I'm not a robot

Wireless technology is difficult to secure, since no one can physically see or sense the data being transmitted over the air. The history of wired equivalent privacy (WEP) cracking is interesting, and today it has become a script kiddies game. It is a well-known fact that WEP key implementations are weak and easy to crack. The problem is compounded by that fact that it is difficult to restrict Wi-Fi signals to within an organization's walls, and to define legitimate usage. A WEP encryption key can be easily cracked using aircrack-ng. This aircrack tutorial will take you through the steps involved in cracking a WEP key using aircrack-ng. It is commonly believed that disabling SSID broadcasts is a security measure. Unfortunately, it isnt, but is instead a mandatory field for any legitimate client to connect to an AP. WEP is defined in the 802.11 standards as a protocol for protecting authorized WLAN users from casual eavesdropping. Since it uses RC4 symmetric encryption, both client and AP use identical data encryption keys. The data is prepended with an initialization vector (IV) field, which contains information about the encryption key in use. Here, my AP has the option to generate four keys based on a given passphrase. The client can use any of them. The three-byte IVs use two bits to define the encryption key in use. That is: 00 : key1 01 : key2 10 : key3 11 : key4 Note that the actual WEP key is 40/104 bits. The 24bit IVs prefixed by the AP take the total to 64/128 bits. This WEP key will perform an XOR operation with the data and CRC integrity and generate the cipher text. The cipher text will again be prepended with the same IV, chosen non-uniquely. When I connect my Blackberry Wi-Fi client to the AP, it asks for a passkey, here is the display: Once the passkey is provided, the AP is accessible from the client, as shown in the figure below. The basic idea behind WEP cracking is to trace weak IVs in the air. And this can be done with a toolkit called the aircrack-ng suite. This aircrack tutorial demonstrates WEP cracking in three steps: 1. Sniffing out packets and collecting weak IVs 2. Boosting traffic to the weak IVs 3. Cracking the WEP key In this aircrack tutorial, we will first sniff the air for packets. Sniffing the air is a simple and totally passive task. No one can really tell that a hacker is sniffing the packets, since it all happens wirelessly. We will first use airomon-ng in this aircrack tutorial to create a promiscuous mode interface (mon0) to sniff the wireless network. The aircrack developers created this brilliant tool with the ability to hop between channels and sniff packets. Note that the client and AP need to be in one channel to communicate. Next, we will use airodump-ng to sniff the packet flow in the air in this aircrack tutorial. The top part of the airodump-ng output lists information about APs in range, and the bottom part lists clients connected to the corresponding APs, in this aircrack tutorial. This command makes airodump-ng sniff traffic from the specified BSSID in channel 11, on which the target AP is running. It will write these packets to a local file called ConnectMeCrack. Passive sniffing takes a lot of time since we need to wait for legitimate IV packets. In this aircrack tutorial, we will use an arpreplay attack to boost weak IV traffic by replicating ARP requests from a legitimate device to the AP. The aireplay-ng command in this aircrack tutorial will fetch ARP packets from the legitimate client specified by the MAC address (-h option), and start sending them to the AP to get more packets with weak IVs. Here we notice that it received 0 ARP requests and 0 ACKs. There are two ways by which we can boost ARP traffic in the air. 1. Try fake authentication with the AP 2. Disconnect the legitimate clients from the access point In the first case, aireplay-ng will craft and send a fake authentication to AP to get more responses containing weak IVs. This command is easy to understand. The 0 parameter to --fakeauth specifies the delay in sending packets, -a specifies the BSSID, and -h the host MAC address. Now in another scenario, a hacker sends de-authentication packets to either one or all legitimate clients. The client(s) will then try to authenticate with the AP, which will eventually increase weak IV traffic. The below screenshot in this aircrack tutorial shows that my client disconnected when I started sending deauth packets, and when it stops deauth flooding, the client will again connect back to AP. Now if we again look up arpreplay results, we find that aireplay-ng has snagged many more ARP packets. The airodump utility in this aircrack tutorial has now created a few files on my system, and the cap files contain the collected weak IVs. Now lets move to the main task of this aircrack tutorial. We will pass the cap file to a utility called aircrack-ng, and it will do the rest. Aircrack-ng uses an algorithm to guess the WEP key from the collected weak IVs. In the screenshot below, aircrack-ng cracked the WEP key using 22412 IVs. If a hacker or pen tester gets access to a corporate wireless network, he can gain a lot more information about the network architecture by looking at the hops next to the wireless router. So wireless hacking doesnt end at cracking the secret key. The impact can go much beyond that. As this aircrack tutorial demonstrates, WEP is a very weak Wi-Fi protection mechanism. WPA or WPA2 provide more security from the kind of attack demonstrated in this aircrack tutorial. However, most Wi-Fi vendors continue to ship wireless routers with a WEP setting. Lets hope they stop supporting the weak WEP encryption standard in the future. About the author: Sanoop Thomas is a security trainer, vulnerability assessor, and penetration tester expert at NII. He has delivered several information security trainings and performed vulnerability assessment, penetration testing for NIIs premier customers. Sanoop is well-versed with the OWASP, OSSTMM and ISO 27001 Standards. He currently serves as an information security analyst and trainer at NII Consulting, focusing on application security, Java & ASP.NET secure coding practices. Sanoop specializes in Web applications, VoIP and wireless security. Please send your feedback to vharan at techtarget dot com. you can follow our Twitter feed at @SearchSecINAlthough it does not cover all the steps from start to finish like this tutorial, the Simple WEP Crack tutorial covers the actual aircrack-ng steps in much more detail. Setting up Hardware, Installing Aircrack-ngThe first step in getting aircrack-ng working properly on your Linux system is patching and installing the proper driver for your wireless card. Many cards work with multiple drivers, some of which provide the necessary features for using aircrack-ng, and some of which do not.Needless to say, you need a wireless card which is compatible with the aircrack-ng suite. This is hardware which is fully compatible and can inject packets. A compatible wireless card can be used to crack a wireless access point in under an hour.To determine to which category your card belongs to, see hardware compatibility page. Read Tutorial: Is My Wireless Card Compatible? if you don't know where to look in this table. It still does not hurt to read this tutorial to build your knowledge and confirm your card attributes.First, you need to know which chipset is used in your wireless card and which driver you need for it. You will have determined this using the information in the previous paragraph. The drivers section will tell you which drivers you need. Get the latest copy of aircrack-ng from the homepage, use our packages or use a penetration testing distribution such as Kali Linux or Pentoo where Aircrack-ng is already installed and up to date.To install aircrack-ng, refer to the documentation on the installation page. Ok, now everything is ready, time to make a pit stop before the action finally starts and learn something about how wireless networks work.The following chapter is very important, if something doesn't work as expected. Knowing what all is about helps you find the problem or helps you at least to describe it so someone else who can help you. This is a little bit scientific and maybe you feel like skipping it. However, a little knowledge is necessary to crack wireless networks and because it is a little more than just typing one command and letting aircrack do the rest. This is a short introduction into managed networks, these ones working with Access Points (AP). Every AP sends out about 10 so called beacon frames a second. These packets contain the following information: Name of the network (ESSID) If encryption is used (and what encryption is used; pay attention, that may not be always true just because the AP advertises it) What MBit data rates are supported Which channel the network is onThis information is then shown in your tool that connects to this network. It is shown when you let your card scan for networks with iwlist scan and when you run airodump-ng.Every AP has a unique MAC address (48 bit, 6 pair of hexadecimal numbers). It looks like 00:01:23:4A:BC:DE. Every network hardware device has such an address and network devices communicate with each other by using this MAC address. So its basically like a unique name. MAC addresses are unique, no two network devices in the world have the same MAC address. If you want to connect to a wireless network, there are some possibilities. In most cases, Open System Authentication is used. (Optional: If you want to learn more about authentication, check this out.)Open System Authentication: Ask the AP for authentication. The AP answers: OK, you are authenticated. Ask the AP for association The AP answers: OK, you are now connected. This is the simplest case, BUT there could be some problems if you are not legitimate to connect: WPA/WPA2 is in use, you need EAPOL authentication. The AP will deny you at step 2. Access Point has a list of allowed clients (MAC addresses), and it lets no one else connect. This is called MAC filtering. The first thing to do is looking out for a potential target. The aircrack-ng suite contains airodump-ng for this - but other programs like Kismet can be used too.Prior to looking for networks, you must put your wireless card into what is called monitor mode. Monitor mode is a special mode that allows your computer to listen to every wireless packet. This monitor mode also allows you to optionally inject packets into a network. Injection will be covered later in this tutorial.To put your wireless card into monitor mode using airmon-ng:airmon-ng start wlan0 It will create create another interface, and append mon to it. So, wlan0 will become wlan0mon. To confirm it is in monitor mode, run iwconfig and confirm the mode.Then, start airodump-ng to look out for networks:airodump-ng wlan0mon If airodump-ng could connect to the WLAN device, you'll see a screen like this:airodump-ng hops from channel to channel and shows all access points it can receive beacons from. Channels 1 to 14 are used for 802.11b and g (in US, they only are allowed to use 1 to 11; 1 to 13 in Europe with some special cases; 1-14 in Japan). 802.11a is in the 5GHz and availability in different countries is more fragmented than on 2.4GHz. In general, known channels starts at 36 (32 in some countries) to 64 (68 in some countries) and 96 to 165. Wikipedia has more details on channel availability. The Linux Central Regulatory Domain Agent takes care of allowing/forbidding transmissions on the different channels for your country; however, it needs to be set appropriately. The current channel is shown in the top left corner.After a short time some APs and (hopefully) some associated clients will show up.The upper data block shows the access points found: BSSID The MAC address of the AP RXQ Quality of the signal, when locked on a channel PWR Signal strength. Some drivers don't report it Beacons Number of beacon frames received. If you don't have a signal strength you can estimate it by the number of beacons: the more beacons, the better the signal quality Data Number of data frames received CH Channel the AP is operating on MB Speed or AP Mode. 11 is pure 802.11b, 54 pure 802.11g. Values between are a mixture ENC Encryption: OPN: no encryption, WEP: WEP encryption, WPA: WPA or WPA2 encryption, WEP?: WEP or WPA (don't know yet) ESSID The network name. Sometimes hidden The lower data block shows the clients found: BSSID The MAC of the AP this client is associated to STATION The MAC of the client itself PWR Signal strength. Some drivers don't report it Packets Number of data frames received Probes Network names (ESSIDs) this client has probed Now you should look out for a target network. It should have a client connected because cracking networks without a client is an advanced topic (See How to crack WEP with no clients). It should use WEP encryption and have a high signal strength. Maybe you can re-position your antenna to get a better signal. Often a few centimeters make a big difference in signal strength.In the example above the net 00:01:02:03:04:05 would be the only possible target because it's the only one with an associated client. But it also has a high signal strength so it's really a good target to practice. Because of the channel hopping you won't capture all packets from your target net. So we want to listen just on one channel and additionally write all data to disk to be able to use it for cracking:airodump-ng -c 11 --bssid 00:01:02:03:04:05 -w dump wlan0mon With the -c parameter you tune to a channel and the parameter after -w is the prefix to the network dumps written to disk. The --bssid combined with the AP MAC address limits the capture to the one AP. The --bssid option is only available on new versions of airodump-ng.Before being able to crack WEP you'll usually need between 40 000 and 85 000 different Initialization Vectors (IVs). Every data packet contains an IV. IVs can be re-used, so the number of different IVs is usually a bit lower than the number of data packets captured.So you'll have to wait and capture 40K to 85K of data packets (IVs). If the network is not busy it will take a very long time. Often you can speed it up a lot by using an active attack (=packet replay). See the next chapter. If you've got enough IVs captured in one or more file, you can try to crack the WEP key:aircrack-ng -b 00:01:02:03:04:05 dump-01.cap The MAC after the -b option is the BSSID of the target and dump-01.cap the file containing the captured packets. You can use multiple files, just add all their names or you can use a wildcard such as dump*.cap.For more information about aircrack-ng parameters, description of the output and usage see the manual.The number of IVs you need to crack a key is not fixed. This is because some IVs are weaker and leak more information about the key than others. Usually these weak IVs are randomly mixed in between the stronger ones. So if you are lucky, you can crack a key with only 20 000 IVs. But often this it not enough and aircrack-ng will run a long time (up to a week or even longer with a high fudge factor) and then tell you the key could not be cracked. If you have more IVs cracking can be done a lot faster and is usually done in a few minutes, or even seconds. Experience shows that 40 000 to 85 000 IVs is usually enough for cracking.There are some more advanced APs out there that use an algorithm to filter out weak IVs. The result is either that you can't get more than n different IVs from the AP or that you'll need millions (like 5 to 7 million) to crack the key. Search in the Forum, there are some threads about cases like this and what to do. Most devices don't support injection - at least not without patched drivers. Some only support certain attacks. Take a look at the compatibility page, column aireplay. Sometimes this table is not up-to-date, so if you see a NO for your driver there don't give up yet, but look at the driver homepage, the driver mailing list or our Forum. If you were able to successfully replay using a driver which is not listed as supported, don't hesitate to update the compatibility page table and add a link to a short howto. (To do this, request a wiki account on IRC.)The first step is to make sure packet injection really works with your card and driver. The easiest way to test it is the injection test attack. Make sure to perform this test prior to proceeding. Your card must be able to successfully inject in order to perform the following steps.You'll need the BSSID (AP MAC) and ESSID (network name) of an AP that does not do MAC filtering (e.g. your own) and must be in range of the AP.Try to connect to your AP using aireplay-ng:aireplay-ng --fakeauth 0 -e "your network ESSID" -a 00:01:02:03:04:05 wlan0mon The value after -a is the BSSID of your AP.If injection works you should see something like this:12:14:06 Sending Authentication Request12:14:06 Authentication successful12:14:06 Sending Association Request12:14:07 Association successful :-) If not double-check ESSID and BSSID make sure your AP has MAC filtering disabled test it against another AP make sure your driver is properly patched and supported Instead of 0, try 6000 -o 1 -q 10 Now that we know that packet injection works, we can do something to massively speed up capturing IVs: ARP-request reinjection ARP works (simplified) by broadcasting a query for an IP and the device that has this IPsends back an answer. Because WEP does not protect against replay, you can sniff a packet, send it out again and again and it is still valid.So you just have to capture and replay an ARP-request targeted at the AP to create lots of traffic (and sniff IVs). First open a window with an airodump-ng sniffing for traffic (see above). aireplay-ng and airodump-ng can run together.Wait for a client to show up on the target network. Then start the attack:aireplay-ng --arpreplay -b 00:01:02:03:04:05 -h 00:04:05:06:07:08 wlan0mon -b specifies the target BSSID, -h the MAC of the connected client.Now you have to wait for an ARP packet to arrive. Usually you'll have to wait for a few minutes (or look at the next chapter).If you were successful, you'll see something like this:Saving ARP requests in replay_arp-0627-121526.capYou must also start airodump to capture replies.Read 2493 packets (got 1 ARP requests), sent 1305 packets... If you have to stop replaying, you don't have to wait for the next ARP packet to show up, but you can re-use the previously captured packet(s) withthe -r option.When using the ARP injection technique, you can use the PTW method to crack the WEP key. This dramatically reduces the number of data packets you need and also the time needed. You must capture the full packet in airodump-ng, meaning do not use the --ivs option when starting it. For aircrack-ng, use aircrack -z . (PTW is the default attack)If the number of data packets received by airodump-ng sometimes stops increasing you maybe have to reduce the replay-rate. You do this with the -x option. I usually start out with 50 and reduce until packets are received continuously again. Better positioning of your antenna usually also helps. Most operating systems clear the ARP cache on disconnection. If they want to send the next packet after reconnection (or just use DHCP), they have to send out ARP requests. So the idea is to disconnect a client and force it to reconnect to capture an ARP-request. A side-effect is that you can sniff the ESSID and possibly