International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228341

WiFi Deauthenticator

Aditya Singh, Anupam Kumar, Yagyansh Sharma, Aditya Sawnat, Prof. Pallavi Bhaskare
Department of Computer Science Engineering, Guide, Professor, Department of Computer Science Engineering, Smt. Kashibai Navale College of Engineering, Pune, Maharashtra, India

Article Info
Volume 8, Issue 3
Page Number : 142-146

Publication Issue :
May-June-2022

Article History
Accepted: 10 May 2022
Published: 22 May 2022

ABSTRACT

As the internet attack rate of the world is having trajectory growth at a significant pace; IEEE 802.11 wireless networks have emerged as a critical branch of security. These days wireless networks are literally on every corner from cafes to airport terminals. Over the years, lots of flaws on wireless systems are discovered ranging from caffe latte attacks to KRACK attacks. Together with these, DOS is not an exception. This paper stays around the Wifi DOS attack and practical detection of it. While Wifi DOS attack is an attack on wireless systems which completely disrupts the connection between Access Point and clients (cell phones, laptops). While some network equipment have built in features to prevent this attack; their performance, effectiveness to defend against this attack is not impressive at all. Consequently, along this whitepaper we will have a fascinating journey to witness how combination of packet crafting skills in scapy and python scripting will assist us to detect this attack.

Keywords : MAC Address ,De-Authentication Attacks, airmon-ng, MDK3

I. INTRODUCTION

WiFi Networks are one of the most used services to browse the internet together with Cellular Data From Mobile Network Providers. As the growth of the internet grows continuously at a significant pace, more people have access to it than ever before. With the growth of digitals transformation, cybersecurity has emerged with an approach to protect digital assets, data from misuse and unauthorized access. In a tree of cyber security, wireless networks have established themselves as critical branches which need regular monitoring. Majority of us use WiFi Networks to a higher extent compared to Cellular data. People rely on WiFi Networks to perform Banking Transactions, Shopping, Browsing and many more activities.However, Most WiFi users tend to have less attention or keep the lowest priority order for security of WiFi Networks. Traditionally, intranet was taken as low Risk Zone in Security but with evolution of Techniques like Web RTC, DNS rebinding, Intranet Pivoting, Server Side Request Forgery it is easier to Hack wireless networks from the internet than ever before. Wireless Deauthentication often referred to as Wifi DOS attack is still relevant till date.

Though, the attack requires the presence of targeted Wifi to be in range Network to broadcast Deauth Frames. Different Attacks like Wifi Phishing make

use of Deauthentication attacks to steal Wifi passwords. Below is the statistics extracted from statistica which justifies user dependency towards wifi networks compared to cellular

II. PROBLEM DEFINITION

To give heads up about how a certain vulnerability can be used against someone and make people aware about the simple solutions to not fall into that trap.

III. CONCEPT

A deauthentication 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 deauthentication is n't an exploit of a bug, it's a IEEE 802.11 protocol that's presently being used in real world operations. Deauthentication attacks use the deauthentication frame. This frame is transferred from a router to a device that forces the device to dissociate. In specialized terms it's called " certified fashion to notify a mischief station that they've been insulated from the network". This suggests that a device is on the network that should n't be on whenever.A deauthentication attack is a Denial of service WiFi attack which targets the connection between router and the device. A deauthentication frame is broadcasted by the router which also fully disables the connection between router and clients.n Effectively disabling the WiFi on the device. Deauthentication attack's use a deauthentication frameAt the time, when a router is passing a deauthentication attack no guests can connect to wifi networks indeed though the router is broadcasting the lamp frames.

