ITEC345/2013fall-ibarland
hw07: Securing a Windows host:
*Answer Sheet*
Due: 2013.Dec.02 (Mon.), 23:59

**Note: The table below enumerates the tasks that need to be accomplished. Please record your answers next to each task. The instructions to accomplish the tasks and the motivation for the tasks are provided after the list of tasks.**

**Note:** This is a group project; ***please work in teams of up to three***.Submit only one solution for your entire team. **All team members must be physically working together** for all parts of each problem.[[1]](#footnote-1) If you are looking for others to work with, post a request on the discussion boards. Before starting, decide which team-member’s Windows XP workstation you will use, from the [hw07-windows-VM-login instructions](http://www.radford.edu/~itec345/2013fall-ibarland/Homeworks/hw07-windows-admin/hw07-windows-VM-login.html). Please try not to use multiple workstations per team, as resources are limited.

**ONLY ONE SUBMISSION PER EACH TEAM REQUIRED. Please state the names of all team members so everyone gets credit. Also please state the team number you used as this is necessary for me to check your solutions.**

**Team Member A: \_\_\_\_\_\_\_\_\_\_\_\_@radford.edu**

**Team Member B: \_\_\_\_\_\_\_\_\_\_\_\_@radford.edu**

**Team Member C: \_\_\_\_\_\_\_\_\_\_\_\_@radford.edu**

**Virtual machine used: team\_\_-WinXP**

**Assignment Deliverables**

If a particular (file)name is asked for, be sure to spell it exactly, including case. For screenshots, you can submit images of *parts* of the screen, as long as it contains the info needed to confirm the task has been completed.

|  |  |
| --- | --- |
| **Task category**  | **Task description (please record/paste your answers for each task into this table)** |
| **SECURE OPERATIONS** |
| **User** **Management:** | 1. Create 2 users using your first name as one user and your last name as another username with limited privileges, and ensure that their passwords are strong.

 **Deliverable**: Screenshots of the new accounts.  **[paste screenshot here]** |
| 1. Identify users with weak passwords.

 **Deliverable**: List the passwords (only) of users that you were able to crack:  |
|  | 1. Set the following account policies:
	1. Password history: remember last 3 passwords (users cannot use the last 3 passwords). This ensures that the user cannot use his/her current password again at least for 3 more times. However, a user can beat the “password history system” by changing the password 3 times within a span of few minutes. To protect against this, we use the next step.
	2. Minimum password age: set this to 5 days. This is the minimum number of days the user has to wait before he/she can change her newly created password.
	3. Maximum password age (maximum number of days you can use the password): set this to 180 days.

**Deliverable:** insert a screenshot of the security settings showing these policies.  |
|  | 1. Identify and disable dormant user accounts. For this homework, disable either of the two accounts you created in step (1).

**Deliverable:** insert a screenshot of the Computer Management window with the “Account is Disabled” option checked.  |
| **File** **Management** | 1. Check permissions: Ensure that system level folders C:\WINDOWS and C:\Program Files are secure: (a) read-only for administrator and (b) no network sharing.

**Deliverable**: insert screen shot of the permissions window for one of the folders.  |
| 1. List the type of users (groups) on the system.

**Deliverable**: Write down the group names here:  |
| 1. Identify all users who have write access to the folder C:\

**Deliverable:** Screenshot showing (i) the output of accesschk and (ii) the command line options you provided to access check.  |
| 1. Identify all the files and folders within C:\ and its sub-folders that “Security Student” has access to.

**Deliverable:** A screenshot showing the resources (only partial view of the resources is fine as generating a list of all the resources is time consuming) |
| 1. Encrypt data files. Create an encrypted folder on the desktop which stores files encrypted with a password.

 **Deliverable**: insert screen shot showing the encrypted folder created using TrueCrypt.  |
| **Process****Management** | 1. Identify processes that are automatically started when you bootup

**Deliverable**: In the table below, list any 3 non Microsoft processes that startup along with their location and any registry keys that they access.

|  |  |  |
| --- | --- | --- |
| Process Name | Location on disk | Registry keys they access (if any) |
| 1.2.3. |  |  |

  |
| 1. Disable the google update process from starting automatically.

Deliverable: Nothing to deliver. |
| **Section 2: Analyze the security of the workstation so far.** |
| **Start up the analysis tool.** | 1. Deliverable: Screenshot of the security console with the snap-in’s: Security configuration and Analysis and Security Templates added.
 |
| **Questions on standard security templates provided by Microsoft** | 1. Deliverable: Answers to the following question:

In the **hisecws (high security workstation template)**, what does initial settings does Microsoft use for:1. the minimum password length?
2. the maximum password age?
3. the account lockout threshold?
 |
| **Is your workstation secure?**  | 1. Deliverable:
2. **T/F: Does the workstation you were assigned initially have the same password policy as hisecws?**
3. **Submit a screenshot of the security console showing how the Password policies of your workstation compare to the hisecws template.**
 |
| **Configure the security of your workstation** | 1. Deliverable: Screenshot showing that the Password Policy has been configured to match that of hisecws.
 |

1. Should you want to add a team member after having already completed problems, you’ll have to *re*-complete those steps with them (presumably letting them ‘drive’ the keyboard). [↑](#footnote-ref-1)