CHAPTER 1

UNDERSTANDING WIRELESS NETWORKS

A wireless network is a data communication system that uses radio frequency and wireless media to communicate by sending and receiving data through the air. They use electromagnetic waves to interconnect an individual point to another without relying on any bodily construction (most of the network). By using wireless networking we can avoid the expensive method of introducing cables into building or as connection between numerous equipment that need to be connected, many households, business or telecommunication networks follow this method. The wireless networks are used in different field such as satellite communication networks, cell phone networks, wireless sensor network and wireless local area network (WLANS). Wireless systems have become increasingly popular, used at many households or industries for convenience. Vulnerabilities exist because of weaknesses in protocols. For instance WEP is vulnerable because of the encryption algorithms are employed. A general configuration of a home network is show in the Figure 1-1.

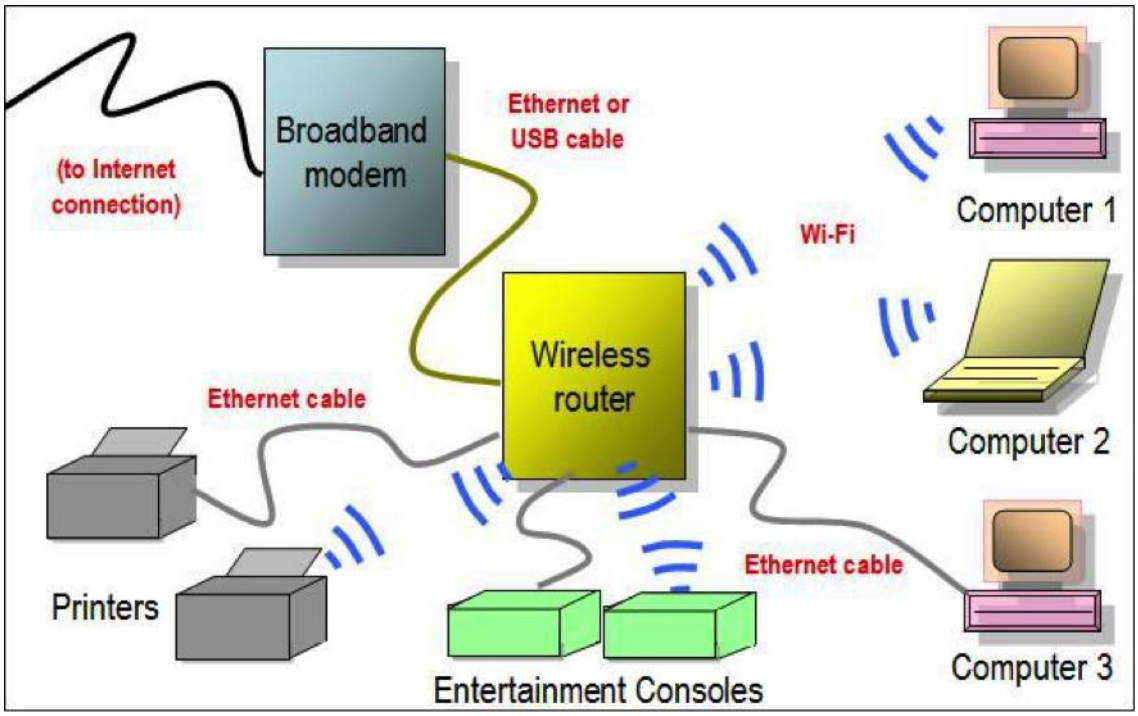

Figure 1-1: General wireless network configuration.

To understand the concepts of wireless networks and vulnerabilities let us see some of the concept.

1.1 UNDERSTANDING DIFFERENT TYPES OF WIRELESS NETWORKS

There are five basic types of wireless networks.

Peer-To-Peer Networks or wireless PAN

In this type of network, every computer can communicate directly with the other computers on the same network without going through an access point. They can share files and printers in this manner. However, they may not be able to access wired LAN resources unless one of the computers acts as a bridge to the wired LAN using special software.

Extension to a Wired Network or wireless LAN

An extension to a wired network can be obtained by placing access points between the wired network and the wireless devices. With this type of network, the access point acts like a hub, providing connectivity for the wireless computers on its system. It can connect a wireless LAN to a wired LAN, allowing wireless computer access to LAN resources such as file servers or existing Internet connections. There are both software and hardware access points. Software access points (SAPs) can be connected to the wired network and run on a computer equipped with a wireless network interface card. Hardware access points (HAPs) provide comprehensive support to most wireless features

Multiple Access Points

This type of network consists of computers connected wirelessly by using multiple access points. If a single large area cannot be covered by a single access point, multiple access points or extension points can be established. Although extension point capability has been developed by some manufacturers, it is not defined in the wireless standard. When using multiple access points, each access point’s coverage area needs to overlap another point’s coverage area. This provides users the ability to move around seamlessly using a feature called roaming. Some manufacturers develop extension points that act as wireless relays, extending the range of a single access point. Multiple extension points can be strung together to provide wireless access to locations far from the central access point.

LAN-To-LAN Wireless Network or wireless MAN

Access points provide wireless connectivity to local computers, and local computers on different networks can be interconnected. All hardware access points have the capability of being interconnected with other hardware access points. However, interconnecting LANs over wireless connections can be a complex task.

Cellular network

A cellular network or mobile network is a wireless network distributed over land areas called cells. There are fixed transceiver for each cell, also known as base station. Each cell uses unique radio frequencies to avoid and interferences from their neighbouring cells.

1.2 UNDERSTANDING DIFFERENT WIRELESS STANDARDS

IEEE (Institute of Electrical and Electronics Engineers) standard 802.11 has grown from a standard of infrared communication to cover most wireless communications used today. It has several issues, such as security, roaming among multiple access points, and quality of service. Therefore, there are many extensions of this standard for different uses. The following are some of the extensions:

Wireless Standard: 802.11a

IEEE 802.11a has the following features:

• Works at 40 MHz in the 5-GHz range

• Theoretical transfer rates up to 54 Mbps

• Actual transfer rates of approximately 26.4 Mbps

• Limited in use because it is almost a line-of-sight transmittal that requires multiple WAPs (wireless access points)

• Uses a modulation technique called coded orthogonal frequency-division multiplexing (COFDM)

• Cannot operate in same range as 802.11b/g

• Absorbed more easily than other wireless implementations

• Overcomes the challenge of indoor radio frequencies

• Uses a single-carrier, delay-spread system

Wireless Standard: 802.11b

IEEE 802.11b was used in most home and office networks before 802.11g. It has the following features:

• Operates at 20 MHz in the 2.4-GHz range

• Theoretical transfer rates up to 11 Mbps

• Actual transfer rates of 5.9 Mbps over TCP, 7.1 Mbps over UDP

• Transmits up to 8 km in a city environment

• Not as easily absorbed as 802.11a

• Can cause or receive interference from the following: Microwave ovens, Wireless telephones, Other wireless appliances operating in the same frequency

Wireless Standard: 802.11g

IEEE 802.11g is replacing 802.11b in most applications. Its features include the following:

• Operates at the same frequency range as 802.11b

• Theoretical transfer rates up to 54 Mbps

• Actual transfer rates of approximately 24.7 Mbps

• Backward compatible with 802.11b

• Same limitations as 802.11b

• May suffer significant decrease in network speeds if entire network is not upgraded from 802.11b

Wireless Standard: 802.11i

IEEE 802.11i uses improved encryption for networks that use the 802.11a, 802.11b, and 802.11g standards. Its security features include the following:

• 802.1x for authentication (EAP and authentication server)

• Robust Security Network (RSN) to keep track of associations

• Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) to provide confidentiality, integrity, and origin authentication

Wireless Standard: 802.11n

IEEE 802.11n is the next-generation Wi-Fi standard developed by Task Group N of the IEEE. This standard merges the use of multiple antennas, more advanced encoding, and optional spectrum doubling to attain data rates of up to 600 Mbps. 802.11n has the following basic features:

• Based on multiple-in/multiple-out (MIMO) technology

• Expected increase of throughput to potentially well over 100 Mbps

• Specifies improvement to the physical layer and medium access control layer

• Improved radio technology to increase physical data transfer

• New methods to implement effective management of improved physical-layer performance modes
• Improved data transfer efficiency to reduce performance impact of physical-layer headers and radio turnaround delays that adversely affect the physical transfer rate Wireless Standard: 802.15.1 (Bluetooth)

IEEE 802.15.1, commonly called Bluetooth, is used for wireless personal area networks, or WPANs. It is used in short-range, low-power, low-cost small networks such as the connection between a cellular phone and headset, or computer and mouse. Bluetooth specifies standards on the physical layer and data-link layer of the OSI model with the following four sublayers:

1. RF layer 2. Baseband layer 3. Link manager 4. Logical Link Control and Adaptation Protocol (L2CAP) Wireless Standard: 802.16 (WiMAX)

WiMAX (Worldwide Interoperability for Microwave Access) is a communication system designed to support point-to-multipoint wireless broadband access. It provides high-speed mobile Internet access with ranges of up to 30 miles and speeds of up to 75 Mbps. There are two types of WiMAX: fixed and mobile. Fixed WiMAX is similar to a cable or DSL modem service and delivers wireless last-mile access (the connection between a communications provider and a customer) for fixed broadband services. Mobile WiMAX supports both fixed and mobile applications.

1.3 UNDERSTANDING SSID

A service set identifier (SSID) is a unique identifier that names a particular WLAN. It is used to establish and maintain wireless connectivity. SSIDs act as a single shared password between access points and clients. Security concerns arise when the default values are not changed since these networks can then be more easily compromised. An unsecure access mode station communicates with access points by broadcasting the configured SSID, a blank SSID, or an SSID configured as "any." Because an SSID is a unique name given to a WLAN, all devices and access points present in the WLAN must use the same SSID. It is necessary for any device that wants to join the WLAN to give the unique SSID. Unfortunately, SSID does not provide security to WLAN, as it can be sniffed in plaintext from packets. An SSID can be up to 32-characters long. The following are some common default SSIDs: Comcomcom, Default SSID, Intel, Linksys, Wireless, WLAN (usually set by the manufacturers).

SSID will not add protection to the network but rather gives away few hints to the attacker to gain access to your network. Most people who are not aware of the network vulnerabilities fail to change the default SSIDs set by their manufactures. Attackers will see this and assume the target has not spent much time securing the network.

Once the attacker knows about SSID of a particular network he can simply sniff packets over the network and get mac address of the connected devices. This opens paths to other attacks, can gain access by DE authenticating the actual use, he can simply impersonate a station by MAC spoofing (chancing of MAC address of the machine) and enter the network.

