Windows Security I

James Madison University Dept. of Computer Science

June 4, 2013

1 Introduction

The Windows platform is the platform that is most likely to be running on any given workstation in the United States. Windows Servers are also widely used. This means securing Windows machines and services is big business, especially for Microsoft. Many different software tools have been created to help secure Microsoft computers, and many tools come built into Windows already.

To note, all software mentioned in this exercise will be available on the desktop of your Virtual Machine.

2 Microsoft Baseline Security Analyzer

MBSA is a tool used to determine if a given microsoft computer is up to date or has obvious misconfigurations. Examples of things MBSA could discover is that the computer is out of date and requires software updates. MBSA could also discover if an administrator account requires no password to log in or if an administrator has an extremely weak password (like *password*). These kinds of misconfigurations would allow an attacker to gain control of the computer with almost no effort.

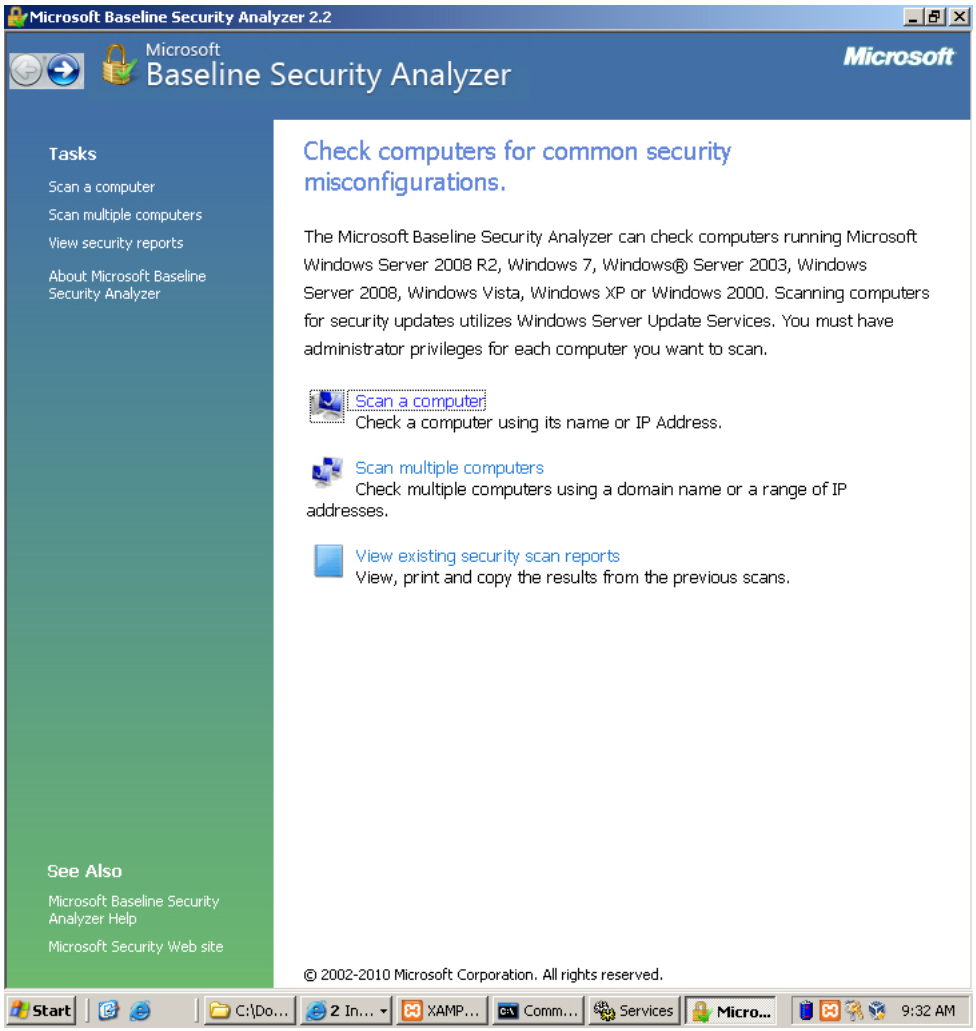

Figure 1: Press Scan this computer.

2.1 Using MBSA

Microsoft Baseline Security Analyzer is very easy to use. After starting the program **Figure 1** shows you what you will see. To Scan your own computer press the Scan your computer button link. **Figure 2** shows the menu for scanning your computer. The default scan is sufficient to determine what may be wrong with your computer. Press Start Scan and wait for your results.

