Wireless Security – An Approach Towards Secured Wi-Fi Connectivity

Nishant Pimple[1]
Department of Computer Engineering
VIVA Institute of Technology
Mumbai, India
[1]jiten.nish@gmail.com

Utkarsha Pawar[2]
Department of Computer Engineering
VIVA Institute of Technology
Mumbai, India
[2]utkarshapawar2299@gmail.com

Tejashree Salunke[3]
Department of Computer Engineering
VIVA Institute of Technology
Mumbai, India
[3]tejashrees04@gmail.com

Janhavi Sangoi[4]
Department of Computer Engineering
Viva Institute of Technology
Mumbai, India –
[4]Janhavisangoi@viva-technology.org

Abstract - **In today's era, the probability of the wireless devices getting hacked has grown extensively. Due to the various WLAN vulnerabilities, hackers can break into the system. There is a lack of awareness among the people about security mechanisms. From the past experiences, the study reveals that router security encrypted protocol is often cracked using several ways like dictionary attack and brute force attack. The identified methods are costly, require extensive hardware, are not reliable and do not detect all the vulnerabilities of the system. This system aims to test all router protocols which are WEP, WPA, WPA2, WPS and detect the vulnerabilities of the system. Kali Linux version number 2.0 is being used over here and therefore the tools like airodump-ng, aircrack-ng are used to acquire access point pin which gives prevention methods for detected credulity and aims in testing various security protocols to make sure that there's no flaw which will be exploited.**

Keywords - Wi-Fi, Security, Wi-Fi Security, WPA/WPA2 ,WPS, WEP.

I. INTRODUCTION

The device is so super-convenient that it analyzes a variety of different networks. Not only that, but it also helps by doing the encryption. It also gives a way to breach all the said networks [12]. It aspires the users to invent an accurate, detailed and useful analysis of network standards. Along with that, it will also suggest various ethical ways to improve these networks. Every other networking encryption standard (WPA/WPA2, WPS) also can be thoroughly discussed in this given system [11][12].

The wide drawbacks into the system of the network are from the time since there was the arrival of the wireless local area network (WLAN) that came into the class of the networks, can be considered as a disadvantage [2]. So we hereby in this system, we look forward upon the newly occurred network-related securities that have risen up. Topics from the decryption and encryption techniques which can guard the essential data are discussed [12]. The effortlessly and easily within a very less time broken Wired Equivalent Privacy (WEP), the WiFi Protected Access (WPA) followed through the WiFi Protected Access II (WPA2) are being severely explored [5][8][9][11]. The systematic procedures for maintaining and providing high levels of security hereby to keep the user protected are discussed [1][3][4]. The most promising feature added in the system is portability.

The system aims to study ethical hacking of WiFi networking encryption protocols [5][6][8][12]. It is made for educational purpose only and aims in bringing awareness among society about the privacy of their respective data and how they can safeguard their data from intruders/crackers.

II. EXISTING SYSTEM

The Wi-Fi encrypted protocols as everyone is aware of very much can be easily cracked, damaged, used and destroyed using several ways is also considered as a drastic and wide category flaw [12]. The most popular and famous procedures or steps that almost every technically sound person knows in cracking the passwords and exploiting the user's network by not letting him know is using "aircrack-ng" [11]. To crack using this method quickly without much major thought or effort, the user has to have a laptop a desktop or a machine with Kali Linux. Along with it a remote card which supports monitor/injection mode. Aside from these apparatuses, the client additionally needs to get an outside remote card which can monitor/injection mode.

The form of packets in the air is transmitted by wifi. By using 'airodump' the captured packets are dumped in the air. The users that are connected to victim's Wi-Fi are selected since cracking isn't possible for this a valid WPA handshake is needed [11][12][13]. The attacker captures handshake by sending de-authentication packets to the host which is connected to Wi-Fi.

This method tests WiFi passwords through a wordlist basically performing a dictionary attack [5][8][11][13]. Also, the time taken is very long. So to overcome this limitation the proposed project comes with much more reliable and standard cracking methods.