1.4 UNDERSTANDING WIRELESS ACCESS POINT

An access point is a piece of wireless communications hardware that creates a central point of wireless connectivity. Similar to a hub, the access point is a common connection point for devices in a wireless network. APs are necessary for strong wireless security. They are also used for increasing the physical range of services. The range of the APs is increased with the help of repeaters, which amplify the network's radio signals. In a corporate setting, wireless access points must be deployed

and managed in common areas of the campus. They must also be coordinated with the telecommunications and network managers.

1.5 UNDERSTANDING WIRELESS MODES

In the process of penetration testing or cracking passwords, we will make use of some advanced modes of the wireless device. Two of these features, monitor and master mode will help us in capturing the traffic and set up virtual rogue access point respectively.

The managed mode

This is the default operating mode for all the domestically used wi-fi cards. In this mode, the wifi adapter is capable of receiving packets only from SSIDs that it is associated with. In this mode, the card is given an IP address and is actively associated to the access point. For example, if a card is associated with an SSID "1", the card would filter all the other packets related to other SSIDs.

The monitor mode

The support for this mode is essential if you want to be able to capture all the traffic on the wireless spectrum.In this mode, the card will not interact with any of the wireless devices around but allows us to sniff and capture the packets in the network for analysing, cracking or decryption.

The master mode

This mode allows us the wireless card to behave as a wireless access point. As a penetration tester, it is common for us to want to emulate an access point where we control the configuration and, more importantly, have visibility about all of the traffic traversing the wireless device. This mode is required for setting up virtual access point or rogue access points.

The ad-hoc mode

This mode is rarely used since the majority of wireless networks participate in infrastructure mode and host clients directly. This mode is used only when an access point is not in place and clients are

participating in a peer-to-peer mesh. The lack of an access point usually restricts the functionality and usefulness of the connecting clients and hence is rarely used in modern deployments.

CHAPTER 2

WIRELESS SECURITY

2.1 UNDERSTANDING WIRED EQUIVALENT PRIVACY

Wired Equivalent Privacy (WEP) is a security protocol designed to provide a WLAN with a level of security equivalent to the security usually expected in wired LAN. Wired LANs have physical security applied to stop unauthorized access to a network. In a wireless LAN, the network can be accessed without physically connecting to the LAN. Therefore, IEEE utilizes an encryption mechanism at the data-link layer for minimizing unauthorized access. This is accomplished by encrypting data with the symmetric RC4 encryption algorithm.

Role of WEP in Wireless communication

WEP depends on a secret shared key to protect the communication from eavesdropping and minimizes unauthorised access. The shared key is used by the access point and the client to encrypt the data. An integrity check is performed to ensure that packets are not altered after transmission. 802.11 WEP encrypts data only between 802.11 stations.

Main Goals of WEP

- Confidentiality: It prevents link-layer eavesdropping
- Access Control: It determines who may access the network and who may not
- Data Integrity: It protects the change of data from a third user
- Efficiency

WEP Flaws

Some basic flaws undermine WEP's ability to protect against a serious attack, including the following:

- No defined method for encryption key distribution.

- Preshared keys are set once at installation and are rarely (if ever) changed.
- It is easy to determine the number of plaintext messages encrypted with the same key.
- Use of RC4, which was designed to be a one-time cipher and not intended for multiple message use.
- The preshared key is rarely changed.
- An attacker monitors the traffic and determines the different ways to decipher the plaintext message.
- With knowledge of the cipher text and the plaintext, an attacker can compute the key.
- Attackers can analyse the traffic from passive data captures and crack the WEP keys with the help of tools such as AirSnort, WEPCrack, and dweputils.
- Key generators that are used by different vendors are vulnerable.
- Key scheduling algorithms are also vulnerable to attack.

How WEP Works

WEP encryption follows the following procedure while encrypting the payload:

- A 32-bit Integrity Check Value (ICV) is calculated for the frame data.
- The ICV is appended to the end of the frame data.
- A 24-bit Initialization Vector (IV) is generated and appended to the WEP encryption key.
- The combination of IV and the WEP key is used as the input to RC4 algorithm to generate a key stream. The length of the stream should be same as the combination of ICV and data.
- The key stream is bit-wise XORed with the combination of data and ICV to produce the encrypted data that is sent between the client and the AP.
- The IV is added to the encrypted combination of data and ICV along with other fields, to generate a MAC frame.

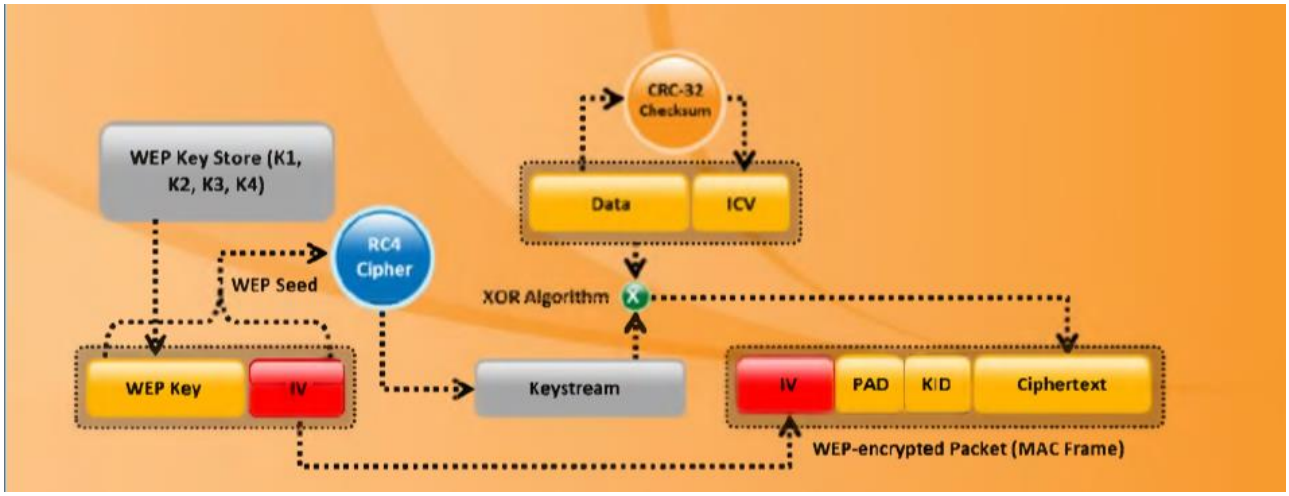

Figure 2-1: WEP encryption process

2.2 UNDERSTANDING WI-FI PROTECTED ACCESS (WPA)

WPA stands for Wi-Fi protected access. It is compatible with the 802.11i security standards. The major drawback for WEP encryption is that it still uses a static encryption key. The attacker can exploit this weakness by using tools that are freely available on the Internet. The Institute of Electrical and Electronics Engineers (IEEE) has defined "an expansion to the 802.11 protocols that can allow for increased security." Nearly every Wi-Fi company has decided to employ a standard for increased security called Wi-Fi Protected Access. The security issue concerning initialization vectors (IVs) is taken care of by WPA. The level of encryption done in WPA is higher compared to WEP, this is because the messages are passed through Message Integrity Check (MIC) using the Temporal Key Integrity Protocol (TKIP).

WPA vulnerabilities

WPA is secure than the WEP protocol but still has some vulnerabilities. WPA is not immune to Denial-of-service attacks. The only way to avoid this attack is to change to WEP until the attack subsides. And the WPA can be cracked with dictionary attacks if the preshared 14-character key is a real word.

WEP, WPA AND WPA2 COMPARISION

WEP's main goal was to provide security to data in level equivalent to wired connections but it fails to meet any of its goals. WPA fixes most of the problems that are present in WEP but it in turn raised new vulnerabilities. WPA2 is expected to make wireless networks as secure as wired networks.

How WPA works

- Temporal encryption key, transmit address, and TKIP sequence counter (TSC) is used as input to RC4 algorithm to generate a key stream.
- MAC Service Data Unit (MSDU) and message integrity check (MIC) are combined using the Michael algorithm.
- The combination of MSDU and MIC is fragmented to generate MAC Protocol Data Unit (MPDU).
- A 32-bit Integrity Check Value (ICV) is calculated for the MPDU.
- The combination of MPDU and ICV is bitwise XORed with a key stream to produce the encrypted data.
- The IV is added to the encrypted data to generate MAC frame.

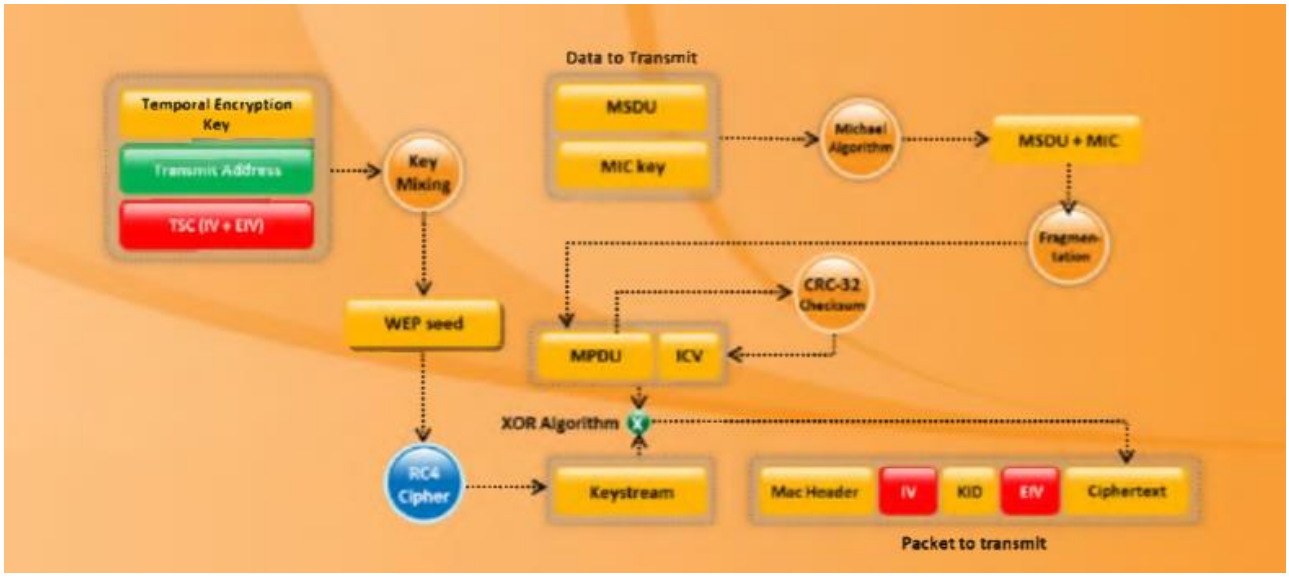

Figure 2-2: Working process of wpa

2.3 CRYPTOGRAPHIC DESCRIPTION OF AES

The National Institute of Standards and Technology (NIST) started development of AES in 1997 when it announced the need for a successor algorithm for the Data Encryption Standard (DES), which was starting to become vulnerable to brute-force attacks.