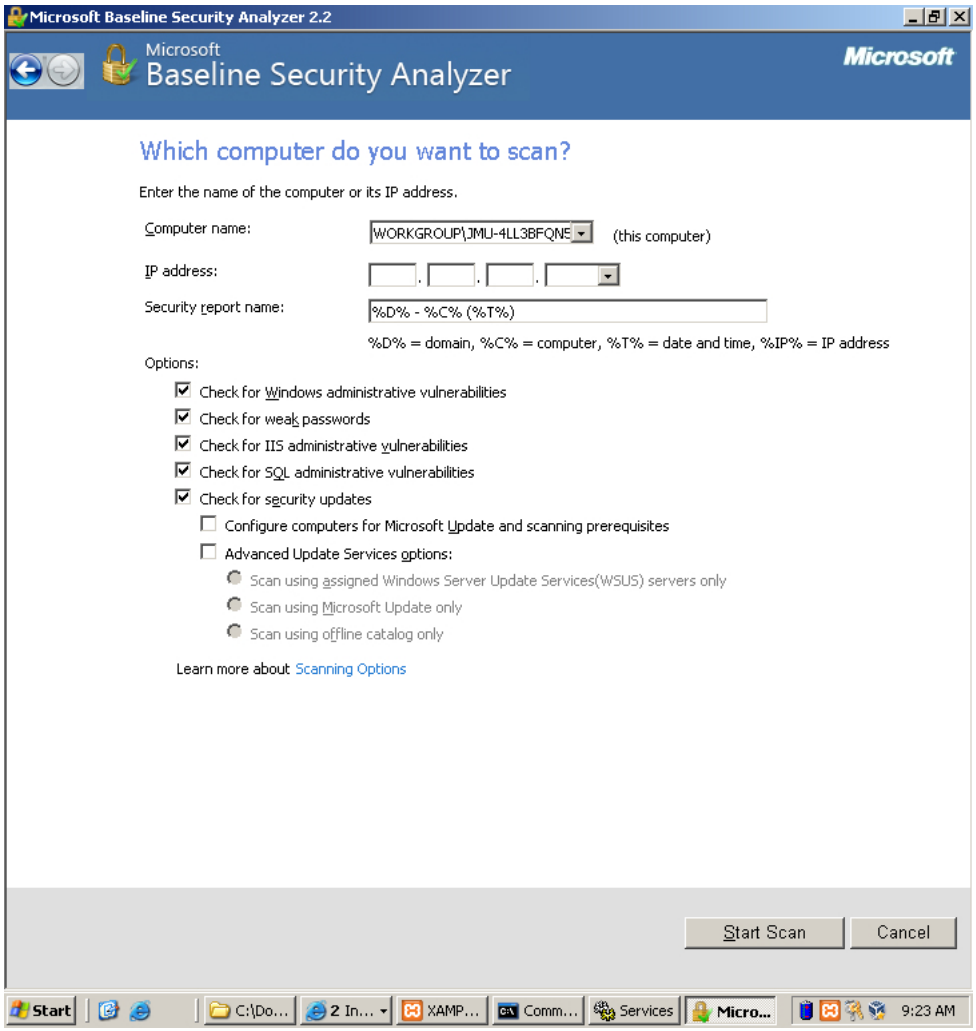

Figure 2: Press Start Scan. This jibberish in the *Computer Name* field means the computer you are are currently using.

2.2 Scan Results

The results from the MBSA scan may seem overwhelming at first but they can be easily understood after a couple minutes of practice. **Figure 3** shows sample output of a scan MBSA scan on newly installed Windows Server 2003 machine. Issues can be identified in the Score column. A green check means that the security configuration test was passed. A Red X means that the security configuration test was failed. A blue exclamation point means that the test was failed but the problem is not critical.

MBSA will also tell you how to fix these issues. One of your blue checks

should say *Microsoft Firewall is disabled.* You could follow the steps listed in *How do I correct this?* to enable your firewall, but we will enable the firewall ourselves later.

Re-run the scan and determine if the Windows Firewall score column has changed to a green check mark.

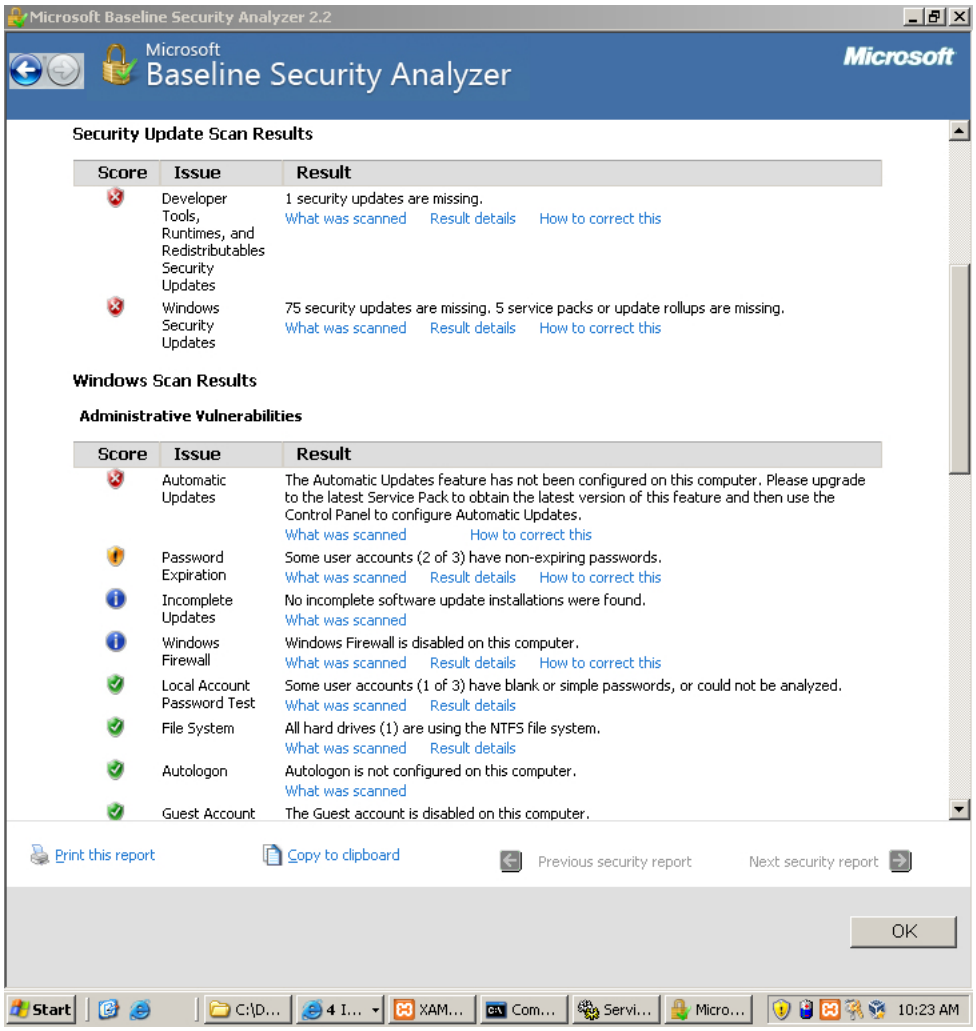

Figure 3: Scan Results

3 Patching

You will notice in the above MBSA scan that the *Security Update Scan Results* section of **Figure 3** mentions that the computer scored a red X for Windows Se-

curity Updates. This is a serious problem. Microsoft releases updates regularly that prevent hackers from attacking your computer with known vulnerabilities. When new attacks are released, Microsoft fixes the issue by determining how the hack worked and then changing their code to prevent it.

Applying these updates is called "patching". You can apply patches by either downloading them through Windows Update or by using a program called CTUpdate. Windows Update requires that you have an internet connection and makes it extremely simple to apply patches. CTUpdate allows for more fine-grained control of which patches you install and does not require an internet connection, but it is not as easy to use and may take more time.

