Chapter eleven

- What is a wireless network?
- How to access a wireless network?
- Wireless Network Authentication WEP & WPA
- How to Crack Wireless Networks
- How to Secure wireless networks
- Hacking Activity: Crack Wireless Password

Introduction

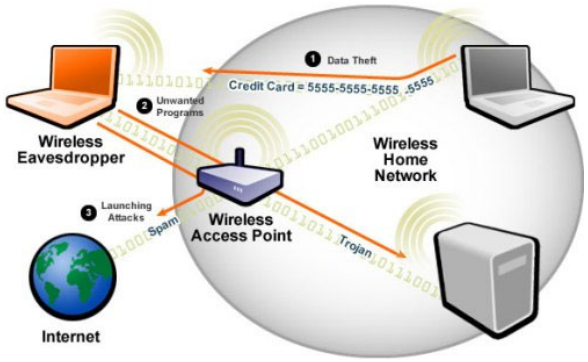
- **Wireless networks are accessible to anyone within the router's transmission radius**. This makes them vulnerable to attacks. Hotspots are available in public places such as airports, restaurants, parks, etc.
- In this chapter, we will introduce you to common techniques used to **exploit weaknesses in wireless network security implementations**. We will also look at some of the countermeasures you can put in place to protect against such attacks.

مقدمة

- **يمكنلأي شخص الوصول إلى الشبكات اللاسلكية داخل نطاق إرسال جهازالتوجيه**. هذا يجعلهم عرضة للهجمات. تتوفر النقاط الساخنة في الأماكنالعامة مثل المطارات والمطاعم والمتنزهات وما إلى ذلك.
- فيهذا الفصل ، سوف نقدم لك التقنيات الشائعة المستخدمة في **استغلالنقاط الضعف في تطبيقات أمن الشبكات اللاسلكية**. سننظر أيضافي بعض الإجراءات المضادة التي يمكنك وضعها للحماية من مثل هذه الهجمات.

What is a wireless network?

- A **wireless network** is a network that uses **radio waves** to link computers and other devices together. The implementation is done at the Layer 1 (**physical layer**) of the **OSI** model.



169

- **أشبكة لاسلكية**هي شبكة تستخدم**موجات الراديو**لربط أجهزة الكمبيوتر والأجهزةالأخرى معاً. يتم التنفيذ في الطبقة 1 (**الطبقة المادية**) التابع**OSI** نموذج.

How to access a wireless network?

- You will need a **wireless network enabled** device such as a **laptop**, **tablet**, **smartphones**, etc. You will also need to be within the transmission radius of a wireless network access point. Most devices (if the wireless network option is turned on) will provide you with a list of available networks. If the network is not password protected, then you just have to click on connect. If it is password protected, then you will need the password to gain access.

كيف تصل إلى شبكة لاسلكية؟

- سوف تحتاج **تمكين الشبكة اللاسلكية** جهاز مثل **حاسوب محمول** و **لوح** و **الهواتف الذكية**، إلخ. ستحتاج أيضاً إلى أن تكون داخل دائرة نصف قطرها للإرسال لنقطة وصول للشبكة اللاسلكية. ستزودك معظم الأجهزة (إذا كان خيار الشبكة اللاسلكية قيد التشغيل) بقائمة بالشبكات المتاحة. إذا لم تكن الشبكة محمية بكلمة مرور ، فما عليك سوى النقر فوق الاتصال. إذا كانت محمية بكلمة مرور ، فستحتاج إلى كلمة المرور للوصول إليها.

Wireless Network Authentication

- Since the network is easily accessible to everyone with a wireless network enabled device, most networks are **password protected**. Let's look at some of the most commonly used authentication techniques.

مصادقةالشبكة اللاسلكية

- نظرألأن الشبكة يمكن الوصول إليها بسهولة لأي شخص لديه جهاز مزود بشبكةلاسلكية ، فإن معظم الشبكات متوفرة**محمي بكلمة مرور**. دعنا نلقيnظرة على بعض تقنيات المصادقة الأكثر استخداماً.

171

171

WEP

- WEP is the acronym for **Wired Equivalent Privacy**. It was developed for **IEEE 802.11 WLAN** standards. Its goal was to provide the privacy equivalent to that provided by wired networks. **WEP** works by encrypting the data been transmitted over the network to keep it safe from eavesdropping.