978-1-7281-5197-7/20/$31.00 ©2020 IEEE

III. PROPOSED METHODOLOGY

This system aims to secure wireless networks. It consists of various integrated tools in it as shown in the below figure. The wireless interface of raspberry pi is used to start the exploitation of the network [7]. This would take you to choose the method pyrit, aircrack-ng to capture the packets for handshaking [11]. This handshaking will be used at the time of authentication when the user is supposed to login into the network.

When the handshaking is captured, it will take the user to the SSL certificate option. This options menu will be prompted in which you can either create an SSL certificate or select a particular SSL in the directory. Next process will be to either select Brute force or Web-Interface [10][11]. Web-Interface is recommended after selecting it, four terminals will be spawned simultaneously consisting of "fake DNS", "DHCP server", "Deauthentication" and "WiFi information" [5][8].

On the user side, the user will get disconnected from its original access point and will force the user to connect to the fake access point. SSL certificates will prompt into the user screen asking to sign to the network because of some security issues [3][4]. Handshaking comes into the picture when a user enters the password and that password is matched with it. If the password is matched, the user gets disconnected from the fake AP and the password is displayed in "Wifi information" terminal [5][8].

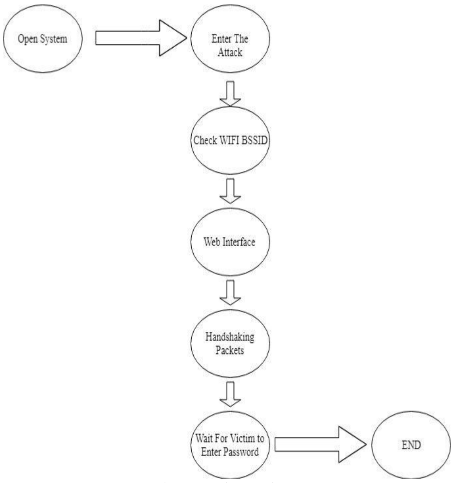


Fig. 1. Flow chart

Fig. 1. shows the flow of the project as in how the systems runs forward from the checking part to the handshaking part.

This method tests WiFi passwords through a wordlist basically performing a dictionary attack [5][8]. Also, the time taken is very long. So to overcome this limitation the system comes with much more reliable and standard cracking methods.

IV. BLOCK DIAGRAM

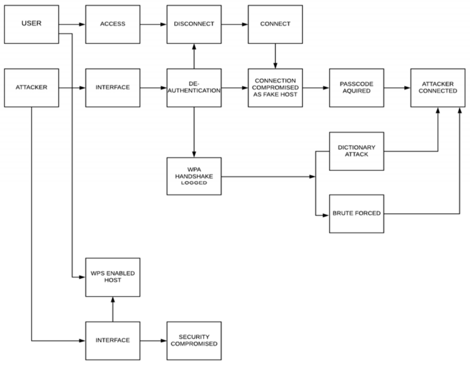


Fig. 2. Block Diagram

In Fig. 2. The block diagram is given. It comprises the structure of the system in a very precise format. It comprises of all the sections stepwise. The details are given below.

Deauthentication :- This assault sends disassociate packets to one or more customers or users into the network which might be presently related with a selected get right of entry to point. The clients are executed for a number of reasons:

Finding a concealed ESSID - This is an ESSID which is not always shown, it is most of the time hidden as per the name suggests. A similar term for this is "cloaked".

Possessing WPA/WPA2 handshakes by way of forcing users to reauthenticate [11].

Form ARP requests (Normal Windows users most often let go off their ARP cache while disconnected).

Dictionary Attack :- A dictionary assault is a procedure or technique used to harm the pc safety of a password-protected machine or server. It attempts to harm an authentication secured mechanism by way of checking into each phrase in a dictionary as a password or trying to decide the decryption key of an encrypted message [12][13].

Brute Force :- A brute pressure attack is an ordeal and error method utilized by application applications to decode encrypted facts together with passwords or Data Encryption Standard (DES) keys, via exhaustive effort in place of employing highbrow strategies [10][11][12].

V. WORKING

1. The hardware part has come up, evolved, has been added through many mindblowing features and developed in through several different types of versions that feature in it several variations in the category of memory capacity and peripheral-device support which is the reason this is used frequently without anything else being used as its replacement [7].
2. This diagram of RPI shows Models A, B, A+, and B+. Model A, A+, and the Pi Zero show the lack of Ethernet, USB components.
3. The Ethernet adapter is further connected to an extra USB port.
4. In following RPI models, the USB port is connected in a straightforward way to the system on a chip (SoC).
5. Upon the RPi 1 Model B+ and above that, the USB and Ethernet chip consists of a five-point USB connector

from which 4 ports are gatherable, whereas the RPi 1 Model B just gives [2][7].

6. In RPi Zero, the USB port is likewise amalgamated legitimately to SoC it utilizes a small scale USB (OTG) port.
7. Raspberry Pi 2 contains a quad-core processor running at 900 MHz with 1 GB RAM [7].
8. It is 4 to 6 times more powerful than its previous processor.
9. The video controller can radiate standard present-day television resolutions, for example, HD, Full HD, and sequential screen resolutions and more established standard CRT television resolutions.
10. The Raspberry Pi can be used with any input peripherals [7].

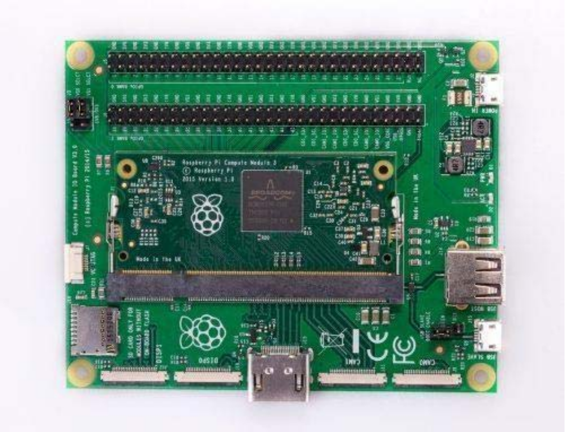


Fig. 3. Raspberry Pi

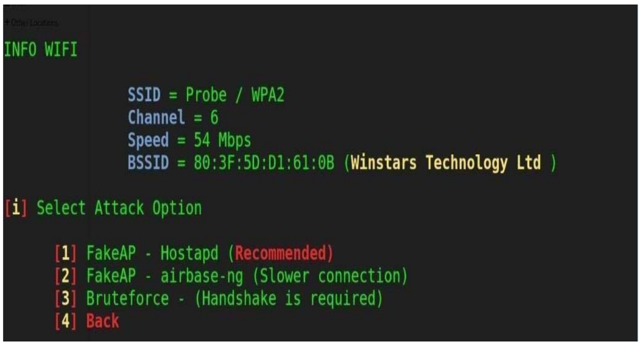
In Fig. 3. the Raspberry Pi components have been depicted. The Raspberry Pi is a junction of small single-board computers and not a huge one that needs more space to be set on somewhere to eat up the unnecessary free part which can be considered as an advantage because more space can end up making the project complex [7]. It was made in the country of the United Kingdom by the Raspberry Pi Establishment to rouse the instructing of fundamental and the basic ideas of it in computer science in schools and in emerging nations so that the students will be aware of the modern and new technology as well which will boost up their technical skills and knowledge [7][16][17][18].

VI. PROTECTION MECHANISM

To provide the security we have incorporated the following measures for the protection of the user network [1][3][4]. As mentioned above we have three major steps in which the system works so the prevention too is different for the different steps. For various different attacks on wireless networks, there are different mitigations on them. For DDoS attack mitigation, it shares the data with AES, u can use any Linux but Kali and parrot sec are well known for pen-testing. For the de-authentication process use the DDoS mitigation or using DDos proof servers. For spoofing prevention never ever give any access or permission to enter into the network to outsiders and change the Mac address at regular intervals. The next is phishing, to stop it from giving access to outsiders and check the domain address properly. For SQL injection attack prevention, weakness in the components used and datasets that contain information that hackers can steal are normally found, so it's indispensable to apply patches and updates [3][4][5]. A WAF can be especially valuable to give some security insurance against another weakness before a patch is accessible. For the prevention of packet sniffing, unauthorized users must not be allowed any communication into the network [1][3][4]. For the MITM attack prevention strong encryption multiple rounds should be performed, it is basic to ensure your default router login is changed [11][12]. In the event that an aggressor finds your switch login certifications, they can change your DNS servers to their vindictive servers. For securing from the password thefts the simple and common rules like having a long series of password with a combination of large that is capital and small alphabets and special characters that are the symbols with numbers.

