



Université Chouaib Doukkali
Ecole Nationale des Sciences Appliquées d'El Jadida
Département Télécommunications, Réseaux et Informatique



Specialization: CyberSecurity and Digital Trust

Level: 2nd Year

MINI-PROJECT

Topic:

VoIP Security Analysis and Real Attack Simulation



Conducted By:

RHOZAN Hajar

BOUKEBI Hayat

MAKMOULI Wiame

ELIRAOUI Soumia

Supervised By:

Prof. AQQAL Abdelhak

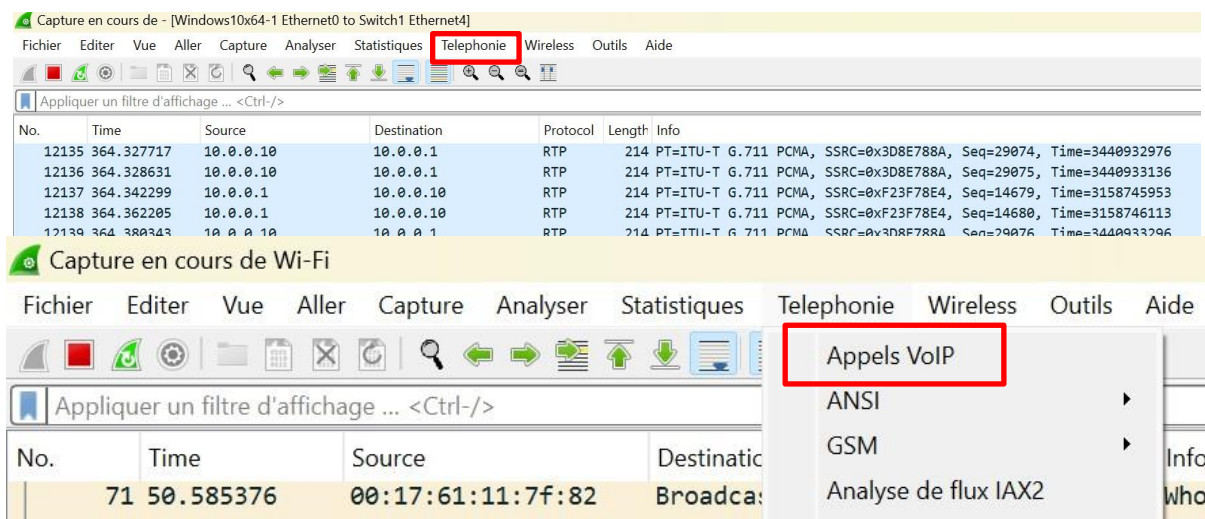
Goal

Attacks on IP telephony (ToIP) exploit vulnerabilities in VoIP networks to disrupt communications or gain unauthorized access. These attacks include eavesdropping, ARP spoofing, and switch attacks, which allow interception of calls and sensitive data. The goal of our practical work is to simulate these attacks in a real environment to understand their associated risks.

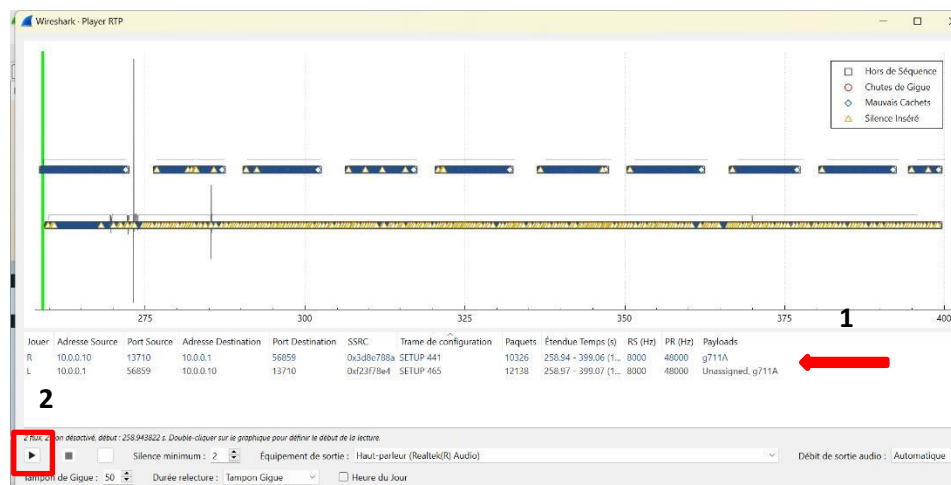
Sniffing Attack Using Wireshark:

If an attacker gains access to a target machine (physically or remotely), they can use Wireshark on the device to capture incoming and outgoing network traffic. This enables them to intercept unencrypted data, such as unsecured VoIP calls. Etapes de lancement d'attaque

- The first step to monitor traffic is to click on “Telephony” and then “VoIP Calls.”



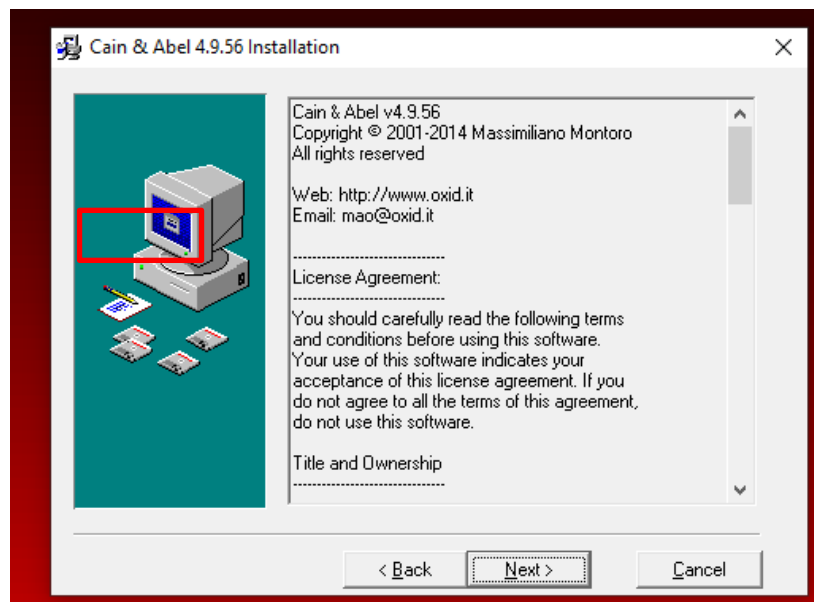
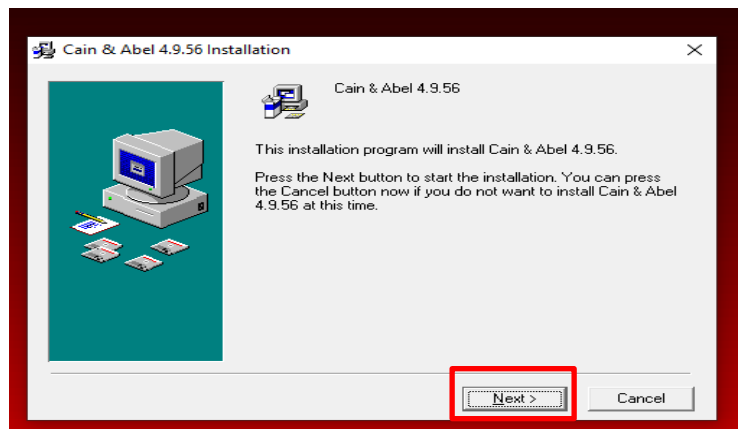
- After selecting the recording, you will see the interface below where you can listen to the traffic.

