|  |  |  |
| --- | --- | --- |
| Name: Adarsh Kumar | SRN No: PES2UG20CS016 | Assignment No: 4 |
| Section: B | Date: 16/09/2022 |

|  |  |
| --- | --- |
| Task 1: | SYN Flooding Attack |
| Command and screenshot | The current size of the victim’s queue for half-opened connections.  # sysctl net.ipv4.tcp\_max\_syn\_backlog    Turn off the SYN cookie countermeasure in the victim machine.  # sysctl -w net.ipv4.tcp\_syncookies=0    To check the usage of the queue before the attack.  # netstat -tna |
| Task 1.1: | Launching the Attack Using Python |
|  | A lot of Foreign address with SYN\_RECV message is present . |
|  | As we can see that telnet connection is established so, our attacked failed.  Now we are reducing the size of the queue to 80 |
|  | As we can see now this time connection failed because of Connection time out so our attack got successful. |
| Task 1.2: | Launching the Attack Using C |
|  | Restoring the queue size to original.    Attacker launching its attach to victim    Trying to establish connection from user1 to victim.    As we can see that using C, we were able to connect telnet connection to victim so attach un successful. |
| Task 1.3: | Enable the SYN Cookie Countermeasure. |
|  | Now we are trying to use SYN cookies counter measure in victim machine.  As we can see that after counter measure, we are able to logging to telnet successfully.  Restoring all the settings to default |
| Task 2: | TCP RST Attacks on Telnet Connections |
|  | Attacker terminal  Here we can see that all information are displayed.    Attack got successful.    What happens to the Telnet connection after that attack?  Ans: As we can see in the above talent connection got closed and on terminal its written that telnet connection closed by foreign host.    On wire shark we can see that after attack happened successfully RST packet is sent. |
|  | Launching the attack automatically |
|  | Launching the attack after connection is established.      This time the connection did not closed automatically even after changing the interface. |
| Task 3: | TCP Session Hijacking |
|  | telnet connection established successfully and next sequence no 3912338564      My telnet connection got frozen after attack and I can’t do anything except forceful terminal close.  Attacker terminal here we can see the pay load at last line.      All the packet transmitted shown in Wireshark |
| Task 4: | Creating Reverse Shell using TCP Session Hijacking |
|  | Connection stabilised successfully between users.    After attack we can see that we got the shell of the victim machine.      Wireshark we can see that all the TCP connection are retransmitted. |