Server 2003 Checklist- Created by Charlie Franks

This checklist is somewhat similar to the Windows 7 checklist, however many tools that exist in Windows 7 don't exist in Windows 2003 server, or are in different locations. Follow this guide for Windows 2003 Server. I created this checklist with a Windows Server 2003 image that was in Portuguese, so the translations may not be 100% correct, just try your best... Sorry for the inconvenience. I didn't have time to create a Table of Contents, hopefully someone can add that in later. It's in a similar order to the Win7 checklist, just follow the steps and you should get anywhere from a 70-100%, anywhere in there should get you set for Round 2. I know I have not included DNS and DHCP guides, I didn't have enough time with the 2008-2003 switch. It's the best I can do, sorry. I've been working like a dog for the past few days to get it ready, and there just wasn't enough time to get it done. There are other guides out there that can help you secure them.

- Before you start
  - Assign half of your total RAM for your VM
  - Research machines are prepped and ready
  - Host machine
  - At least **2** backup machines ready to go (VM's unzipped, but NOT started up)
  - VMware Tools installed
  - Access to the Google Drive

Now, start up the image

THE FIRST THING YOU NEED TO DO IS CHECK TO SEE IF MALWAREBYTES/CCLENAER OR SOMETHING LIKE THAT IS INSTALLED. IF IT IS, UNINSTALL IT IMMEDIATELY, DO NOT USE IT. FOR INSTRUCTIONS ON HOW TO UNINSTALL, SEE NUMBER 4

1. **Clear the DNS Cache**
   a. Open up a command prompt by clicking the **Start** button and typing *cmd*
   b. Select the **cmd.exe** icon, and the command prompt window should open up
   c. Type *ipconfig /flushdns*
2. **Enable Viewing of Hidden Files**
   a. Go to **My Computer**, then go to **Tools**. Select **Folder Options**
   b. Go to the **View** tab
   c. Select the **Show hidden files and folders**
   d. Uncheck the **Hide extensions for known**
   e. Uncheck the **Hide protected OS files**
   f. Uncheck the **Hide empty drives...**

3. **Install MalwareBytes and Process Explorer, and Run MalwareBytes**
   a. First, go to the google doc's site. In case you don't have it, or are too lazy to look it up, here is the link to the google docs page- https://drive.google.com/#folders/0B7FKJ-QDh83GQUFYeDd6cE9lMW8

    i. To download something, **Right Click** it and click **Download**

b. Now, go to the Malware folder, then download **MalwareBytes Installer.exe**

c. We also need **Process Explorer**. Go to the **Processes** folder, and download **Procexp.exe**

d. On **MalwareBytes**, when it gives you the option to update, do it

    i. It may say the installer is out of date, just go along with it. Download and install the newer install version, then Install it.

e. When it finishes installing, uncheck the **Enable Malwarebytes PRO edition** or whatever it is, we don't need that.

f. Select the **Full Scan**, then click **Scan**

g. Scan the **C drive** only

Whiles the Malwarebytes is running, we have to do other stuff, so come back to step g when malwarebytes is done scanning

h. When the scan finishes, select the **Show Results** button, and then make sure each box is selected, and click remove selected.

4. **Stop Network Shares**

a. Open the **Start** menu, and type in *cmd*

b. **Do not hit enter**. Right click, and choose **Run as Administrator**

c. Now, if User account control menu pops up, click yes

d. Type in *net share*

    i. This lists all the active shares from your computer, we are going to kill these now

e. Type *net share /delete INSERT NAME OF NET SHARE HERE*

    i. If the name includes a **$**, that means the share is hidden. Yes you should still delete it, and you have to include the dollar sign in the name to delete it

f. Delete every share that is listed

    i. **IPC$** will be restarted on boot up, this can't be changed, and won't be counted for points ever anyways. The other two default shares are C$ and ADMIN$

