المرحلة الثالثة

مادة الحاسبات

كلية التربية البدنية وعلوم الرياضة

جامعة المستقبل

اعـــــداد

م.م. مصطفى عدنان مدلول البكري

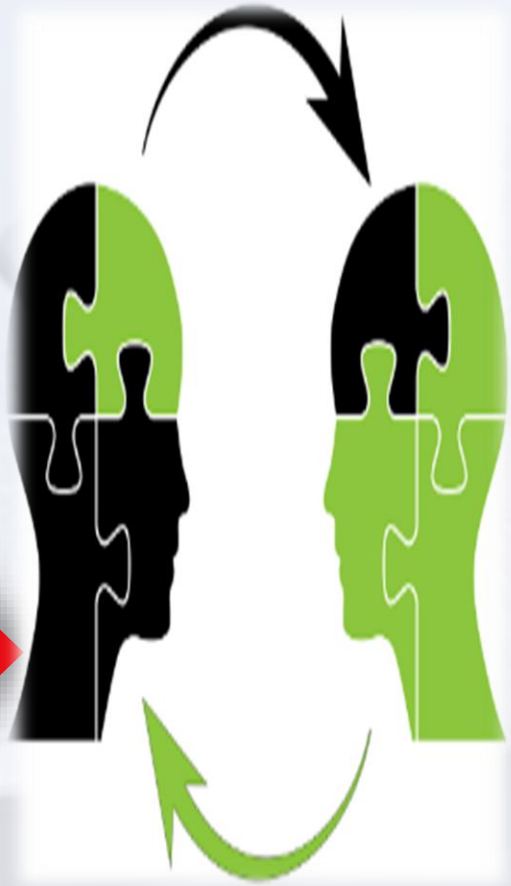
المحاضرة السادسة

اساسيات امن الشبكات والتهديدات

🎯 هدف المحاضرة:

تمكين الطالب من التعرّف على المخاطر وخصائصها في مجال أمن الشبكات

المحتويات



مقدمة عن امن الشبكات

في عصرنا الرقمي الحالي، حيث تعتمد الاتصالات وتبادل البيانات والعمليات التجارية بشكل كبير على شبكات الحاسوب، أصبح أمن الشبكات ضرورة أساسية لا يمكن الاستغناء عنها.

يشير أمن الشبكات إلى مجموعة من التقنيات والسياسات والإجراءات المصممة لحماية سلامة البيانات وسريتها وتوافرها داخل الشبكات.

وسائل الحماية الأساسية

- جدران الحماية
- برامج مكافحة الفيروسات
- أنظمة كشف التسلل
- التشفير
- الشبكات الخاصة الافتراضية
- سياسات التحكم في الوصول وتوعية المستخدمين

أمن الشبكات

هو مجموعة من السياسات والتقنيات والإجراءات التي تهدف إلى حماية البيانات عبر الشبكة من خلال ضمان:

- **السرية:** منع الوصول غير المصرح به إلى البيانات.
- **السلامة:** منع التعديل أو التلاعب غير المصرح به.
- **التوافر:** ضمان بقاء البيانات والخدمات متاحة عند الحاجة.

التهديد

هو أي عامل أو حدث محتمل يمكن أن يستغل ثغرة أمنية بهدف إلحاق الضرر بالأنظمة أو البيانات

يظهر أثره من خلال:

- **الإخلال بالسرية:** تمكين جهات غير مخوّلة من الوصول إلى المعلومات.
- **المساس بالسلامة:** تعديل البيانات أو التلاعب بها دون تصريح.
- **التأثير على التوافر:** تعطيل الخدمات أو الحد من إمكانية الوصول إليها.

التهديدات الشائعة

1- البرمجيات الخبيثة:

وهي برامج ضارة تشمل الفيروسات والبرامج الفدية، تدخل إلى الأنظمة لإحداث ضرر أو لابتزاز المستخدمين ازدادت هجمات برامج الفدية في السنوات الأخيرة، وغالبًا ما تستهدف الأنظمة التي لم تُحدَّث بشكل دوري.

2- التصيد الاحتيالي والهندسة الاجتماعية:

هي هجمات تعتمد على **خداع المستخدمين** لجعلهم يقدمون معلوماتهم الحساسة عبر رسائل أو مواقع مزيفة تُسبب هذه الهجمات خسائر مالية كبيرة للمؤسسات سنويًا وتُعتبر من أكثر وسائل الهجوم شيوعًا.

التهديدات الشائعة

3- هجمات حجب الخدمة الموزعة:

يقوم المهاجمون بإرسال كميات ضخمة من الطلبات إلى الشبكة أو الخادم لإغراقه وجعله غير قادر على الاستجابة مما يؤدي إلى **توقف الخدمات** وخسائر مالية للمؤسسات التي تعتمد على الإنترنت.

