THE ANTILIFE FRAMEWORK

BY: M ZEESHAN ZAFAR

1. CREATE WORDLIST

GOAL: GENERATE A WORDLIST BASED ON USER INPUT.

IMPLEMENTATION: USE ITERTOOLS IN PYTHON TO CREATE WORD COMBINATIONS.

2. CAPTURE HANDSHAKE

GOAL: CAPTURE THE WPA/WPA2 4-WAY HANDSHAKE FOR CRACKING.

IMPLEMENTATION: USE SCAPY OR AUTOMATE AIRODUMP-NG VIA PYTHON TO CAPTURE HANDSHAKE PACKETS.

3. DECRYPT HANDSHAKE (WORDLIST ATTACK)

GOAL: DECRYPT THE HANDSHAKE USING A WORDLIST.

IMPLEMENTATION: USE HASHCAT OR AIRCRACK-NG FOR CRACKING WPA KEYS.

4. DEAUTHENTICATION ATTACK

GOAL: DISCONNECT CLIENTS FROM THE WIFI NETWORK USING DEAUTH FRAMES.

IMPLEMENTATION: SEND CONTINUOUS DEAUTHENTICATION FRAMES TO FORCE THE CLIENT OFF THE NETWORK WITH SCAPY.

5. TRAFFIC INTERCEPT

GOAL: MONITOR NETWORK TRAFFIC ON CONNECTED WIFI NETWORKS.

IMPLEMENTATION: USE SCAPY TO SNIFF AND ANALYZE TRAFFIC, OR PARSE OUTPUT FROM TSHARK.

6. SSL DOWNGRADE

GOAL: DOWNGRADE CLIENT CONNECTION FROM HTTPS TO HTTP.

IMPLEMENTATION: USE BETTERCAP FOR SSL STRIPPING OR CREATE AN HTTP PROXY USING PYTHON.

7. CLIENT MAC OSINT

GOAL: PERFORM OSINT ON CONNECTED DEVICES' MAC ADDRESSES.

IMPLEMENTATION: QUERY PUBLIC MAC DATABASES VIA PYTHON FOR DEVICE INFORMATION.

8. EVIL TWIN ATTACK

GOAL: CREATE A FAKE ACCESS POINT AND PHISHING PAGE FOR CREDENTIALS.

IMPLEMENTATION: USE HOSTAPD FOR THE FAKE AP AND FLASK FOR THE PHISHING PAGE.

9. BLUEJACKING

GOAL: SEND UNSOLICITED BLUETOOTH REQUESTS TO NEARBY DEVICES.

IMPLEMENTATION: USE PYBLUEZ TO SEND MULTIPLE BLUETOOTH MESSAGES.

10. WIRELESS CCTV JAMMING

GOAL: DISRUPT WIRELESS CCTV BY JAMMING ITS COMMUNICATION.

IMPLEMENTATION: USE SCAPY TO FLOOD PACKETS TO JAM THE DEVICE.