5. **Adding or Removing Server Roles**

a. First, read the readme and note down the server roles the server requires

b. Click on **Start**, then click on **Server Manager**

c. Click on **Add or Remove a Role**

d. Click **Next**

e. Select the Server Role you want to remove, then click **Next**

f. Check the bottom check box that says **Remove the _____ server role**

g. Click **Next**, let it remove the server roles

h. Click **Finish**

6. **Firewall**

a. Windows Sever 2003 has a much more basic firewall than Windows 7, its relatively easy to configure
b. Click **Start,** then open the **Control Panel**.
c. Click on **Windows Firewall**
d. Turn the Firewall On, but DO NOT CHECK THE "No exceptions" button
e. Go to the **Exceptions** tab
f. The only exception in there should be **Scoring bot** or **Cyberpatriot**
    i. If anything is in there like netcat or nc or file sharing, uncheck them
g. Go to the **Advanced** tab
h. Click on the **Security Log Configuration** button
    i. Check both boxes at the top
    ii. Increase the Log size limit to **20000 KB**
    iii. Click **OK**
i. Click **OK**

7. **Remote Desktop**
    a. Right click **My Computer** and go to **Properties**
    b. Go to the **Remote** tab
    c. Go to the **Advanced** button
    d. Uncheck **Allow this computer to be controlled…**
    e. Now, uncheck **Allow remote assistance connections…**
    f. Apply, and ok
8. **Power Settings**
    a. Go to the **Control Panel** and go to **Power Options**
    b. Change the **Turn off Monitor** to 5 minutes
    c. Change the **Turn off the hard disk** to 30 minutes
    d. Go to the **Advanced** tab
    e. Select the **Require a Password on Wakeup**
    f. Click **Apply**, then **OK**

9. **Delete Rogue Users**
    a. These steps are running under the assumption you are using Active Directory Users and Groups. To find out how to secure Local Users and Groups, look at the Windows 7 Checklist and follow those steps.
    b. Go to **Start**, type *MMC*, hit enter
    c. Now, go to **File**, **Add/Remove Snap-ins**, scroll down and choose **Active Directory Users and Groups**
    d. Find the users that do not matchup with those in the readme, or default users
        i. Default users are **Administrator**, and **Guest**
    e. Make sure, check again
    f. Now delete them. **Right click** the desired user, and click **Delete**. If a prompt comes up that says **do you want to delete the user's files?** Click **Yes**.

g. We need to rename the guest account (and possibly the Administrator, see below)
    i. Check to see if you are working on the default administrator account. Click **Start**, then on the top right, your username should be displayed. If you are using the default **Administrator**, do NOT change his name. If you are not, rename the **Administrator** account
h. **Right click** the desired user, and click **Rename**. Don't make it guessable, like your name or something. Make it completely random

i. We also need to disable the **Guest** account. **Right click** that account, and click **Disable**
j. Set a password for the remaining user accounts you did not delete
    i. Make this password 8 characters, with 1 number and 1 special letter !@#$%^ etc.

10. Services

a. Before you touch anything with services, make sure you read the readme. If it says you need SMTP running, or SNMP, or Remote Desktop, follow the readme, do not disable ANY of those services, if the readme says so.
b. Open up services by clicking **Start**, then typing *MMC*. Click the MMC icon
c. Now, click **File**, then **Add/Remove Snap-in**.
d. Add in the **Services Snap-in,** then click finish and ok
e. Sort by name, and cross reference with the default services. If you find a service not on this list and are unsure about it, just google it, or follow the steps below
    i. ***DO NOT DELETE ANYTHING TO DO WITH CP, CYBERPATRIOT, SCORING BOT, SAIC etc. Do not even touch them.***
    ii. For other services, **Right Click**, go to **Properties**, and check the **Path to Executable**. It should be on the default page.
    iii. Find the executable file, by putting the location into the **Start** menu, but make sure you don't accidently run it!
    iv. Check the date it was installed, and cross reference the date of installation for Windows 2003 server. If you are still unsure, just google the name of the executable. You will know it is an executable file, because it will end with .exe
f. Default services that are not necessary. IF THE README SAYS OTHERWISE GO BY THE README
g. Here are the Default Services, and their recommended settings for a Windows 7 box-

Service Name	**Required Configuration (CHANGE TO THIS ONE!!)**
ActiveX Installer	Disabled
Adaptive Brightness	Disabled
Application Experience	Manual
Application Identity	Manual
Application Information	Manual

