Module 12– Objectives and Key Instruction Points

Objectives:
Service security was referenced in general in the last module in relation to securing the host or platform. This module is focused on securing key services. A careful balance will be needed between the video and the handouts in order to provide focused context in the video while limiting version specific details that would hasten its obsolescence. The video should include principles, features, threats and behaviors that have and will remain relevant in the foreseeable future.
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. Introduction
2. DNS
3. Mail
   a. ~~Sendmail~~
   b. ~~Authenticated Protocols & Securing Credentials~~
4. Interactive Session Services
   a. SSH
   b. Remote desktop client
5. File Services
   a. FTP
   b. SFTP
   c. HTTP
   d. NFS
   e. Windows File Services
6. Web Server
   a. Apache

Activities

Name	Objectives	Content ideas
Activity1	DNS Hardening	Have students adjust the existing DNS servers in their environments consistent with the DNS hardening guidelines
Activity 2	Mail hardening	Have the students adjust the existing mail environment in manner consistent with the mail hardening guidelines

Activity design

Handouts

Title:
Objectives:
Length: X pages
Notes:

Title: Best Security Practices for DNS Design and Configuration
Objectives: Address the considerations of DNS server location, role designation, authoritative server registration, commonly considered DNS parameters
Length: X pages
Notes:
Inclination is to focus on BIND, but Microsoft's DNS server can be document as time permits. Preference for BIND is its universality and being non-proprietary and transparent in configuration. It being the reference implementation of DNS isn't bad reason either.

Title: Best Security Practices for Internet Mail Design and Configuration
Objectives: Address the considerations of mail server location, role (MTA, MDA, MUA, mailbox hosts) designation, commonly considered DNS and mail configuration parameters
Length: X pages
Notes:
Software will need to be selected in order to make the handout content concrete. Preference would be non-proprietary and preferably free solutions. Configuration transparency is a good feature for whatever software is chosen.

Title: Best Security Practices for OpenSSH Implementation and Configuration
Objectives: Address the installation and configuration of OpenSSH server and clients
Length: X pages
Notes: This handout should address SFTP. Automated machine-to-machine SSH/SFTP connections are fairly common. What suitable advice can we provide for this use case.

Title: Best Security Practices for RDP/RDC Implementation and Configuration
Objectives: Address the installation and configuration of RDP server and clients
Length: X pages
Notes:

Title: Best Security Practices for Enabling SSL on a website
Objectives: Address the installation and configuration of SSL on Apache
Length: X pages
Notes:

Title: Best Security Practices for Windows File Sharing Implementation and Configuration

Objectives: Address the installation and configuration of Windows file servers
Length: X pages
Notes:

Title: Best Security Practices for NFS Implementation and Configuration
Objectives: Address the installation and configuration of NFS server and clients
Length: X pages
Notes: