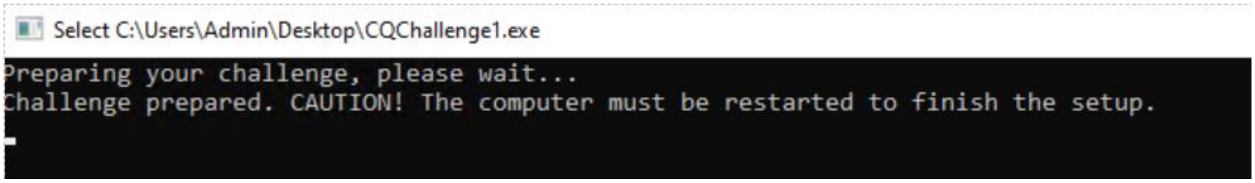
CQURE
ACADEMY

All-New 5-Day Challenge by Paula Januszkiewicz CQURE Academy Experts "Do Cyber Security like a PRO"

Day 1: Dump the LSASS memory

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. Run CQChallenge1.exe as administrator. PASSWORD: CQ5DChallenge2020
3. Once the preparation is done, reboot your test machine (necessary to apply the settings).



```
Preparing your challenge, please wait...
Challenge prepared. CAUTION! The computer must be restarted to finish the setup.
```

4. CQChallenge1.exe set up some protection for LSA Process. After the reboot it is protected.
5. Your task is to create a full dump of LSA process memory (lsass.exe) WITHOUT rebooting the machine.

Your solution should include the following:

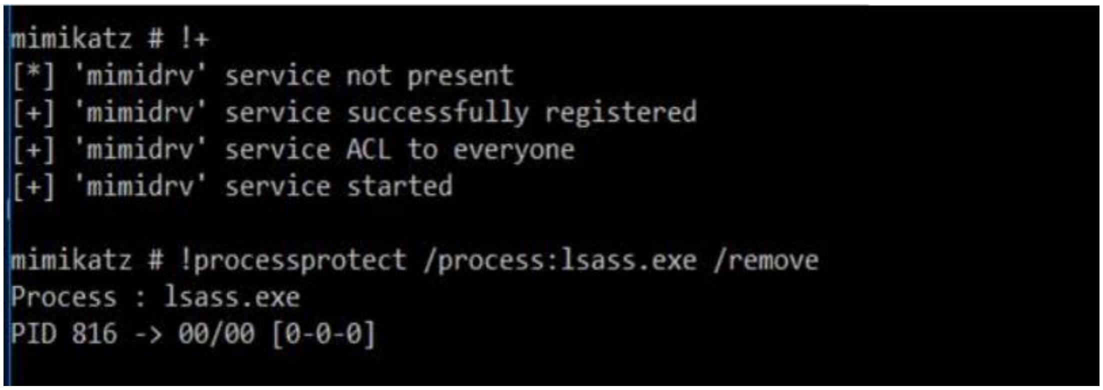
a) What mechanism / solution / setting was protecting your LSA.
b) How to turn off / bypass this protection without rebooting the machine and create a dump of the LSA memory.
c) What are other security measures, which could be used to protect lsass.exe?

TIPS!!!

1. Use Process Explorer (from SysInternals toolkit) to check the properties of lsass.exe process
    a. Open Process Explorer
    b. Find lsass.exe
    c. Right-click and go to Properties
    d. Examine Security tab
2. Now when you know that lsass.exe has been set as Protected Process, you can proceed to unprotecting it. We recommend using mimikatz tool by Benjamin Delpy. Mimikatz (download latest release).
3. To use mimikatz, you will have to create some exclusions or disable Windows Defender / other AV software you have installed. In real life, hackers and penetration testers are using custom and modified versions of this tool to stay under the radar of anti-virus / anti-malware solutions.

    Mimikatz offers quite a lot of functionalities. You should be interested in loading mimikatz driver and unprotecting protected process. You should easily find some guide on the Internet.

    To remove protection of lsass, run mimikatz as admin and use the following commands:



```
mimikatz # !+
[*] 'mimidrv' service not present
[+] 'mimidrv' service successfully registered
[+] 'mimidrv' service ACL to everyone
[+] 'mimidrv' service started

mimikatz # !processprotect /process:lsass.exe /remove
Process : lsass.exe
PID 816 -> 00/00 [0-0-0]
```