WEP

- هواختصار لـ WEP**الخصوصية المكافئة السلكية**. تم تطويره لـ**شبكة IEEE 802.11 WLAN**المعايير. كان هدفها توفير الخصوصية المكافئة لتلك التيtوفرها الشبكات السلكية.**WEP**يعمل عن طريق تشفير البيانات المنقولة عبرالشبكة لحمايتها من التنصت.

172

172

WEP Authentication

- Open System Authentication (**OSA**) – this methods grants access to station authentication requested based on the configured access policy.
- Shared Key Authentication (**SKA**) – This method sends to an encrypted challenge to the station requesting access. The station encrypts the challenge with its key then responds. If the encrypted challenge matches the **AP** value, then access is granted.

مصادقةWEP

- فتحمصادقة النظام (**OSA**) - تمنح هذه الطرق الوصول إلى مصادقة المحطةالمطلوبة بناءً على سياسة الوصول المكونة.
- مصادقةالمفتاح المشترك (**SKA**) - ترسل هذه الطريقة تحدياً مشفراً إلى المحطةالتي تطلب الوصول. تقوم المحطة بتشفير التحدي بمفتاحه ثم تستجيب.إذا كان التحدي المشفر يطابق**AP**القيمة ، ثم يتم منح الوصول.

WEP Weakness

- **WEP** has significant design flaws and vulnerabilities.
  - The integrity of the packets is checked using Cyclic Redundancy Check (**CRC32**). **CRC32** integrity check can be compromised by capturing at least two packets. The bits in the encrypted stream and the checksum can be modified by the attacker so that the packet is accepted by the authentication system. This leads to unauthorized access to the network.
  - WEP uses the **RC4** encryption algorithm to create stream ciphers. The stream cipher input is made up of an initial value (**IV**) and a secret key. The length of the initial value (**IV**) is 24 bits long while the secret key can either be 40 bits or 104 bits long. The total length of both the initial value and secret can either be **64 bits** or **128 bits** long. The lower possible value of the secret key makes it easy to crack it.

ضعفWEP

- **WEP**لديه عيوب تصميم كبيرة ونقاط ضعف.
  - يتمالتحقق من سلامة الحزم باستخدام فحص التكرار الدوري (**CRC32**).يمكن اختراق فحص السلامة عن طريق التقاط حزمتين على الأقل.**CRC32** يمكنللمهاجم تعديل البتات الموجودة في الدفق المشفر والمجموع الاختباري بحيث يتمقبول الحزمة بواسطة نظام المصادقة. هذا يؤدي إلى الوصول غير المصرح به إلى الشبكة.
  - يستخدمWEP ملف**RC4**خوارزمية تشفير لإنشاء أصفار دفق. يتكون إدخال تشفير التدفقمن قيمة أولية (**رابعا**) ومفتاح سري. طول القيمة الأولية (**رابعا**) يبلغ طوله 24 بتأبينما يمكن أن يبلغ طول المفتاح السري 40 بت أو 104 بت. يمكن أن يكون الطول الإجماليلكل من القيمة الأولية والسرية**64 بت**أو**128 بت**طويل. تجعل القيمة المنخفضةالمحتملة للمفتاح السري من السهل كسره.

WEP Weakness-cont.

- Weak Initial values combinations do not encrypt sufficiently. This makes them vulnerable to attacks.
- WEP is based on passwords; this makes it vulnerable to dictionary attacks.
- Keys management is poorly implemented. Changing keys especially on large networks is challenging. WEP does not provide a centralized key management system.
- The Initial values can be reused

- Because of these security flaws, **WEP** has been deprecated in favor of **WPA**

175

ضعفWEP تابع.

- مجموعاتالقيم الأولية الضعيفة لا يتم تشفيرها بشكل كافٍ. هذا يجعلهم عرضة للهجمات.
- يعتمدWEP على كلمات المرور ؛ هذا يجعله عرضة لهجمات القاموس.
- يتمتنفيذ إدارة المفاتيح بشكل سيء. يعد تغيير المفاتيح خاصة على الشبكات الكبيرة أمراًصعباً. لا يوفر WEP نظام إدارة مفتاح مركزي.
- يمكنإعادة استخدام القيم الأولية
- بسببهذه العيوب الأمنية ،**WEP**تم إهماله لصالح **WPA**

WPA

- **WPA is the acronym for Wi-Fi Protected Access**. It is a security protocol developed by the Wi-Fi Alliance in response to the weaknesses found in WEP. It is used to encrypt data on 802.11 WLANs. It uses higher Initial Values 48 bits instead of the 24 bits that WEP uses. It uses temporal keys to encrypt packets.

