# 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 Examples of things MBSA could discover is that the computer is out of date and requires software updates.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.

🐣 Microsoft Baseline Security Analyzer 2.2	
👀 🔮 Baseline Secu	rity Analyzer <i>Microsoft</i>
Which computer	do you want to scan?
Enter the name of the comput	er or its IP address.
Computer name:	WORKGROUP\JMU-4LL3BFQN5 (this computer)
<u>I</u> P address:	
Security report name:	%D% - %C% (%T%)
Options: Check for Windows a Check for weak pass Check for IIS adminis Check for SQL admini Check for security up Configure compu Advanced Updat Scan using ag Scan using of Learn more about Scann	%D% = domain, %C% = computer, %T% = date and time, %IP% = IP address dministrative vulnerabilities words trative vulnerabilities strative vulnerabilities idates ters for Microsoft Update and scanning prerequisites a Services gptions: signed Windows Server Update Services(WSUS) servers only icrosoft Update only ifline catalog only ing Options
	<u>S</u> tart Scan Cancel
🎒 Start 🛛 🚱 🧉 👘 🎦 C:\Do 🛛 🥌	2 In 🗸 🔀 XAMP 🔤 Comm 🎕 Services 🔒 Micro 🏮 🔀 📆 🥸 9:23 AM

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 finegrained 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 *Update Generator.exe* in the CTUpdate folder. You should see a Graphical User Interface like the one in **Figure 4**.

🗊 WSUS Offline Update 8.2 - Generator	×
Download Microsoft updates for           Windows         Office         Legacy products	
Windows Server 2003 (w2k3)         English       French         Spanish       Japanese         Korean       Russian         Polish       Hungarian         Czech         Swedish       Turkish         Greek       Arabic	
Windows XP / Server 2003 x64 editions (w2k3-x64) English French Spanish Japanese Korean Russian Brazilian German	
Windows Vista / Server 2008 (w60 / w60-x64)         x86 Global (multilingual updates)         x64 Global (multilingual updates)	
Windows 7 / Server 2008 R2 (w61 / w61-x64)         x86 Global (multilingual updates)         x84 Global (multilingual updates)	
Windows 8 / Server 2012 (w62 / w62-x64) x86 Global (multilingual updates) x64 Global (multilingual updates)	
Options       Options       Image: Clean up download directories       Image: Clean up download directories	
✓ Include Service Packs       ☐ Include C++ Runtime Libraries and .NET Frameworks         ☐ Include Microsoft Security Essentials       ☐ Include Windows Defender definitions	
Create ISO inage(s)  Create ISO inage(s)  per selected product and language  (most common only	)
USB medium  Copy updates for selected products into directory:  Copy u	
Start         Only prepare ISO / USB         Proxy         WSUS         Donate         Exit	

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.

😰 🔎 Search 🏀 Folders 🛛 🖄 🍙 WSUS Offline Update 8.2 - Downloading updates for w2k3 enu				
uments and Settings(Administrator)Desk Size Trut	Repository info Last download: [None]			
📾 Wget [14%] http://download.windowsupdate.com/microsoftupdate/v6/wsusscan/wsusscn2.cab	≤			
100%[>] 6,776,168 3.22M/s in 2.0s		For For		
2013-03-13 09:47:22 (3.22 MB/s) - `/client/wsus/WindowsUpdateAgent30-x86.exe' saved [6776168/6776168]	डाक्षा क्षेत्र	Hungarian Czech		
-2013-03-13 09:47:22 http://download.vindowsupdate.com/vindowsupdate/redist/ standalone/7.41.7600.226/WindowsUpdateAgent30-x64.exe Newsing.existing.connection to download vyandowsupdate.com:80.	sh I siar	Norwegian Finnish		
Length: "?749976 (7.4M) [application/octet-strean] Saving to: `/client/wsus/WindowsUpdateAgent30-x64.exe'				
100%[>] 7,749,976 3.49M/s in 2.1s	n uş	Justes J		
2013-03-13 09:47:24 (3.49 MB/s) - `/client/wsus/WindowsUpdateAgent30-x64.exe' saved [??499?6/?7499?6]				
2013-03-13 09:47:24 http://download.vindowsupdate.com/nicrosoftupdate/v6/ws usscan/wsusscn2.cab Reusing existing connection to download.windowsupdate.com:80. HTTP request sent, awaiting response 200 OK Length: 6/356486, /664D, Lapplication/vocet-stream]	ıl uş	odates)		
14% [====> ] 9,795,174 3.10M/s eta 18s	idat ibra	tes aries and NET Frameworks		
r Include Microsoft Security Essentials 🔽 Include Windows (	)efend	er definitions		
Create ISO image(s)				
per selected product and language	age,'x	86-cross-product' (most common only)		
USB medium Copy updates for selected products into directory.		🗖 Clean up target directory		
Start Only prepare ISO / USB Proxy VVSUS		Donate Exit		

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**.

Windows Defender		
🕞 🏵 🏠 Home 🔎	Scan   🔹 🦀 History 🔇 Tools 🕐   🔹	<b>Windows</b> Defender
Protection against malicious and	unwanted software	
No unwanted or ha	miul software detected.	
Your computer is runn	ng normally.	
<b>Scan statistics</b>		
(Quick scan)		
Start time:	10:53 AM	
Time elapsed:	00:01:18	
Objects scanned:	427872	
Status		
Last scan:	Today at 10:53 AM. (Quick scan).	
Scan schedule:	Daily around 2:00 AM.	
Real-time protection:	On	
Definition version:	1.145.1584.0 created on 3/11/2013 at 1:47 Pr	ฬ.

