IT Adventures – CDC Curriculum – 2013 – Broad Ideas

After school program offered to students by a sponsoring teacher and supported by professionals who act as mentors.

The in-school program is meant to provide exposure to IT and cyber security in a broad sense. The motivation to achieve this exposure is to be prepared for a competition at the end of the school year that will utilize a number of the concepts.

The objective of the CDC curriculum development effort is to develop plans, learner objectives and content that facilitate learning by students being exposed to classroom instruction as well as assignments. The teacher is a facilitator of content material delivery in a broad sense. The teacher may not be knowledgeable in any of the subject matter, so the materials developed will need "self-delivering."

Historically the materials provided were how-tos on OS installation, hardening, networking and security tools.

A VMWare based "playground" has been developed to allow high school students to perform lab assignments as well as prepare their competition environment.

The students meet 2 -3 times a month. At these meetings the content may be continuation from the previous session. These classroom sessions needed to be complemented with labs and possibly other assignments.

Labs might be performed by an individual, but it would be more manageable if students got into small groups and for small groups to possibly combine to form "teams."

Delivery strategy can include student preparation like reading or viewing a video in advance of a session. But the ideas would need to be incorporated in the session in some fashion (e.g. review)).

The students have no IT background other than what they use in their life. Good chance they have broadband at home. This both provides them potentially useful context for discussions as well as a means to complete labs independent of access to school facilities.

The school year can be divided into two phases. The first and largest phase is for students to learn the base concepts and develop skills in IT and cyber security. The second phase is essentially a capstone project in which student teams are assembled and they build a new environment and prepare it for the CDC competition.

The first phase can be broken into two topic areas.

1. Skills and Concepts of Security Aware IT Design and Operations
2. Skills and Concepts of Security Operations

Tentative Schedule

Dates	Focus	Comments
September – January	Secure IT Design and Operations	
February – Mid March	Security Tools and Processes	
Mid March – IT Olympics	Constructing CDC Environment & Show down preparations	

Body of Knowledge Outline

1. IT Adventure CDC program objectives & schedule
2. IT Environments
    a. Home
    b. School
    c. Small Business
3. IT Concepts (each topic will lead with an intro addressing purpose & function)
    a. Computer
        i. Components – Processor, Memory, Storage, I/O
        ii. Server, PC, Tablet, smartphone
        iii. Physical vs Virtual
    b. Networking
        i. Wired, Wireless
        ii. Personal-, Local-, Wide-Area
        iii. Secure, Not-Secure
    c. Data Representation
        i. Binary
        ii. ASCII/ Unicode, ASN.1,
        iii. XML
        iv. File Formats
    d. Security
        i. Confidentiality, Integrity, Availability
        ii. Identity and Authentication
            1. Password security
            2. Multi-factor authentication
        iii. Authorization
        iv. Accountability
        v. Prevent, Detect, Respond (other models may be better)
        vi. Trust
        vii. Control

viii. Complexity vs Simplicity
ix. Information States (storage, transformation, transmission)
x. Vulnerability
1. Design, Development, Implementation
xi. Risk management
xii. Least privilege
xiii. Need to know
xiv. Policy
1. Administrative control – Organizational Document
2. Technical controls – "Domain" level, Device level
xv. Cryptography
1. Hashes
2. Encryption (symmetric, asymmetric)
3. Digital Signatures
4. Certificates

e. Internet
i. History
ii. Structure
iii. Challenges

f. Operating Systems
i. Lineage of Windows, Mac, *nix
ii. Client vs Server
iii. GUI, command line

g. Applications
i. standalone
ii. Client-Server

h. Networking Protocols
i. Network Services

4. Virtual Computing and VMWare
a. Architecture
b. Functionality
c. Components

5. Playground environment
a. Purpose
b. Setup/Architecture
i. Proxies (outbound access)
ii. Inbound access
iii. Virtual network environments

c. Intended Uses
d. Getting started

6. Operating Systems
a. User vs Administrator
b. Administration (commands & concepts)
i. Configuration
ii. Networking
iii. Services
iv. User Administration
v. Authorization & Access Control

1. File system
2. OS Privileges
3. Roles

vi. File systems (types & structure)

c. Editing & Other file manipulation (tools, commands, concepts)
d. Installation [majority of content provided primarily as supplemental material]
   i. Common objectives in OS installation
   ii. Common confusing issues with OS installation
   iii. Details regarding: Windows, Ubuntu, ??
   iv. Activity will be to build a VM. Go over snapshots and have them do one and revert to it.
e. Supplementary reference of other common commands or tools