176

WPA

- **Wi Fi Protected Access هو اختصار لـ WPA**. إنه بروتوكول أمان تم تطويرهبواسطة Wi Fi Alliance استجابةً لنقاط الضعف الموجودة في WEP. يتماستخدامه لتشفير البيانات على شبكات WLAN 802.11. يستخدم قيماً أوليةأعلى 48 بت بدلاً من 24 بت التي يستخدمها WEP. يستخدم مفاتيح زمنيةلتشفير الحزم.

WPA Weaknesses

- The collision avoidance implementation can be broken
- It is vulnerable to denial of service attacks
- Pre-shares keys use passphrases. Weak passphrases are vulnerable to dictionary attacks.

نقاطضعف WPA

- يمكنكسر تنفيذ تجنب الاصطدام
- إنهعرضة لهجمات رفض الخدمة
- تستخدممفاتيح المشاركات المسبقة عبارات المرور. عبارات المرور الضعيفة عرضة لهجماتالقاموس.

177

How to Crack Wireless Networks

- **WEP cracking**: Cracking is the process of exploiting security weaknesses in wireless networks and gaining unauthorized access. WEP cracking refers to exploits on networks that use WEP to implement security controls. There are basically two types of cracks namely;
  - **Passive cracking**– this type of cracking has no effect on the network traffic until the WEP security has been cracked. It is difficult to detect.
  - **Active cracking**– this type of attack has an increased load effect on the network traffic. It is easy to detect compared to passive cracking. It is more effective compared to passive cracking.

كيفيةاختراق الشبكات اللاسلكية

178

- **تكسيرWEP**: الاختراق هو عملية استغلال نقاط الضعف الأمنية في الشبكاتاللاسلكية والحصول على وصول غير مصرح به. يشير تكسير WEP إلىعمليات الاستغلال على الشبكات التي تستخدم WEP لتنفيذ ضوابط الأمان.هناك نوعان أساسيان من التشققات وهما ؛

- **التكسيرالسلبي**- لا يؤثر هذا النوع من الاختراق على حركة مرور الشبكة حتى يتم اختراقأمان WEP. من الصعب اكتشافها.
- **التكسيرالنشط**- هذا النوع من الهجوم له تأثير تحميل متزايد على حركة مرور الشبكة.من السهل اكتشافه مقارنة بالتكسير السلبي. إنه أكثر فعالية مقارنة بالتكسيرالسلبي.

WEP Cracking Tools

- **Aircrack**– network sniffer and WEP cracker. Can be downloaded from http://www.aircrack-ng.org/
- **WEPCrack**– this is an open source program for breaking 802.11 WEP secret keys. It is an implementation of the **FMS attack**. http://wepcrack.sourceforge.net/
- **Kismet**- this can include detector wireless networks both visible and hidden, sniffer packets and detect intrusions. http://www.kismetwireless.net/
- **WebDecrypt**– this tool uses active dictionary attacks to crack the WEP keys. It has its own key generator and implements packet filters. http://wepdecrypt.sourceforge.net/

179

أدواتتكسير WEP

- **ايركراك**- شبكة الشم و WEP cracker. يمكن تنزيله من ملفات /ng.org-
http://www.aircrack
- **WEPCrack**- هذا برنامج مفتوح المصدر لكسر مفاتيح سرية 802.11 WEP
إنه تنفيذ**هجوم FMS**. http://wepcrack.sourceforge.net/

- **كيسمت**- يمكن أن يشمل ذلك شبكات الكاشف اللاسلكية المرئية والمخفية على حدسواء ، والحزم المتشممة واكتشاف الاختراقات.
http://www.kismetwireless.net/
- **WebDecrypt**- تستخدم هذه الأداة هجمات القاموس النشطة لاختراق مفاتيح WEP. لديها مولد رئيسي خاص بها وتنفذ مرشحات الحزمة. /
http://wepdecrypt.sourceforge.net

