# نماذج الشبكات

- **OSI Model**

يعد نظام Open System Interconnection معيارًا مفتوحًا لجميع أنظمة الاتصالات. تم إنشاء نموذج OSI بواسطة المنظمة الدولية للمعايير (OSI). ويعتبر Open Systems Interconnection نموذجًا مفاهيميًا يميز ويوحد وظائف الاتصالات لنظام الاتصالات أو الحوسبة دون مراعاة البنية الداخلية والتكنولوجيا الأساسية. يتكون هذا النموذج من سبع طبقات:

**This model has seven layers:**

| | |
|---|---|
| **طبقة التطبيق:** تتفاعل مباشرة مع التطبيقات وتوفر خدمات الشبكة للمستخدمين. | Application Layer |
| **طبقة العرض:** تتولى تنسيق البيانات وتنسيقها لتكون قابلة للقراءة من قبل التطبيقات. | Presentation Layer |
| **طبقة الجلسة:** تدير الاتصالات بين التطبيقات وتتحكم في تبادل البيانات. | Session Layer |
| **طبقة النقل:** تضمن وصول البيانات بشكل صحيح وكامل من طرف إلى آخر. | Transport Layer |
| **طبقة الشبكة:** تتولى توجيه البيانات عبر الشبكة من المصدر إلى الوجهة. | Network Layer |
| **طبقة الربط:** توفر الاتصال الموثوق بين العقد على الشبكة وتدير أخطاء البيانات. | Data Link Layer |
| **الطبقة الفيزيائية:** تتعامل مع الإشارات الكهربائية والإرسال المادي للبيانات. | Physical Layer |

- **TCP/IP Model**

**(Transmission Control Protocol/Internet Protocol)** هو النموذج الأساسي الذي يعتمد عليه الإنترنت. هذا النموذج يتألف من أربعة طبقات، وهي:

1- **الطبقة التطبيقية:** تشمل بروتوكولات مثل HTTP وFTP، وتتعامل مع بيانات التطبيقات.
2- **طبقة النقل:** تشمل بروتوكولات مثل TCP وUDP، وتتعامل مع نقل البيانات بين التطبيقات.
3- **الطبقة الشبكية:** تشمل بروتوكول IP، وتتعامل مع توجيه البيانات عبر الشبكة.
4- **الطبقة الرابطية:** تتعامل مع الاتصال الفعلي بالشبكة، مثل .Ethernet

## بروتوكولات الشبكة

1- بروتوكولات الإنترنت: **IP (Internet Protocol)** يحدد كيفية توجيه البيانات،
2- بروتوكولات **TCP (Transmission Control Protocol)** يضمن تسليم البيانات بشكل موثوق.
3- بروتوكولات نقل البيانات: **HTTP (Hypertext Transfer Protocol)** لنقل صفحات الويب،
4- بروتوكولات **FTP (File Transfer Protocol)** لنقل الملفات،
5- بروتوكولات **SMTP (Simple Mail Transfer Protocol)** للبريد الإلكتروني.
6- بروتوكولات الأمان: **SSL (Secure Sockets Layer)**
7- بروتوكولات **TLS (Transport Layer Security)** توفران تشفير البيانات أثناء النقل.

# Network Security امن الشبكات

## ما هو أمن الشبكات؟

أمن الشبكات هو مجال يهتم بحماية البيانات والمعلومات والأنظمة المتصلة في شبكة من التهديدات والهجمات. في عصرنا الحديث الذي يعتمد بشكل كبير على التكنولوجيا والاتصالات، أصبح أمن الشبكات مسألة ذات أهمية حاسمة. يحاول متخصصو أمن الشبكات مواجهة ومنع التهديدات المحتملة للبيانات والمعلومات، وضمان سلامة الشبكات والحفاظ على سرية المعلومات.

