Hacking Mobile Devices Using WiFi Pineapple Nano

Alexis Mojica Serrano
Master in Computer Science
Advisor: Jeffrey Duffany, Ph.D.
Electrical and Computer Engineering and Computer Science Department
Polytechnic University of Puerto Rico

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 and 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. These 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 and how is used as a rogue access point to deceive users to connect to it. Part of the scenarios used in this research provided the opportunity to educate and promote user awareness.*

Key Terms *— Man-in-the-middle (MITM), Rogue Access Points, Secure Socket Layer (SSL), Service Set Identifiers (SSID).*

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.

Hardware Overview

At first glance, the WiFi Pineapple Nano can be confused with a dongle due to its similar size and design. This allows the user to deploy the device in a public environment and be mistaken with a regular computer hardware. The same can be easily connected into any computer or laptop through a standard USB connector. It also has a female USB 2.0 port which can be used to connect to an Android smart phone and use its application to perform any modules within minutes. For instance, the PineAp module which is used to conduct man-in-the-middle (MITM) and phishing attacks can be deployed on the run with the use of a smart phone. The device also comes with a Micro SD card slot for storage expansion, two high gain radio antennas, a configurable reset button and status LED light, along with a variety of modules [1]. Figure 1 “Description of the WiFi Pineapple Nano” shows the previous description.

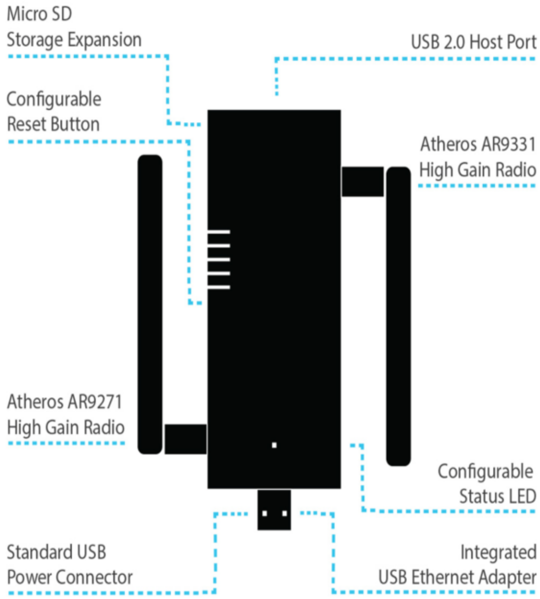


Figure 1
Description of the WiFi Pineapple Nano

OBJECTIVES

Determine if the WiFi Pineapple Nano is capable of performing as advertised.

Determine if it needs to be complemented with additional software to operate.

Who is it for and what is the experience level needed to use it.

Create awareness of the risks and vulnerabilities of access points.

METHODOLOGY

The focus of this research centers on the features and capabilities of four 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 presented in this research were chosen as the most likely in which a Hacker would seek to use this device to gather as much information as possible.

The WiFi Pineapple Nano is used for its ability to passively gather intelligence, target and track Wi-Fi devices (i.e., laptops, phones, tablets) and deploy rogue access points for man-in-the-middle attacks as it acts as a hotspot honeypot. When it comes to auditing and penetration testing wireless networks, the WiFi Pineapple Nano can be used with other tools to gather intelligence, monitor and manipulate clients traffic. This is an important feature as nowadays is important to know that networks are secured, who have access and what devices are being used to access it. The WiFi Pineapple Nano has the capability to scan these networks and gather the MAC Address, Organization's Unique Identifiers (OUI), IP Address, Service Set Identifier (SSID) and Hostnames.

PineAP & Recon

The PineAP stands for Pineapple Access Point. According to its developers, 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 [2] as seen in Figure 2 “PineAP Dashboard”.

PineAP relies on a module call Recon, which is the abbreviation for reconnaissance, the same works in conjunction with PineAP providing information that can be used with other modules. The same is in charged of scanning and gathering information about the wireless landscape just like “war driving”. It provides of all the access points in the area and displayed their information in a dashboard where it can be used to identify and capture potential targets. Recon can be set up to perform scans in live or continuous mode as well as with different time intervals.

