|  |  |  |
| --- | --- | --- |
| Name: Adarsh Kumar | SRN No: PES2UG20CS016 | LAB No:03 |
| Section: B | Date: 10/09/2022 |

Attacker (Host M) - 10.9.0.105

Host A - 10.9.0.5

Host B - 10.9.0.6

|  |  |
| --- | --- |
| **Task 1: ARP Cache Poisoning** | |
| Task 1.A: | Using ARP request |
| Output  Screenshot  -- Without Ether | Before Attack:  Host A:    Host B:    Attacker M: |
| After attack screenshot | Host-A    Host-B    After clearing the cache on Host-A |
| Observation | Without ether we can see that, Viewing the ARP table on host A, it can be seen that the MAC address corresponding to host B is the MAC address of host M. the attack is successful. And in host B we don’t have any cache entry. |
| Output  Screenshot  -- with Ether | Before Attack:  Host A:    Host B:    Attacker M:    After Attack:  Host A:      Host B:    After clearing the cache on Host A: |
| Observation | We can see that after using ether, ARP table of Host A contains only one entry of IP address 10.9.0.6, We have the mapping for the attacker map to Host B’s IP and is host B’s terminal the cache is still empty. |
| Question | Q) What does the ‘op’ in the screenshot of the attacker machine signify? What is its default value?  Ans: Opcode — When its value is 2 it means it’s an ARP Response and when it is 1 it means it’s an ARP Request. Default op is 1.  Q) What was the difference between the ARP cache results in the above 2 approaches? Why did you observe this difference?  Ans: when we use without out ether OS puts the Arp and when we use with ether, we specify the ARP source and destination. |
| Task 1. B | Using ARP Reply |
| Scenario 1  B’s IP is already in A’s cache.  Output  Screenshot | Before attack  Host -A    Host - B    Attacker – Terminal  Running the Attack11.py file create a cache entry in Host A  After Attack  Host - A    Here we see that a valid IP is mapped to the MAC address of Host B.  Host -B |
| Scenario 2  B’s IP is not in A’s cache.  Output  Screenshot | Before Attack  Host - A    Attacker – Terminal    Here we can see that the OP = is-at that means ARP reply.  After attack  Host- A  There is no cache entry, this is because the cache could only be poisoned if there is a pre-existing cache. So, if there are no cash details already existed the we can’t do cache poisoning attack. |
| Question | What does op=2 mean?  Ans: When OP value is 2 it means it is an ARP Response/Reply from Attacker to the host. |
| Task 1.C | Using ARP Gratuitous Message |
| Scenario 1  Output  Screenshot | Attacker – Terminal  Host – A ARP cache    Host – B ARP cache    tcpdump command in Host – A and Host – B to sniff packets.  Before attack  HOST-A    HOST - B    ATTACKER TERMINAL    After the attack  Host – A and ARP cache    Host – B and ARP cache |
| Observation | The source and destination IP addresses are the same, and they are the IP address of the host issuing the gratuitous ARP.  The destination MAC addresses in ARP header and Ethernet header are the broadcast MAC address (ff:ff:ff:ff:ff:ff).  we can see that in the HOST-A ARP Table the mapping of B is holding the MAC address of the attacker. Hence the cache is poisoned. |
| Scenario 2  Output  Screenshot | Clearing the ARP cache    Attacker – terminal  After Attack  Host – A    Host – B    There are no entries in the cache, so this clears that statement that a cache can be poisoned only if there are pre-cache entries are present. |
| Question | Why does VM B’s ARP cache remain unchanged in this approach even though the packet was broadcasted on the network?  Ans: In this approach host machine update outdated information on all the other machine’s ARP cache. The destination MAC address in both the ARP header and Ethernet header are the broadcast MAC address.  Even though the packet is broadcasted, the ARP cache remains unchanged because the attack is done only on the Host A.  Yes, on Host B ARP cache table we can see that all the 3 approach the result is same. |
| **Task 2** | **MITM Attack on Telnet using ARP Cache Poisoning** |
| Step 1 | Launch the ARP cache poisoning attack |
| Output Screenshot | Attacker’s terminal    After Attack  Host - A    Host -B    After attack    Host -A    Host – B    We can see that an entry of 10.9.0.5 is created in the Host -A. |
| Step 2 | Testing |
| Output | Attacker- Terminal    Host – A pinging to Host - B    Host – B ARP cache      Wite shark |
| Observation | We can observe that no response is obtained in the Wireshark. |
| Task 3 | Turn on IP Forwarding |
|  | Attacker- Terminal    Host -A pinging to Host -B    Wireshark Screenshot |
| Observation | Now we turn on the IP forwarding on Host M, so it will forward the packets between A and B.  In the ICMP request packet, the destination address of the link layer is the MAC address of host M, and the source address is the MAC address of host A. The destination address of the IP layer is the IP address of host B.  After receiving the packet, host M modifies the MAC address of the link layer. The destination MAC is the MAC address of host B and the source MAC is its own MAC address. Therefore, the IP layer is that the source address is host A and the destination address is host B, but the link layer is sent from host M to host B. |
| Task 4 | Launch the MITM Attack. |
|  | Attacker Terminal    Host-A    first turn on the data forwarding function on host M, then telnet machine B on machine A, enter the user’s name and password, you can connect, you can normally enter commands and return results.  Wire shark |
|  | Now to perform the Man in the Middle Attack    after establishing the connection, use the following command to turn off IP forwarding.  Enter some content in A's Telnet window. If it is found that it cannot be entered, press enter  after establishing the connection, turn off packet forwarding on machine M and run ARP cache poisoning attack and contracting program.  Attacker – Terminal after establishing connection  Hoat -A    the result is as follows: no matter what is entered, z will be displayed, even if enter, which will make it impossible to execute the command.  However, in the experiment, it is found that the input command can be displayed as the originally set Z, but when a string of characters is input, only the first few letters can be displayed as Z. And the input can be recovered soon. Guess whether it is caused by the short attack time limit on the two hosts and the timely update of the ARP table.  Wireshark |
| Observation | As we can see that in Wireshark it first tries to find who is 10.9.0.5 then we can see that its message is redirected to Attacker ‘s IP addressed and then from attacker machine it’s reaching to the host -B. |
| **Task 3** | **MITM Attack on Netcat using ARP Cache Poisoning** |
| Output screenshot | Attacker      Host - A    Host – B |
| Wireshark |  |
| Observation | When we try to send a 6-letter word (The length of the sequence should be 6, or you will mess up the TCP sequence number) from Host -A it first redirects to host then goes to B. |

THE END