ITEC345/2013spring-ibarland
hw07: **Securing a Windows Host**
*Instructions*

Homework created by Prem Uppuluri; modified by Ian Barland

**Homework summary:** You will learn:

Section 1: Basic steps to secure a multi-user Windows OS

Section 2: Verifying your security configuration against standard templates.

Several issues need to be considered in securing an OS. The following assignment goes through some of the common tasks. Note that installing and updating Anti-Virus software is not included here, despite their importance, since such packages are common and easy to use.

Note that the startup instructions for the virtual machine are in [hw07-windows-VM-login.html](http://www.radford.edu/itec345/2013spring-ibarland/Homeworks/hw07/hw07-windows-VM-login.html). You may work with one partner. Record your answers (and, paste screenshots) into the file [hw07-answer-sheet.docx](http://www.radford.edu/itec345/2013spring-ibarland/Homeworks/hw07/hw07-answer-sheet.docx), which you will submit on D2L (submit only one copy for your team). I suggest having the answer-sheet open alongside this file, and when starting on each task check what deliverables will be required.

**Secure Operations**

**TASK 1: User Management**

 **This task ensures that:**

* + **Users are created with the least privileges required;**
	+ **Their passwords not susceptible to password cracking, and,**
	+ **Dormant users (users who haven’t logged in a while ) are locked out of the system**

*If a user account is dormant, it probably means that a user is no longer using the system. Attackers hack into such accounts because they won’t be noticed for a while.*

1. **Create user accounts and test password security:**

We’ll create 2 user accounts with usernames “Alice” and “Bob”.

* + 1. To create an account browse to *Start > Control Panel > Users Accounts*.
		2. Select “*Create a new account*”.
		3. Type in the username (Bob or Alice), and hit “*Next*”.
		4. In Account Type, select “*Limited*” and create the account.
		5. Repeat this process to create an account for the other user (both Alice and Bob).
		6. Think up passwords for the accounts, and check the password strength with Microsoft’s password checker: <https://www.microsoft.com/security/pc-security/password-checker.aspx>. *Note: you won’t have access to this website through the virtual machine – use the browser on your local system to test.*
		7. Go back to *User Accounts > Change an account > Alice* (and then, *Bob*).
		8. Select “*Create a password*”, using a password vetted by the site above.
1. **Identify users with weak passwords**

Weak passwords are those that can be broken using dictionary attacks, cryptanalytic attacks or a combination of both these attacks. We can test for weak passwords by running a password cracker against each user’s password.

* We’ll use the password cracker software “Cain and Abel”. ***Major warning****: Cain and Abel is a very powerful system tool that can be used by administrators and hackers alike. You should never download this software without proper authorization (unless on a personal computer). The White Hat agreement as well as the acceptable use policies are under effect.*
* Dictionary table we will use*:* rainbow table from Ophcrack.com website.
	1. Click on *Desktop > Security Tools Cain*.

*You might get a warning about Windows firewall; if so, ignore it.*

* 1. Once Cain starts up, select the “**Cracker**” tab.
	2. On the left, select the first option “**LM & NTLM hashes”**; these are the hash functions that Windows uses to hash the passwords.
	3. Next, select the blue colored “**+**” sign from the top menu of Cain. Sometimes this plus sign may not be highlighted – you may notice a greyed out “**+**”. If that is the case:



If the blue colored + sign is not highlighted (**it may be greyed out**): click some other option on the left menu bar (e.g., PWL files) and then select **the LM & NTLM Hashes** option again. This is a bug in Cain’s GUI.

* 1. Once you click the **+** sign – you will see a popup window: “**Add NT Hashes from**”.
	2. Select the “**Import Hashes from local system**” option, as well as “Include Password History Hashes”, and press “**Next->**”
		1. With this option, Cain imports the password file on Windows **(C:\Windows\system32\config\SAM).**



Step e and f.

* 1. On the central Cain window, you will now see the list of all the users along with their hashed passwords.
	2. **Select any user’s password (or, select all the passwords)**
	3. Right-click, and from the drop-down select *Cryptanalysis Attack > LM Hash > via Rainbow Tables (OphCrack)*.
	4. You will get a window with several options; the first input field lets you select a “rainbow table”. To the right of that input field click on the button with three dots, and browse to: *Desktop > Security Tools > tables\_xp\_free\_small*. This file contains pre-computed hashes of passwords. *Source: the file* tables\_xp\_free\_small *is from the site:* [*http://ophcrack.sourceforge.net/tables.php*](http://ophcrack.sourceforge.net/tables.php)*.*

Note that this folder might already be pre-selected, on your disk image.

