WiFi Ace
(Wireless Invasion and Security Tool)

Ashish Chavan, Sonali Jadhav, Payal Chaudhari, Mandar Mankar
B.E-I.T student, Ashish Chavan of Rajiv Gandhi Institute of Technology, Versova, Mumbai, India
B.E-I.T student, Sonali Jadhav of Rajiv Gandhi Institute of Technology, Versova, Mumbai, India
B.E-I.T student, Payal Chaudhari of Rajiv Gandhi Institute of Technology, Versova, Mumbai, India
B.E-I.T student, MandarMankar of Rajiv Gandhi Institute of Technology, Versova, Mumbai, India
Assist.Prof Ankush Hutke of Rajiv Gandhi Institute of Technology, Versova, Mumbai, India

ABSTRACT: With the progression in the remote innovation there are an ever increasing number of gadgets associated over WiFi Network. Security is one of the significant worries about WiFi other than execution, extend, ease of use, etc. WiFi Ace is an accumulation of WiFi testing devices and administrations stuffed together inside Raspberry Pi 3 model B. The WiFi Ace empowers the passageway analyzer to lead WiFi attacks and perception on the picked client or on the whole framework. WiFi Ace is conservative and stealth in this way empowering the attacker to reproduce the ambushes without anyone seeing them. WiFi Ace gives administrations, for instance, think sticking, blocking or impedance with approved remote correspondences which should be possible to the entire system or only a specific hub. WLAN's(Wireless Local Area Network) are most appropriate for home clients, little network, or networks with low security prerequisites.

KEYWORDS: *Wireless Local Area Network, Wireless Fidelity, Raspberry Pi*

*****

I. INTRODUCTION

WiFi was without a moment's delay a product, now it is a need. WiFi arranges that were introduced two or three years back, can never again convey unwavering quality and execution required in a great part of the cases. A larger number of people than some other time as of late are using Smart contraptions, Phones, Tablets and compact workstations. Examining mechanical assemblies offers a WiFi Network Auditing organization which can choose bottleneck and frustration centers. The remote enlisting notices the limit of preparing contraptions to pass on in a casing to set up an area without wired structure (remote), and incorporates those developments joining around IEEE 802.11.x and distinctive remote standards and radio band organizations used by mobile phones. The remote preparing extends this plan to contraptions that enable new sorts of uses and grow an undertaking framework to accomplish puts in conditions that could never have been done by various means. It contains PDA's, telephones, convenient PCs and other adaptable and versatile gadgets. Remote systems including the remote enrolling and the flexible preparing offer (affiliations) business and customers numerous favourable circumstances, for instance, portability, flexibility, extended effectiveness, and lower foundation costs. Remote progressions cover an extensive extent of fluctuating capacities masterminded toward different uses and needs.[1]

WLANs are most proper for home customers, little systems, or systems with low security requirements. With the sending of remote systems in business conditions, affiliations are endeavouring to execute security parts that are tantamount to those of wire-based LANs. An additional piece of this security essential, is the need to restrict access to the remote framework just excessively considerable customers. Physical access to the WLAN isn't same as access to a wired LAN. Existing wired framework approach concentrates, conventionally RJ45 connectors, arranged inside structures which are secured. A customer must utilize physical access at work to associate the client PC to a framework jack. A remote access point (AP) may be accessible anyplace in the event that it has that range. Thus remote systems require secure access to the AP in a substitute route from wired LANs. In particular, it is essential to design AP from within the framework unless; the purpose of approval is affirmed. The contraption associating with the AP must be affirmed. The customer of the contraption can be checked once the device is affirmed by getting to AP. When this is finished the customer gets an ensured channel for additionally work. The 802.11 standard gives the best approach to satisfy these security essentials - endorsement of the passage contraption, customer confirmation and a sheltered channel.[9]

