CH1 Network Security Concepts

2.Definition of Network Security: network security is the process of taking preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure.

CIA: Confidentiality - Integrity – Availability

Confidentiality:السرية

Integrity: التكامل، فالبيانات التي تم إرسالها يجب أن تصل كما هي بسلامة إلى الجهة المقابلة

Availability: التوافر للبيانات عند حاجاتها حسب الجهة العاملة

سؤال امتحان: ماهي مفاهيم الأمان الأساسية لأي نظام معلومات؟

الجواب: Confidentiality - Integrity – Availability

3. Security Policy for Network: 'the set of criteria for the provision of security services.

- Interpret the overall Information Security Policy in the context of the networked environment.
- Defines what is the responsibility of the network and what is not.
- Describes what security is to be available from the network.
- Describes rules for using the network.
- Describes who is responsible for the management and security of the network.

ISO 7498-2 distinguishes between 2 types of security policy:

- Identity–based
- Rule–based

٣- السياسة الأمنية للشبكة: "مجموعة معايير تقديم الخدمات الأمنية.

- تفسير سياسة أمن المعلومات الشاملة في سياق بيئة الشبكات.
- يحدد ما هي مسؤولية الشبكة وما هو ليس كذلك.
- يصف الأمن الذي يجب أن يكون متاحًا من الشبكة.
- يصف قواعد استخدام الشبكة.
- يصف من هو المسؤول عن إدارة وأمن الشبكة.

يميز ISO 7498-2 بين نوعين من سياسة الأمن:

- الهوية القائمة
- المستندة إلى القواعد

4. Security Life Cycle: A security program is not a static assessment

Exam Question: True or False

A security program is a static assessment.

True

False, It's not a static assessment

Therefore, a generic model for the security life–cycle, including network security issues, is as follows:

- Define security policy.
- Analyze security threats (according to policy) and associated risks, given existing safeguards.
- Define security services to meet/reduce threats, to bring risks down to acceptable levels.
- Define security mechanisms to provide services.
- Provide on–going management of security.

A threat is: a possible means by which a security policy may be breached. in other words, a security threat is a person, thing, event, or idea which poses some danger to an asset (in terms of

٤- دورة حياة الأمان: برنامج الأمان ليس تقييمًا ثابتًا

سؤال الامتحان: صح أم خطأ

برنامج الأمان هو تقييم ثابت.

حقيقي

خطأ ، إنه ليس تقييمًا ثابتًا

لذلك ، فإن النموذج العام لدورة حياة الأمان ، بما في ذلك مشكلات أمان الشبكة ، هو كما يلي:

- Define سياسة الأمن.
- تحليل التهديدات الأمنية (وفقًا للسياسة) والمخاطر المرتبطة بها ، بالنظر إلى الضمانات القائمة.
- تحديد خدمات الأمن لمواجهة / تقليل التهديدات ، لتقليل المخاطر إلى المستويات المقبولة.
- تحديد آليات الأمن لتقديم الخدمات.
- توفير إدارة مستمرة للأمن.

التهديد هو: وسيلة محتملة يمكن من خلالها انتهاك سياسة الأمن. بمعنى آخر ، التهديد الأمني هو شخص أو شيء أو حدث أو فكرة تشكل بعض الخطر على أحد الأصول (من حيث السرية أو النزاهة أو التوفر أو الاستخدام المشروع). مثال على التهديدات (تسرب المعلومات ، انتهاك السلامة ، الاستخدام غير المشروع ، ...).

الهجوم هو: إدراك التهديد (على سبيل المثال ، سرقة البيانات ، هجوم رفض الخدمة).

الضمانات هي تدابير (مثل الضوابط والإجراءات) للحماية من التهديدات.

نقاط الضعف هي نقاط ضعف في الضمانات.

الخطر هو: مقياس تكلفة الثغرة الأمنية (النظر في احتمالية هجوم ناجح).

خدمة الأمن هي إجراء يمكن وضعه لمواجهة تهديد (على سبيل المثال ، توفير السرية).

آلية الأمن هي وسيلة لتقديم خدمة (مثل التشفير والتوقيع الرقمي).

confidentiality, integrity, availability or legitimate use). An example of threats (information leakage, integrity violation, illegitimate use, …).

An attack is: a realization of a threat (e.g., stealing data, denial of service attack).

Safeguards are measures (e.g., controls, procedures) to protect against threats.

Vulnerabilities are weaknesses in safeguards.

A Risk is: a measure of the cost of a vulnerability (considering probability of a successful attack).

A security service is a measure which can be put in place to address a threat (e.g., provision of confidentiality).

A security mechanism is a means to provide a service (e.g., encryption, digital signature).

5.Security Attacks

5.1. Passive Attacks

5.2. Active Attacks The most important active attacks are:

- Impersonation (or masquerade): In this type of attack, the attacker pretends to be one of the legitimate parties (the sender or the receiver).
- Replay attack
- Modification of messages
- Denial of services

6.Security Services

6.1. Authentication: (Identification – Verification)

Therefore, authentication can be divided into two services:

- Entity authentication.
- Data origin authentication.

6.2. Data Confidentiality

6.3. Data Integrity

6.4. Access Control

6.5. Nonrepudiation

7.Security Mechanisms

The most important security mechanisms are:

- Encipherment Mechanisms
- Digital Signature Mechanisms
- Access Control Mechanisms
- Data Integrity Mechanisms
- Authentication Exchange Mechanisms
- Traffic Padding Mechanisms

٥- الهجمات الأمنية

٥,١ الهجمات السلبية

٥,٢ الهجمات النشطة - أهم الهجمات النشطة هي:

- انتحال الهوية (أو التنكر): في هذا النوع من الهجوم ، يتظاهر المهاجم بأنه أحد الأطراف الشرعية (المرسل أو المستلم).
- إعادة الهجوم
- تعديل الرسائل
- الحرمان من الخدمات

٦- خدمات الأمن

٦,١ المصادقة: (تحديد - التحقق)

لذلك ، يمكن تقسيم المصادقة إلى خدمتين:

- مصادقة الكيان.
- مصادقة أصل البيانات.

٦,٢ سرية البيانات

٦,٣ تكامل البيانات

٦,٤. صلاحية التحكم صلاحية الدخول

٦,٥. عدم التنصل

٧- آليات الأمن

أهم آليات الأمان هي:

- آليات التشفير
- آليات التوقيع الرقمي
- آليات التحكم في الوصول
- آليات سلامة البيانات
- آليات تبادل المصادقة
- آليات التعبئة المرورية
- Routing آليات التحكم
- آليات الإشعار

- Routing Control Mechanisms
- Notarization Mechanisms

8.Security Services and Layers

Layers \ Service	1	2	3	4	5	6	7
Entity Authentication			Y	Y			Y
Data Origin Authentication			Y	Y			Y
Access Control			Y	Y			Y
Confidentiality	Y	Y	Y	Y			Y
Traffic Flow Confidentiality	Y		Y				Y
Data Integrity			Y	Y			Y
Nonrepudiation							Y

CH2 Security at Network Layers

1.Introduction

In this chapter, we take a layer–by–layer look at the most important network components and protocols, and associated security issues:

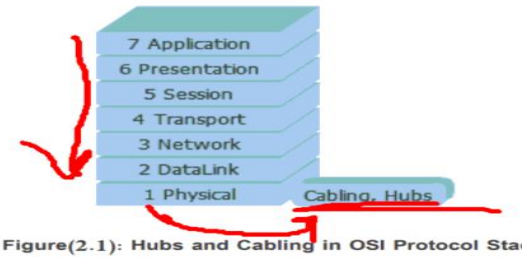
- Cabling and Hubs (Layer 1), Sniffers
- Switches and MAC (Layer 2)
- Routers and IP (Layer 3)
- TCP, UDP and ICMP (Layer 4)

2.Layer 1: Cabling and Hubs

2.1. Cabling Security Issues

All four fundamental threats can be realized by attacks on cabling:

- **Information Leakage**: attacker taps cabling and reads traffic, any intrusion into network cables may threaten your information systems and hence the confidentiality of your information.
- **Integrity Violation**
- **Denial of Service**.
- **Illegitimate Use**: attacker taps cabling and uses network resources.



Figure(2.1): Hubs and Cabling in OSI Protocol Stack

٢- الطبقة ١: الكابلات والمحاور

٢,١. مشاكل أمان الكابلات

يمكن إدراك التهديدات الأساسية الأربعة من خلال الهجمات على الكابلات:

- تسرب المعلومات: ينقر المهاجم على الكابلات ويقرأ حركة المرور ، وأي اختراق في كبلات الشبكة قد يهدد أنظمة المعلومات الخاصة بك وبالتالي سرية معلوماتك.
- انتهاك النزاهة
- رفض الخدمة.
- الاستخدام غير المشروع: ينقر المهاجم على الكابلات ويستخدم موارد الشبكة.

بعض العوامل المساهمة في تقييم المخاطر:

- مبنى فردي أو متعدد الوظائف؟
- كيف يتم التحكم في الوصول إلى الطابق / المبنى؟
- هل تمر كابلات الشبكة عبر المناطق العامة؟
- هل البنية التحتية للشبكة يسهل الوصول إليها أم أنها مشتركة؟
- ما هي البيئة الكهرومغناطيسية مثل؟
- هل هناك أي اتصال لاسلكي في البنية التحتية لشبكتك؟

Some contributory factors in assessing risk:

- Single or multi-occupancy building?
- How is access controlled to floor/building?
- Does network cabling pass through public areas?
- Is the network infrastructure easily accessible or is it shared?
- What is the electromagnetic environment like?
- Is there any wireless connection in your network infrastructure?

Safeguards:

- Consider separating the network wiring from all other wiring, so as to protect and monitor it more easily, and to reduce the danger of accidental electronic interference.
- Where rodent damage is possible, consider installing armored cable.
- For very high-security situations, consider laying the cable in transparent conduit, thereby allowing ready identification of any interference.
- Ensure that all devices such as data scopes, that may facilitate tapping of communications lines, are controlled effectively.
- Ensure that network access points are disabled if equipment is removed.
- Ensure that the incoming and outgoing services, including communications lines, are hidden from view, and are adequately protected against damage.
- Ensure applying the security policy of wireless connections.

الضمانات:

- النظر في فصل أسلاك الشبكة عن جميع الأسلاك الأخرى ، وذلك لحمايتها ومراقبتها بسهولة أكبر ، ولتقليل خطر التداخل الإلكتروني العرضي.
- عندما يكون الضرر بالقوارض محتملاً ، ضع في اعتبارك تركيب كبلات مصفحة.
- في حالات الأمان المشددة للغاية ، ضع في اعتبارك وضع الكبل في قناة شفافة ، مما يتيح التعرف بسهولة على أي تداخل.
- التأكد من أن جميع الأجهزة مثل نطاقات البيانات ، التي قد تسهل التنصت على خطوط الاتصالات ، يتم التحكم فيها بشكل فعال.
- تأكد من تعطيل نقاط الوصول إلى الشبكة في حالة إزالة الجهاز.
- التأكد من أن الخدمات الواردة والصادرة ، بما في ذلك خطوط الاتصالات ، مخفية عن الأنظار ، وأنها محمية بشكل كاف من التلف.
- التأكد من تطبيق السياسة الأمنية للاتصالات اللاسلكية.

٣-متشمم الشبكة

تعمل بطاقات واجهة الشبكة (NIC) عادةً في الوضع غير المختلط. على سبيل المثال ، يستمعون فقط إلى الإطارات باستخدام عنوان MAC الخاص بهم. متلصص الحزم هو تطبيق برمجي يستخدم NIC في وضع مختلط لالتقاط كل حزم الشبكة المرسلة عبر قطاع الشبكة ، أي يقرأ الإطارات بغض النظر عن عنوان MAC.

سؤال الامتحان: صح أم خطأ

تعمل بطاقات واجهة الشبكة (NIC) عادةً في الوضع غير المختلط.

حقيقي

خطأ شنيع

٣,١. كشف المتشمم

يكون الأمر أكثر صعوبة على الشبكة ، وتشمل بعض الأساليب:

- إرسال كميات كبيرة من البيانات ، ثم إرسال طلب ping لـ ICMP ومراقبة التأخير حيث يقوم المتشمم بمعالجة كمية كبيرة من البيانات.
- إرسال البيانات إلى عناوين IP غير المستخدمة ومراقبة طلبات DNS لعناوين IP هذه.

٤. الطبقة ٢: مفاتيح

الشم السلبي مع المحور

نشط شم مع مفتاح

سؤال الامتحان: صح أم خطأ

حدث انتحال ARP عندما أرسل أي شخص طلب ARP عبر الشبكة.

حقيقي

خطأ حدثت المشكلة عندما تم تحديث جدول عناوين MAC بمجرد تلقي رد ARP بدون طلب ARP.

3.Network Sniffers

Network Interface Cards (NICs) normally operate in non-promiscuous mode. i.e., they only listen for frames with their MAC address. A packet sniffer is a software application that uses a NIC in a promiscuous mode to capture all network packet sent across a network segment, i.e., Reads frames regardless of MAC address.

Exam Question: True or False

Network Interface Cards (NICs) normally operate in non-promiscuous mode.