* 1. Click “Start”. After some time, it will guess the password, or *part* of it. Note that the password is usually guessed across multiple steps. E.g., if the password is applesauce, this cryptanalytic attack may first find “apples”, and then later find “auce” on a different line.
	2. You can use these steps to check how secure the passwords you created were. For this assignment, you do not need to wait for more than 5-10 minutes – if it is taking longer, we’ll consider the password as reasonably secure.
	3. Even if the program can’t figure out all of a password, can *you* guess the remaining part, given a partial password?

**(3)- (4) Setting account policies (password expiry etc.) and identifying and disabling dormant user accounts.**

* + 1. To set account policies (password expiry date etc.) expand on **“Account Policies**” (in Local Security Settings). You will see two account policies:
			1. Password policy – yes you guessed it right.
			2. Account lockout policy.
			3. To make changes to either policy, simply right-click on the appropriate field (e.g., to change Maximum Password age, right click on that attribute and select properties.)
		2. To identify dormant user accounts, we must first set the local security policy such that it keeps track of when each user last logged into the system. Users who haven’t logged in for a large number of days are considered dormant. To set the local security policy, in the Local Security Settings look for Local Policy🡪Audit Policy. Turn on the “audit logon events” and log only “Success” attempts.
		3. To lock an account, go to: **Start🡪Control Panel🡪Performance and Maintenance🡪 Administrative Tools🡪Computer Management**
			1. Select **Local Users and Groups 🡪 Users.**
			2. Right click on a user name and select **Properties.**
			3. Check “**Account is disabled”**.

**TASK 2: File Management**

 **This task ensures that:**

* + **Key system files are protected and are not being shared on the network (unless needed).**
	+ **Important documents can be encrypted and stored easily.**
	+ **Identify resources (including files, registry keys) that users have access to.**
	+ **Identify any files that can be written by anyone (permissions on those files must be changed)**

Microsoft Research provides a set of very powerful and useful tools called sysinternals (<http://technet.microsoft.com/en-US/sysinternals>). We will be using one of the tools from this set for this task.

.

 **(5) Check permissions**

 a. To check and change permissions on any folder, right click on that folder/file and select **Properties**.

In Windows (most versions), security policies can be configured and tested easily using the security configuration manager. Windows distinguishes between local and network policies. Local policies are security policies for the local computer while network policies are policies applied across all computers in a network. Given the pre-req for ITEC 345, we will stick with applying local policies (however, doing so for network is not very dissimilar). You can set the local policies as follows:

For the rest of the exercise first go to: **Start🡪Control Panel🡪Performance and Maintenance🡪 Administrative Tools🡪Local Security Policy**

**You will see a window for “Local Security Settings”. The rest of the exercise assumes you are at this stage.**

 **(6) Types of users**

a. **Start🡪Control Panel🡪User Accounts🡪Change Type of Account**.

 **(7) – (8) Identify the resources that users have access on the system**

We will use a tool called **accesschk in the sysinternals toolkit for this (see documentation at:** <http://technet.microsoft.com/en-us/sysinternals/bb664922>). Accesschk can only be used from the command prompt. To use accesschk:

1. Start🡪Run, type “cmd”
2. At the prompt, cd Desktop
3. cd “Security Tools” (note the single space between Security and Tools)
4. cd SysinternalSuite
5. Once you are in the folder SysinternalSuite on the command prompt, here are some ways you can use accesschk (refer to the URL above for more documentation)
	1. accesschk “Security Student” –w \* // shows all the files and folders in the current directory that security student has write access to.
	2. accesschk “Security Student” –ws C:\ // this will recursively travel through all the folders starting from C: and identify the files that Security Student has write access to. This is clearly a lot of files – so simply stop accesschk by pressing Ctrl+C after a few mins.
	3. accesschk –w –d C:\ // lists all the users who have write access to C:

**(9) Encrypt data files**

Use the program **Desktop🡪Security Tools🡪TrueCrypt** to create a volume where you can store encrypted files. You may want to google TrueCrypt and find out information about it. These are some simple steps you can follow to create a folder in which you can store files encrypted with a password as the secret key:

1. Startup **TrueCrypt.**
2. Select **Create Volume. Keep the default option “Create an encrypted file container”. Press Next.**
3. Select **Create an encrypted file container.** Press Next
4. Select **Standard TrueCrypt volume.** Press Next
5. Select file as: Desktop and give a name for the file. Call it: 345\_Encrypted\_Drive. Press Next
6. Choose the AES encryption algorithm. Press Next.
7. Give some volume size – say 10 Mb. Press Next
8. Enter a password. Press Next.
9. Format using FAT file system. Press Format.
10. Once Format is done, press Exit.

Congratulations! Pat yourself on the back. You have created a volume called 345\_Encrypted\_Drive which can now be used to store files in an encrypted manner. Next – let’s us see how to use it.