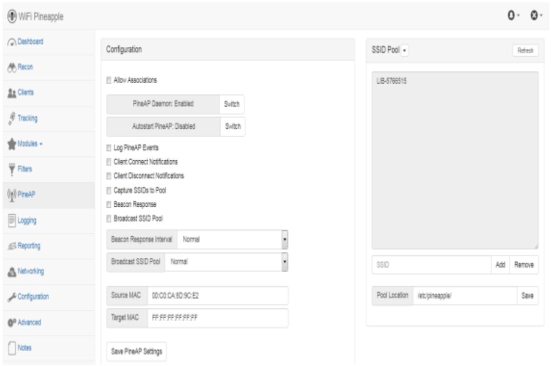
In order to test the scanning capability of the PineAP and Recon, the WiFi Pineapple Nano was deployed from two different locations. The first location was in a home environment, specifically inside an apartment complex. This location presented the best case scenario to scan the greatest amount of access points (i.e., wireless routers) and electronic devices with Wi-Fi capabilities such as laptops, computers, scanners, Internet of Things (IoT), etc. The scanning was conducted in a Live mode for an interval of 30 seconds. Another scan was performed in the same location in a Continuous mode for an interval of 5 minutes.

As a result, the Pineapple Nano performed as advertised in both modes. The Live mode was performed for 30 seconds and was able to capture over fifty access points including the devices that were connected to those access points. It displayed all of the SSIDs, MAC addresses, security protocols, channels and signal strengths of all the access points. In the case of the devices that were shown as connected, it only displayed their MAC address. The Continuous mode was performed for 5 minutes and was able to capture over 80 access points, also displaying all the SSIDs, MAC addresses, security protocols, channels and signal strengths of all the capture access points.

In the second location, the Pineapple Nano was deployed from a parking lot with a variety of fast food establishments and restaurants nearby. In order to compare the scanning capability of the Pineapple Nano in two different locations, the configuration of the PineAP and Recon were also set to run the live mode for an interval of 30 seconds and the second scan in continuous mode for 5 minutes.

As a result, there were fewer devices captured in both tests. But this was expected mainly due to the distance where the Pineapple Nano was deployed and its surroundings at that time. Nevertheless, the same information was capture with the only difference being that most access points were not secure as most these fast food and restaurants had them set up for the use of their customers.

In conclusion, the WiFi Pineapple Nano was able to performed as advertised. Its interface is easy to manage and made easy to configure the PineAP and Recon. Besides the location, the PineAP and Recon performed as expected gathering important information that can be used to tailor more sophisticated attacks. A Hacker could use the Pineapple Nano and perform various of its modules to steal sensitive or confidential information from clients connecting to unsecured Wi-Fi networks.



□ Allow Associations

PineAP Daemon: Enabled

Autostart PineAP: Disabled

□ Log PineAP Events
□ Client Connect Notifications
□ Client Disconnect Notifications
□ Capture SSIDs to Pool
□ Beacon Response
□ Broadcast SSID Pool

Beacon Response Interval: Normal

Broadcast SSID Pool: Normal

Source MAC: 00:C0:CA:8D:9C:E2

Target MAC: FF:FF:FF:FF:FF:FF

LIB-5766515

SSID

Pool Location: /etc/pineapple/

Figure 2
PineAP Dashboard

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 [3]. It has been designed to capture Uniform Resource Locator (URL), cookies, data and images.

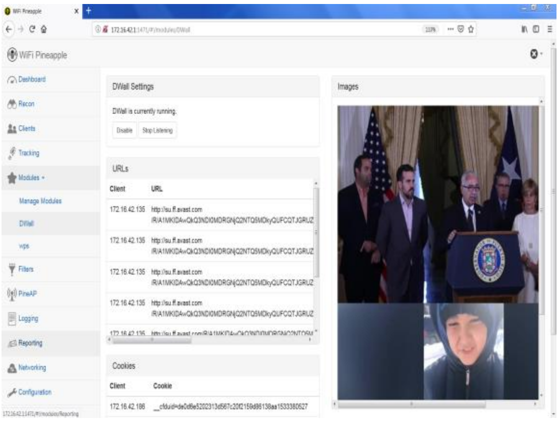
In order to test the Dwall module, the same was first downloaded from the Pineapple's dashboard along with its dependencies. The access point, located in the Networking tab, was configured to “Open SSID” and to display the SSID of "Free Wi-Fi". For this test, it was determined to deploy the Pineapple Nano in a family gathering as this setting provided the perfect opportunity to make users aware of the vulnerabilities that unsecured access points present and the risks they would take if one decides to connect their mobile devices to one. Before deploying the Pineapple Nano, the PineAP was configured to broadcast its Service Set Identifier (SSID) of “Free Wi-Fi”, allow associations between devices, log notifications of clients that connect or disconnect, and to beacon its signal to entice more devices to connect [3].