3.1 CTUpdate

CT Update is a program for updating your Operating System while offline. It is free to download and use from *http://w3stu.cs.jmu.edu/johns3ej/wsusoffline82.zip*, but you can find it on your desktop as well. It can take a long time to update because there may be many security patches to apply.

Run *UpdateGenerator.exe* in the CTUpdate folder. You should see a Graphical User Interface like the one in **Figure 4**.

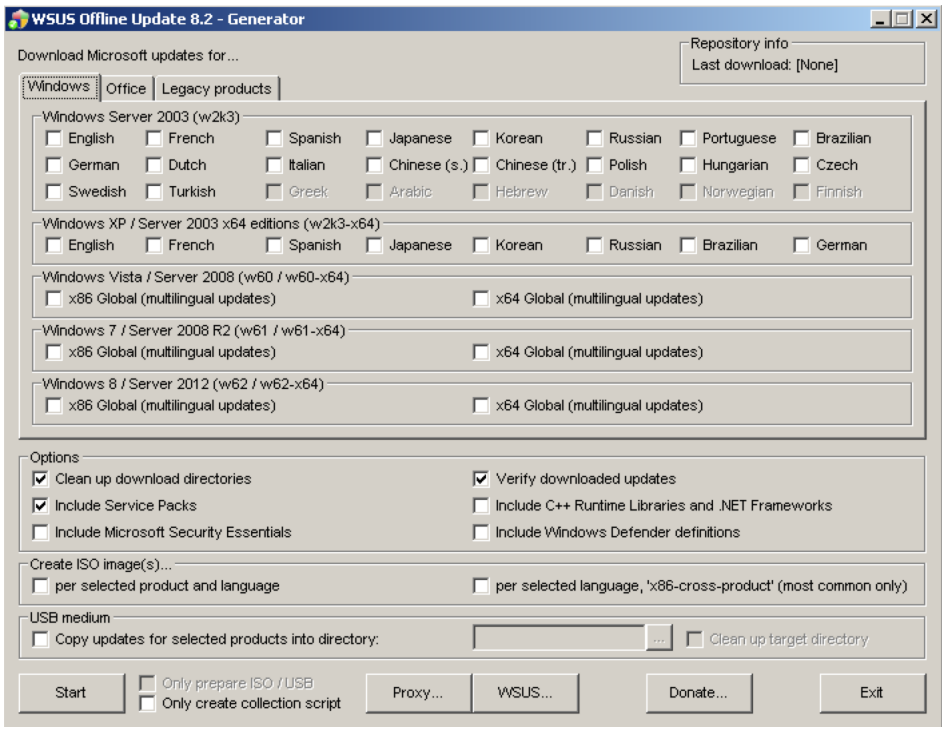

Figure 4: CT Update Graphical User Interface

After the Graphical User Interface loads, in the "Options" section, make sure to check all options and make sure you check your Language preferences at the top. If we were to update using CTUpdate, we would press Start right now but we will update a different way. It should take around twenty-five to thirty minutes to update this way.

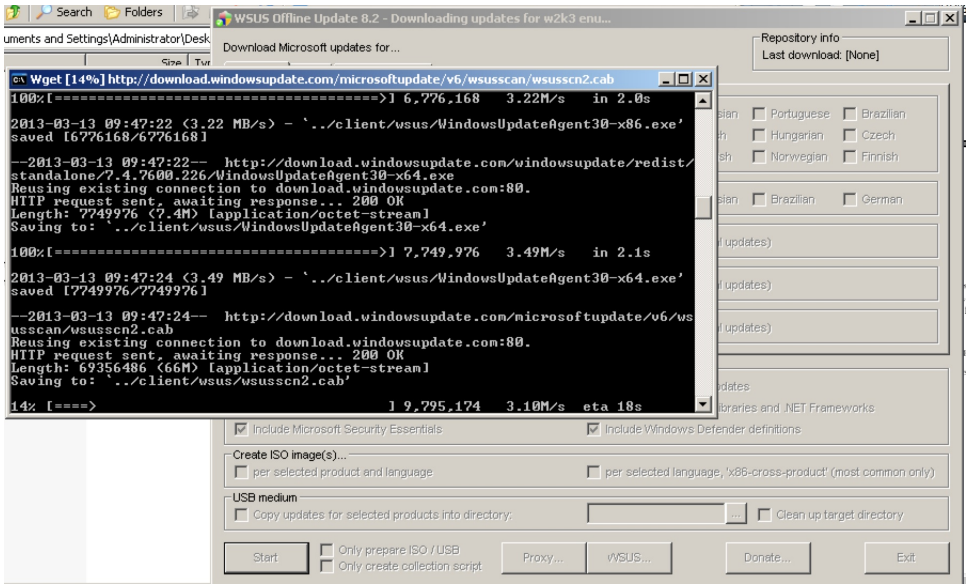

Figure 5: Updating Process

3.2 Windows Update

Windows Update is located in the Start Menu under the *All Programs* tab. You can see it in **Figure 6**. Updating with Windows Update is incredibly easy. After clicking windows update, a web browser will open. Press "Express Update" and follow the wizard. After doing this your computer will begin patching itself. It may take a long time to do complete patching (just like CT Update).

If Windows Update says you need to install a *Service Pack* it may take a long time to complete. Service Packs are large collections of patches. Installing one of these means that your computer is very out of date and most likely a easy target to even an un-experienced hacker.

Figure 6: Start Menu showing Windows Update

Please choose either CT Update or Windows Update and Update your machine at this time. While it is updating, go on to the next section on Anti-Virus.

4 Anti-Virus

Anti-virus is an important tool in every defender's toolbox. The interworkings of Anti-virus is very simple. It works by collecting signatures or samples of many different pieces of malware. When scanning a file for viruses, it takes the signature of the file it is scanning and compares it to the list of signatures it already knows. If there is a match then the software knows it has found a virus. There are many companies that offer anti-virus, but we will use a free anti-virus solution provided by Microsoft.

Windows Server 2003 can use the anti-virus program called Windows Defender. It can be downloaded from *http://www.microsoft.com/en-us/download/confirmation.aspx?id=17* but it is also pre-installed to your desktop. There should be a file called ScanMe.txt in your *My Documents* folder.

Double click the icon on your desktop and scanning your computer is as easy as hitting the scan button in **Figure 7**.

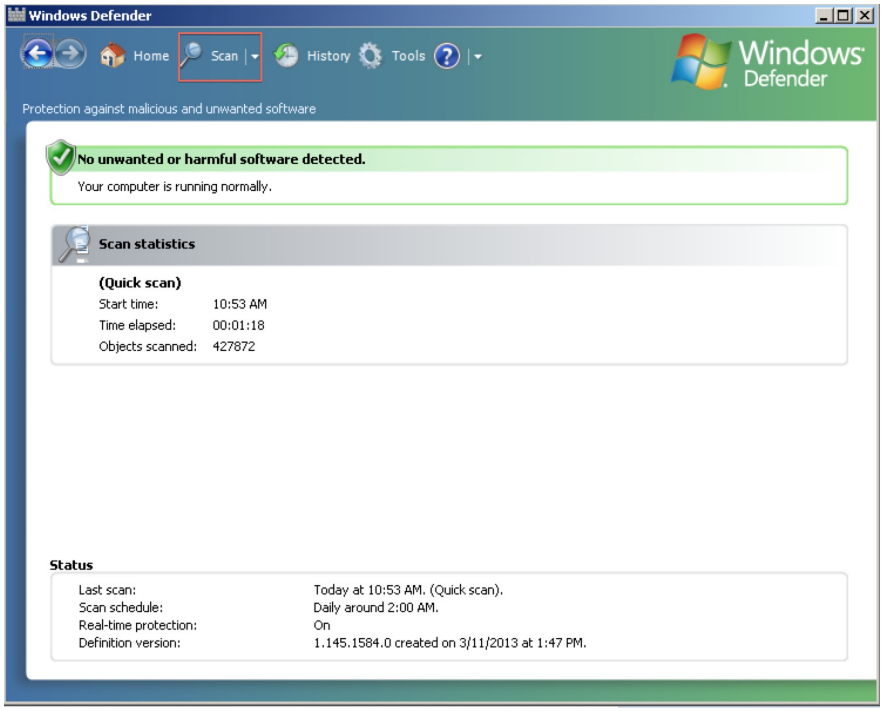

Figure 7: Microsoft Defender

It is also possible to have more fine-grained control over what you are scanning. I'm sure you noticed that Windows Defender has caught some malicious files that were loaded on your computer. Use Windows Defender to remove them.

5 Password Policy, Users, and Groups

All of these are lumped together into one section because all of them have to deal with Authentication. When securing a computer, all of these things are important to be mindful of if you want to keep people out of your computer. Nobody needs to use sophisticated techniques to attack a computer when the administrator password is *password*.

5.1 Policy

Windows Server 2003 comes with lots of software to manage all password and account policy. An example of something that we will manage is password length. An administrator may want to ensure that a user cannot use a password that is very short because a attack may be able to guess it easily. This is something that is possible to control.

As you can see in **Figure 8**, by default, the password policy is extremely weak. It does not have any length requirement for passwords and has no complexity requirements.

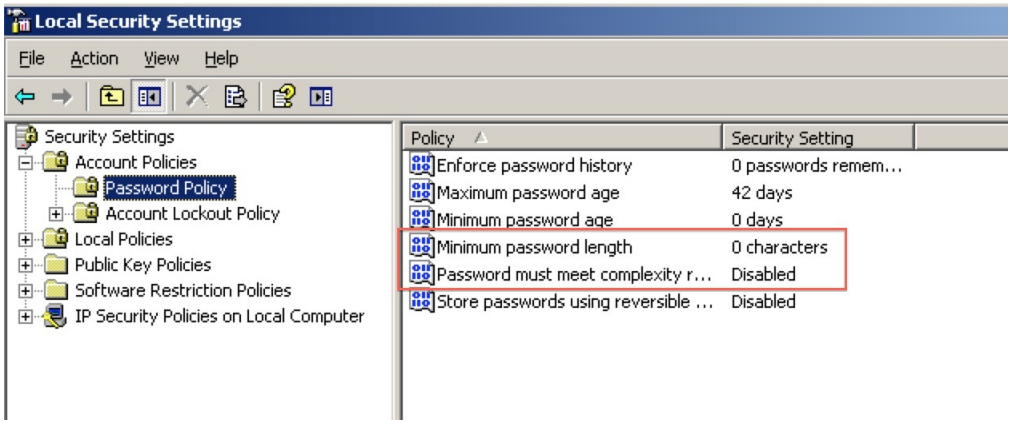

Figure 8: No Password complexity or length requirements.

To set a minimum password length, double click on *Minimum password length* and set it to eight. To require uses to pick strong passwords that meet Microsoft's password complexity requirements, double click on*Password must meet complexity requirement* and select Enabled.

The most important part of changing password policy is now to *change all passwords*. Passwords that were created with the old policy may not abide by the new rules you just created. If this is the case, a user could be using a password with 0 characters! This is just waiting to be hacked!

5.2 Managing Users

In the Administrator panel, there is also a tab that says *Computer Management*. This is an extremely important tab. We will be using it to manage what users can access the computer. Navigate to *Local Users an Groups* in the *System Tools* section. As you can see in **Figure 9**, you can use this to determine the accounts on the computer.

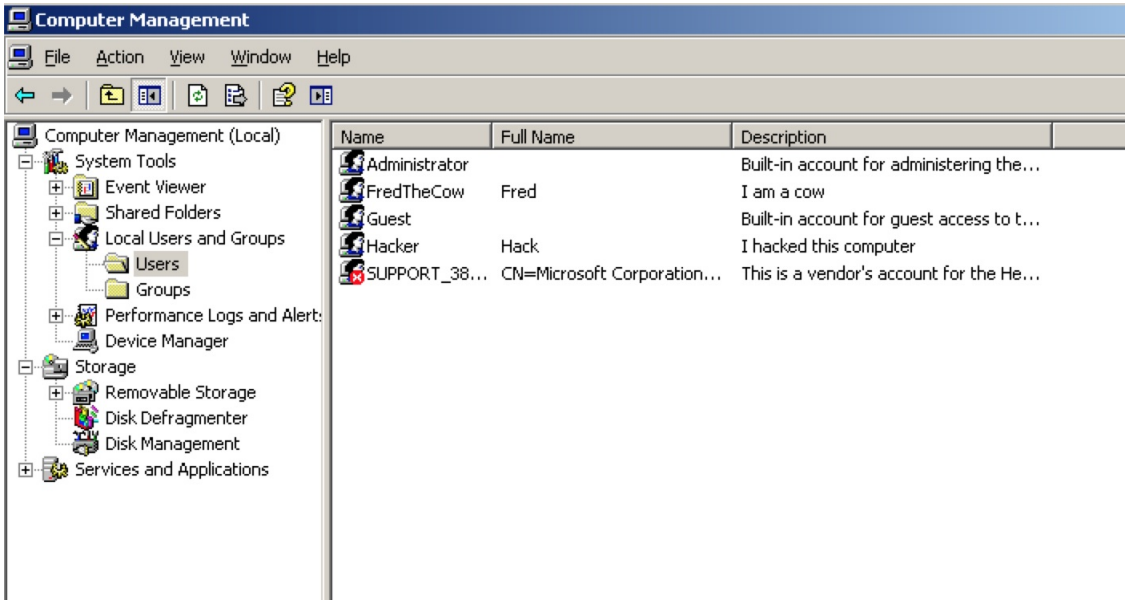

Figure 9: The right side shows the user accounts on the computer.

It is important to disable accounts that you do not want people to log into your computer with. This also includes the Guest accounts. *Hacker*, *Guest*, and *FredTheCow* are not legitimate users and *SUPPORT_38* is not necessary. Delete *FredTheCow*, *Support_38*, and *Hacker* by right clicking on them and clicking "Delete". The *Guest* account comes built into Windows and cannot be removed, but it can be disabled. *Figure 10* shows you how easy it is to disable the guest account.

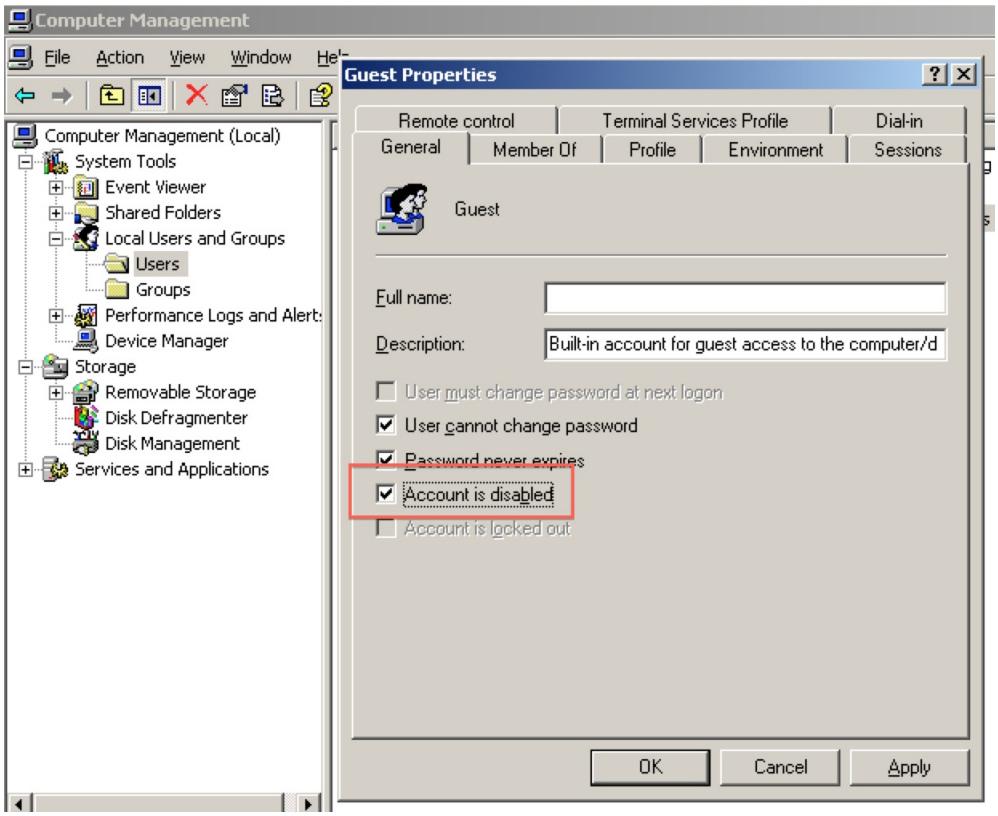

Figure 10: Select Account is disabled and hit apply.

It is important to disable the guest account because, with a guest account, a hacker has a foothold in your system. A hacke

Lastly, it is important to make sure each of these accounts creates a new password that will abide by the password policy we created in the previous section.

In order to ensure each user changes their password double click on each user account, unselect the "Password never Expires" checkbox and select the "User must change password on next login" checkbox.

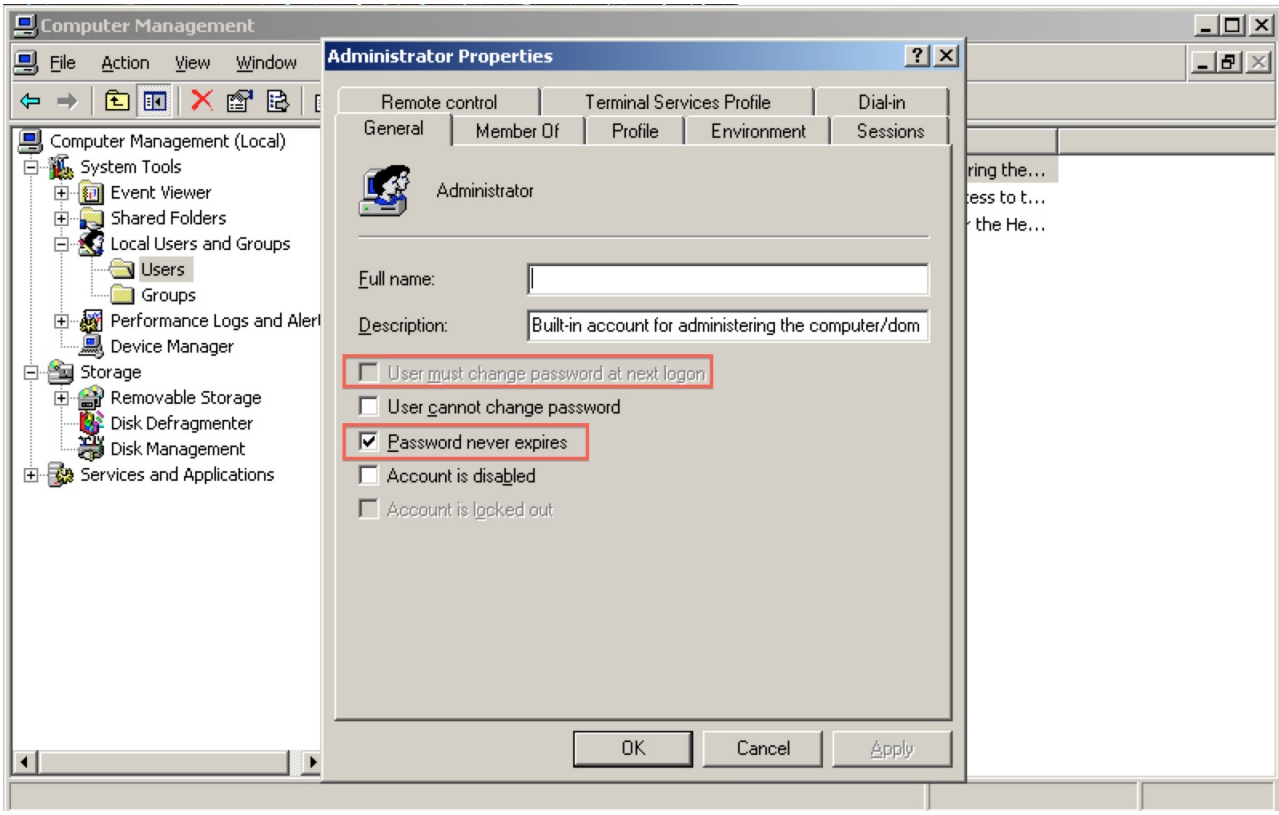

Figure 11: Unselect Password never expires and then select User Must Change.

6 Changing Passwords

Next, as the administrator, we must change your passowrd. Changing your password is very simple to do and very important. Once again, the changes to your password policy will not be reflected in your until your password is changed. To change your own password follow these steps. You should also force all other uses to change their password at this point.

1. Click Start, right-click Administrative Tools, and then click Open. Administrative Tools opens.

2. Double-click Computer Management, click Local Users and Groups, and in the details pane, double-click Users. The Users folder opens.

3. In the details pane, right-click the account that you want to change, and click Set Password. A warning dialog box opens. Read the information

to determine whether you want to proceed with the step to change the password.

4. In New Password, type a password. In Confirm password, retype the password, and then click OK.

7 Services

Knowing what services are running on your windows machine is very important. Having extra services running that are not necessary may add vulnerabilities to your machine. The more services that are running on a machine means the more services you must protect and secure. By default, many software packages install many extra services that you may not want to be running.

7.1 What Services are running?

All Microsoft Windows Server Editions have Graphical User Interfaces to help manage the machines services. The GUI can be accessed in the Start Menu under Administrative Tools by clicking on Services. Figure 1 shows how to access the services GUI from the start menu.

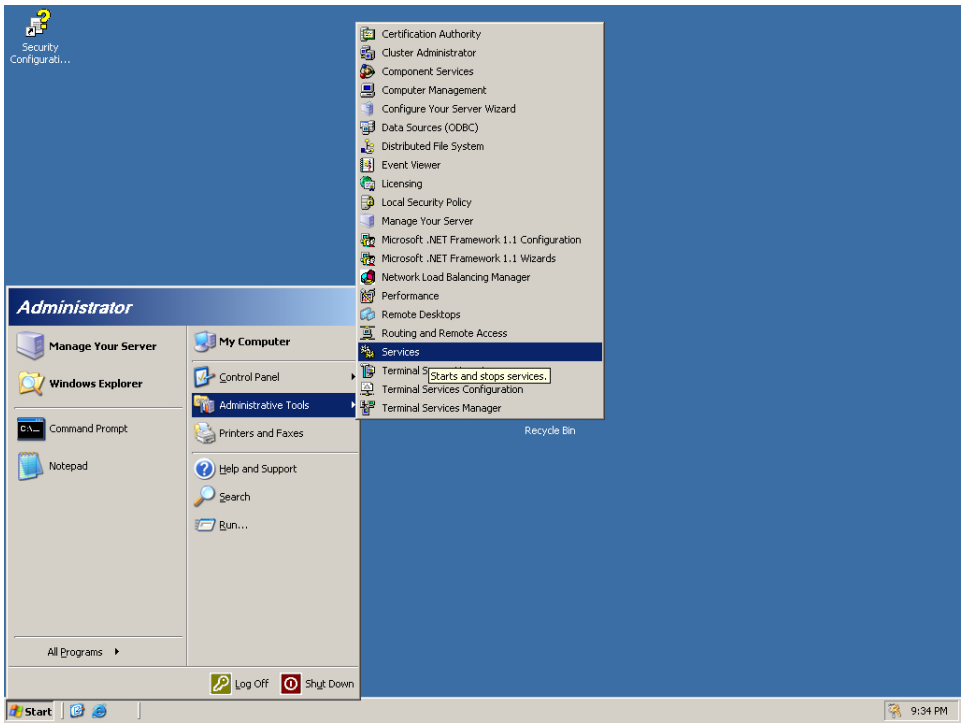

Figure 12: Click on Services to manage what services are running

By default, the list of things on this list is large and difficult to sort through. By default, Windows Firewall is Disabled. This is a very important service. To turn it on, double click on it and change "Disabled" to "Automatic". Figure 2 shows how to do this.

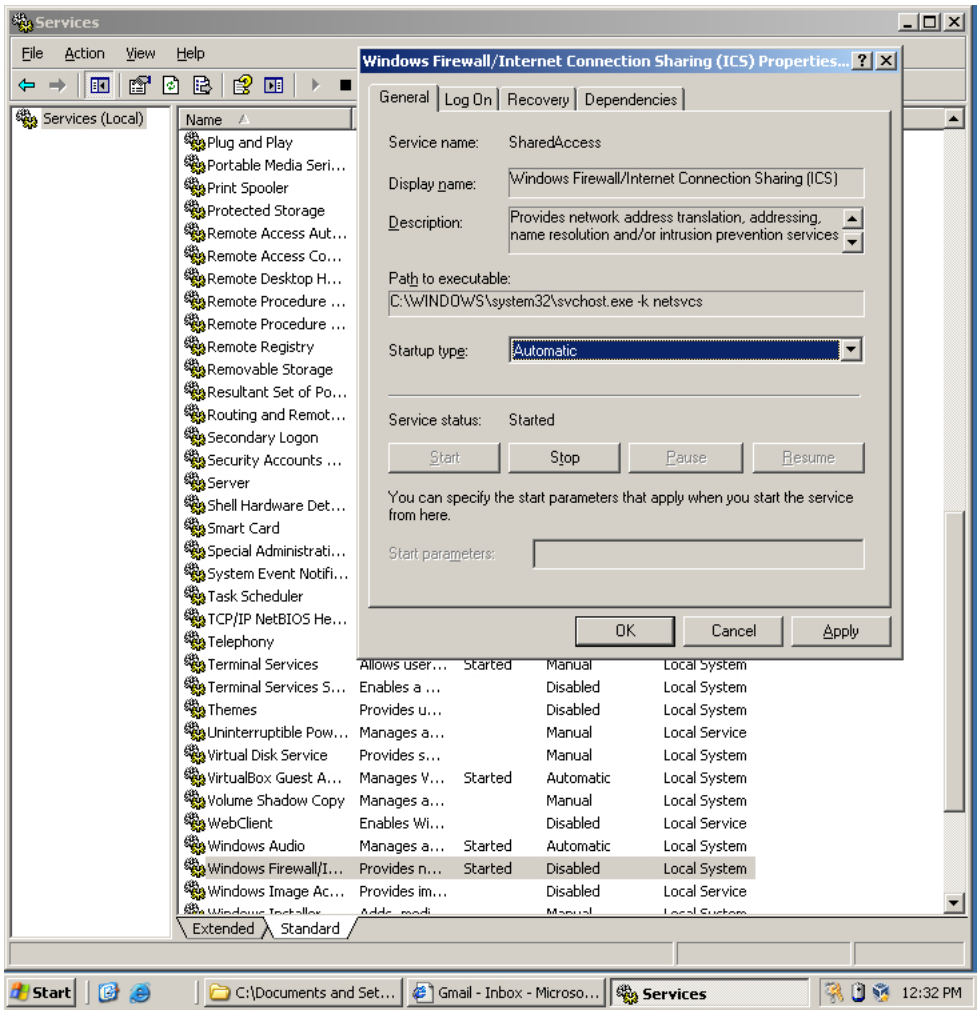

Figure 13: Change Setup type to Automatic to turn the firewall on.

You may also notice that the *File Transfer Protocol* and *Telnet Protocol* may be enabled. It is very important that these should be disabled and they should always be disabled. These protocols are used so remote users can authenticate and use your computer. Remote Authentication is a standard practice, but FTP and Telnet do not do it securely. Telnet and FTP do not encrypt the password used to authenticate with the server when they are sending it over the internet. Any attacker between the computer that is logging in and the server could eavesdrop and read the password while it is being sent over the internet. This would allow an attacker to log in to your server and not need to hack it. If you see SSH or Very Security File Transfer Protocol, these services are okay to use.

8 Firewalls

All Windows distributions come with a built in host based firewall that you can configure. In the real world many companies buy expensive machines that are only a firewall. Even though the Windows Firewall is not expensive and dedicated hardware, it is a great line of defense to keep attackers from accessing ports on your computer that may have a vulnerability.

It is very easy to understand how a firewall works. People connect to your computer through *ports* and a firewall blocks ports. An easy way to think about ports is a lot of tiny mailboxes. Anytime someone wants to communicate with your server they put mail in your mailbox. Each port is for a different purpose. A firewall will block these mailboxes so nobody can put anything in them. This decreases the surface area a hacker could attack you with.

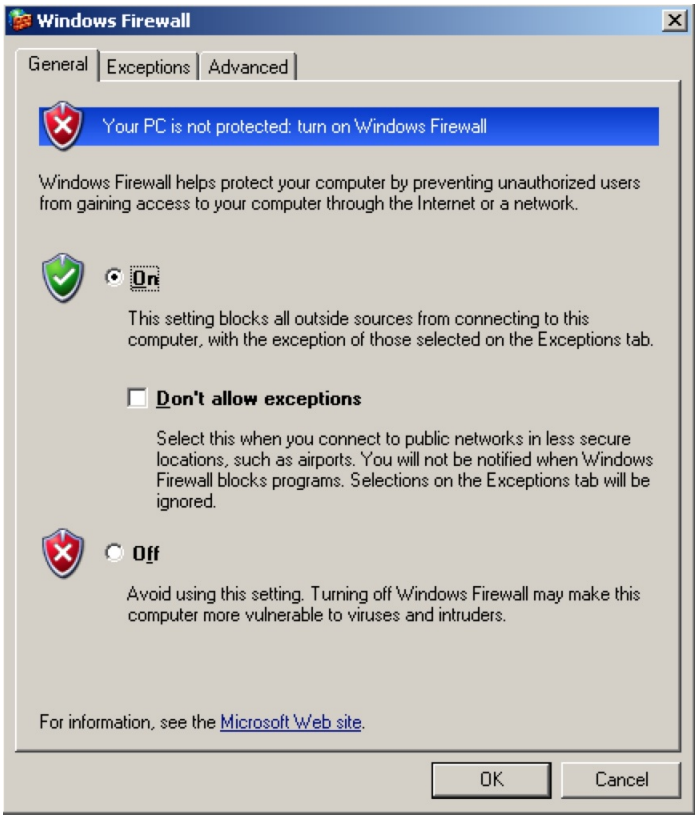

Figure 14: Change Setup type to Automatic to turn the firewall on.

To use the Windows Firewall, you must first enable it. Windows Firewall can be found in the *Control Panel*. After clicking on *Windows Firewall* you

should see a user interface like the one in **Figure 3**. Change Windows Firewall from *off* to *on* and then click the Advanced tab at the top of the interface.