179

WPA Cracking

- **WPA** uses a 256 pre-shared key or passphrase for authentications. Short passphrases are vulnerable to dictionary attacks and other attacks that can be used to crack passwords. The following tools can be used to crack WPA keys.
  - **CowPatty**– this tool is used to crack pre-shared keys (PSK) using brute force attack. http://wirelessdefence.org/Contents/coWPAttyMain.htm
  - **Cain & Abel**– this tool can be used to decode capture files from other sniffing programs such as Wireshark. The capture files may contain WEP or WPA-PSK encoded frames. http://www.softpedia.com/get/Security/Decrypting-Decoding/Cain-and-Abel.shtml

180

تكسيرWPA

- **WPA**يستخدم 256 مفتاح مشترك مسبقاً أو عبارة مرور للمصادقة. عبارات المرورالقصيرة عرضة لهجمات القاموس والهجمات الأخرى التي يمكن استخدامهالاختراق كلمات المرور. يمكن استخدام الأدوات التالية لاختراق مفاتيحWPA.
  - **CowPatty**- تستخدم هذه الأداة لاختراق المفاتيح المشتركة مسبقاً (PSK) باستخدام هجوم القوة الغاشمة.http://wirelessdefence.org/Contents/coWPAttyMain.htm
  - **قابيلوهابيل**- يمكن استخدام هذه الأداة لفك تشفير ملفات الالتقاط من برامج الاستنشاقالأخرى مثل Wireshark. قد تحتوي ملفات الالتقاط على إطارات WEP أو PSK WPA المشفرة.Abel.shtml فك / قابيل - و -/get/Security/Decrypting
http://www.softpedia.com

180

General Attack types

- **Sniffing**– this involves intercepting packets as they are transmitted over a network. The captured data can then be decoded using tools such as **Cain & Abel**.
- **Man in the Middle (MITM) Attack**– this involves eavesdropping on a network and capturing sensitive information.
- **Denial of Service Attack**– the main intent of this attack is to deny legitimate users network resources. **FataJack** can be used to perform this type of attack.

أنواعالهجوم العام

- **شم**- يتضمن ذلك اعتراض الحزم أثناء إرسالها عبر الشبكة. يمكن بعد ذلك فكتشفير البيانات الملتقطة باستخدام أدوات مثل**قابيل وهابيل**.
- **هجومرجل في الوسط (MITM)**- يتضمن ذلك التنصت على شبكة والتقاطمعلومات حساسة.
- **هجومقطع الخدمة**- الهدف الرئيسي من هذا الهجوم هو حرمان موارد شبكةالمستخدمين المشروعة.**فاتجاك**يمكن استخدامها لتنفيذ هذا النوع منالهجوم.

181

Cracking Wireless network WEP/WPA keys

- It is possible to crack the **WEP/WPA** keys used to gain access to a wireless network. Doing so requires software and hardware resources, and patience. The success of such attacks can also depend on how **active** and **inactive** the users of the target network are.
- We will provide you with basic information that can help you get started. **Backtrack(Kali)** is a Linux-based security operating system. It is developed on top of Ubuntu. **Backtrack(Kali)** comes with a number of security tools. Backtrack can be used to gather information, assess vulnerabilities and perform exploits among other things.

تكسيرمفاتيح الشبكة اللاسلكية WEP / WPA

- منالممكن كسر**WPA / WEP**المفاتيح المستخدمة للوصول إلي شبكة لاسلكية.يتطلب القيام بذلك موارد برامج وأجهزة وصبراً. يمكن أن يعتمد نجاحمثل هذه الهجمات أيضاً على كيفية حدوث ذلك**نشيط**و**غير نشط** مستخدموالشبكة المستهدفة هم.
- سنزودكبالمعلومات الأساسية التي يمكن أن تساعدك على البدء.**تراجع** (**كالي**)هو نظام تشغيل أمان يستند إلى Linux. تم تطويره على رأس Ubuntu .**تراجع** (**كالي**)يأتي مع عدد من أدوات الأمان. يمكن استخدام Backtrack لجمعالمعلومات وتقييم نقاط الضعف وتنفيذ عمليات الاستغلال من بين أشياءأخرى.

182

Cracking Wireless network WEP/WPA keys-cont.