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.

📙 Computer Management						
📃 Eile Action Yiew <u>W</u> indow H	lelp					
	]					
📕 Computer Management (Local)	Name	Full Name	Description			
🖻 🌇 System Tools	2 Administrator		Built-in account for administering the			
🕀 🔟 Event Viewer	E FredTheCow	Fred	I am a cow			
🕀 🚽 Shared Folders	Guest		Built-in account for guest access to t			
Local Users and Groups	- 🜆 Hacker	Hack	I hacked this computer			
	SUPPORT_38	CN=Microsoft Corporation	This is a vendor's account for the He			
Performance Loos and Alerty						
Device Manager						
E Storage						
🗄 🎲 Removable Storage						
🚯 Disk Defragmenter						
🚽 🚟 Disk Management						
🗄 🎲 Services and Applications						

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.

📃 Computer Management			
📃 File Action View Window	Administrator Properties	? ×	_8×
Image: Second secon	Remote control       Terminal Services Profile         General       Member Of       Profile       Environment         Image: Security in the component of the	Dial-in Sessions Duter/dom	ring the ress to t r the He

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.

Services					_	
<u>File Action View H</u> elp		Windows Firewall/	Internet Conne	ction Sharing (ICS) P	roperties?X	
		General Log On	Recovery Dep	endencies		
Services (Local) Name	g and Play	Service name:	SharedAccess			
Por State Por	rtable Media Seri nt Spooler	Display <u>n</u> ame:	Windows Firewa	all/Internet Connection Sh	haring (ICS)	
Pro Rei	otected Storage mote Access Aut	Description:	Provides networ name resolution	k address translation, add and/or intrusion preventio	dressing, 🔺	
Rei 🖏 Rei	mote Access Co mote Desktop H	Path to executab	le:		<u> </u>	
Rei	mote Procedure		ystem32\svchost.	exe -k netsvos		
Rei Rei Rei	mote Registry movable Storage	Startup typ <u>e</u> :	Automatic			
No Rei Roi Ma Sei	sultant Set of Po uting and Remot condary Logon	Service status:	Started	,		
Sea Sea	curity Accounts	<u>Start</u>	<u>St</u> op	Pause	<u>Resume</u>	
ីស្ថិរ Shi ស្ត្រីរ Shi	ell Hardware Det art Card	from here.				
Spi Spi Sys Spi	ecial Administrati stem Event Notifi	Start parameters:	ļ			
See To	sk Scheduler P/IP NetBIOS He			OK Cancel		
ି କରୁ Tel କରୁ Tel	ephony minal Services 7	Allows user Start	ed Manual	Local System		
Ter Starthe	rminal Services S E emes F	Enables a Provides u	Disabled Disabled	Local System Local System		
Uni Wirth	interruptible Pow 1 :ual Disk Service 1	Manages a Provides s	Manual Manual	Local Service Local System		
Virt Vol	ualBox Guest A 1 ume Shadow Copy 1	Manages V Start Manages a	ed Automatic Manual	Local System Local System		
ି କରୁ Wi	bClient E ndows Audio I	Enables Wi… Manages a… Start	Disabled ed Automatic	Local Service Local System		
Win Win Win	ndows Firewall/I F ndows Image Ac F	Provides n Start Provides im	ed Disabled Disabled	Local System Local Service		<b>-</b>
Exter	nded Standard	age mod	Macual			
/	C:\Documents and S	5et 🛛 🚑 Gmail - In	box - Microso	Services		2:32 PM

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.

÷			L: 58 C	Windows Firewall
ICMP Settings			×	General Exceptions Advanced
Internet Control Mes a network to share e for information from I	ssage Protocol (ICMP) error and status inform the Internet that this c	) allows the comp nation. Select the computer will resp	outers on requests ond to:	Network Connection Settings Windows Firewall is enabled for the <u>connections</u> selected below. To add exceptions for an individual connection, select it, and then click Settings:
Allow incoming Allow incoming Allow incoming Allow incoming Allow incoming Allow outgoing	echo request timestamp request mask request router request destination unreacha	able		Local Area Connection Settings
Allow outgoing Allow outgoing Allow outgoing Allow redirect Allow outgoing	source quench parameter problem time exceeded packet too big		F	Security Logging You can create a log file for troubleshooting purposes. <u>S</u> ettings
Description Messages sent to sender. This is co to ping a machine allowed if TCP po	this computer will be mmonly used for troub . Requests of this typ t 445 is enabled	repeated back to oleshooting-for e e are automatica	o the xample, Ily	ICMP With Internet Control Message Protocol (ICMP), the <u>Settings</u> computers on a network can share error and status information.
Remote Access	2 KB 5	OK C	ancel 2/1	Default Settings To restore all Windows Firewall settings to a default state, <u>R</u> estore Defaults click Restore Defaults.
rver Licensing	2 KB 5 2 KB 4	Shortcut Shortcut	2/1	OK Cancel
rvices Configuration	2 KB 2	Shortcut	2/1_	

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.