Module 13– Objectives and Key Instruction Points

Objectives:
Network security has been touched in various modules. This module needs to avoid unnecessary redundancy. The focus of this module will be to explore areas of preventative network security. Detection will be started in this module from a specialized security detection standpoint. The next module will finish detection from an aggregate viewpoint and the human aspect of security awareness necessary to supplement prevention efforts.
The guiding question is "What concepts and skills do students need to be successful building an IT environment suitable for the CDC?"

Video Segment 1 –

1. Defense in depth
    a. Attack trees and/or vectors
2. Perimeter – this could be a repeat from 10
3. Firewalls – types, role, configuration, limitations
    a. Routers, Firewalls, Gateways
4. IDS, IPS – this topic is present for completeness
    a. This technology will have limited use in a CDC
5. Netflow?
6. Malware defenses
7. PKI – primarily a topic for completeness. It is not clear that a CA exists in the ISEAGE environment.

Activities

Name	Objectives	Content ideas
Activity1	Use netflow to analyze network usage	Deploy netflow packages, implement a netflow collector and netflow monitoring/reporting software
Activity 2	Use certificates issued by a CA	Secure previously unsecured mail protocols using SSL certificates issued by an ISEAGE CA. The "root" certificate list will need to be updated.

Activity design

Handouts
Title:
Objectives:
Length: X pages
Notes: