INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume 4, Issue 3)
Available online at: www.ijariit.com

Detecting man in the middle attack

Sahil Dambee
sahil.dambee@spit.ac.in
Sardar Patel Institute of Technology, Mumbai, Maharashtra

Nikhita Mangaonkar
nikhita.mangaonkar@spit.ac.in
Sardar Patel Institute of Technology, Mumbai, Maharashtra

ABSTRACT

With Cyber-attacks and cyber-threats are increasing, network security needs to be seen in a new dimension. WLANs (Wireless Local Area Networks) are acquiring their hold in all the verticals of life. As technology is growing, a data breach at any scale, whether at the industry level or private can be menacing to distinct. Man-in-the-Middle is one of the most ruinous attacks in the WLAN. In this work, I propose a solution to detect a Man-in-the-Middle attack in public or home WLANs. The objective of the work is to present a solution which allows individual to keep watch on WLAN based on data packets collected over the network and evaluating its behavior. The proposed detection system is simulated with the help of Kali Linux where the attacker is trying to get a WPA Handshake over the network, a packet sniffer tool which captures the changes over the network during the simulation and one capture analyzing tool which analyze the capture.

Keywords: *Kali Linux, MITM, Network Scanners, Brute force*

1. INTRODUCTION

Wi-Fi connections are all over the place now, whether you are at your home or your favorite coffee shop. Users are using Wi-Fi for paying their bills, buying tickets or transferring money from one to another. In these scenarios, the threat of data theft can prove a loss of money, status or dependence. Cyber-attacks are on the upswing and cyber-crime is here to stay in today's digital era. Security is a major concern for WLANs because of its broadcast nature in communication. Every data packet sent in a wireless medium is broadcast by nature where any user in the communication range can capture the packet. We might feel that by installing a firewall and sitting on the safe side of the network guarding you against the world of the internet is the best defense against cyber-criminals. Nevertheless, the greatest risk to computers and networks today comes not from the front door through the firewall. The only measure most people use to secure their home network is to set up a password and prevent other people from taking control over your data. A grim risk is that an online immoral might exploit your poor Wi-Fi security measures. Through this, he can "listen" to your traffic in order to retrieve sensitive material or take advantage of your network to launch malicious attacks such as Man-in-The-Middle attacks, network sniffing or data theft. Approximately 25% of Wi-Fi hotspots in the world do not use any encryption at all. The effort required to hack a WLAN is less when network setting are set unsuitably and predictable passwords are set by the owner.

Data loss in communication is resulted due to many factors some of them includes data being corrupted or made unreadable by the software or application. Data loss is also referred to as Data leakage. Data loss causes the network to load resources at a slower pace and most of the time it is due to the bad setup of network or wired connection to the router. But when the scenario is not that, it is susceptible for a user to recheck the network behavior and do an analysis to surf safely over the internet. One of the many scenarios and the daunting is network getting attack by Man-in-The-Middle attack. In MITM the network gets compromised by the hacker which is capturing the packets passing over the channel. Those packets can be decrypted by passing them through brute-force or social engineering. A man-in-the-middle attack can be done in many ways, one of the basic and most effectual ways is to get a WPA Handshake. In WPA Handshake the attacker gets a three-way handshake by deauthorizing the station and the client. Here station refers to the router and client refers to the authorized user connected to the router.

Fig. 1: Secured connection over the network

In the above fig. the Client - A is connected over the network with Host –B making a secured connection over the network. The transaction is only between these two nodes and

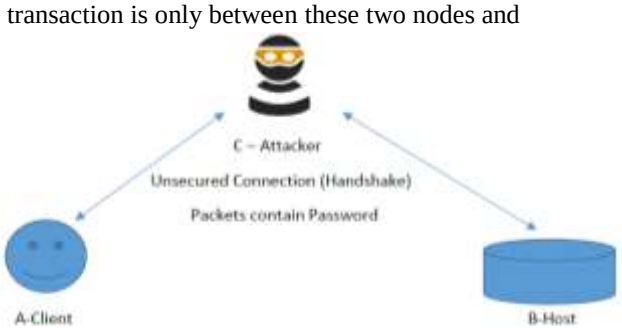

Fig. 2: Unsecured Connection over the network

interference caused will be only due to the environmental factors such as the distance of host from the client, physical interference and load on the network due to other users connected with the host.

In the above figure the Client- A is connected to the network but the connection is compromised in this scenario. The attacker - C has compromised the network by getting a WPA Handshake over the network.

WPA Handshake is basically a negotiation between the clients who want to connect to the router or network. For every client who wants to connect to the network, the password has to be given by client for authentication at first place to make a connection. The basic process of authenticating is quite simple and this is where an attacker takes advantage of it. The attacker with the use of tools such as Aircrack-ng and Airplay-ng disconnects the clients from the host and wait for them to connect back to the host. As soon the clients try to connect back to the host the handshake is established between the host, client and the hacker. As shown in fig 2, the attacker is now the Man-in-The-Middle who will be generating the spoofed keys from both the sides and creating a connection with both the client and the host. In this setup the packets are getting passed through the attacker – C. The packets passing through the network can contain any data like passwords, bank credentials or personal data related to the user. In this setup the response to the request will take more time in comparison to the setup shown in fig 1 because one more hop is added to the network and data loss will be there also. So the data loss over the network will be more and the response time will exceed causing a delay in rendering of the user request. This sudden change over the network should be identified by the user and always susceptible nature should be adapted.

