‹ Dashboard

TRAFFIC ANALYSIS

Basics

Traffic analysis refers to inspecting the captured/stored WiFi traffic to gather information regarding clients, access points and their activities. The labs in this section provide the user with traffic capture PCAPs and suitable tools for analysis.

What will you learn?

- Analyzing WiFi traffic to identify WiFi networks and clients
- Different WiFi frames and frame structure
- Checking client AP connection/disconnection, WPA handshake and SAE handshake
- Observing the difference between different types of security schemes
- Identifying evil twins and impersonating client from traffic captures

References:

1. Pentester Academy's WiFi Security and Pentesting course (https://www.pentesteracademy.com/course?id=9)
2. WiFi Spectrum Analysis (https://mrncciew.com/2014/10/17/cwap-spectrum-analysis/)
3. WiFi Management frames (https://mrncciew.com/2014/09/29/cwap-802-11-mgmt-frame-types/)
4. WiFi Control frames (https://mrncciew.com/2014/10/02/cwap-802-11-control-frame-types/)
5. WiFi Data frames (https://mrncciew.com/2014/10/13/cwap-802-11-data-frame-types/)
6. 4-way handshake (https://mrncciew.com/2014/08/19/cwsp-4-way-handshake/)
7. WPA3 SAE Mode (https://mrncciew.com/2019/11/29/wpa3-sae-mode/)
8. WPA3 SAE Transition Mode (https://mrncciew.com/2019/11/29/wpa3-sae-transition-mode/)
9. Enhanced Open (https://mrncciew.com/2019/11/21/enhanced-open-part-1/)

Labs Covered:

In all the WiFi traffic analysis labs (except the Elasticsearch Kibana lab), the user will be provided with traffic capture PCAP files on a Kali machine. The user can access the Kali GUI. Wireshark is used as the primary analysis tool for this section.

- WiFi Security: Traffic Analysis I

  In this lab, you will learn to analyze the WiFi traffic using Wireshark. The focus of this lab is going to be on basic WiFi traffic analysis.

- WiFi Security: Traffic Analysis II

  In this lab, you will learn to analyze the WiFi traffic using Wireshark. The focus of this lab is going to be on basic WiFi traffic analysis. This is a practice lab with different objectives from the previous lab.

- WiFi Security: Traffic Analysis III

  In this lab, you will learn to analyze the WiFi traffic using Wireshark. The focus of this lab is going to be on basic WiFi traffic analysis. This is also a practice lab with different objectives from the previous labs.

- 802.11ac Packet Analysis

  In this lab, you will learn to analyze the WiFi traffic using Wireshark. The focus of this lab is going to be the analysis of traffic transmitted using high throughput WiFi standard (i.e. 802.11ac).

- 802.11ac Packet Analysis II

  In this lab, you will learn to analyze the WiFi traffic using Wireshark. The focus of this lab is going to be the analysis of traffic transmitted using high throughput WiFi standard (i.e. 802.11ac). This is a practice lab with different objectives from the previous lab.

- Evil Twin Detection

- Impersonating Client Detection
  The focus of this lab is the detection of an impersonating client (a client that has cloned the MAC address of another client to either bypass MAC filter or avoid detection) device by analyzing the traffic dumps using Wireshark.

- WiFi Security: WPA3-SAE Analysis
  The focus of this lab is the analysis of the SAE (Simultaneous Authentication of Equals) scheme of the WPA3 standard using Wireshark.

- WiFi Security: OWE Analysis
  The focus of this lab is the analysis of the OWE (Opportunistic Wireless Encryption) scheme of WPA3 standard using Wireshark.

- WiFi Traffic Analysis with Kibana
  In this lab, you will learn to analyze a large amount of WiFi traffic using elasticsearch-kibana (EK) setup. The EK setup is ideal for analyzing large traffic dumps that are too big for Wireshark to handle.

802.11ac Packet Analysis

Start

802.11ac Packet Analysis II

Start

WiFi Security: Traffic Analysis I

Start

WiFi Security: Traffic Analysis II

Start

WiFi Security: Traffic Analysis III

Start

Evil Twin Detection

Start

Impersonating Client Detection

Start

WiFi Security: WPA3-SAE Analysis

Start