Wifi password hacker

Continue

Also See : 200+ Cyber Security Courses | FULL ACCESS VIP MEMBERSHIP – ENROLL Now In this article we are going to discuss about Wi-Fi Hacking including Hack Wi-Fi Hidden networks, Bypass Mac Filtering. Hack WEP, WPA/WPA2 System requirement Kali Linux How to Change MAC Address, read here. An encrypted network is one that no longer transmits its name or ESSID. Concealed systems are as yet communicating their quality (channel, BSSID). Issue: Can't associate or attempt to split its secret key. Solutions: Airodump-ng can decide ESSID when the system is being used. It keeps one of the clients associated for a brief time frame. So let's start Step 1:- Select the WI-FI for connect >Select network in Kali Linux here we can see all the system accessible for interface but not hidden network so first we need to realize the concealed system name for associate Step 2:- Open terminal and type the following command #>ipconfig To see all the network card details. Note down the interface name. In this example we are using wlan0 Step 3:-#> Type the following command for see the rundown of all dynamic WI-FI its show the ESSID with BSSID else in the event that system is covered up (hidden network), at that point it will not show the ESSID just BSSID appeared. #>airodump-ng wlan0 Result :- Step 4:-#> Open new terminal and type the following command #>airodump-ng –channel [channel number] –bssid [hidden network BSSID here] wlan0 Result:- Step 5:-#> On terminal, go to action and select split terminal horizontal and type the following command for de-authenticate the client after that we can see the ESSID(name) of the target. #>aireplay-ng –deauth 4 -a [router BSSID here] -c [client BSSID here] wlan0 For my situation network encryption is open not wep wpa/wpa2, so there is no need of secret word if there is a case hidden network, it is having encryption wep or wpa/wpa2 security layer at that point move to the breaking technique. Step 6:-#> Now type the following command for change monitor mode to manager mode. #>service network-manager start Step 7:-#> Select the WI-FI Setting> connect to the hidden network> type network name and select WiFi security then connect. Result:- connected.. 2. Hack Wi-Fi WEP Wired Equivalent Privacy (WEP) is the most generally utilized Wi-Fi security convention on the planet. This is a component old enough, in reverse similarity, and the way that it shows up first in the convention determination menus in numerous switch control boards currently it is out of dated. Evidently, various home clients and private ventures purchased their APs years back, have never redesigned, and don't understand or couldn't care less about its absence of security. The blemishes in WEP make it defenseless to different factual breaking procedures. WEP utilizes RC4 for encryption, and RC4 necessitates that the introduction vectors (IVs) be arbitrary. The usage of RC4 in WEP rehashes that IV about each 6,000 casings. On the off chance that we can catch enough of the IVs, we can interpret the key. Also Read – Wi-Fi Network Not Secure in Windows 10 The Risks of Public Wi-Fi so lets start 1. Method :- Wi-Fi WEP cracking manually Step 1:- Open terminal and type the following command #>ipconfig To see all the network card details. Note down the interface name. In this example we are using wlan0 Step 2:-#> Type the following command for see the rundown of all dynamic Wi-Fi, it shows the ESSID with BSSID. #>airodump-ng wlan0 Step 3:-#> Open new terminal and type the following command #>airodump-ng –channel [channel number] –bssid [BSSID of target] –write [file name] wlan0 After that leave this console as it is and start the new console. Step 4:-#> Open new terminal and type the following command which is use for Fake Authentication attack. #>aireplay-ng –fakeauth 0 -a [bssid here] -h [use own mac address here] wlan0 Here we are using client MAC address for showing that how Fake Authentication work. If you don't get Association Successful message then keep on trying until you get success. Step 5:-#>Open new terminal and type the following command #>aireplay-ng –arpreplay -b [BSSID here] -h [client mac address here] wlan0 After that leave this console as it is and start new console Step 6:-#>Open new terminal and type the following command #>aircrack-ng -b (BSSID) (filename.cap) Just wait and watch….. aircrack will do rest of the work. Hurray we got the KEY. 2. Method :- Wi-Fi WEP cracking Automatically using wifite Step 1:- Open terminal and type the following command #>wifite Step 2:- After few minutes press Ctrl + C when ready for select the network Step 3:- Press key for select network press all for select all network for test. For my situation network encryption WEP is in number 1 after that just wait and watch….. wifite will do rest of the work. Hurray we got the KEY. Key is in HEX format just remove the ":" between key. The Password is 1234567890 Note: You can not able to break WPA/WPA2 utilizing wifite, but able to catch the packets (.cap file). Once catch the handshake, then