De-Authentication Attack on Wireless Network

Chintan Kamani, Dhrumil Bhojani, Ravi Bhagyoday, Vivek Parmar, Deepti Dave

ABSTRACT --- These days with convenience of 802.11 networks, the wireless based access networks have had a large boom in the consumer, industrial as well as the military sector. The flaws in the 802.11 protocol have been widely recognized,which has led to rise of malicious Denial of service attacks .In this work the authors will be demonstrating the practical execution of de-authentication attack on wireless network 802.11i using tools such as aireplay-ng and MDK3 in Kali Linux 2018 OS.

Index Terms - De-Authentication, aireplay-ng, MDK3, DOS.

I. INTRODUCTION

Wireless local area networks (WLAN) have changed the way Internet is used in the world today. There days Wireless networks offer great prospective for exploitation for mainly two reasons; they use the airwaves for communication, and wireless-enabled laptops are everywhere. To make the most of their security planning, Organizations need to focus on threats that pose substantial risk. Wireless networks are exposed in innumerable of ways, some of the most likely problems begin from rogue access points (APs) and employees using mobile devices without appropriate security insurance, due to which malicious hacking attempts and denial of service (DOS) attacks are surely possible as well. Wireless technology is situated around in places like Airport, Parks, Hotels, Coffee shops, Schools, Office buildings, etc. An attacker could initiate an attack to an unaware client. The security challenge of WLAN makes it requisite to execute a sequence of penetration test on a WLAN to actualize the threat posed on operation of a WLAN by a client.

II. CONCEPT

A de-authentication attack is a type of attack which targets the data transfer between router and the device, effectively disabling the Wifi card on the device. The de-authentication isn't a exploit of a bug, it's a IEEE 802.11 protocol that is presently being used in real world applications. De-Authentication attacks utilizes the de-authentication frame. This frame is sent from a router to a device forces the device to disconnect. In technical terms it's called: "licensed technique to notify a rogue station that they have been isolated from the network". This suggest that a device is on the network that shouldn't be on the network. The router dispatches a de-authentication frame to the device notifying it that it has been disconnected.

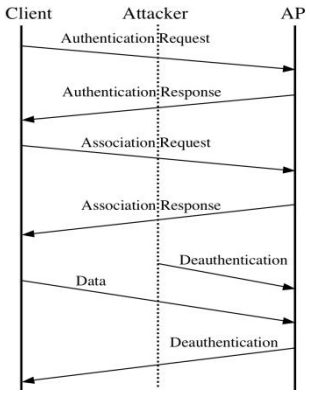


Figure 1. De-Authentication Attack

III. INTRODUCTION TO TOOLS

There are two major tools which are used for de-authentication attack Aireplay-ng and MDK3.

A. Aireplay-ng

Aireplay-ng is an tool which is explicitly used to inject specially created ARP-request packet into an already existing wireless network in order to generate traffic. Its main role is to deauthenticate the already connected users on the wireless network. Aireplay-ng tool is included in the aircrack-ng package

B. MDK3

MDK3 also known as Murder Death Kill 3 is one the most favoured tool to exploit ordinary IEEE 802.11 protocol weakness. It is particularly designed for WLAN environments. The principal operation of this tool is to flush the network with false traffic against the network. Can also be used to perform stress test on 802.11 networks.

IV. IMPLEMENTATION & RESULTS

Demonstration of de-authentication attack using Aireplay-ng and MDK3.

A. Changing mode of wireless adapter

Before getting into monitor mode it is necessary to check the wifi adapter's name. This name will be used at many places in order to perform de-authentication attack. Now in order to find the wifi adapter's name the following command will be used:

Revised Manuscript Received on February 14, 2019.