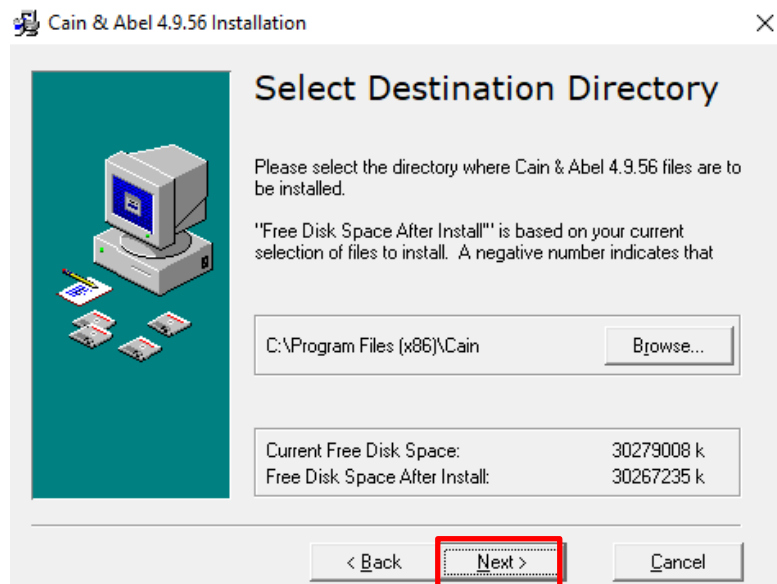


Sniffing Attack Using Cain Tool: Etapes de lancement d'attaque

Step 1: Disable Windows antivirus / Install the Cain tool

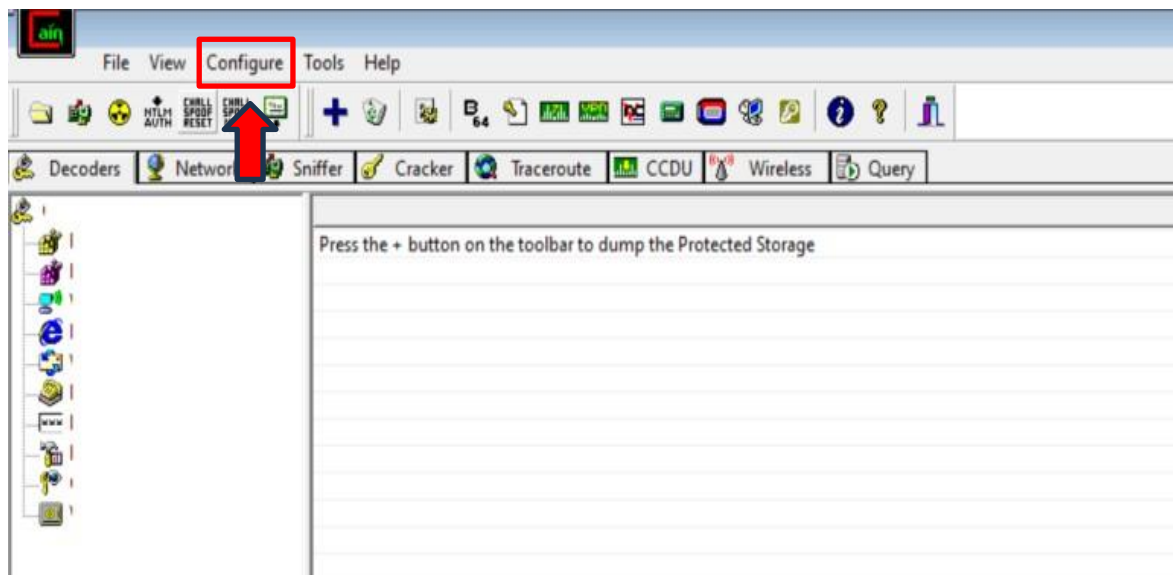
- We must first disable the antivirus to start the installation of the Cain tool.
- Here are the installation steps:



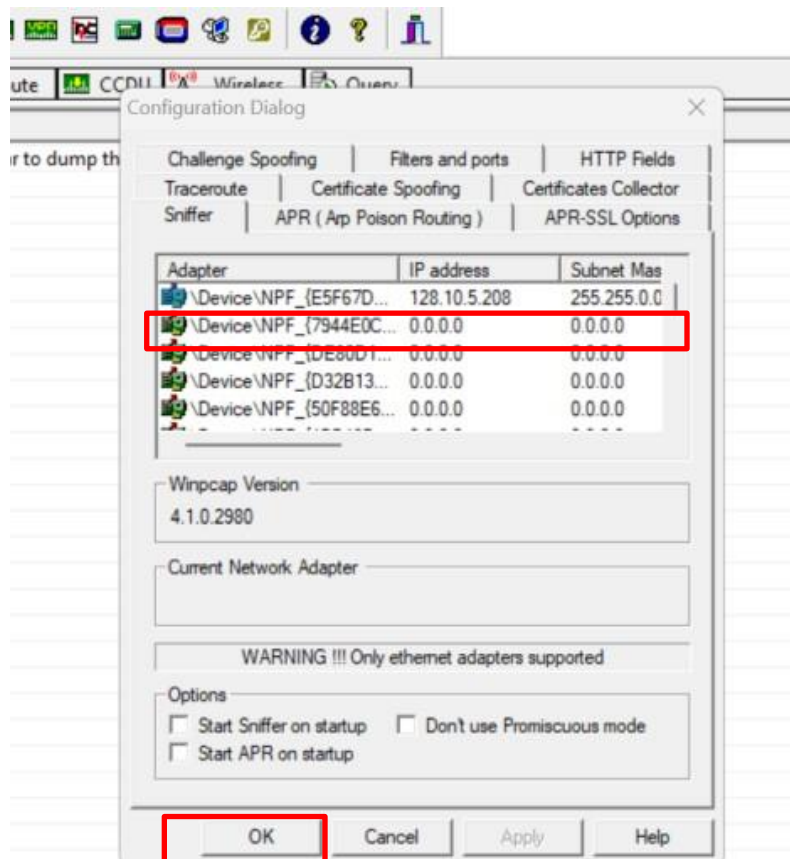


Step 2: Initial Configuration

- **Launch the Cain tool:**
Open the Cain application on your machine. It is a tool used for network security testing, particularly for MITM (Man-in-the-Middle) attacks.
- **Configure the network card:**
Go to **Configure** to select the active network card:



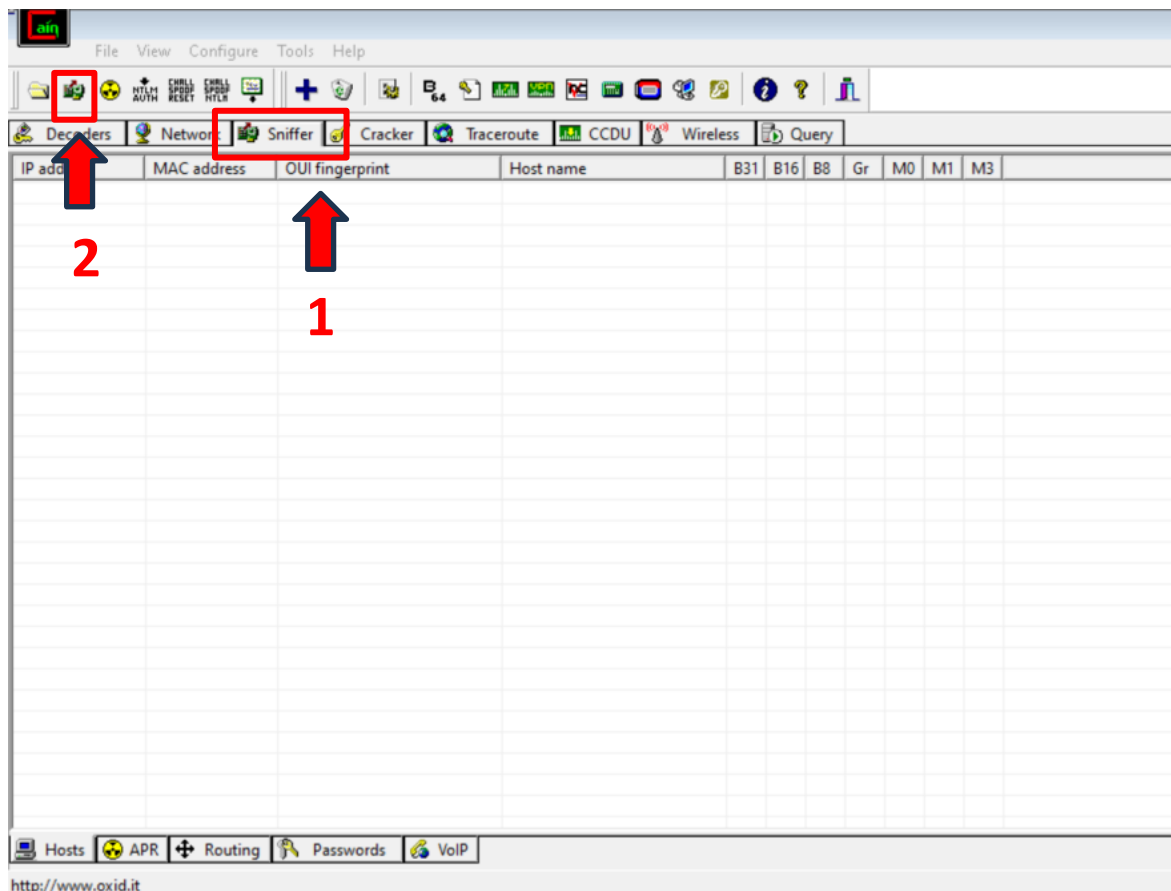
Select the Ethernet network card of your PC and confirm your settings by clicking OK:



Step 3: Enable Sniffer Mode

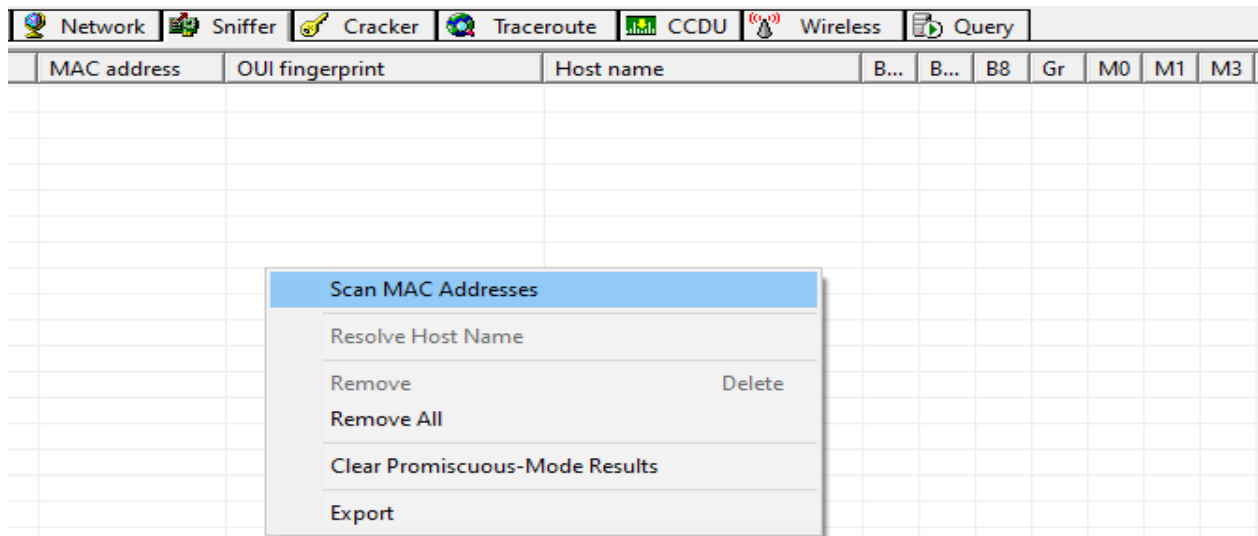
Activate the Sniffer:

Go to the **Sniffer** tab (1) and activate it by clicking the Start/Stop Scan button (2). This allows Cain to capture network traffic.



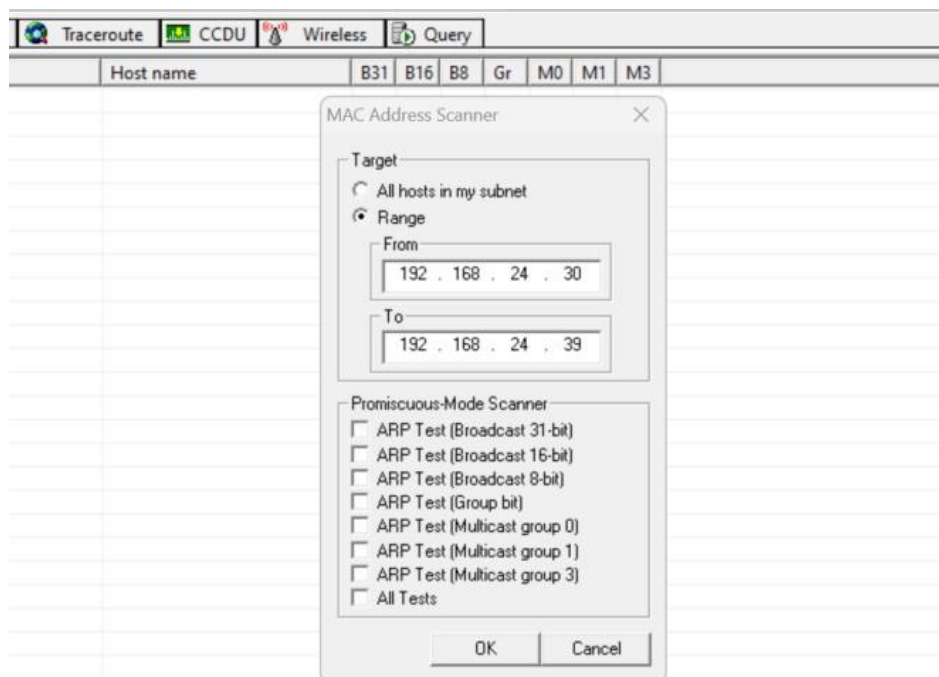
1. Analyze MAC Addresses:

Right-click and select **Scan MAC addresses**. This allows Cain to detect all devices connected to the local network.