use aircrack for get the key. 3. Hack Wi-Fi Mixed WPA-PSK+WPA2-PSK Wi-Fi Protected Access Shortcuts – Pre-Shared Key, additionally called WPA or WPA2 itself, is an approach to get to your WPA2 arrange utilizing Pre-Shared Key (PSK) confirmation, which was intended for clients are at home without a business check server. Scrambling the system with WPA2-PSK doesn't give your switch encryption key, but instead with an unmistakable English and 63 character string. Utilizing an innovation called TKIP (transient Key Integrity Protocol), that express, alongside organize SSID, is utilized to create one of a kind encryption keys for every remote customer. What's more, those composing keys are continually evolving. Despite the fact that WEP additionally bolsters word-handling phrases, it does so just as an approach to disentangle static catches, which are generally made of hex letters 0-9 and A-F. so lets start Method :- WEP cracking manually Step 1:- Open terminal and type the following command #>ipconfig For see all the network card details. Note down the interface name. In this example we are using wlan0 Step 2:-#> Type the following command for see the rundown of all dynamic WI-FI its show the ESSID with BSSID. #>airodump-ng wlan0 Result:- Step 3:-#>Open new terminal and type the following command #>airodump-ng –channel [channel number] –bssid [BSSID of target] –write [file name] wlan0 After that leave this console as it is and start new konsole Step 4:-#>Open new terminal and type the following command #>aireplay-ng –arpreplay -b [Target BSSID here] -h [client mac address here] wlan0 After that leave this console as it is and start new konsole Step 5:-#>Open new terminal and type the following command here we are using -w for dictionary attack #>aircrack-ng (filename.cap) -w (dictionary) Just wait and watch….. aircrack will do rest of the work. If handshake is not done aircrack will not work wait for minutes once handshake will done try again. Hurray! we got a KEY. Note: You can also use reaver tool for automated wpa/wpa2 crack and also cracking WPA/WPA2 much faster using GPU as compare to aircrack. Some important points and commands For cracking with Aircrack for saving aircrack-ng crack process Terminal#>john –wordlist=[name of word list] –stdout –session=upc | aircrack-ng -w – -b [target mac] [capfile] Terminal#>john –restore=upc | aircrack-ng -w – -b [target mac] [capfile] for using huge word lists with aircrack-ng without wasting storage Terminal#>crunch [minum char number] [max char number] | aircrack-ng -w – -b [target mac] [capfile] for saving cracking progress when using huge wordlist without store Terminal#>crunch [minum char number] [max char number] | john –stdout –session=upc | aircrack-ng -w – -b [target mac] [capfile] Terminal#>crunch [minum char number] [max char number] | john –restore=upc | aircrack-ng -w – [capfile] Wireless networks are everywhere; they are widely available, cheap, and easy to setup. To avoid the hassle of setting up a wired network in my own home, I chose to go wireless. After a day of enjoying this wireless freedom, I began thinking about security. How secure is my wireless network? I searched the Internet for many days, reading articles, gathering information, and participating on message boards and forums. I soon came to the realization that the best way for me to understand the security of my wireless network would be to test it myself. Many sources said it was easy, few said it was hard. How a wireless network works? A wireless local area network (WLAN) is the linking of 2 or more computers with Network Interface Cards (NICs) through a technology based on radio waves. All devices that can connect to a wireless network are known as stations. Stations can be access points (APs), or clients. Access points are base stations for the wireless network. They receive and transmit information for the clients to communicate with. The set of all stations that communicate with each other is referred to as the Basic Service Set (BSS). Every BSS has an Identification known as a BSSID, also known as the MAC address, which is a unique identifier that is associated with every NIC. For any client to join a WLAN, it should know the SSID of the WLAN; therefore, the access points typically broadcast their SSID to let the clients know that an AP is in range. Data streams, known as packets, are sent between the Access Point, and it's clients. You need no physical access to the network or its wires to pick up these packets, just the right tools. It is with the transmission of these packets that pose the largest security threat to any wireless network. Wireless Encryption The majority of home and small business networks are encrypted using the two most popular methods: WEP & WPA WEP – Wired Equivalent Privacy – comes in 3 different key lengths: 64, 128, and 256 bits, known as WEP 64, WEP 128, and WEP 256 respectively. WEP provides a casual level of security but is more compatible with older devices; therefore, it is still used quite extensively. Each WEP key contains