The WiFi Pineapple® NANO and TETRA are the 6th generation auditing platforms from Hak5 LLC. Thoughtfully developed for mobile and persistent deployments, they build on over 8 years of WiFi penetration testing expertise. At the core of the WiFi Pineapple is PineAP, an advanced suite of wireless penetration testing tools for reconnaissance, man-in-the-middle, tracking, logging and reporting. Utilizing our unique hardware design, PineAP is the most effective rogue access point suite available. Simplicity is key to any successful audit, which is why management of the WiFi Pineapple is conducted from an intuitive web interface. Built on modern standards for speed and responsiveness, the beautiful web interface puts the penetration tester[2] in control from any device. As a platform, the WiFi Pineapple is home to numerous community developed modules which add features and extend functionality. Modules install free directly from the web interface in seconds. Developing modules is made straightforward with an API friendly to coders at any experience level.[8]

II. Related work

The WiFi Pineapple gadget [12] in figure is a Mastercard estimate box running a bit of firmware known as "Jasager" (which over in Germany implies "The Yes Man") in light of OpenWrt (think of it as Linux for inserted gadgets). Offering for just $100, it packs Wi-Fi limits, a USB jack, and a few RJ45 Ethernet connectors and executes a bit mode remote component known as "Karma". The most straightforward way to deal with consider the Pineapple is as a little device that sits between a dumbfounded customer's PC (or iPhone or other web related device) and the advantage they're attempting to get to. This implies an assailant can dispatch a "Man in the Middle" or MiTM attack by evaluating the data that stream between the casualty and any assets they're getting to on the web. The physical plan of the Pineapple infers that casualties can interface with it by methods for its Wi-Fi connector and it can connect with a PC with a web association by methods for the physical Ethernet connector. It looks to some degree like this:

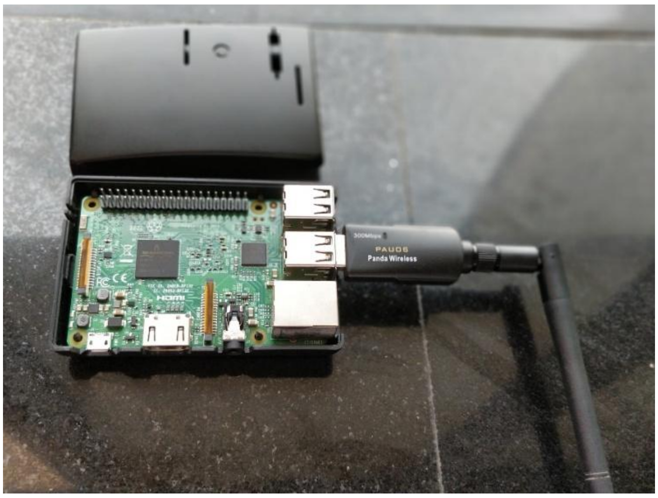


Fig. 1 .WiFi Pineapple Nano

WiFi Pineapple Nano

The WiFi Pineapple NANO was first stripped to its core. Then building on the successes and feedback from its predecessors, we developed a platform centered around performance and usability.The end result is like nothing else that's come before. It isn't a simple client radio, nor just a router or access point. The WiFi Pineapple NANO is a powerful wireless network auditing tool that leverages its unique hardware and intuitive web interface to integrate with your pen test workflow. With an emphasis on workflow and usability, the WiFi Pineapple NANO introduces a completely re-engineered web interface. Built on modern standards, the new WiFi Pineapple web interface is intuitive, fast, responsive and familiar Table views provide a detailed overview of the WiFi landscape. Context menus provide instant access to core Pine-AP features and modules. Modules remain a core feature with over the air downloads of community developed add-ons and web front-ends to popular tools. The new API is extremely simple for seasoned developers and newcomers alike.