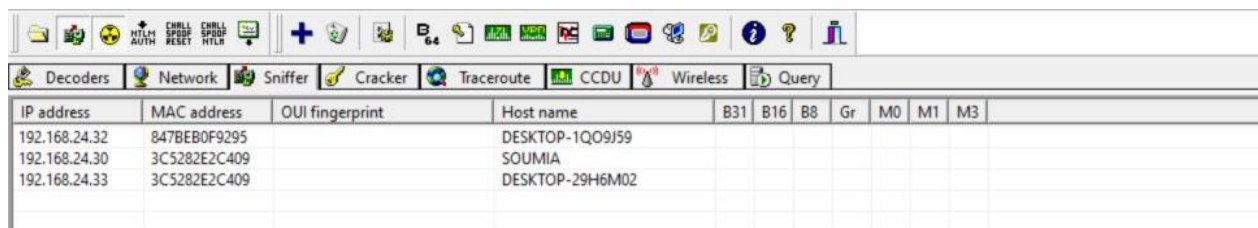


Specify the range of IP addresses to scan.

Do not check any boxes in the additional options; simply click OK.



The MAC addresses of the devices on the network will be listed.

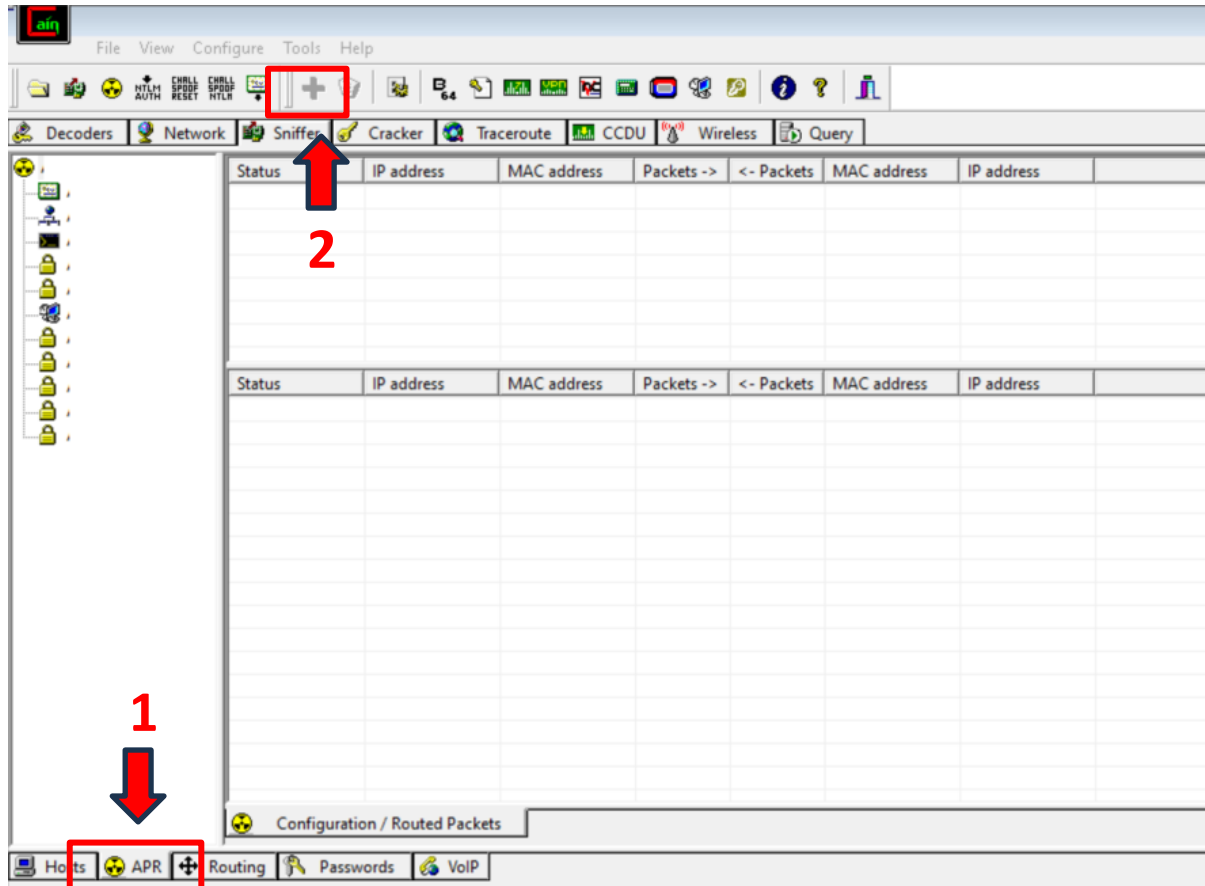


Step 4: Set Up the MITM Attack with ARP Poisoning

Access the APR tab:

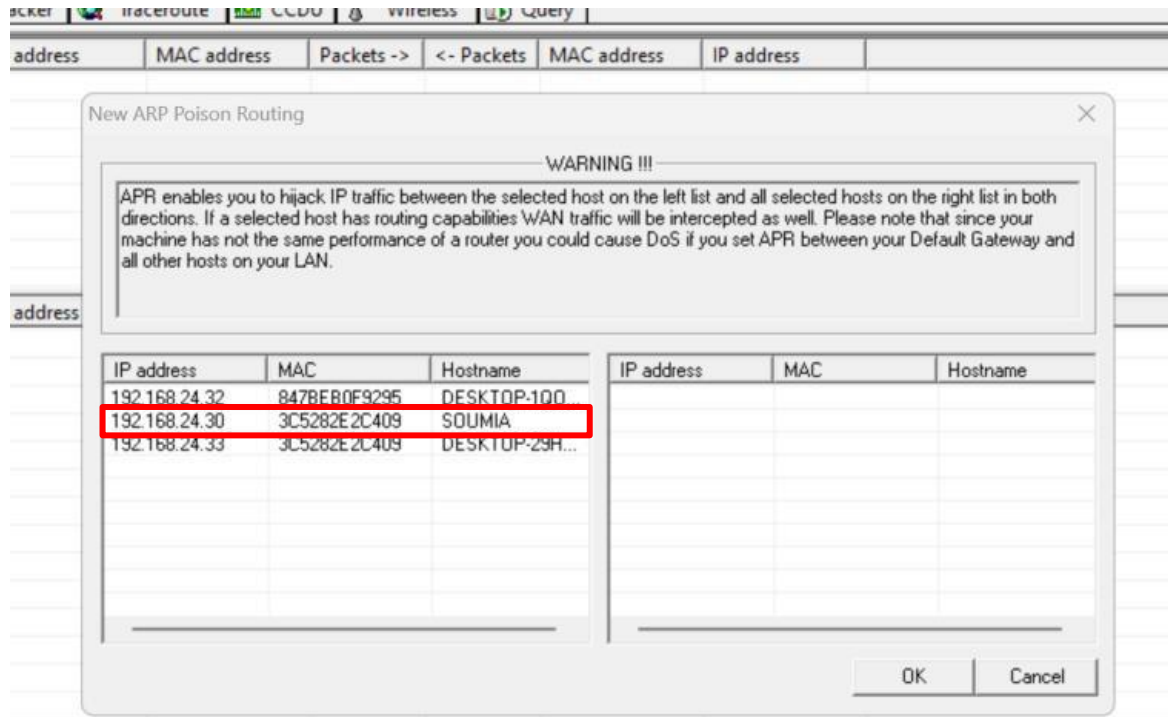
Go to the APR (Address Resolution Protocol) tab.

