International Journal of Engineering Research in Electronic and Communication Engineering (IJERECE) Vol 3, Issue 5, May 2016

A Study on 802.11 Wireless Routers Hacking Techniques and Security Encryption Levels

[1] Amith Raj M.P [2] Sneha H.R, [3] Bindu Bhargavi S.M, [4] Rekha Jayaram
[1][2][3][4] Dayananda Sagar College of Engineering, Bengaluru, India.
[1]amith.veyron@gmail.com, [2]snehahr22@gmail.com, [3]bindu.sm@gmail.com3, [4]rekhajayaram20@gmail.com

***Abstract*— A device that performs both the functions of routing and the functions of a wireless access point is called as a wireless router. It can also be used to provide access to the private computer network or Internet. A set of Media Access Control(MAC) and Physical Layer specifications for implementing wireless local area network (WLAN) computer communication is defined in IEEE 802.11. It supports different connection types like PPPOE, Static IP address, Dynamic IP address and Bridge as provided by the ISP. These devices can also be used as modems and WiFi Router protected with a password. There are various WLAN encryption techniques like WEP, WPA, WPA-2(PSK). But all of these encryptions are vulnerable and can be hacked using certain softwares and techniques. In this paper, a number of hacking techniques using softwares like *Aircrack, WiFite* are explained for research purpose. This paper also discusses about setting up a secure WiFi router using different encryption techniques with combination of security features of routers like Mac Address filtering and Firewalls to protect from hackers and attackers. The primary purpose of this research is to demonstrate a brief idea on ethical hacking and provide sufficient security for home and enterprise network.**

***Index Terms*— Router, Security, Encryption, WPA -2, Aircrack, WEP, WPA, Mac Filtering, Firewalls.**

I. INTRODUCTION

A device which forwards data packets from one node to another among different computer networks is called a router which is connected to two or more data lines from different networks. To determine the destination, the router reads the address information in the packet when the data arrives [6]. A wireless router is a device which performs the functions of a router and also it includes the functions of a wireless access point and it provides access point and provides access to the internet or a private computer network. Wireless router allows greater mobility. Because individual computer IP addresses are not directly exposed to the internet, the use of a router provides superior protection against hacking. Wireless router does not consume computer resources whereas a firewall program does consume [7]. IEEE 802.11 is a set of media access control(MAC) and physical layer specifications for implementing wireless local area network computer communication [8]. It is an effective foundation for the transport of IP packets at the network layer [9]. It also supports static and dynamic IP addresses. The permanent address on the internet assigned to a computer by an ISP is called static IP address whereas the temporary IP address is called a Dynamic IP address [10].

There are a lot of techniques used in hacking, some of them are: Denial of service (DOS), Man-in-the-Middle (MITM) These attack can break connections which are otherwise secure [11]. There is another traditional attack called Brute Force attack. It is like trial and error method, that is used to crack certain information like personal identification number or user password. This attack may also be referred to as brute force cracking [12].

Section I gives a brief Introduction about the paper and Section II explains different Encryption levels and Features of Router and also discusses current literatures from different papers and Section III concentrates on Different Hacking Techniques by an attacker. Section IV shows a real time example and recommends techniques and features to be used to build a secure WiFi Network along with results and observations. Section V Concludes the paper and last section gives Citations and References.

II. ENCRYPTION FEATURES OF ROUTER

Firewall: The firewall will inspect the data that comes from the internet and filters and passes the safe data packets and discards the dangerous packets. The firewall can be either hardware or software. The hardware firewall comes in between the local network of computer and the internet whereas the software firewall can be installed on individual computer networks. [13]

Radius and EAP: WPA implements the Extensible Authentication Protocol (EAP) and the IEEE 802.1x standard for port-based access control to improve the user authentication and access control. This framework uses Radius (Remote Authentication Dial-in User Service) which is a central authentication server that authenticate each user on the network. Different encryption techniques are WEP, WPA and WPA2. WEP (Wired Equivalent Privacy): Currently it is the most widely used Wi-Fi security algorithm. WEP system remains highly vulnerable and the system that rely on it should be upgraded.
WPA (Wi-Fi Protected Access): It was the direct response and replacement to the increasingly apparent vulnerabilities of the WEP standard. WPA uses the keys like 256-bit, a significant increase over the 64-bit and 128-bit keys used in the WEP system.

WPA2(Wi-Fi Protected Access 2): Some notable changes between WPA2 and WPA was the introduction of CCMP (Counter Cipher Mode with Block Chaining Message Authentication Code Protocol) as a replacement for TKIP which is mandatory and the use of AES algorithms. [14]

***MAC (Media Access Control) addresses filtering*:**

It defines list of devices and allows only those devices on Wi-Fi network. Each device is etched with its own MAC address which identifies it on a network. A router will first compare a device's MAC address against an approved list of MAC addresses and only allow a device onto the Wi-Fi network if its MAC address has been approved in MAC address filtering list [15]. MAC address filtering uses blacklist and whitelist. A blacklist which is also called as block list is a basic access control mechanism which blocks the specified MAC addresses only. The opposite to blacklist is a whitelist, which means only items on the list are let through requested gate [16].
S Vinjosh Reddy has discussed in his paper "Wireless Hacking - A WiFi Hack by Cracking WEP". They've talked about the entire process of cracking WEP encryption of Wi-Fi in their paper. They have stated some tools that would give them the ability to break their own WEP key

[1]. Nada CHENDEB has discussed in his paper "Performance evaluation of the security in wireless local area networks (WiFi)." that WEP is absolutely vulnerable and WPA has made improvements. The load, the robustness requested and the importance of transmitted information should be decided by network administrator

[2]. Keun Young Park, Yong Soo Kim and Juho Kim has discussed in their paper "Security Enhanced IEEE 802.1x Authentication Method for WLAN Mobile Router" which is a new IEEE 802.1x based authentication method with enhanced security. The RTR function of TPMs to authentication procedures between APs and servers so that the integrity of the APs requesting access is verified is the proposed method. MITM attacks using rogue APs could be fundamentally blocked by applying their proposed method

[3]. ARASH HABIBI LASHKARI has discussed in his paper "Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)". They discuss about the wireless security protocol as WPA and define the two modes. They also try to describe all major Improvements on WPA such as MIC, cryptographic message integrity code or new IV sequencing discipline, rekeying mechanism and per-packet key mixing function. They make a whole diagram for WPA decryption and encryption. They conclude discussing the major problems on WPA

[4] I. P. Mavridis has discussed in his paper " Real-life paradigms of wireless network security attacks" about three main security protocols WEP, WPA and WPA2. Analytical procedure towards WEP and WPA2 cracking were discussed and presented in detail which were derived from actual situations. Their study however depicted that wireless network is vulnerable to hacking attempts, if it is not protected and carefully set up [5].

III. HACKING TECHNIQUES

Computer criminals to penetrate a network, there are several *common tools* used which are: *Trojan horse*- Malicious programs or legitimate software which is used to set up a backdoor in a system from which criminal can gain access. *Virus*- A self-replicating program which spreads itself into other executable code or documents is called a virus. *Worm* –it is also a virus but the difference between a virus and a worm is that a worm does not attach itself to other code.

***Vulnerability scanner* –** It is a tool that is used by hackers and intruders to check computers quickly on a given network for known vulnerabilities. *Sniffer* – In transit, either within the computer or over the network, captures password and other confidential data. *Exploit* – This is an application that takes advantage and exploit known weakness. *Root kit* – It hides the fact that a computer's security has been compromised after hacking. [17]
***Wireless Spoofing* By** filling selected fields that contain addresses or identifiers with legitimate looking but non-existent values, or with values which belong to others, the attacker constructs frames. Through sniffing, the attacker would collect these legitimate values.

MAC Address Spoofing
The attacker usually wants to be hidden. The activity injects that frames which are observable by system

administrators is probing. The attacker will fill the Sender MAC Address field of the injected frames with a spoofed value so that his equipment would not be identified.

At the time of manufacture, MAC address has to be assigned. But setting the MAC address of a wireless card or AP to an arbitrary chosen value would be a simple matter of invoking an appropriate software tool which engages in a dialog with the user and accepts values. However, the MAC address has to be changed by the attacker programmatically and sends several frames with that address, and repeats this with another MAC address. In certain attacks, the attacker needs to have a large number of MAC addresses than the attacker could collect by sniffing. By selecting an IEEE-assigned three bytes appended with an additional three random bytes, the attacker generates a random MAC address.

IP spoofing

IP spoofing can be defined as the process of replacing the true IP address of the sender with that of different address. A spoofer has to circumvent the IP layer and talk directly to the raw network device, because the IP layer of the OS normally adds these IP addresses to a data packet.

B. Wireless Network Probing

Artificially constructed packets has to be send by the attacker to a target that trigger useful responses which is called as probing or active scanning. To trap the attacker, a honey pot target can be carefully constructed.

Trojan AP

A stronger signal could be received by targeted station by setting up an AP by an attacker. The attacker could have already cracked it, if WEP is enabled. Because of the stronger signal, a legitimate user can select the Trojan AP. For later analysis of the IP traffic, the Trojan AP is connected to a system. Stealing the user's password, network access, compromise the user's system to give himself root access by the attacker. This attack is also known as the Evil Twin Attack. HostAP is an example for a general purpose PC with a wireless card could be turned into a capable AP.

C. Denial of Service

When a system would not provide services to authorized clients because of some resource exhaustion by unauthorized clients an attack can occur which is called A Denial of Service (DOS). Against an individual station, this attack can enable session hijacking. Another underlying technique is called sniffing which is used in tools that would scan the health of a network. Sniffing in wireless networks is easier than in wired ones.

Flooding with Associations:

AP maintains a table in its memory which is called as an association table that would insert the data supplied by the station in the Association Request. An attacker would authenticate several non-existing stations using legitimate-looking by having cracked WEP. To make the association table overflow, the attacker would send a flood of spoofed associate requests which can be prevented by enabling MAC filtering in the AP.

Forged Dissociation:

A spoofed Disassociation frame where the source MAC address would set to that of the AP which would be sent by an attacker. The station can resume sending data, when AP send a Re-association response accepting the station. The attacker can continue to send Disassociation frames for some desired period to prevent Re-association.

Forged De-authentication:

The attacker would send a spoofed De-authentication frame where the source MAC address has to be spoofed to that of the AP when a data or Association Response frame is observed. To prevent a reconnection, the attacker would continue to send De-authentication frames for a desired period. The mischievous packets of Disassociation and De-authentication has to be sent directly to the client.

D. Man-in-the-Middle Attacks

The situation where an attacker on host X Inserts X between all communications between host B and host C, and neither B nor C would be aware of the presence of X is called as a Man-in-the-Middle. All the messages which are sent by B do reach C but via X, and vice versa.

Wireless MITM:

Assume that station B has been authenticated with C, a legitimate AP. Attacker X be a laptop with two wireless cards. Through one card, he can present X as an AP. Attacker X would send De-authentication frames to B by using the C's MAC address as the source, and the BSSID he has collected. B would get de-authenticated and would start a scan for an AP and can find X on a channel different from C. There would be a race condition between X and C. If B is associated with X, the MITM attack would be succeeded. X will re-transmit the frames it receives from B to C, and the frames it receives from C to B after some suitable modifications.

Airjack, the package of tools which includes a program called as monkey_jack which automates the MITM attack.

ARP Poisoning:

To determine the MAC address of a device whose IP address is already known, ARP is used. With a help of table look-up, the translation is performed which is applicable to all hosts in a subnet.

Session Hijacking:

When an attacker causes the user to lose his connection, and the attacker assumes his identity and privileges for a period, hijack is said to occur. Temporarily the user's system is disabled and the attacker then takes the identity of the user by which the attacker has all the access that the user has. Once he is done, the attacker stops the DoS attack, and the user resume. This can be achieved by using forged Disassociation DoS attack.

War Driving:

The war driving refers to equipped with wireless devices and related tools, and driving around in a vehicle or parking at interesting places. War-drivers define war driving as "The benign act of locating and logging wireless access points while in motion."

War chalking:

The practice of marking walls and sidewalks with some special symbols to indicate that wireless access is nearby so that others do not need to go through the trouble of the same discovery is called as war chalking. [18]

IV. REAL TIME WIFI HACKING

An automated hacking tool which minimizes the user inputs by scanning and using Python for automation techniques is called WiFite. WEP, WPA/2 and WPS can be hacked by WiFite. Enabling monitor(mon) mode, Cracking the key, capturing a handshake, validating a handshake, scanning air, Analyzing the output and captured packets etc are done by WiFite. It uses tools like aircrack-ng, Tshark, Cowpatty and reaver for various purposes in the background. [19].

Hack WEP encrypted WiFi Password – using wifite?

Wifite on Kali Linux should be started with any recommended Wifi adapter. All the nearby wifi networks visible and their encryption level along with WiFi name and signal strength. Is shown in WiFite with a number assigned to each of them. The appropriate target NUM (1,2,3,n) is to be chosen to select a network. It is recommended to choose a network which has active clients in it. For an attack to be completed, it won't take more than 10 minutes. It will attack the network with different attacks each and every 10 minutes. WEP WiFi password is nothing but the WEP Key in a Hexadecimal representation. The WEP Key is the actual WiFi password. [20]

Hack WPA/WPA2 encrypted WiFi Password using aircrack? **:** The WPA/WPA2 target must be chosen and should wait. As mentioned earlier it might take few minutes to *Never* to crack the password depending on the strength of WiFi password. The stronger is the password, the difficult and time consuming will be the hacking process.

A file that is usually captured when a router and client communicates with each other during authentication process is called Handshake. Password in encrypted form is present in Handshake file. Brute force technique is used to match the password contained in the handshake file. After handshake is captured, Brute-forcing is done offline. A text file that usually contains all known words and common passwords from different dictionaries and other sources is called dictionary file. Dictionaries usually contain few thousands to billions of passwords. A password dictionary file may contain all possible worlds created using combination of different character and number in a file which is very huge and needs lot of computational power. rockyou.txt, darkcode.lst or crackstation are some of the popular dictionaries-password files which are available online.[20] Aircrack is used for dictionary attacks after handshake capture root@kali: aircrack -ng -w /root/DICTIONARY/rockyou.txt < TEST_C0-B0-CB-03-4C-A8.cap > The above command will crack the saved handshake (TEST_C0-B0-CB-03-4C-A8.cap) by using a password file (rockyou.txt) which exists at /root/DICTIONARY/.

Build a Secure Wifi Network Enable MAC Filtering : The easiest way to keep intruders off the wireless network although the least secure is this method. A MAC Address Whitelist or Blacklist should be enabled and then only the MAC Addresses that is specifically put into this list will be able to use or denied access respectively. *Enable Encryption:* It keeps intruders off the network and it also keeps off eavesdroppers from listening to your network traffic. Encryption is very important in a wireless netowork. a) WEP – It is the most common type of encryption on wireless routers. This can easily be broken by experienced hackers in just about 2 minutes, but this will keep out most passerby's and neighbors.(Basic security) b) WPA2 –WPA2 is much more secure than WEP and has not been cracked yet. Deciding between WPA2, WEP, or MAC Filtering is difficult. **WPA2 Encryption used alongside with MAC filtering feature is the most secure method for keeping hackers off the network. (Advanced Security)**

Use a strong Password *:* The password which is long enough and consists of Alphabets both uppercase and lowercase , Special Characters and Numbers are difficult to hack using Dictionary Attacks, only High end brute forcing will be able to hack the password.

Disable SSID Broadcasting*:* This feature is used to decide whether wireless signal is visible or not. This is not recommended because though this keeps the network

invisible to the common offenders, it will not protect the network from any serious hackers. [21]

Realization of RADIUS in WLAN (Enterprise level security):

A RADIUS protocol as a back-end server authentication protocol can choose and be recommended by IEEE802.1x. Combination of IEEE802.1x and RADIUS, IEEE802.1x Authenticator can serve as a RADIUS client, which can send the billing information and connection request to the RADIUS server. The connection request is accepted or rejected depending on the server processes. If permitted, then the client gets the authentication, and a unique key for the session is generated. The server sends the session key of authenticator. RADIUS which is the back-end server protocol for authentication of IEEE802.1x encapsulates most of the useful information for expansion and application easily. [23]

Location of the Access Points

Topologically, Access Points(AP) should be located outside the perimeter firewalls. The control of the radio-coverage volume should be maintained by corporation or home with the use of directional antennae [18] *Personal Firewall:* A personal firewall on the laptops or desktops , not only helps prevent others accessing vulnerable devices at nearby hotspots but also on some other parts of the Internet as a part of a broad defense against hackers. [24]

Secure Protocols

For later analysis, by radio-silent sniffing, the attacker can capture TCP/IP packets if the WEP is disabled, or after the WEP is cracked. Generally, one should use end-to-end encryption at the application level. [18]

Wireless IDS

A wireless intrusion detection system (WIDS) is a self-contained computer system with specialized hardware and software to detect any anomalous behavior. To rogue clients and APs can be located by including GPS equipment. Its computing engine is so powerful that it can dissect frames and WEP decrypt into IP and TCP components. Since the attacker will not be able to control the firmware of the wireless card, a WIDS can also detect a listed spoofed MAC addresses to insert the suitable sequence numbers into the frame.[18] *Virtual private networks*

A VPN provides better security for a large enterprise, especially an IT corporate by pre installing VPN clients on all the employees' laptops and workstations. The network is secured by end to end connections of the clients to the VPN server on the main company network.[24] *Wireless Auditing*

Every wireless network should be security audited periodically. The main goal of an audit is to verify that there are no violations of the security policy. [18] *Results and Observations :* Table 1, shows the different encryptions of WiFi networks and the time taken by the mentioned software to hack them according to the security severity levels.

Encryption type	Mac Address filtering	Security level	Hacking Software used	Hacking technique used	Time Taken
Open	No	Novice	-	-	0s
Open	Yes	Basic	Mac Spoofing Softwares like *Technitium*	Mac Address Spoofing	1Min
WEP	No	Basic	Wifite	Bruteforce(automatic)	2 -10 Min
WPA	No	Medium	Aircrack	Brute Forcing through known lists	A Few Hours - Few days
WPA2/ PSK	No	Advanced	Aircrack, Airodump,Airplay,Airmon.	Brute Force and Social Engineering	A Few Hours - Few Days
WPA2/ PSK	Yes	High	Aircrack, Airodump,Airplay,Airmon. Technitium	Brute Force and Mac Address Spoofing	A Few Days-Months
WPA2/ WPS	No	Basic	Wifite	Brute Force	A Few mins

Table 1: Results and Observations

V. CONCLUSION

Wi-Fi, a wireless network is vulnerable to the threats of Hacking and is the most spread technology over the world. This paper is a brief study on the wireless networks attacking techniques. Wireless networks will still remain highly insecure since an attacker can sniff and hack without gaining any physical access. A real time example on how a password protected WiFi can be hacked is shown in this paper. This paper has also described several current tools that implement attacking techniques and can be used for auditing which exploits the protocol design weaknesses. This work has pointed out several best practices of using the features of router and encryptions that can mitigate the insecurities to a certain extent. The future work of this paper would be to introduce a better security oriented wireless technology or a better encryption level when compared to the current techniques.

