# CSC436 Lab 07

Take screenshots of the process as you work through the lab, and save them to a single Word or PDF document.

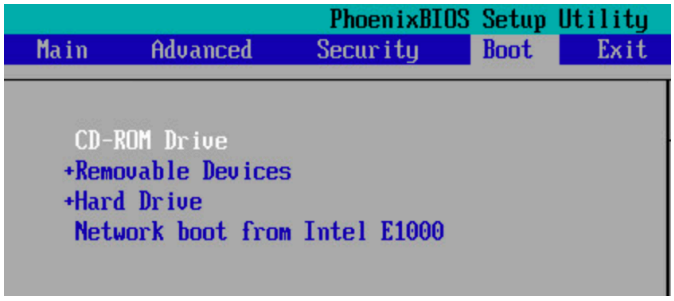
This lab should be completed in the CSC436_Exploitation vApp.

## Local Access

Boot a live Kali CD on the Windows 7 VM. This will simulate us having physical access to the machine, and booting a live Kali CD. We'll then dump password hashes.

### Boot a Live CD

- Right-Click on the Windows 7 VM, and choose Insert CD/DVD from catalog
- Search for Kali, and choose kali-linux-2017.1-amd64.iso
    - Insert the ISO
- With the Windows VM turned on, open the console. Reboot the VM from within Windows.
- When the VM is restarting, you'll have a split second to catch the BIOS/BOOT menus. Watch carefully, and press **F2** to open the BIOS setup.
- You'll then need to boot to the Kali ISO, one method is to edit the boot order as in the following screenshot:




### Mount the Windows Drive

- View the windows partitions by running `fdisk -l` (lowercase L)
    - You'll notice /dev/sda2 as the larger disk
- Create a mount point by running `mkdir /mnt/sda2`
- Mount the drive by running `mount /dev/sda2 /mnt/sda2`

### Removing Passwords

- Use the chntpw to remove the password for the Administrator user.

## Remote Access

If we are able to obtain remote access to a machine, we can also dump hashes and crack them.

### Prepare Windows XP

- Log in to the Windows XP VM, and create a few users. Be sure to give the new users passwords. Feel free to make some easier, some more difficult.

### Exploit Windows XP

- Use Metasploit to exploit the Windows XP VM, and get a meterpreter session.
- Use *hashdump* in meterpreter to dump the password hashes on the Windows XP system. You'll want to copy them to a file.

### Crack the Passwords

- Use John the Ripper to crack the password hashes you just dumped.

## Creating Word Lists

Dictionary attacks are often a faster method than brute-forcing passwords, but have a limitation: The user's password MUST be in the dictionary or word list for you to find it. It may be a good idea to create word lists during the OSINT phase. Pages 34-38 in *The Hacker Playbook 2* outline the *wordhound* and *brutescrape* tools. Please read about these tools, but you do not have to actually run them if you don't want to.

Nothing to turn in for is section, it's more informational.