| Program Name: AAS Cyber Security | Outcomes | IST 108 Microsoft Windows | IST 109 UNIX Operating System | IST 154 Networking Basics | IST 155 Networking I | IST 156 Networking II |
|---|---|---|---|---|---|---|
| **Outcome #1** | Think critically | Implement a functional Windows XP workstation operating environment<br>Improve performance, add features and increase security | Demonstrate effective system administration techniques | Score a passing grade on a simulated Network+ exam by CompTIA | Sucessfully pass Cisco I exam by Cisco | Successfully pass practical lab exam<br>Successfully pass Cisco II exam by Cisco |
| **Outcome #2** | Communicate effectively with both verbal and written forms | Prevent data loss and facilitate security through use of backups, firewalls, antivirus protection | Write efficient, effective scripts and documentation | Submit lab reports in standard format in Blackboard | | |
| **Outcome #3** | Perform and share cooperatively in teams or groups | | Demonstrate effective system administration techniques | Work in teams of 2 for lab assignments | | |
| **Outcome #4** | Review and practice computer and network etiquette and ethics found in working environments | | Demonstrate effective system administration techniques | Practice network etiquette during lab exercises | | |
| **Outcome #5** | Administer and troubleshoot a network infrastructure | Perform basic Windows XP diagnostics using tools and utilities. | | Administer a windows network environment including users and group management.<br>Solve problems in a network enviornment including cabling and nic cards | Install and maintain router configuration environment.<br>Troubleshoot cabling problems within a network. | Install and maintain router configuration environment.<br>Troubleshoot routing problems within a network. |
| **Outcome #6** | Evaluate best practices in security concepts to maintain confidentiality, integrity and availability of computer systems | Practice good file management and disk organization .<br>Demonstrate a working knowledge of the Command line and the Registry<br>Prevent data loss and facilitate security through use of backups, firewalls, antivirus protection. | Choose appropriate UNIX operating system commands to make effective use of the environment to solve problems | Discuss importance of firewalls within a networked environment.<br>Solve problems involving subnets. | | Incorporate new router threories into routers. |

| Program Name: AAS Cyber Security | Outcomes | IST 160 Fundamentals of Security | CYB 210 Ethics in the Information Age | CYB 225 Tactical Perimeter Defense | CYB 240 Ethical Hacking Fundamentals | CYB 245 Introduction to Penetration Testing | IST 261 MCSA/E: Windows Server |
|---|---|---|---|---|---|---|---|
| **Outcome #1** | Think critically | Score a passing grade on a simulated Security+ exam by CompTIA | Read the Association Information Technology Professionals Code of Ethics and Standard of Conduct. Write a paper indicating how the student exemplifies the points within the Code of Ethics | Given a scenario of a network system identify vulnerabilities and recommend mitigating these vulnerabilities. | In closed network environment or virtual network environment employ various reconnaissance, scanning, and enumeration techniques to obtain information regarding a target network system. | Individually and on a team defend and maintain a typical network environment (closed) that is under hacker attack<br><br>Successfully find vulnerabilities in and compromise a simulated network system in a closed environment | Score a passing grade on a simulated Windows Server exam by Microsoft |
| **Outcome #2** | Communicate effectively with both verbal and written forms | Submit lab reports in standard format in Blackboard | Select from a list of Case Studies, research scenario and answer discussion questions regarding the case. Present case and findings to class. | | | | |
| **Outcome #3** | Perform and share cooperatively in teams or groups | | As a member of a team select from a list of Case Studies, research scenario and answer discussion questions regarding the case. Present case and findings to class. | As part of a group create a virtual network with servers, firewalls, VPNs and intrusion detection devices. | Work as part of a team to scan a closed network to determine vulnerabilities of the system. | As a member of a team defend a closed network environemnt against attack | |
| **Outcome #4** | Review and practice computer and network etiquette and ethics found in working environments | | Participate in class discussion/debates regarding ethics in the IT field | Upon completion of lab work return the lab system to its original state. | Upon completion of lab work return the lab system to its original state. | Upon completion of lab work return the lab system to its original state. | |
| **Outcome #5** | Administer and troubleshoot a network infrastructure | Evaluate security risks on a computer workstation | | Strategically place firewalls and routers in the network to better monitor network traffic | Scan a network system, determine it's vulnerabilties, compromise the system and establish access to this system | Defend a closed network.<br>Scan a network for vulnerabilities | Implement and troubleshoot Windows Server into the network environment |
| **Outcome #6** | Evaluate best practices in security concepts to maintain confidentiality, integrity and availability of computer systems | Discuss security policies that should be in practice in organizations | | Given a scenario of a network system identify vulnerabilities and recommend mitigating these vulnerabilities. | Disuss weaknesses in network environments that can be exploited. | Discuss the "Defense in Depth" approach to network defense. | When designing and implementing network environments follow best practices |