# Lecture 2: Security and Networking: Network Security Basics. Understanding Network threats.

# اساسيات امن الشبكات وفهم تهديدات الشبكة

## 1- ماهو أمن الشبكات ؟

**أمن الشبكات** هو مجال يهتم بحماية شبكات الحاسوب من **الاختراقات والتهديدات والهجمات الإلكترونية**.

بمعنى آخر، هو **مجموعة من الإجراءات والتقنيات** التي تضمن أن المعلومات المرسلة أو المخزنة داخل الشبكة تبقى **آمنة وسرية وغير قابلة للتلاعب**.

## 2. أهداف أمن الشبكة

1. **السرية** (Confidentiality): حماية البيانات من الوصول غير المصرح به.
2. **سلامة البيانات** (Integrity): التأكد من أن البيانات لم تتغير أو تتلف أثناء النقل أو التخزين.
3. **التوافر** (Availability): ضمان وصول المستخدمين المصرح لهم إلى الموارد والخدمات عند الحاجة.
4. **المصادقة** (Authentication): التأكد من هوية المستخدم أو الجهاز قبل منح الوصول.
5. **عدم الإنكار** (Non-repudiation): ضمان أن المرسل لا يستطيع إنكار أنه أرسل البيانات.

## 3- انواع التهديدات او الهجمات الشبكية

**اولا : الهجمات الخارجية :** هي الهجمات التي تاتي من خارج الشبكة او المؤسسة الهدف منها هو لتعطيل الخدمة , سرقة البيانات او التحكم في النظام .

**امثلة عن الهجمات الخارجية :**

1-هجمات الحرمان من الخدمة (DDoS) :تعني ارسال كميات كبيرة من الطلبات الى الخادم فيتوقف عن العمل .

2-التصيد : تعني ارسال رسائل مزورة للمستخدم لاعطاء كلمة المرور او معلومات شخصية

3-البرمجيات الخبيثة (الفيروسات) :هي برامج تسرق البيانات او تغلق الجهاز.

**الوقاية** : تحديث الانظمة , استخدام مضادات الفايروسات , الحذر من الروابط الغريبة واستخدام كلمات مرور قوية.

**ثانيا : الهجمات الداخلية :** هي هجمات تاتي من داخل المؤسسة , موظف ضار او جهاز مخترق داخل الشبكة . الهدف منها سرقة بيانات او تعطيل الشبكة او اساءة استخدام الصلاحيات .

**امثلة عن الهجمات الداخلية :**

1- سوء استخدام الصلاحيات : كمثال موظف يدخل على ملفات لايجب ان يراها
2- المستخدم المهمل : مثل فتح ملفات خبيثة او اعطاء بيانات بالخطأ
3- حساب مخترق : كشخص مهاجم خارجي يسيطر على حساب موظف داخلي.

**الوقاية :**

تحديد الصلاحيات فقط حسب الحاجة , مراقبة الانشطة الغريبة ,استخدام كلمات مرور قوية اضافة الى مراجعة الحسابات دوريا.

| المكونات الاساسية لامن الشبكات | | |
|---|---|---|
| المكون الاساسي | الوظيفة الرئيسية | التفاصيل |
| جدار الحماية Firewall | تصفية حركة المرور | يعمل كحاجز بين الشبكة الداخلية والعالم الخارجي، يسمح أو يمنع الاتصال بناءً على قواعد محددة مسبقًا. |
| نظام كشف التسلل IDS | المراقبة والتنبيه | يراقب حركة البيانات داخل الشبكة لاكتشاف أي سلوك غير طبيعي أو اختراق محتمل، وينبه المسؤولين فورًا. |
| نظام منع التسللIPS | المنع والحماية الفعلية | لا يكتفي بالكشف بل يقوم بإيقاف الهجوم مباشرة مثل حجب العناوين أو قطع الاتصال المشبوه. |
| التشفير Encryption | حماية البيانات اثناء النقل او التخزين | يحول البيانات إلى صيغة غير مفهومة إلا للمستقبل المصرح له، مما يمنع التجسس أو السرقة. |
| التحكم في الوصول | تحديد صلاحيات المستخدمين | يضمن أن كل مستخدم يمكنه الوصول فقط إلى الموارد التي يحتاجها، حسب الهوية والدور. |
| ادارة الهوية والمصادقة | التحقق من هوية المستخدمين | تستخدم لتأكيد هوية المستخدمين قبل منحهم صلاحيات الدخول إلى الشبكة. |
| السياسات الامنية | وضع قواعد السلوك والاستخدام | تحدد كيفية استخدام الشبكة، كلمات المرور، إدارة الأجهزة، وإجراءات التعامل مع الحوادث الأمنية. |
| الشبكات الخاصة الافتراضية | تأمين الاتصالات عن بعد | تنشئ قناة اتصال مشفرة بين المستخدمين البعيدين والشبكة الداخلية لضمان الأمان. |
| مكافحة البرمجيات الخبيثة | الكشف عن الفايروسات والبرمجيات الخبيثة | يحمي الأنظمة من الفيروسات، برامج التجسس، وبرامج الفدية. |
| انظمة المراقبة والتحليل | تتبع وتحليل الانشطة | تجمع وتحلل سجلات النظام لتحديد الأنماط المشبوهة وتقديم تنبيهات ذكية. |
| النسخ الاحتياطي والتعافي | ضمان استمرارية العمل بعد الهجمات | تحفظ نسخًا من البيانات الهامة لاستعادتها في حال تعرض النظام لهجوم أو فقد بيانات. |
| تحديث البرمجيات | اصلاح الثغرات الامنية | تحديث الأنظمة والبرامج باستمرار لسد الثغرات التي قد يستغلها المهاجمون. |