III. Proposed work

WiFi-Ace in its center is to some degree like WiFi Pineapple yet out and out various with respect to highlights, value, ease of use and some more. A portion of the administrations gave by it are: ponder sticking, blocking or impedance with approved remote correspondences. This should be possible to the entire system or to only a specific hub. Instructing the WiFi scene and direct assaults from a live recon dashboard and latently checking all gadgets in the region. WiFi examiner can choose certain objectives for performing observation on determined targets. By capturing, the assailant can dispatch a "Man in the Middle" assault by reviewing the information that stream between the casualty and any assets they are getting to on the web. It additionally records and examines logs, create messaged reports at set interims, and recognize defenceless gadgets in your association. It likewise does following in Real time, observing an alarm with respect to the gadgets. WiFi Auditor can be utilized as a part of an expansive number of systems administration or in system of IoT gadgets which utilizes WiFi to play out their assignment. WiFi Auditor finds what can turn out badly if a terrible person tries to abuse WiFi organize loaded with PCs and IoT gadgets. It is shabby if contrasted with different choices like WiFi Pineapple. While different instruments are just intended to perform restricted measure of capacities while WiFi Auditor can play out any sort of task as though it is chipping away at an undeniable working framework.

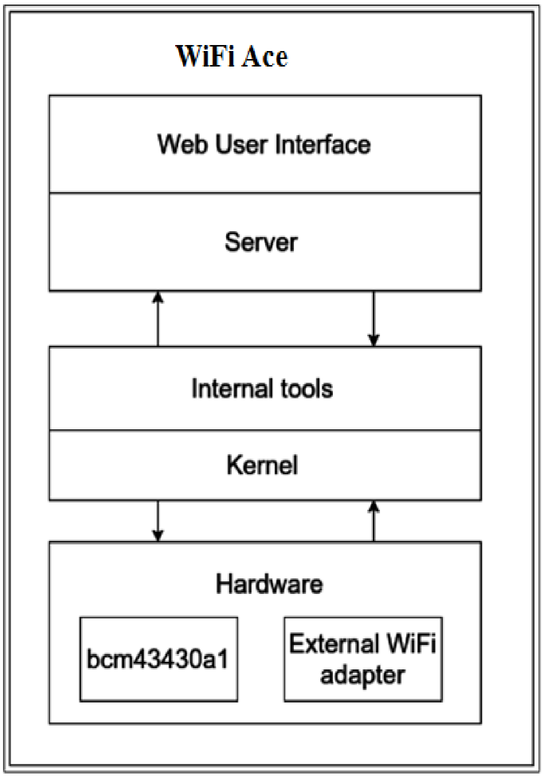


Fig 2. Block Diagram of WiFi Ace

Components Of Wifi-Ace :-

- Web User Interface: An interface is a set of commands or menus through which a user communicates with a program. A command-driven interface is one in which you enter commands. A menu-driven interface is one in which you select command choices from various menus displayed on the screen.

- Web Server : A Web server is a program that uses HTTP (Hypertext Transfer Protocol) to serve the files that form Web pages to users, in response to their requests, which are forwarded by their computers' HTTP clients.

- Internal Tools: The internal tools are made up of suits and packages which are need for pen test , One most import of this tool is the 'Aircrack-ng' it's a set of tools which cover every aspect of WiFi penetration testing .[3]

- Kernel: Most wireless devices including laptops, tablets and smartphones have network software that automatically connects to access points they remember. This convenient feature is what gets you online without effort when you turn on your computer at home, the office, coffee shops or airports you frequent. Simply put, when your computer turns on, the wireless radio sends out probe requests.

- Wifi Adapters: Monitor and Packet mode enabled wifi adapter with their appropriate drivers. This system need two of such driver if we want to perform operation simultaneously on two different channels.

Comparison with Existing Literature

Remote Technology has given numerous adjustments in strategy for correspondence in current days. With the expanded overall work of remote innovation, there is hazard about the security rules of the innovation. Various encryptions and unraveling methodologies have been executed today to transmit data over the systems. Despite that, various verification strategies have been connected. In any case, such strategies must be endorsed to ensure the security of remote systems.

1.Penetration testing is the one which can be used to perceive the obscure void in the system. This makes trial of basic components to favor the security instruments of the structure and aftereffects of Penetration testing could be used to secure the framework.[6]

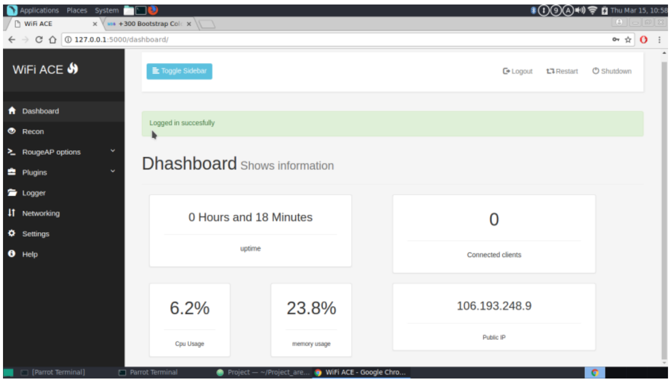
2.This paper will display an audit of Penetration testing and apparatuses. Thus, this paper will review the past work done on the security of remote systems utilizing Penetration testing. This instrument is expected to audit organize and recognize remote interference. The aftereffects of this examination found that WAI-DPS can effectively recognize the assaults to guarantee WLAN.[7]

The point of this paper was to give a general diagram of the infiltration systems utilized before in past examinations also distinguishing the future research headings in entrance testing and remote system security .This sort of assurances and security techniques can be further more created by the most recent innovations on the planet. All inclusive Mobile Telecommunications System can likewise be associated with the Wireless Fidelity (Wi-Fi) arrange. Through these kinds of systems and conventions, a bit of the security issues can be tackled. In future, various most recent innovations will be presented and it will be anything besides hard to deal with the up and coming Wi-Fi issues.[4]

IV.MODULE RESULTS

Dashboard:-

Dashboard gives you the overall status of Wifi-Ace and your device on which it is running eg :computer ,raspberry pi, etc. Dashboard displays uptime, connected clients, public IP,CPU usage and memory usage.[5]



Logged in succesfully

Dhashboard Shows information

0 Hours and 18 Minutes
uptime

0
Connected clients

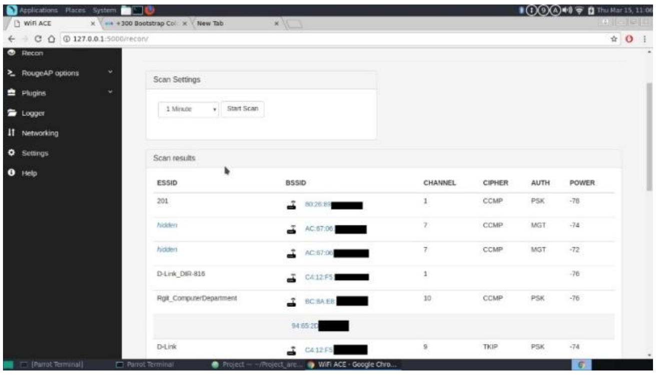
6.2%
Cpu Usage

23.8%
memory usage

106.193.248.9
Public IP

Recon:-

Recon (Reconnaissance) is used to gather information about the wireless devices present in the range of the wireless adapter. WIFIACE uses airodump-ng as a background tool to gather the information.



