# Fundamentals of Network Security
# أساسيات حماية الشبكة

م . إنـاس عدي

# what is network security?

تعريف أمن شبكات المعلومات :

هي مجموعة من الإجراءات التي يمكن خلالها توفير الحماية القصوى للمعلومات والبيانات في الشبكات من كافة المخاطر التي تهددها، وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية.

## Rationale for network security :

- وجود الانترنت طوال الوقت
- ازدياد معدل الجريمة الالكترونية
- تكاثر في التهديدات الأمنية
- تطور التهديدات الأمنية

**الجريمة الإلكترونية : هي الجريمة التي تتم باستخدام جهاز الكمبيوتر من خلال الاتصال بالإنترنت ويكون هدفها اختراق الشبكات أو تخريبها أو التحريف أو التزوير أو السرقة والاختلاس أو قرصنة وسرقة حقوق الملكية الفكرية .**

## Goals of an information security program

**أهداف امن الشبكات هو تحقيق كلا من :**

- ✓Availability (ضمان الوصول إلى المعلومة): هو ضمان وصول المعلومات إلى الأشخاص المصرح لهم بالوصول إليها من خلال توفير القنوات والوسائل الآمنة والسريعة للحصول على تلك المعلومات .
- ✓Data Integrity (سلامة المعلومات): الحفاظ على سلامة هذه المعلومات من التزوير والتغير
- ✓Data Confidentiality (سرية المعلومات):الإجراءات والتدابير اللازمة لمنع إطلاع الاشخاص الغير المصرح لهم على المعلومات التي يطبق عليها بند السرية أو المعلومات الحساسة.

## Risk Management (إدارة المخاطر) :

هي العملية التي تسمح لنا بقياس درجة المخاطر التي تعرضت لها المنظمة وإدارتها .

ملاحظة: إدارة المخاطر تقلل من الإضرار ولكن لا يستطيع مسحها نهائيا .

### Risk Assessment(تقدير المخاطر) :

✓كل نقطة ضعف يكون لها قياس (ان كانت خطيرة ام لا ).

✓حيث تعتبر Risk Management بمثابة أخت , حيث تقوم Risk Assessment بتقدير المخاطر ويقوم Risk Managementبإدارتها .

✓ **Asset Identification** : تطلق على اي ممتلكات موجودة في الشبكة .

- **Categories of asset** : نوع الممتلكات الموجودة في الشركة (ممكن ان تكون أشخاص ، عتاد مادي , عتاد برمجي , نظام , الخ ....) .
- **determine each items relative value**

# Network security "Threat"

## التهديدات الأمنية

أنواع التهديدات الأمنية :

- eavesdropping(التنصت)
- denial of service (حجب الخدمة)
- packet reply
- packet modification
- man – in- the – middle

❖eaves dropping التجسس :

في هذا النّوع من الهجمات يقوم الهاكر بمراقبة الكمبيوتر الشخصي أو الشبكة المتصل بها بهدف التجسس وسرقة المعلومات، يخترق الهاكر جهازك أو الشبكة دون أن يُحدث ضررًا يمكن ملاحظته أو يؤثر على عمل النظام وينتظر مرور المعلومات سواءً كانت بريدًا إلكترونيًّا أو معلومات شخصية أو حتى المعلومات التي تستخدمها في مواقع الإنترنت، فكل هذا سوف يمر عليه في البداية وقد يستخدمه بأكثر من طريقة فيها فائدته ولكنها بالتأكيد ستضرك. وبشكل عام هناك نوعان لهذه الهجمات، النوع الأول Traffic Analysisيقوم فيه المخترق بتحليل الاتصال لتحديد موقعه والأطراف المشاركة فيه وطول ونوع المعلومات المتداولة بينهم دون المساس به أو تعديله، وفي النوع الثاني Release of message contentsيقوم المخترق بالاطلاع على المعلومات المُرسلة بين الطرفين أيًّا كان نوعها، وفي كلا النوعين من الصعب اكتشاف هذا الاختراق لأن المُخترق لا يمسّ المعلومات المرسلة فلا يشعر المُرسل أو المُستقبل بأي شيء. هذا النوع من الهجمات لا يتعلق بالكمبيوتر المكتبي فحسب، بل يمتد إلى الأجهزة اللوحية والمفكرات الشخصية والهواتف المحمولة أيضًا.

❖ denial of service (حجب الخدمة) الهدف من هذا النوع من الهجمات هو إيقاف عمل موقع إنترنت أو شبكة بأكملها. أيّ شبكةٍ أو موقعٍ على الإنترنت يعتمد في عمله على ما يعرف باسم الخادم Serverوهو جهاز كمبيوتر مركزي ينظم ويتحكم في البيانات الخارجة والداخلة من إلى الموقع أو الشبكة، تعمل هذه الهجمات على إرهاق وإنهاك هذه الخوادم بالطلبات بحيث تنهار الخوادم وينهار معها الموقع أو الشبكة المعتمدة عليها. السؤال الآن كيف يقوم الهاكر بفعل ذلك؟ يقوم الهاكر بتجنيد أجهزة كومبيوتر تعرف اصطلاحًا باسم zombie computersلتصبح تابعة له عبر اختراقها أو تثبيت برامج ضارة تقوم بذلك بالنيابة عنه، ثم يستخدم هذه الأجهزة لترسل طلبات دخول مثلًا لموقع ما في نفس الوقت، وعندما لا يتمكن الخادم المسؤول عن المواقع من تنفيذ كافة هذه الطلبات ينهار وينهار معه الموقع.


(d) Denial of service

❖تشير تسمية "الرجل في المنتصف" Man In The Middle واختصارها (MITM)الى عملية يقوم بها المهاجم لاعتراض محادثة جارية بين طرفين ما. تظهر هذه المحادثة وكأنها تجري بين الطرفين مباشرةً، ولكن في الحقيقة يتم التحكّم بها من قبل الشخص المهاجم، حيث يمكن له عرض وإضافة وإزالة وتعديل واستبدال الرسائل التي يتم تبادلها في هذه المحادثة

## Vulnerability( نقطة الضعف):

اي نقطة ضعف في الجهاز تسمى Vulnerability

: Risk management terms

Vulnerability : نقطة الضعف في الجهاز ، أو الشبكة أو النظام .

Threat : التهديد الأمني الذي يستخدمه لاستغلال نقطة الضعف

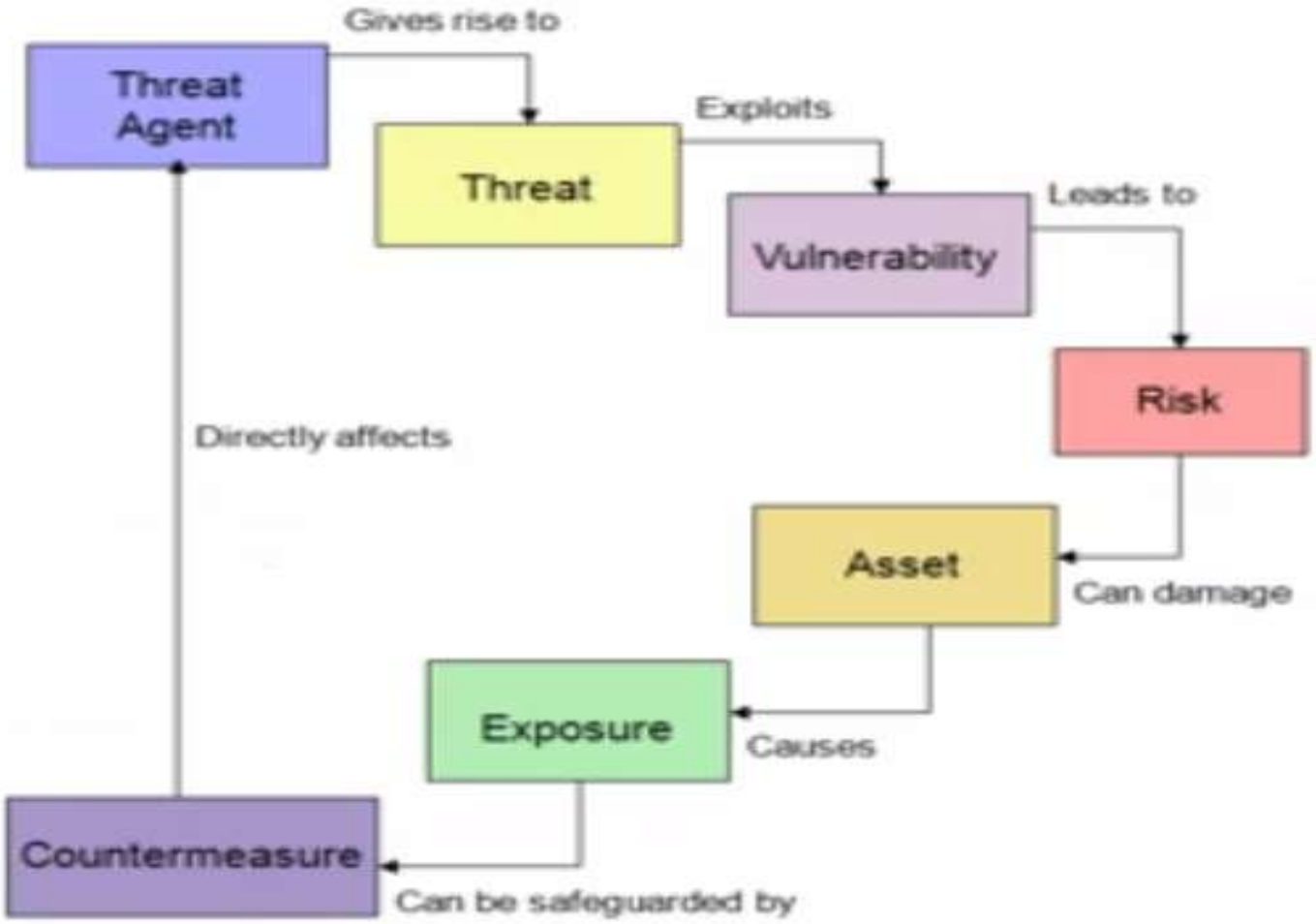
Threat Agent : الشخص الذي يستخدم Threat حتى يقوم بعمليات تخريب على النظام