## أنواع التهديدات والهجمات:-

### 1- هجمات الاختراق

هجمات الاختراق هي إحدى أكثر أنواع التهديدات شيوعًا في عالم أمن الشبكات. تهدف هذه الهجمات إلى اختراق أنظمة الشبكات واستغلال الثغرات الأمنية. من بين أمثلة الهجمات الشهيرة يمكن ذكر هجمات الاختراق التي تستهدف المواقع الحكومية أو الشركات الكبيرة. تعتمد هذه الهجمات على استغلال ضعف الأمان في الشبكات وتطبيقاتها.

### 2- البرمجيات الخبيثة والفيروسات

البرمجيات الخبيثة والفيروسات تمثل تهديدًا آخر لأمن الشبكات. تشمل هذه التهديدات برامج التجسس، وأحصنة طروادة، وبرامج الفدية، وغيرها من البرمجيات الخبيثة التي تستهدف البيانات الحساسة وتسبب ضررًا جسيمًا. يمكن أن تنتشر هذه البرمجيات عبر البريد الإلكتروني المشبوه أو المواقع غير الموثوقة، ومن ثم تصيب أجهزة الكمبيوتر والشبكات بأكملها.

### 3- الهجمات الموجهة والاستنساخ

تشمل الهجمات الموجهة استهداف شبكات محددة، سواء كانت شركات أو أفرادًا. يتعمد المهاجمون في هذه الحالة على تحديد أهدافهم وتصميم هجمات مخصصة لاختراق تلك الشبكات المستهدفة. بالإضافة إلى ذلك، يتم استخدام التكنولوجيا المتقدمة لاستنساخ الشبكات واستغلال الثغرات الموجودة بها.

## أسباب لماذا تحتاج إلى أمان الشبكة

**1- لحماية المعلومات من الوصول غير المرغوب فيه**
من الأسباب الرئيسية لتأسيس أمان الشبكة وامتلاك برنامج أمان الشبكة المناسب هو امتلاك القدرة على حماية المعلومات من الوصول غير المصرح به. نظرًا لأن الأنظمة الإلكترونية عرضة للتهديدات وخروقات البيانات، فمن الآمن القول إنها تقوم بعمل رائع في حماية جميع أجهزتك وبرامجك من مثل هذه الأحداث.

**2- لحماية البيانات من أي تأخير غير مناسب في المسار المتبع لتسليمها إلى الوجهة في الوقت المطلوب.**
إن وجود تدابير أمنية جيدة للبيانات وحماية معلومات الشركة من التأخيرات غير المناسبة هو غرض آخر لتأسيس أمان الشبكة. إنه يحافظ على وقت التسليم أو النشر متسقًا ويعمل بكفاءة.

**3- لحماية البيانات من أي تعديل غير مرغوب فيه**
بصرف النظر عن الوصول غير المصرح به والتهديدات المحتملة، فإن فكرة التعديل غير المرغوب فيه هي سبب آخر لتولي أمن الشبكة المسؤولية. تعمل حماية البيانات ضد التعديلات غير المرغوب فيها على تقليل فرص الحصول على إذن غير مرغوب فيه من مستخدمين ليسوا جزءًا من نظام الأمان.

4- **لمنع مستخدمين معينين في الشبكة من إرسال أي نوع من البريد أو الرسائل بطريقة تظهر للطرف المستلم أنها مرسلة من قبل طرف ثالث.**
باستخدام أمان الشبكة، يمكن حماية إرسال رسائل البريد الإلكتروني، وخاصة من قبل مستخدمين معينين. يؤدي إرسال رسائل البريد الإلكتروني من خلال الحماية إلى إخفاء هوية مرسلي الرسالة الأصلية.

