Change password on built-in admin account before disabling it:

Control Panel > User Accounts and Family Safety > User Accounts > Change your password

Initial Configurations - Admin accounts and passwords:

Control Panel > User Accounts > Manage User Accounts > Add... > [Enter a name and domain for admin account] > Click on new admin account > Change the password > log off and log into new admin account

Finding and disabling and removing old admin account from new admin account:

Open powershell as administrator> type in the next line in this guide > Get-WmiObject -Class Win32_UserAccount -Filter "LocalAccount='True'"

(ALTERNATIVELY, WITHOUT POWERSHELL, YOU CAN USE THE COMMAND PROMPT TO FIND USER ACCOUNT. Administrator highlighted in green means that you can put in any account, besides built-in administrator, to try and delete it.)

run as administrator command prompt > type in "net user" > type in "net user Administrator" to check the status of the built-in Administrator (you can also type in any other account to check it's info)

Start Menu > All Programs > Accessories > [run as administrator] command prompt > type in "net user administrator /active:no" > net user administrator /DELETE

Download Google Chrome:

iexplorer > url: https://www.google.com/chrome/browser/desktop/index.html > download chrome > you can now replace everything that needs iexplorer with chrome

Download Kasperky (Placeholder Antivirus until we figure out what is CCDC Legal):

Download Microsoft Baseline Security Analyzer (needs ports 138 & 139):

iexplorer > search for microsoft baseline security analzyer (https://www.microsoft.com/en-us/download/confirmation.aspx?id=7558) > download it > download it some more > run the installer > remember the destination folder > install it vigorously > run it > scan > copy the results to the clipboard > paste all of that stuff into a notepad or something > make some changes to the system (e.g. apply some updates or patches) > scan with MBSA again > copy it to clipboard and then some sort of file like notepad > compare both with the "compare-object" powershell command as in the example below that is highlighted red **(you will have to make each different file it's own variable and add that into the powershell command)**

Get Scripts for auditing group policies in chapter 18:

------Placeholder-------

Start and Open event viewer:

Start > type in "services.msc" in search bar > click on Windows Event Log > General Tab > Start Windows Event Log

Start > type in "Event Viewer" in search bar > Run it

Enable firewalls and configure deny rules:

Start > Control Panel > System and Security > Windows Firewall > click on "Turn windows firewall on or off > turn on windows firewall for home or work > turn on windows firewall for public network > Checkmark "Notify me when Windows Firewall blocks a new program" for both settings > **Checkmark "Block all incoming connections, including those in the list of allowed programs" for both settings (you will uncheck these options and reconfigure the firewall according to CCDC rules after all other settings below are configured)**

----------Placeholder----------

Firewall state and rules:

Group policy editor > local computer policy > computer configuration > windows settings > security settings > windows firewall with advanced security > windows firewall with advanced security > click on "windows firewall properties" > firewall state: on(recommended) > configure inbound and outbound connections according to CCDC rules

Check arp table:

start > cmd > type in "arp -a" > take a screenshot > place screenshot into word application or whatever you can find

(Create an xml file (enumerate) of all the services and network connections:

start > cmd > type in "powershell" > "get-process > Enumi.xml" > "cat .\Enumi.xml"

$A=Get-process ; Start-Sleep -s 10; $B=Get-process ; compare-object $A $B

Comparing different MBSA notes with eachother via powershell (refer to the MBSA setup that was made earlier):

start > cmd > "powershell" > "$A=cat MBSAedit1.txt ; $B=cat MBSAedit2.txt ; compare-object $A $B"

Download nmap:

start > iexplorer > https://nmap.org/download.html > go to microsoft windows binaries > click on the download "nmap 7.60 setup.exe" > save file to wherever > run file > do all the checkmark thingies > start nmap

Use nmap:

start nmap > input target > choose profile (figure out what would be best for the competition) > press scan > watch the magic happen > take a screenshot of the results and paste it into a word document or whatever

Downloading windows sysinternals:

start > iexplorer > go to "https://docs.microsoft.com/en-us/sysinternals/downloads" (or just search for it *watch out for internet malware and that bad stuff*) > click on Sysinternals Suite > download the file onto your desktop > on desktop, make a new folder called "windows_sysinternals" > extract the contents of the zipped sysinternals file that you just got into the "windows_sysinternals" folder you just created

Checking and deleting autoruns with the sysinternals suite you just downloaded:

start > cmd > type in "dir" (this will tell you where you are in the command line interface and what you can interact with) > change to desktop with "cd desktop" command typed in > change to sysinternals folder with "cd windows_sysinternals" > open up the autorun file by typing in "autoruns.exe" > choose and delete certain autoruns

SKIP MICROSOFT .NET FRAMEWORK 4.7.1 FOR WINDOWS 7 AND WINDOWS 2008 R2 (IT TAKES TOO LONG TO DOWNLOAD [ABOUT 5 MIN])

SKIP MICROSOFT .NET FRAMEWORK 3.5.? FOR WINDOWS 7 AND WINDOWS 2008 R2 (IT TAKES TOO LONG TO DOWNLOAD [ABOUT 5 MIN])

WINDOWS SERVER POWERSHELL COMMANDS FOR LOGGING PEOPLE OFF

qwinsta /server:<servername>

rwinsta <SESSION_ID> /server:<serverName>

Download AVG antivirus:

Go on chrome > https://www.avg.com/en-us/homepage > click on download > run the download > install it > scan > restart to bring up all of AVG's shields > whatever