

Forum:[Hack Forums](#)

Thread: [How To Use WiFi Pineapple - Device for WiFi Attacks](#)

hdo44 - July 8, 2024, 6:29 pm

One must undertake the preparatory measures requisite for the optimal utilization of the WiFi Pineapple, a formidable instrument employed in the realms of network penetration testing and WiFi assaults.

Firstly, the establishment of a physical connection between the aforementioned device and one's computational apparatus is imperative, facilitated by the employment of a micro-USB cable.

Upon the successful consummation of this preliminary step, the activation of the WiFi Pineapple must ensue, whereupon one shall gain access to its Web-based User Interface by entering the prescribed Internet Protocol address, namely 192.168.24.1, into the navigational interface of their preferred web browser. To proceed further, one must authenticate their credentials by supplying the default username and password, both of which are the singular word 'pineapple'.

We must now direct to the inaugural task at hand – the creation of a bespoke deauthentication package. This ingenious contrivance shall enable us to temporarily sever the connection between users and the wireless network.

To commence this endeavor, one must navigate to the 'Tools' section of the Web-based User Interface and select the option labeled 'death'. Thereupon, one shall be presented with a list of potential target networks, from which the desired wireless domain must be judiciously chosen. The next step in this intricate process involves the input of one's unique Media Access Control (MAC) address, a digital identifier that can be readily procured from the roster of connected devices maintained by one's router.

Once these preparatory measures have been meticulously executed, one need only engage the 'Launch' function, and bear witness to the unfolding spectacle as users are systematically disconnected from the wireless network.

Let us now turn our attention to the realm of 'Evilware' – a veritable repository of pre-constructed implements of digital warfare, meticulously crafted for the express purpose of penetration testing and the rigorous assessment of wireless networking security. Upon accessing this hallowed domain through the Web-based User Interface, one is presented with a cornucopia of tools.

We shall direct our focus towards the 'WiFi HoneyPot' – a cunning artifice designed to ensnare the unwary by presenting itself as a legitimate wireless access point, luring them into its embrace with the promise of connectivity. To set this trap in motion, one must first select the 'WiFi HoneyPot' from the array of available implements, and thereafter specify the desired Service Set Identifier (SSID) and accompanying password.

Once these preliminary configurations have been meticulously executed, one need only engage the 'Launch' function, and bear witness as the WiFi HoneyPot springs to life.

In the advanced mode, you can explore 'Ingress Filtering', which prevents unwanted traffic from reaching your devices on the network. This is an important feature to protect yourself from certain types of network attacks. In the Web UI, go to 'Firewall' and then 'Ingress Filtering'. Add the IP addresses and protocols you would like to block and save your changes.

As you become more familiar with your WiFi Pineapple, feel free to explore its many other features

and attack vectors.

Bastille - *July 8, 2024, 11:17 pm*

AI generated, again.

Don't spam this section to get the award. We expect HQ threads for this. What you posted is 10% of what is required for a working tutorial.

DramaKing - *July 9, 2024, 4:24 am*

I got as far as the part where he says that the connection between the Pineapple and "one's computational apparatus" is "facilitated by the employment of a micro-USB cable." That was probably true at one time, but Hak5 switched to USB-C. The default Internet Protocol address is also wrong.