This new, advanced encryption algorithm would be unclassified and had to be "capable of protecting sensitive government information well into the next century," according to the NIST announcement of the process for development of an advanced encryption standard algorithm. It was intended to be easy to implement in hardware and software, as well as in restricted environments (for example, in a smart card) and offer good defences against various attack techniques.

AES features

The selection process for this new symmetric key algorithm was fully open to public scrutiny and comment; this ensured a thorough, transparent analysis of the designs submitted.

NIST specified the new advanced encryption standard algorithm must be a block cipher capable of handling 128 bit blocks, using keys sized at 128, 192, and 256 bits; other criteria for being chosen as the next advanced encryption standard algorithm included:

Security: Competing algorithms were to be judged on their ability to resist attack, as compared to other submitted ciphers, though security strength was to be considered the most important factor in the competition.

Cost: Intended to be released under a global, nonexclusive and royalty-free basis, the candidate algorithms were to be evaluated on computational and memory efficiency.

Implementation: Algorithm and implementation characteristics to be evaluated included the flexibility of the algorithm; suitability of the algorithm to be implemented in hardware or software; and overall, relative simplicity of implementation.

2.4 CRYPTOGRAPHIC DESCRIPTION OF SHA1

CHAPTER 3

WIRELESS PACKET ANALYSIS

CHAPTER 4

VULNERABILITIES AND EXPLOITING NETWORK

4.1 COMMON VULNERABILITIES AND EXPOSURE (CVE)

CVE (Common vulnerability and Exposures) is a list of common vulnerabilities and exposures that aim to provide common names for publicly know problems. The fundamental objective of CVE is to make it easier to share data across separate vulnerability platforms with this “common enumeration”. The MITRE Corporation maintains the CVE site and assures that CVE serves the public interest.

CVEs are identified by a unique identifier also known as CVE identifier. Each CVE identifier includes the following:

- CVE identifier number (i.e., "CVE-2004-0459").
- Indication of "entry" or "candidate" status.
- Brief description of the security vulnerability or exposure.
- Any pertinent references (i.e., vulnerability reports and advisories or OVAL-ID).
- CVE Identifiers are used by information security product/service vendors and researchers as a standard method for identifying vulnerabilities and for cross-linking with other repositories that also use CVE Identifiers.

Vulnearability

An information security "vulnerability" is a mistake in software that can be directly used by a hacker to gain access to a system or network.

Exposure

An information security exposure is a mistake in software that allows access to information or capabilities that can be used by a hacker as a stepping-stone into a system or network.

“cve.mitre.org” website has the details of CVE and also the provision for requesting an ID for a CVE found. The actual database of all the CVE is maintained by National Vulnerability Database (NVD).

4.2 COMMON VULNERABILITIRS IN WIRELESS NETWORK

Here are some CVEs related to wireless networks.

4.2.1 CVE-2004-0459

The Clear Channel Assessment (CCA) algorithm in the IEEE 802.11 wireless protocol, when using DSSS transmission encoding, allows remote attackers to cause a denial of service via a certain RF signal that causes a channel to appear busy (aka "jabber"), which prevents devices from transmitting data.

Impact: A remote user with a physical layer device within range of a wireless local area network (WLAN) can cause the target WLAN to become unavailable.

Solution: No solution was available at the time of this entry. AUSCERT reports that "at this time a comprehensive solution, in the form of software or firmware upgrade, is not available for retrofit to existing devices."

This particular vulnerability has a base score of 5 points and exploitability score of 10.0 according to NVD.

4.2.2 CVE-2007-4928

The AXIS 207W stores a WEP or WPA key in clear text in the configuration file, which might allow local users to obtain sensitive information.

Impact: An attack can be made locally to steal sensitive information.

Solution: No solution or patch file is available to eliminate this vulnerability.

This particular vulnerability has a base score of 4.9 points and exploitability score of 3.9 according to NVD.

4.3 HACK WIRELESS NETWORKS

Techniques to Detect Open Wireless Networks

• Warwalking: walking around to look for open wireless networks.

• Wardriving: driving through a neighbourhood with a wireless-enabled notebook computer, mapping houses and businesses that have wireless access points.

• Warflying: involves flying around in an aircraft looking for open wireless networks.

• Warchalking: This term comes from whackers who use chalk to place a special symbol on a sidewalk or another surface to indicate a nearby wireless network that offers Internet access.

There are different attacks that can be performed based on the situation and requirements. Here are some of the attacks:

MAN-IN-THE-MIDDLE ATTACK (MITM)

There are two types of MITM attacks: Manipulating and Eavesdropping.

Eavesdropping is easy in wireless networks compared to a wired since the data travels in the air in the form of radio waves it is very easy to catch the data if provided the attacker has the right equipment.

Manipulating is a bit complex job compared to eavesdropping. Manipulation occurs if the attacker is able to tamper the traffic to and from the victim. In addition, an attacker can intercept packets with encrypted data and change the destination address in order to forward these packets across the Internet.

The Figure 4-1 below gives an overview of how the MITM is done.

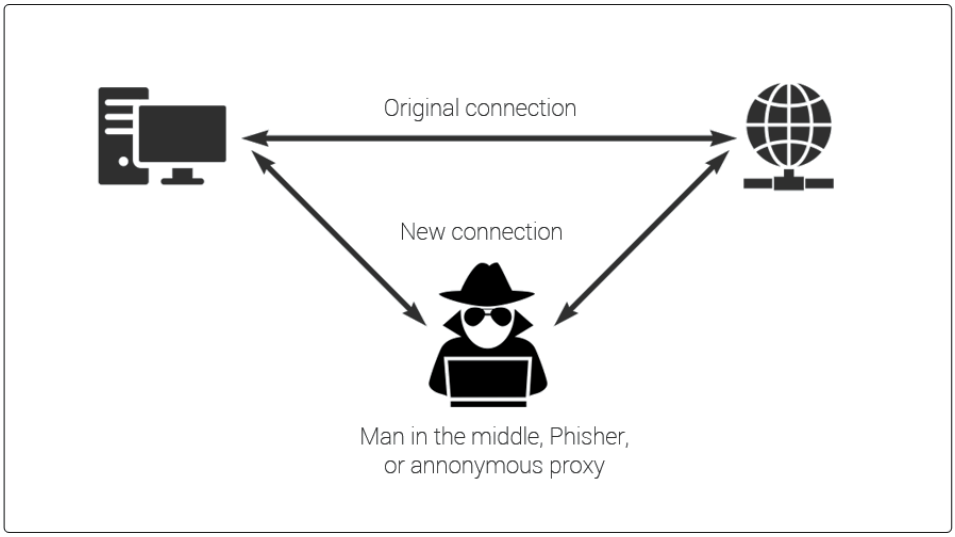

Figure 4-1: Man in the middle attack

DENIAL-OF-SERVICE ATTACKS

This is an attack that is used to shut down or crash the machine or network. This is done by flooding the target with huge loads of traffic or something that trigger a crash. By doing this the attackers makes it inaccessible to its intended users.

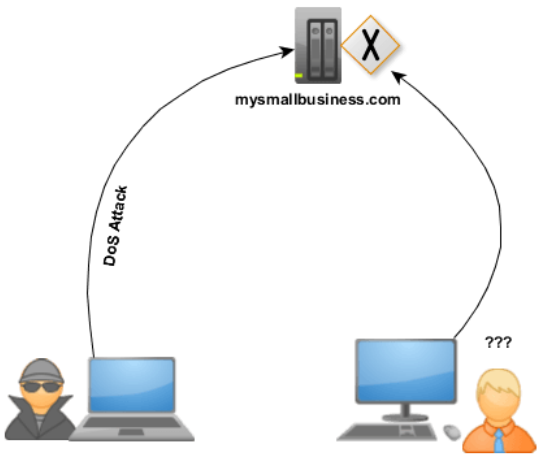

Figure 4-2: Denial of service attack.

A severe disadvantages with this is attack is there should be proper infrastructure to execute the attack and there is a possibility that the victim can trace the attack back to the attacker. Both these problems are solved by Distribute Denial of service attack (DDOS).

A Distributed Denial of Service (DDOS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. The main is difference between DOS and DDOS attacks is the usage of multiple sources in DDOS attacks. This makes the process of tracing the attacker difficult or in some cases impossible. The Figure 4-3 shows gives an overview how the attack is done.

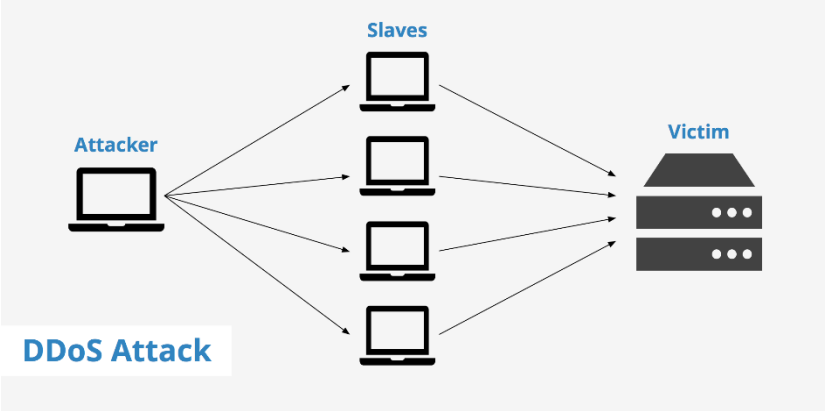

Figure 4-3: DDoS attack overview.

There are a different attacks available in DDOS/DOS attacks, here are 5 attacks summarised:

SYN flood

A SYN flood is a type of DOS attack in which an attacker sends a series of SYN requests to a target's system in an attempt to use vast amounts of server resources to make the system unresponsive to legitimate traffic.

Teardrop attacks

A teardrop attack involves the hacker sending broken and disorganized IP fragments with overlapping, over-sized payloads to the victims machine. The intention is to obviously crash operating systems and servers due to a bug in the way TCP/IP fragmentation is re-assembled. All operating systems many types of servers are vulnerable to this type of DOS attack, including Linux.