Click the "+" button to add an ARP Poisoning attack.



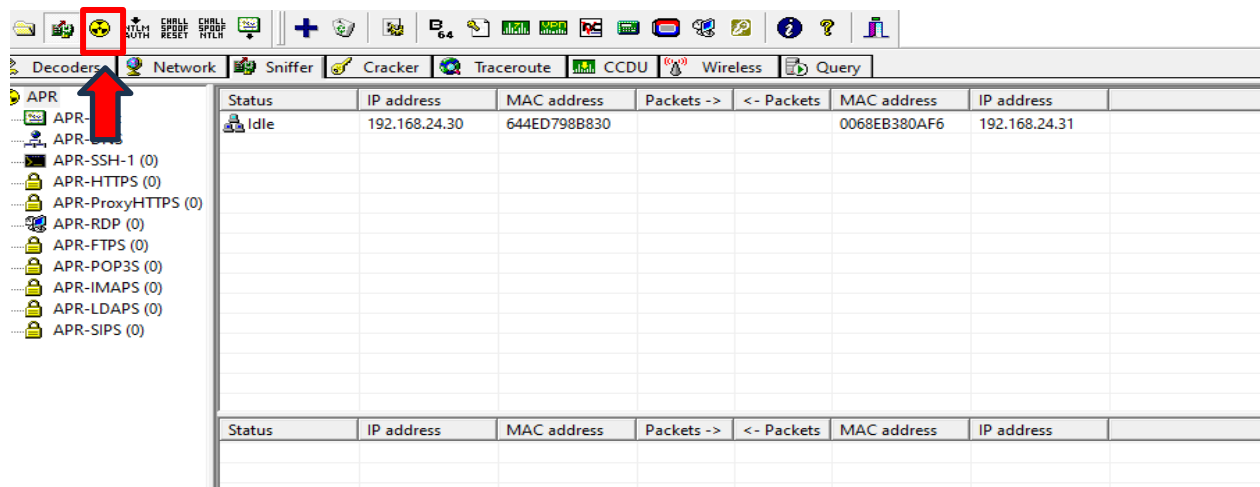
Select the targets:

In the dialog box, select the server as the first target and the target computer as the second target; confirm by clicking OK.



Start ARP Poisoning:

Once the targets are added, activate the poisoning by clicking the Start/Stop APR button in the APR interface.

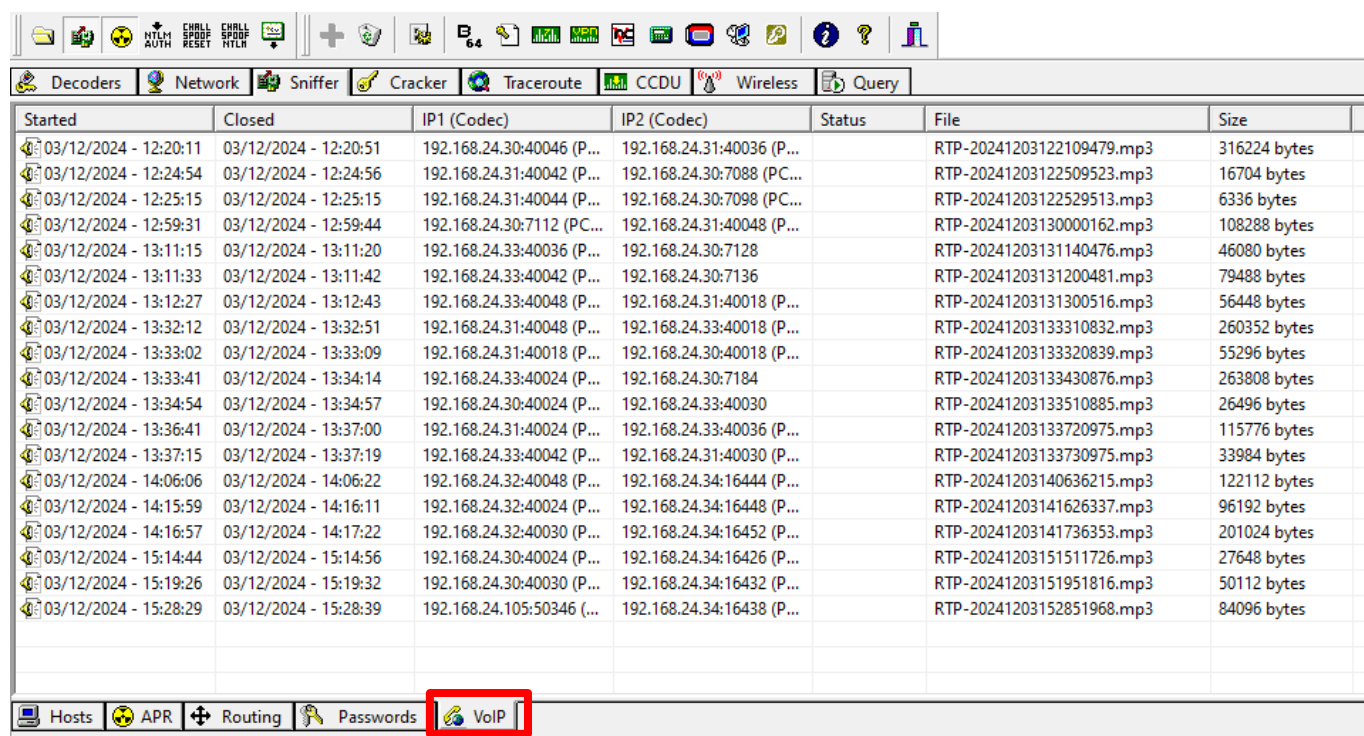


Cain commence alors à intercepter tout le trafic entre le serveur et l'ordinateur cible, le redirigeant à travers votre machine (*Man-in-the-Middle*).

Step 5 : Interception and Recording of VoIP Calls:

Access the VoIP tab:

Go to the VoIP tab to monitor VoIP calls on the network.