2. IMPLEMENTATION

In the simulation carried out on the home connected router where we have one live client connected to the router. The operating system used to perform this simulation (attack on the client and the hots) is Kali Linux OS (64bit). The operating system comes preoccupied with tools like network sniffing, network scanners, exploits, brute force methods and many others.

In this simulation, we used one packet capture tool to capture all the traffic flowing over the network and one other packet capture analyzer which will analyze the capture and gives out the result in the form of statistics.

Fig. 3: Putting network in monitor mode

In figure 3 the network mode is set to the monitor mode to interact with the existing network in the range of Wi-Fi card.

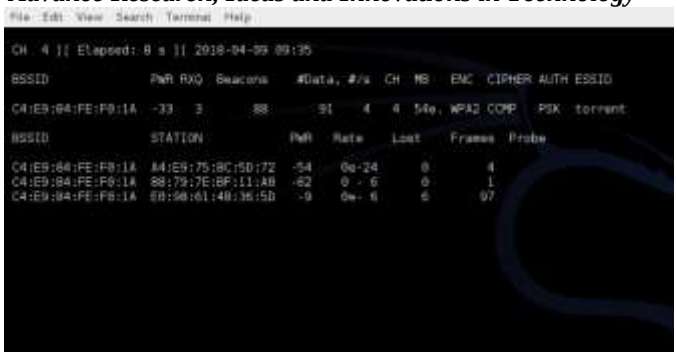

Fig. 4: Selecting network

In figure 4 we are selecting the BSSID (Basic Service Set Identifier) under the ESSID (Extended Basic Service Set ID) on channel "4" under column CH. We can also see the live hosts connected to the network. The command used here is:

airodump-ng –bssid C4:E9:84:FE:F0:1A –c 4 –w capture_file mon0

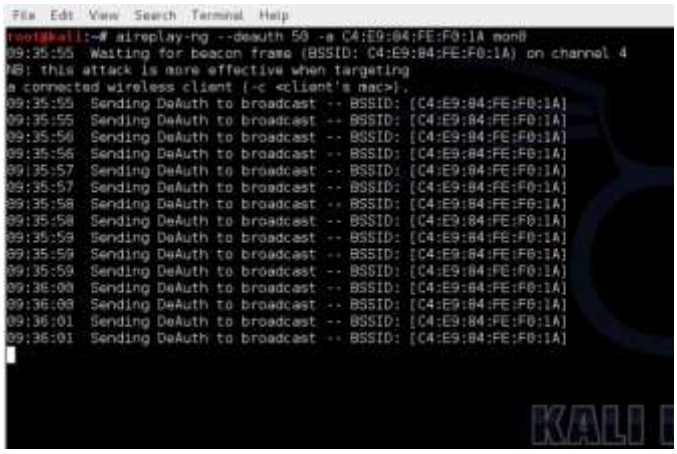

Fig. 5: Deauthorizing user from the network

In above figure, we are deauthorizing the connected clients from the network causing them getting disconnected from the network and connecting again. The moment the client tries to connect again to the network, the attacker gets a handshake as shown in figure 2. The command used here is:

airplay-ng –death 50 –a C4:E9:54:FE:F0:1A mon0

Fig. 6: WPA Handshake (MITM Attack)

In this simulation of network behavior change, data loss and transmission delay over the network is compared over a series of test done with and without the MITM attack by surfing some specific sites for the same amount of time. The changes are behavior can be seen below:

Application	Network Response Time
TCP	207.9 ms
Google	127.5 ms

Fig. 7: Without handshake

Fig. 8: With handshake

3. CONCLUSIONS

The paper has introduced a Man-in-The-Middle detection technique which can be done by users having WLAN setup at their home. The user can keep check of response time by the service and any instance and can compare with the earlier results, provided setup is not changed physically in any way. The inspiration for proposing this arrangement radiated from the thought that users are not that much familiar with the professional techniques of setting up local setup. Keeping track of the network setup and network behavior is essential and as technology is growing, the ways to exploit them are also increasing. The future scope of this research would incorporate more stress about implementing technique which will automatically detect a change in the behavior of the network and take precautionary measures such as changing the password of the router which will trigger the clients connected with the setup and change their password as well.

4. ACKNOWLEDGMENT

The author would like to acknowledge the support provided by his institution: Sardar Patel Institute of Technology and his mentor: Professor Nikhita Mangaonkar

5. REFERENCES

[1] Vikas Kumar, Sandip Chakraborty, Ferdous A Barbhuiya, Sukumar Nandi "Detection of Stealth Man-in-The-Middle Attack in Wireless LAN".

[2] Mauro Conti, Nicola Dragoni, and Viktor Lesyk "A survey of Man in The Middle Attacks".

[3] Kartikey Agarwal, Dr. Sanjay Kumar Dubey "Network Security: Attacks and Defense".