5- **لحماية الأجهزة مثل الأقراص الصلبة وأجهزة الكمبيوتر وأجهزة الكمبيوتر المحمولة من هجوم الفيروسات التي يمكن أن تلحق الضرر بالأنظمة عن طريق إتلاف أو حذف جميع المحتويات المخزنة داخلها.**
الأجهزة والأقراص الثابتة عرضة للتعرض للفيروسات. لهذا السبب يمكن أن تفيد أجهزة الكمبيوتر الشخصية وأجهزة الكمبيوتر المحمولة لأنها يمكن أن تساعد في حماية المحتوى المخزن من الحذف أو التلف.

6- **لحماية جهاز الكمبيوتر من البرامج، والتي إذا تم تثبيتها، يمكن أن تلحق الضرر بالنظام كما يفعل المتسللون.**
يمكن للقراصنة إحداث الكثير من الضرر للأنظمة والبرامج. تعد حماية جهاز الكمبيوتر الخاص بك من البرامج المشبوهة طريقة أخرى لزيادة الحماية ضد الهجمات الإلكترونية.

7- **لمنع أحصنة طروادة وworm من تدمير نظامك تمامًا**
تعد أحصنة طروادة والديدان أنواعًا من البرامج الضارة التي يمكن أن تلحق أضرارًا جسيمة بالنظام. تعمل هذه الفيروسات على تضليل المستخدمين وتسبب الضعف السيبراني في جميع أنحاء الشبكة.

## تقنيات أمن الشبكات

- الحماية بواسطة الجدران النارية

تعتبر الجدران النارية أحد أساسيات أمن الشبكات. تقوم هذه التقنية بمنع وفحص حركة المرور في الشبكة وتصفيتها وفقًا للقواعد المحددة. تعمل الجدران النارية على حماية الشبكة من الهجمات الخارجية وتقييد الوصول غير المصرح به إلى الموارد والأنظمة.

- التشفير والتوقيع الرقمي

يعد التشفير والتوقيع الرقمي جزءًا أساسيًا من أمن الشبكات. يتم استخدام التشفير لحماية البيانات وجعلها غير قابلة للقراءة أو الاستخدام غير المصرح به. أما التوقيع الرقمي، فهو يساعد في التحقق من صحة وأصالة البيانات والتأكد من عدم تعرضها للتلاعب.

- منع الوصول غير المصرح به

يهدف منع الوصول غير المصرح به إلى حماية الشبكات من الاختراقات الداخلية. يتم تطبيق سياسات الوصول وتحديد الأذونات لضمان أن يتم الوصول إلى المعلومات والموارد الحساسة فقط من قبل الأشخاص المصرح لهم.

- اكتشاف التهديدات والمراقبة

يعتبر اكتشاف التهديدات والمراقبة جزءًا هامًا من أمن الشبكات. يتم استخدام أنظمة المراقبة وتحليل سجلات الأحداث لرصد واكتشاف أي تهديدات محتملة للشبكة. يتم اتخاذ إجراءات سريعة لمعالجة هذه التهديدات والتصدي لها قبل أن تتسبب في أضرار جسيمة.

## استراتيجيات الأمان:

هناك استراتيجيات مختلفة من أمان الشبكة. يقوم بإنشاء هيكل لقسم تكنولوجيا المعلومات بالإضافة إلى مساعدة المستخدمين على استخدام البرامج والأجهزة بشكل صحيح.

1- **برنامج مكافحة الفيروسات ومكافحة البرامج الضارة :** يمكن أن يساعد برنامج مكافحة الفيروسات ومكافحة البرامج الضارة الذي لا يحتاج إلى شرح، في تقليل فرص تعرض الأجهزة للبرامج الضارة والفيروسات تمامًا.

2- **أمان التطبيق:** يسمح تطوير أمان الإجراءات باختبار ميزات الأمان التي تعد جزءًا من التطبيق. يحدد هذا ما إذا كان التطبيق آمنًا للاستخدام أو يحتاج إلى تحديث حتى يعمل بشكل أفضل.

