

ARP Poisoning

i). Suppose you have two machines A and B on the same network (take Virtual Machines for the same). Machine A (Client) wants to communicate with Machine B (Server) but is unaware about the MAC address of B. Hence, it sends an ARP broadcast request. Use Wireshark to study and analyse the ARP packet information. In detail, explain all the fields of an ARP packet.

In this scenario, Machine A (the client) wants to communicate with Machine B (the server) on the same network but doesn't know the MAC address of Machine B. To find out the MAC address, Machine A sends an ARP (Address Resolution Protocol) broadcast request.

1. Machine A broadcasts an ARP request packet to all devices on the local network. This ARP request contains Machine A's IP address and MAC address
2. Machine B, upon receiving the ARP request and recognizing its own IP address, responds with its MAC address directly to Machine A. This response is unicast, meaning it's sent only to Machine A.
3. Upon receiving the response, Machine A updates its ARP cache with the MAC address of Machine B. This allows Machine A to communicate directly with Machine B in subsequent network communications without needing to perform another ARP broadcast

Capturing from enp0s3

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	10.0.2.15	142.250.193.66	TLSv1.2	93	Application Data
2	0.001442497	142.250.193.66	10.0.2.15	TCP	60	443 → 55116 [ACK] Seq=1 Ac
3	0.011564497	142.250.193.66	10.0.2.15	TLSv1.2	93	Application Data
4	0.011682951	10.0.2.15	142.250.193.66	TCP	54	55116 → 443 [ACK] Seq=40 A
5	5.092781437	PCSSystemtec_c7:f9:81	52:54:00:12:35:02	ARP	42	who has 10.0.2.2? Tell 10.
6	5.093801600	52:54:00:12:35:02	PCSSystemtec_c7:f9:81	ARP	60	10.0.2.2 is at 52:54:00:12

Frame 5: 42 bytes on wire (336 bits), 42 bytes captured (336 bits) on enp0s3

Ethernet II, Src: PCSSystemtec_c7:f9:81 (08:00:27:c7:f9:81), Dst: 01:00:00:00:00:00 (01:00:00:00:00:00)

Address Resolution Protocol (request)

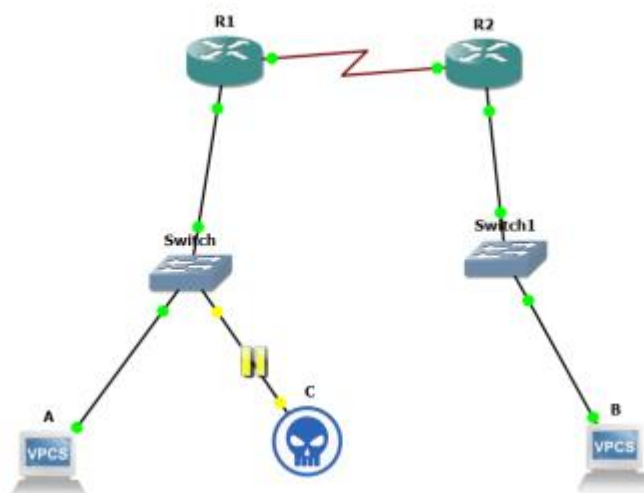
Hardware type: Ethernet (1)
Protocol type: IPv4 (0x0800)
Hardware size: 6
Protocol size: 4
Opcode: request (1)
Sender MAC address: PCSSystemtec_c7:f9:81 (08:00:27:c7:f9:81)
Sender IP address: 10.0.2.15
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 10.0.2.2