In addition, the Recon (reconnaissance) module was run in order to have a better picture of the amount of devices that could potentially connect to the access point. Due to the configuration, the scan not only captured devices from the family gathering, but also from its surroundings. However, part of the information the Recon module provides is the signal strength of the devices. This information helped extract those devices that were in the family gathering from those that were not. The devices that were part of the gathering displayed the strongest signals as they were closer to the Pineapple Nano access point, and the devices that were not, had the lowest signal strength as these were further away from the Pineapple Nano access point.

After activating the Pineapple's access point and waiting a few minutes, a notification was logged showing a device had connected to the access point. This is the first step before starting the module as it is essential to have a device connected to be able to sniff its network traffic. Right then, the module was activated and within seconds it started sniffing some traffic from the user's device as shown in Figure 3 "Dwall Module".

As result, the module was able to log some URLs, cookies, and images of the websites the user was searching online, but not as advertised. Unfortunately, after more than twenty minutes of actively listening to the access point's traffic, there were not that many URL's, cookies or images captured. This was basically due to the limited capability of the Dwall module as it can only sniff plain HTTP traffic. If the user logs into a website that uses Secure Socket Layer (SSL) to secure its web session as HTTPS [4], the Pineapple Nano does not have the capability to strip the SSL off the HTTPS.

In conclusion, Dwall module was set up and configured without any issues. It was able to capture some HTTP traffic, but not as advertised. The URL's, cookies and images that were captured are presented in an organized dashboard that allow the user to follow everything that is happening without any issues. As stated before, if a user connects to the access point using a Virtual Private Network (VPN) or logs to a website that uses SSL to encrypt the session as HTTPS, the module is not capable of sniffing that traffic [5]. The use of these can help discourage a novice or passive Hacker, but not an experienced or persistent one. In such event, an experienced Hacker can complement the Pineapple Nano with a software that strip the Secure Socket Layer and gain access to the user's networking traffic and information. Nevertheless, this served as a good teaching moment for those family members to understand the risks and vulnerabilities of using public or unsecured networks.



DWall Settings

DWall is currently running.

Disable | Stop Listening

URLs

Client	URL
172.16.42.135	http://su.ff.avast.com/R/A1MKIDAwQkQ3NDI0MDRGNjQ2NTQ5MDkyQUFCQTJGRUZ
172.16.42.135	http://su.ff.avast.com/R/A1MKIDAwQkQ3NDI0MDRGNjQ2NTQ5MDkyQUFCQTJGRUZ
172.16.42.135	http://su.ff.avast.com/R/A1MKIDAwQkQ3NDI0MDRGNjQ2NTQ5MDkyQUFCQTJGRUZ
172.16.42.135	http://su.ff.avast.com/R/A1MKIDAwQkQ3NDI0MDRGNjQ2NTQ5MDkyQUFCQTJGRUZ
172.16.42.135	http://su.ff.avast.com/R/A1MKIDAwQkQ3NDI0MDRGNjQ2NTQ5M

Cookies

Client	Cookie
172.16.42.186	__cfduid=de0d6e5202313d567c20f2159d86138aa1533380627

Figure 3
Dwall Module

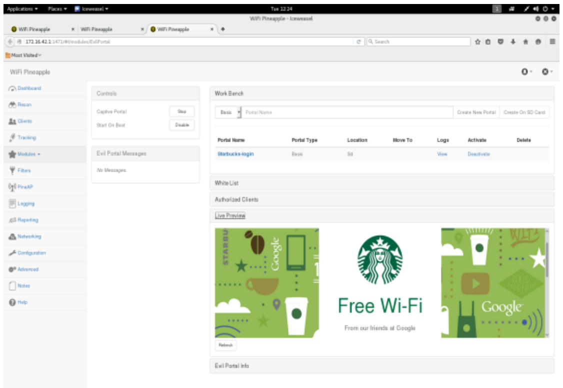
Evil Portal & Portal Auth

Nowadays, captive portals are commonly used by hotels chains, fast food restaurants and coffee shops to provide their clients with a public Wi-Fi hotspot. Some of the more notables establishments that use captive portals include McDonald's, Burger King, and Starbucks. In most, users that connect to their Wi-Fi hotspot are redirected to a web page containing a User Agreement Policy [4]. Once there, users must agree to the terms of the policy to authenticate and use their internet freely. These companies also use captive portals to push to their clients the advertisements of their products and services. The designers of the Pineapple Nano promote the device to users as having the capability, through the Evil Portal module, to create or clone a well-designed web page that can deceive those that connect to the Pineapple Nano's captive portal. A malicious person can use this module to gather sensitive data, retrieve email usernames and passwords, as well as to distribute malware.

In order to test this module and take full advantage of its capabilities, it was determined that it would be best to clone a website from a well-known establishment known to used captive portals. The captive portal would then be used to deceive anyone who connects a mobile device to use the establishment's Wi-Fi network, and to attempt capture the user's credentials. Another option was to test the captive portal that is provided by default in the Evil Portal module, but the purpose of that portal is to gain a better understanding of how the module works. The same is a plain design that just displays a username and a password box. Therefore, it was determined to clone the Starbucks captive portal in order to display a more legit portal that could deceive users once it was deployed, while also taking on a challenge worthy of this research.

This test was performed using the Portal Auth and Evil Portal modules. The Portal Auth was used to capture and create the Starbucks captive portal which would be used as host. While the Evil Portal was used to create and display the captive portal, and to capture and retrieve the user's credentials. The first step was to install the Portal Auth and the Evil Portal modules from the WiFi Pineapple Nano's interface along with its dependencies. Once the two modules were installed, they needed to be configured. In the Portal Auth settings tab, the Starbucks' URL for captive portal was pasted into the "Test Site" box. Then, inside the Evil Portal, in the "Work Bench" tab, a portal was created with the name "Starbucks-Login". Also, the "Index.php" file was modified to capture the credentials (i.e., username and password), and "MyPortal.php" file path was modified to retrieve them from the Notification panel in the Dashboard. Before deploying the captive portal, a new access point was created to display the SSID of "Starbucks Free Wi-Fi", and configured to appear in the pool of available Wi-Fi networks. Once everything was configured, it was time to clone and deploy the captive portal. (Due to legal and ethical concerns, it was determined to test the deployment of the Starbucks captive portal in a house environment.)

As result, the WiFi Pineapple Nano successfully cloned the Starbucks captive portal as shown in Figure 4 "Starbucks Captive Portal".



Controls

Captive Portal Stop

Start On Boot Disable

Evil Portal Messages

No Messages.

Work Bench

Basic | Portal Name | Create New Portal | Create On SD Card

Portal Name	Portal Type	Location	Move To	Logs	Activate	Delete
Starbucks-login	Basic	Sd		View	Deactivate	

White List

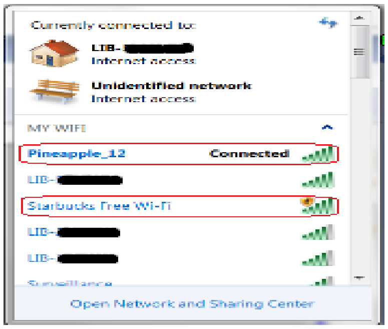
Authorized Clients

Live Preview

Figure 4

Starbucks Captive Portal

It was also successfully deployed as its SSID appeared in the list of available networks which users could connect to as shown in Figure 5 "List of SSIDs".



Currently connected to:

LIB-[redacted]
Internet access

Unidentified network
Internet access

MY WIFI

Pineapple_12 Connected

LIB-[redacted]

Starbucks Free Wi-Fi

LIB-[redacted]

LIB-[redacted]

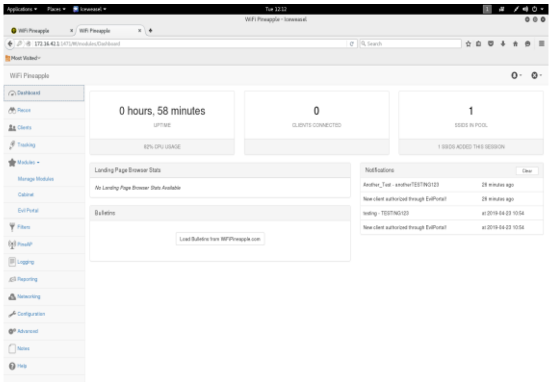
Surveillance

Open Network and Sharing Center

Figure 5

List of SSIDs

As for its performance, it allowed mobile devices to connect and successfully redirected them to the Starbucks captive portal. This demonstrated that in a real-world scenario, any person who had used it would have had to use their credentials to start a session and to use internet. Two tests were performed using a smartphone and a laptop computer. In both tests the captive portal was able to capture and display in the notification panel each time a new user connected to the portal. In the first test, the username “testing” and password “TESTING123” were typed in their corresponding boxes. In the second test the username “Another_Test” and the password “anotherTESTING123” were also typed. In both tests, once the credentials were submitted a message of “Unauthorized Access” was displayed. This message would notify the user that there was an authentication error, which would prevent the client from using the internet. In both tests, the credentials were successfully retrieved and displayed in the Notification panel as shown in Figure 6 “Dashboard Displaying Stolen Credentials”. In a real world scenario, a client would not have realized that their credentials were compromised.