7. Networking (may only be 1 session instead of 2, as originally planned)
   a. Protocol Models (module 3 handout)
   b. TCP/IP (module 3 handout)
   c. Physical Layer (module 3 handout)
   d. VMWare Networking
   e. Common networking components -Bridge/hub, switch, router, firewall (module 3 handout)
   f. Routing (concept and configuration) – (concept covered in module 3)
   g. Tunneling (concept and purpose)
   h. Network addressing
      i. Physical, IP, Transport Layer (covered in module 3)
      ii. Internet Routable, Non-routable (private address space)
      iii. NAT, PAT
8. Network Services (common/reserved ports numbers will be provided)
   a. DNS (purpose & conventions)
      i. "Split DNS"
      ii. DNS in NAT environment
      iii. Key record types
      iv. Record lookup tools
   b. Directory services
   c. Mail
      i. Send (smtp, sendmail)
      ii. Client side read (pop3, imap)
   d. Session services (telnet, ssh, rdp)
   e. File services (ftp, sftp,)
   f. Web (http, ssl+http)
      i. Clients
         1. IE, Firefox, Chrome, Safari
      ii. Server (installation instructions in supplemental material)
         1. Apache
9. Networking tools
   a. Troubleshooting
      i. Ping, traceroute
   b. Traffic analysis
      i. Wireshark
   c. Security testing

        i. Nmap, Nessus
10. IT Services Architecture – thorough treatment may be too abstract -
    a. Zones/"security domains"
    b. Service Collocation
11. OS Hardening (concepts & specific practices)
    a. Bastion host concept
    b. Privileged Ports concept and related security issues
    c. Endpoint security (AV, firewalls)
    d. Windows 7
    e. Ubuntu
    f. ?
12. Network Application and Service Hardening/Securing
    a. DNS
    b. SSH
    c. Sendmail
    d. Apache
    e. FTP
    f. ?
13. Network Security
    a. Defense in depth concept
    b. Perimeter
    c. Firewalls
    d. IDS, IPS
    e. Malware defense
    f. Securing Protocols
    g. PKI
14. Event Management
    a. Purpose
    b. Log Review
        i. OS, Applications (e.g. DNS, Apache)
    c. Monitoring
        i. Operating statistics
        ii. Operating services
        iii. User activities
    d. Analysis tools
    e. Analysis strategies
15. Response Strategies
    a. Resilience
    b. Block
    c. Evaluate, Contain, Eradicate, Recover (addressing vulnerability(s))
16. CDC Environment, Rules, Roles and Objectives
    a. Red, White, Blue, Green teams
    b. iScore
    c. Competition specific challenge
17. CDC Blue Team Strategies
    a. Effective strategies
    b. Common mistakes
18. CDC Lessons Learned

a. Reflect on what the best part of the CDC was
b. Reflect on what went right for the team and personally
c. Reflect on what went wrong and why
d. Reflect on what could have been done better
e. Reflect on how the experience may affect their future decision making
f. Reflect on CD topics that need to be understood better

Note: Topics and concepts that are not directly applicable (e.g. IDS, IPS) to the CDC may only be treated briefly to round out a discussion, but no assignments, labs or supplementary materials would be developed for those items.

Course layout I

Month	Session	Content
September	1	IT Adventure CDC program objectives & schedule IT Environments
	2	IT Concepts I
	3	IT Concepts II (Security focus)
October	1	*Slack – Catch-up session period – Can be "redeemed" anytime in school year before late March (firm date on playground reset)*
	2	Virtual Machines & VMWare Playground Environment
	3	Operating Systems I
	4	Operating Systems II
November	1	Networking I
	2	Networking II
	3	Network Services I
December	1	Network Services II
	2	Networking tools
January	1	IT Services Architecture OS Hardening I
	2	OS Hardening II
February	1	Network Application & Service Hardening/Securing
	2	Network Security I
	3	Network Security II
March	1	Event Management I
	2	Response Strategies
	3	CDC Environment, Rules, Roles and Objectives
April	1	CDC Blue Team Strategies
	2	Competition Scenario I
	3	Competition Scenario II
May	1	Lessons Learned from CDC/What could we do better?

Notes: Students lose access to their CDC environments Wednesday before event
23 Sessions
Session Length – 1 hour. Plan on max content duration to be 48 minutes.