For the prevention of WPS attack disable WPS pin and don't let the Brute Force take place by setting up appropriate delay time [10][11]. For the final prevention that is Evil Twin, the Mac spoofing at regular intervals should be done along with it the prevention from death using high-quality routers like Rufus and more can be done.

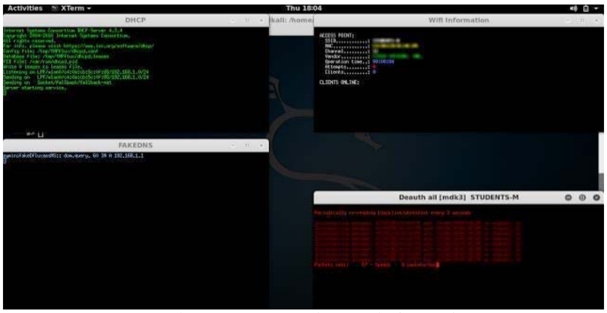
VII. RESULT



```
INFO WIFI

                SSID = Probe / WPA2
                Channel = 6
                Speed = 54 Mbps
                BSSID = 80:3F:5D:D1:61:0B (Winstars Technology Ltd )

[i] Select Attack Option

      [1] FakeAP - Hostapd (Recommended)
      [2] FakeAP - airbase-ng (Slower connection)
      [3] Bruteforce - (Handshake is required)
      [4] Back
```

Fig. 4. Options to Attacks

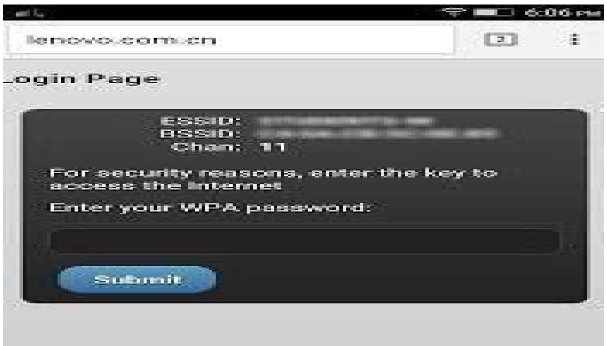
Fig. 4. shows us the way in which the FakeAP instance is started while copying the original access point- You will be given a menu of various fake login pages you can present to the user. These are adaptable with work, yet should coordinate the device and the language.



```
ACCESS POINT:
  SSID............:
  MAC.............:
  Channel.........:
  Vendor..........:
  Operation time..:
  Attempts........:
  Clients.........:

CLIENTS ONLINE:
```

Fig. 5. DHCP and WIFI information

Fig. 5. shows a Spawns of an MDK3 Process- This is the last point to arm the attack; Now, you are prepared to fire, so press enters to dispatch the attack. The attack generates numerous windows to shape a cloned or we can say a copy form of their remote network while simultaneously jamming the typical passage, luring the client to join the indistinguishably named, yet unencrypted, network.



Login Page

ESSID: [redacted]
BSSID: [redacted]
Chan: 11

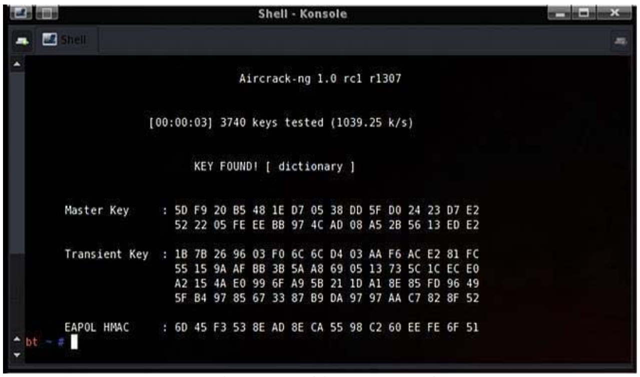
For security reasons, enter the key to access the internet