a keystream during reconnection too. This comes in handy if the ESSID of your target is hidden, or if it uses shared-key authentication.Keep your airodump-ng and aireplay-ng running. Open another window and run a deauthentication attack:aireplay-ng --deauth 5 -a 00:01:02:03:04:05 -c 00:04:05:06:07:08 wlan0mon -a is the BSSID of the AP, -c the MAC of the targeted client.Wait a few seconds and your ARP replay should start running.Most clients try to reconnect automatically. But the risk that someone recognizes this attack or at least attention is drawn to the stuff happening on the WLAN is higher than with other attacks. More tutorials can be found on this page. In this comprehensive Aircrack-ng tutorial, we'll guide you through the ins and outs of using the powerful Aircrack-ng suite to assess and enhance the security of WiFi networks. Whether you're a seasoned ethical hacker or a newcomer to the cyber security field, this tutorial will provide valuable insights and actionable steps to help you understand and effectively use the various tools within the Aircrack-ng suite. Throughout this tutorial, we'll cover the essential tools, including airmon-ng, airodump-ng, airgraph-ng, aireplay-ng, aircrack-ng, and airbase-ng. Along the way, we'll include some helpful commands for each one. Additionally, we'll discuss the requirements, such as compatible wireless adapters and operating systems, to ensure you're well-equipped to tackle any wireless network security challenge. Get ready to dive into wireless network security and auditing with the Aircrack-ng suite, and discover how you can fortify your WiFi network against potential threats. Before diving into how to use Aircrack-ng, it's essential to ensure you have the proper hardware and software requirements to make the most of the tools in the suite. Wireless adapter capable of monitor mode and packet injection. Sufficient storage space and processing power. Aircrack-ng installed or available for installation. A solid understanding of wireless networking concepts. The specific WiFi adapter we're using throughout this article is the Alfa AWUS036ACH, but you can find several others that meet this requirement in our review Best WiFi Adapters for Kali Linux. The processing power of your device really comes into play with aircrack-ng. If you're using Kali Linux as a VM, it may be worth bumping up the processors and RAM allocated more than usual. We ran it with 4 cores and 4096MB of RAM. As mentioned above, Aircrack-ng and all its tools that we'll cover in this article come pre-installed on Kali Linux. However, you can download the suite on any Linux, macOS, or Windows device if you'd prefer. Additionally, you'll need an understanding of wireless networking and the elements involved to truly appreciate the steps you'll execute with some of the tools in Aircrack-ng and how to wargame a strategy for pentesting or ethical hacking. Aircrack-ng is a comprehensive suite of tools designed for auditing and securing WiFi networks. Its primary purpose is to help ethical hackers and security professionals test the security of wireless networks by cracking WEP and WPA keys, creating fake access points, capturing and analyzing network traffic, and performing various other network-based attacks. You can use the Aircrack-ng suite to assess the security posture of your wireless network, identify vulnerabilities, and test the strength of your network's encryption. Additionally, Aircrack-ng can be used to identify rogue access points, simulate various attack scenarios, and perform penetration testing tasks. Using the Aircrack-ng suite involves employing different tools within the suite, depending on the task. Each tool has a specific purpose and can be used independently or in conjunction with other tools in the suite to perform a wide range of wireless network security tasks. Aircrack-ng comes preinstalled on Kali Linux, making it readily accessible for security professionals and ethical hackers alike. In this article, we'll cover the following tools in the Aircrack-ng suite: Airmon-ng: Used to enable monitor mode on a wireless adapter, allowing you to capture network traffic. Airodump-ng: Captures network traffic, focusing on identifying wireless networks and capturing data packets. Airgraph-ng: Generates graphical representations of network traffic based on captured data, providing a visual representation of network activity. Aireplay-ng: Creates network traffic and performs various attacks, such as deauthentication and packet injection, to manipulate network behavior. Aircrack-ng: The flagship tool that cracks WEP and WPA/WPA2 encryption keys, allowing you to assess the strength of your network's security. Airbase-ng: Creates fake access points for testing network security, performing man-in-the-middle attacks, or social engineering purposes. There are other several other tools that fall under the suite, such as airdecap-ng, airdecloak-ng, and airtun-ng. However, for this tutorial, we will cover only the ones listed above because of the prevalence they have in security auditing and network hardening. These selected tools also have a natural flow, as you'll soon see. For the sake of clarity: During this article, we will distinguish between Aircrack-ng (meaning the suite) and aircrack-ng (meaning the tool). We want to be absolutely clear on this point. Even though it might seem innocent enough to perform a scan on your neighbor's wireless network, a server hosting a website, or other networks, dont do it. You need permission from the network owner if you are to do any kind of hacking or penetration testing on their systems. It might not seem like a big deal, but hacking, or even scanning, a system without permission can hold extremely steep legal penalties, including jail time, depending on your location. Such laws include: The Computer Fraud and Abuse Act (United States) Sections 184, 342.1, 380, and 430 of the Criminal Code of Canada (Canada) Computer Misuse Act 1990 (England) Sec. 202a and 202b of the German Criminal Code (Germany) Information Technology Act Sec. 43 and 66 (India) The Act on the Prohibition of Unauthorised Computer Access (Japan) Read our article Is port scanning legal? to learn more about this topic and to make sure youre operating in the clear. Airmon-ng is an essential tool in the Aircrack-ng suite, primarily used to enable monitor mode on your wireless adapter. Monitor mode allows your wireless adapter to listen to all the WiFi traffic in the air, even outside of the network your device belongs to. This is crucial for capturing packets, analyzing network traffic, and injecting packets into the target network when needed. You use airmon-ng at the beginning of any wireless network auditing or penetration testing process. It sets the stage for using other tools in the Aircrack-ng suite, such as airodump-ng, aireplay-ng, and aircrack-ng itself. Using airmon-ng is straightforward. First, identify the interface name of your wireless adapter (e.g., wlan0) using the ifconfig command and iwconfig. Once you have the interface name, you can enable monitor mode with the airmon-ng start command followed by the interface name. Managed Mode: This means that your WiFi adapter is set to only receive packets directed to our specific MAC address. Think of this as only receiving letters delivered to your home. Monitor Mode: When your device is in monitor mode it will be able to receive all packets that are in range of the WiFi adapter, even if they arent addressed to your machines MAC address. Think of this as standing in the postal receiving and sorting room and watching all of the envelopes come in. Typically, you'll run this in the following order: Run ifconfig to first check for the interface name. Run iwconfig to check the mode. If its in managed mode, continue with the next steps. If its already in monitor, then you likely left it in that state from a previous session and can skip the rest of this. Next run sudo airmong-ng check to look for any conflicting process that might interfere with setting up monitor mode. If you find any interesting processes, run sudo airmon-ng check kill to stop them. Finally, run the sudo airmon-ng start , in our example wlan0. This command is used to bring your adapter back up in monitor mode. This will append mon to the end, such as wlan0mon. Common airmon-ng commands: CommandActionairmon-ng check killTerminates interfering processes identified by the "airmon-ng check" command. Example: sudo airmon-ng check killairmon-ng startEnables monitor mode on the specified interface. Example: sudo airmon-ng start wlan0airmon-ng stopDisables monitor mode on the specified interface. Example: sudo airmon-ng stop wlan0monairmon-ng --channel Sets the default channel for the wireless adapter when entering monitor mode. Example: sudo airmon-ng start wlan0 --channel 6 The most common frequency to test is 2.4GHz, and the most common, non-overlapping channels operated are 1, 6, and 11. If you're auditing and testing on 5GHz, there are many more non-overlapping channels. Generally, every fourth channel between 36-144 and 149-165. Using airmon-ng you can enable monitor mode to capture the necessary data and perform various wireless security tests. This crucial first step lays the foundation for the rest of the Aircrack-ng suite to work effectively. Airodump-ng is another critical tool in the Aircrack-ng suite, primarily used for capturing packets from wireless networks. By capturing packets, you can analyze network traffic, identify connected devices, and obtain essential information such as encryption keys and handshakes required for cracking the network's security. You need to use airodump-ng after enabling monitor mode with airmon-ng. It allows you to gather valuable