

### Notes on Windows:

- How to enable God Mode (in Windows)
  - o God Mode: a control panel allowing easy access to all administrative tasks
  - o Go to desktop -> right-click on empty portion in desktop -> New -> Folder -> edit title so its name is GodMode.{ED7BA470-8E54-465E-825C-99712043E01C} -> Enter -> double-click icon to access
  - o To remove: delete folder
- Command Prompt (useful commands)
  - o Useful commands
    - **Help** command: lists all the commands built into the command prompt
      - For information about a particular command type **help commandname**
        - o Example: **help cd** give more info on a command
      - For all commands, type command name followed by a **/?** To see help on the command
        - o Example: **cd /?**
    - **Exit** command: closes command prompt
      - type **exit** -> press enter
    - **CD** command: change current directory or see what directory you are currently in
      - To change directory from one you are in to the one specified: **cd directoryname**
        - o Remember to use paths
      - To change to a directory currently in your current directory: type **cd directoryname** and press enter
        - o Don't need full path
        - o Example: if you are in a directory c:\test, and there were three directories in that the test directory called A, B, and C, you could just type **cd a** and press enter. You would then be in the c:\test\a
      - To change directory to c:\windows\system32 directory: type **cd \windows\system** and press enter
    - **DIR** command: lists files and directories contained in current directory, if used without an argument, or the directory specified as an argument
      - To use: **dir** -> press enter
      - Shows list of current files in directory you are in, including info about file sizes, date and time they were last written to, also shows space files in the directory are using and the total amount of free disk space available on current hard drive
      - Can use \* symbol (wildcard)
        - o Example: **dir \*.txt** lists files that end with .txt
    - **Copy** command: allows copying of files from one location to another
      - To use: type **copy filetocopy copiedfile**
        - o Example: if you have file c:\test\test.txt and would like to copy it to c:\windows\test.txt type **copy c:\test\test.txt c:\windows\test.txt** and press enter
          - o Tells if copy was successful and gives back prompt
      - If copying within same directory you do not have to use the path
      - Examples:
        - o **copy test.txt test.bak**

- Copies test.txt file to new file called test.bak in the same directory
  - o **copy test.txt \windows**
    - Copies test.txt file to \windows directory
  - o **copy \* \windows**
    - Copies all files in current directory to \windows directory
- **Move command:** allows moving of a file from one location to another
  - Examples:
    - o **move test.txt test.bak**
      - Moves test.txt file to new file renaming it to test.bak in same directory
    - o **move test.txt \windows**
      - Moves test.txt file to \windows directory
    - o **move \* \windows**
      - Moves all files in current directory to \windows directory
- o **Redirectors:** manipulation of how output or input of a program is displayed or used
  - Used by appending them to end of a command followed by what you are redirecting to
    - Example: **dir > dir.txt**
    - Four redirectors:
      - o **>**
        - Takes output of a program and stores it in a file
        - if file exists, it will be overwritten, else new file is created
        - Example: command **dir > dir.txt** will take output of the dir command and place it in dir.txt file; if dir.txt exists, it will overwrite it, otherwise it will create it
      - o **>>**
        - Takes output of a program and stores it in a file
        - If file exists, the data will be appended to current data in file rather than overwriting it. If it does not exist it will create a new file.
        - Example: command **dir >> dir.txt** will take output of the dir command and append it to existing data in dir.txt file if file exists; if dir.txt does not exist, it will create the file first
      - o **<**
        - Takes input for a program from a specified file
        - Example: the date command expects input from a user. So if we had the command **date < date.txt**, it would take the input for the date program from the information contained in the date.txt file.
- o **Batch Files (extension .bat):** scripts that contain command prompt commands that will be executed in the order they are listed
  - To create: make a file ending in .bat, such as test.bat, and have the commands you would like inside the file
    - Each command should be on its own line and in the order you would like them to execute
  - Example:
    - **cd**