Low-rate Denial-of-Service attacks

Don't be fooled by the title, this is still a deadly DoS attack! The Low-rate DoS (LDoS) attack is designed to exploit TCP's slow-time-scale dynamics of being able to execute the retransmission time-out (RTO) mechanism to reduce TCP throughput. In short, a hacker can create a TCP overflow by repeatedly entering a RTO state through sending high-rate and intensive bursts – whilst at slow RTO time-scales. The TCP throughput at the victim node will be drastically reduced while the hacker will have low average rate thus making it difficult to be detected.

Internet Control Message Protocol (ICMP) flood

Internet Control Message Protocol (ICMP) is a connectionless protocol used for IP operations, diagnostics, and errors. An ICMP Flood – the sending of an abnormally large number of ICMP packets of any type (especially network latency testing "ping" packets) – can overwhelm a target server that attempts to process every incoming ICMP request, and this can result in a denial-of-service condition for the target server.

Peer-to-peer attacks

A peer-to-peer (P2P) network is a distributed network in which individual nodes in the network (called "peers") act as both suppliers (seeds) and consumers (leeches) of resources, in contrast to the centralized client–server model where the client server or operating system nodes request access to resources provided by central servers.

HIJACKING AND MODIFYING A WIRELESS NETWORK

As TCP/IP packets go through switches, routers, and APs, each device looks at the destination IP address and compares it with the IP addresses it knows to be local. If the address is not in the table, the device hands the packet off to its default gateway. This table is used to coordinate the IP address with the MAC addresses that are known to be local to the device. In many situations, this list is a dynamic one, built up from traffic passing through the device and through Address Resolution Protocol (ARP) notifications from new devices joining the network. There is no authentication or verification that the request the device received is valid. Thus, a malicious user is able to send messages to routing devices and APs stating that his or her MAC address is associated with a known IP address. From then on, all traffic that goes through that router destined for the hijacked IP address will be handed off to the hacker's machine. If the attacker spoofs as the default gateway or a specific host on the network, all machines trying to get to the network or the spoofed machine will connect to

the attacker's machine instead of their intended target. The attacker can use this information only to identify passwords and other necessary information and then route the rest of the traffic to the intended recipients. The end users will have no idea that this man in the middle has intercepted their communications, compromising their passwords and information.

4.3 CRACKING WEP

WEP can be cracked in a very simple way, almost with no effort at all. WEP can be cracked using either passive attacks or active attacks. Passive attacks compromise the confidentiality of the network they do need to have some time and space to be implemented. Active attacks compromise the integrity and availability of the network in a less time and space compared to passive attacks but do increase the chances of being detected. The main goal while cracking the WEP is to generate traffic to collect more IVs.

INITIALIZATION VECTORS (IVs)

An initialization vector (IV) is an arbitrary number that can be used along with a secret key for data encryption. This number, also called a nonce, is employed only one time in any session. The ideal IV is a random number that is made know to the destination computer to facilitate decryption of the data when it is received. The usage of IV prevent the repetition in data encryption making it difficult for a hacker using dictionary attack to find a pattern and break the cipher.

AUTOMATED WEP CRACKERS

There are several automated WEP cracking programs, including the following:

- AiroPeek
- WEPCrack
- AirSnort
- Network Stumbler
- iStumbler
- KisMAC

Stream Cipher

Stream cipher is the process of encrypting text in which the plaintext digits are encrypted one at a time, and the cryptographic key and algorithm are applied to each binary digit in a data stream. The encryption of each digit depends on the current state. Given an initialization vector (IV) and secret key, the stream of bytes (pad) produced is always the same. Knowing all pads is the same as knowing the key. The following are the applications of stream cipher to WEP:

• The pad is produced from the combination of the IV and the WEP key passed through RC4.

• If all the pads are known, then it is similar to knowing the 40-bit or 104-bit secret.

• Weak IVs disclose additional information about the secret.

WEP cracking tools

Aircrack

Aircrack recovers 40-bit to 104-bit WEP keys after the required number of encrypted packets is gathered. It is shown in Figure 4-4. Aircrack traps FMS attacks. In addition, Aircrack has the capability of implementing a new type of attack called Korek. The Fluhrer Mantin Shamir (FMS) attack can capture encrypted traffic in bulk and, with a little CPU power, crack the key using a probabilistic algorithm. The cracking of keys takes places linearly. A 128-bit key takes a longer time to crack than a 64-bit key.

AirPcap

AirPcap enables troubleshooting tools like Wireshark (formerly Ethereal) and WinDump to provide information about wireless protocols and radio signals. AirPcap comes as a USB 2.0 adapter and has been fully integrated with WinPcap and Wireshark. It captures and analyses 802.11b/g wireless traffic including control frames, management frames, and power information.

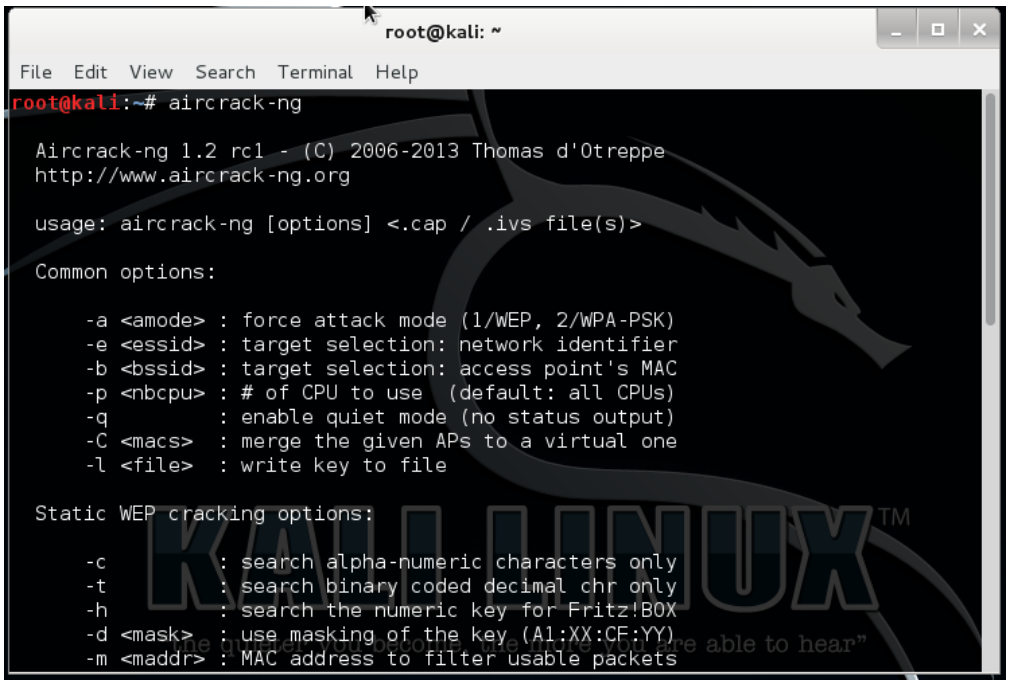

Figure 4-4: aircrack can crack WEP, WPA and WPA-2 keys after sniffing enough packets.

cain and abel

cain and abel is actually a password recovery tool for windows. It is used for easy recovery of several types of passwords through the following methods:

• Sniffing the network

• Cracking encrypted passwords using dictionary, brute-force, and cryptanalysis attacks

• Recording VoIP conversations

• Decoding scrambled passwords

• Recovering wireless network keys

• Revealing password boxes

• Uncovering cached passwords

• Analysing routing protocols

The following are some of the features of Cain & Abel:

• 802.11 Capture Files Decoder can decode wireless capture files from Wireshark and/or Airodump-ng containing WEP or WPA-PSK encrypted 802.11 frames.

• Password decoders can be used to immediately decode encrypted passwords from several sources such as the Windows Protected Store, the Credential Manager, standard edit boxes, LSA secrets, passwords from SQL Enterprise Manager, Windows Mail, dial-up, Remote Desktop profiles, and the Windows Wireless Configuration service.

• WEP Attack, shown in Figure 4-2, covers the same functionality as Aircrack and can quickly recover 64-bit and 128-bit WEP keys if enough unique WEP IVs are available.

• Wireless Scanner detects Wireless Local Area Networks (WLANs) using 802.11x.

• Wireless Zero Configuration Password Dumper enables the recovery of wireless keys stored by Windows's Wireless Zero Configuration Service.

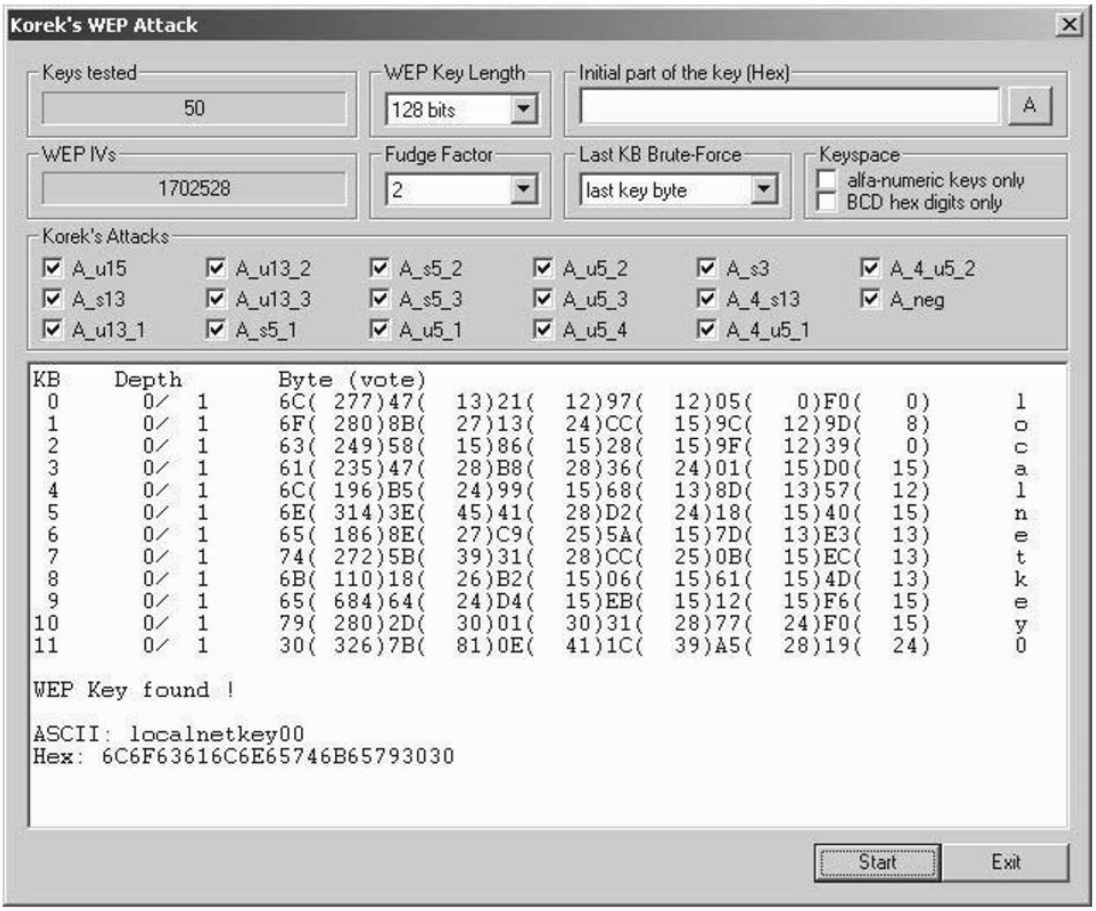

Figure 4-2: cain and Abel's WEP attack has the same functionality as Aircrack.