1. On the TrueCrypt main screen, select “Select File”
2. Select the file you created above (the 345\_Encrypted\_Drive). Press Open.
3. Now Press “Mount”
4. When prompted enter the password that setup for that drive.
5. You will see that the file has been mounted as one of the drives: E – Z. Assuming it is E,
6. Now you can drag and drop files into the E: drive. Any file you drop in here is being encrypted and the only way to view that file is by entering the password.

**TASK 3: Process Management**

 **This task ensures that:**

* + **You identify processes that start up at boot time – many malwares (e.g., spywares start up during boot time)**

Microsoft Research provides a set of very powerful and useful tools called **sysinternals** (<http://technet.microsoft.com/en-US/sysinternals>). We will be using a few of these tools for this task.

1. **–(11) Identify processes that start at bootup and disabling them**.

We will use a utility called “**autoruns**” in sysinternals to check such processes.

1. Browse to the folder “**Desktop🡪Security Tools🡪SysteinternalsSuite**”
2. Look for the program **autoruns** and start the program. (Be sure to open the program, not its help-file-app, like a rather crusty old professor might do by mistake. Hypothetically.)
3. Once Autoruns starts: select the “**Logon**” tab.
4. To filter out those processes that were developed by Microsoft, on the main menu of Autoruns, click on **Options🡪Filter Options🡪Hide Microsoft entries**
5. To disable any process from startup, simply uncheck the “check” mark next to the process.
6. **Not needed for the exercise:** Click on “**Everything**” – this will list all the processes and services that are running on your computer – including any spyware that doesn’t get displayed by the task manager.

**Section 2**

 (*The following is Lab 3.6 as developed by Michael E Whitman and Herbert J Mattord in the book: Hands on Information Security Lab Manual)*.

**Background:** Microsoft provides a set of security templates by default with every Windows XP workstation (similar templates for Windows Server/Vista/7 are also provided). Each template comes with a set of rules – some of them addressing security issues. Now, any user can develop their own customized template.

In this part of the assignment, you will read and analyze one of the default templates.

**(12) Start the Microsoft Management Console (MMC):** This console allows us to configure various system-level policies on Windows. Think of this as a GUI interface to access files similar to those in the /etc directory of a UNIX machine. To start MMC:

* 1. Click **Start**, click **Run…**, and then type **mmc.** Press **Enter.**
	2. Click **File**, click **Add/Remove Snap-in, and then click Add.**
	3. Select **Security Configuration and Analysis.**
	4. Click **Add.** Repeat the step c and d for **Security Templates.**
	5. Click **Close** and then click **OK.**
	6. You should now see a security console with the word **“Console Root”** on the left menu and **“Security Configuration and Analysis”** and **“Security Templates”** on the right window

(13) Examine the **Security Templates. Security Templates** are default sets of security policies – each set of policies for a specific type of installation. E.g., if you are installing Windows in a company that requires high security, you may choose the high security template.

* 1. Click on the **+** sign next to **Security Templates** in the left window.
	2. Click on the **+** sign next to the path name of the templates: **C:\Windows\Security\templates**
		1. **(note: if you do a search you can find templates from other organizations and users).**
	3. **You will see a set of templates each with an acronym. Here are some common ones:**
		1. **hisecws:** High-Security Workstation template
		2. **hisecds:** High-security for domain controllers (useful if the system is setup as a domain controller – something we will pursue in depth in ITEC 455).
		3. **securews:** Secure workstation.
	4. **Analyze the hisecws template.**
		1. For instance to check Password Policies, go to: **Account Policies**, **🡪 Password Policy.**

**(14)-(15) Analyze if the Windows workstation actually enforcing any of these policies.** Even though the workstation has several templates – these templates may not be enabled. In this part of the assignment you will analyze how closely the current security settings of your workstation match those of the hisecws template.

* 1. Click **Security Configuration and Analysis** option in the left pane.
	2. **Right-click** the **Security Configuration and Analysis option and click Open Database.**
	3. Type the following in the file name textbox: <TeamName> -- replace TeamName with your team’s name (the <> symbols should not be typed).
	4. Click **Open**
	5. Select the **hisecws** template name.
	6. Click **Open.**
	7. Next, **right-click** the **Security Configuration and Analysis** option in the left pane and click **Analyze Computer Now.** Leave the default values and click OK.
		1. Once the analysis is done you will now see a list of policy categories in the left pane under the **Security Configuration and Analysis option.**
		2. Click the **+** sign next to Account Policies and click Password Policy.
		3. Where-ever you see a **Red colored X**, it means the policy on the local machine does not match the template.
		4. Now, **you can automatically configure the workstation to enforce those policies –** simply right click on the **Security Configuration and Analysis option again** and **click Configure Computer Now.** Be careful when you do this on a regular production system – you may be enabling security policies that will prevent many tasks from executing(!).