CPTC Homework #2

Resources

Remember to always use safe Internet practices. Here are some resources for accessing Bandit:

1. **Bandit Link**
   a. **https://overthewire.org/wargames/bandit/bandit0.html**
2. **Remoting with SSH using Terminal (Linux + MacOS)**
   a. **https://www.linode.com/docs/guides/connect-to-server-over-ssh-on-linux/**
3. **Remoting with SSH using Powershell**
   a. **https://docs.microsoft.com/en-us/powershell/scripting/learn/remoting/ssh-remoting-in-powershell-core?view=powershell-7.2**
4. **Remoting with SSH using Command Prompt**
   a. **https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/factoryos/connect-using-ssh?view=windows-11#connect**

Questions (34 pts)

1. Provide a reverse shell command for a Linux machine to connect back on port 1337. (10 pts)
   a. What command would you run to create a listener to catch the incoming reverse shell connection?
2. What is a site where you can publish undiscovered vulnerabilities in a responsible way? (5 pts)
3. Provide an nmap command that would conduct a service and default script scan on the host `10.100.10.10`. (5 pts)
4. What is the name of a Metasploit module used for exploiting the EternalBlue vulnerability? (14pts)
   a. What option(s) would you need to set the target to `10.100.10.10` on port 445?

Labs (66 pts)

1. Complete as many levels as you can on Bandit
   a. Each level is worth 2 points

Deliverables

1. **A PDF with all of the following:**
    a. **answers to all of the questions**
    b. **a table with the following:**
        i. **the level name (ex. 0-1, 1-2)**
        ii. **the password found during the level**
        iii. **a short description of the solution you used**
        iv. **any notes you may have taken while solving**
        v. **any resources you found to be helpful**
2. **Make sure all sections are readable and labeled.**
3. **Name the file with the following format: FirstLast_CPTCHomework2.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/SU3hc2WMmB9jeijG8.