Chintan Kamani, B.Tech., Ajeenkya DY Patil University, Pune, India.
Dhrumil Bhojani, B.Tech., Ajeenkya DY Patil University, Pune, India.
Ravi Bhagyoday, B.Tech., Ajeenkya DY Patil University, Pune, India.
Vivek Parmar, B.Tech., Ajeenkya DY Patil University, Pune, India.
Deepti Dave, Ajeenkya DY Patil University, Pune, India.

iwconfig

Iwconfig is command which is dedicated to the wireless interface. It is used to config the parameters of the network interface.

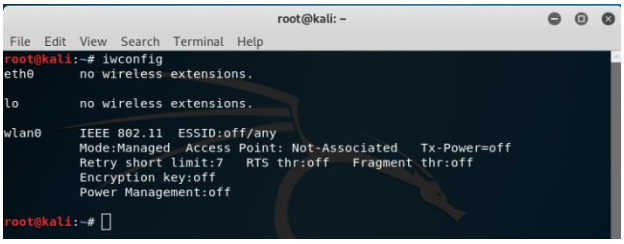


Figure 2. Iwconfig

Monitor mode is also known as RFMON (Radio Frequency Monitor) mode that works by sniffing the packets in the air without linking or associating with an access point. It authorizes a device with an wireless network interface controller to monitor all traffic/packets received from the wireless network.It allows us to capture the traffic without connecting it with an access point. RFMON works only with wireless networks. They require an adapter be placed in monitor mode for tools like Aireplay-ng to work. The commands used to enable the monitor mode:

ifconfig wlan0 down

iwconfig wlan0 mode monitor

ifconfig wlan0 up

ifconfig wlan0 down will temporarily disable the wifi, iwconfig wlan0 mode monitor command will set the wifi adapter to monitor mode, ifconfig wlan0 up will enable the wifi again.

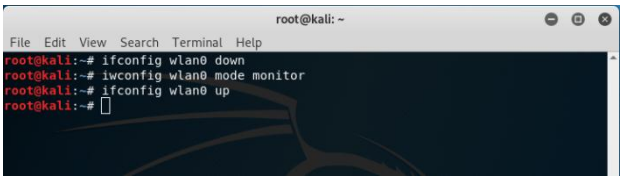


Figure 3. Monitor Mode

B. Kill the process which may interfere

When a card is put into monitor mode,it will involuntarily check for interfering processes . It is strongly proposed that these processes be terminated prior to using aireplay-ng. Because these processes might interfere in the attack and cause an error.

Command used to check the processes which may interfere:

airmon-ng check wlan0

Command used to kill the process which may interfere:

kill <process-id>

After killing the process , to verify use the same command as below:

airmon-ng check wlan0

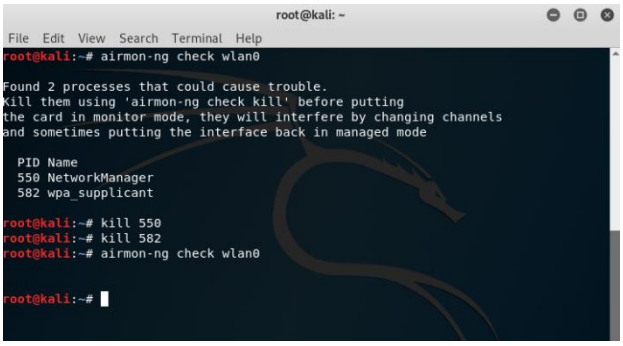


Figure 4. Killing Process

C. Scan network and select target

Scanning the network is done by a packet analysis tool (also known as packet sniffer). Airodump-ng and other packet sniffing tools can be used to scan a network. A packet analyzer intercepts the traffic that passes through a digital network or part of a network. Packet capture is the action of intercepting and logging traffic. As data streams flow over the network, the sniffer records each packet and, if needed, decode the packet's raw data, showing the values of various fields in the packet, and inspect its content according to the appropriate request for command (RFC) or other specifications. The command below can be used to perform the analysis of the network:

airodump-ng wlan0

The command contains the tools name which is Airodump-ng and the wifi adapter's name which is wlan0. Wlan0 is the default wifi adapter name in kali linux operating system.