Learner Objectives

After participating in this IT Adventures over the school year, I will be able to:

Targeted Bloom	Concept	Objective Statement
Application	Security is contextual	Apply security concepts and tools to an environment that serves a purpose.
Comprehension	IT is a means to achieve objectives	Describe how information technology is used to achieve every day objectives.
Application	Preventative practices	Use security concepts, practices and tools to prevent violations of security policy.
Comprehension	Detective practices	Demonstrate how security concepts, practices and tools are used to detect violations to security policy.
Comprehension	Responsive practices	Explain security concepts, practices and tools used to respond to violations to security policy.
Comprehension	CDC events	Describe the CDC environment, rules, roles and objectives.
Application	Virtual computing	Use virtualization to construct an IT environment consisting of multiple virtual components that operate together as an IT environment that serves a purpose.
Application	IT administrative practices	Use IT administrative practices to implement and maintain an IT environment that serves a purpose.
Comprehension	Operating System operations	Describe the types and the uses of Operating Systems used in an IT environment.
Application	Networking	Apply networking concepts, components, tools and services in order to build and maintain a functional IT environment that serves a purpose.
Application	Perimeters and domains	Apply the concepts of perimeters and domains as well as the related components, practices and tools that assist with securing an operational IT environment.
Comprehension	Blue team objectives	Explain the objectives of the Blue team and its members during a CDC event.

Lesson Plans

Developed Content

1. Session Learning content
    a. Question: Are teaching techniques other than lecture format viable?
        i. Yes and other formats will be necessary
    b. Question: Are sufficient numbers of computers/tablets available for small groups to use?
        i. Yes, so long as nothing needs to be installed locally by the students universal access can be assumed. Specifications may need to be documented to clarify what software we will be expecting.
    c. Session content formats
        i. Lecture
        ii. Activities – Labs, Worksheets, Games etc.
    d. Module guidance section will be needed for the teacher, which should contain
        i. Module breakdown by topic and delivery format as well as expected time committment

2. Supplementary materials
    a. Purpose: Provide more granular instruction focused more on what and how.
    b. Approach: Modular materials allowing for changes in technology and focus.
    c. Handouts – useful references later during CDC preparations and after.
    d. Video -
3. Assignments
    a. We won't purposefully design assignments. Session learning content may be assigned by the teacher as an assignment.

Activities Plan

Orchestrate the assignments so that they progressively build to an intended objective. One possible objective is to develop a mock CDC Blue team environment slowly and deliberately over the September to mid-March period. There may be more instances of components than would be normal in order to facilitate a more granular experience for the students. Give each student/small group an opportunity build "one of everything".

Questions to consider:

1. Does it make sense for all of the small group efforts to integrate into a greater system?
    a. Yes, having an opportunity to build each component and integrate them once before should help with CDC scenario construction
    b. This will require a little more forethought on our part.
    c. This will encourage students to consider the impact of their efforts on the greater "organization" which is necessary in practice.
2. How do small group membership changes affect the lab assignments?
3. Do we want to provide intermediate "solutions" for the teacher to introduce to get over any hang-ups?
    a. Yes, the "solutions" should be available. However, the troubleshooting necessary to fix problems is a valuable skill. "Solutions" should be introduced as a last resort.
4. Can we expect every school to have enough competent mentors to bail out each student/student group?

5. Should assignment materials provide supplementary instruction to enable success or should assignments reference an independent set of supplementary materials?

Conventions

1. Module naming. Each module will be assigned a unique module ID.
    a. Modules to be delivered over multiple sessions will not be subdivided in terms of naming.
2. Page numbering of session content. Numbering will restart for each distinct content item (e.g. slides, handouts). The module ID will be clearly marked on each page to ensure the pages are collated properly.
3. Content delivery nomenclature
    a. Video-PP - Powerpoint presentation recorded with voice over track
    b. Video-SS – Video primarily composed of dynamic computer display output with an accompanying voice over track
    c. Handout – Document that is formatted for both printed and viewed in digital forms.
    d. Lab – Hands-on activity that will be situated in the IT Adventures playground virtual environment.
    e. Exercise – An activity that will involve answering questions. Many exercises will be developed to facilitate social learning. The questions may require the students to use a computer to respond to the exercise.

Content Development Strategy

Effort should follow a breadth first development approach. Capturing the intellectual property is of first priority. The actual deliverable elements are much more mechanical in nature and can be given to others to complete.

Video: First objective is to develop the objectives and the information that will fulfill the objectives. Talking points are next, but verbatim language should not be before all the modules are completed. Developing or searching for supplementary images that are ancillary to the developed content should be postponed until after the talking points for all the modules have been developed.

Handouts: Much of the content for the handouts should be established in the first pass. The final presentation can be manipulated later. Content can come from work written by Doug, but the quantity should be limited per work item.

Activities: At first pass the objectives of the activities and the type of activities should be developed. Question oriented activities can be developed with little relative effort. Complicated worksheets, games, labs etc development should be postponed until after the modules have gone through a pass.