3- **التحليلات السلوكية:** التحليلات السلوكية هي أداة رائعة يمكنها مراقبة جميع أنواع الأنشطة التي تجري داخل الشبكة. يساعد هذا في اكتشاف الأنشطة التي يمكن اعتبارها مشبوهة والمحتوى الذي يمكن اعتباره تهديدًا محتملاً. يمكن لهذه الأداة أيضًا أن تبحث في الطرق المحتملة لتحسين أمان الشبكة نفسها.

4- **منع فقدان البيانات(DLP)**:- يمكن أن يأتي هذا كبرنامج أو أدوات يمكن أن تساعد في عملية النسخ الاحتياطي للبيانات المفقودة. كما أنه يضمن عدم وصول بيانات معينة من مستخدمين غير مصرح لهم يمكن أن يستفيدوا من البيانات الحساسة المذكورة.

5- **أمان البريد الإلكتروني:** تأمين رسائل البريد الإلكتروني من التسريب. يساعد هذا النوع المستخدمين من تلقي رسائل البريد الإلكتروني غير المرغوب فيها كما يمنع وصول رسائل البريد الإلكتروني إلى الوجهة الخطأ.

6- **جدران الحماية:** فكر في هذا النوع من أمان الشبكة كعامل تصفية. يمكن أن تسمح للخير وترك الشر. يراقب حركة المرور الواردة والصادرة للمستخدمين أثناء تصفح الويب.

7- **أمان الجهاز المحمول:** يعد الأمان لجهازك المحمول أداة أساسية أخرى. هذا يحمي هاتفك من البرامج الضارة أو المتسللين من سرقة المعلومات المخزنة داخل نظام جهازك المحمول.

8- **تجزئة الشبكة:** تجزئة الشبكة هو إنشاء شبكات فرعية تسمح بتعزيز أداء النظام بالإضافة إلى إفساح المجال للتحسين داخل نظام أمان الشبكة.

9- **معلومات الأمان وإدارة الأحداث (SIEM):-** جزء من قسم فرعي لأمن الكمبيوتر، يوفر SIEM تحليل تنبيه الأمان في الوقت الفعلي مع الوظائف المدمجة لمعلومات الأمان وإدارة الأحداث.

10- **الشبكة الافتراضية الخاصة (VPN):-** غالبًا ما تستخدم أماكن العمل شبكات VPN لحماية المعلومات القيمة التي تخص الشركة. يمكن أن يحمي أنشطة التصفح لمستخدمي العين العامة ويساعد في حماية موظفيك من المستخدمين الآخرين الذين قد يستخدمون شبكة WIFI العامة.

11- **أمان الويب:** أمان موقع ويب أو تطبيق ويب. يُعرف هذا أيضًا باسم الأمن السيبراني، وهذا هو سبب وجوده. يعد الحصول على أمان الويب أمرًا حيويًا لأنه يمكنه اكتشاف التهديدات التي يمكن أن تهاجم النظام ومنعها والاستجابة لها بسرعة.

12- **الأمان اللاسلكي:** يتمثل دور الأمن اللاسلكي في حماية الأجهزة من الوصول غير المصرح به. مثال على الأمن اللاسلكي هو أمان WIFI لأنه شائع بين الشبكات اللاسلكية المعرضة للتهديدات والوصول المفتوح.

13- **تأمين نقطة النهاية :** تأمين نقاط النهاية هو شكل آخر. نظرًا لأن أجهزة الكمبيوتر المكتبية والمحمولة معرضة للتهديدات الضارة، فمن الأهمية بمكان لأمن نقطة النهاية أن يقوم بوظائفه عن طريق منع الهجمات قبل أن يستولي بالكامل على جهاز المستخدم النهائي.

14- **التحكم في الوصول إلى الشبكة (NAC):-** يجمع التحكم في الوصول إلى الشبكة، أو NAC، بين أمان نقطة النهاية ومصادقات النظام جنبًا إلى جنب مع فرض أمان الشبكة. يساعد هذا في فرض السياسات على أجهزة الشبكة الآمنة للمستخدمين.