Started	Closed	IP1 (Codec)	IP2 (Codec)	Status	File	Size
03/12/2024 - 12:20:11	03/12/2024 - 12:20:51	192.168.24.30:40046 (P...	192.168.24.31:40036 (P...		RTP-20241203122109479.mp3	316224 bytes
03/12/2024 - 12:24:54	03/12/2024 - 12:24:56	192.168.24.31:40042 (P...	192.168.24.30:7088 (PC...		RTP-20241203122509523.mp3	16704 bytes
03/12/2024 - 12:25:15	03/12/2024 - 12:25:15	192.168.24.31:40044 (P...	192.168.24.30:7098 (PC...		RTP-20241203122529513.mp3	6336 bytes
03/12/2024 - 12:59:31	03/12/2024 - 12:59:44	192.168.24.30:7112 (PC...	192.168.24.31:40048 (P...		RTP-20241203130000162.mp3	108288 bytes
03/12/2024 - 13:11:15	03/12/2024 - 13:11:20	192.168.24.33:40036 (P...	192.168.24.30:7128		RTP-20241203131140476.mp3	46080 bytes
03/12/2024 - 13:11:33	03/12/2024 - 13:11:42	192.168.24.33:40042 (P...	192.168.24.30:7136		RTP-20241203131200481.mp3	79488 bytes
03/12/2024 - 13:12:27	03/12/2024 - 13:12:43	192.168.24.33:40048 (P...	192.168.24.31:40018 (P...		RTP-20241203131300516.mp3	56448 bytes
03/12/2024 - 13:32:12	03/12/2024 - 13:32:51	192.168.24.31:40048 (P...	192.168.24.33:40018 (P...		RTP-20241203133310832.mp3	260352 bytes
03/12/2024 - 13:33:02	03/12/2024 - 13:33:09	192.168.24.31:40018 (P...	192.168.24.30:40018 (P...		RTP-20241203133320839.mp3	55296 bytes
03/12/2024 - 13:33:41	03/12/2024 - 13:34:14	192.168.24.33:40024 (P...	192.168.24.30:7184		RTP-20241203133430876.mp3	263808 bytes
03/12/2024 - 13:34:54	03/12/2024 - 13:34:57	192.168.24.30:40024 (P...	192.168.24.33:40030		RTP-20241203133510885.mp3	26496 bytes
03/12/2024 - 13:36:41	03/12/2024 - 13:37:00	192.168.24.31:40024 (P...	192.168.24.33:40036 (P...		RTP-20241203133720975.mp3	115776 bytes
03/12/2024 - 13:37:15	03/12/2024 - 13:37:19	192.168.24.33:40042 (P...	192.168.24.31:40030 (P...		RTP-20241203133730975.mp3	33984 bytes
03/12/2024 - 14:06:06	03/12/2024 - 14:06:22	192.168.24.32:40048 (P...	192.168.24.34:16444 (P...		RTP-20241203140636215.mp3	122112 bytes
03/12/2024 - 14:15:59	03/12/2024 - 14:16:11	192.168.24.32:40024 (P...	192.168.24.34:16448 (P...		RTP-20241203141626337.mp3	96192 bytes
03/12/2024 - 14:16:57	03/12/2024 - 14:17:22	192.168.24.32:40030 (P...	192.168.24.34:16452 (P...		RTP-20241203141736353.mp3	201024 bytes
03/12/2024 - 15:14:44	03/12/2024 - 15:14:56	192.168.24.30:40024 (P...	192.168.24.34:16426 (P...		RTP-20241203151511726.mp3	27648 bytes
03/12/2024 - 15:19:26	03/12/2024 - 15:19:32	192.168.24.30:40030 (P...	192.168.24.34:16432 (P...		RTP-20241203151951816.mp3	50112 bytes
03/12/2024 - 15:28:29	03/12/2024 - 15:28:39	192.168.24.105:50346 (...)	192.168.24.34:16438 (P...		RTP-20241203152851968.mp3	84096 bytes

When the target computer receives or makes a VoIP call, it will appear in the VoIP tab of Cain.

Cain will start automatically recording the conversation as an audio file.

1. Listen to the intercepted call:

Pour écouter l'enregistrement, cliquez droit sur l'enregistrement et après cliquez sur *play*.

The screenshot shows the Wireshark network protocol analyzer interface. The main pane displays a list of captured packets. The selected packet is an RTP packet (RTP-20241203152851968.mp3). A context menu is open over the selected packet, showing options: Play, Remove, Delete, and Remove All. Below the packet list, a Media Player window is open, displaying the selected RTP packet and a play button.

Started	Closed	IP1 (Codec)	IP2 (Codec)	Status	File	Size
03/12/2024 - 12:20:11	03/12/2024 - 12:20:51	192.168.24.30:40046 (P...	192.168.24.31:40036 (P...		RTP-20241203122109479.mp3	316224 bytes
03/12/2024 - 12:24:54	03/12/2024 - 12:24:56	192.168.24.31:40042 (P...	192.168.24.30:7088 (PC...		RTP-20241203122509523.mp3	16704 bytes
03/12/2024 - 12:25:15	03/12/2024 - 12:25:15	192.168.24.31:40044 (P...	192.168.24.30:7098 (PC...		RTP-20241203122529513.mp3	6336 bytes
03/12/2024 - 12:59:31	03/12/2024 - 12:59:44	192.168.24.30:7112 (PC...	192.168.24.31:40048 (P...		RTP-20241203130000162.mp3	108288 bytes
03/12/2024 - 13:11:15	03/12/2024 - 13:11:20	192.168.24.33:40036 (P...	192.168.24.30:7128		RTP-20241203131140476.mp3	46080 bytes
03/12/2024 - 13:11:33	03/12/2024 - 13:11:42	192.168.24.33:40042 (P...	192.168.24.30:7136		RTP-20241203131200481.mp3	79488 bytes
03/12/2024 - 13:12:27	03/12/2024 - 13:12:43	192.168.24.33:40048 (P...	192.168.24.31:40018 (P...		RTP-20241203131300516.mp3	56448 bytes
03/12/2024 - 13:32:12	03/12/2024 - 13:32:51	192.168.24.31:40048 (P...	192.168.24.33:40018 (P...		RTP-20241203133310832.mp3	260352 bytes
03/12/2024 - 13:33:02	03/12/2024 - 13:33:09	192.168.24.31:40018 (P...	192.168.24.30:40018 (P...		RTP-20241203133320839.mp3	55296 bytes
03/12/2024 - 13:33:41	03/12/2024 - 13:34:14	192.168.24.33:40024 (P...	192.168.24.30:7184		RTP-20241203133430876.mp3	263808 bytes
03/12/2024 - 13:34:54	03/12/2024 - 13:34:57	192.168.24.30:40024 (P...	192.168.24.33:40030		RTP-20241203133510885.mp3	26496 bytes
03/12/2024 - 13:36:41	03/12/2024 - 13:37:00	192.168.24.31:40024 (P...	192.168.24.33:40036 (P...		RTP-20241203133720975.mp3	115776 bytes
03/12/2024 - 13:37:15	03/12/2024 - 13:37:19	192.168.24.33:40042 (P...	192.168.24.31:40030 (P...		RTP-20241203133730975.mp3	33984 bytes
03/12/2024 - 14:06:06	03/12/2024 - 14:06:22	192.168.24.32:40048 (P...	192.168.24.34:16444 (P...		RTP-20241203140636215.mp3	122112 bytes
03/12/2024 - 14:15:59	03/12/2024 - 14:16:11	192.168.24.32:40024 (P...	192.168.24.34:16448 (P...		RTP-20241203141626337.mp3	96192 bytes
03/12/2024 - 14:16:57	03/12/2024 - 14:17:22	192.168.24.32:40030 (P...	192.168.24.34:16452 (P...		RTP-20241203141736353.mp3	201024 bytes
03/12/2024 - 15:14:44	03/12/2024 - 15:14:56	192.168.24.30:40024 (P...	192.168.24.34:16426 (P...		RTP-20241203151511726.mp3	27648 bytes
03/12/2024 - 15:19:26	03/12/2024 - 15:19:32	192.168.24.30:40030 (P...	192.168.24.34:16432 (P...		RTP-20241203151951816.mp3	50112 bytes
03/12/2024 - 15:28:29	03/12/2024 - 15:28:39	192.168.24.105:50346 (P...	192.168.24.34:16432 (P...		RTP-20241203152851968.mp3	84096 bytes

