International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-6, March 2020

Penetration Testing on WPA2

R.Sam Jasper, P.P Amritha, M. Sethumadhavan

Abstract*: The WLAN devices are used nowadays in many universities, commercial buildings, and organisations which were developed by Wi-Fi alliance to provide interoperability, security and ease of use of wireless devices connected to everywhere, every time to the internet. The WPA2 standard (IEEE 802.11) defines security mechanisms for wireless networks. This paper describes possible attacks launched on Wireless LAN from pre-connection to gaining access to the system and it represents the effect of these attacks on the WLAN along with some mitigations to prevent the devices from the below-defined attacks.

***Keywords*: WPA2, WLAN Attacks, DOS Attacks, WI-FI Attacks,802.11 MAC Attacks, WPA2 Handshake-Keys.**

I. INTRODUCTION

The WI-FI Routers based on the IEEE 802.11 standards and the WLAN environment had used for more than a decade. The WI-FI Routers present in-home or commercial buildings are prone to wireless attacks such as DOS Attack, MITM Attacks, and other wireless attacks. This Paper Studies the various attacks performed on the WPA2 protected home WI-FI networks and also proposes a framework for the different types of attacks such as a pre-connection attack,post-connection attack, gaining access to the system.

In the Pre-connection attack management frame, forging is done, i.e.,de-authentication attack performed. In the second phase of this framework, gaining access to the network is described by performing a brute force attack and the WPS cracking. In the third phase of the framework, we are performing post connection attacks that could only be possible after entering into the victim's network and also performing MITM attacks such as ARP poisoning and DNS Poisoning. These attacks performed using various tools and techniques using the Penetration testing Operating System Kali Linux.

Manuscript received on February 10, 2020.
Revised Manuscript received on February 20, 2020.
Manuscript published on March 30, 2020.
* Correspondence Author
R Sam Jasper* , TIFAC-CORE in Cyber Security Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India. (E-mail: samjasper@protonmail.com)
PP Amritha , TIFAC-CORE in Cyber Security Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India. (E-mail: pp_amritha@cb.amrita.edu)
M Sethumadhavan , TIFAC-CORE in Cyber Security Amrita School of Engineering, Coimbatore, Amrita Vishwa Vidyapeetham, India. (E-mail: m_sethu@cb.amrita.edu)

II. BACKGROUND

2.1 WPA2 Encryption Scheme

The WPA2 standard [1] was ratified by the IEEE in 2004 as 802.11i.[3] Like its predecessor, WPA2 offers the end-user enterprise, personal modes. The enterprise mode is used to protect the enterprise network which is authenticated by a radius server and the personal mode used in non-commercial buildings such as home, public mall etc. which offers various encryption modes such as TKIP (temporal key integrity protocol) and AES (Advanced Encryption Standard) by using these encryption modes the network stands to be protected. The WPA2 networks still have vulnerabilities, and it is considered the most secure wireless security standard that was available. The AES uses three symmetric block ciphers. Each uses 128-bit length keys to encrypts and decrypts data using different key length 128, 192 and 256-bit keys. These kinds of encryption ensure the confidentiality, integrity and availability of the network. WPA2 also the user to move from one Access Point to the other Access Point on the same network without having to be re-authenticated by simply extending the network by using the repeaters which is have to be pre-configured with the existing router which uses the same encryption and the passphrase for the authentication phase. The authentication did by using the PMK key (Pairwise Master Key) caching or authentication.

2.2 The Keys used in Four-way Handshake

The process of exchange of four messages between an AP (authenticator) and the client device (supplicant) to generate some encryption keys which used to encrypt real data sent over Wireless channel. The following keys are discussed below

- MSK (Master Session Key)
- PMK (Pairwise Master Key)
- GMK (Group Master Key)
- PTK (Pairwise Transit Key)
- GTK (Group Temporal Key)
- ANonce
- SNonce
- MIC

The various key is described below which are generated during the four-way handshake and also other variables that are needed to generate these keys.

A.PTK (Pairwise Transit Key): Pairwise transit key [1] used to encrypt all unicast traffic between a client and an AP. PTK is unique between every client and an AP. To generate PTK, the following information is required

PTK = PesudoRandomFunction (PMK + Anonce + SNonce + Mac (AA)+ Mac (SA))

Anonce(AP nonce) is a random number generated by an access point (authenticator)

Snonce (Supplicant nonce) a random number generated by the supplicant device. MAC addresses of a supplicant device and MAC address of authenticator. A pseudo-random function (PRF)which is applied to inputs. PTK is dependent on PMK (pairwise master key) which discussed below.

B.GTK (Group Temporal Key): This key is used to encrypt all broadcast and multicast traffic between an AP and multiple supplicant devices. GTK is shared between all supplicant devices associated with one AP. For every AP, there will be a different GTK which will be divided between its associated devices. GTK depends on another high-level key GMK (group master key) discussed below.

C.PMK (Pairwise Master Key):

PMK used to create the PTK that is derived using the following input.

PTK = PRF (PMK + Anonce + SNonce + Mac (AA)+ Mac (SA))

Pairwise master is key generated from the master session key (MSK).

D.GMK (Group Master Key): The Group master key is used to create Group Temporal Key discussed above. GTK is generated on every access point and shared with the devices connected to this AP.

E.MSK (Master Session Key): The master session is the first key which is derived from PSK authentication. We discussed above keys from bottom to top and how keys are dependent on other essential keys. The 1st level key is generating the MSK during the successful Pre-shared key (PSK) authentication. The 2nd level key that is generated from MSK is the PMK and GMK. PMK is used to create a Pairwise transient key (PTK), and Group master key (GMK) is used to create group temporal key (GTK). The 3rd level keys are the actual keys used for data encryption.

2.3 Frame Encryption

We have our plain-text data to encrypt, now we take the session key(PTK)[2] and combine it with the packet number(nonce) which is incremented by 1, the session key is mixed with unique packet number and end up with the unique per-packet key, and this unique per-packet key is used to encrypt the data frames, and it uses stream cipher to generate the keystream that is XORed with the plain text (PT) that will derive the cipher text (CT). The following point is considered during encryption

• Nonce reuse implies keystream reuse in all WPA2 ciphers.

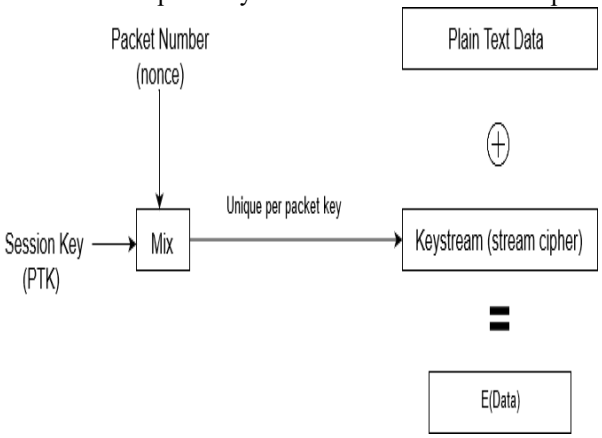

Figure 1 Frame Encryption

2.4 Nine-services of Wireless LAN

The nine services of WLAN defined in 802.11

Table 1: IEEE 802.11 Services

Service	Provider	Supported for
Association	Distribution system	MSDU delivery
Authentication	Station	LAN access and security
Deauthentication	Station	LAN access and security
Dissassociation	Distribution system	MSDU delivery
Distribution	Distribution system	MSDU delivery
Integration	Distribution system	MSDU delivery
MSDU delivery	Station	MSDU delivery
Privacy	Station	LAN access and security
Reassociation	Distribution system	MSDU delivery

The service provider can be the Distribution system (AP). Station services implemented in every 802.11 stations, including AP stations. Distribution services provided between Basic Service Set(BSS).These Services implemented in DS or other devices attached to the DS. These services used to control IEEE 802.11 LAN access and confidentiality.