True

False

3.1. Detecting Sniffer

Over a network it is more difficult, some approaches include:

- Sending large volumes of data, then sending ICMP ping request and observing delay as sniffer processes large amount of data.
- Sending data to unused IP addresses and watching for DNS requests for those IP addresses.

4.Layer 2: Switches

Passive Sniffing with Hub

Active Sniffing with switch

كيف تعمل ثغرة بروتوكول ال ARP؟

لدينا حاسب يريد أن يرسل رسالة معينة إلى جهة ما، فهو يملك عنوان ال IP لهذه الجهة ويحتاج إلى عنوان MAC لأن ال Switch تتخاطب عن طريق ال MAC address، فيقوم الحاسب بأول مرحلة بسؤال جدول ال ARP المبني عنده، في حال كانت المعلومة غير موجودة بجدول ال ARP أي عنوان ال MAC غير معلوم للجهة المستقبلة، فسيقوم الحاسب بإرسال طلب ARP Request من نوع Broadcast عبر الشبكة، والحاسب صاحب ال IP المطلوب يقوم بالرد على الرسالة برسالة MAC address خاصته.

تكمن ثغرة ال ARP في إمكانية إرسال رسائل ARP reply من دون ARP request.

Exam Question: True or False

ARP spoofing happened when anyone sent an ARP request over the network.

True

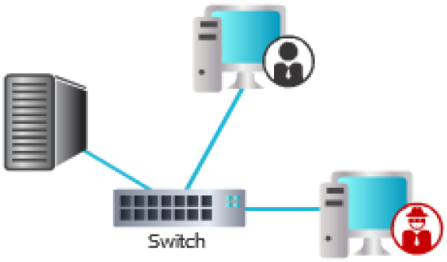
False The problem happened when the MAC address table updated once received an ARP reply without ARP request.

4.4. Mac Flooding

When a malicious device connected to switch, and sends multiple gratuitous ARPs. Each ARP claims a different MAC address. When index fills:

- Some switches act like a hub, where all packets are broadcast to all computers. This is known as a device *failing open*, thus removing all security provisions.
- Devices that *fail close* will incorporate some sort of security measures, such as shutting down all communications, and ignore any new devices attempting to connect.

	Device	MAC address
1	1	00:0e:81:10:19:FC
2	4	00:0e:81:32:96:af
3	4	00:0e:81:32:96:b0
4	4	00:0e:81:32:96:b1
	...	...
9999	4	00:0e:81:32:97:a4



Failing open device, is not recommended at all and there is no security on this.

٤,٥ تبديل الإجراءات الوقائية

- تأمين المفتاح جسديًا: يمنع التهديد بالاستخدام غير المشروع
- يجب أن تكون المفاتيح آمنة من الأعطال عند غمرها بالمياه
- ساعة اليد
- استخدام مخابئ ARP الثابتة
- ميناء الأمن

٥. الطبقة ٣: الموجهات

يعد إرسال واستقبال حزم IP طريقة أساسية تتواصل بها أجهزة الكمبيوتر المتصلة بالشبكة والأجهزة الأخرى ويشكل أساس الإنترنت الحديث.

4.5. Switch Safeguards

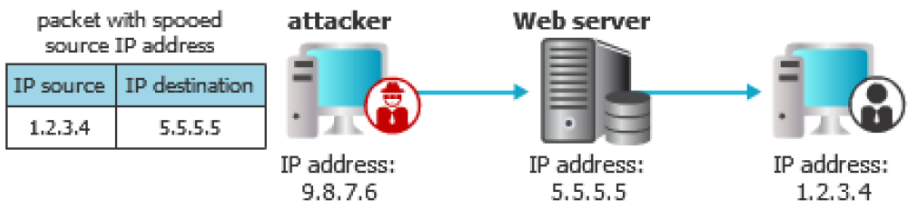
- Physically secure the switch: Prevents threat of illegitimate use

- Switches should failsafe when flooded
- Arpwatch
- Use static ARP caches
- Port security

5.Layer 3: Routers

Sending and receiving IP packets is a primary way in which networked computers and other devices communicate and constitutes the basis of the modern internet.

5.1.IP Spoofing



5.2.Reflected Denial of Service Attack (DoS)

- DNS amplification: An ANY query originating from a target's spoofed address is sent to numerous unsecured DNS resolvers.

Each 60-byte request can prompt a 4000-byte response, enabling attackers to magnify traffic output by as much as 1:70.

- Smurf attack: An ICMP Echo request is sent from a target's spoofed address to an intermediate broadcast network, triggering replies from every device on that network. The degree of amplification is based on the number of devices to which the request is broadcast. For example, a network with 50 connected hosts results in a 1:50 amplification.
- NTP amplification: A get monist request, containing a target's spoofed IP address, is sent to an unsecure NTP server. As in DNS amplification, a small request triggers a much larger response, allowing a maximum amplification ratio of 1:200.

5.2هجوم رفض الخدمة المنعكس (DoS)

•تضخيم DNS: يتم إرسال أي استعلام ينشأ من عنوان مخادع لهدف إلى العديد من محللي DNS غير الآمنين. يمكن أن يؤدي كل طلب بحجم ٦٠ بايت إلى استجابة ٤٠٠٠ بايت ، مما يتيح للمهاجمين تضخيم ناتج حركة المرور بنسبة تصل إلى ١:٧٠.

• هجوم Smurf: يتم إرسال طلب ICMP Echo من عنوان مخادع للهدف إلى شبكة بث وسيطة ، مما يؤدي إلى ردود من كل جهاز على تلك الشبكة. تعتمد درجة التضخيم على عدد الأجهزة التي يتم بث الطلب عليها. على سبيل المثال ، تؤدي الشبكة التي تحتوي على ٥٠ مضيفًا متصلًا إلى تضخيم بنسبة ١:٥٠.

• تضخيم NTP: يتم إرسال طلب الحصول على monist ، الذي يحتوي على عنوان IP المخادع للهدف ، إلى خادم NTP غير آمن. كما هو الحال في تضخيم DNS ، يؤدي الطلب الصغير إلى استجابة أكبر بكثير ، مما يسمح بنسبة تضخيم قصوى تبلغ ١: ٢٠٠.

٥,٣ حماية انتحال الملكية الفكرية

ترشيح الدخول هو شكل من أشكال تصفية الحزمة يتم تنفيذه عادةً على جهاز حافة الشبكة الذي يفحص حزم IP الواردة وينظر في رؤوس المصدر الخاصة بها. بالإضافة إلى ذلك ، باستخدام مرشح ingress ، يمكننا منع عمليات البث الواردة من الإنترنت إلى شبكاتنا ومنع الحزم الواردة من الشبكات غير القابلة للتوجيه.

٥,٤. تهديدات معلومات التوجيه

٦. الطبقة ٤: TCP، UDP، ICMP Issues

عندما يتم إقران منفذ بعنوان IP الخاص بالجهاز البعيد الذي نهتم بمنفذه ، يُعرف الكيان المقترن باسم المقبس.

٦,١ هجوم الفيضانات

تتكون العملية من التبادل التالي لحزم التزامن (SYN) والإقرار (ACK) (انظر الشكل ٢,١٢):

- حزمة SYN من المرسل إلى المتلقي. "أيمكننا أن تحدث؟"
- حزمة SYN / ACK من المتلقي إلى المرسل. "حسنًا - جاهز للبدء؟"
- حزمة ACK من المرسل إلى المستلم. "طيب بداية"

تم استلام طلب SYN ملفق آخر. يؤدي هذا إلى إرباك موارد النظام المستهدف ويمنع المستخدمين الشرعيين من إنشاء اتصالات.

5.3. IP Spoofing Safeguard

Ingress filtering is a form of packet filtering usually implemented on a network edge device which examines incoming IP packets and looks at their source headers. In addition, by using ingress filter we can Forbid inbound broadcasts from the internet into our networks and forbid inbound packets from non-routable networks.

5.4. Routing Information Threats

6.Layer 4: TCP, UDP, ICMP Issues

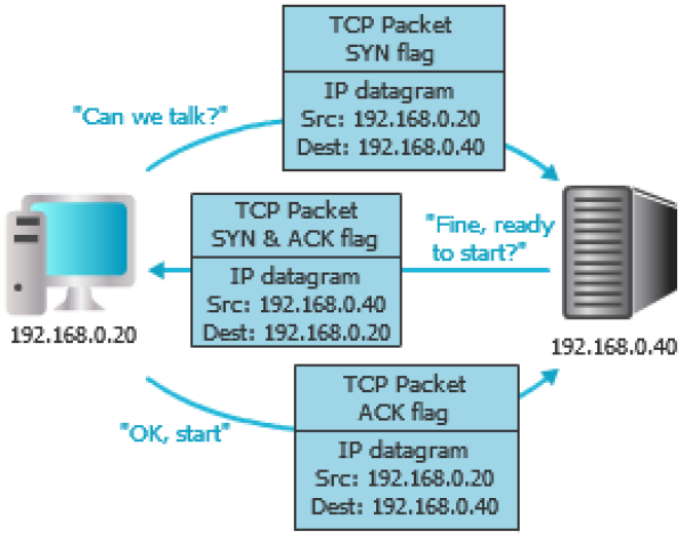
When a port is paired up with the IP address of the remote machine whose port we are interested in, the paired entity is known as a socket.

6.1.SYN Flooding Attack

The process consists of the following exchange of synchronization (SYN) and acknowledgement (ACK) packets (see figure 2.12):

- A SYN packet from sender to receiver. “Can we talk?”
- An SYN/ACK packet from receiver to sender. “Fine – ready to start?”
- An ACK packet from sender to receiver. “OK, start”

another fabricated SYN request is received. This overwhelms the target system’s resources and prevents legitimate users from establishing connections.



Figure(2.12): TCP Handshake

Exam Question: What is the reason of IP spoofing?

Because of any one in the network can send a message with fake IP address.

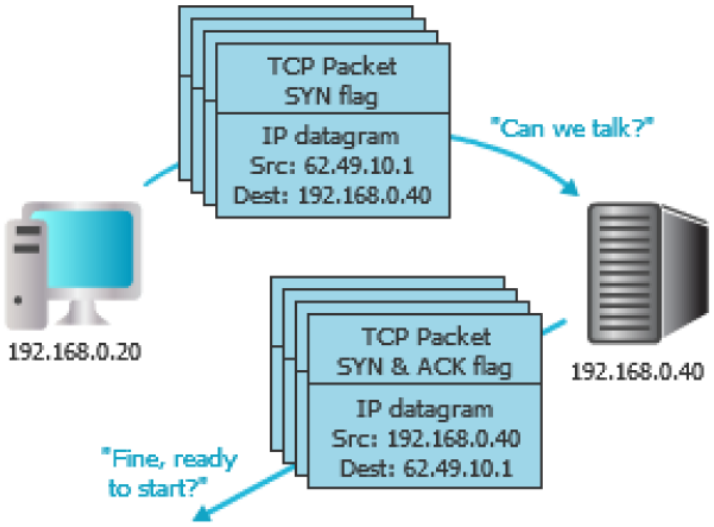
Exam Question: What is the reason of SYN flooding?

Not send an ACK flag reply.

سؤال الامتحان: ما هو سبب انتحالIP ؟ بسبب أي شخص في الشبكة يمكن إرسال رسالة بعنوان IP وهمية.

سؤال الامتحان: ما هو سبب فيضانSYN ؟ عدم إرسال رد علم.ACK

6.2.TCP Denial of Service + IP Spoofing



Figure(2.13): TCP DOS Attack + IP Spoofing

Safeguard: There are several common techniques to mitigate **SYN flood attacks**, including:

SYN Cookies: using cryptographic hashing, the server sends its SYN-ACK response with a sequence number that is constructed from the client IP address, port number, and possibly other unique identifying information. When the client responds, this hash is included in the ACK packet. The server verifies the ACK, and only then allocates memory for the connection.

RST Cookies: for the first request from a given client, the server intentionally sends an invalid SYN-ACK. This should result in the client generating an RST packet, which tells the server something is wrong. If this is received, the server knows the request is legitimate.

Stack Tweaking: administrators can tweak TCP stacks to mitigate the effect of SYN floods. This can either involve reducing the timeout until a stack frees memory allocated to a connection, or selectively dropping incoming connections.

Exam Question: The safeguards from SYN flooding are:

- **SYN Cookies**
- **RST Cookies**
- **Stack Tweaking**
- Html Cookies

6.3.UDP Flooding Attack

UDP flood DOS attacks are exceptionally dangerous because they can be executed with a limited number of resources.

6.4. The Internet Control Message Protocol (ICMP)

Exam Question: True or False

Trace route is using to test the connection between two devices.

True

✓ False It's PING not Trace Route.

الحماية: هناك العديد من التقنيات الشائعة للتخفيف من هجمات فيضان SYN ، بما في ذلك:

ملفات تعريف الارتباط SYN: باستخدام التجزئة المشفرة ، يرسل الخادم استجابة SYN-ACK الخاصة به برقم تسلسلي تم إنشاؤه من عنوان IP للعميل ورقم المنفذ وربما معلومات تعريف فريدة أخرى. عندما يستجيب العميل ، يتم تضمين هذه التجزئة في حزمة ACK. يتحقق الخادم من ACK ، وعندها فقط يخصص ذاكرة للاتصال.