In figure 5. there are some important information which one should know for better understanding of the attack. BSSID (Basic Service Set Identification) is the MAC (Media Access Control) address of the WAP (Wireless Access Point), ESSID (Extended Service Set Identification) is the name of the AP (Access Point), CH means the channel at which AP is connected this is important because it helps provide the channel no. of the target for attacking, PWR is Signal level reported by the card. ... If the basic service set identification of PWR is -1, then the driver doesn't support signal level reporting. ENC means encryption it gives the information like which type of encryption is used for that particular device.

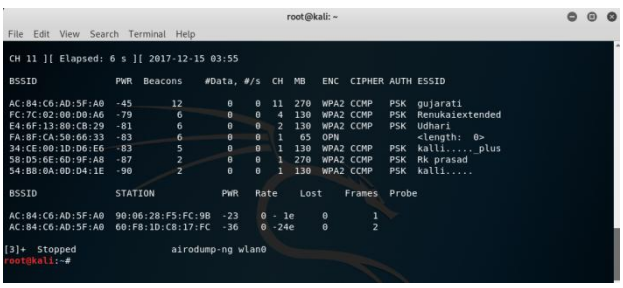


Figure 5. Scanning Network

D. Sending de-authentication packets

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

1. De-authentication using aireplay-ng

After scanning the network, select the ESSID="gujarati" as a demo target. In order to perform this attack on gujarati, some information about gujarati is required which is shown in "figure 5. Scanning Network". BSSID and CH of gujarati is required to perform the task. Now set the Wifi adapter as the same channel of the target router's channel using following command:

iwconfig wlan0 channel 11

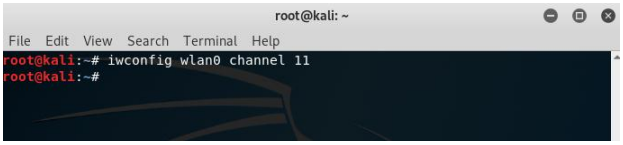


Figure 6. Changing Channel

Now the system is ready to send the de-authentication packets. To send de-authentication packets use the following command:

aireplay-ng -0 0 -a AC:84:C6:AD:5F:A0 wlan0

Here aireplay-ng is a tool which will be used to perform the attack, -0 sends the de-authentication packets and 0 refers to the number of packets, here 0 refers that it will keep sending the packets until the process is terminated manually, -a refers the MAC address of AP, "-a AC:84:C6:AD:5F:A0" refers the target which is "gujarati".

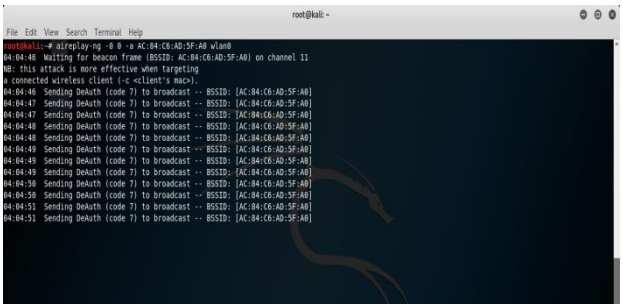


Figure 7. Attack Using Aireplay-ng

2. De-authentication using mdk3

After scanning the network, the ESSID="gujarati" as a demo target is selected. In order to perform the attack on gujarati ,some information about gujarati is required from "figure 5. Scanning Network". BSSID and CH of gujarati is used to perform the task. Now the system is ready to send the de-authentication packets. De-authentication packets are sent using the following command:

mdk3 wlan0 d AC:84:C6:AD:5F:A0 -c 11

MDK3 is used to perform the attack, d refers to the type of attack (d=de-authentication), AC:84:C6:AD:5F:A0 is the BSSID of the target which is "gujarati", -c refers to the channel of the target.