Risk : هو ان يقوم Threat Agent باستخدام Threat و Vulnerability

Exposure : احتمالية حصول فقدان في البيانات بسبب Threat Agent

countermeasure : هي الاجراءات المضادة حتى يتم التاكد من عدم وجود اي تهديد او نقاط ضعف في الشبكة .

# Understanding Risk



## type of attacks : أنواع الهجوم من حيث التخطيط

- structured attacks
- unstructured attacks
- external attacks
- internal attacks
- passive attacks
- active attacks

1- الهجوم السلبي (Passive Attack) : بغرض الحصول على معلومات تستخدم في انواع اخرى من الهجمات مثل الحصول على كلمات السر.

التجسس – snooping.

تحليل البيانات المرسلة – Traffic Analysis.

2- الهجوم النشط (Active Attack) : يتضمن الدخول الى النظام واحداث الضرر المقصود.

التعديل – modification

التنكر – snooping

إعادة الإرسال – Replaying

الإنكار – Repudiation

حجب الخدمة – Denial of Service

3- الهجوم الموزع (Distributed Attack) : توزيع عنصر الهجوم مثل فيروس حصان طروادة (Trojan horse) على عدة شركات ومستخدمين بهدف احداث ضرر او تغيير في البيانات او في المعدات (hardware).

4- الهجوم الداخلي (Insider Attack) : يمكن للمهاجم الداخلي الذي هو جزء من النظام ان يقوم بكافة الاضرار للجزء الذي يعمل به والذي هو مخول بالعمل به وقد يتجاوزه الى اجزاء اخرى.

مهاجمة كلمة السر (Password attack): ويتضمن استخدام تقنيات كسر دوال التشفير لمعرفة كلمة السر او استخدام طرق توقع السر من خلال معلومات المستخدم الشخصية او عن طريق محاولة جميع استخدام جميع الرموز الموجودة لكشف كلمة السر.

هجوم اغراق المخزن المؤقت (Buffer overflow) : ويتضمن ارسال كم كبير غير متوقع من البيانات لوسيلة خزن معينة مما الى عدم استيعاب وسيلة الخزن الخاصة بالنظام وتوقفه.

# specific network attack

- ARP Attack
- Brute Force Attack
- Worms
- Flooding
- Sniffers
- Spoofing
- Redirected Attacks
- Tunneling Attack
- Covert Channels

Internet queries

Ping sweeps

Port scans

## stage of attack : مراحل الهجوم

- Reconnaissance
- Scanning (addresses, ports, vulnerabilities)
- Gaining access
- Maintaining Access
- Covering Tracks