جامعة المنارة

كلية الهندسة

قسم المعلوماتية

أمن المعلومات

مدرسة المقرر

د.بشرى علي معلا

عناوين المحاضرة الأولى

- مقدمة
- تعريف أمن المعلومات
- العلاقة بين مفهومي الأمن والشبكة
- أنواع التحكم بأمن المعلومات
- متطلبات أمن المعلومات
- ما الفرق بين مفهومي أمن المعلومات و الأمن السيبراني؟
- **مقارنة عملية بين أمن المعلومات والأمن السيبراني**
- مفهوم الهجمات وتصنيفها
- نموذج أمن الشبكة
- الجدران النارية

مقدمة

- مع ظهور شبكة الانترنت واتساع نطاق استخدامها بدأت تظهر مشكلة ضعف السرية في نقل المعلومات والبيانات عبر هذه الشبكة.
- مما زاد من سخونة قضية أمن المعلومات هو انتشار ظاهرة كسر شيفرة بطاقات الائتمان والوصول إلى المصارف والمؤسسات الأمنية الحيوية.
- من هنا جاءت أهمية توفير الأمن للمعلومات بالحفاظ على سريتها، وعدم العبث بمحتواها

مفهوم أمن المعلومات (Information Security)

- هو العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من المخاطر التي تهددها ومن أنشطة الاعتداء.
- أي هو العلم الذي يبحث في التقنيات التي تمنع الحصول على المعلومات و/أو تعديلها إلا من قبل المخّول لهم بذلك.
- **عرفت لجنة أنظمة الأمن القومي Committee on National Security Systems (CNSS) أمن المعلومات بأنه: حماية المعلومات وكل المكونات الحرجة من الأنظمة و التجهيزات الصلبة التي تستخدم أو تختزن أو ترسل تلك المعلومات.**

العلاقة بين مفهومي الأمن والشبكة

الأمن		شبكة
اتصالات مغلقة (Closed Communication)	←	اتصالات مفتوحة (Open Communication)
وصول مقيد Full Lockdown	←	وصول كامل Full Access

يجب تحقيق التوازن بين المفهومين

أنواع التحكم بأمن المعلومات (1/3)

- يوجد ثلاث فئات أساسية للتحكم بأمن المعلومات:

١. فيزيائي:

يمثل المكونات المادية التي تؤمن الحماية من اللصوص والمخربين، مثال استخدام أجهزة كالأقفال و كاشفات الحركة..

أنواع التحكم بأمن المعلومات (2/3)

- يوجد ثلاث فئات أساسية للتحكم بأمن المعلومات:

٢. منطقي

يمثل برمجيات التحكم بالوصول، البرمجيات المضادة للفيروسات، كلمات المرور والبطاقات الذكية.

أنواع التحكم بأمن المعلومات (3/3)

- يوجد ثلاث فئات أساسية للتحكم بأمن المعلومات:

٣. إداري:

يتعلق بالإجراءات المرتبطة بالأشخاص والخاصة بإدارة سلوك الأفراد، وهو يشمل التدريب على محددات الأمن وتقييم الأداء ...

جَـامعة المَـنارة

متطلبات أمن المعلومات
(Security Requirements)

١. الموثوقية /السرية (Confidentiality/Privacy)
٢. تكاملية المعطيات (Data Integrity)
٣. المصادقة (Authentication)
٤. التحكم بالوصول (Access Control)
٥. التوافرية (Availability)
٦. الترخيص / التفويض (Authorization)
٧. عدم التنصل (Non-Repudiation)

الموثوقية/السرية
(Confidentiality/Privacy)

المَـنارة

✓ تسمح بالحماية من الإطلاع غير الشرعي على المعلومات من قبل غير المخول لهم بذلك.

