Module 11– Objectives and Key Instruction Points

Objectives:
Historically operating system installation utilities were designed primarily to promote convenience to the administrator without much priority given to the security consequences of this convenience. The result was an insecure default installation. Today, it is still necessary to ensure systems subject to significant residual risk or operate in a high threat environment be deliberately secured from a configuration and software-vulnerability remediation perspective as well as active security controls.
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. Host/Platform Security
    a. Why is it necessary?
    b. The scope of the term "Host/Platform Security"
    c. Approaches to Host Security
        i. Bastion Host
        ii. Endpoint security
2. Bastion Host
    a. Operational role and operating environment
    b. OS Hardening
        i. Patches
        ii. Configuration
            1. Adjusting operating behavior
            2. Disabling or removing the unnecessary
    c. Service-software security
        i. Design and implementation
        ii. Patches
        iii. Configuration
            1. Adjusting operating behavior
            2. Disabling unnecessary features
3. Endpoint security
    a. Firewall
    b. HIDS/HIPS
    c. Anti Virus
    d. File system integrity monitoring
    e. Disk encryption
    f. Strong console authentication

Activities

| Name | Objectives | Content ideas |
|---|---|---|
| Activity1 | Practice building a bastion host with Windows | After cloning an existing Windows VM, have students harden it per available hardening |

Revision: 20130930

| | | |
|---|---|---|
| | | recommendations. The lab should include functional objectives for the host and possibly some experiments that reveal the functional limitations of a hardened host. |
| Activity 2 | Practice building a bastion host with Unix | After cloning an existing Unix VM, have students harden it per available hardening guidelines. . The lab should include functional objectives for the host and possibly some experiments that reveal the functional limitations of a hardened host |

Activity design

Handouts
Title:
Objectives:
Length: X pages
Notes:

Title: Hardening Windows 7
Objectives: Explain the process and reasons for altering Windows 7 to make it a suitable bastion host.
Length: X pages
Notes:
Explain any significant functional consequences resulting from a hardening step. Identify procedural dependencies within the procedure, so the reader understands the downstream (from a process perspective) consequences of not performing a particular step. Hardening at times raises tradeoffs between functionality and security, and is good the reader understands the tradeoff.

Title: Hardening Ubuntu
Objectives: Explain the process and reasons for altering Ubuntu to make it a suitable bastion host.
Length: X pages
Notes:
Explain any significant functional consequences resulting from a hardening step. Identify procedural dependencies within the procedure, so the reader understands the downstream (from a process perspective) consequences of not performing a particular step. Hardening at times raises tradeoffs between functionality and security, and is good the reader understands the tradeoff.