ملفات تعريف الارتباط RST: للطلب الأول من عميل معين ، يرسل الخادم عن قصد SYN-ACK غير صالح. يجب أن يؤدي هذا إلى قيام العميل بإنشاء حزمة RST ، والتي تخبر الخادم بوجود خطأ ما. إذا تم استلام هذا ، يعرف الخادم أن الطلب شرعي.

التغيير والتبديل في المكدس: يمكن للمسؤولين تعديل حزم TCP للتخفيف من تأثير فيضانات SYN. يمكن أن يتضمن ذلك إما تقليل المهلة حتى يحرر المكدس الذاكرة المخصصة للاتصال ، أو بشكل انتقائي إسقاط الاتصالات الواردة.

سؤال الامتحان: الضمانات من فيضان SYN هي:

- ملفات تعريف الارتباط SYN
- ملفات تعريف الارتباط RST
- التغيير والتبديل المكدس
- ملفات تعريف الارتباط Html

٦,٣ هجوم الفيضانات UDP

تعتبر هجمات UDP فيض DOS خطيرة بشكل استثنائي لأنه يمكن تنفيذها بعدد محدود من الموارد.

٦,٤. بروتوكول رسائل التحكم في الإنترنت (ICMP)

سؤال الامتحان: صح أم خطأ

يستخدم مسار التتبع لاختبار الاتصال بين جهازين.

حقيقي

خطأ إنه أمر PING وليس تتبع المسار

What is ICMP Used For?

The primary purpose of ICMP is for error reporting. The traceroute utility is used to display the routing path between two devices.

The traceroute utility is used to display the routing path between two Internet devices.

A ping will test the speed of the connection between two devices and report exactly how long it takes a packet of data to reach its destination and come back to the sender's device.

6.5. ICMP Security Vulnerabilities

Ping sweep

Ping flood

ICMP tunneling

Forged ICMP redirects

6.6. Securing Against Denial-of-Service Attacks

How to Mitigate DoS Attacks

IP Whitelisting/Blacklisting

Upstream Filtering: For example, Amazon Shield and Cloudflare both offer products that allow for protection against DoS and DDoS attacks by checking incoming packet IPs against known attackers and botnets and attempt to only forward legitimate traffic.

ما هو استخدام ICMP؟
الغرض الأساسي من ICMP هو الإبلاغ عن الأخطاء. تُستخدم الأداة المساعدة traceroute لعرض مسار التوجيه بين جهازين.
تُستخدم الأداة المساعدة traceroute لعرض مسار التوجيه بين جهازي إنترنت.
سيختبر ping سرعة الاتصال بين جهازين ويبلغ بالضبط المدة التي تستغرقها حزمة البيانات للوصول إلى وجهتها والعودة إلى جهاز المرسل.
٦,٥. ثغرات أمان ICMP
اكتساح بينغ
فيضان بينغ
نفق ICMP
عمليات إعادة توجيه ICMP المزورة
٦,٦. الحماية من هجمات رفض الخدمة
كيفية التخفيف من هجمات DoS
قائمة IP البيضاء / القائمة السوداء
التصفية الأولية: على سبيل المثال ، يقدم كل من Amazon Shield و Cloudflare منتجات تسمح بالحماية من هجمات DoS و DDoS عن طريق التحقق من عناوين IP للحزم الواردة ضد المهاجمين والشبكات الروبوتية المعروفة ومحاولة إعادة توجيه حركة المرور المشروعة فقط.

Ch3 Network Security Technologies

2.Firewalls: The following capabilities are within the scope of a firewall:

1. A firewall defines a single choke point that keeps unauthorized users out of the protected network, prohibits potentially vulnerable services from entering or leaving the network, and provides protection from various kinds of IP spoofing and routing attacks.
2. A firewall provides a location for monitoring security-related events.
3. A firewall is a convenient platform for several Internet functions that are not security related. These include a network address translator,
4. A firewall can serve as the platform for IPsec.

٢-الجدران النارية: القدرات التالية تدخل في نطاق جدار الحماية:
١. يحدد جدار الحماية نقطة الاختناق الفردية التي تُبقي المستخدمين غير المصرح لهم خارج الشبكة المحمية ، ويمنع الخدمات التي يُحتمل تعرضها للخطر من دخول الشبكة أو مغادرتها ، ويوفر الحماية من أنواع مختلفة من انتحال بروتوكول الإنترنت وهجمات التوجيه.
٢. يوفر جدار الحماية موقعًا لمراقبة الأحداث المتعلقة بالأمان.
٣. جدار الحماية عبارة عن منصة ملائمة للعديد من وظائف الإنترنت التي لا تتعلق بالأمان. يتضمن ذلك مترجم عناوين الشبكة
٤. يمكن أن يعمل جدار الحماية كمنصة لـ IPsec.
للجدران النارية حدودها ، بما في ذلك ما يلي:
١. لا يمكن لجدار الحماية الحماية من الهجمات التي تتجاوز جدار الحماية.
٢. قد لا يوفر جدار الحماية الحماية الكاملة من التهديدات الداخلية ،
٣. قد يتم الوصول إلى شبكة LAN لاسلكية مؤمنة بشكل غير صحيح من خارج المؤسسة.
٤. قد يتم استخدام الكمبيوتر المحمول أو المساعد الرقمي الشخصي أو جهاز التخزين المحمول وإصابته خارج شبكة الشركة ، ثم يتم توصيله واستخدامه داخليًا. (BYOD)

Firewalls have their limitations, including the following:

a) The firewall cannot protect against attacks that bypass the firewall.

b) The firewall may not protect fully against internal threats,

c) An improperly secured wireless LAN may be accessed from outside the organization.

d) A laptop, PDA, or portable storage device may be used and infected outside the corporate network, and then attached and used internally. (BYOD)

3.Types of Firewalls

The choice of which level is appropriate is determined by the desired firewall access policy. It can operate as a **positive filter**, allowing to pass only packets that meet specific criteria, or as a **negative filter**

3.1. Packet Filtering Firewall

Two default policies are possible:

- Default discard:

That which is not expressly permitted is prohibited.

- **Default forward**:

That which is not expressly prohibited is permitted.

One advantage of a packet filtering firewall is its **simplicity**.

The main weaknesses of packet filter firewalls are:

- Because packet filter firewalls do not examine upper-layer data,
- Because of the limited information available to the firewall, the logging functionality present in packet filter firewalls is limited.
- Packet filter firewalls are generally vulnerable to attacks and exploits that take advantage of problems within the TCP/IP specification and protocol stack, such as network layer address spoofing.
- Finally, due to the small number of variables used in access control decisions, packet filter firewalls are susceptible to security breaches caused by improper configurations.

3.2. Stateful Inspection Firewalls (Dynamic Packet Filtering)

The main advantages of stateful inspection firewalls are:

- A stateful firewall provides full protocol inspection, thereby eliminating additional attacks surface.
- A stateful firewall acts a building block for more advanced application layer firewalls or gateways.
- A stateful firewall understands the network flow and can

٣. أنواع جدران الحماية

يتم تحديد اختيار المستوى المناسب من خلال نهج الوصول إلى جدار الحماية المطلوب. يمكن أن تعمل **كمرشح إيجابي** ، السماح بتمرير الحزم التي تلبي معايير محددة فقط ، أو كعامل **تصفية سلبي**

٣,١. جدار حماية تصفية الحزمة

هناك سياستان افتراضيتان ممكنتان:

- **الإهمال الافتراضي**: يحظر ما هو غير مسموح به صراحة.
- **إعادة التوجيه الافتراضي: ما هو غير محظور صراحة مسموح به.**

تتمثل إحدى ميزات جدار حماية تصفية الحزمة في بساطته.

نقاط الضعف الرئيسية في جدران الحماية لمرشح الحزمة هي:

- لأن جدران الحماية لمرشح الحزمة لا تفحص بيانات الطبقة العليا
- نظرًا لمحدودية المعلومات المتاحة لجدار الحماية ، فإن وظيفة التسجيل الموجودة في جدران الحماية لمرشح الحزمة محدودة.
- تعد جدران الحماية لمرشح الحزمة عرضة بشكل عام للهجمات وعمليات الاستغلال التي تستفيد من المشكلات الموجودة في مواصفات TCP / IP ومكدس البروتوكولات ، مثل انتحال عنوان طبقة الشبكة.
- أخيرًا ، نظرًا للعدد القليل من المتغيرات المستخدمة في قرارات التحكم في الوصول ، فإن جدران الحماية لمرشح الحزمة عرضة للانتهاكات الأمنية التي تسببها التكوينات غير الصحيحة.

٣,٢ جدران حماية فحص الحالة (تصفية الحزمة الديناميكية)

المزايا الرئيسية لجدران الحماية ذات الحالة الخاصة هي:

- يوفر جدار الحماية المصمم للحالة فحصًا كاملاً للبروتوكول ، وبالتالي يقضي على سطح الهجمات الإضافية.
- يعمل جدار الحماية الذي يتمتع بالحالة على كتلة إنشاء لجدران حماية أو بوابات طبقة التطبيقات الأكثر تقدمًا.
- يتفهم جدار الحماية ذو الحالة الخاصة تدفق الشبكة ويمكنه تحديد حزم البيانات الخاصة بالتدفق ، وبالتالي تمكين كتابة القواعد البسيطة للاتصالات ثنائية الاتجاه أو بروتوكولات شبكات الحالة الزائفة.
- نظرًا لأن جدار الحماية ذي الحالة يمكن أن يبحث بشكل أعمق في حمولات الحزمة ، فيمكنه فهم البروتوكولات المعقدة التي تتفاوض على منفذ الاتصال والبروتوكول في وقت التشغيل وتطبيق سياسات جدار الحماية وفقًا لذلك. ومن أمثلة هذه البروتوكولات FTP وبروتوكولات P2P وما إلى ذلك.

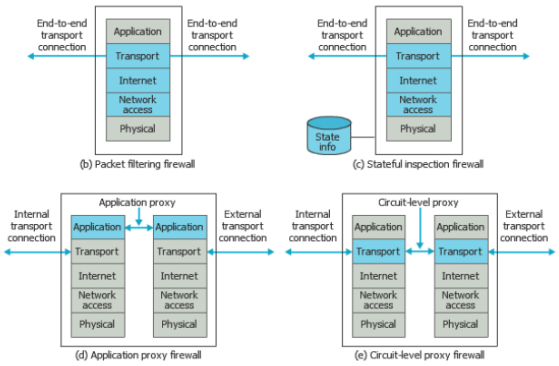
٣,٣ وكيل مستوى التطبيق

٣,٤. بوابة على مستوى الدائرة

identify data packets of a flow, thereby enabling simple rule writing for bidirectional connections or pseudo state networking protocols.

• Since a stateful firewall can look deeper into packet payloads, it can understand complex protocols that negotiate communication port and protocol at runtime and apply firewall policies accordingly. Examples of such protocols are FTP, P2P protocols, etc.

3.3.Application Level Proxy
3.4. Circuit -Level Gateway



Figure(3.1): Type of Firewalls [1]

3.5. Choosing a Firewall

The most secure firewall is Application Proxy firewall

The less security firewall is Packet filtering firewall

The most speed firewall is Stateful inspection firewall

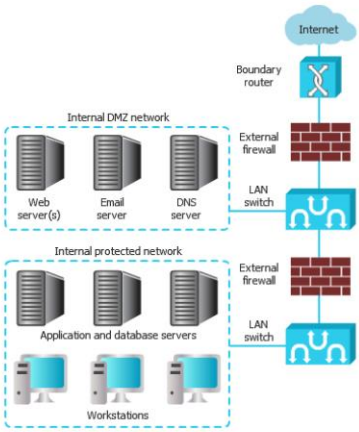
The less speed firewall is Application Proxy firewall

The firewall which checks the TCP connection is Circuit–Level firewall

٣,٥ اختيار جدار حماية
جدار الحماية الأكثر أمانًا هو جدار حماية وكيل التطبيق
جدار الحماية الأقل أمانًا هو جدار حماية تصفية الحزمة
أسرع جدار حماية هو جدار حماية التفتيش الحاصل
جدار الحماية الأقل سرعة هو جدار حماية وكيل التطبيق
جدار الحماية الذي يتحقق من اتصال TCP هو جدار الحماية على مستوى الدائرة

4.Firewall Location and Configuration

4.1.DMZ Networks



Figure(3.2): Firewall Networking [2]

٤. موقع جدار الحماية والتكوين
٤,١.DMZ Networks

سؤال الامتحان: ⍰ لا يمكننا الاحتفاظ بالخوادم التالية في منطقة ⍰ :DMZ
خوادم قواعد البيانات
خوادم الويب
سؤال الامتحان: أي خادم يمكننا الاحتفاظ به في منطقة DMZ:
خوادم قواعد البيانات
خوادم الويب

٥. ما الذي لا تفعله جدران الحماية؟
أهمها:
- الاستخدام الضار للخدمات المصرح بها
- المستخدمون لا يمرون عبر جدار الحماية
- الهندسة الاجتماعية
- عيوب في نظام التشغيل المضيف
- لا يقوم مرشح الحزمة ومستوى الدائرة والجدران النارية ذات الحالة بفحص المحتوى. (سؤال الامتحان)

البيانات المشفرة مشكلة للجدران النارية.