Application Layer Gateway Service	Disabled
Background Intelligent Transfer Service	Manual
Base Filtering Engine	Automatic
BitLocker Drive Encryption Service	Manual
Bitlock Level Backup Engine Service	Disabled
Bluetooth Support Service	Disabled
Certificate Propagation	Disabled
CNG Key Isolation	Manual
COM+ Event System	Manual
COM+ System Application	Manual
Computer Browser	Manual
Credential Manger	Manual
Cryptographic Services	Automatic
DCOM Server Process Launcher	Automatic
Desktop Window Manager Session Manager	Automatic
DHCP Client	Automatic
Diagnostic Policy Service	Disabled
Diagnostic Service Host	Disabled
Diagnostic System Host	Disabled
Disk Defragmenter	Disabled
Distributed Link Tracking Client	Manual
Distributed Transaction Coordinator	Manual
DNS Client	Automatic
Encrypting File System	Manual
Extensible Authentication Protocol	Manual
Fax	Disabled
Function Discovery Provider Host	Manual
Function Discovery Resource Publication	Manual
Group Policy Client	Automatic
Health Key and Certificate Management	Manual
HomeGroup Listener	Disabled
HomeGroup Listener	Disabled
Human Interface Device Access	Disabled
IKE and AuthIP IPsec Keying modules	Manual
Interactive Services Detection	Disabled
Internet Connection Sharing	Disabled
IP Helper	Manual
IPsec Policy Agent	Manual
KtmRm for Distributed Transaction Coordinator	Disabled
Link-Layer Topology Discovery Mapper	Manual
Microsoft .NET Framework NGEN v2.0	Manual
Microsoft iSCSI Initiator Service	Disabled
Microsoft Software Shadow Copy Provider	Disabled
Multimedia Class Scheduler	Disabled
Net.Tcp Port Sharing Service	Disabled

Netlogon	Disabled
Network Access Protection Agent	Manual
Network Connections	Manual
Network List Service	Manual
Network Location Awareness	Manual
Network Store Interface Service	Automatic
Parental Controls	Disabled
Peer Name resolution Protocol	Disabled
Peer Networking Grouping	Disabled
Peer Networking Identity Manager	Disabled
Performance Logs & Alerts	Manual
Plug and Play	Disabled
PnP-X IP Bus Enumerator	Disabled
PNRP Machine Name Publication Service	Disabled
Portable Device Enumerator Service	Disabled
Power	Automatic
Print Spooler	Disabled
Problem Reports and Solutions Control Panel Support	Manual
Program Compatibility Assistant Service	Manual
Protected Storage	Manual
Quality Windows Audio Video Experience	Disabled
Remote Access Auto Connection Manager	Disabled
Remote Access Connection Manager	Disabled
Remote Desktop Configuration	Disabled
Remote Desktop Services	Disabled
Remote Procedure Call (RPC)	Automatic
Remote Procedure Call (RPC) Locator	Manual
Remote Registry	
RIP Routing	^^ Dis-Disabled
Routing and Remote Access	Disabled
RPC Endpoint Mapper	Automatic
Secondary Logon	Disabled
Secure Socket Tunneling Protocol Service	Disabled
Security Accounts Manager	Automatic
Security Center	Automatic
Server	Disabled
Shell Hardware Detection	Disabled
Smart Card	Disabled
Smart Card Removal Policy	Disabled
SNMP Trap	Disabled
Software Protection	Automatic
SPP Notification Service	Manual
SSDP Discovery	Disabled
Superfetch	Manual
System Event Notification Service	Automatic

Tablet PC Input Service	Disabled
Task Scheduler	Disabled
TCP/IP NetBIOS Helper	Disabled
Telephony	Disabled
Telnet	Disabled
Themes	Manual
Thread Ordering Server	Manual
TP AutoConnect Service	Disabled
TP VC Gateway Service	Disabled
TPM Base Services	Disabled
UPnP Device Host	Disabled
User Profile Service	Automatic
Virtual Disk	Manual
VMware Snapshot Provider	Manual
VMware Tools	Automatic
Volume Shadow Copy	Disabled
WebClient	Disabled
Windows Audio	Disabled
Windows Audio Endpoint Builder	Disabled
Windows Backup	Manual
Windows Biometric Service	Disabled
Windows CardSpace	Disabled
Windows Color System	Disabled
Windows Connect Now	Disabled
Windows Defender	Automatic
Windows Driver Foundation	Manual
Windows Error Reporting Service	Manual
Windows Event Collector	Disabled
Windows Event Log	Automatic
Windows Firewall	Automatic
Windows Font Cache	Disabled
Windows Image Acquisition	Disabled
Windows Installer	Manual
Windows Management Instrumentation	Automatic
Windows Media Player Network Sharing Service	Disabled
Windows Modules Installer	Manual
Windows Presentation Foundation	Disabled
Windows Remote Management	Disabled
Windows Search	Automatic
Widows Time	Manual
Windows Update	Automatic
WinHTTP Web Proxy AutoDiscovery Service	Disabled
Wired Autoconfig	Manual
WLAN AutoConfig	Manual
WMI Performance Adapter	Disabled