- cd \test
  - dir
  - cd \
- o **Console Programs:** created for solely running within a command prompt, or console window
  - <http://unxutils.sourceforge.net/>
- Windows Forensics: Have I Been Hacked?
  - o **Creating Computer Forensics Tool belt**
    - **Process Explorer:** lists all open processes and delineate between parent processes and processes spawned by the parent
      - useful for seeing programs running on your computer and how they were launched
      - <http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>
    - **Process Monitor:** real time display of all processes, Windows Registry, and file activity on computer
      - useful when concerned that a hacker may be connected to your computer and you wish for a general idea of what they are doing
      - <http://technet.microsoft.com/en-us/sysinternals/bb896645.aspx>
    - **Show Hidden:** lists all hidden folders, and files, on your computer
      - easier to find hidden folders that appear suspicious
      - <https://www.bleepingcomputer.com/download/show-hidden/>
    - **TCPView:** list all programs on your computer that are connected to a remote computer or are waiting for a connection, will also list all connected IP addresses and perform reverse DNS on them so that you can get useful information on who is connected
      - <http://technet.microsoft.com/en-us/sysinternals/bb897437.aspx>
    - **TreeSize Free:** scans drive and easily shows folders on your hard drives that are using the most space; if concerned that server was hacked to distribute copyrighted programs and videos, you can use this tool to search for large folders to investigate
      - [https://www.jam-software.de/customers/downloadTrial.php?article\\_no=80&language=EN&PHPSESSID=ekvd5m6mr4gbfl3s032umssr56](https://www.jam-software.de/customers/downloadTrial.php?article_no=80&language=EN&PHPSESSID=ekvd5m6mr4gbfl3s032umssr56)
    - **Wireshark:** allows you to see data flowing through your network, can use to look at the raw TCP/IP packets to see if any nefarious activity is taking place
      - <http://www.wireshark.org/>
  - o **How to tell if hacked**
    - When hacked/accessed remotely, it is done over a TCP/IP network
      - Hacker will usually install a backdoor to get back in regardless of security measures taken
      - Only time a hacker does not leave something behind is when they are hacking the computer for specific info or an item
      - Hackers may also install RATs (Remote Access Trojans) or other backdoors to connect remotely
        - o Listen on TCP or UDP connections & connect to an IRC (Internet Relay Chat) channel where they can then be controlled by an operator or act as the hacker's backdoor
    - To see programs running on the computer's TCP or UDP ports, run TCPView
      - Displays list of all programs connected to the network
      - Program is broken up into 5 columns

- o **Process:** This column displays the name of the program that is connected to the remote device or is waiting for an incoming connection.
- o **PID:** This column shows the process ID for the particular program.
- o **Protocol:** This column displays whether the particular row is using TCP or UDP.
- o **Local Address:** This column shows the hostname or IP address of the local computer's connection..
- o **Local Port:** This column will show the port number being used by the local connection. If the port number corresponds to a standard service, it will show the service name instead.
- o **Remote Address:** This is the IP address or hostname remote device the particular program is connected to.
- o **Remote Port:** This column will show the port number being used by the remote connection. If the port number corresponds to a standard service, it will show the service name instead.
- o **State:** This column shows the state of the program's connection.

These states are:

- **Established** - A connection that is established means that there are is an active connection between your computer and the remote computer.
  - **Close Wait** - The remote connection has closed the connection. This entry will eventually time out and be removed from the TCPView list.
  - **Time Wait** - Your computer has closed the connection. This entry will eventually time out and be removed from the TCPView list.
  - **Listening** - This state means that the program is listening for an incoming connection from a remote computer. The port that it is listening on can be found in the local address column.
- To see if traffic is legit, use <http://www.dnsstuff.com/>
    - o If IP address shows location to another country that you shouldn't be connected to, be concerned
  - Examine programs listed in TCPView
    - o If unsure about a program, right-click and select **Process Properties**
    - o Investigate using <http://www.virustotal.com/>

- Don't need to be concerned about svchost.exe, wininit.exe, services.exe, lsass.exe, and some processes labeled as System Processes
- To terminate processes and end connections, right-click on the file and click on the **End Process** option
- Once you determine that a program should not be there, you need to determine where it is starting from
  - Use programs such as DDS or Autoruns
  - shows all programs that automatically start in Windows
- **Looking for further suspicious activity**
  - Use tools such as Process Explorer, Process Monitor, ShowHidden, TreeSize Free, and Wireshark to dig deeper for non-network related suspicious activity
  - **Process Explorer**
    - can be used to view all running processes on your computer
    - Helps find programs that do not appear legitimate and gather more information about them
    - To examine a process, double-click and a properties screen will open
      - This screen contains tabs providing a variety of information about the particular process
      - Be concerned with the information on the **Image** tab and the **Strings** tab
        - Strings tab will contain a list of strings found within the executable
        - May provide a clue as to what the process is doing
        - Image tab will display information about who created the file, its name, where it is located on your hard drive, commands used to execute the program
  - **Process Monitor** allows you to watch all the activity a particular process is performing on your computer
    - When run, it displays an overwhelming amount of data
    - Configure display filters that will allow you to specify the particular processes that you wish to see information for
  - **Show Hidden** lists all of the folders on your computer that have the hidden attribute
    - If you use the **-f** command line argument, then it will list all hidden files as well
    - When a computer is hacked, hacker typically creates a folder containing a variety of tools and programs that they need to hack other computers or setup various programs (will usually be hidden)

