WLAN Security: Active Attack of WLAN Secure Network (Identity theft)

Anil Kumar Singh[1], Bharat Mishra[2]

[1] Jagran Institute of Management
Kanpur- 208014 (India)

[2] MGCGV, Chitrakoot
Satna (M.P.) India

Abstract

In Wireless Local Area Network data transfer from one node to another node via air in the form of radio waves. There is no physical medium for transferring the data like traditional LAN. Because of its susceptible nature WLAN can open the door for the intruders and attackers that can come from any direction. Security is the most important element in WLAN. MAC address filtering is one of the security methods for securing the WLAN. But it is also vulnerable. In this paper we will demonstrate how hackers exploit the WLAN vulnerability (Identity theft of legitimate user) to access the Wireless Local Area Network.

Keywords: - *WLAN, MAC address, Access Point, WNIC, Wi-Fi*

Introduction

Wi-fi technology has played a very significant role in IT revolution and continues to do so. After 2 decades it is very popular among the It fraternity. Many companies, Educational Institutions, Airports as well as domestic users make use of the WLAN facility. Security is an important factor of Wireless Local

Area Network because of its nature. D-Link, Linksys are providing the WLAN security with the help of MAC address.[1] and WEP key. It is noted that the MAC address filtering is the gateway for hackers to enter and access the facility of Wireless Local Area Network.

Material and methods

The research was carried out to reveal WLAN Security: Active Attack on WLAN Secure Network

(Identity theft). The work was conducted at Department of Information Technology, Jagran Institute of Management. Materials used and the procedures employed are as follows: We can design a scenario after understanding the theory of WLAN security with the help of MAC address filtering. We have taken the Colasoft MAC Scanner 2.2 Pro Demo. There are hardware such as: HCL Desktop, Toshiba Laptops, AP (D-Link 2100 Series Access Point) and Wireless card (D-Link DWA 510).

Softwares such as: Operating System (Windows XP) and other application softwares. One client is used to communicate with Access Point. Another client is used to keep track of the network traffic as a hacker and listens to the WLAN. AP is linked to LAN with wires. Figure 1 is the illustration of Identity theft job.

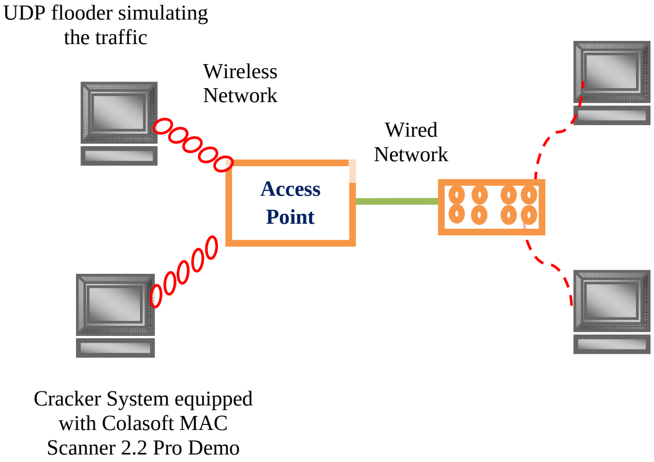
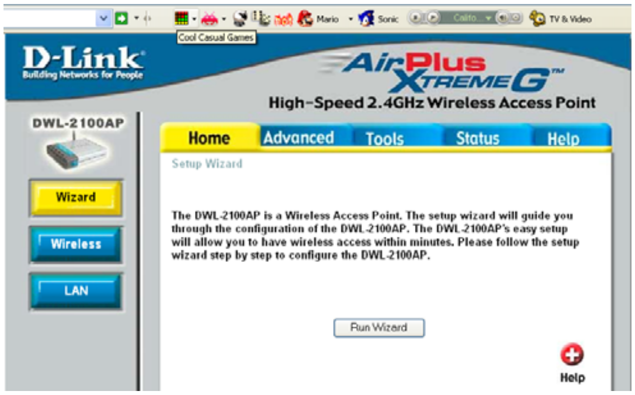


