CSEC2228 - Network Defense

Credits:	3 (2/1/0)
Description:	This course introduces students to the various methodologies for defending the information technology network infrastructure. Students will be introduced to the concepts, principles, type and topologies of firewalls to include packet filtering, proxy firewalls, application gateways, circuit gateways and stateful inspection.
Prerequisites:	• CSEC1110 OR • CPTR2236
Corequisites:	
Pre/Corequisites*:	
Competencies:	1. Outline physical security measures to current best practices. 2. Identify personnel security practices and procedures. 3. Explain software security best practices. 4. Outline network security. 5. Describe administrative security procedural controls. 6. Define cryptosecurity. 7. Indicate proper key management procedures. 8. Interpret transmission security models. 9. Name the elements of TEMPEST security. 10. Complete firewall cryptography strategies. 11. Distinguish firewall cryptography strategies. 12. Construct a packet filtering firewall. 13. Implement a proxy server.
MnTC goal areas:	None

**Can be taking as a Prerequisite or Corequisite.*