CHAPTER 5

SECURING WIRELESS NETWORKS

Now since we have seen the vulnerabilities in wireless networks, let us now take a look at how to secure the wireless networks. There different methods to solve this problem, either by doing it manually by yourself or using some tools to do it.

5.1 MANUALLY DEFENDING WIRELESS ATTACKS

To do it manually a basic knowledge of network and networking devices is necessary.

- Change the default SSID after WLAN configuration.
- Do not set a simple password, use a combination of alphabets, numbers and symbols.
- Enable MAC filtering on access point or router. That is adding the MAC address of the permitted devices to the access point.
- Stop broadcasting the SSID.
- By default, certain messages broadcast the ID to everyone stop this by using SSID cloaking.
- Check the wireless devices for configuration or setup problems regularly.
- Frequently check for updates on all the wireless equipment and keep them updated.
- Place the wireless equipment of the access point in a properly secured place.
- Implement WPA2 Enterprise instead of wi-fi protected access (WEP).
- Using a centralised server for authentication is best preferred in corporate sectors.
- Use a firewall or packet filter in between the AP and the corporate intranet.

5.2 DEFENDING WIRELESS ATTACKS USING TOOLS

Wireless networks can be secured not only with manual methods but also with wireless security tools. These tools can be helpful in securing the WLAN more secure when combined with the manual methods. In a sense, tools are just automation for few things that can be done manually.

Rogue Scanner

It is an opens source networks security tool for automatically discovering rogue wireless access point that might provide to access your data. It can also be used for network asset discovery. The Figure 5-1 below shows the rogue scanner displaying all the network connected devices such as printers, routers and computer.

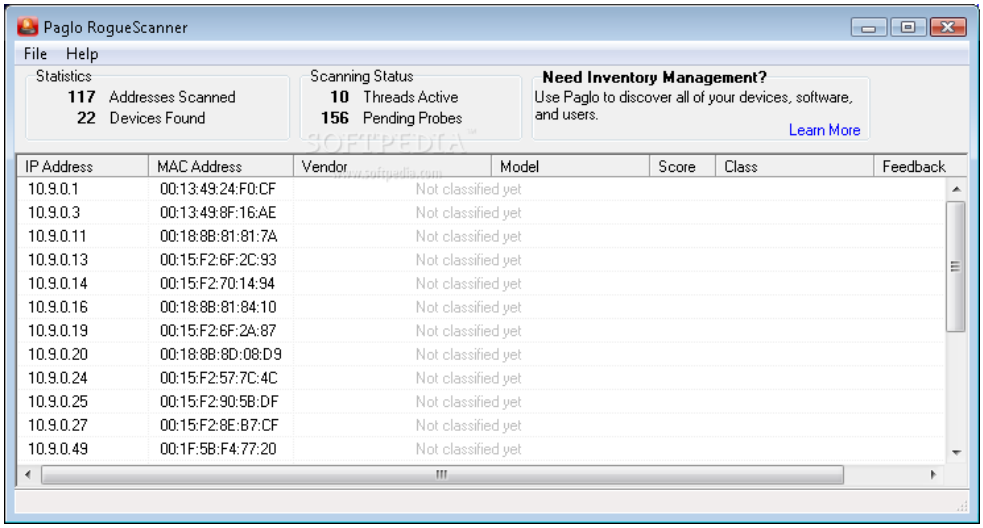

Figure 5-1 RogueScanner discovers rogue wireless access points.

AirDefence

AirDefence shown in the Figure 5-2 is an 802.1/a/b/g, a UI-based platform for wireless monitoring, wireless LAN intrusion detection and security solution that recognizes security risks and attack. It observes the condition of the wireless LAN and offers a real-time stats.

Its features include the following:

• It detects all rogue WLANs.

• It secures a wireless LAN by recognizing and responding to intruders and attacks as they occur.

• It carries out real-time network audits to record all hardware, track all wireless LAN activity, and enforce WLAN policies for security and management.

• It observes the health of the network, identifying and responding to hardware failures, network interferences, and performance degradation.

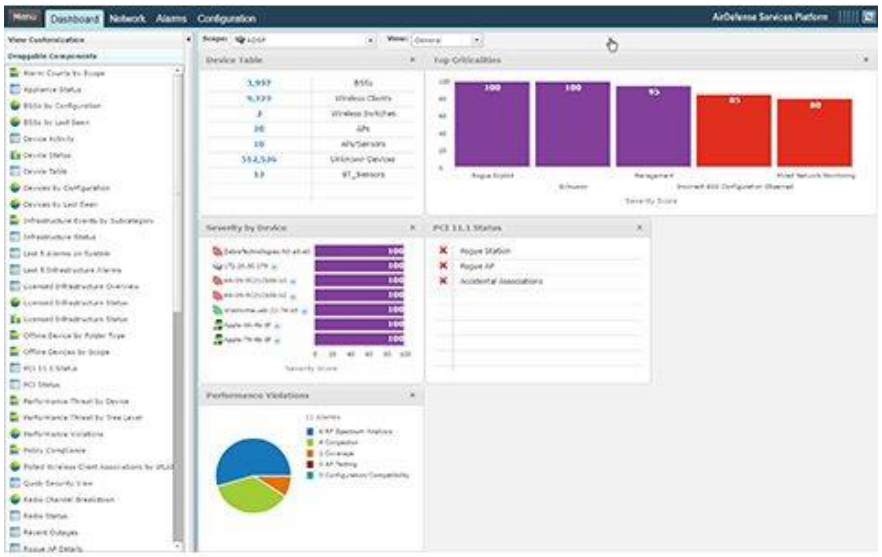

Figure 5-2 AirDefence tool screenshot.

CommView for WiFi PPC

CommView for WiFi PPC is a special, lightweight edition of CommView for WiFi that runs on Pocket PC handheld computers. It is designed for express wireless site surveys, as well as capturing and analyzing network packets on wireless 802.11b/g networks. With CommView for WiFi PPC, shown in Figure 5-3, the user can do the following:

• Scan the air for Wi-Fi signals

• Select channels for monitoring

• Detect access points and wireless stations

• Capture packets

• Measure signal strength

• View the list of network connections

• Examine and filter individual packets

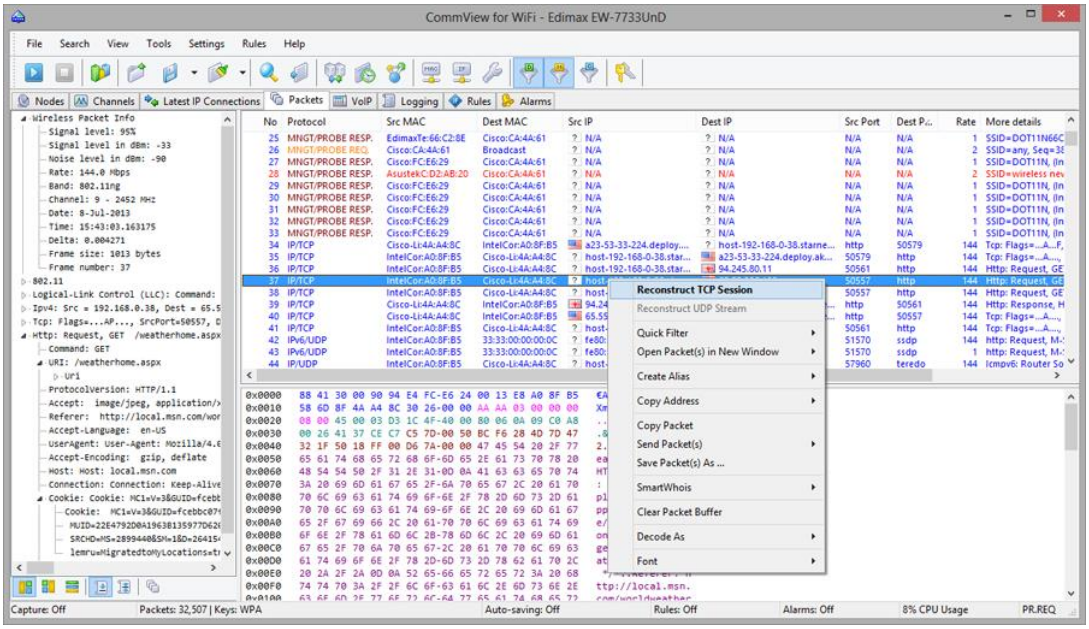

Figure 5-3 commView analyses network data.

Airmagnet analyser

AirMagnet analyser shown in Figure 5-4 is a standard tool for automatically detecting vulnerabilities that are often overlooked, perform a live interactive network test to pinpoint network problems, track down rogues and block them either wirelessly or at the wired port.

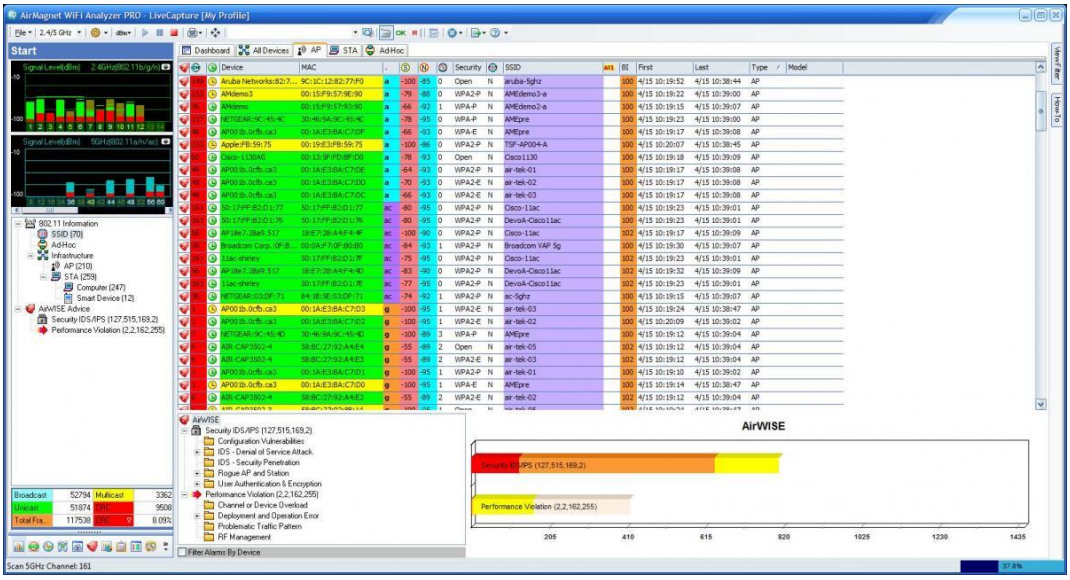

Figure 5-4 AirMagnet wifi analyser screenshot

There are other tools that can help, but these are some of the best and enough for protecting a wireless network.

