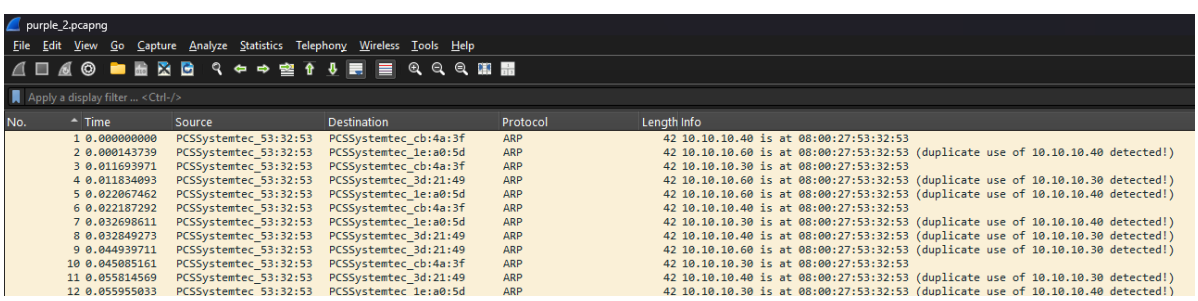
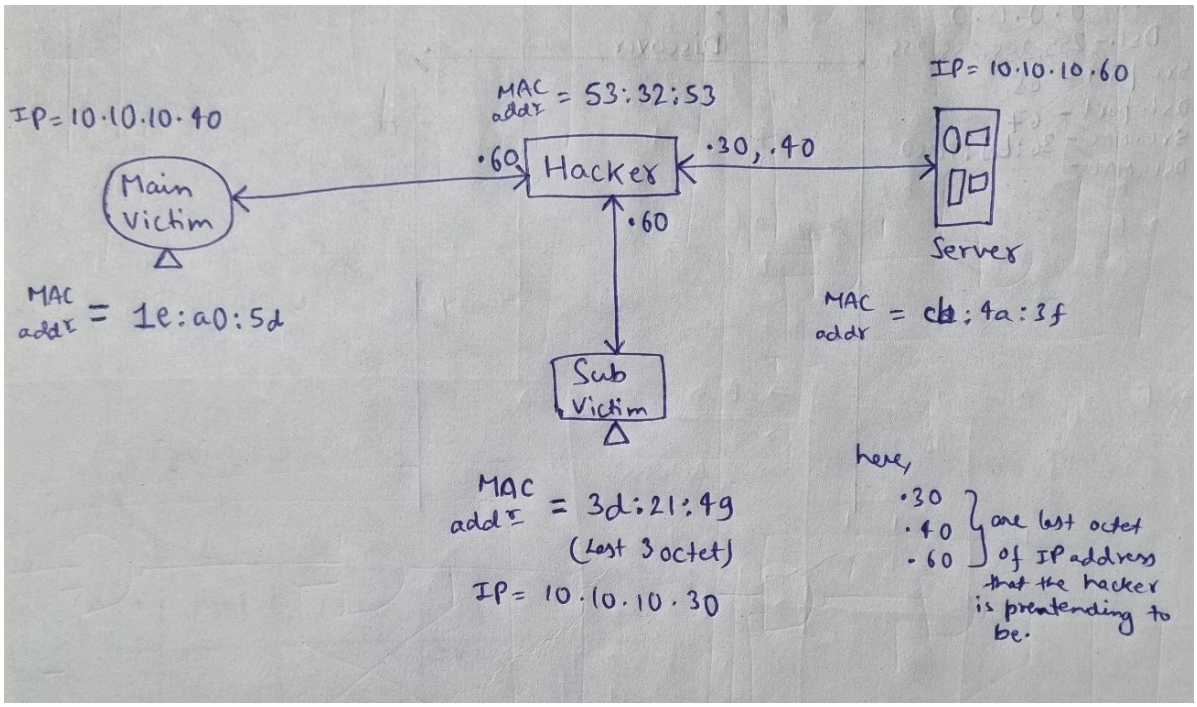
Scenario 2 - Something is wrong!

