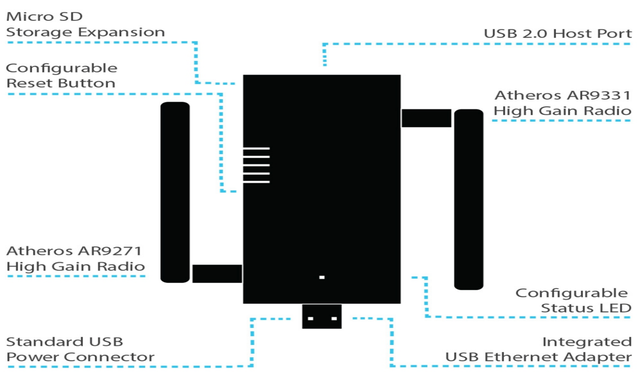
Hacking Mobile Devices With WiFi Pineapple Nano

Author: Alexis Mojica Serrano
Advisor: Dr. Jeffrey Duffany
Electrical & Computer Engineering and Computer Science Department
Capstone Design Course SP-19

Abstract

Nowadays wireless access points can be found everywhere from fast food restaurants to private companies embracing Bring Your Own Device (BYOD) policies. These access points present a flexible solution in which different mobile devices can be connected to a wireless network and still perform effectively. Often the main concern with the use of access points is the lack of security they have. Most of the time users connect to wireless access points not knowing if they are genuine or malicious, or knowing of the vulnerabilities and risks that these represent to their devices or to their networks. Even more, they are not aware of the types of attacks that can come from "rogue" access points set up by Hackers, and the type of information they can capture. Hackers use the lack of user awareness to their advantage to gain access to sensitive or confidential information. The objective of this assessment is to examine the effectiveness of the WiFi Pineapple Nano, how is used as a rogue access point and as an opportunity to educate and promote awareness.



Background

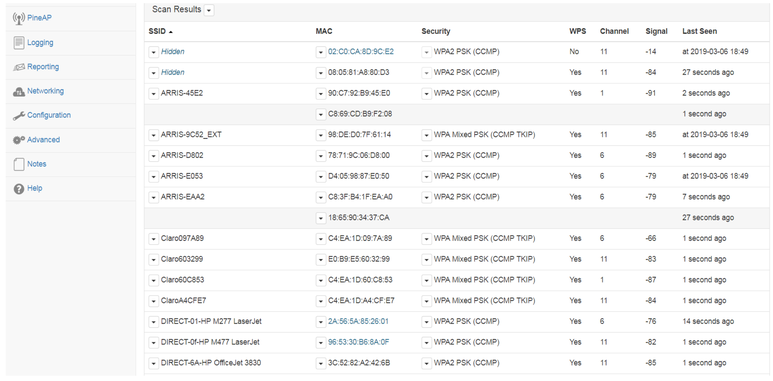
The WiFi Pineapple Nano is a device that has been designed for authorized and comprehensive wireless network audits including penetration tests. It allows its users to search and find vulnerabilities in wireless networks, analyze and identify potential targets, and promptly take corrective actions before a network is compromised. The device also provides, in its web interface, an array of modules that can be configured and used for reconnaissance, man-in-the-middle, tracking, logging and reporting the activities of these networks. Even though the device was designed to be used for audits and for the penetration testing of wireless networks, the same is constantly used by Hackers due to all of its features and capabilities. Several of its applications and modules can be used to create fake access points, spoof Domain Name Servers (DNS), sniff cookies and intercept communications in public access points. The device is gaining popularity due to its accessible price and all the applications and modules that can be downloaded free of charge from the WiFi Pineapple's web interface. Its unique design and size allows users to discreetly carry the device and perform any of its feature functions anywhere. Even though there are numerous devices in the market that can perform as well as the WiFi Pineapple Nano, this assessment centers around the device's capabilities and ease of use.

Methodology

The focus of this research centered on the features and capabilities of modules that were found to be the most commonly used with the WiFi Pineapple Nano. The modules Dwall, Evil Portal,PineAP, Portal Auth and Recon were put to test in specific environments in which the objectives set for this research could be measured. The environments were chosen as the most likely in which a Hacker would seek to use such device to gather information.

