Contents at A Glance

Story

You are Sherlock Holmes, a private investigator and have been commissioned to solve the kidnapping of Mrs Vista, a teacher at Central School. You have managed to access Mrs Vista's work computer and you are attempting to hack the laptop of the Headmaster that might have data about the kidnapper. All Central School PCs are running Windows 7 Professional operating systems.

1. Getting to the Start Line

a. **Mrs Vista's** user was restricted on her working PC. Log on as Mrs Vista and find a file located in a disguised folder on the Desktop. This file contains a binary representation of a hexadecimal password.

Clue from Dr. Watson: *Use a special Calculator Mode to convert binary to hexadecimal.*

b. Log on into the Admin account using the hexadecimal password so that you will have unrestricted access to all administrative tasks.

Clue from Dr. Watson: Did you know about the Windows+L shortcut?

2. The First Mystery

The Admin's desktop has undergone a crime against *Windows 7*. Search for a hidden file on the Desktop that will help you connect to the network. After finding the file, make sure you change its extension to .txt.

Clue from Dr. Watson: Use Folder Options or **dir /?** *from the command prompt.*

3. Getting Connected

It's time to get outside the box. Follow the instructions:

a. From either the command prompt or from GUI, modify the IPv4 settings for the **Local Area Connection** so that they match the exact values written in the file previously discovered.

Clue from Dr. Watson: run **ncpa.cpl** *in Start Menu*

b. Verify your configurations. Can you ping the default gateway? What about google.com?

Clue from Dr. Watson: run **ipconfig /all** *in command prompt*

c. Using DNS queries determine the IP addresses of **catc.ro**.

Clue from Dr. Watson: nslookup

d. Discover the Central School topology using a tool from Network and Sharing Center. Find the **IP of the Headmaster laptop** on the map and remember it, as you'll need it later. You should be able to ping this IP from command prompt.

Clue from Dr. Watson: ping 1.2.3.4

e. Open **www.catc.ro** in a web browser. Create a firewall rule, called **block_catc.ro,** to block **HTTP traffic** to **www.catc.ro**. Verify this rule by opening **www.catc.ro** again.

Clue from Dr. Watson: Windows Firewall with Advanced Security – create a custom rule, on the specific TCP remote port 80.

4. A Power Beyond Imagination: PowerShell

On the Headmaster laptop, there is a **shared folder** on the Desktop, named PowerShell with relevant clues for the next tasks. The user is **Headmaster** and the password is **goodluckSherlock.** Copy these files to your drive C:\. Follow the next steps:

a. Open PowerShell. Use the command **"Set-ExecutionPolicy unrestricted"** so you can run scripts later.
b. Use the basic commands needed to view PowerShell commands and their aliases.

Clue from Dr. Watson: Have you checked the files from the Headmaster?

c. Run the command from task_c.txt file. What does this command do? Use ps in a similar way to print only the processes that consume more than 30% of the resources of the CPU.

Clue from Dr. Watson: ***-eq*** *mean equal*
-ge *means greater or equal*
-le *means lower or equal*

d. Run the **task_d.ps1** script. What does it do? Modify it so that your PC pings every IP in the range **141.85.157.57 – 141.85.157.65.** If the ping is successful, it should print the message "A good day for Holmes", or else "Not such a good day for Holmes". Test your script.

*Clue from Dr. Watson: To run this script, use "****cd C:****" and "****.\script_name****".*

e. Run the **task_e.ps1**. What does it do? Modify it so that it creates 2 folders: School and SHARE. The script should also create the following School subfolders: 9A, 9B, 9C, 10A, 10B, 10C, 11A, 11B, 11C, 12A, 12B and 12C.

You need the SHARE folder to complete the following tasks.

5. Hacking the Laptop

It's just between you and the Headmaster laptop now. Watson is already connected to the Headmaster laptop and will help you along the way. Try not to make any mistakes.

a. Create an Administrator user called Sherlock. Configure a password of your choice.
b. Log into the Sherlock user. Share the folder SHARE with read/write rights for Everyone.
c. Create a text file called sherlock.txt in the SHARE folder. It should contain the Sherlock user password.
d. Enable Remote Desktop Connection so Watson can have remote access to your computer.
   Clue from Dr. Watson: From start menu, type Remote Desktop Connection

e. Schedule a task using Task Scheduler that will send the message "I know who the kidnapper is" when someone will log in remotely to your computer.

   Clues from Mr. Watson:

   - *Choose "Create task..."*
   - *In the General tab, Security Options choose your user account*
   - *From the Triggers tab, add a trigger "On connection to user session"*
   - *From the Actions tab, add the action "Display a message"*

f. From the command prompt, initiate a ping with the –t option using the IP of the Headmaster laptop. This is a secret signal for Watson.
g. In about 1 minute, Watson will connect to your computer by Remote Desktop Connection. This will log you off. Wait 2 minutes before you log back in so Watson will have enough time to put important data on your computer. Watson will place on your desktop a file containing his user and password for the laptop.

6. Approaching the Finish Line

Try to access the Headmaster laptop through Remote Desktop Connection, using the username and password from Watson. This should reveal important information regarding the kidnapping!