: *CISB 11 or CISN 21*

Operating systems security concepts and techniques: covers how attackers operate, how viruses strike, strengthening operating systems, repelling attacks, and applying security techniques to different operating systems like Windows, Unix, Linux, etc.

CISS 21 Network Vulnerabilities and Countermeasures
3 Units (Degree Applicable, CSU)
Lecture: 54
Corequisite: *CISS 21L*
Advisory: *CISN 11*

Network vulnerabilities from a hacker's perspective. Cyber security legal and ethical issues. Written security, use policy, and instance response policy. Scanning and penetration tests, vulnerability assessments, and countermeasures for Windows and Linux operating systems. Secure programming, virtual private network (VPN), cryptography, wireless, Web, and remote access securities. Student must be enrolled in CISS 21L, a concurrent lab co-requisite.

CISS 21L Network Vulnerabilities and Countermeasures Laboratory
0.5 Units (Degree Applicable, CSU)
Lab: 27
Corequisite: *CISS 21*

Laboratory for network vulnerabilities from a hacker's perspective. Cyber security legal and ethical issues. Written security, use policy, and instance response policy. Scanning and penetration tests, vulnerability assessments and countermeasures for Windows and Linux operating systems. Secure programming, virtual private network (VPN), cryptography, wireless, Web, and remote access securities. Student must be enrolled in CISS 21, a concurrent lecture co-requisite.

CISS 23 Cyber, Cloud Network Intrusion Detection/Prevention Systems (IDS/IPS)
3 Units (Degree Applicable, CSU)
Lecture: 54
Corequisite: *CISS 23L*
Advisory: *CISN 11*

Computer forensic, Penetration (PEN) testing, and packet crafting tools to monitor, troubleshoot, identify threads and traffic from Cyber, Cloud, and local networks. Configure, deploy, detect, and block attacks using Cisco Adaptive Security Appliance IDS/IPS, Windows Snort IDS/IPS, and open-source IDS/IPS including Linux Snort, OSSEC, and Security Onion (Snort/Suricata). Student must be enrolled in CISS 23L, a concurrent lab co-requisite.

CISS 23L Cyber, Cloud Network Intrusion Detection/Prevention Systems (IDS/IPS) Laboratory
0.5 Units (Degree Applicable, CSU)
Lab: 27
Corequisite: *CISS 23*

Laboratory course for computer forensic, Penetration (PEN) testing, and packet crafting tools to monitor, troubleshoot, identify threads and traffic from Cyber, Cloud, and local networks. Configure, deploy, detect, and block attacks using Cisco Adaptive Security Appliance IDS/IPS, Windows Snort IDS/IPS, and open-source IDS/IPS including Linux Snort, OSSEC, and Security Onion (Snort/Suricata). Student must be enrolled in CISS 23, a concurrent lecture co-requisite.

CISS 25 Cyber, Cloud Network Security and Firewalls
3 Units (Degree Applicable, CSU)
Lecture: 54
Corequisite: *CISS 25L*
Advisory: *CISN 11*

Design, configure, deploy, and maintain Cisco Adaptive Security Appliance (ASA), Windows, and Linux firewalls to secure Cyber, Cloud, and local networks. Topics include IPsec and TLS Virtual Private Network (VPN) remote clients, Access Control Lists (ACL), Confidentiality Integrity Availability (CIA), Radius, and Certificate Authentication (CA). Student must enroll in CISS 25L concurrently.

CISS 25L Cyber, Cloud Network Security and Firewalls Laboratory
0.5 Units (Degree Applicable, CSU)
Lab: 27
Corequisite: *CISS 25*

Laboratory course to design, configure, deploy, and maintain Cisco Adaptive Security Appliance (ASA), Windows, and Linux firewalls to secure Cyber, Cloud, and local networks. Topics include IPsec and TLS Virtual Private Network (VPN) remote clients, Access Control Lists (ACL), Confidentiality Integrity Availability (CIA), Radius, and Certificate Authentication (CA). Student must enroll in CISS 25L concurrently.

CISS 27 Cyber Defense
1 Unit (Degree Applicable)
Lab: 54
Advisory: *CISN 11 and CISN 11L*

Cyber security hands-on activities in defending, responding, mitigating, and analyzing attacks through IT infrastructure and application service vulnerabilities. Prepare students to secure, configure, monitor, and analyze computer, switch, router, firewall, Intrusion Prevention Systems (IPS), Voice over IP (VoIP), smart phone, and application services such as Web, email, Structured Query Language (SQL) database, Domain Name Systems (DNS), and Virtual Private Network (VPN).

CISS 29 CNASM Service Learning
1 Unit (Degree Applicable, CSU)
(May be taken for option of letter grade or Pass/No Pass)
Lab: 54

Explore career objectives and advanced skills from Computer Network Administration and Security Management (CNASM) courses through lab activities and community services.

CISS 81 Work Experience in Computer Security
1-4 Units (Degree Applicable)
(May be taken for Pass/No Pass only)
Lab: 60-300
Prerequisite: *Compliance with Work Experience regulations as designated in the College Catalog.*

Provides students with actual on-the-job experience in computer security at an approved work site, which is related to classroom based learning. A minimum of 75 paid clock hours or 60 non-paid clock hours per semester of supervised work is required for each one unit of credit. It is recommended that the hours per week be equally distributed throughout the semester. Work experience placement is not guaranteed, but assistance is provided.