- Can create a list of hidden files and folders that can then be examined to see if they should be there
  - NOTE: will be MANY legitimate hidden folders, so do not delete anything unless you know for sure it does not belong
- **TreeSize Free** generates list of all folders on a drive and how much hard drive space they take up
  - When a hacker sets up a Warez distribution site on your computer, the files typically take up a great deal of space
  - Helps find folders that consume a lot of space and investigate them for suspicious file
- **What if a tool states another program is running but I can't find it!!!?!**
  - have the option set to see all hidden and system files
    - <https://www.bleepingcomputer.com/tutorials/how-to-see-hidden-files-in-windows/>
  - If doing directory listing in command prompt, use /a flag with the **dir** command to see hidden files
  - If still unable to see files, possible a Rootkit is installed (program used to hide files, Windows Services, and Windows Registry information so that they cannot be seen and removed with normal tools)
    - First scan computer with Rootkit detector
      - <https://www.bleepingcomputer.com/download/malwarebytes-anti-rootkit/>
      - <https://www.bleepingcomputer.com/download/panda-anti-rootkit/>
      - <https://www.bleepingcomputer.com/download/trend-micro-rootkitbuster/>
      - <https://www.bleepingcomputer.com/download/rootrepeal/>
      - <https://www.bleepingcomputer.com/download/tdsskiller/>
      - <https://www.bleepingcomputer.com/download/gmer/>
      - <https://www.bleepingcomputer.com/download/aswmbbr/>
    - If no rootkit detected, bypass rootkit and see hidden files using a bootable CD
      - Boot computer into Windows Recovery Environment
      - gives you to your file system and Windows Registry using a command prompt
        - <https://www.bleepingcomputer.com/tutorials/how-to-install-the-windows-xp-recovery-console/>
        - <https://www.bleepingcomputer.com/tutorials/command-prompt-in-windows-recovery-environment/>

- o **Other Hacks? And are they detectable?**
  - **Alternate Data Streams (ADS):** introduced into NTFS volumes to support the Macintosh Hierarchical File System and are widely undocumented
    - Hacker can hide files, even executables, and make them almost invisible to the operating system and therefore yourself
    - Tools such as [LADS](http://www.heysoft.de/en/software/lads.php?lang=EN) or [ADS Spy](https://www.bleepingcomputer.com/download/ads-spy/) that enable you to see ADS files and remove them
      - o <http://www.heysoft.de/en/software/lads.php?lang=EN>
      - o <https://www.bleepingcomputer.com/download/ads-spy/>
  - **Kernel and Device Driver hacks:** An experienced hacker may be able to patch system drivers, device drivers, or system calls
    - Enables them to issue commands to OS as Ring0 or at the operating system's kernel security level
    - Best solution is to backup data and reinstall the OS because if hacker has that access to the box, then unknown what else has been compromised
    - If it is necessary to try and detect and remove hacks, use the **SFC** command from the Windows Recovery Console to find patched system files
- How Malware hides and is installed as a Service
  - o **Service Configuration**
    - Services are loaded on startup by either using svchost.exe or by windows directly launching the application
    - If a service is loaded directly by windows, the associated file name that launches the service can be found in the ImagePath value under the following registry entry
      - **HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\service name**
    - When the service is being launched by svchost.exe, it will be placed in a particular service group, which is then launched by svchost.exe
      - Can be found here: **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Svchost**
      - Contains multiple services that will be launched when the group is loaded by svchost.exe
        - o loaded by following command: **svchost.exe -k netsvcs**
        - o loads all services found under netsvcs group in above key and appear as one process under the process list
        - o each time a new group is loaded by svchost.exe, you will find a new svchost.exe process listed in memory
      - To see via command prompt: **tasklist /SVC**