- From the first 12 packets we can observe that the device having MAC address 08:00:27:53:32:53 is multicasting unsolicited ARP reply packets (reply without response) to multiple hosts that includes MAC addresses 08:00:27:cb:4a:3f, 08:00:27:1e:a0:5d, 08:00:27:3d:21:49.
- For simplicity let's give short names to devices that are as follows:
  1. MAC address 08:00:27:53:32:53 = HACKER
  2. MAC address 08:00:27:cb:4a:3f = SERVER
  3. MAC address 08:00:27:1e:a0:5d = MAIN VICTIM
  4. MAC address 08:00:27:3d:21:49 = SUB VICTIM
- By carefully analysing the ARP packet, IP address and MAC address we can say that HACKER is trying to pretend as SERVER, to the MAIN VICTIM and SUB VICTIM, and HACKER is trying to pretend itself as MAIN VICTIM and SUB VICTIM to SERVER, Thus, HACKER in this case is performing Man in the middle ARP poisoning attack.
- Screenshot



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	PCSSystemtec_53:32:53	PCSSystemtec_cb:4a:3f	ARP	42	10.10.10.40 is at 08:00:27:53:32:53
2	0.000143739	PCSSystemtec_53:32:53	PCSSystemtec_1e:a0:5d	ARP	42	10.10.10.60 is at 08:00:27:53:32:53 (duplicate use of 10.10.10.40 detected!)
3	0.011693971	PCSSystemtec_53:32:53	PCSSystemtec_cb:4a:3f	ARP	42	10.10.10.30 is at 08:00:27:53:32:53
4	0.011834093	PCSSystemtec_53:32:53	PCSSystemtec_3d:21:49	ARP	42	10.10.10.60 is at 08:00:27:53:32:53 (duplicate use of 10.10.10.30 detected!)
5	0.022067462	PCSSystemtec_53:32:53	PCSSystemtec_1e:a0:5d	ARP	42	10.10.10.60 is at 08:00:27:53:32:53 (duplicate use of 10.10.10.40 detected!)
6	0.022187292	PCSSystemtec_53:32:53	PCSSystemtec_cb:4a:3f	ARP	42	10.10.10.40 is at 08:00:27:53:32:53
7	0.032698611	PCSSystemtec_53:32:53	PCSSystemtec_1e:a0:5d	ARP	42	10.10.10.30 is at 08:00:27:53:32:53 (duplicate use of 10.10.10.40 detected!)
8	0.032849273	PCSSystemtec_53:32:53	PCSSystemtec_3d:21:49	ARP	42	10.10.10.40 is at 08:00:27:53:32:53 (duplicate use of 10.10.10.30 detected!)
9	0.044939711	PCSSystemtec_53:32:53	PCSSystemtec_3d:21:49	ARP	42	10.10.10.60 is at 08:00:27:53:32:53 (duplicate use of 10.10.10.30 detected!)
10	0.045085161	PCSSystemtec_53:32:53	PCSSystemtec_cb:4a:3f	ARP	42	10.10.10.30 is at 08:00:27:53:32:53
11	0.055814569	PCSSystemtec_53:32:53	PCSSystemtec_3d:21:49	ARP	42	10.10.10.40 is at 08:00:27:53:32:53 (duplicate use of 10.10.10.30 detected!)
12	0.055955033	PCSSystemtec_53:32:53	PCSSystemtec_1e:a0:5d	ARP	42	10.10.10.30 is at 08:00:27:53:32:53 (duplicate use of 10.10.10.40 detected!)