Exam Question:

We can't keep the following servers in DMZ zone:

Database servers

Web servers

Exam Question:

Which server we can keep it in DMZ zone:

Database servers

Web servers

5.What Do not Firewalls Do?

The most important ones are:

- Malicious use of authorized services
- Users not going through the firewall
- Social engineering
- Flaws in the host operating system
- Packet filter, circuit level, and stateful firewalls do not check content. **(Exam Question)**

Encrypted data is a problem for Firewalls.

7.Intrusion Detection System (IDS)

The following capabilities are within the scope of Intrusion detection systems:

- Monitoring and analysis of system events and user behaviors.
- Testing the security states of system configurations.
- Baselining the security state of a system, then tracking any changes to that baseline.
- Managing operating system audit and logging mechanisms and the data they generate.
- Alerting appropriate staff by appropriate means when attacks are detected.
- Measuring enforcement of security policies encoded in the analysis engine.
- Providing default information security policies.
- Allowing non-security experts to perform important security monitoring functions.

Intrusion detection systems have their limitations, including the following:

- Directly detecting, reporting, and responding to an attack, when there is a heavy network or processing load.
- Automatically investigating attacks without human intervention.
- Compensating for problems with the fidelity of information sources.
- Dealing effectively with switched networks.

٧- نظام كشف الاقتحام (IDS)

القدرات التالية تقع ضمن نطاق أنظمة كشف التطفل:

- رصد وتحليل أحداث النظام وسلوكيات المستخدم.
- اختبار الحالات الأمنية لتكوينات النظام.
- تحديد معايير الحالة الأمنية لنظام ما ، ثم تتبع أي تغييرات تطرأ على خط الأساس هذا.
- إدارة تدقيق نظام التشغيل وآليات التسجيل والبيانات التي تولدها.
- تنبيه الموظفين المناسبين بالوسائل المناسبة عند اكتشاف الهجمات.
- قياس تطبيق السياسات الأمنية المشفرة في محرك التحليل.
- توفير سياسات أمن المعلومات الافتراضية.
- السماح للخبراء غير الأمنيين بأداء وظائف مراقبة أمنية مهمة.

أنظمة كشف التسلل لها حدودها ، بما في ذلك ما يلي:

- الاكتشاف المباشر للهجوم والإبلاغ عنه والاستجابة له ، عند وجود شبكة ثقيلة أو حمولة معالجة.
- التحقيق تلقائيًا في الهجمات دون تدخل بشري.
- التعويض عن مشاكل دقة مصادر المعلومات.
- التعامل بفاعلية مع الشبكات المحولة.

٩. نهج كشف الاقتحام

كشف قائم على التوقيع

يحدد التوقيع خصائص الهجوم (بروتوكول ، خدمة ، مصدر ، ونمط). قد تتضمن أمثلة التوقيعات ما يلي:

- عدة محاولات تسجيل دخول فاشلة مؤخرًا على مضيف حساس
- نمط معين من البتات في حزمة IP
- أنواع معينة من حزم TCP SYN ، مما يشير إلى هجوم DoS فيضان SYN

كشف الشذوذ الإحصائي

يثير هذا مسألة

الإيجابيات الكاذبة

(يتم الإبلاغ عن الهجوم عندما لا يحدث - إنذار كاذب)

والسلبيات الكاذبة

(تم تفويت الهجوم لأنه وقع في حدود السلوك الطبيعي).

9.Intrusion Detection Approach

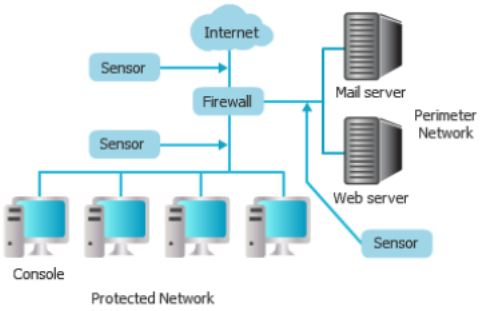
1-Signature Based Detection

A signature defines the characteristics of an attack (protocol, service, source, and pattern). Example signatures might include:

- Several recent failed logins attempt on a sensitive host
- A certain pattern of bits in an IP packet
- Certain types of TCP SYN packets, indicating a SYN flood DoS attack

2-Statistical Anomaly Detection

This raises the issue of
false positives
(an attack is flagged when one was not taking place – a false alarm) **and**
false negatives
(an attack was missed because it fell within the bounds of normal behavior).



Figure(3.4): Placement of Network-based IDS

10.Types of IDS

1-Network Intrusion Detection System (NIDS)

NIDS usually consists of a network appliance (or sensor) with a Network Interface Card (NIC) operating in promiscuous mode (sniffer) and a separate management interface.

2-Host Intrusion Detection System (HIDS)

A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.

These controls may include:

System processes, registry entries, CPU Usage, file access and integrity checking, audit policies,

The most Deployment options are:

- Key servers that contain mission-critical and sensitive information
- Web servers
- FTP and DNS servers
- E-commerce database servers, etc.

Network-based IDS vs. Host-based IDS

HIDS systems have some advantages comparing to NIDS:

- They can verify if an attack was successful or not, whereas a network-based IDS only give an alert of the attack.

١٠- أنواع IDS

نظام كشف التسلل إلى الشبكة (NIDS)

تتكون NIDS عادةً من جهاز شبكة (أو جهاز استشعار) مزود ببطاقة واجهة شبكة (NIC) تعمل في الوضع المختلط (الشم) وواجهة إدارة منفصلة.

نظام كشف اختراق المضيف (HIDS)

يراقب HIDS الحزم الواردة والصادرة من الجهاز فقط وينبه المسؤول في حالة اكتشاف نشاط مشبوه أو ضار.

قد تشمل هذه الضوابط: عمليات النظام ، وإدخالات التسجيل ، واستخدام وحدة المعالجة المركزية ، والوصول إلى الملفات والتحقق من النزاهة ، وسياسات التدقيق ،

أكثر خيارات النشر هي:

- الخوادم الرئيسية التي تحتوي على معلومات حساسة ومهمة
- خوادم الويب
- خوادم FTP و DNS
- خوادم قواعد بيانات التجارة الإلكترونية ، إلخ.

IDS المستندة إلى الشبكة مقابل IDS المستندة إلى المضيف

تتمتع أنظمة HIDS ببعض المزايا مقارنةً بـ NIDS:

- يمكنهم التحقق مما إذا كان الهجوم ناجحًا أم لا ، في حين أن نظام IDS القائم على الشبكة يعطي فقط تنبيهًا بالهجوم.
- يمكنهم مراقبة أنشطة جميع المستخدمين وهو أمر غير ممكن في نظام قائم على الشبكة.
- يمكنهم تحديد الهجمات التي تنشأ من داخل المضيف.
- يمكن للنظام القائم على المضيف تحليل حركة المرور التي تم فك تشفيرها للعثور على توقيع الهجوم - وبالتالي منحهم القدرة على مراقبة حركة المرور المشفرة.
- لا تتطلب أي أجهزة إضافية حيث يمكن تثبيتها في الخوادم المضيفة الحالية.
- أنها فعالة من حيث التكلفة لشبكة صغيرة بها عدد قليل من الأجهزة المضيفة.
- بعض الأمثلة على الهجمات التي تم منعها بواسطة HIDS والتي لا يمكن منعها بواسطة NIDS هي: نص تسجيل الدخول إلى حصان طروادة ، والانتقال إلى هجوم لوحة المفاتيح غير المراقب ، وحركة المرور المشفرة ،

• They can monitor all users' activities which is not possible in a network-based system.

• They can identify attacks that originate from inside the host.

• A host-based system can analyze the decrypted traffic to find attack signature-thus giving them the ability to monitor encrypted traffic.

• They do not require any extra hardware since they can be installed in the existing host servers.

• They are cost effective for a small-scale network having a few hosts.

• Some examples of attacks that are prevented by HIDS and cannot be prevented by NIDS are: Trojan login script, walk up to unattended keyboard attack, encrypted traffic, …

11.Response Options for IDSs

Active Responses

1. Collect additional information
2. Change the Environment: It is very difficult to block a determined and knowledgeable attacker, but IDSs can often deter expert attackers or stop novice attackers by taking the following actions:

• Injecting TCP reset packets into the attacker's connection to the victim system, thereby terminating the connection.

• Reconfiguring routers and firewalls to block packets from the attacker's apparent location (IP address or site).

• Reconfiguring routers and firewalls to block the network ports, protocols, or services being used by an attacker.

3. Act against the intruder

Passive Responses

Alarms and Notifications: This is displayed on the IDS console or on other systems as specified by the user during the configuration of the IDS. Some products also offer email as another notification channel.

١١. خيارات الاستجابة لنظام كشف التسلل

الردود النشطة

١. جمع معلومات إضافية

٢. تغيير البيئة: من الصعب للغاية منع مهاجم حازم وواسع المعرفة ، لكن أنظمة كشف التسلل يمكن غالبًا ردع المهاجمين الخبراء أو إيقاف المهاجمين المبتدئين من خلال اتخاذ الإجراءات التالية:

• إدخال حزم إعادة تعيين TCP في اتصال المهاجم بالنظام الضحية ، وبالتالي إنهاء الاتصال.

• إعادة تكوين أجهزة التوجيه والجدران النارية لحظر الحزم من الموقع الظاهر للمهاجم (عنوان IP أو الموقع).

• إعادة تكوين أجهزة التوجيه والجدران النارية لحظر منافذ الشبكة أو البروتوكولات أو الخدمات التي يستخدمها المهاجم.

٣. التصرف ضد الدخيل

الردود السلبية

التنبيهات والإخطارات: يتم عرض هذا على وحدة تحكم IDS أو على أنظمة أخرى كما هو محدد من قبل المستخدم أثناء تكوين IDS. تقدم بعض المنتجات أيضًا البريد الإلكتروني كقناة إعلام أخرى

ChΣ Symmetric Cryptography

1.Introduction

Cryptography is the study of methods of sending messages in disguised form so that only the intended recipients can remove the disguise and read the message. The message to be sent is called *plaintext*. The disguised message is called the *ciphertext*.

Cryptographic techniques are divided into 3 types:

1. Symmetric-key Cryptography
2. Public-key Cryptography
3. Keyless Cryptography (also called hash functions or message digest functions).

١ المقدمة
التشفير هو دراسة طرق إرسال الرسائل في شكل مقنع بحيث يمكن للمستلمين المقصودين فقط إزالة التمويه وقراءة الرسالة.
تسمى الرسالة المراد إرسالها نص عادي. الرسالة المقنعة تسمى النص المشفر.
تنقسم تقنيات التشفير إلى ٣ أنواع:
١. تشفير المفتاح المتماثل
٢. تشفير المفتاح العام
٣. التشفير بدون مفتاح (ويسمى أيضًا وظائف التجزئة أو وظائف ملخص الرسائل).

Figure(4.1): Symmetric Encryption

2.Symmetric Encryption

There are two requirements for secure use of symmetric encryption:

1. We need a strong encryption algorithm.
2. Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure.

There are two general approaches to attacking a conventional encryption scheme:

- Cryptanalysis
- Brute-force attack

Therefore, all that the users of an encryption algorithm can strive for is an algorithm that meets one or both of the **following criteria:**

1– The cost of breaking the cipher exceeds the value of the encrypted information.

2– The time required to break the cipher exceeds the useful lifetime of the information.

Symmetric-key algorithms can be divided into:

3– Stream ciphers encrypt the bits of the message one at a time

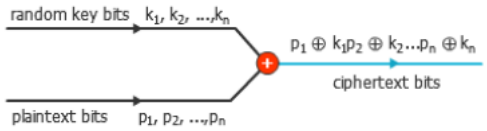
4– Block ciphers take several bits and encrypt them as a single unit

٢. التشفير المتماثل
هناك نوعان من المتطلبات للاستخدام الآمن للتشفير المتماثل:
١. نحن بحاجة إلى خوارزمية تشفير قوية.
٢. يجب أن يكون المرسل والمتلقي قد حصلوا على نسخ من المفتاح السري بطريقة آمنة ويجب أن يحافظوا على تأمين المفتاح.
هناك طريقتان عامتان لمهاجمة نظام التشفير التقليدي:
- تحليل الشفرات
- هجوم القوة الغاشمة

لذلك ، كل ما يمكن أن يسعى إليه مستخدمو خوارزمية التشفير هو خوارزمية تلبي أحد **المعايير** التالية أو كليهما:
١- تكلفة كسر التشفير تتجاوز قيمة المعلومات المشفرة.
٢- الوقت المطلوب لكسر التشفير يتجاوز العمر المفيد للمعلومات.
يمكن تقسيم خوارزميات المفتاح المتماثل إلى:
٣- دفق الأصفار تشفير بتات الرسالة واحدة تلو الأخرى
٤- تأخذ الشفرات المحظورة عدة بتات وتقوم بتشفيرها كوحدة واحدة

3.Stream Cipher

If the key string is randomly chosen and if the message and never used again, then Vernam cipher is called a one-time pad, Perfect cryptosystem. It produces random output that bears no statistical relationship to the plaintext. Because the ciphertext contains no information whatsoever about the plaintext, there is simply no way to break the code.



