



This section covers luring the client using honeypot (or evil twin) and recovering the correct user credentials from WiFi networks protected by enterprise WiFi networks security schemes like WPA-EAP, PEAP-MSCHAP2 and PEAP-TTLS.

What will you learn?

- Creating honeypot and evil twin
- The difference in TTLS and PEAP schemes
- Using EAPhammer and Mana toolkit

References:










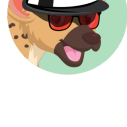
1. Cracking EAP-PEAP-MSCHAPv2 (<https://www.pentesteracademy.com/video?id=508>)
2. EAP TLS vs EAP TTLS vs EAP-PEAP (<https://security.stackexchange.com/questions/147344/eap-tls-vs-eap-ttls-vs-eap-peap>)

Labs Covered:

- [Mana: Attacking PEAP-GTC](#)
In this lab, you will learn to create a honeypot network for a WPA-Enterprise (PEAP-GTC) network using Hostapd-mana and steal a user's credentials.
- [Mana: Attacking PEAP-MSCHAPv2](#)
In this lab, you will learn to create a honeypot network for a WPA-Enterprise (PEAP-MSCHAPv2) network using Hostapd-mana, steal a user's username/hash and use Asleep to crack the hash to recover the password.
- [Mana: Attacking TTLS-PAP](#)
In this lab, you will learn to create a honeypot network for a WPA-Enterprise (TTLS-PAP) network using Hostapd-mana and steal a user's credentials.
- [Mana: Attacking TTLS-CHAP](#)
In this lab, you will learn to create a honeypot network for a WPA-Enterprise (PEAP-CHAP) network using Hostapd-mana, steal a user's username/hash.
- [Mana: Attacking TTLS-MSCHAPv2](#)
In this lab, you will learn to create a honeypot network for a WPA-Enterprise (TTLS-MSCHAPv2) network using Hostapd-mana, steal a user's username/hash and use Asleep to crack the hash to recover the password.
- [Evil Twin](#)
In this lab, you will learn to create an evil twin network for a WPA-Personal (WPA2-PSK) network using Hostapd and force the client to connect to this network by launching a deauth attack with aireplay-ng.
- [Evil Twin - WPA Enterprise \(Mana\)](#)
In this lab, you will learn to create an evil twin network for a WPA-Enterprise (TTLS-PAP) network using Hostapd-mana, force the client to connect to this network by launching a deauth attack with aireplay-ng and steal a user's credentials.
- [Evil Twin - WPA Enterprise \(EAPHammer\)](#)
In this lab, you will learn to create an evil twin network for a WPA-Enterprise (TTLS-PAP) network using EAPHammer, force the client to connect to this network by launching a deauth attack with aireplay-ng and steal a user's credentials.
- [Karma Attacks \(Mana\)](#)

- [Karma Attacks \(EAPHammer\)](#)

In this lab, you will learn to create an evil twin network that responds to all probe requests and lures the client to connect to it for WPA-Enterprise networks using EAPHammer. Multiple clients will connect to the same honeypot and reveal user credentials.

	Evil Twin	⚡ Start
	Evil Twin - WPA Enterprise (Mana)	⚡ Start
	Evil Twin - WPA Enterprise (EAPHammer)	⚡ Start
	Mana: Attacking PEAP-GTC	⚡ Start
	Karma Attacks (Mana)	⚡ Start
	Mana: Attacking PEAP-MSCHAPv2	⚡ Start
	Karma Attacks (EAPHammer)	⚡ Start
	Mana: Attacking TTLS-PAP	⚡ Start
	Mana: Attacking TTLS-CHAP	⚡ Start
	Mana: Attacking TTLS-MSCHAPv2	⚡ Start