Unit 3: Attacks On Wireless Networks

3

Unit Structure

3.1 LEARNING OBJECTIVE

After studying this unit student should be able to:

- To Learn different wireless network standards.
- Current Issues with Wireless Network.
- Different attacks on wireless networks and their mitigation strategies.
- Tips to remain secure during wireless connection
- Introduction to Snort how to use it.

3.2 INTRODUCTION

In today's time, the wireless network is present everywhere from home to data centers. They make life easy from the long and bulky cables and its related issues. While ensuring the proper network connectivity with the internet to perform our everyday task. In order to learn the wireless (In short Wi-Fi which came from wires fidelity) networks. It was first invented by AT&T in the Netherlands in 1991. We will also see the basics of the wireless networks first and it's different standards, security issues, and attacks and mitigation strategies. Also, we will learn about the SNORT tools which is basically and IDS/IPS tool used for securing and monitoring the network.

3.3 BASICS OF WIRELESS NETWORK

Wireless network in simple terms means the transformation of the information or power between two nodes without any kind of physical electrical conductor. Wireless technology uses radio waves for short and long-distance communication.

There is a wide range of application of this wireless technology such as in telecommunication, satellite communications, mobiles, etc. There are multiple types of wireless network exists which I am sure you will be aware by the names as Wide Area Network(WAN), Local Area Network(LAN), Mobile Adhoc Network(MANET).

All these different types of networks are used for a different purpose but using wireless technology is at the core of all this. This network is a very popular choice for home users and from the small and medium size organization. There are three essential components of the wireless network that are radio signals, antenna, and router. The radio waves are the key which makes the Wi-Fi networking possible. Which are then converted to signals and picked by the Wifi receivers which is transmitted by the antenna. Then users are connected through the router for the communication.

The access point or router has a unique feature called as a beacon transmission, where it keeps on sending a signal on the wireless radio spectrum. This signal contains the network identification known as the service set identifier (SSID) and some trivial error correction information.

The wireless receiver such as a laptop or any wireless device detects this signal in order to show it in the list of available wireless networks. It also detects whether or not the access point is using any security, and what level of security protocol, etc.

The access point or router contains TCP/IP stack which responds to ARP requests when a node tries to connect to it. Since wireless can allow multiple nodes at any instance, it is essential to have an authentication layer prior to starting the data transfer. It is the responsibility of the access point to ensure this security and monitor the packet transmission and data integrity.

3.4 STANDARDS IN WIRELESS NETWORKS

For the wireless networks, 802.11 is the working group from the Institute of Electrical and Electronics Engineers (IEEE) who defines the standard of operation for a specific technology. They are the group of expert members who works on it. There is multiple version of this. In each version, there is an improvement in the features of 802.11.

Standard	Frequency	Speeds	Interoperates with
802.11a	5 GHz	54 Mbps	None
802.11b	2.4 GHz	11 Mbps	None
802.11g	2.4 GHz	54 Mbps	802.11b

802.11n	2.4 / 5 GHz	100 Mbps	802.11b, 802.11g
802.11ac	5 GHz	1.3 Gpbs	802.11a, 802.11n

There are some common properties between all these standards there is also difference exist between these standards. Such as in terms of speed and speed and modulation. Whether they are backward compatible or not.

There is some difference in protocols and how the data is handled by different standards. But the attack and defense strategy will remain the same most of the time.

The 802.11 standards, will prescribe which frequencies these technologies work as well as which channel which also depends on the geographical locations. In the United States, There are 11 different channels available from 1 to 11 all are separate and they will not interfere with one another.

The wireless network can work in two different modes such as Infrastructure and Ad-Hoc.

There are some terminologies need to understand which are useful before moving forward and are related to understanding the wireless networks and communications.

SSID: Service Set Identifier is a human-readable name associated with an 802.11 wireless network. It is normally known as the network name.

BSSID: Basic Service Set Identifier uniquely identifies a specific access point and it is of the similar format as of the MAC address of the access point.

ESSID: Extended Service Set Identifier can essentially be thought of as a group of BSSID which shares the same layer of the network and same SSID.

As the wireless network doesn't have the in-built security mechanisms. Due to which a secure layer is built on top of the wireless network protocol stack.

This is achieved by the encryption and authentication techniques such as WEP(Wired Equivalent Privacy) or WPA (Wi-Fi Protected Access). It is very important to secure the wireless networks as it can easily be intercepted.

Let us now discuss in details regarding the attacks on the wireless networks. We will also in details regarding the steps of how to crack the wireless networks from the learning perspective which will help indirectly in how to design and implement the wireless network effectively with robust security features in an organization.

Also for the wireless network, the security comes from the selection of the security technique or the authentication method which is adopted. There are various different security technique which is available such as WEP (Wired Equivalent Privacy), WPA2(Wifi Protected Access II). WPA1 provides two different modes of operation which includes Personal or Pre-Shared Key(PSK) and Enterprise.

WEP: WEP is a very basic and original part of the 802.11 wireless standards. It provides encryption at layer 2 in an OSI layer. WEP utilizes the RC4 encryption algorithm to encrypt data and uses a shared key-system. It uses either 40 bit or 104 bit WEP key to encrypt data.