Figure(4.2): One Time Pad

٣. دفق التشفير
إذا تم اختيار سلسلة المفاتيح بشكل عشوائي وإذا لم يتم استخدام الرسالة مرة أخرى ، فإن تشفير Vernam يسمى لوحة لمرة واحدة ، نظام تشفير مثالي. ينتج مخرجات عشوائية لا تحمل أي علاقة إحصائية بالنص العادي. نظرًا لأن النص المشفر لا يحتوي على أي معلومات من أي نوع حول النص العادي ، فلا توجد طريقة لكسر الشفرة.

The one-time pad offers complete security but, in practice, has two fundamental difficulties:

1. There is the practical problem of making large quantities of random keys.
2. Even more daunting is the problem of key distribution and protection.

توفر لوحة المرة الواحدة أمانًا كاملاً ، ولكن في الممارسة العملية ، تواجه صعوبتين أساسيتين:
١. هناك مشكلة عملية في عمل كميات كبيرة من المفاتيح العشوائية.
٢. الأمر الأكثر صعوبة هو مشكلة توزيع المفاتيح وحمايتها.

٣,٢ خصائص تيار الأصفار

• يمكن أن تكون الأصفار المتدفقة مفيدة في الحالات التي تتطلب سرعة نقل عالية جدًا مثل قنوات الاتصال المتعددة جيجابت.
• من المستحسن أيضًا استخدام الأصفار المتدفقة حيث يكون الانتشار الصفري أمرًا مطلوبًا مثل الاتصالات الراديوية.
• أصفار البث مرغوب فيها أيضًا حيث لا يمكن تحديد طول الرسالة مسبقًا ، ويكون تأخير الإدخال / الإخراج أقل مطلوبًا كما في حالة اتصال (GSM (RC4.

العيوب الرئيسية لتشفير الدفق هي:

يجب أن تتم مزامنة المرسل والمستقبل بشكل صحيح من أجل فك التشفير الصحيح.
حظر التشفير
تشفير الكتلة هو مخطط تشفير يقسم رسالة النص العادي إلى كتل ذات طول ثابت وينتج كتل نص مشفر بنفس الطول. يعتمد التحقيق الدقيق لتشفير الكتلة المتماثل على اختيار المعلمات وميزات التصميم التالية.
• حجم الكتلة: أحجام الكتل الأكبر تعني أمانًا أكبر ، ولكن سرعة تشفير / فك تشفير أقل. حجم الكتلة ١٢٨ بت هو مقايضة معقولة ويكاد يكون عالميًا بين تصميمات تشفير الكتلة الحديثة.
• حجم المفتاح: يعني الحجم الأكبر للمفتاح أمانًا أكبر ولكنه قد يقلل من سرعة التشفير / فك التشفير.
• عدد الجولات: يكمن جوهر التشفير الكتلي المتماثل في أن الجولة الواحدة توفر أمانًا غير كافٍ ولكن الجولات المتعددة توفر أمانًا متزايدًا.

3.2. Properties of Stream Ciphers

• Stream ciphers can be useful in cases where very high-speed throughput is required like multi gigabit communication channels.

• Stream ciphers are also desirable where zero error propagation is required like radio communication.

• Stream ciphers are also desirable where the length of the message cannot be predetermined, and smaller input/output delay is required as in the case of GSM communication (RC4).

The sender and receiver should be synchronized properly for correct decryption.

4.Block Cipher

A block cipher is an encryption scheme which breaks up the plaintext message into blocks of a fixed length and produces ciphertext blocks of the same length. The exact realization of a symmetric block cipher depends on the choice of the following parameters and design features.

• Block size: larger block sizes mean greater security, but reduced encryption/decryption speed. A block size of 128 bits is a reasonable trade-off and is nearly universal among recent block cipher designs.

• Key size: Larger key size means greater security but may decrease encryption/ decryption speed.

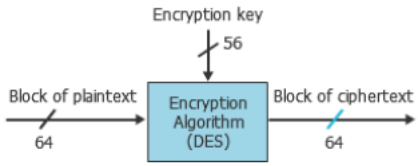
• Number of rounds: The essence of a symmetric block cipher is that a single round offers inadequate security but that multiple rounds offer increasing security.

4.1. Symmetric Block Encryption Algorithms خوارزميات تشفير الكتلة المتماثلة

Data Encryption Standard (DES)) معيار تشفير البيانات DES(

A serious concern is key length. With a key length of 56 bits, there are possible keys, which is approximately 56^2

مصدر قلق خطير هو طول المفتاح. مع طول مفتاح ٥٦ بت ، هناك مفاتيح ممكنة ، وهو ما يقرب من ٥٦٢

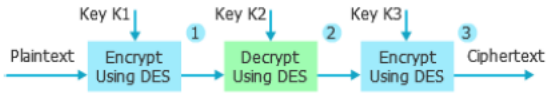


Figure(4.3): DES Algorithm

Triple DES (3DES)

With three distinct keys, 3DES has an effective key length of 168 bits. it is three time slower than DES. The main disadvantage of 3DES is it is three time slower than DES.

ثلاثية (3DES) DES مع ثلاثة مفاتيح متميزة، ٣ DESلديه طول مفتاح فعال يبلغ ١٦٨ بت. إنه أبطأ بثلاث مرات من DES. العيب الرئيسي ل ٣ DESهو أنه أبطأ بثلاث مرات من.DES



Figure(4.4): 3DES algorithm

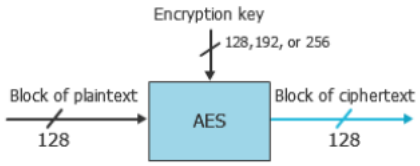
Advanced Encryption Standard (AES)

In November 2001 the USA NIST announced Rijndael algorithm as the AES to replace DES as a FIPS 197. AES uses a block size 128, rounds 10, 12, or 14 depending on the key size (128, 192, or 256). The main steps of AES encryption are:

1. A plaintext of 128−bit block is arranged as a 4 X 4 array of bytes called the “state,” which is modified in place in each round.

معيار التشفير المتقدم (AES)

في نوفمبر ٢٠٠١ ، أعلن NIST الأمريكي عن خوارزمية Rijndael باعتبارها AES لتحل محل DESك. FIPS 197 تستخدم AES حجم كتلة ١٢٨ أو تقريب ١٠ أو ١٢ أو ١٤ اعتمادا على حجم المفتاح (١٢٨ أو ١٩٢ أو ٢٥٦). الخطوات الرئيسية لتشفير AES هي: يتم ترتيب نص عادي من كتلة ١٢٨ بت كمصفوفة ٤ × ٤ بايت تسمى "الحالة" ، والتي يتم تعديلها في مكانها في كل جولة.



Figure(4.5): AES Algorithm

Exam Questions: What 3DES algorithm and what it’s type?

It’s Symmetric encryption algorithm, Block cipher type.

Exam Questions: What Vernam algorithm and what it’s type?

It’s Symmetric encryption algorithm, Stream cipher type.

Exam Questions: What RC4 algorithm and what it’s type?

It’s Symmetric encryption algorithm, Stream cipher type.

أسئلة الامتحان: ما هي خوارزمية DES٣ وما هو نوعها؟
إنها خوارزمية التشفير المتماثل ، نوع التشفير الكتلي.
أسئلة الاختبار: ما هي خوارزمية Vernam وما نوعها؟
إنها خوارزمية تشفير متماثل ، نوع دفق التشفير.
أسئلة الامتحان: ما هي خوارزمية RC4 وما نوعها؟
إنها خوارزمية تشفير متماثل ، نوع دفق التشفير.

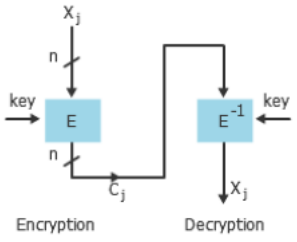
5.Mode of Operation

A mode of operation is a technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application, such as applying a block cipher to a sequence of data blocks or a data stream.

1. ECB −Electronic Code Book.
2. CBC −Cipher Block Chaining.
3. CFB −Cipher Feedback.
4. OFB −Output Feedback.
5. CTR – Counter.

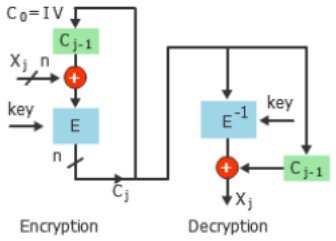
٥. طريقة العملية
أسلوب التشغيل هو تقنية لتحسين تأثير خوارزمية التشفير أو تكييف الخوارزمية لتطبيق ما ، مثل تطبيق تشفير الكتلة على سلسلة من كتل البيانات أو تدفق البيانات.
١. البنك المركزي الأوروبي - كتاب الشفرة الإلكترونية.
٢. CBC -Cipher Block Chaining.
٣. تعليقات شفرات CFB.
٤. OFB -Output Feedback.
٥. نسبة النقر إلى الظهور - العداد.

Electronic Code Book (ECB)



Figure(4.6): ECB Mode

i



Figure(4.7): CBC Mode

Exam Questions: Which mode operation input to the encryption algorithm is the XOR of the current plaintext block and what it's type?

Answer: Cipher Block Chaining (CBC)

Exam Questions: What is the technique for enhancing the effect of a cryptographic algorithm or adapting the algorithm for an application?

Answer: Mode of Operation.

5.2. Advantages & Disadvantages of Symmetric Encryption

The most significant advantage when it comes to the symmetric encryption method is its simplicity. It has an issue known as "key distribution"

أسئلة الاختبار: ما هو وضع إدخال عملية الإدخال إلى خوارزمية التشفير هو XOR الخاص بكتلة النص العادي الحالي وما هو نوعه؟
الإجابة: تسلسل كتل التشفير(CBC)
أسئلة الاختبار: ما هي تقنية تحسين تأثير خوارزمية التشفير أو تكييف الخوارزمية لتطبيق ما؟
الجواب: طريقة العملية.
5.2مزايا وعيوب التشفير المتماثل
الميزة الأكثر أهمية عندما يتعلق الأمر بطريقة التشفير المتماثل هي بساطتها. لديها مشكلة تعرف باسم "توزيع المفتاح"

CH5 Asymmetric Cryptography التشفير الغير متناظر

1.Introduction

The first problem is that of key distribution. For example, if a cryptosystem has n users, each user must have (n -1) keys, and the total number of keys is $\frac{n2 - n}{2}$

2.Public Key Cryptography

Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman. A public key known to everyone (widely distributed) A private or secret key known only to the recipient of the message.

Exam Questions: Bob and Alice are sending encrypted messages between them, and the message encryption is happened by Bob's private key, the decryption is happened by:

- Bob's private key
- Bob's public key
- Alice's private key
- Alice's public key

١ المقدمة
المشكلة الأولى هي مشكلة توزيع المفاتيح. على سبيل المثال ، إذا كان نظام التشفير يحتوي على عدد n مستخدمين ، فيجب أن يكون لدى كل مستخدم مفاتيح (n -1) ، ويكون العدد الإجمالي للمفاتيح (n2 - n) / 2
٢- تشفير المفتاح العام
تم اختراع تشفير المفتاح العام في عام ١٩٧٦ من قبل ويتفيلد ديفي ومارتن هيلمان. مفتاح عام معروف للجميع (يتم توزيعه على نطاق واسع) مفتاح خاص أو سري معروف فقط لمستلم الرسالة.
أسئلة الاختبار: يرسل بوب وأليس رسائل مشفرة بينهما ، ويتم تشفير الرسالة من خلال مفتاح بوب الخاص ، ويتم فك التشفير عن طريق:
المفتاح الخاص لبوب
مفتاح بوب العمومي
مفتاح أليس الخاص
مفتاح أليس العام

3.Hybrid Encryption

Public key encryption and decryption algorithms tend to be incredibly slow relative to symmetric key algorithms. Public key algorithms tend to be about 1000 times slower than AES. In general, Hybrid encryption (or digital envelop), a mash up of symmetric and asymmetric encryption, provides an elegant solution that preserves the speed of symmetric encryption, while maintaining the security and exchange flexibility of Asymmetric encryption.

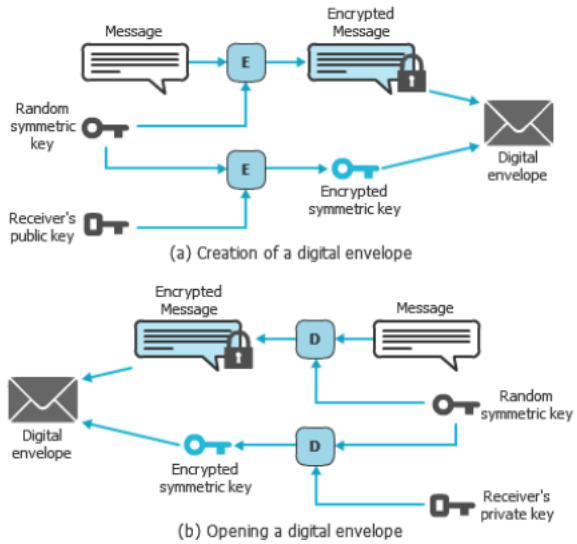
Hybrid encryption is used in all forms of internet communication between client and server these days. SSL/TLS, IPsec and SSH are good examples of Hybrid encryption.