Media Player

0:00:02 0:00:08

RTP-20241203152851968

Port Mirroring Attack

The port mirroring attack involves configuring a network switch to duplicate traffic from certain ports to a specific port, allowing an attacker to intercept and monitor data flowing through the network. This can be maliciously used to capture sensitive information, such as communication data, without the users or the network being aware.

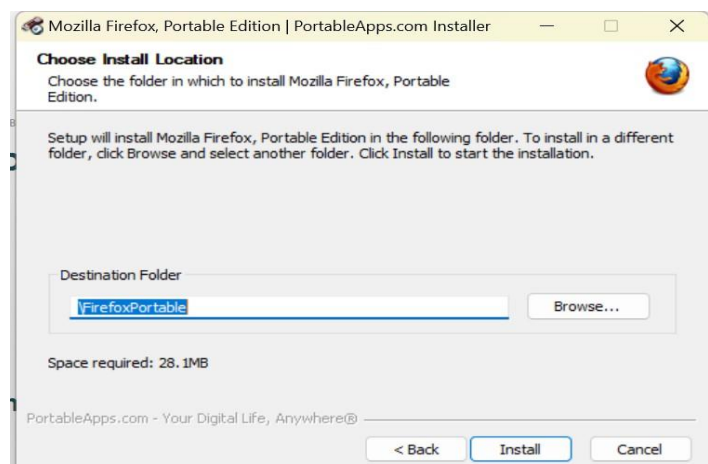
Steps to Launch the Attack

The first step to launch the attack on the switch port is to download a newer version of a browser. In our simulation, we will install version 3.6.11 (2010) of the Mozilla Firefox browser.

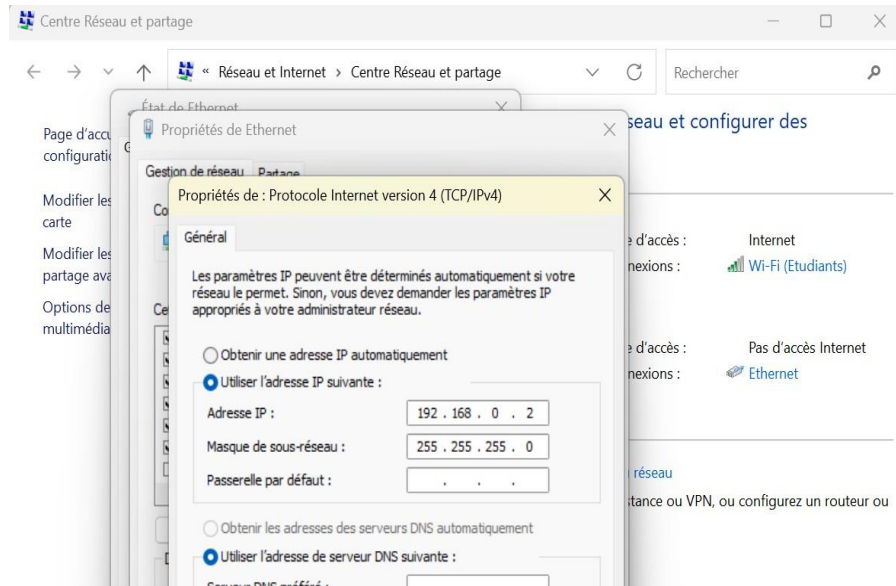
To install it, please visit the following link: <https://mozilla-firefox-portable.fr.uptodown.com/windows/versions>



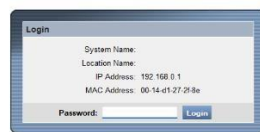
Click on **Next** to start the installation, then choose a location for the destination folder.



Once the installation is complete, it's time to change the attacker's IP address (192.168.0.2) to a static one in order to connect to the switch, which has an IP address of 192.168.0.1.

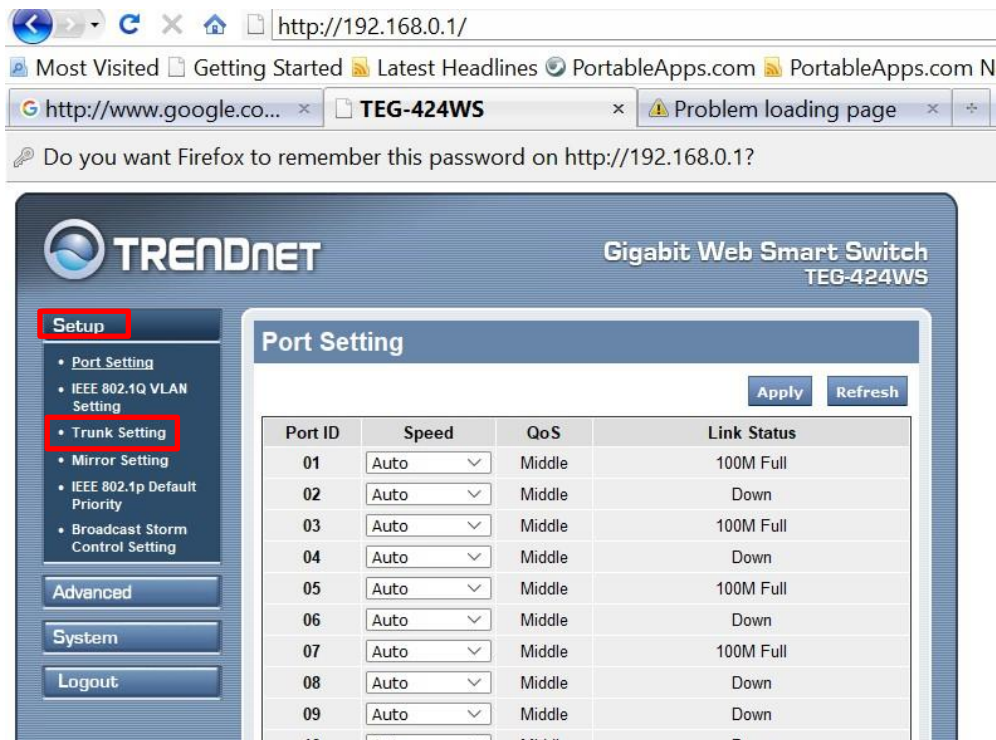


Then, open the Firefox browser we just installed, type the switch's IP address "192.168.0.1" in the URL bar, and enter the password "admin."

