BREAKING WIFI & SSH

LeetSec

Contents

Chapter 1

Introduction

This projects aims to introduce you to network concretes knownledges & practice.

You will hacked your first (or not) WPA2 network, which came after WPA & WEP, which both had different importants vulnerability that make them obsolescent in 2022.
At the end of this project, you will be able to understand how packets, local network & authentification are working, how to capture packets between different devices & decrypt an AES encrypted packages.

Chapter 2

Mandatory part

You will need to go to the cluster 2 (or close), you'll see a access point named "LeetSec_AP" available.

Now that you can see the wifi, use a VirtualMachine or your own PC with Linux, to capture the handshake of this wifi. The wifi should be available for few weeks to let you the time to capture it.
(Will be up 6december at 23:59, until the end of the month, for those who need more time, go to discord)

(If you don't have a wifi card compatible with monitor mode, go to the discord of the club we'll find a solution to shift several wifi card for several students

> You should not use Automatic Script for capturing the handshake. This project was made for you to practice this so try to use aircrack-ng & airodump-ng youselves.

Chapter 3

Bonus part

Bonus list:

- Now that you've decrypt the handshake, you should be able to connect into the WIFI network.
- Scan the local network and find the machine ssh port.
- Get access to the only machine with SSH port open by BruteForcing password. You should connect into the "leetsec" user.
- Find the "SECRET_CODE.txt" and copy paste the file inside your folder /phase-1/network-hack/{your login}/secret_code.txt

> The Bonus can only be done if your finished the mandatory part. You'll need access to the wifi "LeetSec_AP" to do the bonus.