2.5 IEEE 802.11 MAC Frame Format

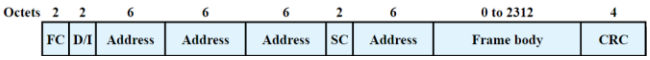

Figure 2 802.11 MAC Format

Figure 2 shows the 802.11 frame format [5].

This general format used for all data and control frames, but not all fields used in all contexts. The fields are as follows:

Frame Control: It represents frame type (control, management, data) which are 2 bytes long.

Duration /Connection ID: This is a 4-byte long that represents the time (ms), and if connection ID is used, it will have an association or connection identifier.

Address 1-4: This is a 6-byte long , which contains physical address of system(48 bit each).

Sequence Control: It has two sub-fields of 16 bytes long containing fragmentation (4 bit) and sequence number (12 bit) used to number frames between a sender and receiver.

Frame Body: This is a variable-length area, containing information of individual frames that are explicitly transferred from a sender to the receivers.

CRC: To ensure an error free frame and it is 4-byte long .

III. PROPOSED FRAMEWORK

3.1 Scope of the System:

The Proposed System has three different phases and shows how intruder gain access to the network and also shows the way to find the identify that attack and prevent it.

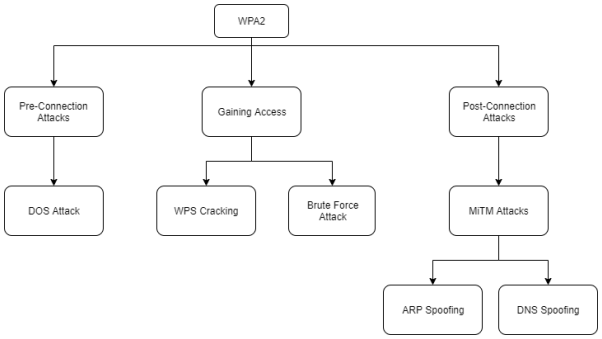

Figure 3 Proposed Architecture

3.1.1 Pre-Connection Attacks

The pre-connection attack is the first phase of network penetration testing. To performing this attack, the attacker or the pentester will scan for the beacon signals around his station by using the wireless adapters which are put on the monitor mode to scan for the available access points. This attack is basically performs deauthentication by removing the end-user that connected to the AP without knowing the Passphrase of the network.

DOS Attack: In wireless networks, management frames are essential to provide and maintain connectivity. When the client comes in the range of AP (access point), then it first sends the association request to the AP to ask to be associated then AP responds with proper acknowledgement or it denies the request. Similarly, authentication request frame is sent, and deauthentication frame also launched from the client and replied by the AP and for sending a frame, there is no restriction so an attacker can also send the Multiple frame and this way the attack is generated. Now, these management frames are responsible for DOS attacks [8] on WLAN. The wireless security protocol uses various encryption algorithms but cannot have control over management frames so threats are still available. Strongest WLAN protocol WPA2 [4] uses the AES (Advanced Encryption Standard) Algorithm [5]. Now we discuss most common DoS attacks [6] on IEEE 802.11 wireless network as Deauth Frames:

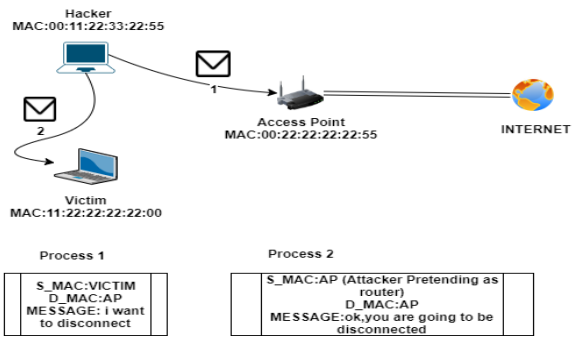

Figure 4 Deauthentication Process

Deauthentication frames [6,9,10] are continuously sent by an intruder to its victim as shown in figure 4. These types of frames are the notification frames that are sent by the AP, which can't be ignored by the receiver or the client device. The attacker sends a large number of frames continuously to the client device (victim device) which makes the victim's buffer full with these type of request frames so it consumes victim's all the resources to process DeauthFrames and waste time correspondingly to this, victim cannot process other requests or notifications coming from the other clients or AP because victim buffer is full with the intruder's deauthFrames so for this amount of time client is disconnected to the other devices.

The Linux command is given below for two scenario's

• To deauthenticate all clients

aireplay-ng --deauth [no of pkts] -a [AP] [INTERFACE]

• To deauthenticate Specific Client

aireplay-ng --deauth [number of deauth pkts] -a [AP] -c [target] [interface]

If intruder wants to make this attack worse, then intruder will make an attack on the access point (AP) because in this case all legitimate users will be disconnected from the whole networks which are already connected with the same AP.

3.1.2 Gaining Access

It is the second part of the network penetration testing framework. In this phase, we will connect to the network. This way the pentester gain access to the system and allow the pentester to launch even more powerful attacks and get more information. If a network said to be open we can simply connect to it but if it has encryption, the pentester should break the authentication by performing some brute force technique or if it is WPS enabled the WPS-Pin can found using the tool like reaver.

WPS Cracking:

The Wi-Fi protected setup (WPS) is a wireless network security standard that attempts to establish a fast connection between a router and client devices. The WPS-PIN is an 8-digit numeric code which is provided by the AP. The Reaver tool Preforms a brute-force attack on the AP by attempting every possible combination to guess the 8-digit pin. Since the PINs are numeric, it is easy for the reaver to crack as it would have only 108 Combinations, i.e. possible values for any given PIN, considering 00,000,000 is not the key.

Stages involved in Reaver:

1. Put WIFI Adaptor in monitor Mode
2. Scanning the Air for WPS network using the following command

wash -i interface[monitor mode]

Example: wash -i mon0

3.Reaver Command:

reaver -i [interface monitor mode] -c [target's channel] -b [target's bssid] -[verbose]

Example: reaver -i mon0 -c 6 -b 00:23:69:48:33:95 –vv

Brute-Force Attack

It is the method of breaking the password-protected device using n- number of possible combinations of passwords contained in a file.

The aircrack suite takes wordlist as input along with the captured .pcap file. The handshake will have the following parameters such as STA address, AP nonce, STA nonce, EAPOL, Payload and MIC.

The aircrack generates and check the MIC for each password in wordlist and matches with the one in the handshake if a match is found it says "password found".

The Following Process are required to perform a brute-force attack

Use airodump-ng suite to capture the handshake file Linux Command:

airodump-ng –bssid (target) –channel (target) –write (store captured pcap file) interface (interface in monitor)
Generate a wordlist using the crunch tool Linux Command:
Crunch [min] [max] [characters] –t [pattern of password] –o [output file]
Use aircrack-ng suite against the wordlist Linux Command:
aircrack-ng [.cap file] -w[wordlist]

3.1.3 Post-Connection Attacks

In this section, we discuss the post connection attack, that means the attacks that we can do after connecting to the network. Now, it doesn't matter that the network is a wireless or a wired network and it doesn't matter that the target was using the WPA or WPA2, we can launch all of the attacks that we're going to talk about in this section. In all the previous attacks, we kept our wireless card in monitor mode, so that we could capture any packet that goes in the air. In this section, we're going to use our wireless card in the managed mode because we have access to the network, so we don't need to capture everything, we only want to capture packets that are directed to us.

MITM ATTACKS: This is the most dangerous attacks that we can carry out on any network. We can only perform this attack once we have connected to the network. This attack redirects the packets from any client to the attacker device. This means that any packet that is sent to or from the clients will have to go through the attacker's machine. Now, we will know the password and key to the network, so we will be able to read those packets, modify them, drop them. This attack is so effective and so powerful because it's tough to protect against it. This is due to the way that the ARP protocol works.

ARP Poisoning Attack:

ARP Poisoning [7] is one of a kind, in which sends fake ARP message sent over a local network with malicious intent. This would link the Intruder's MAC address to a valid IP address in the system. Once the physical address of the attacker's machine connected to a trusted IP address on the network, the Intruder will start sniffing the data on the network. This attack can also prevent transit data from being intercepted, modified, or stop the data transit. This attack can be implemented only on LAN environment that use the Address Resolution Protocol.

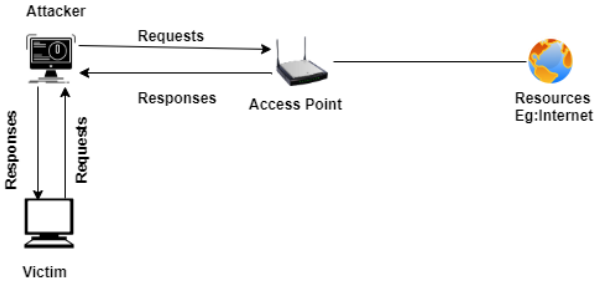

Figure 5 ARP Poisoning

Implications of ARP Poisoning: The consequences of the ARP poisoning attacks could have severe consequences for organisations. In the most basic use, ARP poisoning attacks used to steal sensitive information. In addition, ARP poisoning attacks are often used to facilitate other attacks:

1. Denial of service attack: DOS attacks often use ARP poisoning to connect multiple IP addresses to a target's physical address. As a result, the proposed transport destination for various Internet protocol addresses will be diverted to the targets physical address, and the target can be loaded by traffic.
2. Session or Cookie hijacking: Session hijack or cookie hijack would be possible for the intruder to steal current session ID's, allowing the intruder to gain access personal information and confidential data.
3. MITM attacks: MITM attacks can use of ARP poisoning to intercept and change the data traffic among the legitimate users.

DNS Spoofing

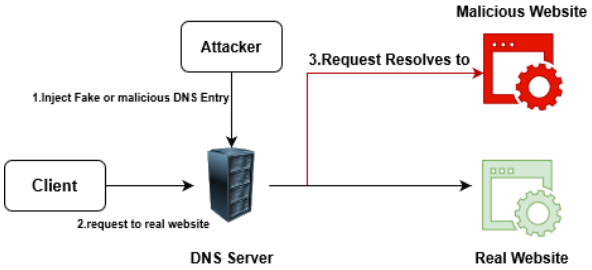

Figure 6 DNS Poisoning Architecture

The Figure 6 shows the Domain Name Server (DNS) spoofing or DNS cache poisoning [8]. This type of attack that exploits vulnerabilities in the DNS to redirect Internet traffic away from legitimate servers and towards the malicious website which is not intended by the user and the mitigations are discussed in [11].