## استراتيجيات الصيانة الشبكات :

تشمل التحديثات الدورية والتأكد من وجود نسخ احتياطية.

1- **إعداد كلمات مرور قوية:** أفضل ممارسة للحفاظ على أمان أنظمتك وشبكتك هي إعداد كلمة مرور آمنة. سواء كانت ثمانية أحرف أو أكثر، يجب أن تكون أنواع كلمات المرور المراد إنشاؤها قوية بما يكفي لحماية جميع معلوماتك. حتى لا تنسى، أنشئ كلمة مرور يسهل تذكرها لاستخدامها.

2- **إنشاء جدار حماية:** يحمي هذا النوع من أجهزة أمان الشبكة الشاشات من حركة المرور الواردة والصادرة. كما أنه يساعد على منع تسرب المعلومات السرية.

3- **تثبيت الحماية من الفيروسات:** الحماية من الفيروسات هي طريقة أخرى فعالة للحفاظ على نظامك وشبكتك آمنة. سيحميك هذا البرنامج من الفيروسات وتهديدات البرامج الضارة الأخرى التي قد تصيب النظام.

4- **تحديث نظام باستمرار:** الحفاظ على تحديث أنظمتك هو ممارسة أخرى. نظرًا لأن الهجمات غالبًا ما تحدث للبرامج والأنظمة القديمة، فمن الأفضل حماية نفسك من خلال تحديث شبكتك لحماية نفسك من الهجمات المحتملة.

5- **حماية أجهزة الكمبيوتر المحمولة والهواتف المحمولة:** حماية أجهزة الكمبيوتر المحمولة والهواتف الخاصة بك من السرقة أو القرصنة هي طريقة أخرى لترقية أمان الشبكة. سواء كان ذلك فعليًا أو من خلال نظام، من الضروري عدم ترك الأجهزة الإلكترونية القيمة بعيدًا عن الأنظار. قم بتثبيت برنامج الأمان وإعداد عمليات المصادقة الثنائية لمنع ذلك.

6- **السماح بالنسخ الاحتياطي في الوقت المحدد:** النسخ الاحتياطية في الوقت المحدد جزء من تحديث الأنظمة باستمرار. سيؤدي السماح بالنسخ الاحتياطي التلقائي في الوقت المناسب إلى إصلاح عملية حماية أمان الشبكة. إنه سريع جدًا ولا يتطلب الكثير من العمل لأدائه.

7- **تصفح ذكي على الويب:** يتصفح الجميع الويب. ولكن الحل الأفضل هو التصفح بذكاء. يعد تصفح الويب بذكاء حلاً آخر لحماية نظامك وشبكتك. ضع في اعتبارك الشبكات الخاصة الافتراضية، أو شبكات VPN، التي يمكن أن تساعد في التصفح وتساعد في حمايتك من مواجهة البرامج الضارة والتهديدات الأخرى التي قد تظهر على شاشتك.

8- **التكوين الآمن:** عمليات التهيئة الخاطئة الآمنة هي أسباب تمكن المتسللين من الوصول إلى الأنظمة نظرًا لأن الثغرات الشائعة يمكن أن تستغل المعلومات. من خلال التكوين الآمن، يمكن بسهولة الاحتفاظ بتثبيت الأجهزة وأمان الشبكة بالترتيب مع تقليل فرص تهديد الأنشطة الإلكترونية.

9- **السماح بالتحكم في الوسائط القابلة للإزالة:** يمكن أن يؤدي السماح بالتحكم في الوسائط القابلة للإزالة إلى تقليل فرص مواجهة انتهاكات الشبكة. بمجرد اتصال الوسائط بأجهزة تحتوي على معلومات شخصية، سيكون من السهل على المهاجمين الوصول إليها، مما يتسبب في نقاط الضعف السيبرانية.