- Actual filename when launched this way:  
**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\servicename\Parameters\ServiceDll**

#### O Listing and Analyzing the services

- Batch file of configured services on computer:  
<https://www.bleepingcomputer.com/download/getservices/>
  - Unzip file and make sure to run as a user with Administrator privileges
- Make sure to look at following information in Home Search Assistant
  - **SERVICE\_NAME:** name the service goes by and is what it is stored in the registry under
  - **BINARY\_PATH\_NAME:** file being used to launch the service
  - **DISPLAY\_NAME:** name service appears under in the services.msc in the control panel
  - **START\_TYPE:** tells if service is disabled, manually started, or automatically started
- To find the actual file name for a particular service, check the following registry key:  
**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\pnpsvc\Parameters\ServiceDll**
- The value of the ServiceDLL key is the actual file that we want to get rid of.

#### O Removing a Service

- Can be dangerous to your computer
- Service entries are stored in registry under a section called ControlSet (complete copy of the configuration that is used to successfully launch services and other critical files & drivers for Windows) located under the following key:  
**HKEY\_LOCAL\_MACHINE\SYSTEM**
- Will always be at least two ControlSets and one CurrentControlSet
  - One of numbered control sets refers to default configuration that used when computers normally boot
  - Other numbered control set refers to one used when you choose to boot up using the Last Known Good Configuration
  - CurrentControlSet, is an exact mirror of the ControlSet used to boot into Windows, so that if you make a change CurrentControlSet it will automatically appear in the ControlSet it is mirroring and vice-versa
- To know which ControlSet the CurrentControlSet is pointing to you can examine the following key: **HKEY\_LOCAL\_MACHINE\SYSTEM\Select**
  - Contains following values:
    - O **Current:** contains the number of the ControlSet that we are currently using and which CurrentControlSet points to




- o **Default:** contains the number of the ControlSet that Windows uses by default when booting
  - o **Failed:** indicates with ControlSet was the one that failed on last boot. If it is 0, then there was no failures.
  - o **LastKnownGood:** contain the number of the ControlSet that Windows uses when we choose the Last Known Good Configuration
- To manually remove a service from the registry, removed it only from numbered control sets
- Malware may install under these keys (as subkeys called **LEGACY\_svcname**):
  - **HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\Root**
  - **HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet002\Enum\Root**
  - Should be deleted
  - Requires changing of permissions to delete, change security permissions on keys to Everyone (Full) and delete
- **How to use the Windows 8 System Recovery Environment Command Prompt**
  - o **How to start the Recovery Environment Command Prompt in Windows 8**
    - Go to **Command Prompt**
  - o **List of Windows 8 Recovery Environment Command Prompt commands**
    - **attrib:** change permissions on files
    - **bcdboot:** used to quickly set up a system partition, or to repair the boot environment located on the system partition
    - **bcdedit:** Displays and allows you to change how Windows boots up. This command is useful for people who are having trouble with the Windows Boot Manager
    - **cd:** Changes the current directory to another directory
    - **chkdsk:** Checks a hard disk for errors and attempts to repair them
    - **copy:** Copy a file from one location to another
    - **defrag:** defrag hard drive
    - **del:** deletes a file
    - **dir:** Lists files and folders in current directory
    - **diskpart:** Load the Windows disk management program. From this program you can create, delete, shrink, and expand your existing partitions as well as get information about partitions and hard drives
    - **format:** format drives
    - **icacls:** Change file and folder permissions and display or modify access control lists (ACLs)
    - **manage-bde.exe:** Configure BitLocker drive encryption on disk volumes
    - **mkdir:** creates new folder
    - **more:** displays content of a file one page at a time

- **move:** moves a file or folder
- **recover:** Allows attempt to recover files from a damaged drive
- **reg:** Perform Windows Registry operations
- **ren:** Rename a file or folder
- **rd:** Remove empty folder
- **sfc:** Scans and checks the integrity of your Windows files. Useful way to see if a system file is missing or has been tampered with
- **type:** Displays contents of file
- **xcopy:** Copies folders or files to another location
- Windows Program Names:
  - **bmrui.exe:** command will open the System Image Recovery screen to restore Windows from an image
  - **Notepad.exe:** Opens up the Windows Notepad so you can view and edit text files. You can also use the file browser when click the **File -> Open** menus to copy, move, rename, and delete files
  - **Regedit.exe:** Windows Registry Folder
  - **rstrui.exe:** System Restore console where you can restore your computer back to earlier restore points

