CPTC Week 2 Homework

Intro to Pentesting

Part 1: Questions (34 Points)

1. Explain what a Command and Control (C2) is. Provide 2 examples of well known C2s. Why would someone use a C2 over multiple reverse shells? (8 pts)
2. Generate an `msfvenom` reverse shell that connects back to `192.168.1.10` on any port as … (10 pts)
    a. An MSI package
    b. An ELF executable
    c. Also provide a method of catching the reverse shell connection/callback
3. Provide an `nmap` command that… (6 pts)
    a. Scans the host `172.168.12.73`.
    b. Conducts the default scripts and version scan
    c. Changes the minimum packet sending rate of `1000` packets per second
4. What is the name of a Metasploit module used for exploiting the EternalBlue vulnerability? (10 pts)
    a. What option(s) would you need to set the target to 10.100.10.10 on port 445?

Part 2: Lab (66 Points)

Bandit Link

- https://overthewire.org/wargames/bandit/bandit0.html

Complete as many levels of Bandit as possible. Each level is worth **2** points. Provide information on how you completed each level

Part 2 Alternative: Starting Point (66 Points)

Starting Point Link

- https://app.hackthebox.com/starting-point

Complete **ONE** box **FROM EACH TIER** (0-2)
Explain your thought process in completing each box

Deliverables

1. Submit a PDF with all of the following:
    a. Answers to all the questions
    b. Solutions to each Bandit level or each Starting Point box
2. Make sure all sections and images are readable and labeled.
3. Name the file with the following format: `FirstLast_CPTCHomework2.pdf`