CSCN250N : Network Security Analysis

Network Security Monitoring is an essential activity for enterprise cybersecurity. This course will expand on tools and methods needed for carrying out this task. In today's environment it is unlikely that a network will be free of any intrusion attempts. Detecting these attempts and mitigating them makes a difference between a small incident and a major compromise of the network. The students will learn to use open source solutions such as Security Onion and Snort for collecting data, detecting intrusion, and analyzing the data. Upon completion of this course students will have the skills needed to be an effective network security analyst. This course requires a strong understanding of the TCP/IP suite of protocols and the Linux operating system prior to starting.

Class Hours 2
Lab Hours 2 **Credits** 3
Prerequisites
CSCN170N and CSCN216N or CCNA Certification, and CSCN211N or CyberOPs Associate Certification.