#### o How to load a registry hive in the Recovery Environment Command Prompt

- Registry hive is loaded using **reg** command
  - For more info on command, type **reg load/?** and press Enter
  - Example:
    - o Type **REG LOAD HKLM\WinSoft**  
:**\Windows\System32\config\software** and press **Enter** to load the HKLM\Software Registry hive as the **WinSoft** key.
    - o Type **regedit.exe** and press **Enter** to start the Windows Registry Editor. When the Registry editor is started, browse to **HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run** key.
    - o Look for the Registry value that is loading the computer infection and delete it.
    - o Close the Windows Registry Editor.
    - o In the command prompt type **REG UNLOAD HKLM\WinSoft** and press **Enter** to unload the Registry hive.
    - o Type **exit** and press **Enter** on your keyboard to go back to the Advanced Options screen. You can then reboot your computer from there.

#### o How to determine the drive letter of your Windows drive

- Use **bcdedit.exe** program by typing **bcdedit** | find “**osdevice**” in Command Prompt and press **Enter**
  - Will display output similar to **os device partition=D:**
    - Letter after **partition=** is the drive where Windows installation resides
  - To change current working directory, type **D:** (or the drive letter shown) and press **Enter**
- **How to start Windows in Safe Mode (Windows 10)**
  - Way of booting up your Windows operating system in order to run administrative and diagnostic tasks on your installation
  - Detailed: <https://www.bleepingcomputer.com/tutorials/how-to-start-windows-10-in-safe-mode-with-networking/>
  - Steps:
    - Press the **Ctrl+Alt+Delete** keys at the same time to enter the Windows security screen
    - While holding down the Shift key, click on the Power button () and then click on **Restart**
    - When Windows 10 restarts, you will be at the **Choose an Option** screen as shown below. At this screen, click on the **Troubleshoot** button to access the Troubleshoot options
    - At the Troubleshoot screen, click on the **Advanced Options** button to open the advanced options screen
    - At the Advanced Options screen, click on the **Startup Settings** option. This will open the Startup Settings screen
    - At the Startup Settings screen, click on the **Restart** button. Windows will now restart
    - After restarting you will be shown a Startup Settings screen. At this screen you should press the number **5** key on your keyboard to enter Safe Mode with Networking
    - Your computer will now reboot. Once rebooted, you will be at a login prompt. Login to access Safe mode with Networking
  - **Problems that could occur from forcing Safe Mode using System Configuration Utility**
    - If stuck with a computer constantly attempting to get into safe mode and not being able to do so:
      - Try renaming your boot.ini file
      - use a boot disk to start your computer
        - <https://www.bleepingcomputer.com/tutorials/create-floppy-boot-disk-in-windows/>

- o If computer does not have a floppy disk, then you can typically boot off the Windows CD that came with your computer in order to access the Windows Recovery Console
    - <https://www.bleepingcomputer.com/tutorials/how-to-install-the-windows-xp-recovery-console/>
  - o Once booted to a command prompt, you would simply rename your **C:\Boot.ini** file to another name like **C:\Boot.ini.bak**
    - To rename in Command Prompt: **ren C:\Boot.ini Boot.ini.bak**
  - o When booting up after the rename, do not be surprised if you see an error stating that you do not have a valid Boot.ini file. When you get back to normal Windows mode, you can then rename **C:\Boot.ini.bak** to **C:\Boot.ini** and run Msconfig again to remove the /safeboot flag
- **How to determine what services are running under a SVCHOST.EXE process**
  - o Using TaskList
    - Click on the **Start** button and then click on the **Run** menu command
    - In the Open: field type **cmd** and press **enter**
    - You will now be presented with a console window. At the command prompt type **tasklist /svc /fi "imagename eq svchost.exe"** and press the **enter** key. You will see a list of the processes on your computer as well as the services that a SVCHOST.EXE process is managing
  - o In Windows 8
    - Go to **Task Manager** (search it up, or do **Ctrl + Shift + Esc**)
    - To see list of processes, click on the **More details** option
    - Scroll down until you see the Windows Processes category and look for the **Service Host** entries
    - Next to each Service Host row process will be a little arrow. Click on this arrow to expand that particular Service Host entry to see what services are running under it
    - Under the expanded Service Host, you will now see the list of services that is running under it. This allows you to easily determine what services a particular SVCHOST process is managing in Windows 8
  - o Advanced Info
    - Services grouped together under a SVCHOST instance are determined by the settings in the following Windows Registry key:  
**HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\SVCHOST**