Capturing from enp0s3						
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help						
Apply a display filter ... <Ctrl-/>						
No.	Time	Source	Destination	Protocol	Length	Info
2	0.001442497	142.250.193.66	10.0.2.15	TCP	60	443 → 55116 [ACK] Seq=1 A
3	0.011564497	142.250.193.66	10.0.2.15	TLSv1.2	93	Application Data
4	0.011682951	10.0.2.15	142.250.193.66	TCP	54	55116 → 443 [ACK] Seq=40
5	5.092781437	PCSSystemtec_c7:f9:...	52:54:00:12:35:02	ARP	42	Who has 10.0.2.2? Tell 10
6	5.093801600	52:54:00:12:35:02	PCSSystemtec_c7:f9:...	ARP	60	10.0.2.2 is at 52:54:00:1
7	50.796539617	10.0.2.15	142.250.193.66	TLSv1.2	93	Application Data
8	50.797068642	10.0.2.15	142.250.193.66	TLSv1.2	78	Application Data
9	50.797109718	142.250.193.66	10.0.2.15	TCP	60	443 → 55116 [ACK] Seq=40
10	50.797900986	10.0.2.15	142.250.193.66	TCP	54	55116 → 443 [FIN, ACK] Se
11	50.798795342	142.250.193.66	10.0.2.15	TCP	60	443 → 55116 [ACK] Seq=40
12	50.798795619	142.250.193.66	10.0.2.15	TCP	60	443 → 55116 [ACK] Seq=40
13	50.803959886	142.250.193.66	10.0.2.15	TCP	60	443 → 55116 [FIN, ACK] Se
14	50.803990460	10.0.2.15	142.250.193.66	TCP	54	55116 → 443 [ACK] Seq=104
15	50.8039945355	PCSSystemtec_c7:f9:...	52:54:00:12:35:02	ARP	42	Who has 10.0.2.2? Tell 10
16	56.040711525	52:54:00:12:35:02	PCSSystemtec_c7:f9:...	ARP	60	10.0.2.2 is at 52:54:00:1

Frame 6: 60 bytes on wire (480 bits), 60 bytes captured (480 bits)	0000	08 00 27 c7 f9 81 52 54 00 1
Ethernet II, Src: 52:54:00:12:35:02 (52:54:00:12:35:02), Dst: PCSS	0010	08 00 06 04 00 02 52 54 00 1
Address Resolution Protocol (reply)	0020	08 00 27 c7 f9 81 0a 00 02 0
Hardware type: Ethernet (1)	0030	00 00 00 00 00 00 00 00 00 0
Protocol type: IPv4 (0x0800)		
Hardware size: 6		
Protocol size: 4		
Opcode: reply (2)		
Sender MAC address: 52:54:00:12:35:02 (52:54:00:12:35:02)		
Sender IP address: 10.0.2.2		
Target MAC address: PCSSystemtec_c7:f9:81 (08:00:27:c7:f9:81)		
Target IP address: 10.0.2.15		

ii). Consider Machines A and B on different networks. Consider another machine C (you may take it as a default gateway). Create a scenario in which ARP MAC entry corresponding to Machine B is poisoned in the local ARP cache of Machine A and instead a MAC entry of Machine C is placed and returned. Similarly, to Machine B, the corresponding entry to Machine C is there instead of A. (Machine C acting as a mediator and performing the Man-in-the-Middle attack). Show the packet transmission being carried out after ARP Poisoning.

Initial Setup: Machines A and B are on different networks. Machine C is positioned between A and the gateway/router for A's network.



ARP Poisoning: Machine C sends ARP spoofed packets to Machine A and the router, claiming to be the router. Both Machine A and the router update their ARP cache with Machine C's MAC address associated with the router's IP address.

Man-in-the-Middle Setup: Machine C now intercepts traffic between Machine A and the router.

Packet Transmission from A to C to B: When A wants to communicate with B, it sends packets to the router, but they're intercepted by C. C inspects/modifies the packets and forwards them to B.

MitM Attack Execution: B responds to the intercepted packets, thinking they're from the router. C intercepts these responses, potentially modifying them, before forwarding them to A.

Inspection and Manipulation: Throughout, C can inspect, modify, or drop packets, potentially compromising the communication between A and B

