



Congratulations on your decision to attend the DHS Cyber Emergency Response Team (DHS ICS-CERT) training. We think you will find it informative and rewarding. Please know that the Industrial Control Systems Security training courses (202 and 301) are hands-on classes, which require a laptop to complete the class exercises and labs.

### Laptop FAQ

1. Why do I need to have a Laptop?

Both the (202) and (301) level classes include hands-on labs and exercises that require access to a laptop.

2. What are the laptop system requirements?

- a. 1 Gigahertz speed processor minimum
- b. 64 bit operating system/hardware platform
- c. 4 Gigabytes of random access memory (RAM) minimum required; more is always better.
- d. 1 DVD-ROM drive capable of reading and booting off of a DVD; if you do not have an internal or external DVD drive for your laptop, a Virtual Machine can be loaded from a USB thumb.
- e. x86 processor (Windows and Macintosh)
- f. During the hands-on training and exercises, you will connect your laptop into our networks to practice with the tools on the Kali distribution. For the (301) course, you will need Ethernet capability. A wireless adaptor is required for the (202) course.

3. Do you prefer any particular OS or applications on the laptop?

The live Kali DVD will open in a Linux environment. From our testing, it seems to work on both PCs and Macs.

4. Will we run Kali as a Live DVD, or will we perform a hard disk install of Kali?

You will be running the modified Kali as a Live DVD. When you plug your computer into our networks, you will be able to see all the computers on the network—which means you can reach out and touch the corporate, DMZ, or control system computers that we have set up as well as your neighbors'. So before we start the hands-on portion of the training, we will remind you of that potential concern and give you the opportunity to remove your hard disk.

5. Can I use my employer-provided laptop?

Please check with your IT department for approval. In many cases, attendees prefer to use their home/private laptop to avoid violating any security policies. Regardless, you will need administrator access to set the boot order to boot from the DVD.

6. Can I use my Macintosh MacBook or MacBook Pro?

Yes, as long as it has an x86 processor. To verify you can click the Apple icon in the top left corner of your MacBook's screen and select "About This Mac." A small box should then open with details about your processor.

7. How do I boot off the class-provided DVD disk?

Your instructors will walk you through how to use the disk and boot from the DVD drive. In the event that you'd like additional or advanced information, the following information has been compiled:

#### Windows

You will need to access your laptop's BIOS to configure your laptop to boot from the internal DVD drive. Depending on your vendor, you may need to hold down the F2, F12, or escape keys to access the BIOS. From there, you need to navigate to "Boot Sequence" (again different manufacturers label this differently).

In most cases, once you've set the laptop to boot first from the DVD drive you hit the escape key and select "save changes." You can then insert the class DVD disk and reboot.

#### Macintosh

Insert the disc then power off the computer. Restart the laptop while holding down the "option" key. This should allow you to select to boot off of a DVD. Alternatively, on the most recent Apple laptops, you may need to hold down the "C" keys during startup to access the screen to select a boot up device.

8. What if I do not have a laptop I feel comfortable using?

In the event that you do not have a laptop that you feel comfortable using, you may contact [cssp\\_training@hq.dhs.gov](mailto:cssp_training@hq.dhs.gov) to see if an extra laptop can be provided. If there isn't one available, you can still participate in the training and follow along with the person sitting next to you. While you won't have the benefit of being able to navigate through the toolkit firsthand, you will still be able to learn the basic concepts and overall idea of how a cyber-attack can be conducted to impact a control system.