أي : السماح للأشخاص الشرعيين فقط بالوصول إلى المعلومات المخول لهم الحصول عليها: مثلاً، في الخدمات المدفوعة (التلفزيون باستخدام الانترنتIPTV، التعليم عن بعد، ..)، يحق فقط للأشخاص الذين دفعوا الحصول على الخدمة

✓ يعد التشفير من أكثر الطرائق شيوعاً لضمان سرية المعلومات.

تكاملية المعطيات

Data Integrity

- ✓ تسمح بالتحقق من أن المعطيات لم يطرأ عليها أي تعديل من قبل أي كيان غير مخول له بذلك سواء بشكل مفاجئ أو مقصود.
- ✓ يمكن التعديل بالطرائق المسموحة ومن قبل المفوضين بذلك فقط.
- ✓ من طرائق ضمان تكاملية المعطيات : تقنيات الترميز، التواقيع الرقمية، توابع البعثرة، برمجيات التحري عن الفيروسات واكتشافها ...

التو افرية

(Availability)

- ➢ التأكد من **استمرار** عمل النظام المعلوماتي، أي استمرار القدرة على التفاعل مع المعلومات، تقديم الخدمة وضمان وصول الأشخاص المخولين إلى المعلومات عندما يريدون.

المصادقة

Authentication

- ✓ تسمح بالتحقق من هوية الكيان أو المصدر الذي يرسل الرسالة
- ✓ طريقة المصادقة الأكثر بساطة هي:
استخدام الزوج: اسم المستخدم/كلمة المرور

أمثلة توضح الفرق بين المفاهيم الثلاث السابقة(1/2)
(Confidentiality, Integrity, Availability)

- مثال١: سرقة نسخة من ملف غير مشفر
  - الموثوقية Confidentiality: غير محققة لأن الملف لم يعد سرياً
  - التكاملية Integrity: محققة لأنه لم تُجر أية عملية تعديل
  - التو افرية Availability: محققة لأن الملف لا يزال متاح و يستطيع المستخدمون الوصول إليه
- مثال٢: إرسال ملف مشفر فيه معلومات مزيفة
  - الموثوقية Confidentiality: محققة لأن الملف بقي سرياً
  - التكاملية Integrity: غير محققة لأنه حُشرت معلومات غير صحيحة ضمن الملف
  - التو افرية Availability: محققة لأن الملف لا يزال متاح و يستطيع المستخدمون الوصول إليه

دراسة حالة عن (التو افرية، التكاملية، السرية)
(Confidentiality, Integrity, Availability)

تعرضت إحدى المستشفيات لهجوم خبيث ، قام المهاجم بتشفير جميع سجلات المرضى (بما في ذلك التقارير الطبية والأشعة)، مما جعلها غير قابلة للقراءة. كما منع الأطباء من الوصول إلى هذه السجلات لتقديم الرعاية للمرضى. قرر المهاجمون فك التشفير فقط إذا دفعت المستشفى فدية، المطلوب:

١. أي متطلب أمني انتهكه الهجوم بشكل أساسي عندما جعل سجلات المرضى غير قابلة للقراءة من قبل الأطباء؟

متطلب التو افرية : لأن النتيجة النهائية هي منع الأطباء من استخدام البيانات لتقديم الرعاية أي الهجوم حرم المستخدمين المصرحين من استخدام البيانات عندما يحتاجونها

2 . هل يمكن اعتبار أن "التكاملية " قد انتهكت في هذا الهجوم؟ لماذا؟.

نعم. لأن المهاجم غير بالبيانات عندما غير شكلها بتطبيق التشفير عليها.

3 . كيف انتهك الهجوم متطلب "السرية "؟

إن المهاجم اطلع على معلومات سجلات المرضى وهو لا يحق له الاطلاع عليها

التحكم بالوصول (Access Control)

✓ تسمح بالتحقق من أن أي كيان لا يمكن له الوصول **إلا إلى** الخدمات والمعلومات المسموحة .