information about the target network and its clients, which will help you better understand the network's structure and identify potential vulnerabilities. Using airodump-ng involves executing the tool with the monitoring interface (e.g., wlan0mon) and specifying various parameters such as the channel to monitor, the BSSID to filter, and the output file prefix for the captured data. Once started, airodump-ng will display live information about the networks and clients it detects. See all networks in range: sudo airodump-ng wlan0mon Common airodump-ng commands: CommandAction--channelSpecifies the channel to listen on. Example: --channel 6--bssidFilters the captured data to a specific BSSID. Example: --bssid AA:BB:CC:DD:EE:FF-wSets the output file prefix for the captured data. Example: -w output--encryptFilters the captured data to networks with a specific encryption type. Example: --encrypt WPA--showackDisplays acknowledgment statistics for each client, useful for identifying packet injection vulnerabilities. Example: --showack Example of a packet capture: sudo airodump-ng wlan0mon --channel 6 --bssid AA:BB:CC:DD:EE:FF -w output Utilizing airodump-ng effectively, you can gather essential data (such as AP and client MAC addresses) for further analysis and set yourself up for more advanced attacks or security assessments using other tools in the Aircrack-ng suite. Airgraph-ng can be a valuable tool in the Aircrack-ng suite, used to create graphical representations of wireless networks and their associated clients. These visualizations can help you better understand the relationships between networks and devices, making it easier to identify potential targets and vulnerabilities. You would use airgraph-ng after capturing packets with airodump-ng. By converting the captured data into a graphical format, you can gain a clearer understanding of the network's structure, which can help you plan and execute more targeted and effective attacks or security assessments. Using airgraph-ng involves providing an input file (CSV) generated by airodump-ng and specifying an output file for the generated graph. The tool supports multiple graph types, allowing you to choose the one that best suits your needs. Common airgraph-ng commands: CommandAction-iSpecifies the input CSV file generated by Airodump-ng. Example: -i output-01.csv-oSets the output file for the generated graph. Example: -o output.png-gSpecifies the graph type to generate. Example: -g CAPR or -g CPG-cSets the channel filter for the generated graph. Example: -c 6--essidFilters the graph data to networks with a specific ESSID. Example: --essid MyNetwork Example of generating a graph from the captured data: sudo airgraph-ng -i output-01.csv -o output.png -g CAPR Using Airgraph-ng, you can visually analyze the relationships between networks and clients, helping you identify potential targets and better understand the overall structure of the wireless environment. This insight can be crucial for planning and executing advanced wireless security assessments or ethical hacking operations. If youre going through this tutorial to improve your skills as an ethical hacker, you might be wondering which certificate is best to market yourself. Take a look at our article, CEH vs OSCP: Which One Should You Pursue?, for some helpful insight. Aireplay-ng is a great tool in the Aircrack-ng suite, designed to generate, inject, and manipulate wireless network traffic. It supports various attack types, including deauthentication, fake authentication, and ARP request injection, which can help facilitate different stages of wireless security assessments or ethical hacking operations. You would use aireplay-ng after capturing packets with airodump-ng and analyzing the network traffic. Based on the information gathered, aireplay-ng can be employed to speed up the cracking process, force client disconnections, or test network security by injecting custom packets. When you execute a deauthentication (deauth) attack with aireplay-ng, the tool sends a series of deauthentication frames to the target device and access point. These frames are designed to mimic legitimate management packets from the access point or the client device, instructing them to disconnect from each other. As a result, the target device is disconnected from the WiFi network, forcing it to re-establish the connection, which can be used to capture the handshake. Using aireplay-ng involves specifying the attack type, target network, and relevant parameters depending on the attack. You may need to provide the monitoring interface (e.g., wlan0mon) and the MAC addresses of the target access point and client devices. Common aireplay-ng commands: CommandAction--deauthExecutes a deauthentication attack, disconnecting clients from the target network. Example: --deauth 100--fakeauthPerforms a fake authentication attack, simulating a client connecting to the target network. Example: --fakeauth 60--arpreplayConducts an ARP request replay attack to generate more IVs for WEP cracking. Example: --arpreplay-aSpecifies the target access point's BSSID. Example: -a AA:BB:CC:DD:EE:FF-cSets the target client's MAC address. Example: -c 11:22:33:44:55:66 Example of a deauthentication command: sudo aireplay-ng --deauth 100 -a AA:BB:CC:DD:EE:FF -c 11:22:33:44:55:66 wlan0mon When using aireplay-ng effectively, you can manipulate wireless network traffic, test network security, and gather additional information to aid in cracking WiFi encryption or identifying vulnerabilities. Its various attack types make it a valuable addition to the Aircrack-ng suite, offering flexibility and adaptability for different wireless security scenarios. Aircrack-ng is the flagship tool of the Aircrack-ng suite, primarily used for cracking wireless networks encryption keys, such as WEP and WPA/WPA2. It employs various algorithms and techniques to recover encryption keys, enabling you to gain unauthorized access to a wireless network or verify the strength of your own network's security. You would use aircrack-ng after capturing packets with airodump-ng and potentially manipulating traffic with aireplay-ng. Once you have collected enough data, such as a WPA handshake or a sufficient number of WEP IVs (Initialization Vector), aircrack-ng can be employed to attempt a key recovery using a dictionary or brute-force attack. Using aircrack-ng involves providing the captured data (in .cap format) and specifying the attack parameters, such as the dictionary file or the key length for brute-force attacks. The tool will then analyze the captured data and attempt to recover the encryption key. Common aircrack-ng commands: CommandAction-wSpecifies the wordlist or dictionary file for a dictionary attack. Example: -w dictionary.txt-bSets the target access point's BSSID. Example: -b AA:BB:CC:DD:EE:FF-eSpecifies the target network's ESSID. Example: -e MyNetwork-aForces the attack mode to use between WEP and WPA/WPA2-PSK. Example (WPA/WPA2-PSK): -a 2 Hidden Networks Cracking WPA/WPA2-PSK networks where the ESSID is not broadcasted (hidden) requires that the ESSID be specifically tagged as an optional command with -e . Example of cracking a WPA key: sudo aircrack-ng -w dictionary.txt -b AA:BB:CC:DD:EE:FF output-01.cap Executing aircrack-ng effectively, you can attempt to crack wireless network encryption keys and assess the security of WiFi networks. Its various attack options and algorithms make it a powerful tool for ethical hackers and security professionals alike, providing insights into potential vulnerabilities and the effectiveness of network security measures. The Aircrack-ng suite is very powerful, but there are a host of other tools that come pre-installed on Kali Linux to help you with your ethical hacking efforts. Check out some of our top picks in 25 Top Penetration Testing Tools for Kali Linux. Airbase-ng is a powerful and fun tool within the Aircrack-ng suite, designed to create fake access points (APs) for various purposes, such as testing client devices' behavior, performing man-in-the-middle attacks, or social engineering attacks. By emulating legitimate access points, airbase-ng can trick nearby devices into connecting to the fake AP, allowing you to monitor or manipulate their network traffic. You would use airbase-ng after gathering information about the target network and clients using tools like airodump-ng and aireplay-ng. Once you've identified a suitable target, airbase-ng can be employed to create a fake access point, luring unsuspecting users into connecting and potentially revealing sensitive information. Airbase-ng involves specifying the parameters for the fake access point, such as the ESSID, channel, and encryption type. You will need to provide the monitoring interface (e.g., wlan0mon) and may need to configure additional settings to match the target network's characteristics. Common airbase-ng commands: CommandAction-aSets the fake access point's BSSID (MAC address). Example: -a AA:BB:CC:DD:EE:FF--essidSpecifies the fake access point's ESSID (network name). Example: --essid MyFakeAP--channelSets the channel for the fake access point. Example: --channel 6-W 1Enables WEP encryption for the fake access point. Example: -W 1-zSets the fake access point to use WPA/WPA2 encryption. Example: -z 2 (for WPA2) Example usage: sudo airbase-ng -a --essid --channel wlan0mon By using airbase-ng correctly, you can create fake access points for various purposes, such as testing network security, performing man-in-the-middle attacks, or social engineering. Its flexibility and adaptability make it a valuable tool in the Aircrack-ng suite, offering unique opportunities for ethical hackers and security professionals to assess the behavior of client devices and the effectiveness of network security measures. Throughout this Aircrack-ng tutorial, we've explored the powerful features of the Aircrack-ng suite and demonstrated how it could be used to assess and enhance the security of WiFi networks. If youd like to see all of these steps chained together in a demonstration of hacking a WiFi network, you can find that in How to Hack WiFi With Kali Linux Like a Pro. Remember that ethical hacking and network security testing should only be performed on networks you have permission to access, and always adhere to legal and ethical guidelines. As you continue to develop your skills in the cyber security field, using tools like Aircrack-ng will empower you to take a proactive approach to wireless network security, ensuring that your WiFi connections remain safe and secure in an ever-evolving digital landscape. Elevate your cyber security expertise to new heights by enrolling in our StationX Master's Program, designed to empower you with valuable knowledge and practical skills. Yes, WPA2 can be cracked, but it is generally more secure than WEP and WPA. The most common method for cracking WPA2 involves capturing the four-way handshake that occurs when a client connects to the network and then performing a brute-force or dictionary attack to guess the pre-shared key. However, this can be a time-consuming process, and the chances of success depend on the strength of the password and the attacker's resources.WPA2 is not easy to hack compared to its predecessors, WEP and WPA. WPA2 has improved encryption and security measures that make it more challenging for attackers. However, it is still vulnerable to specific attacks, such as capturing the four-way handshake and performing a brute-force or dictionary attack. To protect your WPA2 network, use a strong, unique password and keep your router firmware up-to-date. Can Aircrack-ng use GPU for password cracking?Aircrack-ng itself does not support GPU acceleration for password cracking. However, there are other tools, like hashcat, that can leverage the power of GPUs to perform password cracking more efficiently. You can use Aircrack-ng to capture the handshake and then use hashcat (included with Kali Linux) with GPU support to perform the password-cracking process. What is the most secure WiFi password?A secure WiFi password should be long, unique, and contain a mix of uppercase and lowercase letters, numbers, and special characters. In line with NIST 800-63b guidelines, consider using a passphrase (a sequence of words or other text) instead of a traditional password. If using a passphrase, consider inserting random characters, numbers, or special characters in between the words.Aim for a password or passphrase that is at least 12-16 characters long. Avoid using common words, phrases, or easily guessable information like names, birthdays, or addresses. A strong password or passphrase reduces the likelihood of a successful brute-force attack.Heres a step-by-step guide on how to use Aircrack-ng, a powerful suite of tools designed for assessing the security of Wi-Fi networks, particularly for capturing packets and cracking encryption keys.Step 1: InstallationOn Linux1. Install via Package Manager: For Ubuntu/Debian: ```bash sudo apt-get update sudo apt-get install aircrack-ng ```- For Fedora: ```bash sudo dnf install aircrack-ng ```2. Install from Source: Download the latest version from [Aircrack-ngs official site](. Extract the tar file: ```bash tar -zxvf aircrack-ng-X.X.tar.gz cd aircrack-ng-X.X ``` Compile the source code: ```bash make sudo make install ```On Windows1. Download the latest version of Aircrack-ng from [here](.2. Install it and use it through the command prompt or the included GUI.Step 2: Put Your Wireless Card into Monitor ModeTo capture packets, your wireless network card must be in **monitor mode**. This enables your card to listen to all wireless traffic.1. Identify your wireless interface: ```bash sudo airmon-ng ```Note the name of your wireless interface (e.g., `wlan0`).2. Put your wireless card into monitor mode: ```bash sudo airmon-ng start wlan0 ```This will create a new interface like `wlan0mon` in monitor mode.3. Check for Processes: Stop any processes that could interfere with packet capturing (optional but recommended): ```bash sudo airmon-ng check kill ```Step 3: Capturing Packets with Airodump-ngThe next step is to capture packets from the target Wi-Fi network.1. Start capturing packets on all available networks: ```bash sudo airodump-ng wlan0mon ```2. Identify the target network: Youll see a list of Wi-Fi networks, their BSSID (MAC address), and other details like signal strength (PWR) and encryption type. Take note of the **BSSID** and the **channel (CH)** of your target network.3. Capture packets on a specific network: Once youve identified the target network, capture packets from it using the following command: ```bash sudo airodump-ng bssid channel -w wlan0mon ```Replace `` with the networks BSSID and `` with the channel. The `-w` option specifies the name of the file where the packets will be saved.Step 4: Deauthenticate Clients (Optional but Useful for WPA/WPA2)To capture the 4-way handshake needed for WPA/WPA2 cracking, you may need to disconnect a client from the network, forcing it to reconnect. This will generate the handshake, which can be captured.Deauthenticate a client from the target network: ```bash sudo aireplay-ng deauth 10 -a -c wlan0mon ```- `-a` is the target networks BSSID. `-c` is the MAC address of a connected client (you can get this from the airodump-ng output). `10` is the number of deauth packets to send.You should now see the handshake being captured by `airodump-ng`. Look for a message saying WPA handshake in the airodump-ng window.Step 5: Cracking the WPA/WPA2 Key Using Aircrack-ngOnce youve captured the handshake, its time to crack the WPA/WPA2 key.1. Run Aircrack-ng on the captured handshake file: ```bash sudo aircrack-ng -w -b ```- `-w ` is the path to your wordlist (like `rockyou.txt`). `-b ` is the BSSID of the target network. `` is the file that contains the captured handshake (created by airodump-ng in Step 3).2. Cracking process: Aircrack-ng will now attempt to crack the key using the wordlist. This process can take time, depending on the strength of the password and the size of your wordlist.Step 6: WEP Cracking (For Older Networks)The process is different if the target Wi-Fi network uses WEP encryption (very outdated but sometimes still in use).1. Start capturing packets on a WEP-encrypted network using the same `airodump-ng` command as in Step 3.2. Inject ARP packets to speed up packet collection: ```bash sudo aireplay-ng arpreplay -b wlan0mon ```3. Crack the WEP key using Aircrack-ng once you have enough IVs (Initialization Vectors). WEP keys can often be cracked after collecting around 10,00020,000 IVs: ```bash sudo aircrack-ng ```Step 7: Additional FeaturesAircrack-ng offers several additional tools you can use to analyze networks and perform specific attacks:Airbase-ng: Creates fake access points.Aireplay-ng: Injects and replays packets for network attacks.Airdecap-ng: Decrypts captured traffic from WEP/WPA encrypted networks.Depending on your goals, you can use these tools to perform more advanced attacks or experiments on Wi-Fi networks.Step 8: Returning Your Wireless Card to Normal ModeOnce youre done with your testing, return your wireless card to its original state:1. Stop monitor mode: ```bash sudo airmon-ng stop wlan0mon ```2. Restart networking services: If you stopped any services in Step 2, restart them: ```bash sudo service NetworkManager start ```Important NotesLegal Considerations: Always ensure you have permission to test Wi-Fi networks. Unauthorized cracking of networks is illegal.Wordlists: A strong wordlist (e.g., `rockyou.txt`) is critical for WPA/WPA2 cracking. Without a robust wordlist, cracking strong passwords is nearly impossible.Hardware: Some wireless network adapters do not support monitor mode, so check compatibility before starting.With this step-by-step guide, you should now have a basic understanding of how to use Aircrack-ng to assess the security of Wi-Fi networks.Aircrack-ng is a powerful network security software suite designed to assess WiFi network security. It is widely used for tasks such as monitoring, attacking, testing, and cracking WiFi networks. One of its primary functionalities is to crack WEP and WPA/WPA2 keys from captured packet handshakes. This suites advanced capabilities make it an invaluable tool for security professionals and network administrators when auditing wireless networks.Use Case 1: Crack Key from Capture File Using WordlistCode:aircrack-ng -w path/to/wordlist.txt path/to/capture.capMotivation:This use case allows a user to crack the encryption key of a WiFi network by using a wordlist. This method is particularly useful when you have an existing database of possible passwords and want to test a batch of these against a captured handshake file (.cap). By trying each password in the wordlist, Aircrack-ng attempts to find the correct encryption key, enabling you to access the network.Explanation:aircrack-ng: This is the command itself, part of the Aircrack-ng suite, specifically aimed at cracking encryption keys.