- Some of the popular tools that backtrack has includes;
  - Metasploit
  - Wireshark
  - Aircrack-ng
  - NMap
  - Ophcrack
- Cracking wireless network keys requires patience and resources mentioned above. At a minimum, you will need the following tools

183

تكسيرمفاتيح الشبكة اللاسلكية WEP / WPA - تابع.

- تتضمنبعض الأدوات الشائعة التي يتضمنها التراجع ؛
  - ميتاسبلويت
  - وايرشارك
  - ايركراك- ng
  - NMap
  - Ophcrack
- يتطلباختراق مفاتيح الشبكة اللاسلكية الصبر والموارد المذكورة أعلاه. كحدأدنى ، ستحتاج إلى الأدوات التالية

183

Cracking Wireless network WEP/WPA keys-cont.

- A wireless network adapter with the capability to inject packets (**Hardware**)
- **Kali Operating System**. You can download it from here https://www.kali.org/downloads/
- Be within the target network's radius. If the users of the target network are actively using and connecting to it, then your chances of cracking it will be significantly improved.
- Sufficient knowledge of Linux based operating systems and working knowledge of **Aircrack** and its various scripts.
- Patience, cracking the keys may take a bit of sometime depending on a number of factors some of which may be beyond your control. Factors beyond your control include users of the target network using it actively as you sniff data packets.

184

تكسيرمفاتيح الشبكة اللاسلكية WEP / WPA - تابع.

- محولشبكة لاسلكية لديه القدرة على حقن الحزم (**المعدات**)
- **نظامتشغيل كالي**. يمكنك تحميل البرنامج من هنا / https://www.kali.org/downloads
- كنضمن دائرة نصف قطر الشبكة المستهدفة. إذا كان مستخدمو الشبكة المستهدفةيستخدمونها ويتصلون بها بنشاط ، فستتحسن فرص اختراقها بشكل كبير.
- معرفةكافية بأنظمة التشغيل المستندة إلى Linux ومعرفة عملية بـ**ايركراك** ونصوصهالمختلفة.
- قديستغرق الصبر ، كسر المفاتيح بعض الوقت اعتماداً على عدد من العوامل التي قديكون بعضها خارج عن إرادتك. تشمل العوامل الخارجة عن إرادتك مستخدمي الشبكةالمستهدفة التي تستخدمها بنشاط أثناء شم حزم البيانات.

184

How to Secure wireless networks

- In minimizing wireless network attacks; an organization can adopt the following policies
  - Changing **default** passwords that come with the hardware
  - Enabling the **authentication** mechanism
  - Access to the network can be restricted by allowing only registered **MAC addresses**.
  - Use of strong **WEP** and **WPA-PSK** keys, a combination of **symbols**, **number** and **characters** reduce the chance of the keys been cracking using dictionary and brute force attacks.
  - **Firewall** Software can also help reduce unauthorized access.

كيفيةتأمين الشبكات اللاسلكية

185

- في**تقليل** هجمات الشبكة اللاسلكية ؛ يمكن للمنظمة اعتماد السياسات التالية
  - التغيير**تقصير**كلمات المرور التي تأتي مع الجهاز
  - تمكين**المصادقة**آلية
  - يمكن**تقييد** الوصول إلى الشبكة بالسماح فقط بالتسجيل**عناوين MAC**.
- استخدام**قوي**WEP**و**WPA PSK**مفاتيح ، مزيج من**حرف او رمز**ورقم**و**الشخصيات تقليل**فرصة اختراق المفاتيح باستخدام القاموس وهجمات القوة الغاشمة.
- **جدارالحماية**يمكن أن يساعد البرنامج أيضاً في تقليل الوصول غير المصرح به.

185

Hacking Activity: Crack Wireless Password

- In this practical scenario, we are going to use **Cain and Abel** to decode the stored wireless network passwords in Windows. We will also provide useful information that can be used to crack the **WEP** and **WPA** keys of wireless networks.