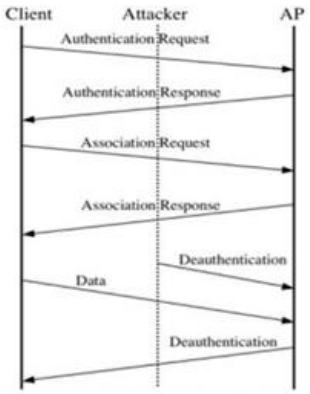


Figure 1. De-Authentication Attack

IV. INTRODUCTION TO TOOLS

There are two major tools which are used for deauthentication attack airmon-ng and MDK3. airmon-ng airmon-ng is a tool which is explicitly used to fit specially created ARP- request packets into an formerly wireless network in order to induce business. Its main part is to deauthenticate the formerly connected druggies on the wireless network. The airmon-ng tool is included in the aircrack-ng package. MDK3 MDK3 also known as Murder Death Kill 3 is one the most favoured tool to exploit ordinary IEEE802.11 protocol weakness. It's particularly designed for WLAN surroundings. The top operation of this tool is to flush the network with false business against the network. Can also be used to perform stress tests on802.11 networks. Demonstration of deauthentication attack using airmon-ng and MDK3. Changing mode of wireless appendage Before getting into examiner mode it's necessary to check the wifi appendage's name. This name will be used at numerous places in order to perform deauthentication attacks. Now in order to find the wifi appendage's name the following command will be used

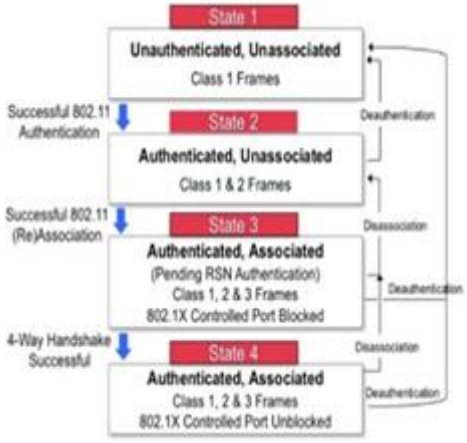


FIGURE 2. DATA FLOW DIAGRAM

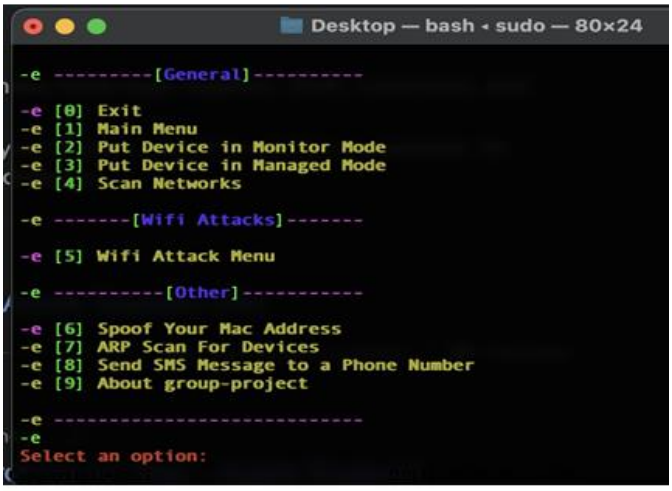
FIGURE 3. USE CASE DIAGRAM

V. Implementation and Results

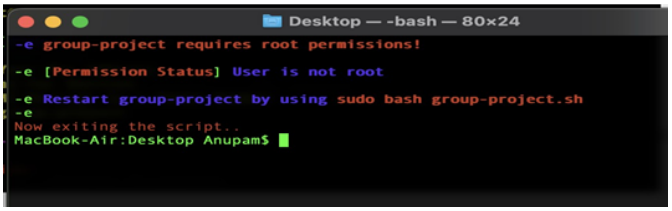
Note: Launching a Deauthentication Attack against the network you don't own is a crime and I request you to try this in your owned Access Point. We will now launch Deauthentication Attack in 4 simple Steps:

1: Identifying Wireless Network Interface Name Step
2: Checking for root access
3: Turning NIC into monitor mode
4: Broadcast Deauth Packets

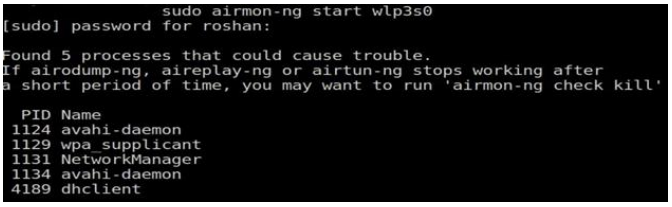
1. Identifying Wireless Network Interface Name Step : iwconfig The command provided my interface name is wlp3s0. Note your interface.



