COMPUTER NETWORKS
echoEvil - PROJECT ABSTRACT

Praveshini S B
22PC26

This project aims to develop a Python based tool that performs the Evil Twin Attack. The implementation involves creating a rogue AP that spoofs the characteristics of a legitimate AP, enticing unsuspecting users to connect. The Evil Twin Attack is a particularly insidious threat, manipulating users' trust in seemingly legitimate wireless access points (APs) to intercept sensitive information.

Network Adapter: ALFA Network AWUS036NHA

1. Network Scanning
    - The adapter(in monitor mode) scans for Wi-Fi networks nearby by capturing and searching for Dot11 packets(Wi-Fi).
    - All such networks are displayed along with their SSID,BSSID and channel number.

2. Interception of clients' data
    - A specific network is chosen and the details of the devices connected to that network are found by capturing the associated packets and are displayed.

3. Deauthentication of a specific client
    - Deauthentication packets are created using Scapy and are sent to the target device chosen until the device is disconnected.
    - The packets are created with the source as the network to be spoofed and the client as the target device.

4. Rogue AP Creation
    - dnsmasq: DHCP server. It assigns IP addresses to devices that connect to the fake AP.
    - hostapd: Used to manage the fake AP. It provides the SSID,interface and channel number for configuration.
    - IP Address for network of AP: 10.0.0.0
      Gateway:10.0.0.1

5. Capturing information
    - Once the device connects to the fake AP, the captive portal is opened where the user enters details for "logging in".
    - These details are captured and stored in a file.
    - After this,the adapter is switched back to managed mode(normal mode).