|  |  |  |
| --- | --- | --- |
| Name: Adarsh Kumar | SRN No: PES2UG20CS016 | Assignment No: 02 |
| Section: B | Date: 02/09/2022 |

|  |  |
| --- | --- |
| Task 2.1 A | Understanding how a Sniffer Works |
| Output Screenshot | Host-A Terminal:    From host-A pinging IP 10.9.0.1 and sent 13 packets  Attacker Terminal:    Attacker sniffing packets from host-A and gathering information such destination IP & host IP. |
| Question 1: | Describe the sequence of the library calls that are essential for sniffer programs.  This is meant to be a summary?  Ans: Fundamental function calls that are used for sniffing programs include   1. Determining and setting up type of ethernet interface that the program will utilize. 2. The initialization of the PCAP to create a session, typically there is on session per device to be sniffed. 3. The call to set traffic filtering rules, this ensures that the type of traffic sniffed on an interface is the type one is going for. 4. The execution of the sniff. 5. Termination of the session |
| Question 2: | Why do you need the root privilege to run sniffex? Where does the program fail if executed without the root privilege?  Ans: In Linux whenever network interfaces need to be access it is required to have root access, in this case, the program needs the ability to utilize raw sockets to send packets in the way it does, without the root user capacities the Network Interface Card would be inaccessible hence the ability to use/create raw sockets is lost.  Screenshots: |
| Question 3: | Please turn on and turn off the promiscuous mode in your sniffer program. The value 1 of the third parameter in the pcap\_open\_live() function turns on the promiscuous mode (use 0 to turn it off).  Ans: switching of the promiscuous mode will not let us see network traffic of other IP address i.e those IP address which are not ours and it will not allow us to use both wifi and network ethernet at same time.  Output screenshots:  Host-A Terminal: I am pinging to IP 10.9.0.6    Attacker Terminal:    If we switch of the promiscuous mode then we are unable to sniff packet which are not intended for our IP. |
| Task 2.1 B | Capture the ICMP packets between two specific hosts? |
| Output Screenshot | Host-A Terminal  From host-A pinging to 10.9.0.6, 9 packet transmitted .    Attacker Terminal:  On attacker terminal all ICMP packet received send by the host-A. |
| Q) | Capture the TCP packets that have a destination port range from to sort 10 - 100. |
| Output Screenshot | Host-A Terminal:  Pinging to telnet 10.9.0.6 it will initiate a TCP connection to login to telnet portal.    Attacker Terminal    As we can see that the Protocol field IS TCP now it is capturing TCP packets only. |
| Task 2.1 C | Please show how you can use your sniffer program to capture the password when somebody is using telnet on the network that you are monitoring |
| Output Screenshot | Host-A Terminal:  Host -A is trying to login to the telnet portal by pinging to telnet IP 10.9.0.6    Attacker Terminal:    As we can see in the above picture that when host-A was logging to telnet portal our program sniffed that packet and able to locate information like login ID and login Password. As well as the telnet welcome page. |
| Task 2.2 | Spoof an ICMP Echo Request packets |
| Output Screenshot | Attacker Terminal:  Trying to spoof a echo request packet with IP of 1.2.3.4  Wireshark:    In Wireshark we can see that a packet is sent to IP of 10.9.0.6 from IP source IP 1.2.3.4  And echo reply is also being sent to 10.9.0.6 |
| Question 4: | Using the raw socket programming, do you have to calculate the checksum for the IP header?  Ans: With the raw socket programming, checksum is not to be calculated separately. This is because Ubuntu calculate the checksum of IP header before transmitting it, irrespective of the fact whether the value is mentioned or not.  The kernel or the underlying operating system builds the packet including the checksum for your data.  NOTE: ICMP IP packet will not be formed if some arbitrary value is given to the IP length field. This is because the length should actually be the sum of the size of IP header and the size of the ICMP header. If the condition is not met, the packet is considered unfit and dropped away, thus yielding of failed attack. |
| Question 5: | Why do you need the root privilege to run the programs that use raw  sockets? Where does the program fail if executed without the root privilege?  Ans: yes, need root privilege to run raw program. To perform the spoofing of the packets, we need to have the access to an NIC. In short this is how it is defined by the authorities who set networking rules. Due to the fact one can create custom packets that could prove detrimental to a network configuration. |
| Task 2.3 | Sniff and then Spoof at same time? |
|  | While complaining got some warning request invigilator to explain why    Host-A Terminal:    Pinging to some non-existing IP address 1.2.3.4 but still able to ping then.  Attacker Terminal:    As we can see that messages that are sent from 10.9.0.5 are sniffed here and it is using ICMP protocol. Message are intended for the IP 1.2.3.4 |
| Wireshark | We can see in Wireshark both ICMP echo request and response messages are exchanged between IP 10.9.0.5 and 1.2.3.4 |