CHAPTER 6

WIRELESS VULNERABILITY TESTING

1. VERIFY WIRELESS CARD

The first thing we have to do is to check if we have the wifi card connected or not. Type the command "iwconfig" in the terminal and you will get all the connected wireless networking devices.

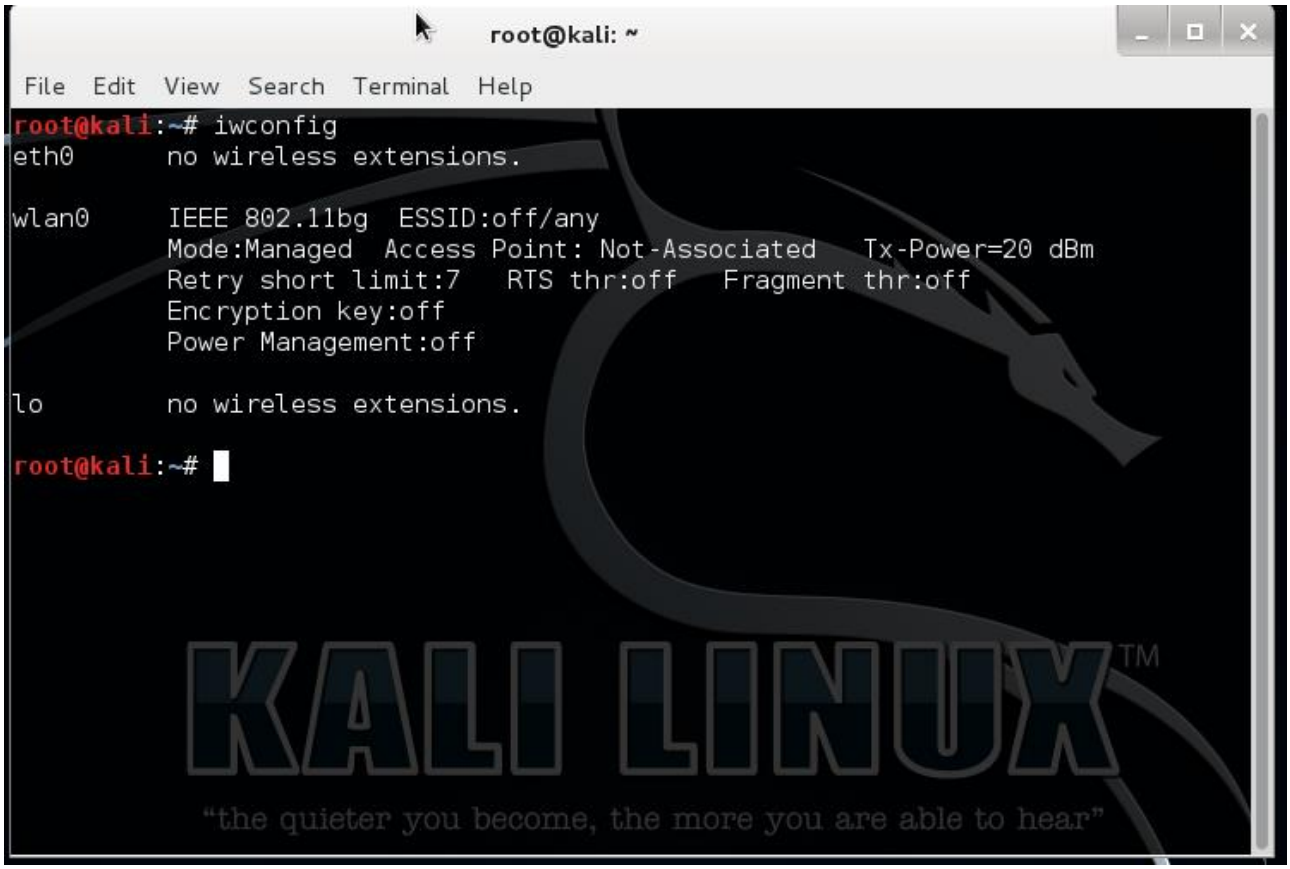

Figure 6-1:iwconfig command output

We can also check by typing "ifconfig -a". This gives a total description of all the networking devices connected.

2. ACTIVATE THE MONITOR MODE ON THE CARD

After checking the card for connection and noting the name of the card, next we have to put it into monitor mode. Monitor mode can be activated with airmon-ng.

Use command **airmon-ng start wlan0,** since the network we are going to use has the name wlan0.

Figure 6-2: setting the card to monitor mode.

This creates a new virtual interface called mon0. Can check with “iwconfig” command.

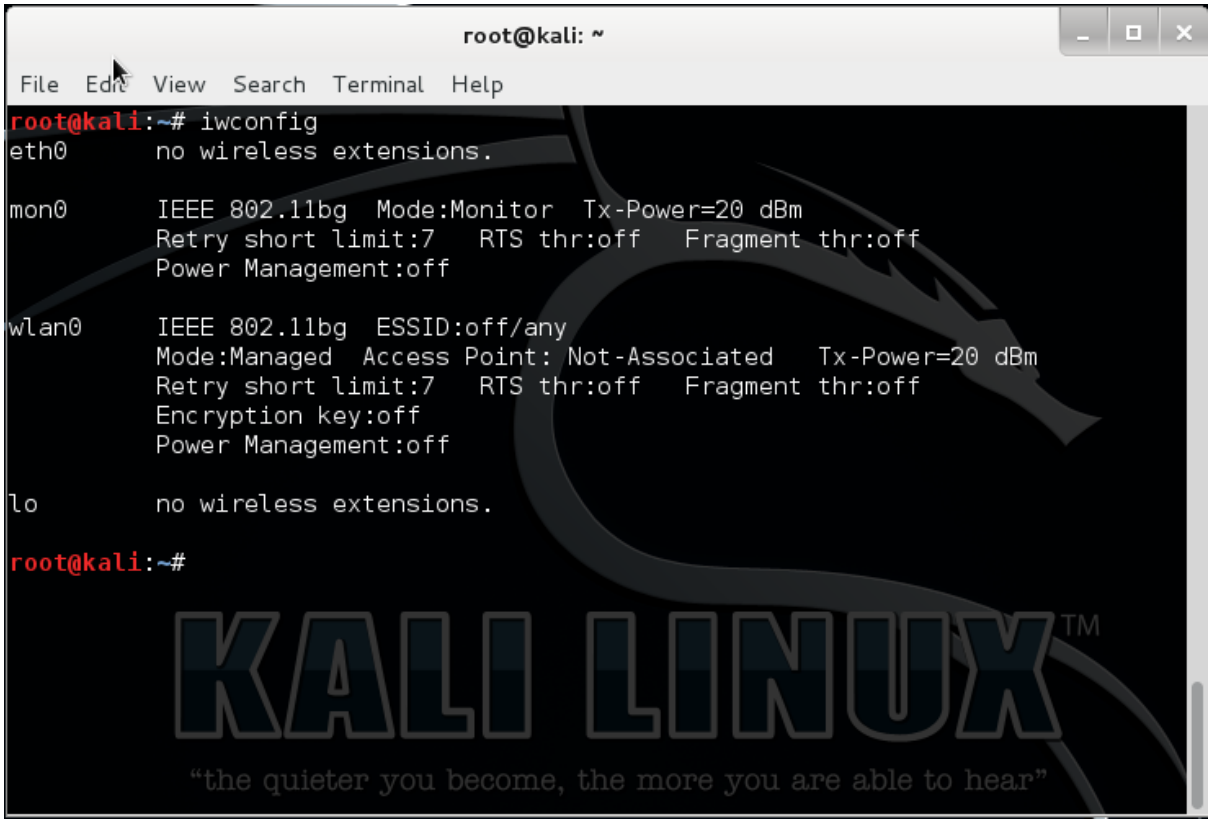

Figure 6-3: checking the monitor mode instance.

3. SCAN ALL WIFI NETWORKS

Wi-Fi uses radio and like any radio it needs to be set to a certain frequency. Wi-Fi uses 2.4GHz and 5GHz (depending on which variation you are using). The 2.4GHz range is split into a number of "channels" which are 5MHz apart. To get two channels which don't overlap at all they need to be spaced around 22MHz apart (but that also depends on which variation of the Wi-Fi standard is being used). That is why channels 1, 6 and 11 are the most common channels as they are far enough apart so that they don't overlap.

To capture data via a Wi-Fi adapter in "monitor" mode you need to tell the adapter which frequency to tune into, i.e. which channel to use. To see which channels are in use around you and which channel is being used by the target Wi-Fi service you wish to test then use the *airodump-ng* command.

Use **airodump-ng mon0** command , since the network instance created here is mon0.

