|  |  |  |
| --- | --- | --- |
| Name: Adarsh Kumar | SRN No: PES2UG20CS016 | Assignment No:10 |
| Section: B | Date: 16/11/2022 |

|  |  |
| --- | --- |
| **Task 1:** | **Lab Setup:** |
|  | Configure the DNS server for Attacker machine.    modify the related IP address.    We are modifying the IP tables so that to make believe related IP address is on the server machine. |
| **Task 2:** | **Lab Tasks** |
|  | Step 1:  Making attack.py file executable by giving permission to make a file or folder accessible to everyone.    Running the attack.py code on the Attacker machine      In the above two screen short we can see that Attack.py is a program that will send out the malicious heartbeat request to the server www.heartbleedlabelgg.com and in response, it will get random data from the server.  It aslo says that this server is vulnerable because it is sending more data than it should. |
| **Step 2:** | **Explore the damage of the Heartbleed attack** |
|  | Step 2(a): On the Victim Server:  visit the https://www.heartbleedlabelgg.com website and Send Boby a private message.  Screenshot 1: loging to heartbleedlabelgg.com    Screenshot 2: Added Boby as a friend      Screenshort 3: Sending Boby a message. |
| Step 2(b): | On Attacker machine: |
|  | 1) Find out the Username & Password:    As we can see that is above screenshot in the last line, we can see that user name and password.  Username: admin  Password: seedelgg  2) Find the exact content of the private message    In this screenshot we can see that the message info  Subject: hi  Body: how are you my friend |
| **Step 3:** | **Investigate the fundamental cause of the Heartbleed attack** |
|  | changing the value of the payload length variable.  $ python /home/seed/attack.py www.heartbleedlabelgg.com --length 40    $ python /home/seed/attack.py www.heartbleedlabelgg.com --l 0x012B    As we can see that changing the value of payload, we are able to get the different amount of data because of which we can ask the server as much amount of data as we want. |
| **Step 4:** | **Find out the boundary value of the payload length variable.** |
|  | Using length 23 results in data is being returned before that length data is not returning.    Using an attack length of 22 bytes results in an empty response:    So, we can consider that 22 byte is the boundary value as after that the attack start returning some data. |
| **Step 5:** | **Countermeasure and bug fix** |
|  | To fix the Heartbleed vulnerability, the best way is to update the OpenSSL library to the newest version. But doing that we get that to know that ubuntu 12 is not giving update properly because it is outdated not.  I am attaching those screenshots bellow which gives us error.  $ sudo apt-get update      We received error while updating.  $ sudo apt-get upgrade      We received error while upgrading as well    The Heartbleed bug (CVE-2014-0160) what there because there isn’t any check to determine whether or not ‘pl’ is a valid value, a memory breach can occur.  That can be fixed by:   1. requires the program to know the allowed boundary while performing the copy, which could be difficult to implement. 2. requires the server to calculate the packet size at runtime, and although this entails overhead in the server application, it is less computationally demanding. |

THE END