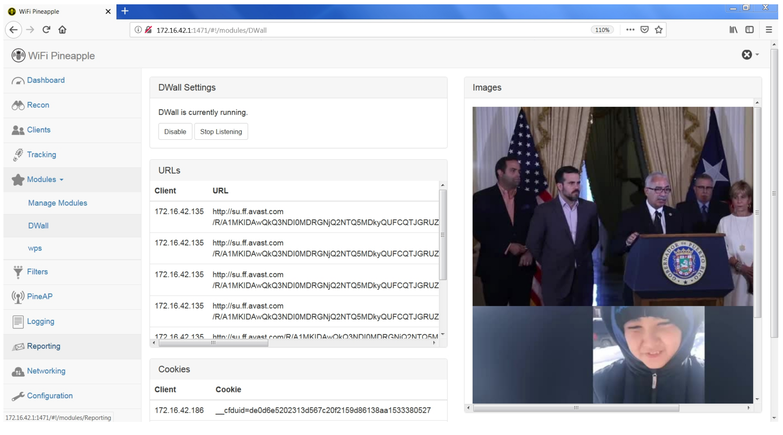
PineAP & Recon

The PineAP stands for Pineapple Access Point. This is the bread and butter of the WiFi Pineapple Nano. It provides multiple tools that can be used to perform a variety of tests: recon, traffic analysis, capture Service Set Identifiers (SSIDs), broadcast becons of SSIDs, tracking client devices as well as allowing associations and performing deauthentications



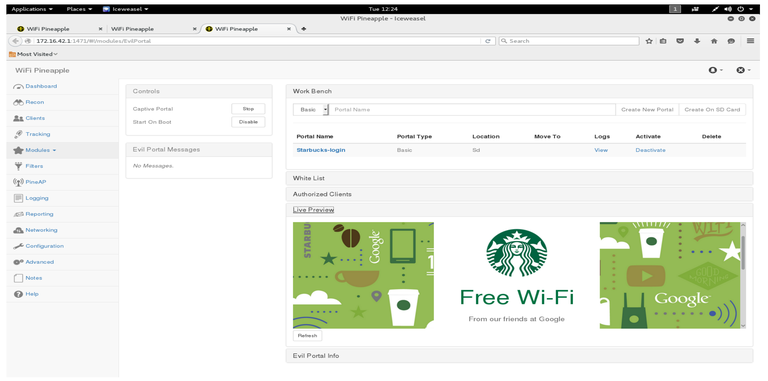
Dwall

The Dwall is a module that is described as a wall-of-sheep type feature. The same is advertised as having the capability of listening and sniffing all network traffic from users using Wi-Fi public networks or from those using rogue access points. It has been designed to capture Uniform Resource Locator (URL), cookies, data and images.



Evil Portal & Portal Auth

The use of Evil Portal and Portal Auth allows the user to create a captive portal. Captive portals have the potential of being used maliciously by hackers. By providing clients with a well-designed captive portal that displays a professional appearance, criminal hackers are able to deceive unsuspecting clients and provide them with a sense of legitimacy. Through the use of captive portals, hackers can distribute malware, gather login credentials, email addresses, and financial information. These portals are commonly used by hotels chains, fast food restaurants and coffee shops to provide their clients with a Wi-Fi hotspot. Some of the more notables establishments that use captive portals include McDonald's, Burger King, and Starbucks.



Conclusion

The WiFi Pineapple Nano is a device that proved capable of performing the modules that were tested as advertised. The PineAP and the Recon modules were used in conjunction. The PineAP is where configurations are set for how Recon will scan. The device was able to scan the Wi-Fi landscape without any issues picking up SSIDs, MAC addresses, WPS, types of security from routers and mobile devices that were beaconing their signals as shown in the image "PineAp & Recon". Such information can be used to tailor more sophisticated attacks. Dwall module was capable of sniffing some Wi-Fi network traffic, but not all as it is advertised. The image in "Dwall" shows some URLs, cookies and images captured from the devices that connected to the rogue access point. The module was only capable of sniffing plain HTTP traffic. Traffic through Virtual Private Network (VPN) or HTTPS web sites, could not be captured by the device due to the use of Secure Socket Layer (SSL). The Evil Portal and Portal Auth modules were used to clone and configure the Starbucks captive portal as show in image "Evil Portal & Portal Auth". The portal was successfully deployed and was able to deceive users into believing it was legitimate. Users were able to connect to the portal and browse the internet unsuspecting of a man-in-the-middle (MITM) attack.

References

Hak5, 2019. WiFi Pineapple Sale. Available*: https://www.wifipineapple.com/pages/nano*
Del Peón, Emiliano, 2017, July 6. *Pineapple 101: Modules' Review and Testing*, Available: https://maedium.com/@aedelpeon_33472/pineapple-101-modules-review-and-testing-part-1-c2afebba6ba0