

De-Authentication attack on wireless network 802.11i using Kali Linux

Deep Joshi¹, Dr. Ved Vyas Dwivedi², K.M.Pattani³

¹P.G.Student, Dept. of E&C, C U Shah College of Engg & Tech, Wadhwan, Gujarat, India

²Director/Pro Vice Chancellor, C. U. Shah University, Wadwan City, Gujarat, India

³Asst. Professor, Dept. of E&C, C U Shah College of Engg & Tech, Wadhwan, Gujarat, India

Abstract – De-Authentication attack on wireless network 802.11i with WEP(Wired Equivalent Privacy),WPA(Wi-Fi Protected Access) and WPA2(Wi-Fi Protected Access 2) security standards or open public access resources to exploit poor management frame structure using kali linux 2016.2 rolling OS. In this work the author demonstrate practical implementation of De-Authentication attack on wireless network 802.11i using several tools in kali linux 2016.2 OS and also reveals truth that someone without provide him/her legitimacy to resources ,attempt De-Authentication attack to disturb communication between Wi-Fi access point and client.

Key Words: De-authentication, Access Points, DoS, Wireless Security, 802.11i, Flooding attacks, Penetration testing, Kali Linux.

1. INTRODUCTION

Wireless local area network (WLAN) has change the way Internet is used in the world today. Wireless technology can be seen in every aspect of human life-Education, Business, Transport, and Communication etc. There has been a great demand for wireless access around the world nowadays; this result in its demand far exceeding the technology thereby resulting in an unsolved security issues. Since the WLAN has been integrated into virtually all devices around; PDA, desktop computers, laptops, notebooks, smart phones, palm tops, and other small devices. The idea of wireless network brings to mind lot of ways of attacking and penetrating a network compared to the traditionally wired network. Because wireless typically extends beyond walls and boundaries, it has become prone to attacks. Wireless technology is deploying around in places like Schools, Office buildings, Airport, Parks, Hotels, coffee shops, etc. An attacker could launch an attack to an unsuspecting client. The security challenge of WLAN makes it necessary to perform a series of penetration test on a WLAN to actualize the dangers posed on using a WLAN by a client.

2. CONCEPT OF DE-AUTHENTICATION ATTACK

The attack can be made by a penetration tester on a company’s wireless network, if the company or organization wishes to check the robustness of its own wireless security. The tester then sends a report of the findings to the company.

But some hackers mount such attacks simply to create a nuisance for users.

The connection between the clients and Access Points (APs) has been established by the exchange of various frames as shown in Fig 1. The communication between the client and the AP has been established after probing the available wireless APs. After that the exchange of the series of management frames like authentication and association request frame takes place [5] . Then the AP responds by sending authentication response and association response via the authentication server [2].

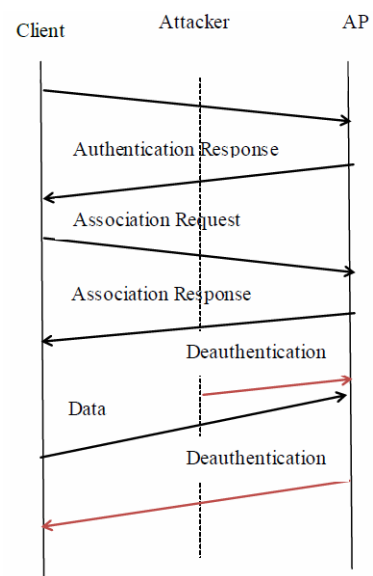


Fig -1: De-authentication attack [3]

As these frames are unprotected and sent in clear. So these frames has been spoofed by the attacker [6]. The attacker then sends de-authentication requests with the client’s address set as the source. Then the AP responds by sending the de-authentication response to the client. Thus the communication between the client and the AP has been halted [4]. As de-authentication requests are notifications, so cannot be ignored and the AP responds instantly to these requests [5]. The attacker can periodically scan all the channels and send these spoofed messages to valid clients thus terminating their connection [7].

3. IMPLEMENTATION OF DE-AUTHENTICATION ATTACK

3.1 Testing network card for wireless sniffing

All network cards do not supports wireless sniffing, we will show how to carry out an injection test to determine if a network card supports packet injection and sniffing, Injection test also determines the ping response time to the access point. When the test is performed, it lists all the access point available in the area which responds to broadcast probes. Next it performs a 30 packets test for each discovered access point to indicate the connection quality. These connection qualities show the ability of the network card to successfully send and receive response to the packets it sent. Injection test can be used to test a specific access point by specifying the name and MAC address of the access point. The test initially sends out broadcast probe requests, these are probe requests that ask any access point listening to respond with a description of itself. A list of responding access points is assembled and will be used to carry out the next test (30 packet test) for each access point listed. If any access point responds, a message is printed on the screen indicating that the card can successfully inject.

The commands below can be used to perform an injection test

```
ifconfig wlan0 up
airmon-ng start wlan0
iwconfig wlan0 channel 1
iwconfig mon0 channel 1
aireplay-ng --test mon0
```

Note that the wireless card must be put in monitor mode and desired channel before carrying out the test. The closer the wireless card is, to the network the more the success rate of the injection.