إنه أسلوب ينظم **مَنْ وماذا يمكن عرضه أو استخدامه من الموارد في نظام ما**

أي : تحدد مستوى الوصول المسموح به لكل مستخدم

✓يرتبط غالباً بالمصادقة: فبعد أن تنفذ عملية المصادقة يحدد النظام ما هو مسموح به، وبذلك يتجنب النظام المستخدمين غير المخول لهم الوصول إلى البيانات.

مثال عن التحكم بالوصول (Access Control) (1/3)

بفرض لدينا نظام إدارة المستندات في شركة ما. لنفترض أن الشركة لديها **مجلد مشترك** يحوي المستندات التالية المرتبة من الأهم إلى الأقل أهمية :

خطة التوسع_2025.pdf ، الهيكل التنظيمي.pptx، إجازات الموظفين.xlsx

ناقش الحالتين الآتيتين:

1 . دون تطبيق أي سياسة من سياسات التحكم بالوصول

بإمكان أي موظف في الشركة رؤية وحتى تعديل كل هذه الملفات، بما في ذلك الخطط السرية للتوسع.

2 . مع تطبيق أي سياسة من سياسات التحكم بالوصول، املأ الجدول الآتي :

علماً أن الصلاحيات المستخدمة هي : قراءة فقط، تعديل فقط، تحكم كامل

مثال عن التحكم بالوصول (Access Control) (2/3)

النتيجة العملية	صلاحية الوصول	الملف	المستخدم
		إجازات_الموظفين.xlsx	**جميع الموظفين**
		إجازات_الموظفين.xlsx	**مدير قسم الموارد البشرية فقط**
		خطة_التوسع2025.pdf	**أعضاء مجلس الإدارة فقط**
		خطة_التوسع 2025.pdf	**مدير التطوير الاستراتيجي فقط**
		الهيكل_التنظيمي.pptx	**جميع الموظفين**
		جميع الملفات	**مدير النظام**

مثال عن التحكم بالوصول (Access Control) (3/3)

النتيجة العملية	صلاحية الوصول	الملف	المستخدم
أي موظف يمكنه فتح الملف ومعرفة سياسة الإجازات، لكن لا يمكنه تعديلها.	قراءة (Read)	إجازات الموظفين.xlsx	**جميع الموظفين**
فقط المدير المختص يمكنه تحديث جدول الإجازات وإجراء تغييرات على الملف.	تعديل (Modify)	إجازات الموظفين.xlsx	**مدير قسم الموارد البشرية فقط**
فقط أعلى مستوى إداري في الشركة يمكنه الاطلاع على هذه الخطة السرية. الموظف العادي لا يرى الملف أصلاً.	قراءة (Read)	خطة التوسع2025.pdf	**أعضاء مجلس الإدارة فقط**
فقط المدير المسؤول يمكنه تحرير وتحديث خطة التوسع.	تعديل (Modify)	خطة التوسع 2025.pdf	**مدير التطوير الاستراتيجي فقط**
الجميع يمكنهم رؤية الهيكل التنظيمي للشركة.	قراءة (Read)	الهيكل التنظيمي.pptx	**جميع الموظفين**
يمكنه تعيين الصلاحيات، حذف الملفات، أو تعديل أي شي	تحكم كامل (Full Control)	**جميع الملفات**	**مدير النظام**

مثال عن التحكم بالوصول (Access Control) (1/3)

3. اعتماداً على الجدول السابق ، ماذا يحدث عملياً عندما يحاول موظف عادي :

❖ الوصول إلى احازات الموظفين:

النتيجة: يتم منحه الوصول (Access Granted) يستطيع فتح الملف وقراءته فقط.

السبب: هو ينتمي إلى مجموعة "جميع الموظفين" التي لديها صلاحية "قراءة".

❖ الوصول إلى خطةالتوسع_2025:

النتيجة: يتم رفض الوصول (Access Denied) يظهر له رسالة مثل "ليس لديك إذن للوصول إلى هذا الملف".