٣. التشفير الهجين

تميل خوارزميات تشفير المفتاح العام وفك التشفير إلى أن تكون بطيئة بشكل لا يصدق بالنسبة لخوارزميات المفاتيح المتماثلة. تميل خوارزميات المفاتيح العامة إلى أن تكون أبطأ بنحو ١٠٠٠ مرة من AES. بشكل عام ، يوفر التشفير الهجين (أو الغلاف الرقمي) ، وهو مزيج من التشفير المتماثل وغير المتماثل ، حلاً أنيقًا يحافظ على سرعة التشفير المتماثل ، مع الحفاظ على الأمان ومرونة التبادل للتشفير غير المتماثل.

يستخدم التشفير الهجين في جميع أشكال اتصال الإنترنت بين العميل والخادم هذه الأيام. تعد SSL / TLS و IPsec و SSH أمثلة جيدة على التشفير الهجين.

.



Figure(5.2): Hybrid Encryption

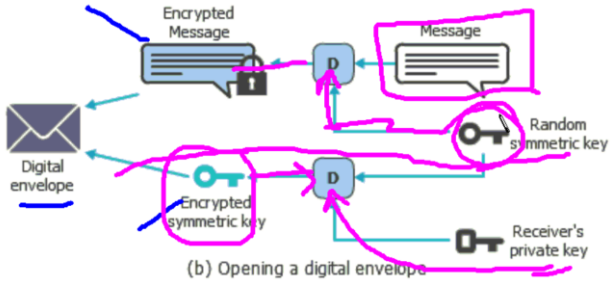
Rule: Data block has been encrypted by Symmetric encryption, but the keys encrypted by Asymmetric encryption.

القاعدة: تم تشفير كتلة البيانات بواسطة التشفير المتماثل ، ولكن المفاتيح المشفرة بواسطة التشفير غير المتماثل .

Exam Questions: What the digital envelope contents?

Encrypted message by Symmetric encryption + Encrypted key by Asymmetric encryption.

أسئلة الامتحان: ما محتويات المغلف الرقمي؟ رسالة مشفرة عن طريق التشفير المتماثل + مفتاح مشفر عن طريق التشفير غير المتماثل.



Figure(5.2): Hybrid Encryption

4.Cryptography Hash Function

A hash function H is a transformation that takes an input m and returns a fixed size string.

When employing in cryptography, the function H must have the following properties:

1. The input m can be of any length.
2. The output has a fixed length.

٤. وظيفة تجزئة التشفير

دالة التجزئة H هي تحويل يأخذ إدخال m ويعيد سلسلة ذات حجم ثابت.

عند الاستخدام في التشفير ، يجب أن يكون للوظيفة H الخصائص التالية:

١. يمكن أن يكون الإدخال م بأي طول.

٢. الإخراج بطول ثابت.

وظائف التجزئة الأكثر استخدامًا اليوم هي خوارزمية التجزئة الآمنة (SHA) بإصدارات مختلفة (SHA-1 و SHA-2 و SHA-3) بإخراج مختلف (١٦٠ ، ٢٢٤ ، ٢٥٦ ، ٣٨٤ ، و ٥١٢) بت.

The most used hash functions today are the secure hash algorithm (SHA) with different versions (SHA-1, SHA-2, and SHA-3) with different output (160, 224, 256, 384, and 512) bits long.

Exam Questions: True or False

Is Hash function achieving data confidentiality?

- True
- False It's achieved data integrity only

Exam Questions: True or False

Is Hash function achieving integrity?

- True
- False

أسئلة الاختبار: صح أم خطأ

هل تحقق وظيفة التجزئة سرية البيانات؟

- حقيقي
- خطأ لقد تحقق تكامل البيانات فقط

أسئلة الاختبار: صح أم خطأ

هل دالة Hash تحقق النزاهة؟

- حقيقي

خطأ شنيع

٥. تطبيقات لأنظمة تشفير المفتاح العام

القاعدة: للتشفير المتماثل وظيفة واحدة وتشفير بياناته ، لكن التشفير غير المتماثل له ثلاث وظائف على النحو التالي:

١- تشفير البيانات وفك تشفيرها

٢- التوقيع الرقمي

٣- اتفاقية مفتاح

القاعدة: التوقيع الرقمي لا يساوي الشهادات الرقمية

القاعدة: التوقيع الرقمي **لا يوفر السرية** ، ولكنه يوفر ما يلي:

١- الأصالة.

٢- عدم الطلاق

٣- النزاهة عن طريق دوال التجزئة

5.Applications for Public-Key Cryptosystems

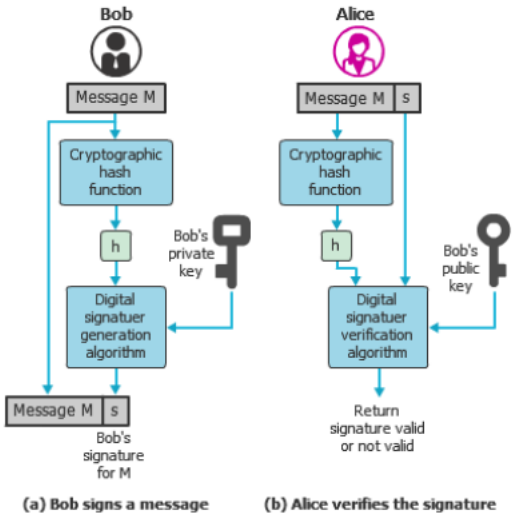
Rule: Symmetric encryption has one function and its data encryption, but Asymmetric encryption has three functions as follow:

1- Data encryption and decryption
2- Digital signature
3- Key Agreement

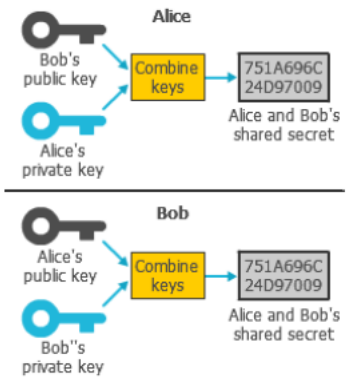
Rule: Digital signature not equal Digital certificates

Rule: Digital signature **does not provide confidentiality**, but providing the follow:

1- authenticity.
2- Non-repudiation
3- Integrity by hash functions



Figure(5.4): Public Key (Digital Signature)



Figure(5.5): Public Key (Key Agreement)

6.A Trapdoor One Way Function

Factorization of Big Integer

The Discrete Logarithm Problem: However, given a, b, and a^bmod n (when n is a large prime), calculating b is regarded by mathematicians as a hard problem

7.Diffie-Hellman Algorithm

The Diffie–Hellman (DH) key exchange technique was first defined in their seminal paper in 1976.

Exam Questions: True or False

We use Diffie-Hellman for encrypt and decrypt data?

- True
- False It's **only Key Exchange**.

طريقة واحدة وظيفة 6.A Trapdoor

عامل عدد صحيح كبير

و b و a مشكلة اللوغاريتم المنفصل: ومع ذلك ، بالنظر إلى

يعتبره b عددًا أوليًا كبيرًا) ، فإن حساب n عندما يكون) abmod n

علماء الرياضيات مشكلة صعبة

خوارزمية ديفي هيلمان -7

لأول مرة في Diffie-Hellman (DH) تم تحديد تقنية تبادل المفاتيح

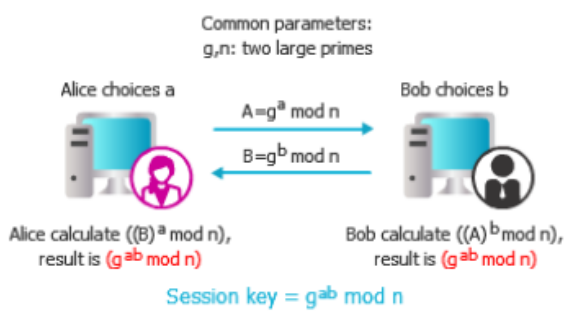
ورقتهم الأساسية في عام ١٩٧٦.

أسئلة الاختبار: صح أم خطأ

لتشفير البيانات وفك تشفيرها؟ Diffie-Hellman نستخدم

حقيقي -

خطأ ، إنه تبادل المفاتيح فقط -.



Figure(5.6): Diffie–Hellman Key Exchange

```
n, g    >> public
Alice a >> private .... A= g^a mod n >> public
Bob   b >> private .... B= g^b mod n >> public

Alice Ka = B^a mod n >> Ka =(g^b)^a mod n>> =g^b*a mod n
Bob   Kb = A^b mod n >> Kb =(g^a)^b mod n>> =g^a*b mod n
```

Shared key is very important in Exam

DH key exchange

8.The RSA Algorithm

It is named after the three researchers Ron Rivest, Adi Shamir and Len Adleman who first published it.

8.خوارزمية RSA سميت على اسم الباحثين الثلاثة رون ريفيست وعدي شامير ولين أدلمان الذين نشروها لأول مرة.

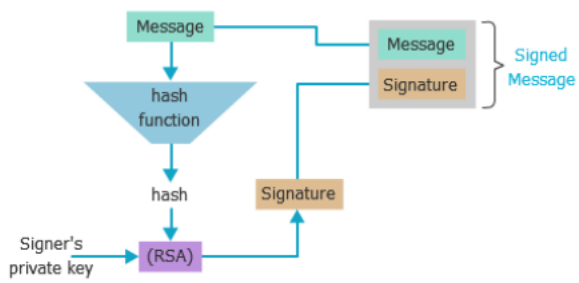
```
RSA
1-      q, p >>> 2 large prime ....secret
2-      n=p*q    .... public
3-      fi(n)= (p-1)*(q-1)
4-      e >> public
5-      e.d= 1 mod fi(n) >> d private
        e.d mod fi(n) = 1


C= M^e mod n
M= C^d mod n
حيث
C= النص المشفر
M= النص قبل التشفير
```

Exam Questions: The rule of RSA Encryption.

Answer: $C = M^e \bmod n$

$M = C^d \bmod n$

RSA Signature:



Figure(5.7): RSA signature

8.2. Security of RSA

1− $C = M^e \bmod n$

2− must factor n (problem of prime factorization), hard mathematical problem or Big Integer Factorization.

8.2 أمن RSA

1- C = Me mod n

مشكلة التحليل الأولي) ،) n يجب أن يكون العامل ??? مشكلة رياضية صعبة أو عامل صحيح كبير.

شهادة المفتاح العام ??

في جوهرها، تتكون الشهادة من مفتاح عام بالإضافة إلى معرف مستخدم لمالك المفتاح ، مع توقيع الكتلة بالكامل بواسطة طرف ثالث موثوق به. تتضمن الشهادة أيضًا بعض المعلومات حول الطرف الثالث بالإضافة إلى إشارة إلى فترة صلاحية الشهادة. عادةً ما يكون الطرف الثالث هو المرجع المصدق (CA) ، الذي يثق به مجتمع المستخدمين

9.Public Key Certificate

In essence, a certificate consists of a public key plus a user ID of the key owner, with the whole block signed by a trusted third party. The certificate also includes some information about the third party plus an indication of the period of validity of the certificate. Typically, the third party is a certificate authority (CA) that is trusted by the user community,

$$C_A = \left\{ Alice, K_{u_a}, DS_{kv}\left(K_{u_a} \| Alice \| T\right) \right\}$$

Where:

K_{u_a} is Alice public key

Key certificate fields in X.509v3 (RFC 5280):

- Version
- Serial number (unique)
- Signature algorithm identifier: hash algorithm
- Issuer's name, uniquely identifies issuer
- Interval of validity
- Subject's name, uniquely identifies subject
- Subject's public key
- Signature

حقول الشهادة الرئيسية في:X.509v3 (RFC 5280)

- الإصدار
- الرقم التسلسلي (فريد)
- معرف خوارزمية التوقيع: خوارزمية التجزئة
- اسم المُصدر يحدد المصدر بشكل فريد
- فترة الصلاحية
- اسم الموضوع ، يحدد الموضوع بشكل فريد
- المفتاح العام للموضوع
- التوقيع

10.Public Key Infrastructure (PKI)

A Public Key Infrastructure (PKI) is a set of services and policies that lays the framework for binding a public key to an identity and distributing that binding.

A PKI has three basic processes which are:

1. Certification
2. Validation
3. Certificate Revocation

البنية التحتية للمفتاح العام (PKI)

البنية التحتية للمفتاح العام (PKI) هي مجموعة من الخدمات والسياسات التي تضع إطار العمل لربط مفتاح عام بهوية وتوزيع هذا الارتباط.

تشتمل البنية التحتية للمفاتيح العمومية (PKI) على ثلاث عمليات أساسية هي:

١. شهادة
٢. التحقق من الصحة
٣. إبطال الشهادة

CH6 Security Protocols

1.Introduction

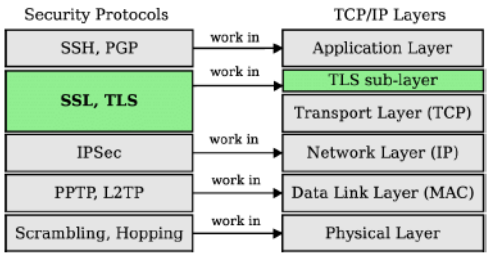


Figure (6.1): Relative Location of Security Protocols in TCP/IP Stack

2.IP Security (IPsec)

IPsec is not a single protocol, but rather a set of services and protocols that provide a complete security solution for an IP network.