Scan Settings

1 Minute ▾ Start Scan

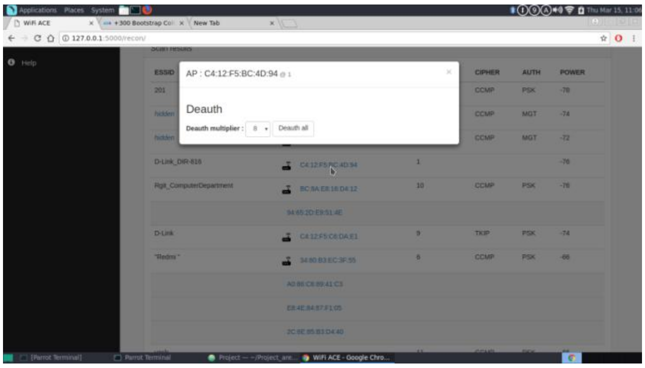
Scan results

ESSID	BSSID	CHANNEL	CIPHER	AUTH	POWER
201	80:26:89[redacted]	1	CCMP	PSK	-78
hidden	AC:67:06[redacted]	7	CCMP	MGT	-74
hidden	AC:67:06[redacted]	7	CCMP	MGT	-72
D-Link_DIR-816	C4:12:F5[redacted]	1			-76
Rgit_ComputerDepartment	BC:8A:E8[redacted]	10	CCMP	PSK	-76
	94:65:2D[redacted]				
D-Link	C4:12:F5[redacted]	9	TKIP	PSK	-74

Scan Settings : Used to scan the locality for N number of minutes. The adjustment in the amount of time spend in scanning allows you to capture valuable information like hidden SSID names (if they client and AP did handshake during the scan), probe request's, etc.

Scan Results : Presents information about the ESSID(Extended Service Set Identifier) i.e. the name of the Access Point. BSSID operating Channel. Cipher used like TKIP, CCMP, WRAP, etc. for protected communication between the client and the Access Point. Auth give's information about the authentication protocol like WEP,WPA/WPA2,etc used. PWR represents the signal strength of the access point, higher PWR value that much closer you are to the access point. That PWR value depends on the drivers so it can var. Apart from the above information the Scan Results display the associated the access point and their clients. Add to allow list/Add to deny list will add the selected MAC address to MAC filtering list.

Deauth : Used to deauthenticate the clients format the client from the Access Point, to use this option just simply click on the BSSID of the access point or the client, selecting the access point will deauth all the connected clients whereas selecting the client will only deauthenticate selected client. Deauth has multiplier's which allows you to regulate the number of packets send for deauth. The number of packets send are doubled eg : 1 = 10 packets 2 = 20 packets 3 = 40 packets 4 = 80 packets and so on.



127.0.0.1:5000/recon/

AP : C4:12:F5:BC:4D:94 @ 1

Deauth

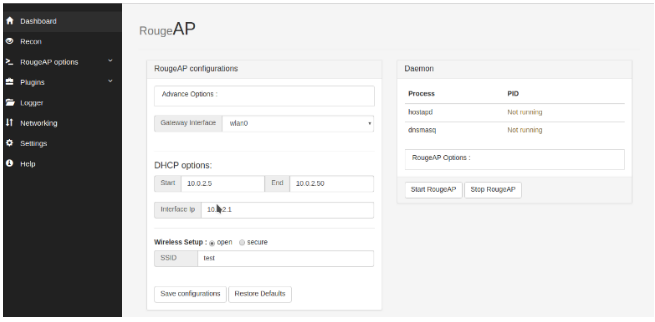
Deauth multiplier : 8

ESSID				CIPHER	AUTH	POWER
201				CCMP	PSK	-78
hidden				CCMP	MGT	-74
hidden				CCMP	MGT	-72
D-Link_DIR-816		C4:12:F5:BC:4D:94	1			-76
Rgit_ComputerDepartment		BC:9A:E8:16:D4:12	10	CCMP	PSK	-76
	94:65:2D:E8:51:4E					
D-Link		C4:12:F5:C6:DA:E1	9	TKIP	PSK	-74
"Redmi "		34:80:B3:EC:3F:55	6	CCMP	PSK	-66
	A0:86:C6:89:41:C3					
	E8:4E:84:87:F1:05					
	2C:8E:85:B3:D4:40					

Unassociated clients: Displays the unassociated client. Unassociated clients are those which are not connected to any access point tent to send the probe requests to check if any of their home access point or the access point to which they have connected previously are present.

RogueAP options:-

Setup RogueAP create a rogue access point or just normal access point using hostapd-mana with Karma attacks and MANA (MitM and Authenticated Network Attack toolkit) attacks.