IV. EXPERIMENT RESULTS

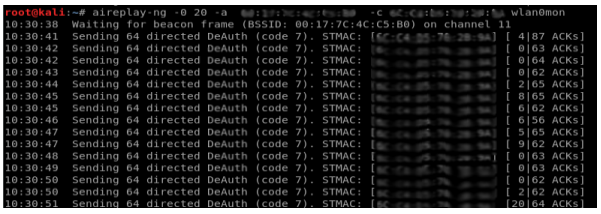

Figure 7 DEAUTH STA

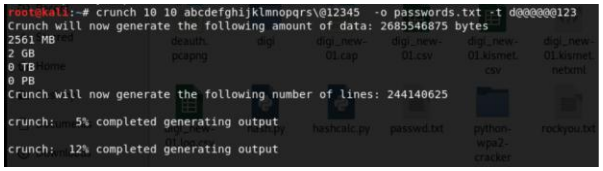

Figure 8 Generating Wordlist

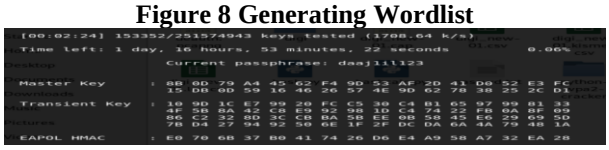

Figure 9 Cracking the WPA2 Passphrase

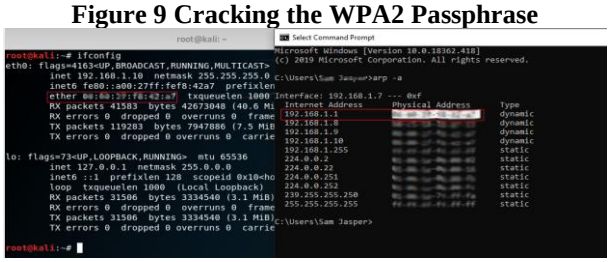

Figure 10 Successful ARP Poisoning

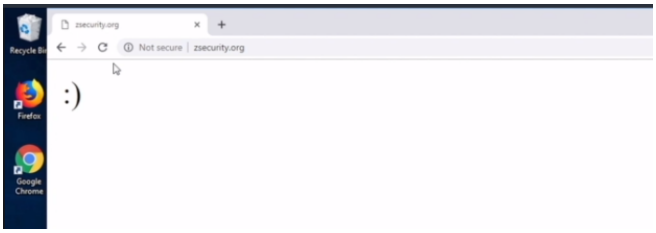

Figure 11Successful DNS Poisoning

V. CONCLUSION AND FUTURE WORK

We proposed several advanced attacks against the wireless network and also demonstrated how to gain access to the network and performed Possible MITM attacks on the network. These varieties of approaches show that wireless LAN environment is still vulnerable to many attacks which will lead to data theft, loss of money, and can even compromise the whole network. Thus make a countermeasure against these attacks on timely manner will protect the individual or the entire network from future cyber attacks. As a future work conduct a security assessment on the WPA3 and perform various attacks against the network to see if the WLAN devices are protected against the variants of DOS attacks.So that the up-time of the network is guaranteed and users can have reliable network service.

REFERENCES

1. S. A. Visan, “WPA/WPA2 password security testing using graphics processing units,” Journal of Mobile, Embedded and Distributed Systems, vol. 5, no. 4, pp. 167–174, 2013.
2. M. Vanhoef and F. Piessens, “Key reinstallation attacks: Forcing nonce reuse in wpa2,” in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security, pp. 1313–1328, ACM, 2017.
3. “IEEE std 802.11ai. 2016. amendment 1: Fast initial link setup,”
4. A. Tsitroulis, D. Lampoudis, and E. Tsekleves, “Exposing wpa2 security protocol vulnerabilities,” International Journal of Information and Computer Security, vol. 6, pp. 93–107, 03 2014.
5. W. STALLINGS, “Data and computer comunications,” 2014.
6. A. Gupta and M. Garg, “Dos attacks on ieee 802.11 wireless networks and its proposed solutions,” Available at SSRN 1645757, 2010.
7. VERACODE, “ARP Spoofing.” https://www.veracode.com/security/ arp-poisoning. imperva, “DNSSEC.” https://www.imperva.com/learn/application-security/ dnssec/.
8. C. Liu and J. Yu, “Review and analysis of wireless lan security attacks and solutions,” Journal of International Engineering Consortium, vol. 59, pp. 539–554, 2006.
9. C. Liu and T. Y. James, “An analysis of dos attacks on wireless lan.,” in Wireless and Optical Communications, 2006.
10. Kumar, A. Aswin, Ashok Kumar Mohan, and P. P. Amritha. "Deceiving attackers in wireless local area networks using decoys." Journal of Cyber Security and Mobility 7.1 (2018): 201-214.