WPA2-PSK: It utilizes a shared key that is communicated to both sides access point and client before establishing a wireless connection. This key is then used for secure communication.

WPS2-Enterprise: It is also known as 802.1X which uses a RADIUS server for the authentication purpose. IT is achieved using EAP (Extensible Authentication Protocol which is defined in RFC 3748).

3.4 WIRELESS NETWORK ATTACK

Any kind of wireless network attack is vulnerable and can cause the potential business impact. We will see several classifications which are described as below:

1. **Access Control Attack:** This attack tries to penetrate the wireless network or evading the access control mechanisms.

War Driving: To discover wireless LAN network by listening to beacons using sniffing tools.

Rogue Access Point: Installing an unsecured or fake access point inside the firewall.

Ad Hoc Associations: Connecting directly to an unsecured station.

MAC Spoofing: To bypass the MAC filtering policy in access points attackers used to change the MAC address which matches to the access point MAC address whitelist. SMAC tool can help in changing the MAC address in windows.

RADIUS Cracking: RADIUS(Remote Authentication Dial In User Service) is a server which is used to authenticate client and server. This attack can be performed using a brute force attack to obtain the secret key.

2. Confidentiality Attack: In **t**hese types of attacks attackers try to intercept the private information which is sent over a wireless network.

Eavesdropping: To capture the unprotected network traffic. Attackers mostly target the public wifi where the network usually does not have strong security measures.

WEP Key Cracking: To capture the network packets to recover the WEP key using active or passive methods.

Man In The Middle Attack: Attackers will try to capture the SSL connections in wireless networks and proxy them to web page logins to conduct the phishing attack. It can successfully complete this attack by first setting up the rogue access point and try to behave like a legitimate access point.

There are several steps involved to conduct such an attack which is listed below.

1. Select and target the access point and associated clients.

2. Identify the security protocol used such as WEP/WPA2 and crack the key.

3. Configure the wireless card as a rogue access point.

4. Use Airplay-ng to send de-authentication packets to target the host to disconnect from the network.

5. The disconnected client will reconnect after scanning with the fake access point.

3. Integrity Attack: These types of attacks send the forged control and management or data frames over the wireless network to misguide them or to fulfill another attack.

Frame Injection: Specifically crafting and forging the 802.11 packets.

RADIUS Replay: To capture RADIUS accept and reject messages for later reply.

4. Authentication Attack: Attackers try to steal legitimate user identities and credentials to access private network and services.

VPN Login Craking: To get the credentials using the brute force attacks on VPN authenticated protocols.

PSK Cracking: To crack and recover the password of WPA/WPA2-PSK from captured key handshake frames using dictionary attack tools.

5. Availability Attacks: These attacks stop the delivery of wireless services to legitimate users by denying them from accessing the WLAN resources.

Beacon Flood: Generating thousands of fake beacons to make it hard for stations to find a legitimate access point.

The next point we are going to see is to see how to crack the wireless network and get the encryption key. Also, we will see the process and tools usage which are mainly present in Kali Linux operating system.

But above all, it starts from understanding the basic cryptographic algorithm before starting to break it. As it is just built by using mathematical functions.

Always under certain circumstances, weak implementation of the security mechanisms allows an attacker to reverse engineer it. It applies to the wireless network protocols too.

When a WEP encrypted packets are captured using Wireshark or any other similar tool, there is a field which is labeled as IV(Initialization Vector). Every packet has a different IV. IV is a 24-bit pseudo-random number which is there with every packet.

By passively capturing(stealth mode capture) the traffic to capture enough packets, WEP key can be cracked. As for 24-bit pseudo-random number, there are around 16 million unique IV's, which can easily be got by capturing the busy network traffic. So there are chances that multiple packets can have the same IV's.

Let us see the process.

1. Identify the target wireless network.

2. Passively monitor the encrypted packets between an access point and client using a sniffer tool.

3. Monitor ARP packets, as ARP packets are very small and having a unique size, also it would be easy for an attacker to reply for an ARP request and to start capturing.

4. Continue to send ARP request and get unique IV's.

5. Save around 50,000 encrypted packets to determine the WEP key.

6. Use the aircrack-ng program against the saved packets to obtain the WEP key.

(aircrack-ng tools can be found pre-installed in Kali Linux).

There are other tools which are present and used for wireless network attacks. Such as:

Airmon-ng: Bash script to enable monitor mode on a wireless interface.

Airodump-ng: Wireless packet capturing tool designed for capturing packet for aircrack-ng.

Airplay-ng: Packet Injection Tool for the wireless network to generate the traffic.

Aircrack-ng: It is a tool used for cracking key of WEP or WPA/WPA-PSK wireless network.

Various commands line utility or tools which are used for basic information gathering of wireless network which is listed below.

iwlist: Command line utility for identifying the wireless network

Kismet: Linux wireless network detection suite.

Netstumbler: Windows-based wireless network detection suite.

We have seen the basic overview of the WEP cracking, but now we will look inside each step in detail with commands. To start from identifying the NIC cards, scanning wireless networks in surroundings.