3.2 Entering into Monitor mode

Monitor mode refers to an operational mode of wireless hardware that makes any type of valid IEEE 802.11 frames user-accessible. In contrast, a device operating in promiscuous mode accepts frames not destined for the local node as indicated by the receiver address but does not make available management and control frames. Frame injection, i.e., transmission of cooked frames including link layer header, is allowed only in monitor mode [1].

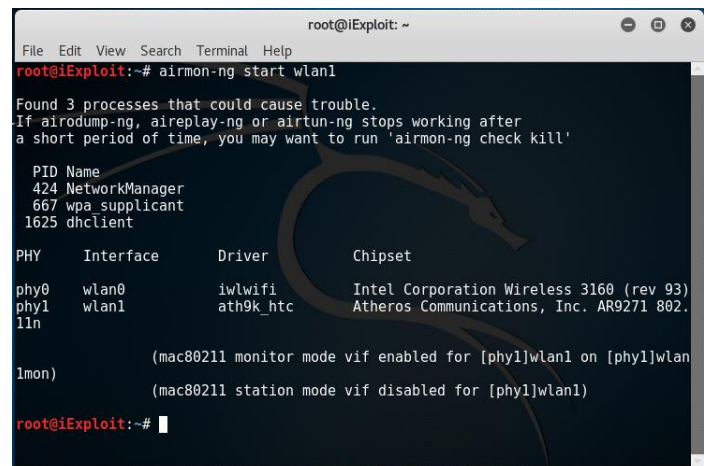
airmon-ng script can be used to enable monitor mode on wireless interfaces [8]. It may also be used to go back from monitor mode to managed mode. Entering the *airmon-ng* command without parameters will show the interfaces status. When putting a card into monitor mode, it will automatically check for interfering processes.

It is strongly recommended that these processes be eliminated prior to using the *aircrack-ng* suite.[8] "*check kill*" will check and kill off processes that might interfere with the

aircrack-ng suite. The command *airmon-ng check kill* stops network managers then kill interfering processes left:

It is very important to kill the network managers before putting a card in monitor mode. As we can see, it created a monitor mode interface called *wlan0mon* and it notified there are a few processes that will interfere with the tools.

The next command *airmon-ng start wlan1* sets our wireless card on monitor mode, which means *wlan1mon* as shown in below Figure.



```
root@iExploit: ~
File Edit View Search Terminal Help
root@iExploit:~# airmon-ng start wlan1
Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

PID Name
424 NetworkManager
667 wpa_supplicant
1625 dnclient

PHY Interface Driver Chipset
phy0 wlan0 iwlwifi Intel Corporation Wireless 3160 (rev 93)
phy1 wlan1 ath9k_htc Atheros Communications, Inc. AR9271 802.11n

(mac80211 monitor mode vif enabled for [phy1]wlan1 on [phy1]wlan1mon)
(mac80211 station mode vif disabled for [phy1]wlan1)
root@iExploit:~#
```

Fig -2: Entering into Monitor mode

3.3 Packet Capturing

airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with *aircrack-ng*. If you have a GPS receiver connected to the computer, *airodump-ng* is capable of logging the coordinates of the found access points. Additionally, *airodump-ng* writes out several files containing the details of all access points and clients seen [8].

After killing interfering processes I typed *airodump-ng wlan1mon* as shown in Figure 3 to find out about all the APs in the vicinity.

In Figure 3, important information like the MAC address, channel number and Extended Service Set Identification (ESSID) of the AP is available. Here Basic Service Set Identification (BSSID) is the MAC address of AP, and STATION means all wireless devices are connected to the AP. Now I choose one victim: AC:38:70:A7:91:B8.

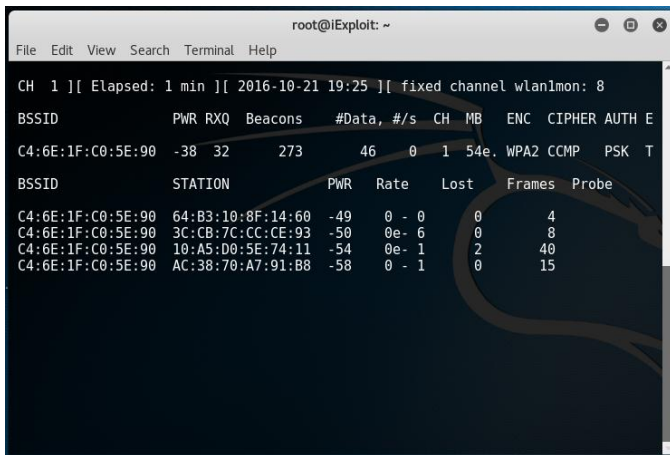


Fig -3: Packet Capturing

3.4 Frame Injecting

aireplay-ng is used to inject frames[8]. The primary function is to generate traffic for the later use in *aircrack-ng* for cracking the WEP and WPA-PSK keys. There are different attacks which can cause de-authentications for the purpose of capturing WPA handshake data, fake authentications, Interactive packet replay, handcrafted ARP request injection and ARP-request reinjection.