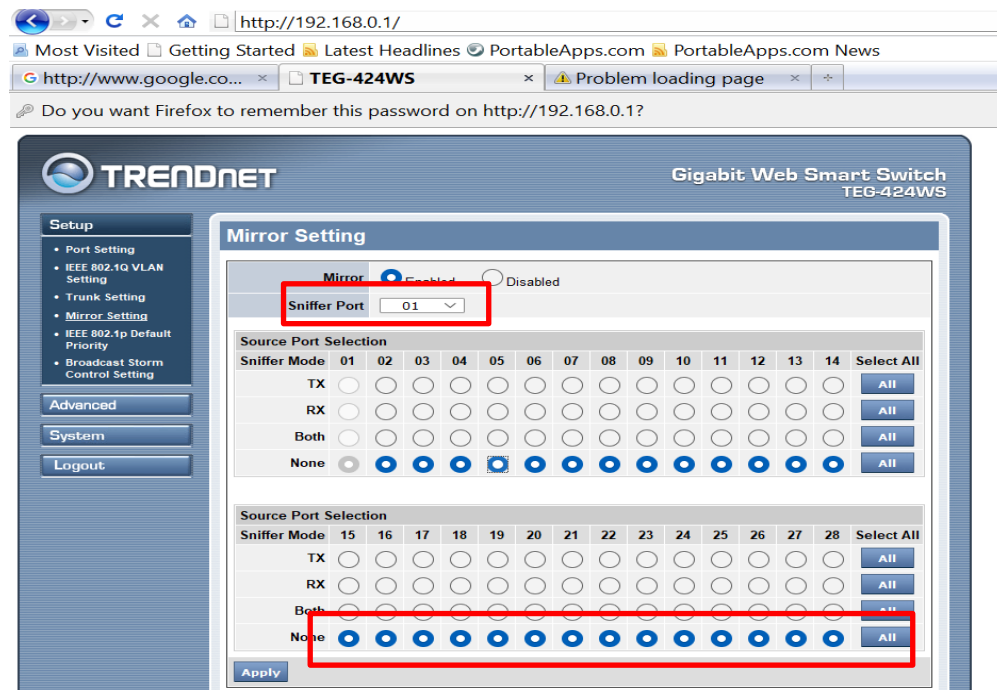


This page is best viewed at 1024x768 with Internet Explorer 5.0+ or Netscape 6.0+

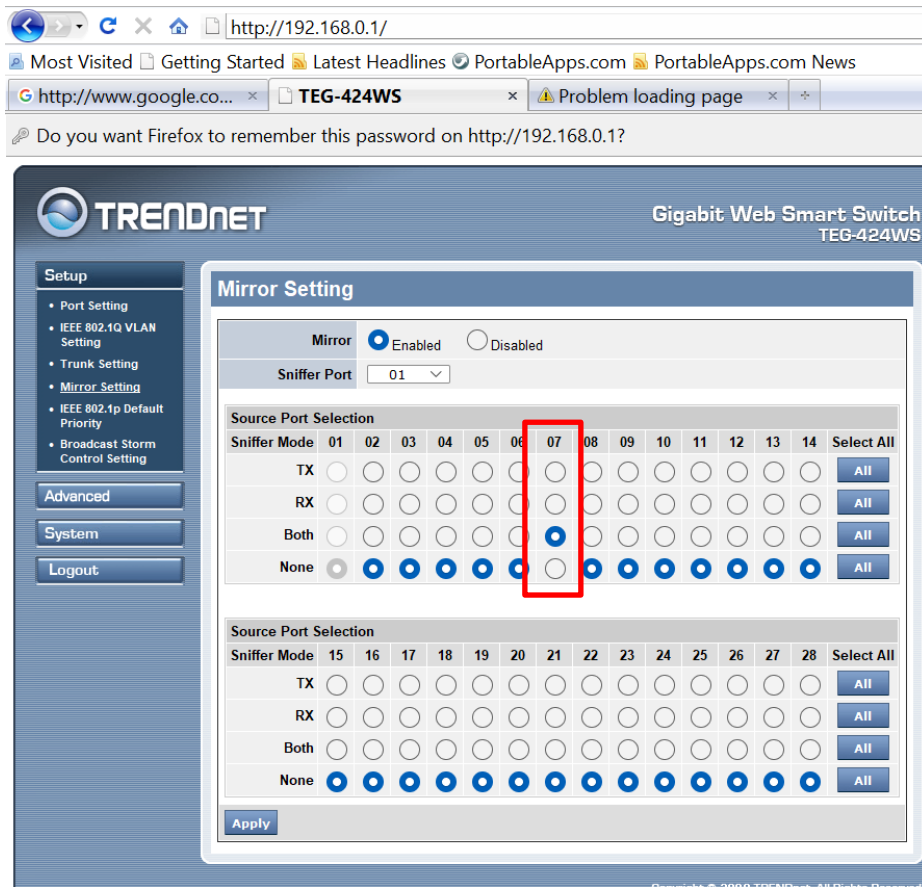
Once authentication is complete, on the page below, click on **Setup**, then on "**Mirror Setting.**"



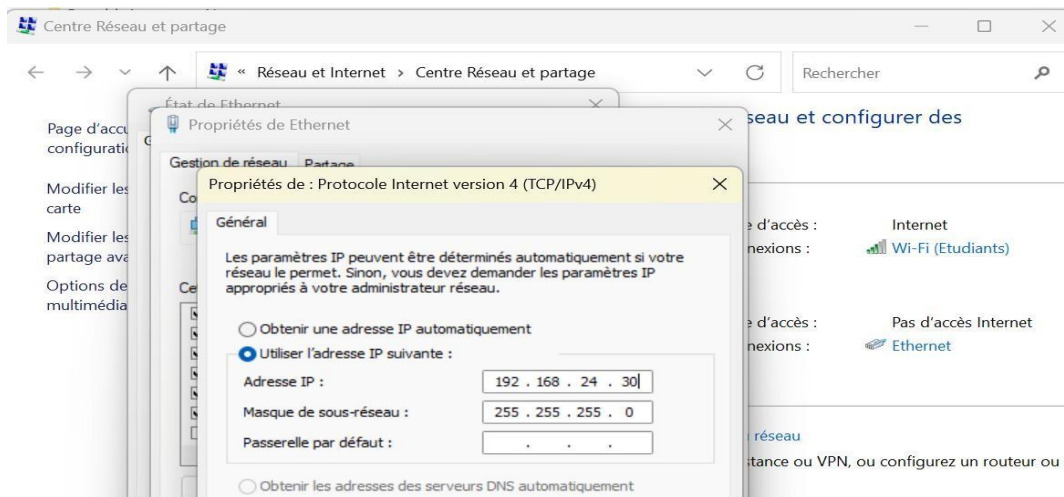
Once the "Mirror Setting" interface is displayed, you will notice that all the "Source Port Selection" options are not set to sniffing mode by default ("none"). The attacker's sniffing port is "01" (this is the port to which we want to redirect the traffic).



Therefore, to launch the attack on port "7," we will change the sniffer mode to "both." This means the attacker can receive both the incoming and outgoing packets from the target machine.



Don't forget to reassign the initial IP address to reconnect to the network.



Finally, the attacker simply needs to launch Wireshark to view the packets and listen to the call (see the steps outlined in the sniffing attack section).