REFERENCES

[1] 2010 2nd International Conference on Education Technology and Computer (ICETC). Wireless Hacking - A WiFi Hack by Cracking WEP. S Vinjosh Reddy, K SaiRamani, K Rijutha, Sk Mohammad Ali, CR. Pradeep Reddy

[2] Performance evaluation of the security in wireless local area networks (WiFi). Nada CHENDEB, Bachar El HASSAN and Hossam AFIFI

[3] Security Enhanced IEEE 802.1x Authentication Method for WLAN Mobile Router. Keun Young Park, Yong Soo Kim, Juho Kim

[4] 2009 International Conference on Signal Processing Systems, Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA), ARASH HABIBI LASHKARI, MASOOD MANSOORI, AMIR SEYED DANESH

[5] 2011 Panhellenic Conference on Informatics. Real-life paradigms of wireless network security attacks, I. P. Mavridis, A.-I. E. Androulakis, A. B. Halkias, Ph. Mylonas

[6] https://en.m.wikipedia.org/wiki/Router_(computing)- Router (computing)

[7]http://searchmobilecomputing.techtarget.com/definition/wireless-router- Wireless Router

[8] https://en.m.wikipedia.org/wiki/IEEE_802.11 - IEEE 802.11

[9] http://whatismyipaddress.com/ppp-pppoe - What is PPP and PPPoE?

[10]http://searchwindevelopment.techtarget.com/definition/static-IP-address-dynamic-IP-address-static IP address/dynamic IP addres

[11]http://cecs.wright.edu/~pmateti/InternetSecurity/Lectures/WirelessHacks/Mateti-WirelessHacks.htm-Hacking Techniques in Wireless Networks

[12] https://www.techopedia.com/definition/18091/brute-force-attack - Brute Force Attack

[13] http://smallbusiness.chron.com/difference-between-hardware-firewall-software-firewall-65471.html -The Difference Between a Hardware Firewall and a Software Firewall

[14] http://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/ - HTG Explains: The Difference Between WEP, WPA, and WPA2 Wireless Encryption (and Why It Matters)

[15] http://www.howtogeek.com/204458/why-you-shouldn%E2%80%99t-use-mac-address-filtering-on-your-wi-fi-router/ -Why You Shouldn't Use MAC Address Filtering On Your Wi-Fi Router

[16] https://en.m.wikipedia.org/wiki/Blacklist_(computing) - Blacklist (computing)

[17] International Journal of Advanced Research in Computer Science and Software Engineering, Ethical Hacking: A Security Technique, Sonal Beniwal, Sneha

[18] Hacking Techniques in Wireless Networks, Prabhaker Mateti, Department of Computer Science and Engineering, Wright State University, Dayton, Ohio 45435-0001

[19] http://www.rootsh3ll.com/2015/10/rwsps-automated-wifi-wep-wpa2-wps-cracking-ch4/ -RWSPS: Automated WiFi Cracking [ch4]

[20] http://himanshunegi.in/hack-wifi-password-wifite/ - How to Hack WiFi Password? Cracking WEP, WPA/WPA2, WPS with Wifite!

[21]http://www.whoisonmywifi.com/How_To_Make_A_Wireless_Network_Secure.pdf - How to Make a Wireless Network Secure

[22] Hacking Techniques in Wireless Networks, Prabhaker Mateti, Department of Computer Science and Engineering, Wright State University, Dayton, Ohio

[23] 2010 International Conference on Computer Application and System Modeling (ICCASM 2010) WLAN Security System based on the 802.1 and AES, Dushuqin, Qin Yi

[24] Securing Wi-Fi Networks, Kjell J. Hole, Erlend Dyrnes, Per Thorsheim