Labs

‹ back to dashboard

Live Network Traffic Analysis ♥ EXPIRED

Perform live analysis on wired and wireless network traffic

`15-45 Minutes` `540 Points` `6/10 Difficulty`

Start Stop

✓ You have already completed this exercise.

Mission Statement | Verify Flags | Solution

rootsh3ll Bank is a multinational bank that serves over 100 million customers and has over 13,000 branches worldwide.
One of your colleagues has installed a Kali-based dropbox on rootsh3ll Bank's wired network. The dropbox has an embedded wireless NIC capable of monitor mode and packet injection.

With remote access to the dropbox, your job is to silently sniff on the wired network and look for interesting information. Make sure to not transmit any packet over the network, or you might get banned from rootsh3ll Bank's wired network.

For wireless, to prevent detection, you'd have to decrypt the live WPA2-PSK data in monitor mode, without actually connecting to the target access point.
Refer to the "**Helpful tips**" section below for the target wireless access point and its passphrase.

Objective:

1. Analyze live wireless traffic
2. Decrypt WiFi traffic without authenticating with the router.
3. Grok user behaviour from packet data analysis.
4. Perform sniffing over wired LAN
5. Extract assets from the captured data stream

Helpful tips:
A wireless access point named: `Coherer` is active in your vicinity. Use Wireshark to decrypt the live wireless traffic from this access point with the password: `Induction`
Use Wireshark's filter `wlan.addr == 00:0C:41:82:B2:55` to filter the target SSID's traffic and save it to a pcap file for further processing.

Note:
This lab is an environment dedicated to you exclusively. That means this environment is never shared with any other student. So, no downtime or connection drops you would have faced in a shared-server CTF-like environment