CPTC Homework #4

Resources

1. **TryHackMe link: https://tryhackme.com/room/windows10privesc**
2. **Kali creds are kali:kali**
    a. **Neo4j creds are neo4j:bruh**
3. **You can attempt to stylize your report based off of prior CPTC ones**
    a. **https://github.com/globalcptc/report_examples/tree/master/2020**

Questions (20 pts)

1. Give a mimikatz command that dumps passwords and hashes from SAM. Assume that you are already at Administrative level privileges. (5 pts)
2. Write a MSSQL query that grants command execution on the host. Assume that xp_cmdshell is disabled and that you have the role DBO on the database. (5 pts)
3. Provide the name of a SMB exploit, a command to discover that vulnerability, and a high level overview of how you could exploit it. (5 pts)
4. What are the differences between an ASREPRoast and Kerberoast attack, in regards to the stage of Kerberos authentication in which they occur, and the prerequisite conditions to perform the attacks.

Labs (80 pts)

1. Conduct a penetration test against the target: 192.168.1.2 and create a report. The report must have a Title Page, table of contents, and at least 3 technical findings. No other components are necessary (ie: Executive Summary, Attack narrative, topology, etc.), but it is encouraged that you attempt to include them. (50 points)
2. Complete the following TryHackMe Room: Windows Privesc (30 points)

Deliverables

1. **A PDF with all of the following:**
    a. **answers to all of the questions on the first page**
    b. **a screenshot that proves that you finished the TryHackMe room**

   c. **the penetration test report**
      i. **Include this within the same file, but make sure the Title Page takes up a whole page rather than being on the same page as the questions and TryHackMe screenshot.**
2. **Make sure all sections are readable and labeled.**
3. **Name the file with the following format: FirstLast_CPTCHomework4.pdf**

If you are trying out for the team, make sure you submit your PDF in Canvas.

Otherwise, please use this form if you want to be graded: https://forms.gle/mvXSZnd6Fv8NTCrY8.