-w path/to/wordlist.txt: This argument specifies the path to the wordlist file containing possible passwords. The -w flag indicates that the following path specifies a wordlist.path/to/capture.cap: This is the path to the capture file that contains the handshake data. This file is the target input that aircrack-ng will test passwords against to find a match for the encryption key.Example Output:Opening capture.capReading packets, please wait...Passphrase not in dictionaryIf successful, this output would instead show the correct key once it is found.Use Case 2: Crack Key from Capture File Using Wordlist and the Access Points ESSIDCode:aircrack-ng -w path/to/wordlist.txt -e essid path/to/capture.capMotivation:In this scenario, adding the ESSID (Extended Service Set Identifier) can help in scenarios where multiple networks might exist within the capture file, or when the capture file contains handshakes from various networks. By specifying the ESSID, you narrow down the search to a particular network, which can speed up the cracking process and increase the likelihood of success by ensuring the attack is correctly targeted.Explanation:aircrack-ng: The command for attempting to crack encryption keys.-w path/to/wordlist.txt: The path specified for the wordlist to test against the capture file.-e essid: The ESSID (network name) of the particular access point you aim to target. This argument helps focus the attack on a specific network.path/to/capture.cap: Path to the capture file containing the handshake that you aim to crack.Example Output:Reading packets, please wait...Targeted ESSID: [NetworkName]Passphrase not in dictionaryIf successful, the output would display the correct key relevant to the targeted ESSID.Use Case 3: Crack Key from Capture File Using Wordlist and the Access Points MAC AddressCode:aircrack-ng -w path/to/wordlist.txt --bssid mac path/to/capture.capMotivation:Utilizing the access points MAC (Media Access Control) address to crack a key can be useful in dense environments where multiple networks have similar ESSIDs, or where networks are hidden. This feature is particularly useful to enhance accuracy by precisely targeting a specific network based on its unique hardware address.Explanation:aircrack-ng: The basic command for cracking WiFi network keys.-w path/to/wordlist.txt: Denotes the location of the wordlist utilized for cracking.--bssid mac: The MAC address of the specific network you are targeting. Precise targeting is possible with the MAC address, ensuring the correct AP is selected in complex environments.path/to/capture.cap: The path to the capture file which includes the necessary handshake data for cracking.Example Output:Reading packets, please wait...Targeted BSSID: [XX:XX:XX:XX:XX:XX]Passphrase not in dictionaryThis output would change to display the correct passphrase when found.Conclusion:Aircrack-ng provides a comprehensive suite for network security evaluation. By using different parameters and options available in these examples, users can effectively and efficiently assess the vulnerabilities in wireless networks. Understanding these use cases allows network professionals to enhance their strategies for ethical hacking and penetration testing, ensuring a robust defense against unauthorized access. However, it is crucial to only use these techniques on networks you own or have explicit permission to test to ensure legal compliance. Aircrack-ng is a powerful suite of tools for assessing the security of Wi-Fi networks. It allows users to perform various functions, including monitoring, attacking, and cracking WEP and WPA/WPA2 encryption keys. While Aircrack-ng is primarily designed for Linux systems, it has become more accessible to Windows users, especially with the advent of Windows 11. In this article, we will explore how to install and use Aircrack-ng on Windows 11, along with practical guidance on its functionalities, legal considerations, and troubleshooting tips.What is Aircrack-ng?Aircrack-ng is an open-source software suite used for network auditing and penetration testing. It consists of various tools to perform tasks related to Wi-Fi security, including:Airmon-ng: Used for enabling monitor mode on your wireless adapter.Airodump-ng: Captures raw 802.11 packets and helps find nearby access points and clients.Aireplay-ng: Focuses on replaying and injecting packets.Aircrack-ng: The final tool for determining the WEP or WPA/WPA2 key from the captured packets.Before diving into the tools usage, its crucial to acknowledge the ethical considerations surrounding its deployment. Aircrack-ng is designed for testing the security of your own networks. Using it on networks you do not own without permission is illegal and unethical.Getting StartedPrerequisitesCompatible Wireless Adapter: For Aircrack-ng to function optimally, you need a wireless adapter that supports monitor mode. Not all adapters have this capability; common options include adapters with atheros or rtl8187 chipsets.Windows Subsystem for Linux (WSL): Since Aircrack-ng is optimized for Linux environments, well use WSL in this guide.Installing Windows Subsystem for Linux (WSL)Open Windows Terminal: Press Windows + X and select Windows Terminal (Admin) to open it with administrative privileges.Enable WSL: Type the following command and press enter:wsl --installSelect a Distribution: By default, WSL installs Ubuntu, which is commonly used and well-supported. You can also install other distributions later via the Microsoft Store.Restart Your Computer: Follow any prompts to restart your computer.Set Up Linux Distribution: After the restart, open the Ubuntu (or your chosen distribution) app from the Start Menu. Follow the prompts to set up a user account and password.Install Aircrack-ngOnce WSL and your Linux distribution are set up, you can install Aircrack-ng:Update Package Lists: Open your Linux terminal and type:sudo apt updatesudo apt upgradeInstall Aircrack-ng: Run the following command to install Aircrack-ng:sudo apt install aircrack-ngVerify the Installation: After installation, you can verify it by running:aircrack-ng --versionConfiguring Your Wireless AdapterTo use Aircrack-ng effectively, your wireless adapter needs to operate in monitor mode. Lets break down how to do this within WSL.Check Wireless AdapterList Network Interfaces: Enter the command:iwconfigThis will list your wireless interfaces. Look for a device name like wlan0.Enable Monitor ModeAs of now, enabling monitor mode directly in WSL can be tricky and may require additional configurations, often involving running a virtual machine or dual-booting with a dedicated Linux distribution. Its worth noting that not all wireless drivers support monitor mode in WSL.For experimentation purposes, some users opt for a USB live session of Kali Linux, offering broad compatibility with various Wi-Fi devices, alongside more pre-installed penetration testing frameworks.If youre running a compatible Linux environment, heres how to enable monitor mode:sudo airmon-ng start wlan0This command will create a new interface named wlan0mon, enabling you to capture Wi-Fi data.Basic Usage of Aircrack-ng Tools1. Airodump-ngAirodump-ng is crucial for gathering information about nearby wireless networks.Running Airodump-ngUpdate Drivers Fix Your PC Open your terminal and type:sudo airodump-ng wlan0monReplace wlan0mon with your actual monitor interface name. This command will provide a list of nearby Wi-Fi networks, including their SSID (network name), BSSID (MAC address), encryption type, and the number of connected clients.2. Capturing WPA/WPA2 HandshakeTo crack WPA/WPA2 keys, you need to capture the handshake. This requires you to monitor a specific target network.Select Target Network: Identify a network from the Airodump-ng output to capture its handshake.Capture the Handshake: Use the following command:sudo airodump-ng -c --bssid -w wlan0monReplace with the channel number of the network.Replace with the networks BSSID.Replace with your chosen filename for the captured data.Force a Handshake Capture: To improve your chances of capturing a handshake, you can deauthenticate a connected client:sudo aireplay-ng --deauth 10 -a wlan0monThis command will send deauthentication packets to the specified BSSID, prompting a reconnection from the client.3. Aircrack-ngOnce you have the handshake captured, the next step is to crack the password.Running Aircrack-ngCrack the Handshake: Use the following command to start cracking:aircrack-ng .cap -w Replace with the name of the captured file.Replace ` with the path to your chosen wordlist file. You can download common wordlists likerockyou.txt`, which comes pre-installed in some penetration testing distributions.Example CommandsTo illustrate, heres an example of the complete process flow:Driver Updater - Update Drivers Automatically Start monitoring a particular network:sudo airodump-ng -c 11 --bssid 00:11:22:33:44:55 -w captured wlan0monForcefully deauth a client to capture the handshake:sudo aireplay-ng --deauth 10 -a 00:11:22:33:44:55 wlan0monFinally, crack the WPA/WPA2 handshake:aircrack-ng captured-01.cap -w /path/to/rockyou.txtIf the password exists in your wordlist, Aircrack-ng will reveal it in a matter of seconds to minutes, depending on the complexity of the password.Legal ConsiderationsUsing Aircrack-ng carries significant ethical and legal responsibility. It is crucial to always ensure you have explicit permission to test the security of the networks you are evaluating. Unauthorized network access or penetration testing is illegal in most jurisdictions and can lead to severe penalties.Always familiarize yourself with local laws regarding network security testing, and only use tools like Aircrack-ng for ethical purposes.Troubleshooting Common IssuesPoor Adapter PerformanceNot all wireless adapters work well with Aircrack-ng. If you experience issues:Check Compatibility: Refer to a list of compatible adapters.Update Drivers: Ensure you have the latest drivers installed.Permission IssuesIf you encounter permission issues during connectivity or actions:Run Commands as Root: Use sudo before commands that require administrative privileges.Handshake Not CapturedMonitor Mode Enabled: Ensure your adapter is in monitor mode.Proximity to