What is a wireless pineapple and how does it work

Technology, Information Technology

COMPUTER SCIENCE Wireless or “ WiFi Pineapple Mark V is the latest generation wireless networkauditing tool from Hak5. With its custom, purpose built hardware and software, the WiFi Pineapple enable users to quickly and easily deploy advanced attacks using the intuitive web interface from a man-in-the-middle hot-spot honey pot to an out-of-band pentest pivot box, the WiFi Pineapple is unmatched in performance, value and versatility. Basically Wifi Pineapple is allows users to carry out man-in-the-middle attacks. Connected clients traffic go through the attacker which makes the attacker capable of pulling a number of tricks. Wifi Pineapple Mark V is Equipped with 2 radios it can work in client mode meaning it can piggyback on a nearby WiFi network and bridge the victims connections . Hak5 focuses on making easily accessible, affordable and infinitely expandable wireless hacking tools. Since 2008 the WiFi Pineapple has been serving penetration testers, law enforcement, military and government with a versatile wireless auditing platform for almost any deployment scenario.” (Mark, 2014)

The wireless pineapple works in a unique way. Normally, any wireless devise would try to connect to the previous or last websites that were used. The Karma method often sends out probe request to want information from a specified point by SSID or access points that are specified by the broadcast SSID. The correct access point-AP, will always probe a response in which the client will initiate an association thus connection to home networks. However, a malicious device can break the code based system making the pineapple to responds to whatever AP the device has asked therefore deceiving it into believing they are home. This will make the attackers to access the information that they are not supposed to view.

The WIFI pineapple is subjected to numerous risks. Ordinarily, the honey pots are usually set to get the traffic of the browser. When an individual sends data using the attackers system he or she opens herself to sslstrip risks. This sslstrip often rechannel the HTTPS traffic to HTTP equivalent thereby opening way to attackers. However, these risks can be mitigated using the following ways: (Anonymous, 2012)

I. One should not connect to open networks: When one uses open networks he or she should ensure that the networks can be controlled. This often can open to attackers of the information.

II. Verify SSL: One should ensure that he is connected to the purposed website. This is confirmed by checking the SSL/TLS certificate which is often hard to break by attackers.

III. VPN: This ensures that the information is safe because it is passed through a secure channel and therefore the attackers will not get your information.

IV. HSTS: Ensure that you use HSTS since browsers will always use secure HTTPS connections avoiding the insecure HTTP protocol thereby moderating sslstrip risks.

V. PineAP. This is " the next-gen rogue AP". This reduces Karma attack by sending Broadcast probe request only instead of all the SSIDs. This enables the APs to with a beacon with the information they are broadcasting. This enables the customer to decide on the one to connect to making it secure. The PineAP has several modules that make it to work efficiently. It has beacon responses module that sends a beacon with the same SSID just like the probe response with SSID sent by Karma making it legitimate. Secondly,

it has a dogma module which sends beacon frames of SSIDs that has been selected by attacker. This enables the fraud to be detected in advance. Lastly, it has auto harvester module that collects leaking SSIDs from the potential clients making the system to be secure. (Anonymous, 2012)

Works Cited

Anonymous. (2012). Beware the Pineapple: An overview of WiFi Pineapple Mark V. Retrieved 2015, from http://volkanpaksoy. com/archive/2015/02/25/beware-the-pineapple-an-overview-of-wifi-pineapple-mark-v/

Mark. (2014). Wifi Pineapple. Retrieved 2015, from https://www. wifipineapple. com/