Figure - 1 Identity Theft gears

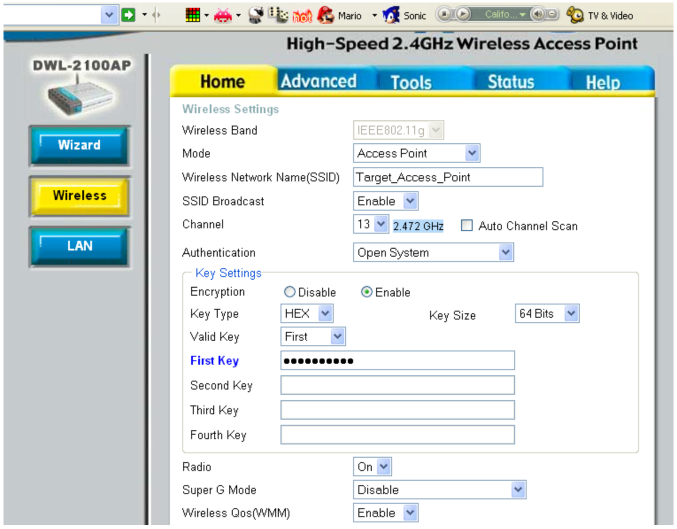
Open the internet explorer and type the IP of the access point 80.0.99.6 in address bar and press enter, Access Point will display the following window



Setup Wizard

The DWL-2100AP is a Wireless Access Point. The setup wizard will guide you through the configuration of the DWL-2100AP. The DWL-2100AP's easy setup will allow you to have wireless access within minutes. Please follow the setup wizard step by step to configure the DWL-2100AP.

Click on wireless tab



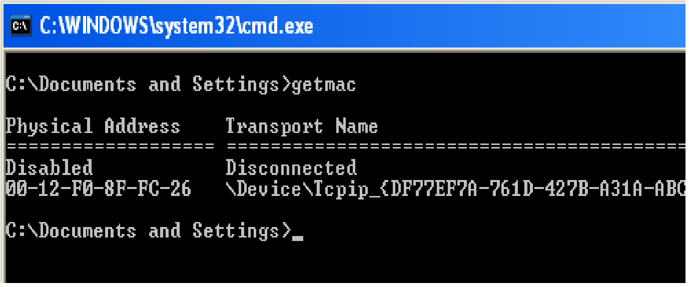
Wireless Settings

Wireless Band: IEEE802.11g
Mode: Access Point
Wireless Network Name(SSID): Target_Access_Point
SSID Broadcast: Enable
Channel: 13 2.472 GHz □ Auto Channel Scan
Authentication: Open System

Key Settings
Encryption ○ Disable ● Enable
Key Type: HEX Key Size: 64 Bits
Valid Key: First
First Key: ●●●●●●●●●●
Second Key:
Third Key:
Fourth Key:

Radio: On
Super G Mode: Disable
Wireless Qos(WMM): Enable

Click on advance tab, Click on filter, write the MAC address of legitimate user. For searching the MAC address click on start, click on run, type **cmd** and



C:\WINDOWS\system32\cmd.exe

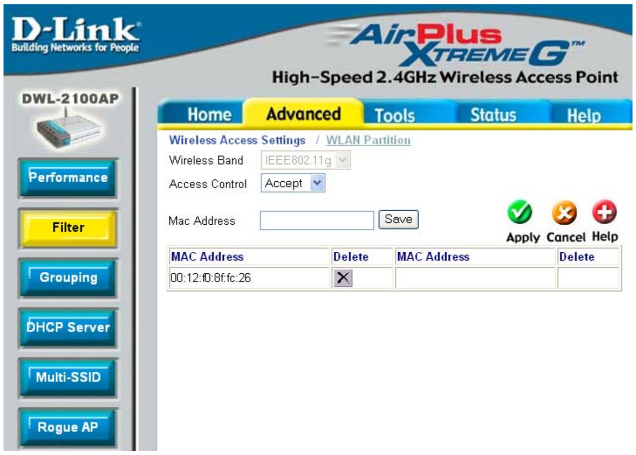
```
C:\Documents and Settings>getmac

Physical Address    Transport Name
=================== ==========================================
Disabled            Disconnected
00-12-F0-8F-FC-26   \Device\Tcpip_{DF77EF7A-761D-427B-A31A-ABC

C:\Documents and Settings>_
```

again type **getmac**, this command will display the MAC address of the WNIC

Click on access control displays three options namely disable, accept and reject, click on accept it means only authorized MAC address can access the WLAN, write the MAC address and save.