a 24 bit Initialization Vector (IV), and a user-defined or automatically generated key; for instance, WEP 128 is a combination of the 24 bit IV and a user entered 26 digit hex key. ((26*4)+24=128) WEP also comes in WEP2 and WEP+, which are not as common and still as vulnerable as the standard WEP encryption. WPA – WiFi Protected Access – comes in WPA and WPA2, and was created to resolve several issues found in WEP. Both provide you with good security; however, they are not compatible with older devices and therefore not used as widely. WPA was designed to distribute different keys to each client; however, it is still widely used in a (not as secure) pre-shared key (PSK) mode, in which every client has the same passphrase. To fully utilize WPA, a user would need an 802.1x authentication server, which small businesses and typical home users simply cannot afford. WPA utilizes a 48 bit Initialization Vector (IV), twice the size of WEP, which combined with other WEP fixes, allows substantially greater security over WEP. Packets and IVs It's all in the packets. The bottom line is – while you may be able to employ several security features on your WLAN – anything you broadcast over the air can be intercepted, and could be used to compromise the security on your network. If that frightens you, start stringing wires throughout your home. Every encrypted packet contains a 24 or 48 bit IV, depending on the type of encryption used. Since the pre-shared key is static and could be easily obtained, the purpose of the IV is to encrypt each packet with a different key. For example, to avoid a duplicate encryption key in every packet sent, the IV is constantly changing. The IV must be known to the client that received the encrypted packet in order to decrypt it; therefore, it is sent in plaintext. The problem with this method is that the Initialization Vectors are not always the same. In theory, if every IV was different, it would be nearly impossible to obtain the network key; this is not the case. WEP comes with a 24 bit IV; therefore, giving the encryption 16 million unique values that can be used. This may sound like a large number, but when it comes to busy network traffic, it's not. Every IV is not different; and this is where the issues arise. Network hackers know that all the keys used to encrypt packets are related by a known IV (since the user entered WEP part of the key is rarely changed); therefore, the only change in the key is 24 bits. Since the IV is randomly chosen, there is a 50% probability that the same IV will repeat after just 5,000 packets; this is known as a collision. If a hacker knows the content of one packet, he can use the collision to view the contents of the other packet. If enough packets are collected with IV matches, your network's security can be compromised. The crack Two of the most popular programs used for actually cracking the WEP key are Airsnort and Aircrack. Airsnort can be used with the .dump files that Kismet provides; and Aircrack can be used with the .cap files that Airodump provides. Airsnort can be used on it's own without any other software capturing packets; although, it has been reported to be extremely unstable in this state, and you should probably not chance loosing all your captured data. A better method would be to let Airsnort recover the encryption key from your Kismet .dump file. Kismet and Airsnort can run simultaneously. For this demonstration, we'll be using Aircrack. You can use Airodump to capture the packets, and Aircrack to crack the encryption key at the same time. With Airodump running, open a new command window and type: aircrack -f 3 -n 64 -q 3 george.cap The -f switch followed by a number is the fudgefactor; which is a variable that the program uses to define how thoroughly it scans the .cap file. A larger number will give you a better chance of finding the key, but will usually take longer. The default is 2. The -n switch followed by 64 represents that you are trying to crack a WEP 64 key. I knew because it was a setup; In the real world there is no way to determine what WEP key length a target access point is using. You may have to try both 64 and 128. The -q 3 switch was used to display the progress of the software. It can be left out altogether to provide a faster crack; although, if you've obtained enough unique IVs, you should not be waiting more than a couple minutes. A -m switch can be used, followed by a MAC address, to filter a specific AP's usable packets; this would come in handy if you were collecting packets from multiple APs in Airodump. Aircrack recovered my WEP 64 key within 1 minute using 76,000 unique IVs; the whole process took around 34 minutes. The same experiment was repeated with WEP 128 and it took about 43 minutes. The reason it was not substantially longer is because I simply let Airplay replay more packets. Sometimes you can get lucky and capture an ARP Request packet within a few minutes; otherwise, it could take a couple hours. Other resources TOOLS Disclaimer: This Tutorial is knowledge Purpose only.