- We can reach to following diagram after the analysis of first 12 packets:

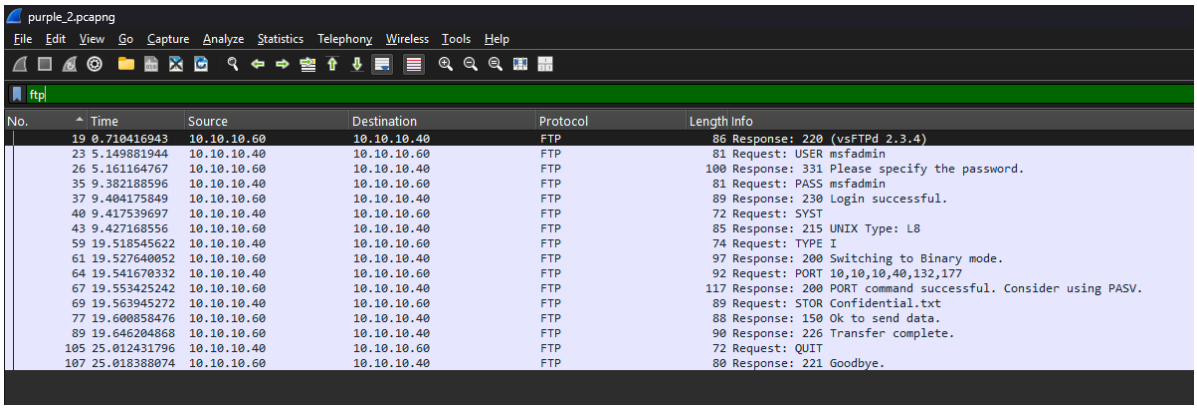


- Now after successfully poisoning the ARP Table of all the VICTIMS and SERVER, the HACKER can now capture and sniff/listen the traffic and that is what exactly happening. The HACKER is intercepting FTP packets that the MAIN VICTIM is sending to the SERVER in which we can clearly see that HACKER has intercepted following login credentials:

  `USER = msfadmin`

  `PASSWORD = msfadmin`

- Also the HACKER has intercepted the file name as `confidential.txt` that is being transferred from SERVER to the MAIN VICTIM. After that (after packet 69) the connection is closed using FIN, ACK, FIN, ACK, four way handshake.
- Screenshot:



No.	Time	Source	Destination	Protocol	Length	Info
19	0.710416943	10.10.10.60	10.10.10.40	FTP	86	Response: 220 (vsFTPd 2.3.4)
23	5.149881944	10.10.10.40	10.10.10.60	FTP	81	Request: USER msfadmin
26	5.161164767	10.10.10.60	10.10.10.40	FTP	100	Response: 331 Please specify the password.
35	9.382188596	10.10.10.40	10.10.10.60	FTP	81	Request: PASS msfadmin
37	9.404175849	10.10.10.60	10.10.10.40	FTP	89	Response: 230 Login successful.
40	9.417539697	10.10.10.40	10.10.10.60	FTP	72	Request: SYST
43	9.427168556	10.10.10.60	10.10.10.40	FTP	85	Response: 215 UNIX Type: L8
59	19.518545622	10.10.10.40	10.10.10.60	FTP	74	Request: TYPE I
61	19.527640052	10.10.10.60	10.10.10.40	FTP	97	Response: 200 Switching to Binary mode.
64	19.541670332	10.10.10.40	10.10.10.60	FTP	92	Request: PORT 10,10,10,40,132,177
67	19.553425242	10.10.10.60	10.10.10.40	FTP	117	Response: 200 PORT command successful. Consider using PASV.
69	19.563945272	10.10.10.40	10.10.10.60	FTP	89	Request: STOR Confidential.txt
77	19.600858476	10.10.10.60	10.10.10.40	FTP	88	Response: 150 Ok to send data.
89	19.646204868	10.10.10.60	10.10.10.40	FTP	90	Response: 226 Transfer complete.
105	25.012431796	10.10.10.40	10.10.10.60	FTP	72	Request: QUIT
107	25.018388074	10.10.10.60	10.10.10.40	FTP	80	Response: 221 Goodbye.

FINAL CONCLUSION

We detected Man in the Middle ARP poisoning attack.