Wireless Band: IEEE802.11g
Access Control: Accept
Mac Address:

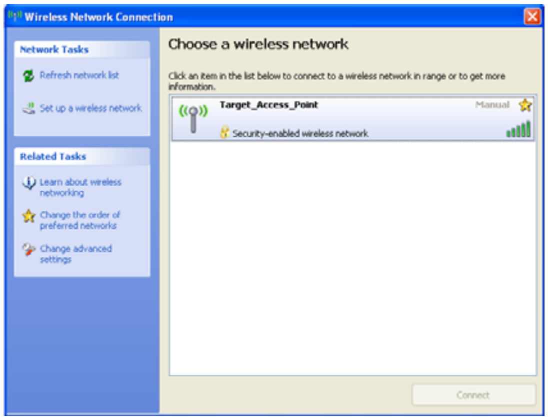
MAC Address	Delete	MAC Address	Delete
00:12:f0:8f:fc:26	☒		

Now we are going to another computer to access the wireless local area network which MAC address is displaying below:

```
C:\>getmac

1C-AF-F7-0C-CC-8C   \Device\Tcpip_{12361AAF-5538-4489-87B4-C9BB984E1299}
```

Now we are trying to connect the Target_Access_Point wireless network


Wireless Network Connection
Network Tasks
Refresh network list
Set up a wireless network
Related Tasks
Learn about wireless networking
Change the order of preferred networks
Change advanced settings
Connect

Choose a wireless network

Click an item in the list below to connect to a wireless network in range or to get more information.

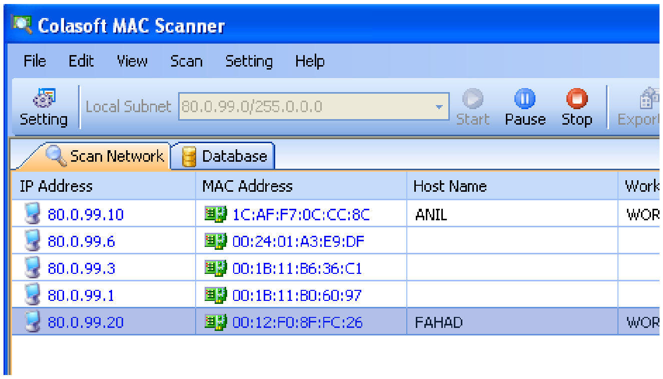
Target_Access_Point — Manual
Security-enabled wireless network

After that the system is not connected the wireless LAN.

Then we hack the MAC address of the legitimate user with the help of Cola soft MAC Scanner 2.2 Pro Demo [2].

After that the system will not be connected to the wireless LAN, and then we hack the MAC address of legitimate user with the help of Colasoft MAC Scanner 2.2 Pro Demo (it can be downloaded to http://www.colasoft.com /mac_scanner/

Double click on colasoft Scanner



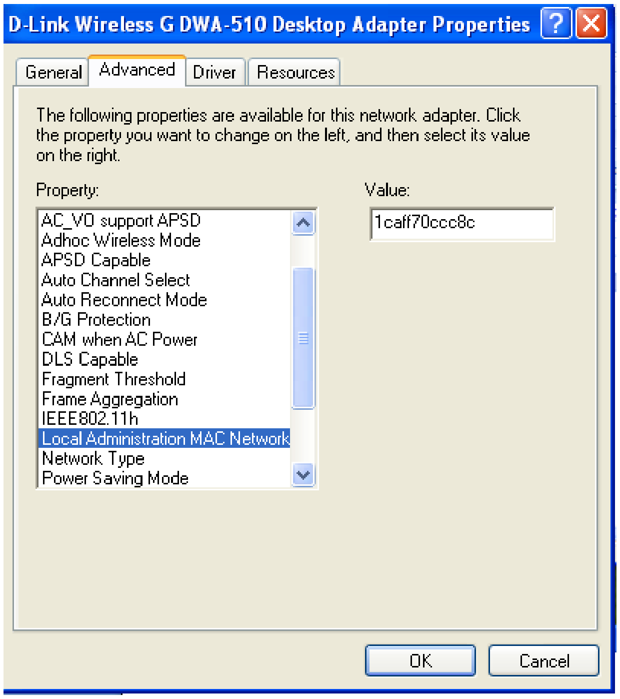
Local Subnet 80.0.99.0/255.0.0.0

IP Address	MAC Address	Host Name	Work
80.0.99.10	1C:AF:F7:0C:CC:8C	ANIL	WOR
80.0.99.6	00:24:01:A3:E9:DF		
80.0.99.3	00:1B:11:B6:36:C1		
80.0.99.1	00:1B:11:B0:60:97		
80.0.99.20	00:12:F0:8F:FC:26	FAHAD	WOR

Here you can see the highlighted MAC address. This is the identity of authorized user namely FAHAD.