0 hours, 58 minutes
UPTIME
82% CPU USAGE

0
CLIENTS CONNECTED

1
SSIDS IN POOL
1 SSIDS ADDED THIS SESSION

Landing Page Browser Stats
No Landing Page Browser Stats Available

Bulletins
Load Bulletins from WiFiPineapple.com

Notifications
Clear

Another_Test - anotherTESTING123	28 minutes ago
New client authorized through EvilPortal!	28 minutes ago
testing - TESTING123	at 2019-04-23 10:54
New client authorized through EvilPortal!	at 2019-04-23 10:54

Figure 6
Dashboard Displaying Stolen Credentials

The results of this test demonstrated that in a live setting the captive portal would have been capable of deceiving users that connect to the Pineapple Nano's access point. Clients would have connected to the Wi-Fi network not knowing that it was a cloned network. Someone with malicious intentions could use this module to capture sensitive or confidential information and perform more advanced attacks that could cause harm. Even though there are other tools that are known to be better suited to perform this type of social engineering attack (i.e., Linux Social Engineering Tool Kit), the Portal Auth and the Evil Portal performed better than anticipated and seemed to be two viable and reliable options.

CONCLUSION

In conclusion, the WiFi Pineapple Nano is a device that proved to be capable of performing the modules that were tested as advertised. The PineAP and the Recon module performed better than expected. The two modules were used in conjunction as the PineAP is where users would set the configurations for how Recon will scan. In both locations the device was able to scan the Wi-Fi landscape without any issues picking up SSIDs, MAC addresses, WPS, and the security from routers and the different mobile devices connected to them. Such information could be used to perform other types of attacks. The two modules performed as well as other devices and applications used to scan mobile devices.

Dwall was another module that was tested in this research. When put to test, the same was capable of sniffing some Wi-Fi network traffic. The same displayed some URLs, cookies and images captured from the devices that connected to the rogue access point. The module was only capable of sniff plain HTTP traffic. If a user uses a VPN to browse the internet or only connects to HTTPS web sites, the module is not able to capture any traffic due to the use of Secure Socket Layer (SSL) by those web sites. As a result, the effectiveness of the module will depend on the user's web browsing tendencies and awareness level. If a user is aware of the risks of connecting to an unsecured network and use some of the available options to secure his network traffic [5], Dwall won't be able to capture any traffic.

Finally, the last modules that were tested in this research were Evil Portal and Portal Auth. These two modules were put to test in conjunction to clone and configure a captive portal. The captive portals are commonly cloned to deceive users into believing is a legit portal to take advantage and steal their credentials (i.e., username and password). In order to prove the capability of these modules the Starbucks captive portal was cloned, configured and deployed successfully. For legal and ethical concerns, the same was deployed in a house environment. During the test, the captive portal performed as expected capturing what would have been user's credentials.

Overall, the Wi-Fi Pineapple Nano is a capable device that provides different features in the form of modules. It has some uniqueness to it as all of its features can be downloaded from the WiFi Pineapple's interface free of charge. Otherwise, the user would have to download different applications from different locations to perform some features. In that sense, there are numerous software applications and devices on the market that can perform as well, if not better, than the WiFi Pineapple Nano.

When it comes to the objectives set in this research, the device performed as advertised without the need to complement it with other applications, while the experience level needed to use it will depend on the type of module and the results that the user is seeking. In either case, the device can be used by different users regardless of experience level.

References

[1] Hak5. (2019). *WiFi Pineapple Sale*. [Online]. Available*:* https://www.wifipineapple.com/pages/nano.

[2] E. Del Peón. (2017, July 6). *Pineapple 101: Modules' Review and Testing (Part 1)* [Online]. Available: https://medium.com/@edelpeon_33472/pineapple-101-modules-review-and-testing-part-1-c2afebba6ba0.

[3] Reyvan. (2018, December 18). *Using Dwall in WiFi Pineapple* [Online]. Available: https://medium.com/@edelpeon_33472/pineapple-101-modules-review-and-testing-part-1-c2afebba6ba0.

[4] Maxpower. (2017, July 24). *Pineapple 101: Modules' Review and Testing (Part 2)* [Online]. Available: https://medium.com/@maxpowersii/pineapple-101-modules-review-and-testing-part-2-600538b492aa.

[5] R. Velasco. (2017, June 28). *Wi-Fi Pineapple, qué es la piña Wi-Fi y qué tiene que ver con la seguridad* [Online]. Available: https://www.redeszone.net/2017/06/28/wi-fi-pineapple-hacking-etico/.