ARIEL UNIVERSITY

Assignment 1: Evil Twin Attack

Wireless and Mobile Network Security

Department of Computer Science
Course #: 2-7038910-1
Ariel University

Instructor: Dr. Eyal Berliner

Email: eyalbe@ariel.ac.il

April 9, 2025

Contents

1 Background

The Evil Twin attack is an implementation of a classic attack in the wireless cybersecurity world known as a Rogue AP. The principle is simple: a legitimate user who is accustomed to connecting to the "good twin" network can no longer connect to it. The user then attempts to manually connect to what appears to be the same network (the "evil twin"), and because both networks appear identical, they succeed in connecting.

From there, the attack typically progresses with browsing attempts redirected to a Captive Portal that demands the username and password for the network in order to proceed. This type of attack allows bypassing a well-secured network or creating better conditions for obtaining sensitive information.

2 Assignment Objectives

- **Understand 802.11 WLANs:** Develop a thorough understanding of 802.11 WLAN communication networks, including establishment requirements and inherent vulnerabilities such as the difficulty in verifying packet sender identity and the ease of creating attacker-controlled networks.
- **Develop Attack Tools:** Create a complete Evil Twin attack tool as described in the background. Through this process, you will learn how easily endpoint data can be collected in WLANs without connection to their network association.
- **Implement Countermeasures:** Develop effective defense mechanisms to detect and prevent such attacks.
- **Technical Skill Development:** Acquire skills in Python programming and the SCAPY library for networking operations, particularly in WLAN environments. The assignment will also develop your abilities in planning/designing attack/defense tools and working with Linux Shell.

3 Important Notes

- **Individual Defense Requirement:** Each student must undergo a frontal defense (in-person or via ZOOM) of their group's submission.
- **Grading Structure:** The assignment grade consists of:
  - A base grade for the group submission
  - An individual grade for each student's defense performance
- **Defense Expectations:** During the defense, you will be tested on:
  - Your understanding of WLAN technology with emphasis on course material
  - Implementation details and how concepts from class are applied in your code
  - Functional understanding is necessary but not sufficient

- **Independent Development:** While research and inspiration from various sources is encouraged, **the submitted tools must be developed independently and originally**.
- **Environmental Flexibility:** Your code must work with different hardware and communication environments beyond your testing environment. Submissions will typically be evaluated in a DragonOS operating environment or similar Linux distribution.
- **Virtual Machine Considerations:** If using a VM, consider that special settings may be required for full hardware access despite appearances to the contrary.

SEVERE WARNING

Do not use pre-made tools like those in the Aircrack toolkit. Any submission that uses such a tool will be immediately disqualified!

4 Assignment Requirements

4.1 Required Deliverables

1. An attack tool that performs the Evil Twin attack as detailed below
2. A defense tool that identifies the attack and enables preventative actions
    - A small bonus will be awarded for implementing preventive actions that do not affect the victim's network operation

4.2 General Overview of the Evil Twin Attack Stages

1. **Network Discovery**
    - Scan and identify all WLAN networks in the device's environment (one-minute scan)
    - Your tool should display networks with relevant details (SSID, signal strength, security type, etc.)
2. **Target Selection**
    - Select one of the networks found
    - The user interface should allow easy selection from discovered networks
3. **Victim Identification**
    - Identify and select an active client on the chosen network
    - Display relevant client information (MAC address, connection, etc.)
4. **Malicious Network Creation (Evil Twin)**
    - Create and operate a malicious twin network
    - Implement all communication services required for proper operation

- Ensure the twin appears identical to the legitimate network

5. **Targeted Disconnection**
   - Disconnect only the selected victim from the chosen network
   - Implement this without affecting other network clients
6. **Credential Capture**
   - Create a mechanism to obtain username and password
   - Implement storage for obtained credentials
   - Provide user feedback when the credentials are obtained.

4.3 Tool Implementation Guidelines

In this course, a tool is defined as a system under one wrapper and interface from which all required actions are performed without additional need to adapt code, type parallel commands in a separate shell wrapper, etc. The tool will enable good situation awareness about the attack status and outcome as described later on.
Remember that SCAPY is not capable of managing the hardware.
A good tool will achieve two key objectives:

1. **User-Friendly Setup:** Allow quick process configuration while preventing errors and disruptions
2. **Real-Time Feedback:** Provide the user with situation awareness to understand what is happening at each stage

Therefore, it is mandatory to create appropriate feedback for each stage. For example:

- Display available hardware components for selection
- Show scanning status and results in a clear format
- Notify when a user connects to the Evil network
- Indicate when the attack has concluded successfully
- And so on...

Think of your tool as allowing the user to conduct an orchestra — timely activating different components with minimal effort while simultaneously monitoring the results and knowing exactly the state of each component.

5 Required Hardware

A wireless network adapter (WLAN Network Interface Controller) that supports:

- Monitor mode/Debug mode operation:
  - Passive sensing
  - Packet injection in the 802.11 standard

Adapters available for borrowing during the course period:

- EDUP AX3000 (EP-AX1672)
- Tenda N150
- VIA 9271

6 Base Grading Criteria

Each group submission will be evaluated based on:

Criteria	Weight	Description
Functionality	50%	Does the tool perform all required stages correctly?
Code Quality	20%	Is the code well-structured, documented, and maintainable?
Defense Mechanism	20%	How effective is the detection and prevention solution?
User Interface	10%	How effective and intuitive is the tool interface?

Table 1: Base Grading Criteria

7 Submission Guidelines

- **Deadline:** TBA (Around 6 weeks)
- **Submission Method:** You may submit files as a compressed archive or provide a GitHub repository link

SEVERE WARNING

Do not make any changes in the submission after the final Deadline!
This will immediately disqualify the group's submission!

7.1 Required Submission Components

1. **Verified Code Files:**
   - All Python scripts and supporting files
   - Well-commented and organized code
2. **Documentation:**
   - README file containing:
     - Group details and individual contributors
     - Installation and required setup instructions
     - Known limitations
     - Hardware requirements and configuration details
3. **Test Results** (optional but recommended):
   - Screenshots or logs demonstrating successful execution
   - Test environment details

8 Resources

- **SCAPY Documentation:** `https://scapy.readthedocs.io/`
- **iwconfig command in Linux with Examples:** `https://www.geeksforgeeks.org/iwconfig-command-in-linux-with-examples/`
- **DragonOS:** `https://cemaxecuter.com/`
- **DragonOS Documentation:** `https://github.com/DragonOS-Community`

9 Contact Information

If you have any questions or concerns, please don't hesitate to contact me, just kindly add CWN 2025 in the email subject:

- **Instructor:** Dr. Eyal Berliner
- **Email:** eyalbe@ariel.ac.il
- **Office Hours:** [Insert schedule or "By appointment"]

Remember: If there is doubt, there is no doubt that you should contact me—either by email, in class, or during office hours.

Best of luck,

Eyal