Now we change the identity with the help of following process:

Click on start, Go to control panel, double click on Network connection, right click on Wireless Network connection, click on configure, click on advance



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

AC_VO support APSD
Adhoc Wireless Mode
APSD Capable
Auto Channel Select
Auto Reconnect Mode
B/G Protection
CAM when AC Power
DLS Capable
Fragment Threshold
Frame Aggregation
IEEE802.11h
Local Administration MAC Network
Network Type
Power Saving Mode

Value: 1caff70ccc8c

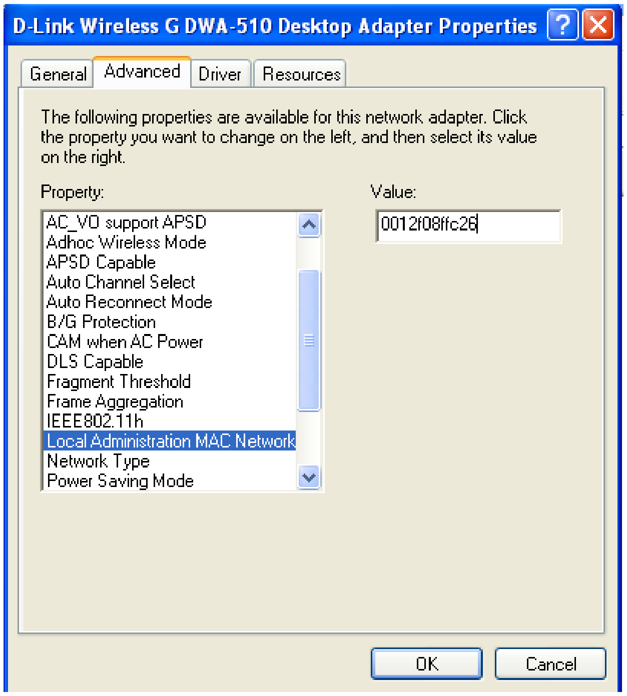
Select Local Administration MAC network, here you can see in value column it displays the MAC address. Now you can replace the identity of the existing user.

Type the MAC address in value column
0012f08ffc26

After changing the MAC address the hacker can easily access the WLAN without any barrier.

Conclusion

Due to the broadcast nature of the wireless communication, it becomes an easy prey for an attacker to capture wireless communication or to disturb the normal operation of the network by injecting additional traffic.



The following properties are available for this network adapter. Click the property you want to change on the left, and then select its value on the right.

Property:

AC_VO support APSD
Adhoc Wireless Mode
APSD Capable
Auto Channel Select
Auto Reconnect Mode
B/G Protection
CAM when AC Power
DLS Capable
Fragment Threshold
Frame Aggregation
IEEE802.11h
Local Administration MAC Network
Network Type
Power Saving Mode

Value: 0012f08ffc26

WLAN is also prone to unauthorized intervention by hackers where they create conditions for the theft of the identity (MAC address) of an authorized user. The access point cannot filter the MAC address. Because it checks their database and matches the MAC address, if found it allows accessing the WLAN.

To avoid this type of vulnerability we will strongly recommend that the administrator should use the combination of enabling WEP key and MAC address filter security mechanism. [3]

References

1. **Bradley Mitchell,** Enable MAC Address Filtering on Wireless Access Points and Routers Improve home network security
2. **Downloaded Cola soft MAC Scanner 2.2 Pro Demo by :** http://www.colasoft.com/mac_scanner/
3. **Anil Kumar Singh, (2011),** Wireless Local Area Network: Security from unauthorized access, proceedings of NCICT, Ewing Christian College Allahabad, Excel India Publishers New Delhi

Anil Kumar Singh, MCA – Asst. Professor, Jagran Institute of Management, Kanpur. Currently pursuing the Doctoral programme in WLAN Security Vulnerability Threats and Alternative Solution at MGCV Satna (M.P.)

Dr. Bharat Mishra, Ph.D., Dept. of Physical Science. MGCGV Satna (M.P.)