2.1.IPsec Components

Authentication Header (AH)

Encapsulation Security Payload (ESP): These are confidentiality, integrity, origin authentication, and anti-replay protection. Confidentiality ensures data is encrypted. Integrity ensures data in transit has not been tampered with. Origin authentication ensures the remote peers are who they claim to be, and anti-replay protection will ensure duplicated traffic is not accepted which would prevent DOS attacks, as well as spoofed traffic.

٢- أمان IP (IPsec)

IPsec ليس بروتوكولًا منفردًا ، ولكنه مجموعة من الخدمات والبروتوكولات التي توفر حلاً أمانًا كاملاً لشبكة IP.

٢,١. مكونات IPsec

رأس المصادقة

حمولة أمان التغليف (ESP): هذه هي السرية والنزاهة والمصادقة الأصلية والحماية من إعادة التشغيل. السرية تضمن تشفير البيانات. تضمن النزاهة عدم العبث بالبيانات أثناء النقل. تضمن مصادقة المنشأ أن الأقران البعيدين هم من يدّعون أنهم كذلك، وستضمن الحماية ضد إعادة التشغيل عدم قبول حركة المرور المكررة والتي من شأنها منع هجمات DOS، بالإضافة إلى حركة المرور المخادعة.

بروتوكول تبادل مفتاح الإنترنت (IKE)

٢,٢. تطبيقات IPsec

- اتصال مكتب فرعي آمن عبر الإنترنت: VPN

٢,٣ فوائد IPsec

- IPsec يقع أسفل طبقة النقل (TCP، UDP) وبالتالي فهو شفاف للتطبيقات.
- يمكن أن تكون IPsec شفافة للمستخدمين النهائيين.

٢,٤ أوضاع IPsec

أسئلة الاختبار: أي وضع IPsec سيكون الرأس هو نفسه بدون أي تغييرات أثناء إرسال الحزم؟

الإجابة: وضع النقل IPsec

أسئلة الاختبار: أي وضع IPsec سيتم تشفير الرأس بحمولة البيانات وإضافة رأس جديد؟

الإجابة: وضع نفق IPsec

Internet Key Exchange (IKE) Protocol

2.2. Applications of IPsec

- Secure branch office connectivity over the Internet: VPN

2.3. Benefits of IPsec

- IPsec is below the transport layer (TCP, UDP) and so is transparent to applications.
- IPsec can be transparent to end users.

2.4. IPsec Modes

Exam Questions: Which IPsec mode the header will be same without any changes during the sending the packets?

Answer: IPsec Transport mode

Exam Questions: Which IPsec mode the header will be encrypted with the data payload and adding a new header?

Answer: IPsec Tunnel mode

3.Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

One of the most widely used security services is the Secure Sockets Layer (SSL) and the follow-on Internet standard, the Transport Layer Security (TLS) Protocol (RFC 4346). TLS is a general-purpose service implemented as a set of protocols that rely on TCP. Most browsers come equipped with TLS, and most Web servers have implemented the protocol. HTTP, which provides the transfer service for Web client/server interaction, can operate on top of TLS.

3.1.TLS Protocols

1Record Protocol**:

The TLS Record Protocol provides two services for TLS connections:

- **Confidentiality**: The Handshake Protocol defines a shared secret key that is used for symmetric encryption of TLS payloads.
- **Message integrity**: The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).

2The Handshake Protocol**:

The security goals of the handshake protocol are:

- Entity authentication of participating parties:

  Participants are called ‘client’ and ‘server’.
- Establishment of a fresh, shared secret
- Secure ciphersuite negotiation

Exam Questions: True or False

The security goals of the handshake protocol are: Entity authentication of participating parties, Establishment of a fresh, shared secret and Secure cipher suite negotiation?

- True

  False

3.Secure Sockets Layer (SSL) and Transport Layer Security (TLS

واحدة من أكثر خدمات الأمان استخدامًا هي طبقة مآخذ التوصيل الآمنة (SSL) ومعيار الإنترنت التالي ، بروتوكول أمان طبقة النقل TLS. (RFC 4346) (TLS) هي خدمة للأغراض العامة يتم تنفيذها كمجموعة من البروتوكولات التي تعتمد على TCP. تأتي معظم المتصفحات مجهزة بـ TLS ، وقد طبقت معظم خوادم الويب البروتوكول. يمكن أن يعمل HTTP ، الذي يوفر خدمة النقل لتفاعل عميل / خادم الويب ، فوق TLS.

3.1.TLSبروتوكولات

بروتوكول السجل –

يوفر بروتوكول سجل TLS خدمتين لاتصالات:TLS

•**السرية**: يحدد بروتوكول المصافحة مفتاحًا سريًا مشتركًا يُستخدم للتشفير المتماثل لحمولات.TLS

•**سلامة الرسالة**: يعرّف بروتوكول المصافحة أيضًا مفتاحًا سريًا مشتركًا يُستخدم لتكوين رمز مصادقة رسالة.(MAC)

بروتوكول المصافحة:

الأهداف الأمنية لبروتوكول المصافحة هي:

•مصادقة الكيان للأطراف المشاركة: يُطلق على المشاركين اسم "العميل" و "الخادم."

•إنشاء سر مشترك جديد

Secure •التفاوضciphersuite

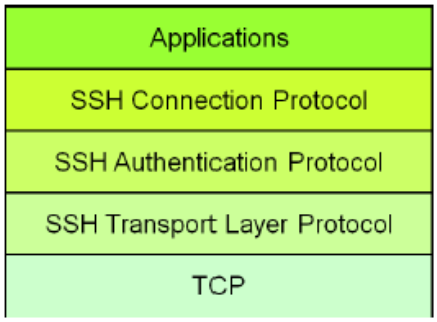
أسئلة الاختبار: صح أم خطأ

الأهداف الأمنية لبروتوكول المصافحة هي: مصادقة الكيان للأطراف المشاركة ، إنشاء مفاوضات مجموعة تشفير آمن وسري جديد ومشترك؟

- حقيقي

خطأ شنيع

4.The Secure Shell (SSH)



Figure(6.7): SSH Architecture

.5مقارنة IPsec و SSL / TLS وSSH

•يمكن استخدام الثلاثة لبناء شبكات.VPN

أسئلة الاختبار: صح أم خطأ

يمكن استخدام جميع بروتوكولات الأمان لبناء شبكات.VPN

- حقيقي

خطأ شنيع

5.Comparing IPsec, SSL/TLS, and SSH

• All three can be used to build VPNs.

Exam Questions: True or False

All security protocols can be used to build VPNs.

- True

False

Ch 7 :User Authentication

1. Introduction

Typically, user authentication is established at the start of a connection. User authentication process consists of two steps:

1. Identification step
2. Verification step

2.Entity Authentication Functions

1. Something that you have.
2. Something that you are.
3. Something that you know.

Multifactor authentication (MFA) uses any two or more authentication factors.

2.1. Something you have Authentication

1. Dumb tokens
2. Smart cards

2.2. Something you are Authentication

1. Morphological
2. Behavioral is related to the behavior of a person such as gait, signature, keystroke dynamics, etc.
3. Biological is related to the inner part of a living organism such as heartbeat, DNA, blood.

2.3. Something you Know Authentication

Something the individual knows: Examples include a password, a

.?مقدمة

عادةً ما يتم إنشاء مصادقة المستخدم في بداية الاتصال. تتكون عملية مصادقة المستخدم من خطوتين:

.1خطوة تحديد الهوية

.2خطوة التحقق

.2وظائف مصادقة الكيان

.1شيء لديك.

.2شيء ما أنت عليه.

.3شيء تعرفه.

تستخدم المصادقة متعددة العوامل (MFA) أي عاملين أو أكثر من عوامل المصادقة.

.2.1شيء لديك مصادقة

.1الرموز الغبية

.2البطاقات الذكية

.2.2شيء أنت المصادقة

.1الصرفي

.2يرتبط السلوك بسلوك الشخص مثل المشي والتوقيع وديناميات ضغط المفاتيح ، إلخ.

٣. يرتبط البيولوجي بالجزء الداخلي من الكائن الحي مثل نبضات القلب والحمض النووي والدم.

٢,٣ شيء تعرفه المصادقة

شيء يعرفه الفرد: تتضمن الأمثلة كلمة مرور أو رقم تعريف شخصي (PIN) أو عبارة مرور أو إجابات لمجموعة من الأسئلة التي تم ترتيبها مسبقًا.

هذه الطريقة بعيدة كل البعد عن طريقة المصادقة الأكثر استخدامًا.

personal identification number (PIN), passphrase, or answers to a prearranged set of questions.
This method is far from the most used authentication method.

Attack on Passwords

- Brute force attack

Selecting a Good Password

- Contain both upper– and lower–case characters (e.g., a–z, A–Z).
- Have digits and punctuation characters as well as letters e.g., 0–9, @#$%^&*()_+|~– =\`{}[]:",'<>?,./).
- Are at least 12 alphanumeric characters long and is a passphrase.
- Are not a word in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on–line.
- Try to create passwords that can be easily remembered

Cryptographic Challenge-response based Authentication

PAP (Password Authentication Protocol)

CHAP (Challenge Handshake Authentication Protocol) CHAP is a challenge–based authentication protocol, but the transmission of a hashed password is still a problem due to brute force and dictionary attacks.

الهجوم على كلمات المرور

- هجوم القوة الغاشمة

اختيار كلمة مرور جيدة

- تحتوي على كل من الأحرف الكبيرة والصغيرة (على سبيل المثال، a-z، A-Z).
- لديك أرقام وعلامات ترقيم بالإضافة إلى أحرف مثل ، ٠-٩ ، @ # $٪ ^ & * () _ + | ~ - = \ `{} []:"، '<>؟،. /).
- تتكون من ١٢ حرفًا أبجديًا رقميًا على الأقل وهي عبارة مرور.
- ليست كلمة في أي لغة ، عامية ، لهجة ، المصطلحات ، إلخ.
- لا تستند إلى معلومات شخصية أو أسماء العائلة وما إلى ذلك.
- لا ينبغي أبدًا تدوين كلمات المرور أو تخزينها عبر الإنترنت.
- حاول إنشاء كلمات مرور يسهل تذكرها

مصادقة مشفرة قائمة على الاستجابة للتحدي

بروتوكول مصادقة كلمة المرور (PAP)

CHAP (بروتوكول مصادقة مصافحة التحدي)

CHAP هو بروتوكول مصادقة قائم على التحدي ، لكن إرسال كلمة مرور مجزأة لا يزال يمثل مشكلة بسبب القوة الغاشمة وهجمات القاموس.

CH8 Wireless Security

1.Introduction

A wireless local area network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air.

2.WLAN Architecture

IEEE 802.11 is a family of standards for wireless LANs, the most used home standards are:

- 802.11b: 5.5 Mbps and 11 Mbps.
- 802.11g: Supports up to 54Mbps. Average throughput of ~20 Mbps, range of 30–40m (indoor).
- 802.11n (WI–FI 4): Typical 75Mbps and maximum of 300Mbps.Range of 70m (indoor).
- 802.11ac (Wi–Fi 5): Typical speeds ranging from 433 Mbps all the way up to several Gigabits per second, range of 30–40m (indoor).
- 802.11ax (Wi–Fi 6): Offers higher data rates and capacity, up to 9.6 Gbps, range of 30m (indoor).

2.1. WLAN Components

Access Points

Stations

2.2.WLAN Architecture Model

Infrastructure WLAN (basic service set (BSS)): BSS WLAN consists of wireless stations and access points (AP).
if one station in the BSS wants to communicate with another station in the same BSS, the frame is first sent from the originating station to the AP and then from the AP to the destination station.

Independent WLAN (ad hoc LAN): The simplest WLAN configuration is an independent (or peer-to-peer) WLAN. In other word, in this mode no infrastructure is required, and the stations are self-organized.

١ المقدمة

شبكة المنطقة المحلية اللاسلكية (WLAN) هي نظام اتصالات بيانات مرن يمكنه استخدام تكنولوجيا الأشعة تحت الحمراء أو تردد الراديو لنقل المعلومات واستقبالها عبر الهواء.

٢.WLAN العمارة

IEEE 802.11 هي مجموعة معايير للشبكات المحلية اللاسلكية ، ومعايير المنزل الأكثر استخدامًا هي:

- ٨٠٢,١١ b: 5.5 ميجابت في الثانية و ١١ ميجابت في الثانية.
- ٨٠٢,١١ g: يدعم حتى ٥٤ ميجابت في الثانية. متوسط الإنتاجية حوالي ٢٠ ميجابت في الثانية ، المدى من ٣٠-٤٠ م (داخلي).
- 802.11n (WI-FI 4): نموذجي ٧٥ ميجابت في الثانية والحد الأقصى ٣٠٠ ميجابت في الثانية. نطاق ٧٠ م (داخلي).
- 802.11ac (Wi-Fi 5): سرعات نموذجية تتراوح من ٤٣٣ ميجابت في الثانية وصولاً إلى عدة جيجابت في الثانية ، نطاق ٣٠-٤٠ م (داخلي).
- ٨٠٢,١١ ax (Wi-Fi 6): يوفر معدلات وسعة بيانات أعلى ، تصل إلى ٩,٦ جيجابت في الثانية ، ونطاق يصل إلى ٣٠ مترًا (داخلي).

