PEN-210 Lab Report

v.2.0

student@youremailaddress.com

OSID: XXXXX



Copyright © 2023 Offsec Ltd. All rights reserved.

No part of this publication, in whole or in part, may be reproduced, copied, transferred or any other right reserved to its copyright owner, including photocopying and all other copying, any transfer or transmission using any network or other means of communication, any broadcast for distant learning, in any form or by any means such as any information storage, transmission or retrieval system, without prior written permission from Offsec.

Table of Contents

[1.0 Offensive-Security PEN-210 Lab Documentation 3](#_heading=h.gjdgxs)

[1.1 Objective 3](#_heading=h.30j0zll)

[1.2 Requirements 4](#_heading=h.1fob9te)

[2.0 Modules 5](#_heading=h.3znysh7)

[2.1 Summary Overview 5](#_heading=h.2et92p0)

[2.2 Equipment 5](#_heading=h.tyjcwt)

[3.0 Exercises 6](#_heading=h.3dy6vkm)

[5.0 Wireshark Essentials 6](#_heading=h.1t3h5sf)

 [5.1.4 Saving and Exporting Packets 6](#_heading=h.4d34og8)

[4.0 Additional Items Not Mentioned in the Report 9](#_heading=h.lnxbz9)

# 1.0 Offensive-Security PEN-210 Lab Documentation

The following pages contains the lab exercises for the WiFu course and should be attempted only inside the Offensive Security hosted lab environment. Please note that most of the attacks described in the lab guide would be illegal if attempted on machines that you do not have explicit permission to test and attack. Since the Offensive Security lab environment is segregated from the Internet, it is safe to perform the attacks inside the lab. Offensive Security does not authorize you to perform these attacks outside its own hosted lab environment and disclaims all liability or responsibility for any such actions.

## 1.1 Objective

We recommend that you fully complete the exercises for each module prior to moving on to the next module. They will test your understanding of the material and build your confidence to move forward.

Depending on your existing skill set, it may take considerable time and effort to complete the exercises. Nevertheless, we encourage you to be persistent, especially with tougher exercises. Persistence is an essential trait to develop as part of the OffSec "Try Harder" mindset.

Offensive Security Wireless Attacks is completed at home by the student, so the prerequisites necessary for this course are different from the other courses provided by Offensive Security. If not already owned, the student will need to purchase a dedicated wireless Access Point and a wireless card that supports traffic injection. More information can be found in the respective course description and course documentation.

**Note that copy-pasting code from the book modules into a script may result in unintended whitespace or newlines due to formatting.**

## 1.2 Requirements

The student will be required to fill out this lab report fully and to include the following sections:

* High-Level summary of assignment solutions.
* Methodology walkthrough and detailed outline of steps taken through analysis and all written code.
* Each finding with included screenshots, walkthrough, sample code or reference.
* Screenshots of the final working exploit against your target.

# 2.0 Modules

## 2.1 Summary Overview

A brief description of the exercises that were solved, including the overall exploitation / development steps within your personal lab.

## 2.2 Equipment

What equipment was used to complete the following exercises.

* Alfa AWUS036NHA
* NETGEAR AC1000 (R6080)

# 3.0 Exercises

## 5.0 Wireshark Essentials

### 5.1.4 Saving and Exporting Packets

1. Plug in your wireless card and enable monitor mode.

* Confirming if my adapter is found in Kali

kali@kali:~$ sudo airmon-ng

PHY Interface Driver Chipset

phy0 wlan0 ath9k\_htc Qualcomm Atheros Communications AR9271 802.11n

* Checking what the adapter is able to support by running the *sudo iw list* command

kali@kali:~$ sudo iw list

Wiphy phy0

 ...

 Supported interface modes:

 \* IBSS

 \* managed

 \* AP

 \* AP/VLAN

 \* monitor

 \* mesh point

 \* P2P-client

 \* P2P-GO

 \* outside context of a BSS

 Band 1:

 Capabilities: 0x116e

 HT20/HT40

 ...

 ...

 HT TX/RX MCS rate indexes supported: 0-7

 Bitrates (non-HT):

 \* 1.0 Mbps

 \* 2.0 Mbps (short preamble supported)

 \* 5.5 Mbps (short preamble supported)

 \* 11.0 Mbps (short preamble supported)

 \* 6.0 Mbps

 \* 9.0 Mbps

 \* 12.0 Mbps

 \* 18.0 Mbps

 \* 24.0 Mbps

 \* 36.0 Mbps

 \* 48.0 Mbps

 \* 54.0 Mbps

 Frequencies:

 \* 2412 MHz [1] (20.0 dBm)

 \* 2417 MHz [2] (20.0 dBm)

 \* 2422 MHz [3] (20.0 dBm)

 \* 2427 MHz [4] (20.0 dBm)

 \* 2432 MHz [5] (20.0 dBm)

 \* 2437 MHz [6] (20.0 dBm)

 \* 2442 MHz [7] (20.0 dBm)

 \* 2447 MHz [8] (20.0 dBm)

 \* 2452 MHz [9] (20.0 dBm)

 \* 2457 MHz [10] (20.0 dBm)

 \* 2462 MHz [11] (20.0 dBm)

 \* 2467 MHz [12] (20.0 dBm)

 \* 2472 MHz [13] (20.0 dBm)

 \* 2484 MHz [14] (disabled)

 ...

* Creating a new interface to enable monitor mode on *wlan0* and confirming its enabled

kali@kali:~$ sudo iw dev wlan0 interface add wlan0mon type monitor

kali@kali:~$

*kali@kali:~$ sudo iw dev wlan0mon info*

Interface wlan0mon

 ifindex 4

 wdev 0x1

 addr 0c:0c:ac:ab:a9:08

 type monitor

 wiphy 0

 channel 11 (2462 MHz), width: 20 MHz, center1: 2462 MHz

*2.* Open Wireshark and start capturing frames.



# 4.0 Additional Items Not Mentioned in the Report

This section is placed for any additional items that were not mentioned in the overall report.