Target Network: Ensure youre within range of the network and capturing enough packets.ConclusionUpdate Drivers Fix Your PC Aircrack-ng is an invaluable tool for network security assessment, allowing both professionals and enthusiasts to evaluate the robustness of Wi-Fi networks. While its primary ecosystem is Linux-based, Windows 11 users can leverage WSL to install and utilize Aircrack-ng effectively.Remember that with power comes responsibility; always engage with network testing ethically and legally. By adhering to best practices and constantly updating your techniques, you can ensure a safer digital environment for everyone. Happy hacking! Aircrack-ng is a suite of wireless security tools that enables users to evaluate the security of their wireless networks and carry out security audits. This tutorial will help you set up your environment for using aircrack-ng by providing information on the necessary hardware and software, installation, and wireless card configuration. Setting Up the Environment To use aircrack-ng, you will need a computer with a supported operating system, such as Linux or Windows, and a wireless card that supports monitor mode. A list of compatible wireless cards can be found on the aircrack-ng website. Installing aircrack-ng To install aircrack-ng on a Linux system, use the following command: sudo apt-get install aircrack-ng For other operating systems, instructions for installation can be found on the aircrack-ng website. Configuring Wireless Card Once aircrack-ng is installed, you need to configure your wireless card for use with the software. This involves setting the card into monitor mode, which allows it to capture and analyze wireless traffic. The command to set a wireless card into monitor mode depends on the card and operating system. Here is an example for setting a wireless card into monitor mode on Linux: sudo airmon-ng start wlan0 In this example, wlan0 is the name of the wireless card. Replace it with the name of your own wireless card if it is different. By following these steps, you will have successfully set up your environment for using aircrack-ng. Understanding WLAN and Wireless Security Wireless Local Area Network (WLAN) A WLAN, or Wireless Local Area Network, is a type of network that allows devices to connect to the internet or to each other wirelessly, using a wireless router or access point. WLANs are commonly used in homes, offices, and public spaces such as coffee shops and airports. Types of Wireless Security Wireless networks are vulnerable to a range of security threats, such as unauthorized access, data theft, and interference from other devices. To mitigate these risks, there are several types of wireless security, including: A. Wired Equivalent Privacy (WEP) Wired Equivalent Privacy (WEP) was one of the first forms of wireless security, and it was designed to provide a similar level of security to that of a wired network. WEP uses a static encryption key, which is shared between the access point and clients, to encrypt data transmitted over the wireless network. However, WEP has been found to have several weaknesses, such as a limited key length and a lack of proper authentication mechanisms. As a result, WEP is no longer considered secure and should not be used for protecting modern wireless networks. B. Wi-Fi Protected Access (WPA) Wi-Fi Protected Access (WPA) was developed to address the weaknesses of WEP. WPA uses a dynamic encryption key, which is generated for each transmission, to encrypt data transmitted over the wireless network. WPA also includes an authentication mechanism, known as the Temporal Key Integrity Protocol (TKIP), to prevent unauthorized access to the network. TKIP provides per-packet key mixing and a message integrity check to prevent attacks such as replay attacks. C. Wi-Fi Protected Access II (WPA2) Wi-Fi Protected Access II (WPA2) is an improved version of WPA, which was developed to provide a higher level of security for wireless networks. WPA2 uses the Advanced Encryption Standard (AES) to encrypt data transmitted over the network, which provides stronger encryption compared to WPA. WPA2 also includes improved authentication mechanisms, such as the 802.1X standard, to provide stronger protection against unauthorized access. D. Wi-Fi Protected Access III (WPA3) Wi-Fi Protected Access III (WPA3) is the latest standard for wireless security, which was released in 2018. WPA3 provides stronger encryption and improved authentication mechanisms compared to previous versions of WPA. WPA3 introduces a new encryption protocol, called the Simultaneous Authentication of Equals (SAE), which provides stronger protection against attacks such as dictionary attacks and brute force attacks. WPA3 also includes improved encryption for open networks, which are networks without a password, to provide better privacy for users. How Wireless Security Works Wireless security works by encrypting the data transmitted between devices and the access point. The encryption algorithm used depends on the type of wireless security in place. For example, WEP uses a static encryption key that is shared between the access point and clients, while WPA and WPA2 use a dynamic key that changes for each transmission. In addition to encryption, wireless security also involves authentication, which ensures that only authorized devices can access the network. This is typically accomplished through the use of usernames and passwords, or by using a technology such as 802.1X, which requires clients to present digital certificates to the access point before being granted access. By understanding WLANs and wireless security, you will be better equipped to use aircrack-ng to assess the security of your own wireless networks and identify any potential vulnerabilities. Wireless Network Scanning Introduction to Network Scanning Network scanning is the process of identifying active network devices, such as access points and clients, on a network. Network scanning is a crucial step in the process of assessing the security of a wireless network, as it provides information about the devices on the network, their configurations, and the type of security in place. Understanding the Output of Network Scanning The output of network scanning can include information such as the Media Access Control (MAC) address of the device, its IP address, the type of wireless security in use, the type of encryption being used, and the strength of the signal. This information can be used to identify potential vulnerabilities in the network, such as the use of outdated security protocols or weak encryption algorithms. How to Perform Wireless Network Scanning with Aircrack-ng Aircrack-ng is a popular suite of tools for wireless network security, which includes a network scanning tool called airodump-ng. Airodump-ng can be used to perform wireless network scanning and collect information about the devices on a network. To perform wireless network scanning with aircrack-ng, you will need to first set up the environment as described in Part II of this tutorial. Once the environment is set up, you can use the following commands to perform wireless network scanning: # Start the wireless card in monitor modesudo airmon-ng start wlan0# Perform network scanning using airodump-ngsudo airodump-ng wlan0mon The output of the airodump-ng command will display information about the devices on the network, including their MAC addresses, signal strength, and the type of wireless security in use. This information can then be used to further assess the security of the network and identify any potential vulnerabilities. Cracking WEP Networks A. Understanding WEP Security Wired Equivalent Privacy (WEP) is a form of wireless security that was designed to provide a similar level of security to that of a wired network. WEP uses a shared encryption key to encrypt data transmitted over the wireless network. However, WEP has several weaknesses, such as a limited key length and a lack of proper authentication mechanisms, which make it relatively easy to crack. As a result, WEP is no longer considered secure and should not be used for protecting modern wireless networks. How to Capture Packets with Aircrack-ng In order to crack WEP passwords, it is necessary to capture enough packets from the wireless network to analyze. The process of capturing packets from a wireless network is called packet sniffing. Aircrack-ng includes a packet sniffing tool called airodump-ng, which can be used to capture packets from a WEP network. To capture packets with aircrack-ng, you will need to first set up the environment as described in Part II of this tutorial. Once the environment is set up, you can use the following commands to capture packets: # Start the wireless card in monitor modesudo airmon-ng start wlan0# Capture packets using airodump-ngsudo airodump-ng wlan0mon -c [channel number] -w [capture file name] --bssid [BSSID of target network] How to Crack WEP Passwords with Aircrack-ng Once you have captured enough packets from the WEP network, you can use aircrack-ng to crack the password. Aircrack-ng includes a tool called aircrack-ng, which can be used to crack WEP passwords. To crack WEP passwords with aircrack-ng, you can use the following command: # Crack the WEP password using aircrack-ngsudo aircrack-ng [capture file name].cap Aircrack-ng will analyze the captured packets and attempt to crack the WEP password. If the password is successfully cracked, aircrack-ng will display the password in plain text. Please note that cracking WEP passwords is illegal in many jurisdictions, and you should only attempt to crack passwords on networks for which you have explicit permission to do so. Cracking WPA/WPA2 Networks Understanding WPA/WPA2 Security Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) are forms of wireless security that were designed to provide stronger security than WEP. WPA/WPA2 use a combination of a shared encryption key and a user password to encrypt data transmitted over the wireless network. WPA/WPA2 are considered much more secure than WEP, but they are still vulnerable to certain types of attacks, such as dictionary attacks. Dictionary Attack with Aircrack-ng A dictionary attack is a type of attack that uses a list of words (dictionary) to try to crack a password. Aircrack-

