**EXPERIMENT NO. 2**

|  |
| --- |
| **Student Name and Roll Number:Harshit Parashar/18CSU81** |
| **Semester /Section:5th semester / CS-V-CSA** |
| **Link to Code:** |
| **Date:10 SEPTEMBER 2020** |
| **Faculty Signature:** |
| **Marks:** |

|  |
| --- |
| **Objective:** Setting up Honeypot |
| **Outcome:** Set up honeypot on the system to collect malware samples |
| **Problem Statement:**  Gather malware samples on the system by setting up honeypot |
| **Background Study:** Honeypots are systems that are designed to be exploited, whether through emulated vulnerabilities, real vulnerabilities, or weaknesses. By creating such systems, you can attract and log activity from attackers and network worms for the purpose of studying their techniques.  High interaction:   * Systems with a real non-emulated OS installed on them that can be accessed and explored by attackers. * These systems may be virtual machines or physical machines that you can reset after they are compromised * To gain insight into techniques and toolkits used by attackers.   Low interaction:   * Systems that only simulate parts of an operating system. * These systems are most frequently used to collect malware |
| **Algorithm/Flowchart:** |
| **Code(Solution):** |
| **Sample Outputs:**  **On the VM, run the following commands:**   * **wget https://raw.githubusercontent.com/aschmitz/nepenthes/master/script/install-nepenthes-server.sh**        * **chmod +x install-nepenthes-server.sh**       **sudo ./install-nepenthes-server.sh**  **NOTE DOWN THE PASSWORD**  **Username: netpen**  **Password: Y2odnfvJ**      **http://ubuntu:8080/**    **DONE!!!** |
| **Question Bank:**   1. What is the purpose of a shadow honeypot? a) To flag attacks against known vulnerabilities b) To help reduce false positives in a signature-based IDS c) **To randomly check suspicious traffic identified by an anomaly detection system** d) To enhance the accuracy of a traditional honeypot   2. Which of the following is a honeypot-detection tool?  a) Honeyd  b) Specter  c) KFSensor  d) **Sobek**  3. Which of the following is a system designed to attract and identify hackers?  a) **Honeypot**  b) Firewall  c) Honeytrap  d) IDS  4. Bypassing a device, or performing another action, to attack or place malware on a target network without being detected.  a) Packet Filter  b) State Table  c) **Evasion**  d) Honeypot |