4- هجمات الرجل في المنتصف:

يقوم هذا النوع من الهجمات **باعتراض الاتصالات** بين طرفين بهدف سرقة البيانات أو تعديلها أو إدخال برمجيات ضارة غالبًا ما تحدث في **الشبكات غير الآمنة مثل شبكات الوأي فأي العامة**.

التهديدات الشائعة

5- حقن قواعد البيانات:

يستغل المهاجم **الثغرات الموجودة في قواعد البيانات** لإدخال أوامر خبيثة تتيح له التلاعب بالمعلومات أو سرقتها

غالبًا ما تستهدف المواقع الإلكترونية ضعيفة الحماية.

6- الثغرات غير المكتشفة:

هي هجمات تستغل **نقاط ضعف لم يتم اكتشافها أو إصلاحها بعد** في البرامج أو الأنظمة

تُعتبر من أخطر أنواع الهجمات لأنها تحدث قبل أن تصدر تحديثات الأمان.

التهديدات الشائعة

7- التهديدات الداخلية:

تنشأ من داخل المؤسسة نفسها، إما **بشكل متعمد** من موظف يريد الإضرار بالمؤسسة أو **بشكل غير مقصود** نتيجة الإهمال

تُعد من أخطر التهديدات لأن صاحبها يمتلك صلاحيات دخول موثوقة.

8- تهديدات أجهزة إنترنت الأشياء والأنظمة التشغيلية:

تشمل الأجهزة المتصلة بالإنترنت مثل الكاميرات، والطابعات الذكية، وأجهزة التحكم الصناعية.

غالبًا ما تفتقر هذه الأجهزة إلى الحماية الكافية، مما يجعلها **نقطة دخول سهلة للمخترقين** إلى الشبكة.

مهم جدا

ت	نوع التهديد	المثال	الوصف
1	البرمجيات الخبيثة (برامج ضارة)	برنامج فدية يقوم بقفل الملفات	برامج تُصمَّم لإتلاف الأنظمة أو التحكم بها أو ابتزاز المستخدم. تشمل الفيروسات والديدان وبرامج الفدية.
2	التصيد الاحتيالي (خداع إلكتروني)	رسالة بريد إلكتروني مزيفة تدّعي أنها من بنك	محاولة خداع المستخدم للحصول على معلومات حساسة مثل كلمات المرور عبر رسائل أو مواقع مزيفة.
3	هجمات حجب الخدمة الموزعة (إغراق الخوادم)	توقف موقع تسوّق إلكتروني بسبب طلبات كثيرة جدًا	هجوم يعتمد على إرسال عدد ضخم من الطلبات لتعطيل الخادم ومنعه من العمل.
4	هجمات الرجل في المنتصف (اعتراض الاتصال)	التنصت على مستخدم في شبكة واي فأي عامة	يقوم المهاجم باعتراض الاتصال بين طرفين لسرقة البيانات أو التعديل عليها.
5	حقن قواعد البيانات (إدخال أوامر ضارة)	سرقة بيانات العملاء من موقع إلكتروني	استغلال ثغرة في قاعدة البيانات لإدخال أوامر تخريبية تسمح بالتعديل أو السرقة.
6	الثغرات غير المكتشفة (نقاط الضعف المخفية)	الهجوم على الأنظمة الصناعية مثل ستوكسنت	هجمات تستغل أخطاء لم يتم اكتشافها بعد في البرامج أو الأنظمة قبل صدور تحديثات الأمان لها.
7	التهديدات الداخلية (مخاطر من داخل المؤسسة)	موظف يسرب بيانات الشركة	ضرر يحدث من داخل المؤسسة، بشكل متعمد أو بسبب الإهمال، من شخص يملك صلاحيات.
8	تهديدات أجهزة إنترنت الأشياء (الأجهزة المتصلة)	هجوم "ميراي" الذي أصاب كاميرات وأجهزة ذكية	استغلال الأجهزة المتصلة بالإنترنت ذات الحماية الضعيفة للوصول إلى الشبكة أو تنفيذ هجمات أكبر.

نشاط

ماهي التهديدات الشائعة

- البرمجيات الخبيثة
- التصيد الاحتيالي والهندسة الاجتماعية
- هجمات حجب الخدمة الموزعة
- هجمات الرجل في المنتصف
- حقن قواعد البيانات
- الثغرات غير المكتشفة
- التهديدات الداخلية
- تهديدات أجهزة إنترنت الأشياء والأنظمة التشغيلية

شكراً لحسن اصغائكم