٢,١. مكونات WLAN

نقطة وصول

المحطات

٢,٢ نموذج معماري لشبكة WLAN

البنية التحتية WLAN (مجموعة الخدمات الأساسية (BSS)): تتكون BSS WLAN من محطات لاسلكية ونقاط وصول (AP).

إذا أرادت إحدى محطات الخدمة BSS الاتصال بمحطة أخرى في نفس الخدمة BSS ، يتم إرسال الإطار أولاً من المحطة الأصلية إلى نقطة الوصول ثم من نقطة الوصول إلى المحطة الوجهة.

شبكة WLAN المستقلة (شبكة محلية مخصصة): أبسط تكوين لشبكة WLAN هو شبكة WLAN مستقلة (أو نظير إلى نظير). بمعنى آخر ، في هذا الوضع لا توجد بنية تحتية مطلوبة ، والمحطات منظمة ذاتيًا.

Microcell and Roaming (مجموعة الخدمة الممتدة (ESS)):

Microcells and Roaming (extended service set (ESS)):

3.Security Threats for WLAN

- Channel Jamming
- Unauthorized Access
- Traffic Analysis

The second category includes attacks against the communication between the station and the AP.

- Eavesdropping
- Message Forgery: When the wireless link is not protected for message integrity, the attacker can inject forged messages into both directions of the communication.
- Message Replay
- Man-in-the-middle Attack
- Session Hijacking

4.Securing Wireless Transmissions

4.1. Wired Equivalent Privacy (WEP)

- Encryption: WEP encrypts data using an RC4-based stream cipher to achieve data confidentiality.
- Integrity checksum: WEP uses cyclic redundancy check (CRC) to compute integrity checksums for the messages.
- Authentication

Insecurity of WEP

- Keystream reuse
- Linear checksum
- Weak RC4 keys: Real implementations show that it requires only 20000 packets to recover the key, which takes less than 1 min in a loaded AP.

4.2.Wi-Fi Protected Access (WPA)

WPA is still based on the RC4 stream cipher to reuse the specialized hardware that off-load the computation-intensive RC4 functions from the CPU.

The IEEE 802.11 Task Group proposed RSN (or 802.11i), a new security standard for WLANs. 802.11i was adopted as the next-generation WPA, or so-called WPA2. The new cryptosystem used in 802.11i is the Advanced Encryption Standard (AES).

4.3.Robust Security Network (RSN) WPA2 Program

٣. التهديدات الأمنية لشبكة WLAN

- قناة التشويش
- الوصول غير المصرح به
- "تحليل حركة المرور"

الفئة الثانية تشمل الهجمات على الاتصال بين المحطة ووكالة الأسوشييتد برس.

- التنصت
- تزوير الرسائل: عندما لا يكون الارتباط اللاسلكي محميًا لسلامة الرسالة ، يمكن للمهاجم إدخال رسائل مزورة في كلا الاتجاهين للاتصال.
- إعادة عرض الرسالة
- هجوم رجل في الوسط
- جلسة الاختطاف

٤- تأمين الإرسال اللاسلكي

٤,١ الخصوصية المكافئة للشبكات السلكية (WEP)

- التشفير: يقوم WEP بتشفير البيانات باستخدام تشفير دفق قائم على RC4 لتحقيق سرية البيانات
- المجموع الاختباري للنزاهة: يستخدم WEP فحص التكرار الدوري (CRC) لحساب المجاميع الاختبارية للتكامل للرسائل.
- المصادقة

عدم أمان WEP

- Keystream إعادة استخدام
- المجموع الاختباري الخطي
- مفاتيح RC4 ضعيفة: تظهر عمليات التنفيذ الحقيقية أنها تتطلب ٢٠٠٠٠ حزمة فقط لاستعادة المفتاح ، وهو ما يستغرق أقل من دقيقة واحدة في نقطة وصول محملة.

٤,٢ الوصول المحمي بشبكة WPA (Wi-Fi)

لا يزال WPA يعتمد على تشفير دفق RC4 لإعادة استخدام الأجهزة المتخصصة التي تعمل على تفريغ وظائف RC4 كثيفة العمليات الحسابية من وحدة المعالجة المركزية.

اقترحت مجموعة مهام IEEE 802.11 RSN (أو i٨٠٢,١١) ، وهو معيار أمان جديد لشبكات WLAN. تم اعتماد i٨٠٢,١١ باعتباره الجيل التالي من WPA ، أو ما يسمى WPA2. نظام التشفير الجديد المستخدم في i٨٠٢,١١ هو معيار التشفير المتقدم (AES).

٣,٤برنامج WPA2 لشبكة الأمان القوية (RSN)

٥. تأمين الشبكات المحلية اللاسلكية

تعيين وفرض سياسات WLAN

تكوين نقاط الوصول اللاسلكية بشكل صحيح:

الخطوة ١: بيانات تسجيل الدخول هذه ليست فريدة من نوعها ، حيث إنها هي نفسها لجميع الأجهزة من الطراز المعني ، كما أنه من السهل جدًا تذكرها ، مثل "admin" (كلمة المرور واسم المستخدم) أو "١٢٣٤".

الخطوة ٢: حدد WPA2 كطريقة تشفير.

الخطوة ٣: قم بإنشاء كلمة مرور آمنة لشبكة WLAN.

الخطوة ٤: حدد اسم شبكة غير معروف.

الخطوة ٥: قم بتشغيل تحديثات البرامج الثابتة التلقائية.

5.Securing Wireless LANs

Set and Enforce WLAN Policies

Configuring the Wireless Access Points Correctly:

Step 1: This log-in data is not unique, since it is the same for all devices of the respective model and is also very easy to remember, such as 'admin' (password and username) or '1234'.

Step 2: Select WPA2 as the encryption method.

Step 3: Create a secure WLAN password.

Step 4: Specify an unidentifiable network name.

Step 5: Turn on automatic firmware updates.

٥. تأمين الشبكات المحلية اللاسلكية

تعيين وفرض سياسات WLAN

تكوين نقاط الوصول اللاسلكية بشكل صحيح:

الخطوة ١: بيانات تسجيل الدخول هذه ليست فريدة من نوعها ، حيث إنها هي نفسها لجميع الأجهزة من الطراز المعني ، كما أنه من السهل جدًا تذكرها ، مثل "admin" (كلمة المرور واسم المستخدم) أو "١٢٣٤".

الخطوة ٢: حدد WPA2 كطريقة تشفير.

الخطوة ٣: قم بإنشاء كلمة مرور آمنة لشبكة WLAN.

الخطوة ٤: حدد اسم شبكة غير معروف.

الخطوة ٥: قم بتشغيل تحديثات البرامج الثابتة التلقائية.

CH9 Vulnerability Assessment and Mitigating Attacks

تقييم نقاط الضعف والتخفيف من الهجمات CH9

1.Introduction

The tasks of vulnerability assessment are the following:

- Identification, quantification and ranking of vulnerabilities found in network infrastructure, software and hardware systems, and applications.
- Explaining the consequences of a hypothetical scenario of the discovered security ‘holes.
- Developing a strategy to tackle the discovered threats.
- Providing recommendations to improve a company’s security posture and help eliminate security risks.

2.Vulnerability Assessments and Penetration Testing

Vulnerability assessment and penetration testing (or pen test) are complementary techniques.

3.Ways to Reveal Network Vulnerabilities

Black Box Method
White Box Method
Gray Box Method

4.A Scenario of Network Vulnerability Assessment

Step 1. Planning and Defining the Scope
Step 2. Gathering Information on the Network Infrastructure
Step 3. Scanning, Detection and Assessment of Network Vulnerabilities
Step 4. Reporting the Final Results and Identifying Countermeasures

5.Understanding the Security Testing Methodology

1. Reconnaissance
2. Network and Port Scanning
3. Policy Scanning
4. Vulnerability Probes and Fingerprinting
5. Penetration
6. Enumeration and Cracking
7. Escalation: The tester obtains administrative privileges on systems.
8. Backdoors
9. Exfiltration

The Open Web Application Security Project (OWASP) created a free, well-crafted method for web vulnerability assessment, which can be found at https://www.owasp.org.

١ المقدمة

مهام تقييم الضعف هي كما يلي:

- تحديد وتقدير وتصنيف الثغرات الموجودة في البنية التحتية للشبكة والبرمجيات وأنظمة الأجهزة والتطبيقات.
- شرح نتائج السيناريو الافتراضي للثغرات الأمنية المكتشفة.
- تطوير استراتيجية لمواجهة التهديدات المكتشفة.
- تقديم توصيات لتحسين الوضع الأمني للشركة والمساعدة في القضاء على المخاطر الأمنية.

٢. تقييمات الضعف واختبار الاختراق

يعتبر تقييم الضعف واختبار الاختراق (أو اختبار القلم) من الأساليب التكميلية.

٣. طرق الكشف عن نقاط ضعف الشبكة

طريقة الصندوق الأسود
طريقة الصندوق الأبيض
طريقة الصندوق الرمادي

٤-سيناريو تقييم ضعف الشبكة

الخطوة ١. تخطيط وتحديد النطاق
الخطوة ٢. جمع المعلومات حول البنية التحتية للشبكة
الخطوة ٣. مسح واكتشاف وتقييم نقاط الضعف في الشبكة
الخطوة ٤. الإبلاغ عن النتائج النهائية وتحديد الإجراءات المضادة

٥. فهم منهجية اختبار الأمان

١. الاستطلاع
٢. فحص الشبكة والمنافذ
٣. فحص السياسة
٤. تحقيقات الضعف وبصمات الأصابع
٥. الاختراق
٦. العد والتكسير
٧. التصعيد: المختبر يحصل على امتيازات إدارية على الأنظمة.
٨. backdoors
٩. التهريب

أنشأ مشروع أمان تطبيق الويب المفتوح (OWASP) طريقة مجانية جيدة الإعداد لتقييم ثغرات الويب ، والتي يمكن العثور عليها على https://www.owasp.org.

6.Intrusion Prevention Systems (IPS)

The intrusion prevention system (IPS), also known as intrusion detection and prevention system (IDPS), is an extension of an IDS that includes the capability to attempt to block or prevent detected malicious activity. Like an IDS, an IPS can be host-based, network-based,.

Examples of the types of malicious behavior addressed by a HIPS include the following:

- Modification of system resources
- Privilege–escalation exploits
- Buffer–overflow exploits.
- Access to e–mail contact list
- Directory traversal

HIPS typically offers the following desktop protection:

- System calls: The kernel controls access to system resources such as memory.
- I/O devices, and processor.
- File system access
- System registry settings
- Host input/output

Sandboxes are especially suited to mobile code, such as Java applets and scripting languages.

Network-based IPS

In terms of the general methods used by a NIPS device to identify malicious packets, the following are **typical**:

- Pattern matching
- Stateful matching
- Protocol anomaly
- Statistical anomaly

7.Honeypots

Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems

- Divert an attacker from accessing critical systems.
- Collect information about the attacker's activity.
- Encourage the attacker to stay on the system long enough for administrators to respond.

٦- أنظمة منع الاقتحام (IPS)

يعد نظام منع التطفل (IPS)، المعروف أيضًا باسم نظام اكتشاف ومنع التطفل (IDPS)، امتدادًا لنظام IDS الذي يتضمن القدرة على محاولة منع أو منع النشاط الضار المكتشف. مثل IDS، يمكن أن تكون IPS قائمة على المضيف، وقائمة على الشبكة،

تتضمن أمثلة أنواع السلوك الضار التي يعالجها HIPS ما يلي:

- تعديل موارد النظام
- استغلال تصعيد الامتياز
- مآثر Buffer-overflow.
- الوصول إلى قائمة الاتصال بالبريد الإلكتروني
- اجتياز الدليل

يوفر نظام HIPS عادةً الحماية التالية لسطح المكتب:

- استدعاءات النظام: تتحكم النواة في الوصول إلى موارد النظام مثل الذاكرة.
- أجهزة I / O والمعالج.
- الوصول إلى نظام الملفات
- إعدادات تسجيل النظام
- إدخال / إخراج المضيف

تعتبر Sandboxes مناسبة بشكل خاص لرمز الهاتف المحمول ، مثل تطبيقات Java الصغيرة ولغات البرمجة النصية.

IPS القائمة على الشبكة

فيما يتعلق بالطرق العامة التي يستخدمها جهاز NIPS لتحديد الحزم الضارة ، فإن ما يلي **نموذجي**:

- نمط مطابقة
- مطابقة الحالة
- بروتوكول شذوذ
- الشذوذ الإحصائي

٧- مواضع الجذب

مواضع الجذب هي أنظمة خادعة مصممة لجذب مهاجم محتمل بعيدًا عن الأنظمة المهمة

- صرف المهاجم عن الوصول إلى الأنظمة الهامة.
- جمع المعلومات حول نشاط المهاجم.
- شجع المهاجم على البقاء على النظام لفترة كافية حتى يستجيب المسؤولون.