Enter your WPA password:

Submit

Fig. 6. Fake login page (SSL certificate)

Fig. 6. displays a DHCP server launched in the FakeAP network. A fake DNS server is initiated in order to gather all of the DNS requests and divert all of them to the host with the help of running the script. When we knowingly or unknowingly enter the wrong password, then there occurs failure of the handshake check, and the client is incited to attempt once more. And now when we knowingly or unknowingly enter the correct password without a single mistake, it verifies whether it is right or not and stores the password to a text file while showing it on the screen. The user is then additionally redirected to a "thank you" screen or interface as the jamming stops and the fake AP shuts and closes down.



```
                          Aircrack-ng 1.0 rc1 r1307


                 [00:00:03] 3740 keys tested (1039.25 k/s)


                          KEY FOUND! [ dictionary ]


     Master Key     : 5D F9 20 B5 48 1E D7 05 38 DD 5F D0 24 23 D7 E2
                      52 22 05 FE EE BB 97 4C AD 08 A5 2B 56 13 ED E2

     Transient Key  : 1B 7B 26 96 03 F0 6C 6C D4 03 AA F6 AC E2 81 FC
                      55 15 9A AF BB 3B 5A A8 69 05 13 73 5C 1C EC E0
                      A2 15 4A E0 99 6F A9 5B 21 1D A1 8E 85 FD 96 49
                      5F B4 97 85 67 33 87 B9 DA 97 97 AA C7 82 8F 52

     EAPOL HMAC     : 6D 45 F3 53 8E AD 8E CA 55 98 C2 60 EE FE 6F 51
bt ~ #
```

Fig. 7. Cracking Password

Fig. 7. gives us a clear idea about every password which is submitted is verified against the handshake from the previous stage. The attack will be automatically closed after the correct password is submitted.

VIII. FEATURES

Kali Linux is an operating system especially built-in for network penetration testing which makes it reliable for the system. The microcontroller used in the system is Raspberry Pi3 [7]. The Raspberry Pi is a junction of small single-board computers and not a huge one that needs more space to be set on somewhere to eat up the unnecessary free part which can be considered as an advantage because more space can end up making the project complex [7]. Due to its super-portable capability and small size, it may become the most popular ethical hacking systems [6]. Hence, less size so is the cost. Tested over millions of Raspberry Pi is produced to date, Module IO pins have 35u hard gold plating [7]. The system aims to bring awareness among people to select good and strong passwords to keep their data safe. The system tests the WiFi security mechanism and aims in enhancing advance encryption protocols [1][4][5][8][12]. Security analysts/penetration testers can use the system to test security mechanisms [1][4]. It would be helpful for naïve users to test their home network. Institutes and organizations will use to test their business network.

IX. CONCLUSION

There are many different ways for the important and personal information to be forged, so theft should be reduced by providing network protection and to lower the risk of leaking important information into the wrong hands hence security is needed. Despite the fact that there isn't an approach to make the information 100% secure, regardless of whether it is simple or advanced; it can be made difficult to acquire by others.

The system addresses ethical hacking from several perspectives. The study of cracking protocols to test the security mechanism of a router and to fix the vulnerabilities and safeguard the confidentiality of the user is the objective.

X. FUTURE SCOPE

The system can be enhanced in terms of portability. Updates will be provided. Better GUI improvement will be made. Security logs will be given.

ACKNOWLEDGEMENT

We would like to express a deep sense of gratefulness towards our mentor Dr Tatwadarshi Nagarhalli, Department of Computer Engineering for his constant support, motivation and valuable suggestions. This work that we have been able to present is because of his timely guidance and encouragement.

REFERENCES

[1] Radhi S Nair, Prof. Ashok Babu, Dr Vinodh P Vijayan, "A Survey on Wi-Fi Security Techniques", International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 04, Apr-2018, pp 4705 - 4707.