نشاطالقرصنة: كسر كلمة المرور اللاسلكية

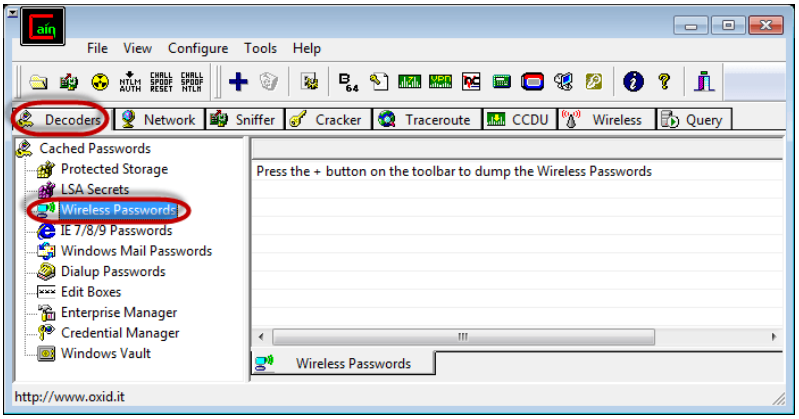
- في**هذا** السيناريو العملي ، سنستخدم**قابيل وهابيل**لفك تشفير كلمات مرور الشبكة**اللاسلكية** المخزنة في Windows. سنوفر أيضاً معلومات مفيدة يمكن استخدامها**لاختراق** ملفات**WEP**و **WPA**مفاتيح الشبكات اللاسلكية.

186

186

Decoding Wireless network passwords stored in Windows

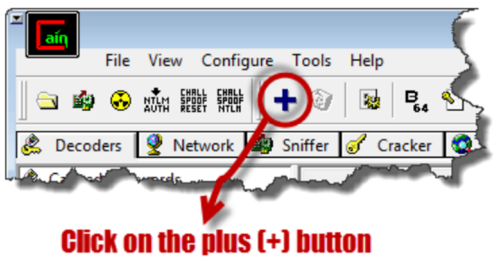
- Download Cain & Abel from the link provided above.
- Open Cain and Abel



187

Decoding Wireless network passwords stored in Windows-cont.

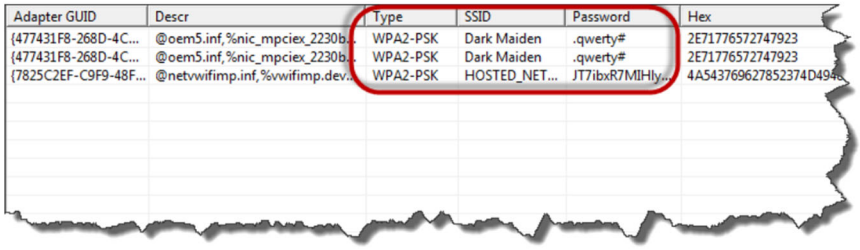
- Ensure that the Decoders tab is selected then click on Wireless Passwords from the navigation menu on the left-hand side
- Click on the button with a plus sign



188

Decoding Wireless network passwords stored in Windows-cont.

- Assuming you have connected to a secured wireless network before, you will get results similar to the ones shown below



Adapter GUID	Descr	Type	SSID	Password	Hex
{477431F8-268D-4C...	@oem5.inf,%nic_mpciex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E71776572747923
{477431F8-268D-4C...	@oem5.inf,%nic_mpciex_2230b...	WPA2-PSK	Dark Maiden	.qwerty#	2E71776572747923
{7825C2EF-C9F9-48F...	@netvwifimp.inf,%vwifimp.dev...	WPA2-PSK	HOSTED_NET...	JT7ibxR7MIHly...	4A543769627852374D494...

- The decoder will show you the encryption type, SSID and the password that was used.

189

- يمكن رؤية موجات نقل الشبكة اللاسلكية من قبل الغرباء ، وهذا ينطوي على العديد من المخاطر الأمنية.
- بها عيوب أمنية تجعل من السهل كسرها مقارنة بتطبيقات الأمان الأخرى. Wired Equivalent Privacy هو اختصار لـ WEP.

Summery

- WEP لديها أمان مقارنة بـ Wi Fi Protected Access. هو اختصار لـ WPA
- يمكن أن تساعد أنظمة كشف التسلل في الكشف عن الوصول غير المصرح به
- يمكن لسياسة الأمان الجيدة أن تساعد في حماية الشبكة.

- Wireless network transmission waves can be seen by outsiders, this possesses many security risks.
- WEP is the acronym for Wired Equivalent Privacy. It has security flaws which make it easier to break compared to other security implementations.
- WPA is the acronym for Wi-Fi Protected Access. It has security compared to WEP
- Intrusion Detection Systems can help detect unauthorized access
- A good security policy can help protect a network.

190