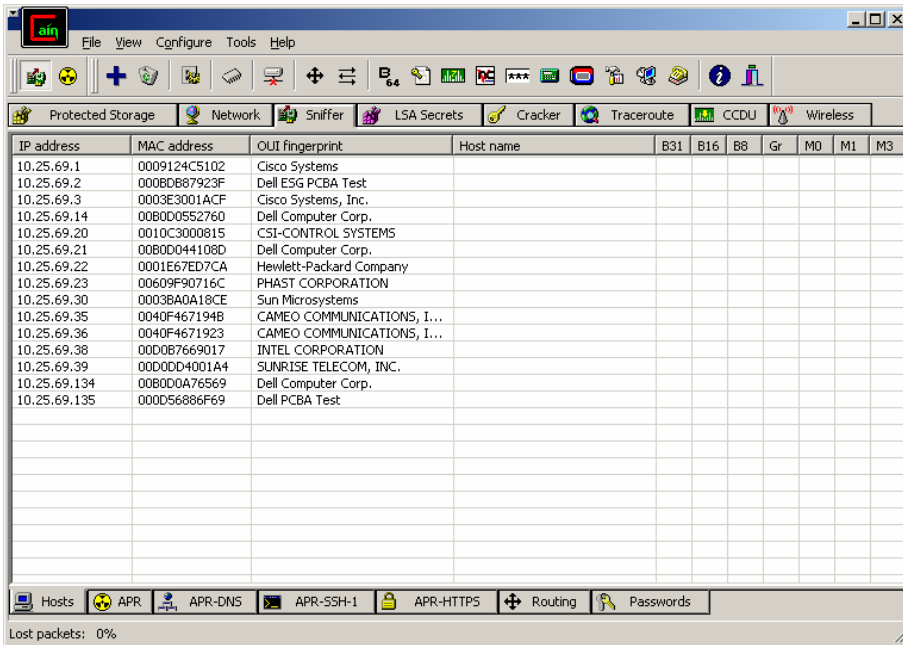
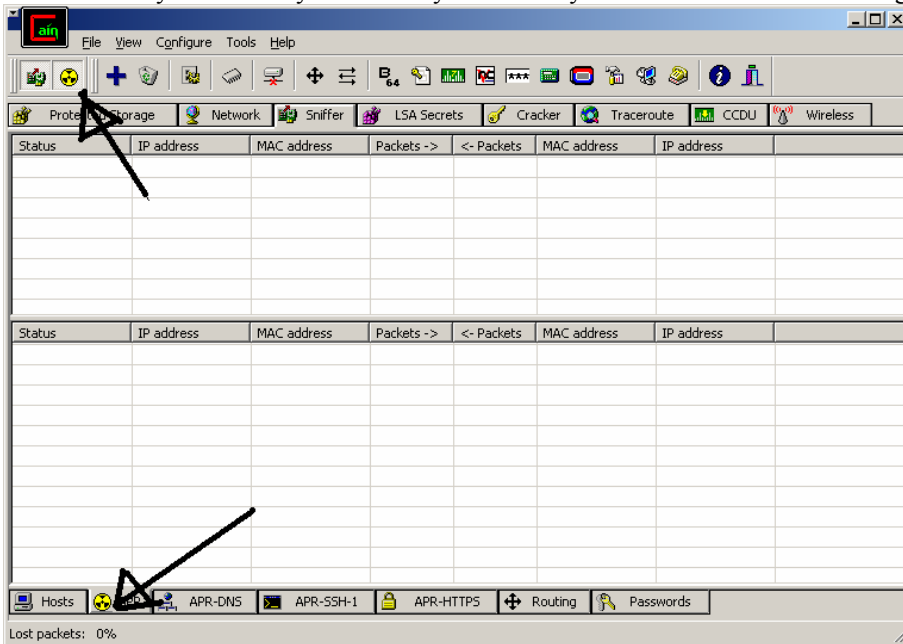


Cain and ARP Poisoning By Slimjim100

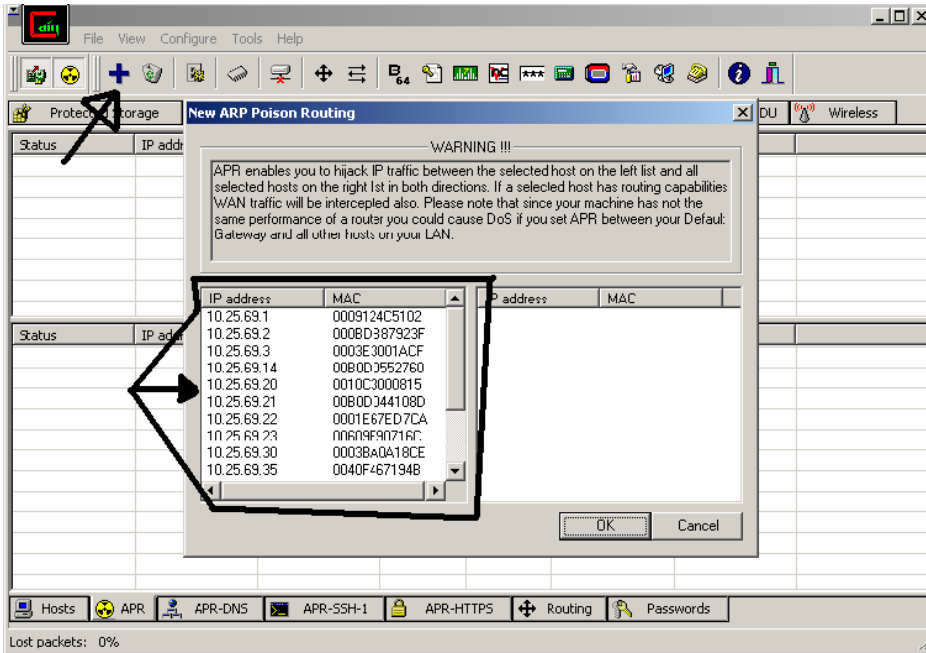
1. Turn on Cain and scan for local host on the tab labeled Sniffer