Workstation	Automatic
WWAN AutoConfig	Manual

The following are common, but not default Windows Services. Disable all of the following, **unless the readme says otherwise!**

i. SMTP
ii. Bonjour
iii. Remote Access Auto Connection manager
iv. Remote Access Connection manager
v. Remote Desktop Config
vi. Remote Desktop services
vii. Remote Registry
viii. RIP routing
ix. World Wide Web Publishing service- This means you have IIS server running

Remember to check on MalwareBytes!!

11. **Processes and Open Ports**
    - **a.** Open ports are one of the most important things to check- because hard to find programs will almost always open ports.
    - **b.** Open up a command prompt, and type *netstat –ano*
        i. This will list the port number, the IP, and the PID
    - **c.** Now, we need **Process Explorer**
        i. Go to the **Downloads** folder, and click on **Procexp.exe**.
            1. It will ask you to agree, just click **Yes**
    - **d.** Click on the **Options** menu, then select **Verify Image Signatures**. This will ensure that an executable actually is made by who they say. They can fake the creator/signature.
    - **e.** Now, go to the **View** tab, and click on **Select Columns**. Make sure the following are selected:
        i. PID
        ii. Company Name
        iii. Verified Signature
        iv. Image Path
    - **f.** Now, we need to figure out what Processes open which Ports
    - **g.** Cross reference the **Open Ports' PID** with the **PID's from Process Explorer**. These are normal **Default Windows Processes**-
        i. System Idle Process

ii. **System**
iii. **Smss.exe**
iv. **Crss.exe**
v. **Services.exe**
vi. **Winnit.exe**
vii. **SearchIndexer.exe**
viii. **Lsass.exe**
ix. **Winlogon.exe**
x. **Dwm.exe**
xi. **Svchost.exe (YOU NEED TO CHECK ALL OF THESE BECAUSE A LOT OF MALWARE LIKES TO HIDE UNDER THIS PROCESS NAME!)**
xii. **Explorer.exe**

h. Make sure you have cross referenced each the **PID's** from the **Command Prompt** and **Process Explorer**
i. If you are unsure if a process is malicious or not, look at the company name, and the Verified Signature. If it is a **SVChost** with **Microsoft** Company name and it is verified, then it is OK. However, we don't want all products from **Microsoft Corporation**, such as a **Telnet Server**, or SMTP server running (Unless the readme says so.) If you are unsure, google it.
j. To end a malicious or unneeded process, the first thing you need to do is write down the Path. This will be important later on
k. Now, we need to right click the process, and select **Kill Process**. This will stop the **Process** from running.
l. However, our job is not done yet, we need to delete the .exe file that was running the process. Take note that you do **NOT** need to do this for verified Microsoft Corporation products, like Telnet or SMTP. However, make sure you have disabled the service
m. Take the file path (I really, really hope you wrote it down…) and click **Start** and copy it in to the search bar. Be careful not to accidently run the .exe file again.
n. We need to delete the file, so go into the folder containing the file, and hold down the **SHIFT + DELETE** keys. This will permanently delete the file, instead of just sending it to the recycle bin.
o. Triple check to make sure you want to delete it
p. Click **Yes**
q. Rinse and repeat until you have checked all of the **Processes**

12. **Disable Write Debugging Information**
    a. Right click **My Computer** and go to **Properties**
    b. Go to the **Advanced** tab
    c. Go to **Startup and Recovery** and go to **Settings**
    d. Change **Write Debugging Information** to **None**