RougeAP configurations

Advance Options :

Gateway Interface: wlan0

DHCP options:

Start: 10.0.2.5 End: 10.0.2.50

Interface Ip: 10.0.2.1

Wireless Setup : ● open ○ secure

SSID: test

Daemon

Process	PID
hostapd	Not running
dnsmasq	Not running

RougeAP Options :

RogueAP configuration :

Gateway interface : The interface that will bridge with the wireless adapter that is used to create the access point, this interface will provide internet connection to the clients.

DHCP options : Used to allocate the range of the IP address that would be assigned to the RogueAp clients. 'Start' set the start range and 'End' sets the ending range of IP addresses. 'Interface IP' sets the IP for the adapter that will be used to create the access point.

Wireless setup : Used to set the authentication of the access point secure option used WPA2/PSK.

Advance Options :

Enable MANA : Karma attacks with more enhanced hostapd-mana attacks,enabling this option makes RogueAP to respond to all the probe requests from the wireless devices searching for the Wireless Access Points.

Aggressive MANA : With "Enable Mana option the RogueAP will only respond to the probe request received to the respective devices , but in Aggressive mode it will rebroadcast all the Access Point to all the devices.

Enable MAC Filter : Allow/Disallow only the devices with their MAC address listed in the filter option. Similar to the MAC filter in the router.

Probe MAC Filter : Enhanced MAC filter from hostapd-mana, even blocks the probes to the listed devices.

Daemon : Displays the process id of the running hostapd-mana and DNSmasq processes.

Save Configuration & Restore Defaults : Save will create a new file containing all the above selected options and launch the hostapd-mana and DNSmasq. Restore will restore all the changes made by the user to default.

RogueAPoptions : Same as Advance Options but allows to turn ON or OFF the advance options when RogueAp is running.

Conclusion And Future Work

Remote systems give extraordinary comfort to us however accompanies dangers and vulnerabilities (as all accommodations in IT). The equipment is getting littler and all the more intense regular so the instruments, for example, WiFi inspector can help relieve the danger of remote assaults. WiFi evaluator gives an adaptable interface to surveillance, assaulting and revealing everything under one rooftop. WiFi entrance won't be the same again attempt WiFi examiner now. Future Scope of this paper is bolster for 5 GHz and custom module underpins.

References

[1] B. M. Mehtre, Sugandh Shah,"An overview of penetration testing techniques", Springer Journal of Computer, pp 27-49, 2014.

[2] Shao-Long WANG, Jian WANG, Chao FENG and Zhi-Peng PAN Wireless Network Penetration Testing and Security Auditing Nov 23, 2016.

[3] Suraj S. Mudalik," Penetration testing: An Art of Securing the System (using Kali Linux)", International Journal of advanced research in Computer Science and Software Engineering, ISSN: 2277 128X ,Volume 5, Issue 10, October-2015.

[4] AkshikaAneja ,"A Study of Security Issues Related With Wireless Fidelity (WI-FI) " Garima Sodhi Assistant professor Department of Computer Science, GNDU Department of Computer Science, DAV College Amritsar – India, Volume 4 Issue 2, Mar - Apr 2016

[5] Dinndorf J., "Performance Comparisons of Operating Systems for the Raspberry Pi", The 14th Winona Computer Science Undergraduate Research Symposium, Winona State University, 2014

[6] Deris Stiawan1, Mohd Yazid etc," Penetration Testing and Mitigation of Vulnerabilities Windows Server", International Journal of Network Security, Vol.18, No.3, PP.501-513, 2016.

[7] Jason Andress, and Ryan Linn, "Coding for Penetration Testers", Elsevier, Syngress Publication, 2015.

[8] Jai Narayan Goel, BM Mehtre," Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology", 3rd International Conference on Recent Trends in Computing 2015 (Elsevier), Procedia Computer Science 57,pp 710-715, 2015.

[9] https://en.wikipedia.org/wiki/Penetration_test

[10] https://en.wikipedia.org/wiki/Raspberry_Pi

[11] https://www.troyhunt.com/the-beginners-guide-to-breaking-website

[12] https://www.wifipineapple.com/pages/nano