ng includes a tool called aircrack-ng, which can be used to perform a dictionary attack on WPA/WPA2 networks. To perform a dictionary attack with aircrack-ng, you will need to capture enough packets from the wireless network and have a dictionary file. You can use the following command to perform a dictionary attack with aircrack-ng: # Perform a dictionary attack with aircrack-ngsudo aircrack-ng [capture file name].cap -w [dictionary file name].txt Aircrack-ng will analyze the captured packets and attempt to crack the WPA/WPA2 password using the words in the dictionary. If the password is found in the dictionary, aircrack-ng will display the password in plain text. How to Crack WPA/WPA2 Passwords with Aircrack-ng In addition to dictionary attacks, aircrack-ng can also be used to perform a brute force attack on WPA/WPA2 networks. A brute force attack is a type of attack that tries every possible combination of characters until the password is found. Brute force attacks can take a very long time, but they are guaranteed to find the password if it exists in the character set being used. To perform a brute force attack with aircrack-ng, you can use the following command: # Perform a brute force attack with aircrack-ngsudo aircrack-ng [capture file name].cap -a 2 -b [BSSID of target network] -l [output file name].txt Aircrack-ng will analyze the captured packets and attempt to crack the WPA/WPA2 password using a brute force attack. If the password is successfully cracked, aircrack-ng will display the password in plain text. Please note that cracking WPA/WPA2 passwords is illegal in many jurisdictions, and you should only attempt to crack passwords on networks for which you have explicit permission to do so. Conclusion In conclusion, aircrack-ng is a powerful tool for wireless network security analysis and cracking. With the knowledge and understanding of wireless security, network scanning, and cracking WEP and WPA/WPA2 passwords with aircrack-ng, you can now assess the security of your own wireless network and identify vulnerabilities. However, its important to use aircrack-ng for educational purposes only and never for illegal activities. Remember to always respect the security of others and their networks, and to always follow the laws and regulations regarding wireless network security. With the right knowledge and tools, we can all work together to ensure the security and privacy of our wireless networks. If you want to know how to hack WiFi access point just read this step by step aircrack-ng tutorial, run the verified commands and hack WiFi password easily.With the help a these commands you will be able to hack WiFi AP (access points) that use WPA/WPA2-PSK (pre-shared key) encryption.The basis of this method of hacking WiFi lies in capturing of the WPA/WPA2 authentication handshake and then cracking the PSK using aircrack-ng.How to hack WiFi the action plan:Download and install the latest aircrack-ngStart the wireless interface in monitor mode using the airmon-ngStart the airodump-ng on AP channel with filter for BSSID to collect authentication handshake[Optional] Use the aireplay-ng to deauthenticate the wireless clientRun the aircrack-ng to hack the WiFi password by cracking the authentication handshake1. Aircrack-ng: Download and InstallThe Latest Version Only: If you really want to hack WiFi do not install the old aircrack-ng from your OS repositories. Download and compile the latest version manually.Install the required dependencies:$ sudo apt-get install build-essential libssl-dev libnl-3-dev pkg-config libnl-genl-3-devDownload and install the latest aircrack-ng (current version):$ wget -O - | tar -xz$ cd aircrack-ng-1.2-rc4$ sudo make$ sudo make installEnsure that you have installed the latest version of aircrack-ng:$ aircrack-ng --help Aircrack-ng 1.2 rc4 - (C) 2006-2015 Thomas d'Otreppe . Airmon-ng: Monitor ModeNow it is required to start the wireless interface in monitor mode.Monitor mode allows a computer with a wireless network interface to monitor all traffic received from the wireless network.What is especially important for us monitor mode allows packets to be captured without having to associate with an access point.Find and stop all the processes that use the wireless interface and may cause troubles:$ sudo airmon-ng check killStart the wireless interface in monitor mode:$ sudo airmon-ng start wlan0InterfaceChipsetDriverwlan0Intel 6235iwlwifi - [phy0](monitor mode enabled on mon0)In the example above the airmon-ng has created a new wireless interface called mon0 and enabled on it monitor mode.So the correct interface name to use in the next parts of this tutorial is the mon0.3. Airodump-ng: Authentication HandshakeCool Tip: Want to have some fun? Create a Linux fork bomb! One small string that is able to hang the whole system! Read more Now, when our wireless adapter is in monitor mode, we have a capability to see all the wireless traffic that passes by in the air.This can be done with the airodump-ng command:$ sudo airodump-ng mon0All of the visible APs are listed in the upper part of the screen and the clients are listed in the lower part of the screen:CH 1][Elapsed: 20 s][2014-05-29 12:46BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID00:11:22:33:44:55 -48 212 1536 66 1 54e WPA2 CCMP PSK CrackMe66:77:88:99:00:11 -64 134 345 34 1 54e WPA2 CCMP PSK SomeAPBSSID STATION PWR Rate Lost Frames Probe00:11:22:33:44:55 AA:BB:CC:DD:EE:FF -44 0 - 1 114 5600:11:22:33:44:55 GG:HH:II:JJ:KK:LL -78 0 - 1 0 166:77:88:99:00:11 MM:NN:OO:PP:QQ:RR -78 2 - 32 0 1Start the airodump-ng on AP channel with the filter for BSSID to collect the authentication handshake for the access point we are interested in:$ sudo airodump-ng -c 1 --bssid 00:11:22:33:44:55 -w WPAcrack mon0 --ignore-negative-oneOptionDescription-cThe channel for the wireless network--bssidThe MAC address of the access point-wThe file name prefix for the file which will contain authentication handshakemon0The wireless interface--ignore-negative-oneFixes the fixed channel : -1 error messageNow wait until airodump-ng captures a handshake.If you want to speed up this process go to the step #4 and try to force wireless client reauthentication.After some time you should see the WPA handshake: 00:11:22:33:44:55 in the top right-hand corner of the screen.This means that the airodump-ng has successfully captured the handshake:CH 1][Elapsed: 20 s][2014-05-29 12:46 WPA handshake: 00:11:22:33:44:55BSSID PWR Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID00:11:22:33:44:55 -48 212 1536 66 1 54e WPA2 CCMP PSK CrackMeBSSID STATION PWR Rate Lost Frames Probe00:11:22:33:44:55 AA:BB:CC:DD:EE:FF -44 0 - 1 114 564. Aireplay-ng: Deauthenticate ClientCool Tip: Want to stay anonymous? Learn how to use PROXY on the Linux command line. Read more If you cant wait till airodump-ng captures a handshake, you can send a message to the wireless client saying that it is no longer associated with the AP.The wireless client will then hopefully reauthenticate with the AP and well capture the authentication handshake.Send deauth to broadcast:$ sudo aireplay-ng --deauth 100 -a 00:11:22:33:44:55 mon0 --ignore-negative-oneSend directed deauth (attack is more effective when it is targeted):$ sudo aireplay-ng --deauth 100 -a 00:11:22:33:44:55 -c AA:BB:CC:DD:EE:FF mon0 --ignore-negative-oneOptionDescription--deauth 100The number of de-authenticate frames you want to send (0 for unlimited)-aThe MAC address of the access point-cThe MAC address of the clientmon0The wireless interface--ignore-negative-oneFixes the fixed channel : -1 error messageCool Tip: Need to hack WiFi password? Dont wast your time! Use John the Ripper the fastest password cracker! Read more 5. Aircrack-ng: Hack WiFi PasswordUnfortunately there is no way except brute force to break WPA/WPA2-PSK encryption.To hack WiFi password, you need a password dictionary.And remember that this type of attack is only as good as your password dictionary.You can download some dictionaries from here.Crack the WPA/WPA2-PSK with the following command:$ aircrack-ng -w wordlist.dic -b 00:11:22:33:44:55 WPAcrack.capOptionDescription-wThe name of the dictionary file-bThe MAC address of the access pointWPAcrack.capThe name of the file that contains the authentication handshake Aircrack-ng 1.2 beta3 r2393 [00:08:11] 548872 keys tested (1425.24 k/s) KEY FOUND! [987654321] Master Key : 5C 9D 3F B6 24 3B 3E 0F F7 C2 51 27 D4 D3 0E 97 CB F0 4A 28 00 93 4A 8E DD 04 77 A3 A1 7D 15 D5 Transient Key : 3A 3E 27 5E 86 C3 01 A8 91 5A 2D 7C 97 71 D2 F8 AA 03 85 99 5C BF A7 32 5B 2F CD 93 C0 5B B5 F6 DB A3 C7 43 62 F4 11 34 C6 DA BA 38 29 72 4D B9 A3 11 47 A6 8F 90 63 46 1B 03 89 72 79 99 21 B3 EAPOL HMAC : 9F B5 F4 B9 3C 8B EA DF A0 3E F4 D4 9D F5 16 62Cool Tip: Password cracking often takes time. Combine aircrack-ng with John The Ripper to pause/resume cracking whenever you want without loosing the progress! Read more Was it useful? Share this post with the world!

How to download aircrack ng. How to aircrack ng kali. How to use aircrack ng. How to install aircrack ng on ubuntu. How to use aircrack ng on windows 10. How to install aircrack ng. How to install aircrack ng in termux.