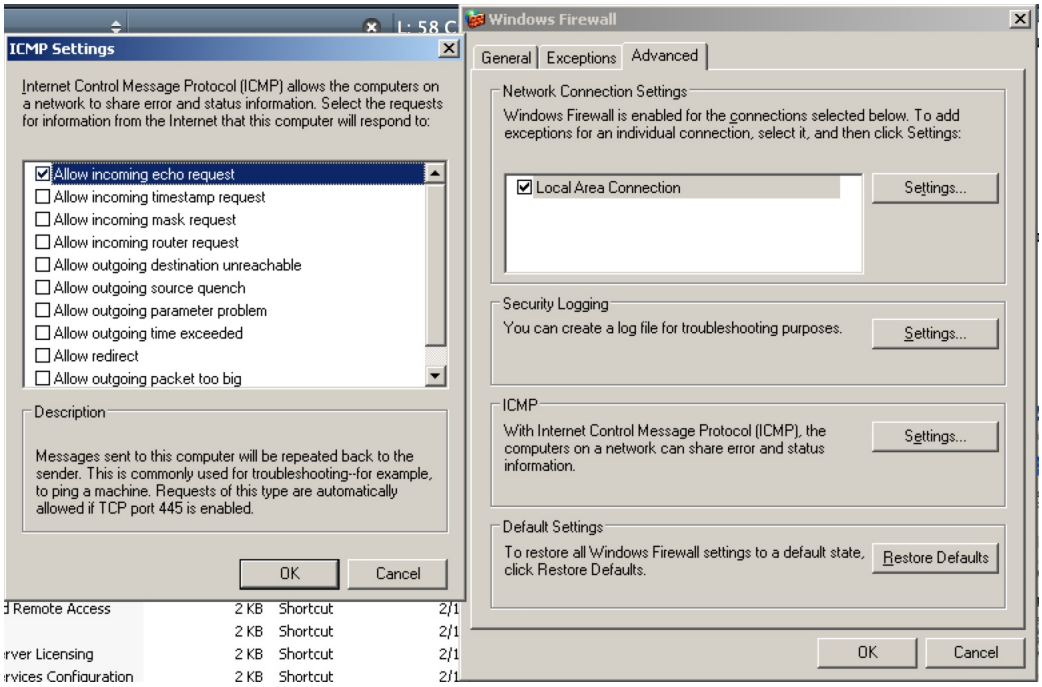

Figure 15: Change Setup type to Automatic to turn the firewall on.

In the advanced tab, click *Settings* within the *ICMP* settings. When the ICMP Settings user interface pops up select *Allow incoming echo requests* and then Ok. This allows other computers to *ping* your computer. Ping is special and does not use a port, but your firewall is still able to block it. Next click on the Exceptions tab at the top of the Windows Firewall.

Click on the *Add Port* button in the Exceptions tab to add exceptions to the Firewall. By default, Windows Firewall will block all ports and you only open the ones you need. This is much easier than leaving all open and blocking the ones you don't want because there are 65,536 ports. Your computer is running a webserver. Webservers generally use port 80 to communicate with computers that request webpages.

Figure 5 shows you how to unblock port 80. After pressing Ok in Windows Firewall, your Firewall changes will take affect and your firewall will be active.

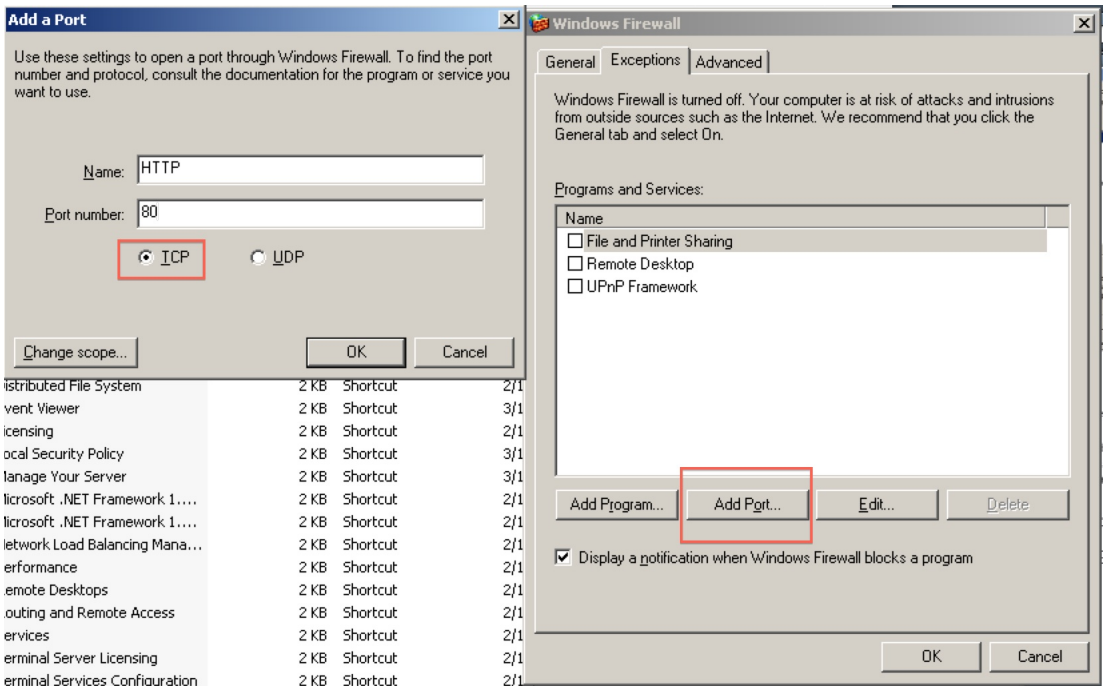

Figure 16: Make sure to select TCP after hitting pressing Add Port.

9 Conclusion

We have performed basic hardening on this computer and an attacker will either have to resort to more advanced attacks, or simply move on.

It is a good idea to re-run the MBSA scan from the very first section and see how much you have improved. If there are any mistakes you made, MBSA can be used to help you recognized them.

There are still many more things defenders can do to protect themselves. This tutorial has only made your computer safe from the most obvious and easiest attacks. A skilled group of defenders jobs are never over, and they will attempt to attack their own network, setup intrusion detection systems, and constantly monitor their network. These topics will be covered in greater depth in later exercises and lectures.