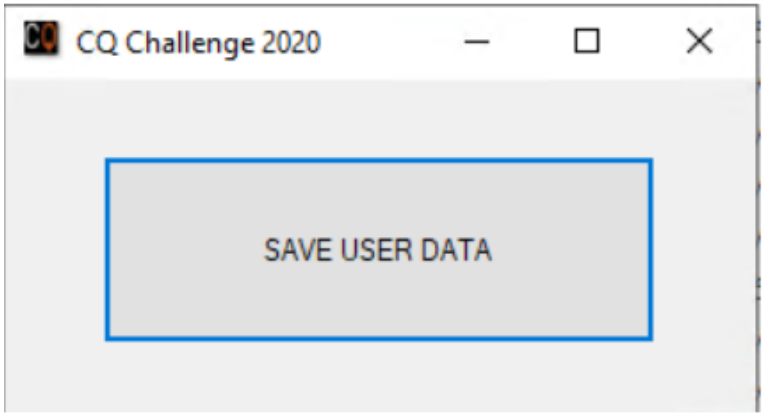
All-New 5-Day Challenge

by Paula Januszkiewicz CQURE Academy Experts "Do Cyber Security like a PRO"

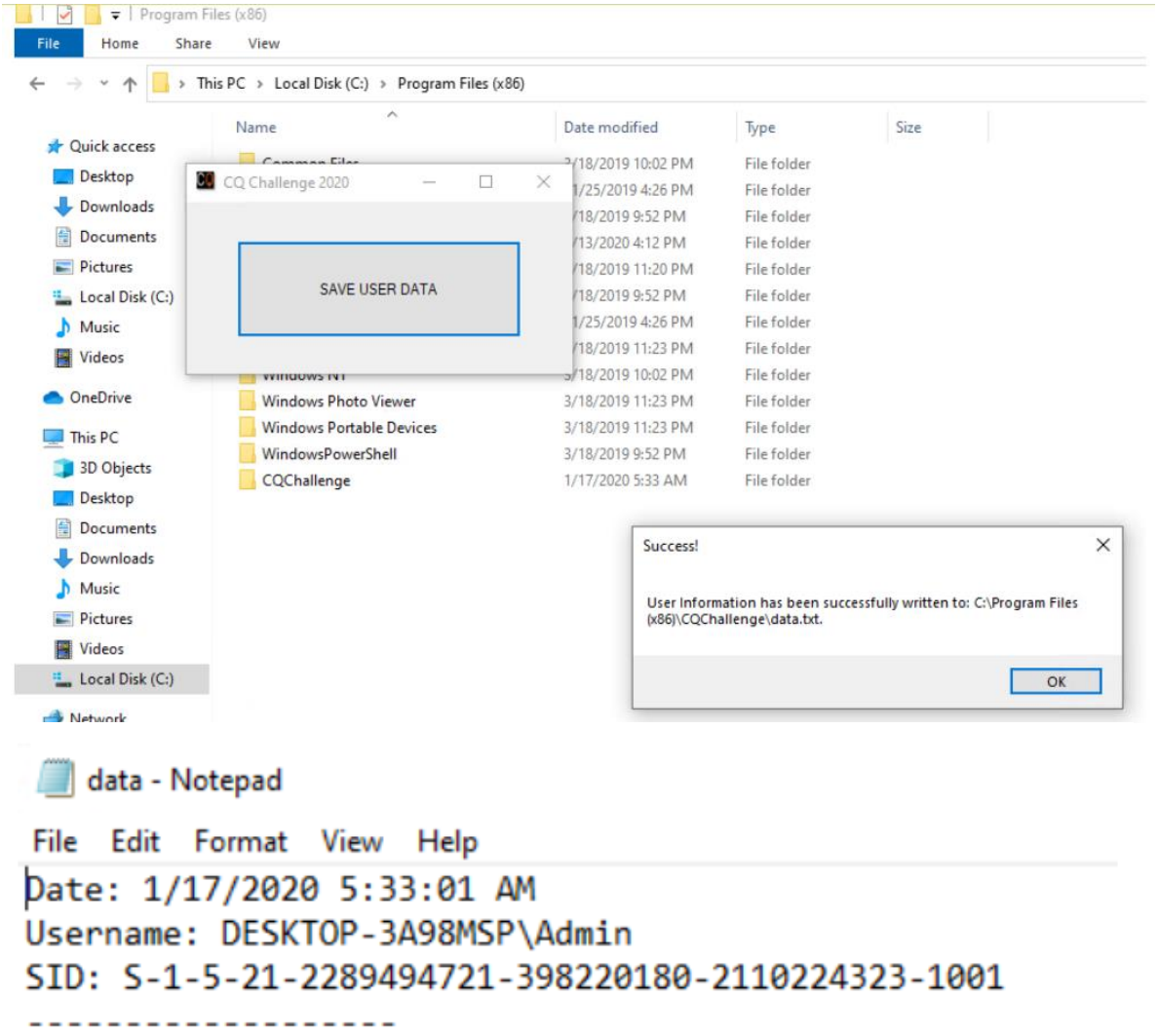
Day 2: File System Virtualization

INSTRUCTION

1. Please use clean, test and up to date Windows 10 machine (physical or virtual). We do not recommend running this challenge on any production OS. If the file will be detected by your AV as malicious, please set up appropriate exception.
2. CQChallenge2.exe is a simple application designed to get current user information and write it to a log file placed in %ProgramFiles(x86)%\CQChallenge\data.txt (the directory will be automatically created).
3. Please test the app by running CQChallenge2.exe as administrator and clicking SAVE USER DATA Button: PASSWORD:CQ5DChallenge2020

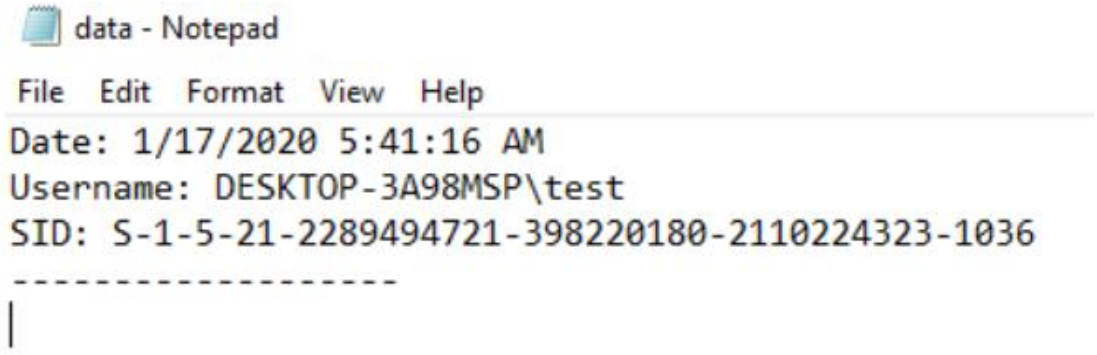


4. If you have run the app as admin, data should be written without any issues:



5. Now, please try running the app using another, unprivileged account. Repeat the same procedure by clicking SAVE USER DATA BUTTON. Was it successful? Why?

6. Your task is to make the application running for ordinary, unprivileged user WITHOUT changing any NTFS permissions (Hint! The actual location where data.txt file will be saved can change).



Your solution should include the following:

a. Why it is not possible to simply save the user data to %ProgramFiles(x86)%\CQChallenge\data.txt as an unprivileged user?
b. How to run the application as unprivileged user and make it running fine without changing any NTFS permissions. When mechanism / feature can be useful in a real life?
c. Is it possible to make it running with UAC Virtualization Enabled automatically?

CQURE ACADEMY

TIPS!!!

1. Read about UAC Virtualization and run the application with UAC Virtualization enabled.