13. **Remove Programs from Startup**.
    i. Go to **Run** (Windows Key + R)
    ii. Type *msconfig*
    iii. Go to the **Startup** tab
        1. Only these should be listed:
            a. Any type of **VMware** software
            b. **Malwarebytes** if you installed it yourself
            c. Anything **Cyberpatriot** or **Scoring Bot** related
        2. We don't need anything else.
        3. Write down the name, and the location of the file. Then, follow the **Processes and Ports** module to find out if it is malicious. If it's something like **Netcat**, **bfk**, **nc**, **ncat**, **telnet**, an alarm should go off in your head. You need to uncheck these immediately
        4. Disable the startup things you don't need- See list above
    iv. This makes it so that the program doesn't restart when we turn the computer off and on again

14. **Adding/Removing Windows Components**
    a. Check the readme to make sure you are removing things you do NOT need.
    b. Open up a Control Panel
    c. Go to the **Programs** menu, then click on **Programs and Features**
    d. On the left pane, select **Turn Windows Features On or Off**
    e. Turn off these features, unless the readme says otherwise-
        i. Games
        ii. Internet Information Services
        iii. Internet Information Services Hostable Web Core
        iv. Media Features
        v. Print and Document Services
        vi. RIP
        vii. SNMP
        viii. Telnet Client
        ix. Telnet Server
        x. TFTP Client/Server
        xi. Windows PowerShell
        xii. XPS Services
        xiii. XPS Viewer

15. **Policies**
    a. Open up the **MMC**
    b. Add in the **Group Policy Object Editor** Snap-in

i. If the computer doesn't have GPOE, then you either need to update it, or it is home basic, in which just skip this step. Although I doubt you will get a home basic image.

c. A few things to note- **READ THESE BEFORE YOU START**

i. In the policy list, I'm not going to include Network and Local Service. **IF YOU SEE THESE IN THE LIST, DO NOT REMOVE THEM**

ii. **DO NOT REMOVE THE CYBERPATRIOT SCORING BOT USER FROM ANYTHING**

iii. **Even if it says no one, DO NOT REMOVE NETWORK/LOCAL SERVICE FROM ANYTHING**

d. Configure the Policies as you see Below

Password Policy	
Enforce Password History	8
Maximum Password Age	14
Minimum Password Age	8
Minimum Password Length	8
Password must meet…	Enabled
Store Passwords using…	Disabled
Account Lockout Policy	
Account Lockout Duration	10
Account Lockout Threshold	7
Reset Account Lockout Counter…	10
User Rights Assignment	
Access credential manager as a…	Admin
Access this computer from the network	No One
Act as part of the OS	No One
Add workstation to domain	No One
Adjust memory quotas for a process	No One
Allow logon locally	Admin
Allow logon through RDS	No One
Backup files/directories	Admin
Bypass traverse checking	No One
Change the system time	No One
Change the time zone	No One
Create a page file	No One
Create a token object	Admin
Create global objects	Admin
Create permanent shared objects	No One
Create symbolic links	Admin

Debug programs	No One
Deny access to this computer…	No One
Deny logon as a batch job	No One
Deny logon as a service	No One
Deny logon locally	No One
Deny logon through RDS	No One
Enable computer and User Accounts…	Admin
Force shutdown from a remote system	No One
Generate security audits	No One
Impersonate a client after authentication	No One
Increase a process working set	No One
Increase scheduling priority	Admin
Load and unload device drivers	Admin
Lock pages in memory	Admin
Logon as a batch job	No One
Logon as a service	No One
Manage auditing and Security log	Admin
Modify an object label	Admin
Modify firmware environment values	Admin
Perform volume maintenance tasks	Admin
Profile single process	Admin
Profile system performance	Admin
Remove computer from docking station	Admin
Replace a process level token	Admin
Restore files and directories	Admin
Shutdown the system	Admin
Synchronize directory service data	Admin
Take Ownership of files…	Admin
Security Options	
Admin Account	If you are logged on as the default Admin, enabled. If not, Disabled
Guest Account	Disabled
Limit Local use of Blank Passwords	Enabled
Rename Admin account	If you are logged on as the default Admin, do not rename it If not, rename it
Rename Guest account	Rename it
Audit the access of…	Enabled
Audit the use of…	Enabled
Force audit policy…	Enabled
Shutdown the machine if unable to log security audits	Disabled
Machine access restrictions	Not Defined

