Explanation of step 7, 6 (ping)

A ping is way of using a network utility to test the connectivity and measure the response time between the two devices. The process begins with the source PC1 sending an ICMP (Internet Control Message Protocol) Echo Request packet to the destination PC2. This packet includes a sequence number and a timestamp. The Echo Request packet travels through the network, passing through various routers and switches until it reaches the destination PC. Upon arrival, the destination PC2 recognizes the request and responds with an ICMP Echo Reply packet, which includes the same sequence number and timestamp.

The Echo Reply packet then travels back through the network to the source PC1. When the source PC2 receives the reply, it calculates the round-trip time by comparing the current time with the timestamp from the original request. The results, including the round-trip time and the success or failure of the ping request, are then displayed on the source PC1. If the destination PC2 is reachable and responds, the source PC1 will show the time it took for the packet to travel to the destination PC2 and back. If the destination PC2 does not respond within a specified timeout period, an error message such as "Request timed out" or "Destination Host Unreachable" may be displayed.

Explanation of step 7, 6 (arp -a)

When you ping a PC1 from another PC2, the ARP (Address Resolution Protocol) cache tables of both devices may be updated to facilitate communication. Initially, the source PC1 checks its ARP cache to see if it already has the MAC address associated with the destination PC2's IP address. If the MAC address is not found, the source PC1 broadcasts an ARP request to the local network, asking for the MAC address corresponding to the destination IP address. Upon receiving this request, the destination PC2 replies with its MAC address. The source PC1 then updates its ARP cache with this information, storing the IP-to-MAC address mapping for future use. Similarly, the destination PC2 may also update its ARP cache with the source PC1's IP and MAC address if it doesn't already have this information. This process ensures that both PCs can effectively communicate by resolving and storing the necessary MAC addresses, thereby streamlining future network interactions.

No nothing was showing for devices were not ping for arp command

Explanation of step 12, 13 (spoofing attack)

When the command `nemesis arp -v -S <pc1 IP> -D <pc2 IP> -h <MAC of eve> -m <MAC of pc2>`, it sends a forged ARP reply to PC2, falsely indicating that the IP address of PC1 is associated with the MAC address of Eve. This causes PC2 to update its ARP cache, incorrectly mapping PC1's IP address to Eve's MAC address. Consequently, when you ping PC1 from PC2, the network traffic intended for PC1 is mistakenly sent to Eve's MAC address instead. This enables Eve to intercept or manipulate the network traffic between PC1 and PC2, a classic example of an ARP spoofing attack.