2. Check if the application is run using super user to provide root access for the script to perform actions.



3. Turning NIC card into Monitor Mode Now, we have identified our wireless interface name, let us turn NIC card into monitor mode.



4. Broadcast Deauth Packets We will use airmon-ng to broadcast deauth packets you can explore more options in it using airmon-ng -h. I will send deauth packets referencing Mac address of target but you can conduct with ssid name also. I expect this example to be relevant in Hidden Wifi also , so I conducted using the mac address. command: airmon-ng -0 0 -a

VI. CONCLUSION

Wireless technologies ranging from IEEE802.11 to draft standard IEEE 802.11 s are susceptible to DOS attacks. We've enforced the deauthentication and disassociation DOS attacks over the factual Wireless mesh testbed.Although Wireless Mesh Networks decide their security from the IEEE 802.11 i standard grounded protocol WPA2. This protocol can give security to only the data frames. The operation frames and the control frames are unencrypted and have been transferred in clear. Therefore DOS attacks have been launched by the bushwhacker after spoofing and masquerading these frames.

We've anatomized the impact of these attacks over the real Wireless Mesh Networks testbed. It has been noticed from the graphs that the network performance measured in terms of bandwidth and outturn appeared to be normal before the attack. But after the launch of the attack network performance starts dwindling and may reach zero. So for this we've proposed a security algorithm for the discovery of these deauthentication/ disassociation DOS attacks. This algorithm has reduced the generation of false cons results. In this we've increased the number of criteria and grounded on all of these we've linked whether the attack has passed or not. Although Airdefense has proposed several tackle outfit that may raise alert in case of the attacks. Although these tools have succeeded in icing secure communication in associations where security is the primary concern, cost is an issue associated with this result. Therefore there's the need to concoct an encyclopedically feasible cost effective result. Also the security mechanisms that have been proposed so far can only describe the circumstance of these DOS attacks. So there's an imperative need to develop the security results for the forestallment of DOS attacks.

VII. ACKNOWLEDGMENT

The success and final outcome of this project required a lot of guidance and assistance from many people and we are extremely privileged to have got this all along the completion of my project. All that we have done is only due to such supervision and assistance and we would not forget to thank them. We respect and thank our HOD, Prof. R. H. Borhade, for providing me an opportunity to do the project work in Smt. Kashibai Navale College of Engineering Pune and our project guide Prof. Pallavi Bhaskare, who took keen interest in our project work and guided us all along, till the completion of our project work by providing all the necessary information for developing a good system.

VIII. REFERENCES

[1]. Stuart Compton, Charles Hornat. May 17th 2007 802.11 Denial Of Service Attacks and Mitigation. SANS Institute InfoSec Reading Room.

[2]. Asier Martinez, Urko Zurutuza, Roberto Uribe Etxebarria, Miguel Fernandez, Jesus lizarraga, Ainhoa Serna and Inaki Velez 4-7th March 2008 Beacon frame Spoofing Attack Detection in IEEE 802.11 Networks. In the proceedings of the third international conference on Availability, Reliability and Security (ARES08). Barcelona.

[3]. Joshua Wright Jan 21, 2003 Detecting wireless LAN MAC Address spoofing. GCIH, CCNA, pp 1-5.

[4]. Chintan Kamani, Dhrumil Bhojani, Ravi Bhagyoday, Vivek Parmar, Deepti Dave . February 2019, Deauthentication Attack on Wireless Network. International Journal of Engineering and Advanced Technology (IJEAT)

[5]. Rupinder Cheema, Divya Bansal, Dr. Sanjeev Sofat. June 2011 Deauthentication/Disassociation Attack: Implementation and Security in Wireless Mesh Networks. International Journal of Computer Application

Cite this article as :

Aditya Singh, Anupam Kumar, Yagyansh Sharma, Aditya Sawnat, Prof. Pallavi Bhaskare, "WiFi Deauthenticator", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 3, pp. 142-146, May-June 2022.
Available at doi : https://doi.org/10.32628/CSEIT228341
Journal URL : https://ijsrcseit.com/CSEIT228341