Machine launch restrictions	Not Defined
Allow undock without having to logon	Disabled
Allowed to format and eject removable media	Admin only
Prevent users from installing printer drivers	Enabled
Prevent CD-ROM access	Enabled
Restrict floppy access	Enabled
Allow server operators to schedule tasks	Disabled
LDAP Server signing requirements	Require it
Refuse machine account password changes	Enabled
Digitally encrypt or sign secure channel data	Enabled for all of them
Disable machine account password changes	Enabled
Maximum machine password age	13 days
Require strong (Windows 2000 or later) session key	Enabled
Display user information when the session…	Do not Display user information
Do not display last user name	Enabled
Do not require CTRL + ALT + DEL	Disabled
Message Text for users attempting to logon	leave blank
Message Title for users attempting to logon	leave blank
Number of previous logons to cache	0
Prompt user to change password before expiration	8 days
Require domain controller authentication…	Disabled
Require smart card	Disabled
Smart card removal behavior	No action
Digitally sign communications	Disabled
Send unencrypted passwords to 3rd party SMB servers	Disabled
Amount of Idle time before suspending session	45 minutes
Digitally sign communications	Disabled
Disconnect clients when logon hour expires	Disabled
Server SPN target name	Leave it alone
Allow Anonymous SID/Name Translation	Disabled
Do not allow anonymous enumeration of SAM accounts	Enabled
Do not allow anonymous enumeration of SAM accounts and shares	Enabled
Do not allow storage of passwords…	Enabled
Let everyone permissions apply to anonymous users	Disabled
Name pipes that can be accessed anonymously	Disabled
Remotely accessible ANYTHING	Remove all text

Restrict anonymous access	Enabled
Shares that can be accessed anonymously	Delete everything
Sharing and security	Classic
Allow local system to use…	Disabled
Allow local system to null session fallback	Leave alone

16. **Uninstalling Internet Explorer**
    a. Now technically, Windows 2003 server shouldn't have Internet Explorer Installed, since it's a Windows Server machine, so there wouldn't be a reason to browse the web. So we are going to uninstall it.
    b. Go to the **Control Panel**, then go to **Programs**, then go to **Add/Remove Windows Components**
        i. **I know this was covered earlier, I'm just making sure you actually uninstalled it.**
    c. Find **Internet Explorer**, and uncheck it
    d. Now, click next and uninstall **Internet Explorer**

17. **Power Settings**
    a. Go to the **Control Panel** and go to **System and Security**
    b. Go to the **Power Options** menu
    c. Select the **Require a Password on Wakeup**
    d. Select the **Require a password**
    e. Save changes

18. **Data Execution Prevention**
    a. Go to the **Control Panel**, and go to the Top right corner. Change **View by:** to **Small Icons**
    b. Then, look for the **Performance Icon**
    c. Now, go to **Adjust Visual Effects** option
    d. Navigate to the **Data Execution Prevention** tab
    e. Select **Turn on DEP for All Programs and Services Except those I Select** (don't put any in there)
    f. Apply and ok

19. **IIS Lockdown**
    a. A lot of this tool depends on the readme, and what it says you need. If you need SMTP or something else, then make sure you don't uninstall it.
    b. Get the IIS Lockdown tool from the Google docs
    c. Open the tool, and click **Next**
    d. Click on the **Other**
    e. Remove all of the checks that you do not need (Consult the readme), and click **Next**

f. Uncheck the unneeded Script Maps, and click **Next- For Example-** If you don't need printing, uncheck internet printing
g. Check the **IISAdmin, IIS Samples, MSADC, IISHelp,** and **Scripts**. Check both **Running System Utilities** and **Writing to content directories**. Check *Disable Web Distributed Authorizing,* and Click **Next**
h. Click Next/Finish
i. I'm not too sure how this tool will react with CyberPatriot, so be very careful when you finish that you don't uninstall something you need.

20. Alternate Data Streams (ADS)

a. ADS is alternate data streams. It is a vulnerability in the way NTFS works, so files can hide themselves. We have to get a scanner to remove it
b. Get the **ADSspy** from the google docs. It is on the Cyber Toolkit main page
c. Install **ADSspy**
d. Select **Full Scan (all NTFS drives)** so it scans the whole box. This will let you know what streams come up, and you can remove them from there. You can skip ahead to the next step while it is scanning the image.