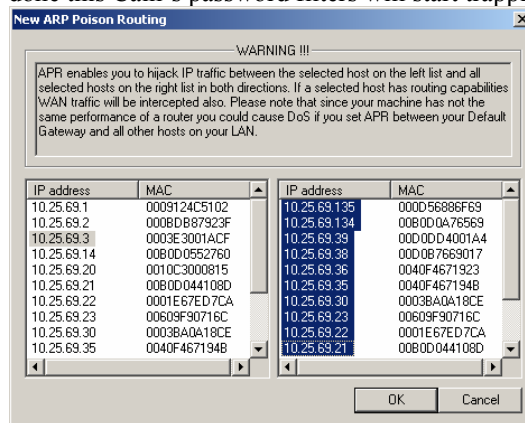
2. Now that you see how you have on your Subnet you can turn on ARP Poisoning.



3. Now you will need to add the host to the ARP Poisoning table. Click on the + sign. And select the Host to poisoning.



- The best method to getting all traffic is to highlight all hosts and any combination of the host to spoof. Once you have done this Cain's password filters will start trapping the Subnets passwords.



- Now that you're trapping password on the subnet you can also steal HTTPS certificates and send the host a fake cert. With this future it allows you to see traffic in secure sites too. Also look to the bottom tabs to see what you have collected. Under the top table you will see the routes to the host and the info you are getting. Half routing is when you can only see half the connection and in this case you can't steal the passwords. But if you also load Etherpeek in the background and record the session you can look for clues in the half-routing traffic.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.25.69.2	000BD87923F	0	0	0040F4671923	10.25.69.36
Poisoning	10.25.69.3	0003E3001ACF	0	0	000D56886F69	10.25.69.135
Poisoning	10.25.69.1	0009124C5102	0	0	0010C3000815	10.25.69.20
Poisoning	10.25.69.1	0009124C5102	0	0	00D0DD4001A4	10.25.69.39
Poisoning	10.25.69.2	000BD87923F	0	0	0003E3001ACF	10.25.69.3
Poisoning	10.25.69.2	000BD87923F	0	0	00B0D0A76569	10.25.69.134
Poisoning	10.25.69.1	0009124C5102	0	0	000BD87923F	10.25.69.2
Poisoning	10.25.69.3	0003E3001ACF	0	0	0003BADA18CF	10.25.69.30

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Half-routing	10.3.100.51	0009124C5102	6	0	0010C3000815	10.25.69.20
Full-routing	10.25.69.134	00B0D0A76569	4	3	0009124C5102	10.25.64.12

6. Now that you have been running the ARP Poisoning for a little while look at the passwords you have collected. Well to crack them you will have to send them to the crack in Cain. Remember that Cain supports Rainbow Tables so to save yourself a lot of time running dictionary and Brut forcing just run the password against the rainbow Tables and you should have your password in less than 10 minutes.

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Poisoning	10.25.69.2	000BD87923F	0	0	0040F4671923	10.25.69.36
Poisoning	10.25.69.3	0003E3001ACF	0	0	000D56886F69	10.25.69.135
Poisoning	10.25.69.1	0009124C5102	0	0	0010C3000815	10.25.69.20
Poisoning	10.25.69.1	0009124C5102	0	0	00D0DD4001A4	10.25.69.39
Poisoning	10.25.69.2	000BD87923F	0	0	0003E3001ACF	10.25.69.3
Poisoning	10.25.69.2	000BD87923F	0	0	00B0D0A76569	10.25.69.134
Poisoning	10.25.69.1	0009124C5102	0	0	000BD87923F	10.25.69.2
Poisoning	10.25.69.3	0003E3001ACF	0	0	0003BADA18CF	10.25.69.30

Status	IP address	MAC address	Packets ->	<- Packets	MAC address	IP address
Half-routing	10.3.100.51	0009124C5102	100	0	0010C3000815	10.25.69.20
Full-routing	10.25.69.134	00B0D0A76569	22	18	0009124C5102	10.25.64.12
Full-routing	10.25.69.2	000BD87923F	194	200	0009124C5102	10.25.64.10
Full-routing	10.25.69.2	000BD87923F	1	1	0009124C5102	10.3.20.14
Full-routing	10.25.69.2	000BD87923F	1	1	0009124C5102	10.3.20.13
Full-routing	10.25.69.2	000BD87923F	3	4	0009124C5102	10.25.64.12
Full-routing	10.25.69.135	000D56886F69	178	176	0009124C5102	10.25.64.10
Full-routing	10.25.69.135	000D56886F69	2	2	0009124C5102	10.3.20.13
Full-routing	10.25.69.135	000D56886F69	21	18	0009124C5102	10.25.64.12
Full-routing	10.25.69.2	000BD87923F	24	21	0009124C5102	10.62.200.96
Full-routing	10.25.69.14	00B0D0552760	8	8	0009124C5102	10.3.20.14
Full-routing	10.25.69.14	00B0D0552760	8	8	0009124C5102	10.3.20.13
Full-routing	10.25.69.2	000BD87923F	18	15	0009124C5102	10.25.64.11

Good luck and have fun!

Slimjim100