- Under this key are a set of values that group various services together under one name. Each group is a REG\_MULTI\_SZ Registry value that contains a list of service names that belong to that group
  - Group names/services in the group
    - **LocalService** -> Alerter, WebClient, LmHosts, RemoteRegistry, upnphost, SSDPSRV
    - **NetworkService** -> DnsCache
    - **netsvcs** -> 6to4, AppMgmt, AudioSrv, Browser, CryptSvc, DMServer, DHCP, ERSvc, EventSystem, FastUserSwitchingCompatibility, HidServ, Ias, Iprp, Irmon, LanmanServer, LanmanWorkstation, Messenger, Netman, Nla, Ntmsvc, NWCWorkstation, Nwsapagent, Rasauto, Rasman, Remoteaccess, Schedule, Seclogon, SENS, Sharedaccess, SRService, Tapisrv, Themes, TrkWks, W32Time, WZCSVC, Wmi, WmdmPmSp, winmgmt, TermService, wuauserv, BITS, ShellHWDetection, helpsvc, xmlprov, wscsvc, WmdmPmSN
    - **rpcss** -> RpcSs
    - **imgsvc** -> StiSvc
    - **termsvcs** -> TermService
    - **HTTPFilter** -> HTTPFilter
    - **DcomLaunch** -> DcomLaunch, TermService
  - Each of the service names in these groups corresponds to a service entry under the Windows Registry key:  
**HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services**
  - Under each service entry there is a Parameters subkey containing a ServiceDLL value which corresponds to the DLL used to run the service
- Windows 8 System Restore Guide (to previous state)
    - Search up **Create a restore point** to be brought to the System Protection tab of the System Properties control panel
    - To restore your computer, click on the System Restore button to be presented with the main screen for System Restore. Now click on the Next button to be shown a list of available restore points that you can restore
    - Select the restore point you wish to restore by left-clicking on the entry once. This will then make the **Scan for affected programs** button available. If you click on that button you will be shown a list of programs that will be removed when you perform a restore
    - After ok-ing programs to be deleted, click on **Close** button, and then **Next** button at the restore point selection screen to go to screen asking if you would like to perform the restore
    - Click **Finish** button, and then **Yes** to confirm

#### o To undo System Restore

- Go to **Create a restore point** and click on **System Restore** button
- Select **Undo System Restore** and then click on **Next** button
- To confirm you wish to perform the Undo: Restore Operation, click **Finish** and then **Yes**
- o **Manually Creating Restore Points**
  - Go to **Create a restore point**
  - Click on **Create** button
  - Enter a descriptive name to call the new restore point and click on the **Create** button
  - Click on **Close** button after done
- o **Disabling System Restore**
  - Advised against unless it is after cleaning infections from your computer
    - By disabling System Restore after an infection cleanup you will disable all restore points that may reinfect you if you restore them in the future
    - Enabling System Restore after these potentially infected restore points are deleted allows you to start with a clean slate
  - Go to **Create a restore point**
  - To disable, you need to disable it for each drive currently protected
    - Left-click on each drive listed in the **Protection Settings** box so that it becomes highlighted -> Click on **Configure** button to open up System Protection properties for selected drive
  - Select **Disable system protection** option -> click on **Apply** button and **OK** button
  - Once all drives are disabled, System Restore will be disabled
- o **Enabling System Restore**
  - Follow the steps in the previous section until you are at the System Protection properties for a particular drive
  - Select the **Turn on system protection** option and then press the **Apply** button followed by the **OK** button
  - Perform this step for each drive on your computer for your system to be fully protected
- Information on Windows Sysinternals
  - o <https://docs.microsoft.com/en-us/sysinternals/>
- Information on Networking
  - o <http://techgenix.com/networking/page/2/>