21. Malicious Drivers

a. Download the tool **Uniblue DriverScanner** (Its not on google docs :(you have to find it yourself)
b. Install the tool
c. Scan the system- this will let you know if any drivers are out of date, and if there are any malicious drivers on the system. Update them as recommended by the program

22. GMER scan

a. GMER scans for rootkits on the system which is great. Get it from the google docs, in the **Rootkits** folder
b. Run the GMER scan, and remove any programs that it turns up

23. CCleaner

a. Get CCleaner installer from the **Malware** folder in google docs
b. Download and install CCleaner with the recommended settings
c. On the **Intelligently Scan for Cookies to keep** popup menu, click **No**
d. Click **Analyze** and let CCleaner run
e. Check all of the boxes it turns up, and click **Run Cleaner**
f. Now, go to the **Registry** Tab, and click **Scan for Issues**
g. Let it scan, then click all the boxes, and say **Fix Selected Issues**
h. Click **Yes**, and save the .reg file when it comes up

24. Microsoft Baseline Security Analyzer scan

a. Get MBSA from the google docs, under the **Malware** folder

b. Install MBSA using recommended settings
c. Startup MBSA, and click **Scan a Computer**
d. Find out what MBSA says your image is not good with, and fix it

25. Installing an Anti-Virus

a. Download the **AVG installer.exe** from the google docs, in the **Antivirus** folder
b. Install **AVG.** Choose **Basic Protection**, and **Custom Install**
   i. Uncheck each box from the custom install, we don't want any of their bloatware
   ii. Uncheck each box from the **Component Selection**
   iii. Finish Installing it

DO NOT TURN OFF YOUR COMPUTER WHEN IT IS INSTALLING UPDATES. MAKE SURE YOU ARE PLUGGED IN

26. Updating via Control Panel

a. Open up the **Control Panel**, and click **System and Security**
   i. You may have the other version, just click **Windows Update**
   ii. Under **Windows Update**, click **Check for Updates**.
   iii. Install all of the required updates

27. Service Packs

a. Get the Services packs from the Google Docs, in the **Service Packs** folder. Make sure you have selected the right operating system
b. Install the service pack by double clicking it and let it run.

The following are registry keys and advanced policies. Follow exactly what they say, or you will mess up your image. Be extremely careful and triple check what you are doing

28. Advanced Policies

a. Open up an **MMC**, Add in the **Group Policy Object Editor** Snap-in, Go to **Computer Configuration**, then go to **Administrative Templates**. I don't know exactly where all of these are located, and I don't have time to look them up right now, the checklist deadline is coming up fast. Try to find all of these, and apply them as such.

1. Prevent redirection of USB devices- Enabled
2. Allow Printers to be published- Disabled
3. Allow Print Spooler to Accept Client Connections- Disabled
4. Disallow Installation of Printers using Kernel-mode Drivers- Enabled
5. Prevent Metadata Retrieval from the Internet- Enabled

6. Enforce Disk Quota Limit- Enabled
7. Lock Enhanced Storage When the Computer is locked- Enabled
8. Enable NTFS Page file Encryption- Enabled
9. Require a Password when the Computer Wakes- Enabled
10. Detect Application Installers that need to be run as Admin- Enabled
12. Allow Users to Access Troubleshooting Content- Disabled
13. Allow Users to Access and Run Troubleshooting Wizards- Disabled
14. Prevent Access to 16-bit Applications- Enabled
15. Turn off auto play- Enabled
16. Prevent the User from Running Backup Status and Configuration Program- Enabled
17. Prevent Backing up to Network Location- Enabled
18. Prevent Backing up to Optical Media- Enabled
19. Prevent the Computer from Joining a Home group- Enabled
20. Disable Remote Desktop Sharing- Enabled
21. Prohibit New Task Creation- Enabled
22. Always Install with Elevated Privileges- Disabled
23. Prohibit User Installs- Enabled
24. Allow Remote Shell Access- Disabled
25. Disable Automatic Install of Internet Explorer Components- Enabled
26. Always Prompt Client for a Password on Connection- Enabled
27. Encryption levels- High (128 bit)
28. Password Protect the Screensaver- Enabled

Hopefully at this point you guys are set to go. If you feel nervous with an 80 or 90, try looking online for tools like MBSA or nessus, and use them to scan your box and find vulnerabilities you may have missed.