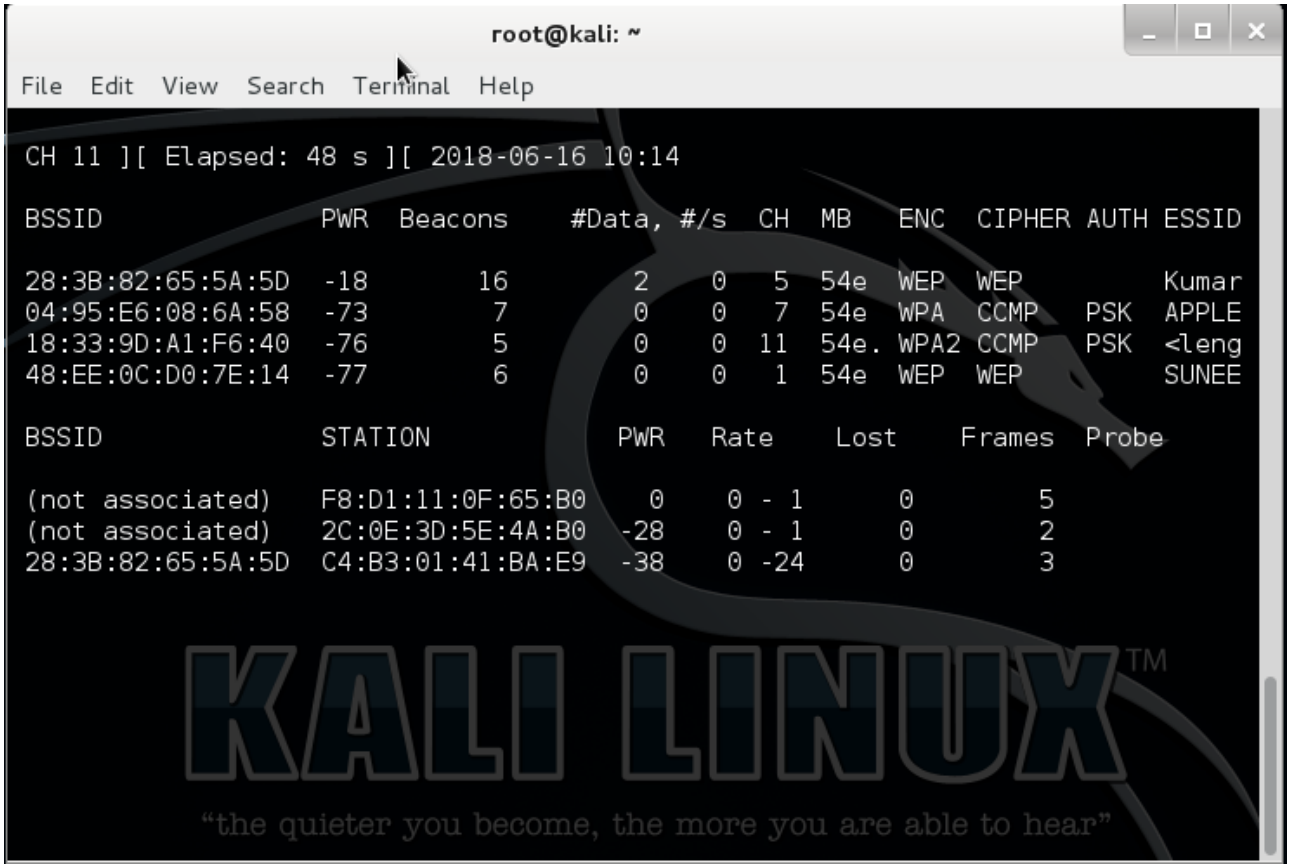

Figure 6-4: capturing data using airodump

The first list shows the Wi-Fi networks within reach of your laptop. The "CH" tells you which channel number each network is using (11, 6, 1 and 11) and the "ESSID" shows the names of the networks (i.e. the service set identifiers). The "ENC" column reveals if the network is using encryption and if so, what type of encryption. The network with ESSID Kumar is selected.

4. SCAN AND MONITOR SELECTED NETWORKS

Since the wifi that is selected is on channel 5 as seen from Figure 6-4 we are going to capture packets from channel 5 and particularly of bssid 28:3B:82:65:5A:5D.

Use code **airodump-ng –w wep –c 5 –bssid 28:3B:82:65:5A:5D mon0**

Here:

-w wep is the name of the files that store the captured data.

-c 5 is setting the channel to 5

--bssid 28:3B:82:65:5A:5D is capturing packets to and from the target network.

And mon0 is the monitor mode instance.

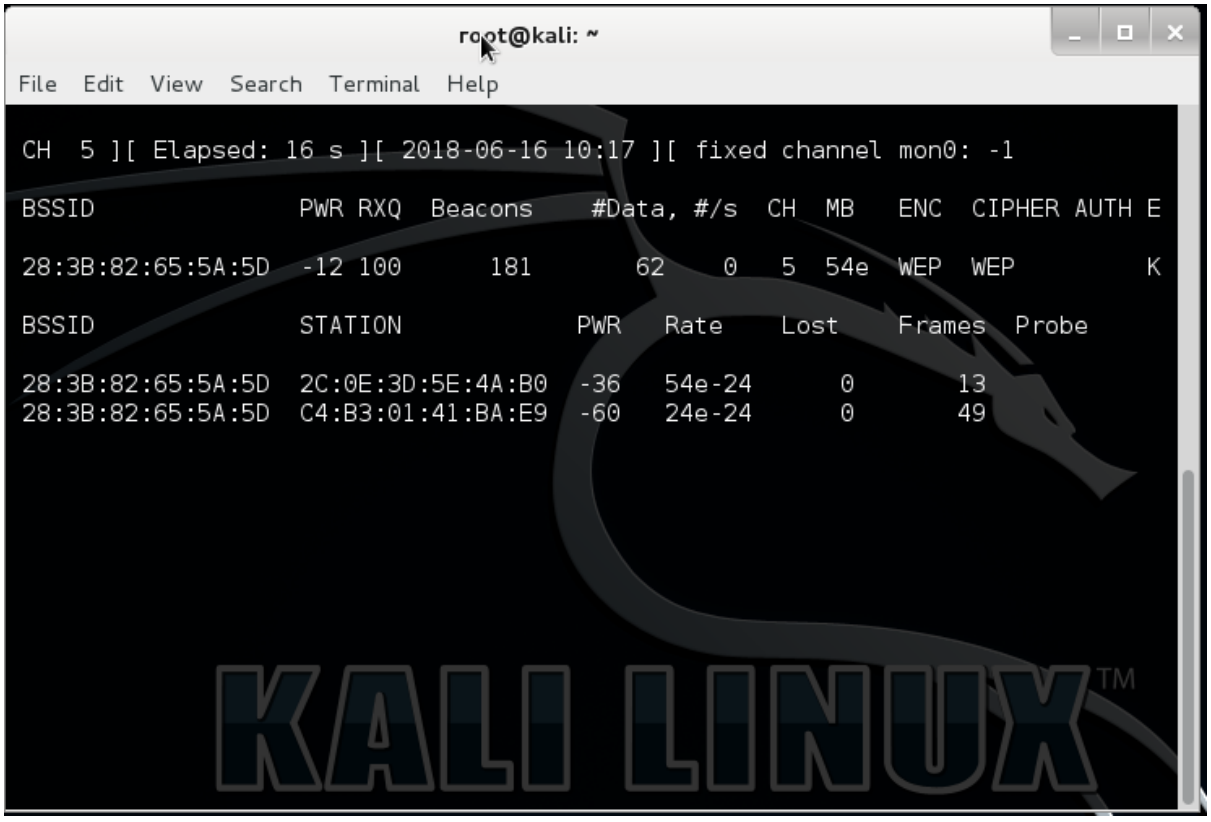

Figure 6-5 : capturing data from particular channel

5. CREATE FAKE TRAFFIC AND CAPUTURE IV

To create fake traffic in the network we can use aireplay suite. First we will be authenticating our machine as one of the devices on the network.

Use code **aireplay-ng -1 0 –a 28:3B:82:65:5A:5D –h f8:d1:11:0f:65:b0 –e Kumar –ignore-negative-one mon0**

Here,

-1 means fake authentication

0 reassociation timing in seconds

-e Kumar is the wireless network name

-a 28:3B:82:65:5A:5D is the access point MAC address

-h f8:d1:11:0f:65:b0 is our card MAC address

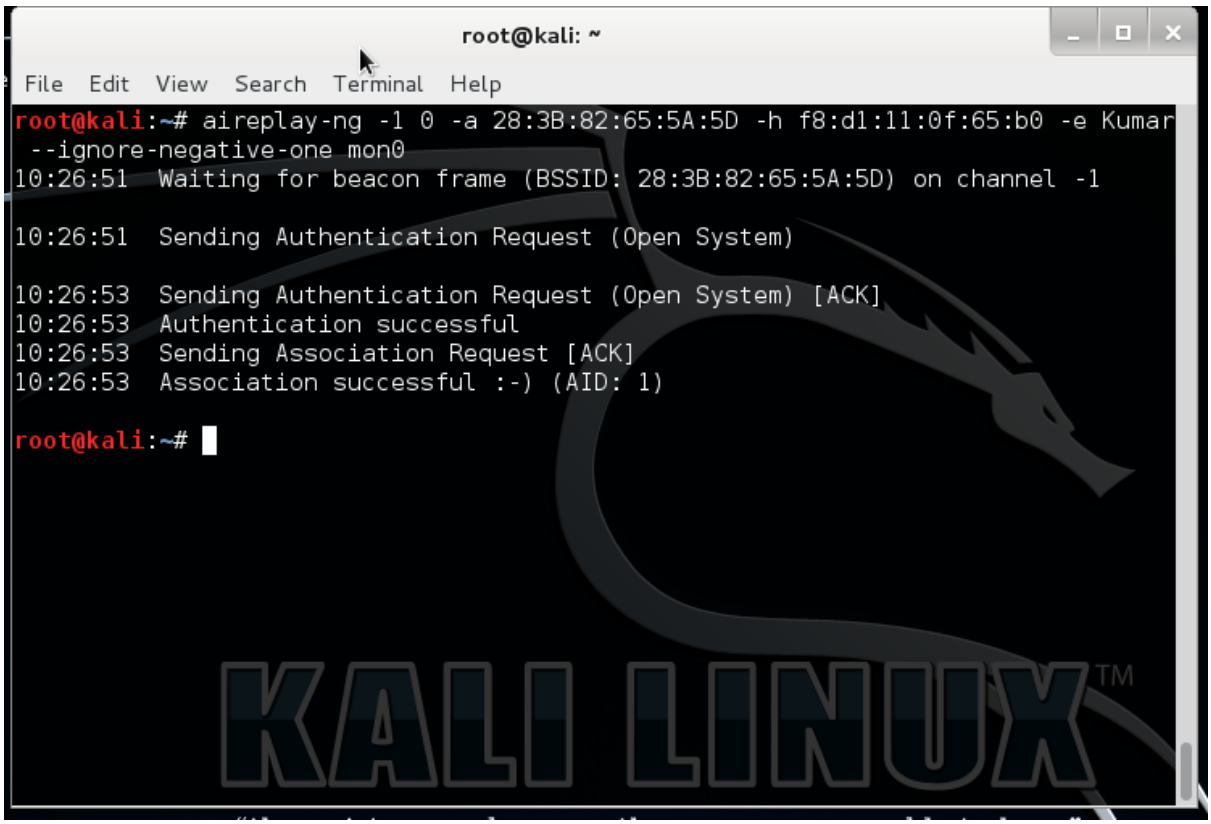

Figure 6-6: fake authentication using aireplay

Now to perform Arp request replay attack use the code **aireplay-ng -3 –b 28:3B:82:65:5A:5D –h f8:d1:11:0f:65:b0 –ignore-negative-one mon0.**

