**EXPERIMENT NO. 9**

|  |
| --- |
| **Student Name and Roll Number:Harshit Parashar 18csu081** |
| **Semester /Section:5th semester CS-V-CSA** |
| **Link to Code:** |
| **Date: 27/10/2020** |
| **Faculty Signature:** |
| **Marks:** |

|  |
| --- |
| **Objective:** Setup ApateDNS on your system and run a malware to generate fake responses |
| **Outcome:** Generate fake DNS response using ApateDNS |
| **Problem Statement:** Generate fake DNS response using ApateDNS by creating a fake network |
| **Background Study:** Malware often beacons out and eventually communicates with a command and control server. You can create a fake network and quickly obtain network indicators, without actually connecting to the Internet. ApateDNS, a free tool from Mandiant, is the quickest way to see DNS requests made by malware. |
| **Algorithm/Flowchart:** |
| **Code(Solution):** |
| **Sample Outputs:**  **DOWNLOAD THE ApateDNS from fireeye.com**    **>>insert the ip address to which you want to divert the dns request and then start the server** |
| **Question Bank:**  Write down the different ways to create a fake network along-with their advantages and drawbacks.  Ans.Different ways to create a fake network are as follows:  1.Osinato  2.Nping  3.mitMAP git clone https://github.com/xdavidhu/mitmAP.git Attribution link: <https://latesthackingnews.com/2018/11/27/mitmap-an-open-source-tool-to-create-a-fake-access-point-and-sniff-data/>  It is another tool to create fake network and sniff traffic  The major advantage of creating a fake network is that we can capture the malicious file and trap them in the network and analyze it further  We can divert the traffic and analyze the inbound traffic.  Disadvantage of using fake network is that managing a large network is complicated.  No firewall,security can be implemented on fake network resulting in the spread of severe malware throughout the network of organization when not deal with care.. |