|  |  |  |
| --- | --- | --- |
| Name: Adarsh Kumar | SRN No: PES2UG20CS016 | Assignment No: ICMP Attack |
| Section: B | Date: 20/10/2022 |

|  |  |
| --- | --- |
|  | **Task 1: Launching ICMP Redirect Attack** |
| Screenshot  of command | # ip route  # sysctl net.ipv4.conf.all.accept\_redirects=1  We stopped the counter measure of the ICMP Redirect attack |
| Task 1A | make the Victim Machine route its packets through the Malicious router |
|  | Here from victim’s terminal we are trying to ping host 192.168.60.5    When the victim was pinging the host, we launched a ICMP redirect attack which sent redried message to the victim machine        We can see in the cache of the victim container that it is trying to reach host 198.168.60.5 from our malicious-Router 10.9.0.111 not from the genuine router 10.9.0.11 this can be also observed via mtr command clearly. |
| Question 1: | Can you use ICMP redirect attacks to redirect to a remote machine? Namely, the IP address assigned to icmp.gw is a computer not on the local LAN. Please show your experiment result, and explain your observation. |
| Solution | NO, we cannot use ICMP redirect attacks to redirect to a remote machine.  There are usually two situations in which an ICMP redirect occurs:  1) When the router receives data from an interface and needs to forward the data from the same interface;  2) When the router finds that the source IP address and the next hop belong to the same network segment when sending data to the remote network from an interface.  Both of these conditions require the redirected address to be on the same LAN as itself. If the redirected gateway points to an address not on the same LAN (eg 8.8.8.8), it will not be written to the victim's cache.  NOTE: (Since it has not been written, the screenshot is not shown) |
| Question 2: | Can you use ICMP redirect attacks to redirect to a non-existing machine on the same network? Namely, the IP address assigned to icmp.gw is a local computer that is either offline or non-existing. Please show your experiment result, and explain your observation |
| Solution | I cannot use ICMP redirect attacks to redirect to a non-existing machine on the same network. I tried to direct the victim message to a non-existent URL 10.9.0.10, and the figure appeared:    As can be seen from the figure, after receiving the reconnection, the victim will look for the MAC address of the target website through ARP, and at the same time maintain the original connection. However, since the MAC address of the target URL is not found, the original transmission is maintained.  During the experiment, I tried to direct the packet to 10.9.0.105, and found that IP forwarding was not turned on, so a redirect packet was sent to the victim. As shown in the figure:    At the same time, it can be associated with the previous question and the ARP poisoning experiment at the same time as SEED: it can deceive the existence of a non-existent URL to tell the victim, and direct the packet to the attacker's host, while hiding the attacker's real IP. address. |
| Question 3: | If you look at the docker-compose.yml file, you will find the following entries for the malicious router container. What are the purposes of these entries? Please change their value to 1, and launch the attack again. Please describe and explain your observation |
| Solution | As shown in the figure, and the test results I got in the previous question, our malicious router sent the redirect message by itself: |
|  | **Task 2: Launching the MITM Attack** |
|  | Wireshark    We can see that TCP packet are retransmitted and the message is also present there. |
| Task 2B | To launch the MITM Attack |
|  | Turning off IP forwarding on malicious router terminal    Now launching the man in the middle attack    Sending a message from victim container to host    As we can observe that the message is changed here that means our message might have been intersected in the middle and changed.    This confirmed that message is sent to the malleolus server and it was changed there. |
| Question 4: | In your MITM program, you only need to capture the traffic in one direction. Please indicate which direction, and explain why. |
| Solution | Because we only induce the sending direction to the victim host, only the victim will send the message to the malicious route, but not to the target host, so there is no need to formulate the message for the opposite direction (yes, but not necessary) |
| Question 5: | In the MITM program, when you capture the nc traffic from A (10.9.0.5), you can use A’s IP address or MAC address in the filter. One of the choices is not good and is going to create issues, even though both choices may work. Please try both, and use your experiment results to show which choice is the correct one, and please explain your conclusion. |
| Solution | MAC addresses should be used for filtering, because using IP can create forwarding storms.  Which can be seen in the below Wireshark screenshot. |