[2] Dongsheng Yin and Kai Cui, "A Research into The Latent Danger of WLAN", The 6th International Conference on Computer Science & Education (ICCSE 2011), August 3-5, 2011, pp 1085 – 1090.

[3] Dr. Glen Sagers, Dr.Bryan Hosack, Dr RJ Rowley, Dr Douglas Twitchell, Ms Ranjitha Nagaraj, "Where's the Security in WiFi? An Argument for Industry Awareness", 2015, 48th Hawaii International Conference on System Sciences, pp 5453-5461.

[4] Austin Gilbert, "Wireless Security Study Guide: Mediocre at Best", IEEE DISTRIBUTED SYSTEMS ONLINE 2005 Published by the IEEE Computer Society, Vol. 6, No. 11, November 2005, pp 1 - 3.

[5] Andrew Zafft and Emmanuel Agu, "Malicious WiFi Networks: A First Look", 7th IEEE Workshop on Security in Communication Networks 2012 SICK 2012, Clearwater" pp 1038-1043.

[6] Ranjini Mukhopadhyay and Asoke Nath, "Ethical Hacking: Scope and challenges in 21st century", International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163, Volume 1 Issue 11, November 2014, pp 30 – 37.

[7] Maryna Yevdo, NymenNo, Elsayed Mohamed, Paul OnwuaNpa Arinze, "Ethical Hacking and Penetration Testing Using Raspberry PI", 2017 4th International Scientific-Practical Conference Problems of Info-communications, October 10-13, 2017, pp 1791-84.

[8] Haishen Peng, "WIFI network information security analysis research" 2012 IEEE, pp 2243 – 2245.

[9] S Vinjosh Reddy, K SaiRamani, K Rijutha, Sk Mohammad Ali, CR. Pradeep Reddy, "Wireless Hacking - A WiFi Hack By Cracking WEP", 2010 2nd International Conference on Education Technology and Computer (ICETC)", 2010, pp 189-193.

[10] Saif Ur Rehman, Saeed Ullah, Sardar Ali, "On Enhancing the WEP Security Against Brute-force and Compromised Keys", 2010 International Conference on Computer Information Systems and Industrial Management Applications (CISIM), 2010, pp 250 - 254.

[11] Yonglei Liu, Zhigang Jin, Ying Wang, "Survey on security scheme and attacking methods of WPA/WPA2", 2010 IEEE, pp 10-13.

[12] Chen and Tien-Ho Chang, "The Cryptanalysis of WPA & WPA2 in the Rule-Based Brute Force Attack", An Advanced and Efficient Method 2015 10th Asia Joint Conference on Information Security, 2015, pp 37 – 41.

[13] Omar Nakhila, Afraa Attiah, Yier Jin, Cliff Zou, "Parallel Active Dictionary Attack on WPA2-PSK Wi-Fi Networks", 2015 Track 3 - Cyber Security and Trusted Computing, 2015, pp 665 – 670.

[14] Ankit Fadia, Nishant Das Patnaik., "Software Hacking", 2010, pp. 125-215.

[15] Ankit Fadia, "An Ethical Hacking Guide to Corporate Security", 2004, pp. 202-235.

[16] Ankit Fadia, "An Ethical Guide to Hacking Mobile Phones", 2005, pp. 110-175.

[17] Kevin Beaver, Stuart McClure, "Hacking For Dummies", 2004, pp. 258-303.

[18] Peter T. Leeson, Christopher J. Coyne, "The Economics of Computer Hacking", 2006, pp. 75-88.

[19] Paul A Taylor, "From Hackers to Hacktivists: Speed Bumps on the Global Superhighway", 2005, pp. 243-261.

[20] M.G. Siriam, "The Modus Operandi of Hacking", 2006, pp. 148-177.

[21] Bryan Smith, William Yurick, David Doss, "Ethical Hacking: The Security Justification", 2002, pp. 228-232.

[22] Matthew Tanase, "IP Spoofing: An Introduction", 2003, pp. 17-44.

978-1-7281-5197-7/20/$31.00 ©2020 IEEE