The simplest way to identify the network wireless network cards in your system is using iwconfig. It will list out all network interfaces which are present in the system.

There will be a wireless card which will be shown as *wlan0* which will support the majority of all standards from (a,b,g, and n).

Next step is to use an iwlist command which will help to gather initial information.

iwlist wlan0 scanning

This command will give information such as ESSID, channel, frequency such information will be useful in later stages.

There are several fields which will be seen in the output and use to perform the following tasks.

Encryption key: If this is set on, then the access point is using WEP encryption.

Channel: To see the current wireless channel for the specific BSSID.

Mode: If the mode is set to master, then it is an access point or else it is an Ad-Hoc Network.

Use the MAC address statically while performing such kind of testing. For cloning MAC address in Linux it is essential to bring down the interface first and to start again, this can be performed using the *ifconfig* command.

Let’s begin with the process.

1. Identify the insure network using an *iwlist* command, which will consist of BSSID along with the channel.
2. Start the wireless card interface wlan0 into monitor mode using airmon-ng. For eg:

   >>airmon-ng start wlan0

   Start capturing the network traffic associated with the network using airodump-ng.
3. *>>airodump-ng –w DUMP –c <channel> --bssid <MAC Address> mon0*

   -w DUMP: It will tell airodump to name all files in output to start with DUMP*.

   -c <channel>: It tells airodump to stay connected on the channel specified, instead to jump In different channels.

   --bssid: Just capture traffic related to target bssid.

Keep the window open until we do not capture the sufficient numbers of packets. We have already seen that we need thousands of packets to gather enough number of IV to crack the WEP key.

Goto the current working directory where you will see some pcap files which can be open and view with Wireshark.

Now use aircrack-ng to see that pcap file to check how any number of packets are captured and how many numbers of unique IV are there. It will automatically tell whether we need more packets or we have enough number of the packet.

4. *>>aircrack-ng *.cap*

   If it shows “Failed”. Then try again using ARP reply attack to capture enough number of packets. As without a few thousand unique IV, we won't be able to crack the key.

5. *>>airplay-ng –arprepaly –b <MAC Address>*

   --arpreplay: Attack method.

   ARP replay attack takes time to complete the packet capturing process. Sometimes in several scenarios, if the packet capturing is not started then we have to cancel the process using CTRL-C and we have to start again.

   -b: Target MAC address.

   After some time again check with

   *>>airplay –ng *.cap*

   This will shows if the number of IV are gathered it will automatically crack the key and will show in hexadecimal form. Convert the same in ASCII format for text representation.

Now we will see about the WPA which is known as Wifi Protected Access. It has got two different versions, WPA and WPA2(802.11i).

The initial 3 steps of WEP cracking are the same for the cracking the WPA2-PSK encrypted are same but in later stages, the process becomes different which we will see below.

4. After performing the 3rd step the output will defer from what we have seen in the WEP process. Where the BSSID will show that the encryption used is WPA2 and PSK as the authentication method. Also, we can see the clients connected with the wireless network.

   Now, we can wait for another client to connect with the wireless aces point or we can deauthenticate the current client and capture the WPA handshake.

   Use the airplay-ng utility to deauthenticate if there is any existing client connected with the network.

5. *>>airplay-ng –deauth=5 –a <MAC Address> mon0*

   -- deauth=5: To deauthenticate the client and retry it 5 times if it fails on the first time. We can set this value as per our requirement. Make a note of STMAC address in output which represents the station MAC Address which will be required in a further step.

   -a: Provide target MAC Address

   Now, this method will not work on a large network, this will be not in a stealthy mode which we want to be. Also broadcasting the deauthentication message will not make sure that client will reconnect to it.

   Use the –c flag in the above command to make it effective.

   >>airplay-ng –deauth=5 –a <MAC Address> -c <STMAC> mon0

   After deauthentication of the client, it will automatically reconnect with the network and we will have the proper authentication handshake and start collecting in the pcap file. This can be seen using aircrack-ng command.

   *>>aircrack-ng *.cap –w /usr/share/dict/words.*

   -w: Word list can be a user-specified directory where the file is located.

   Aircrack-ng checks around 1000 passwords per second. In the output, you will get the text representation of the key obtained.

Check Your Progress 1

1. List out all the commands in a sequence which is used to crack WEP encryption.

3.5 LET US SUM UP

In this chapter, we have what all kind of wireless network attacks are there. Also, we have seen how to gather initial information or how to a reconnaissance of the wireless network to crack the key. It is important to understand the commands and what it does instead of blindly entering the command in the terminal.

We have also seen the tools which can be used for a different operating system platform. Also, this does not ensure that the process mentioned will work on all environments. This can differ as per the infrastructure and network devices used. Type of the wireless network card also sometimes can create some issues related to some software or packages dependencies.

3.6 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

Check Your Progress 1

```
>>airmon-ng start wlan0 <channel>
>>airodump-ng -w OUT -c <channel> –bssid <MAC Address> mon0
>>aireplay-ng --arpreplay -b <MAC Address> mon0
>>aircrack-ng *.c
```