Teacher notes for SANS Cyber Aces Online

These notes are based on the 2013 Cyber Aces Modules. The Modules themselves were developed by SANS and CounterHack, and are copyrighted by SANS. General Cyber Aces information can be found at http://www.cyberaces.org/.

We taught a semester course to high school seniors based on the Cyber Aces Modules. The modules are meant to be done by students who are working independently, so they include all the necessary materials. Most students will have a better experience if they have someone to guide them, however.

Teacher Preparation

This class can be taught by any teacher who is comfortable installing operating systems and has basic experience in programming. I highly recommend that teachers build their own labs and work through the previous year's modules as preparation. While Cyber Aces is in progress, mentors are available for both teachers and students via the Cyber Aces web site at https://online.cyberaces.org/home/mentor. Additionally, teachers may contact Cyber Aces (ssandelius@sans.org) or myself (yorkj@brcc.edu) for assistance.

Building a Lab

In our class, we found the students would much rather be given computer exercises to do than listen to lectures. Therefore each student needed their own computer.

Internet Access

The Cyber Aces modules are slides with audio instruction. They are now released as YouTube videos, so the students will need Internet access with decent bandwidth and YouTube will have to be allowed through the school web filter. The instructor should download the Virtual Machine (VM) images ahead of time, as they can be quite large.

Software

The current version of VMware Player (Windows or Linux) or VMware Fusion must be installed. VMware Player is available as a free download from http://my.vmware.com. VMware Fusion is not free. Instructions for installing VMware Player and Fusion are found in the first Cyber Aces module, Operating Systems.

Computer Requirements

The computers for this course don't have to be the most modern, but they should have at least 4 GB of RAM. Ours had 8GB and did well.

School Computer Labs

School computer labs are often locked down. If VMware Player is installed on the lab computers by the school IT department ahead of time, these computers can be used for Cyber Aces classes with some minor workarounds.

1. Administrative rights. If the lab computers run Windows but do not allow students administrative rights, the students can create Windows VMs and run them inside VMware Player. (VMware Player installed by school IT)
2. Storage space. Students will need one Windows VM and one CentOS VM. Although Windows exercises can be run on the lab computer itself, it's a good practice to practice using a VM. Ideally, students would have 20GB for the Windows VM, 10GB for the CentOS VM, with room for a spare of each VM in its initial condition. If students use the Live CD version of CentOS (described below) and don't install a Windows VM, disk space used can be kept to a minimum.
    a. Desirable 60 GB
    b. Workable 20 GB
    c. Absolute minimum, run Windows exercises on the lab computer 0 GB

    Note on minimum disk space. It is possible to do the exercises without students having their own permanent disk space. However:
    A) If you use the LiveCD you don't have to save the VM. The problem is any changes you make will always be lost and you'll have to add your .iso as a VM every time you start up.
    B) It also assumes you have admin rights so you can do all the windows exercises on the host so you don't need a Windows VM.

3. Often, computer labs do not allow students to store large (or any) files on the lab computers. If this is the case, students can store their VMs on external USB hard drives, or large flash drives. I have VMs on a USB 3.0 hard drive. Although they run (load, especially) more slowly than VMs on the hard drive, they work fine. VMs on flash drives or USB 2.0 drives are slower, but still useable. The advantage of external or flash drives is that the students can also use them at home.

Media for installing Windows and CentOS VMs

A 90 day trial version of Windows 8 may be downloaded from http://technet.microsoft.com/en-US/evalcenter . Click Evaluate Now to see which downloads are available. You may have to create a login to the site. Please see the current SANS Cyber Aces Online Operating Systems tutorial for updated information.

There are two options for installing the CentOS virtual machine, full installation and Live CD. The 2013 Cyber Aces used the Live CD method, which runs directly from the CD or ISO file without installation. The advantages of the Live CD are that it doesn't require the students to go through the installation process, and the Live CD takes much less disk space. The disadvantage to the Live CD is that any changes the student makes (installing Apache web server, PHP, etc.) are lost if the student reboots the VM. The students can avoid this by suspending the VM (the button looks like a pause button) before quitting VMware Player, provided they have disk space available. It's easy to forget, though.

The download button on the current CentOS site (http://www.centos.org/download/) takes you to links that download the most current full installation version of CentOS. If the Cyber Aces slides are using a slightly older version, or if you want the Live CD version, you'll need to select "alternative downloads" and select a mirror site. Navigate to the version you want, i386 or x86_64 (32 bit or 64 bit, 64 bit is

preferred) and select the ISO you need. For Live CD, you'll see Live CD included in the file name. If you want the full install, the file name will include x86_64-DVD.

Both the Windows and CentOS files can be quite large. Students should not be allowed to download them from a computer lab, at least not all at once. Most likely they won't download completely, and it may well bring the school network to its knees. Instead, the instructor should download the files ahead of time and make them available to the students via DVDs or on a classroom server. For our class, we used a spare workstation with Windows and a file share to distribute the ISOs. We needed to give it a Gigabit port on the classroom switch, though. When several students tried to copy the ISOs when the classroom server had a 100 Mb connection, it was slow. Be careful when downloading the files, and when burning them to DVDs. There are often errors, so it is good to test your final product (DVD or classroom share) before the students use it. (CentOS will give you an MD5 hash you can check, but Windows often does not.)

Installing VMs

The Cyber Aces modules have good instructions for installing the Windows and CentOS VMs. Instructions for installing Windows 8 are in CyberAces_Module1-Windows_2_InstallingWindows_20130831.pdf and instructions for CentOS Linux (Live CD) are in CyberAces_Module1-Linux_1_VMware_20130910.pdf. If you opt to fully install CentOS, allow for 10 to 20 GB when you configure the VM's hard disk. The lessons use SSH, Apache and PHP. If you make the default LAMP installation (Linux, Apache, MySQL, PHP) you should be ok.

Networking

After a VM is installed, Edit Settings, Network Adapter, in VMware Player allows three choices for networking:

1) NAT (This stands for Network Address Translation, described in the Networking module.) This is the default mode and the one that should normally be used. VMware uses NAT to allow external communications from the VM to use the host machine's existing IP address to communicate with the web.
2) Bridged. This mode allows the VM to take direct control of the host computer's network adapter and request a new IP address for the host using DHCP. It is used when the VM must be reachable from the outside, and is not necessary for this course. Avoid its use in computer labs—a sudden doubling (or more, if multiple VMs are running) of the need for IP addresses in the lab could cause problems for your IT staff.
3) Host-only. In this mode VMs can communicate with the host computer and with each other but cannot talk to anything outside the host computer. This is a very good mode to use if you are practicing with scanners or attack tools. Your VMs can scan or attack each other, but you won't be able to scan or attack the school network by mistake.
   Note: there is no use of attack tools in Cyber Aces.

John York, Network Engineer at Blue Ridge Community College, a SANS Cyber Aces Online Mentor and mentor at Shenandoah Valley Governors School, VA.