1. Perform a service and version scan using Nmap to determine which services are up and running:  
   * Run the Nmap command that performs a service and version scan against the target.  
       
       
      Answer: Nmap -sV was able to find multiple open ports running the services below and the associated port.

25 - smtp SLmail smtpd 5.5.0.443

135 - msrpc Microsoft windows rpc

139 - netbios-ssn microsoft windows netbios-ssn

445 - microsoft-ds?

3389 - ms-wbt-server Microsoft Terminal Services

8000 - http Icecast Streaming Media Server

1. From the previous step, we see that the Icecast service is running. Let's start by attacking that service. Search for any Icecast exploits:  
   * Run the SearchSploit commands to show available Icecast exploits.  
       
       
      Answer: The only exploit available within metasploit for icecast is the icecast header overwrite exploit.
2. Now that we know which exploits are available to us, let's start Metasploit:  
   * Run the command that starts Metasploit:  
       
       
      Answer: Metasploit is run by msfd. The exploit was then ran after. See attached picture.
3. Search for the Icecast module and load it for use.  
   * Run the command to search for the Icecast module:  
       
       
      Answer: search
   * Run the command to use the Icecast module:  
       
      **Note:** Instead of copying the entire path to the module, you can use the number in front of it.  
       
       
      Answer: exploit windows/http/icecast\_header
4. Set the RHOST to the target machine.  
   * Run the command that sets the RHOST:  
       
       
      Answer: rhost=192.168.0.20
5. Run the Icecast exploit.  
   * Run the command that runs the Icecast exploit.  
       
       
      Answer: run
   * Run the command that performs a search for the secretfile.txt on the target.  
       
       
      Answer: (must be in the C: drive directory) search -f \*secretfile.txt
6. You should now have a Meterpreter session open.  
   * Run the command to performs a search for the recipe.txt on the target:  
       
       
      Answer: search -f \*recipe.txt
   * **Bonus**: Run the command that exfiltrates the recipe\*.txt file:  
       
       
      Answer:
7. You can also use Meterpreter's local exploit suggester to find possible exploits.  
   * **Note:** The exploit suggester is just that: a suggestion. Keep in mind that the listed suggestions may not include all available exploits.