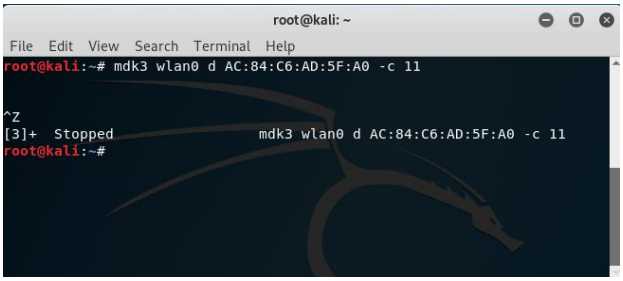


Figure 8. Attack Using Mdk3

V. DIFFERENCE BETWEEN AIREPLAY-NG AND MDK3

Aireplay-ng works flawless, The de-authetication is done pretty quickly, wherein user can choose how long to de-authenticate (0 for infinity). Although sending one de-authentication packet doesn't work in most of the cases. Aireplay directly won't work for some AP and Client, because it only sends a de-authentication packet, unlike MDK3. Resulting in an failure. On the contrary MDK3 is a software that uses the OSDEP library from aircrack-ng project that does the identical thing, but with greater certainty. MDK3 sends both de-authentication packets as well as de-association packets which makes it superior at its job. And MDK3 provides options too, suited for advanced users.

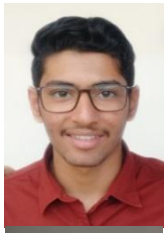
MDK3 is superior, though its de-authentication is slow in execution, it has been tested on different networks which makes it easier to get handshakes with MDK3 when compared to aireplay-ng.

REFERENCES

1. B. Flek, J. Dimov, Wireless access point and ARP poisoning: wireless vulnerabilities that expose the wired network, White paper, 12/10/2001.
2. G. Lin, G. Noubir, On link layer denial of service in data wireless LANs, Wiley journal on wireless Communication and Mobile Computing 5 (2005) 273-284.
3. Motorola White Paper (2011), Can Wireless LAN Denial of Service Attack Be Prevented? Understanding WLAN DoS Vulnerabilities & Practical Countermeasures.
4. IEEE 802.11 Wireless Local Area Network Task Group I, TGI – MAC Enhancements for Enhanced Security
5. Stuart Compton and Charles Hornat (2010)'802.11 Denial of Service Attack and Mitigation', SANS Institute.
6. Airecrack-ng official website http://www.aircrack-ng.org/
7. https://www.networkworld.com/article/2300056/the-importance-of-wireless-security.html
8. https://hackernoon.com/forcing-a-device-to-disconnect-from-wifi-using-a-deauthentication-attack-f664b9940142
9. https://en.wikipedia.org/wiki/Packet_analyzer
10. https://tools.kali.org/wireless-attacks/aireplay-ng
11. https://kalilinuxtutorials.com/mdk3/
12. https://www.yeahhub.com/ddos-wifi-network-mdk3-tool-kali-linux/
13. https://en.kali.tools/?p=34

AUTHORS PROFILE

Chintan Kamani is currently pursuing his B.tech degree in Cloud Computing and Information Security at Ajeenkya DY Patil University, ,Pune India and pass out in the year 2021.Currently following his passion about the world.



Dhrumil Bhojani is a cyber security enthusiastic currently pursuing his B.tech in Cloud technologies and Information security at ADYPU, Pune India. Currently researching on new technologies in cyber security field and Penetration testing.

Ravi Bhagyoday is pursuing his B.tech in Cloud technologies and Information security at ADYPU, Pune India. He is also researching new technologies in Cloud technology and working on different cloud platforms like AWS, Google Cloud, Azur, etc.

Vivek Parmar is currently pursuing his B.tech degree in Cloud Computing and Information Security at Ajeenkya DY Patil University Pune. Currently interested in machine learning and Artificial Intelligence.

Deepti Dave working as a Senior Faculty in Ajeenkya D Y Patil University Pune has completed her masters and has interest in security field and has done Information Security Professional certification.