LAB 7

Malware

DUE 04/12/2020 11:59:59 PM

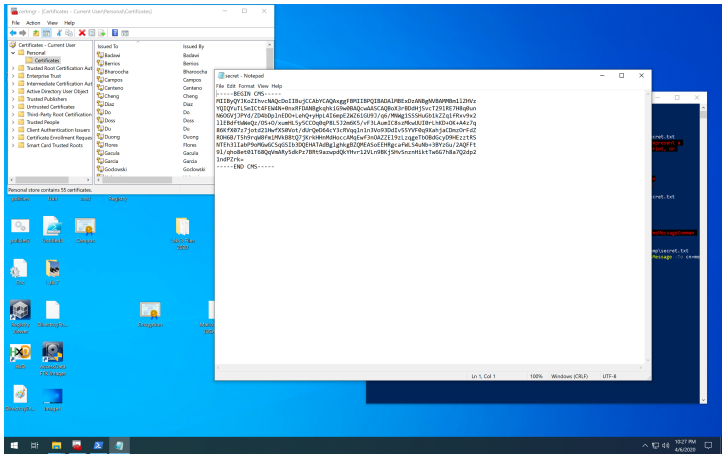
Revised Version

Instructions Assignment (100 points total)

- Instructor will not be responsible for any machines that get infected or destroyed for improper follow up.
- You are going to get INFECTED!
- Create a virtual machine.
- Disable your anti-virus/anti-malware and firewall application

Part I (50 points total)

1. Unzip the certificate inside the Lab 7 zip file
2. Using the certificate provided, create an encrypted message. You will do this by either using step 4 or step 5. However, before you continue, answer the following:
    a. You created a few certificates in Lab 5, why can't aren't you able to use one of those certificates to encrypt your message?
    b. Why does the certificate provided works?
    c. What are some of the differences between all the 3 certificates(Root, <Last Name_Server>, Encryption?
        Hint: Yes, I know the name is different, the serial number, etc. I am looking for something that will tell what each does.
    d. Take a screenshot showing all of your 3 certificates inside certmgr
3. You can create the encrypted message by running the Message (double click) or type the next command.
4. "<Message already inside file!>" | Protect-CmsMessage -To cn=< Common Name of the certificate provided> -OutFile C:\<Last name>_SecretMessage.txt
5. Hash the file with SHA1, SHA2 and SHA512
6. Take a screenshot of your PowerShell console showing your hashes and include it in the lab
    a. Upload your encrypted file with your lab report.
7. Open up your .txt file and take a screenshot. It should look something like this.



8. Now this is the fun part download the piece of malware and run it on your virtual machine and answer the following.

LAB 7

Malware

DUE 04/12/2020 11:59:59 PM

Revised Version

Part II (50 points total)

1. What was the message you encrypted?
2. What happened right after you let the malware lose? Did you follow the right precautions to not get infected? (Besides your VM)

   If not, what else got infected?

   - List all of the precautionary steps you took
3. Is the encrypted file safe, since it is encrypted? Or did the malware take over it as well? Try opening it. What happened?
4. How does this piece of Malware work? (Need a full explanation not just a sentence, list any sources used)
5. Once you enabled your anti-virus. Did your VM get cleaned up?
6. What did your anti-virus do? (Again, I need a technical explanation)
7. What do anti-virus or Malwarebytes looks for in order to detect this?

Remember there are 3 Easter Eggs for you guys! If you find them, write or insert them here.

Easter egg 1 →

Easter egg 2 →

Easter egg 3 →

Have fun ☺