The attacks can obtain packets to replay from two sources. The first being a live flow of packets from our wireless card. The second being from a pcap file. Standard Pcap format (Packet CAPture), is recognized by most commercial and open-source traffic capture and analysis tools. Reading from a file is an often overlooked feature of *aireplay-ng*. This allows us to read packets from other capture sessions. Various attacks generate pcap files for easy reuse.

In the attack, I used *aireplay-ng* to send the de-auth packet.

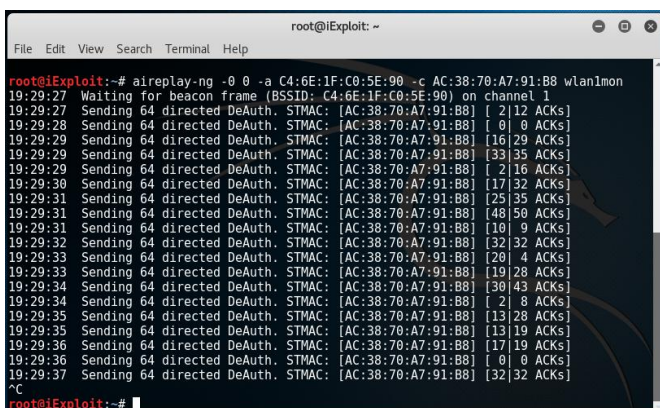


Fig -4: De-authenticate Particular user

Here is a description of this command:

- -0 sends the de-auth packet
0 refers to the number of packets
- -a is the MAC address of the AP
- -c is the MAC address of the client to be de-authenticated.

We also de-authenticate all clients connected to AP as shown in blow figure.

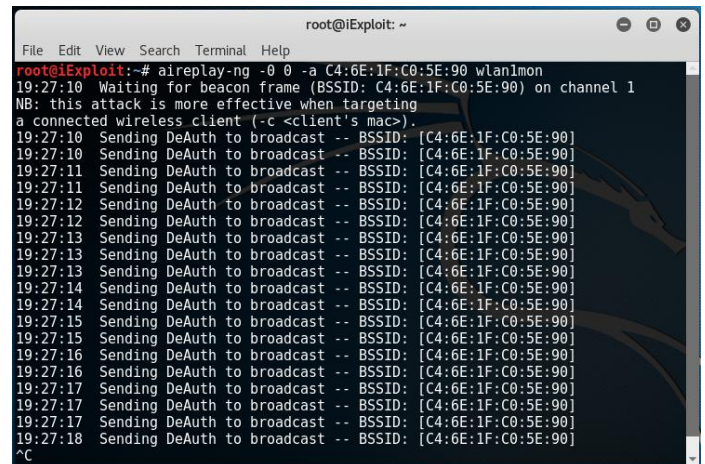


Fig -5: De-authenticate all connected users

So after this, all users connected to AP are de-authenticated and unable to connect the AP during period of De-authentication attack.

4. CONCLUSION

Now a days, set up of Off-The-Shelf network is becoming popular and very easy just like plug and play devices but at the same time hackers community becomes active and try to exploit this type of network and find available loop holes. De-Authentication attack is worked as a window in fully protected system and access point abruptly receive packets without any knowledge of authorized user and becomes busy to de-authenticate authorized user. During the busy time of access point, attacker can established successful WPA handshake and purpose of this type of network might be dangerous so it is necessary to equip our access point with some more advance features and need a faster, more immediate means of threat detection to prevent severe damage resulting in only authorized person can communicate with access point.

REFERENCES

- [1] Stephan M. Günther, Maurice Leclaire, Julius Michaelis and Georg Carle, "Analysis of injection capabilities and media access of IEEE 802.11 hardware in monitor mode", IEEE Network Operations and Management Symposium (NOMS) 2014, IEEE, pp. 1-9, June 2014.
- [2] A. Gerkis and J. Purcell. Sep 2006 A Survey of Wireless Mesh Networking Security Technology and Threats. Sans Infosec Reading Room.
- [3] Rupinder Cheema, Divya Bansal and Dr. Sanjeev Sofat, "Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks", International Journal of Computer Applications, Volume 23- No.7, June 2011.
- [4] E. D Cardenas. MAC Spoofing -An Introduction. <https://www.giac.org/paper/gsec/3199/mac-spoofing-an-introduction/105315>.
- [5] John Bellardo and Stefan Savage, "802.11 Denial of Service Attacks: Real Vulnerabilities and Practical Solutions", 12th USENIX Security Symposium, pp.15-28, August 2003.
- [6] Joshua Wright, "Detecting wireless LAN MAC Address spoofing", GCIH, CCNA, pp 1-5, Jan 21, 2003.
- [7] White papers, "Can Wireless LAN Denial of Service Attacks Be Prevented? Understanding WLAN Vulnerabilities and their Countermeasures"
- [8] Aircrack. <https://www.aircrack-ng.org/>