Here

3 means standard arp request replay

-b 28:3B:82:65:5A:5D is the access point MAC address

-h f8:d1:11:0f:65:b0 is the source MAC address (either an associated client or from fake authentication)

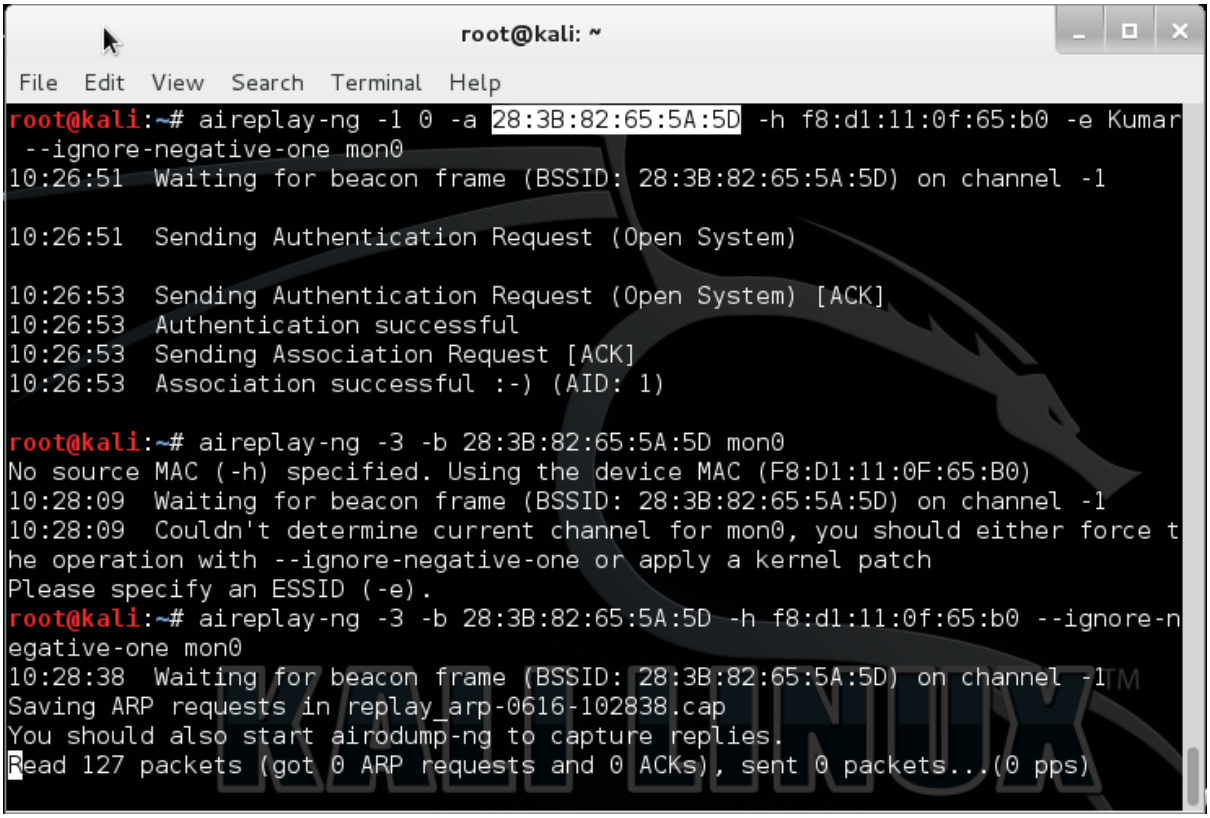

Figure 6-7 : ARP replay request attack.

This attack tries to catch the arp request packets and tries to resend them can be seen in the Figure 6-8. This produces a huge traffic on the network.

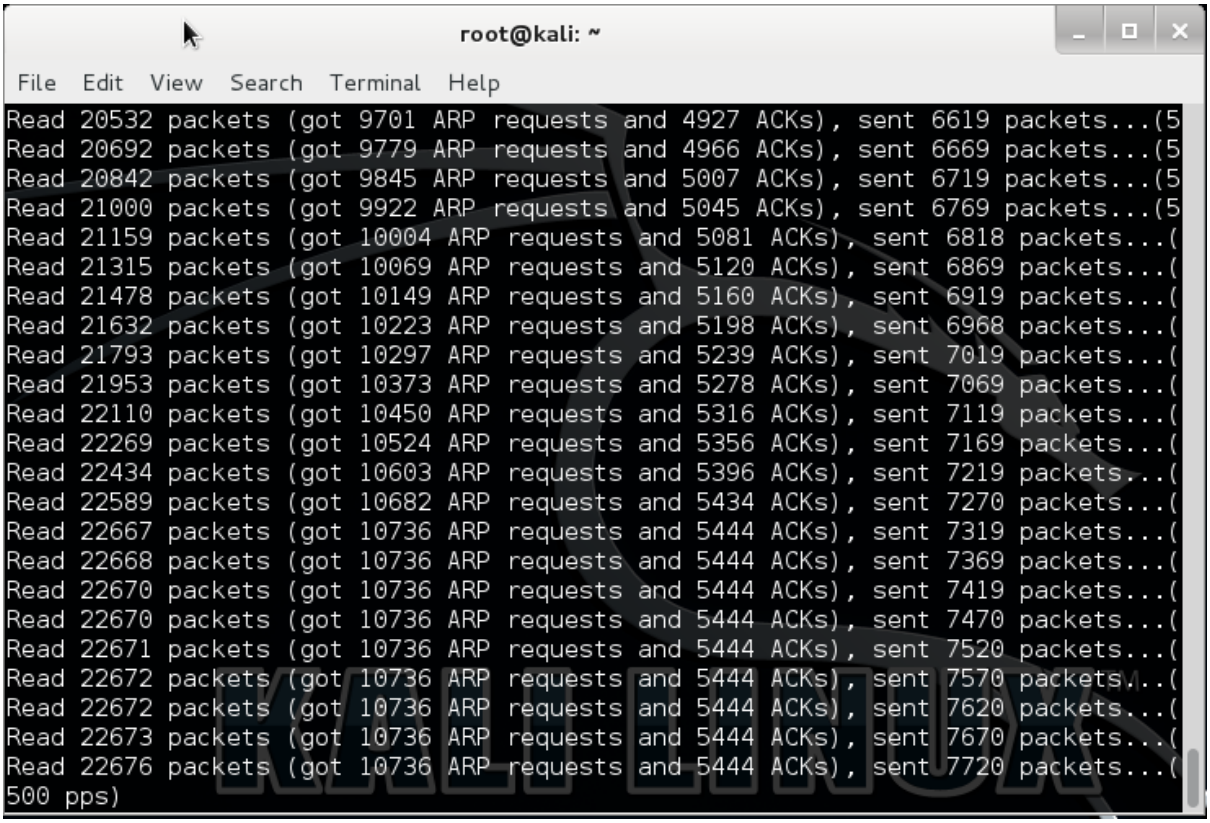

figure 6-8: arp attack in progress.

6. CRACK FOR PASSWORD (MEANWHILE TRY CONNECTING WIFI NETWORK TO GAIN IVS)

The collected data is used to crack the wifi password using aircrack.

Use code **aircrack-ng wep-01.cap**

Wep-01.cap is the file containing the IVs.

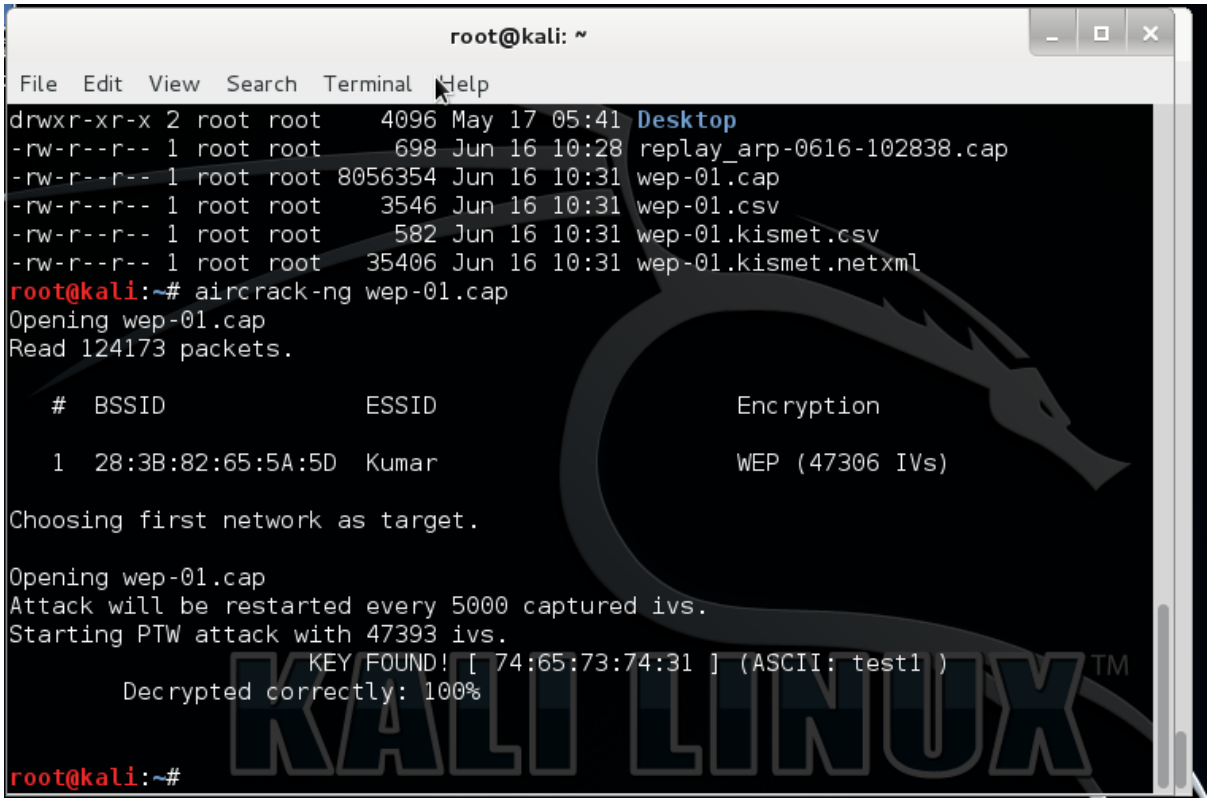

figure 6-9: Cracking password using aircrack.

We can see from the Figure 6-9, it give the cracked password **test1** in this case.