

ITSY 2400 – Operating System Security (4:3-2)

Collins, Spring 2007

Informal Description: The world today is relies heavily on computers. This course introduces students to protecting computers & networks using operating system software tools and utilities.

Textbooks/Reference/Materials

- Guide to Operating Systems Security , Michael Palmer, ISBN 0-619-16040-3
- Access to <http://www.templejc.edu/dept/cis/CCollins/Collins.htm>
- Floppy disks or other file storage (home computer, removable USB drive, etc.)

Course Competencies

CIP Code: 11.0901 (Computer Systems Networking and Telecommunications)

Course Title: Operating System Security

Course Level: Intermediate

Course Description: Safeguard computer operating systems by demonstrating server support skills and designing and implementing a security system. Identify security threats and monitor network security implementations. Use best practices to configure OS to industry security standards.

Learning Outcomes: Discover network security risks, proper security design, and monitoring solutions; identify sources of computer threats, evaluate potential practices, tools, and technologies to protect individual network systems; establish and sustain an operating system security plan utilizing systems and application security tools; implement procedures to secure and monitor audit logs and set system administrator alerts; and develop an organizational operating system security plan that provides for periodic reviews of security policies, procedures, authorized users list, and software update patches.

Suggested Prerequisite: ITSY 1x42

COURSE CALENDAR

6 Week Semester	16 Week Semester	Notes	Lecture Topics	Labs
Week 1	Week 1		Syllabus/Orientation	
	Week 2		Chapter 1: OS Security	Lab 1 due
	Week 3		Chapter 2: Malicious Software	Lab 2 due
Week 2	Week 4		Chapter 3: Authentication	
	Week 5	Review	Catch Up	Lab 3 due
	Week 6	Test 1	Chapter 4: Account Based Security	Lab 4 due
Week 3	Week 7		Chapter 5: Resource Security	Lab 5 due
	Week 8		Chapter 6: Firewalls	Lab 6 due
	Week 9	Review	Chapter 7: Physical Security	
Week 4	Week 10	Test 2	Chapter 8: Wireless Security	
	Week 11		Chapter 9: Remote Access	Lab 7 due
	Week 12		Chapter 10: Email	Lab 8 due
Week 5	Week 13		Chapter 11: Disaster Recovery	
	Week 14	Review	Chapter 12: Monitoring	Lab 9 due
	Week 15	Test 3		Capstone Lab 10 due
Week 6	Week 16	Final		

See course website for current semester's calendar, and holidays

Notes:

ITSY 2400, Continued: COURSE COMPETENCIES

1. *evaluate* network security risks
 - a. *illustrate what OS security means*
 - b. *demonstrate why security is necessary*
 - c. *assess cost factors*
 - d. *evaluate system hardening*
 - e. identify sources of computer threats
 - i. *diagram how virus and worms spread*
 - ii. *discover other malicious software*
 - iii. *apply recovery tools after the fact*
2. *design* proper security design
 - a. establish/sustain an operating system security plan utilizing systems & application security tools
 - i. *examine encryption*
 - ii. *apply authentication*
 - iii. *configure IP security*
 - iv. *develop account security*
 1. *configure account/log on policies*
 2. *implement global access privileges*
 - v. *design group policies*
 1. *Implement directory, folder, and file security*
 - vi. *Configure shared resources*
 - vii. *Apply groups security*
 - viii. *Troubleshoot*
 - ix. *Implement border security on TCP, UDP, and IP*
 1. *Configure firewall*
 - x. *diagram physical security*
 1. *implement network topology solutions*
 2. *use structured network design*
 - xi. *configure wireless security*
 1. *explain 802.11 and Bluetooth weaknesses*
 2. *discuss wireless security measures*
 - xii. *discover Internet security*
 1. *browser security*
 2. *remote access*
 3. *VPN*
 - xiii. *Configure email tools*
 1. *SMTP*
 2. *certificates and encryption*
 - xiv. *originate Disaster recovery*
 1. *manage UPS*
 2. *implement redundancy and fault tolerant*
 - a. *configure RAID*
 3. *create Backups*
 - b. develop an organizational operating system security plan that provides for periodic reviews of security policies, procedures, authorized users list, and software update patches
3. monitor solutions
 - a. evaluate potential practices, tools, and technologies to protect individual network systems
 - i. *choose appropriate intrusion detection*
 - b. implement procedures to secure and monitor audit logs and set system administrator alerts
 - i. *inventory audit trails*
 - ii. *investigate log users*
 - iii. *monitor network*