السبب: هو ليس عضواً في مجموعة "أعضاء مجلس الإدارة" أو "مدير التطوير الاستراتيجي".

❖ حذف ملف الهيكل التنظيمي:

النتيجة: يتم رفض الإجراء (Action Denied) لن يجد خيار "حذف" أو إذا حاول سيظهر له خطأ.

السبب: صلاحيته هي "قراءة" فقط، وليس "تعديل" أو "تحكم كامل".

الترخيص/ التفويض (Authorization)

- ✓ عملية الحصول على تفويض للوصول إلى مستوى معين
- ✓ أي ماذا يُسمح لك أن تفعل؟
- ✓ تشمل أنواع حقوق الوصول في نظام الملف الممنوحة في عملية الترخيص :
  - **قراءة:** السماح بقراءة الملفات أو عرض محتويات المجلدات.
  - **كتابة:** السماح بالكتابة في الملفات أو بإضافة ملفات إلى المجلدات.
  - **تنفيذ:** السماح بتنفيذ برنامج ما.
  - **إضافة:** السماح بإضافة بيانات إلى الملفات أو وضع مجلدات فرعية ضمن مجلدات أخرى.
  - **حذف:** السماح بحذف ملفات أو مجلدات.

عدم التنصل
(Non-Repudiation)

- ✓ تسمح بالحماية من إنكار الاستقبال أو الإرسال في حالة الاتصال.
- ✓ تهدف إلى ضمان عدم قدرة المستخدم على إنكار أنه هو الذي قام بالتصرف، وهي ذات أهمية بالغة في بيئة الأعمال الإلكترونية والتعاقدات (التجارة الإلكترونية) (عملية التحقق والتأكد من التواقيع)
- ✓ عملية تعريف المستخدمين بطريقة لا يستطيعون معها في وقت لاحق إنكار اشتراكهم في المداولة أو العقد، وذلك عن طريق طرف ثالث موثوق به.

مثال عن عدم التنصل (Non-Repudiation) (1/2)

معاملة بنكية إلكترونية

السيناريو: تحويل أموال من أحمد إلى مريم. ناقش الحالتين:

1 . دون تطبيق نظام "عدم التنصّل".

١. **أحمد** يحوّل 5000 دولار إلى **مريم** عبر الإنترنت
٢. **بعد أسبوع**، أحمد يتصل بالبنك ويقول: "لم أقُم بهذا التحويل! شخص ما اخترق حسابي!"
٣. **البنك** لا يملك دليلاً قوياً لإثبات أن أحمد هو من قام بالتحويل
٤. **النتيجة:** خسارة مالية للبنك

مثال عن عدم التنصل (Non-Repudiation)(2/2)

معاملة بنكية إلكترونية

السيناريو: تحويل أموال من أحمد إلى مريم. ناقش الحالتين:

2 . مع تطبيق نظام "عدم التنصّل".

١. **أحمد** يحوّل 5000 دولار إلى **مريم** عبر الإنترنت هذا التحويل موثق من خلال طابع زمني وتوقيعه الكتروني

٢. **بعد أسبوع**، أحمد يتصل بالبنك ويقول: "لم أقُم بهذا التحويل! شخص ما اخترق حسابي!"

٣. **البنك** يكون لديه دليلاً قوياً لإثبات أن أحمد هو من قام بالتحويل

٤. **النتيجة:** عدم قدرة أحمد إنكار التحويل وبالنتيجة حماية أموال البنك

المثلث الأمني CIA

(Confidentiality, Integrity, Availability)

يمكننا أن نقول أن المعلومات آمنة إذا تحقق المثلث الأمني

ما الفرق بين مفهومي أمن المعلومات و الأمن السيبراني؟ (1/ 2)

- يختلفان عن بعضهما من حيث الهدف و المجال المطبق ضمنه ، لكن غالباً ما يستخدم المصطلحان لطرح نفس الفكرة .

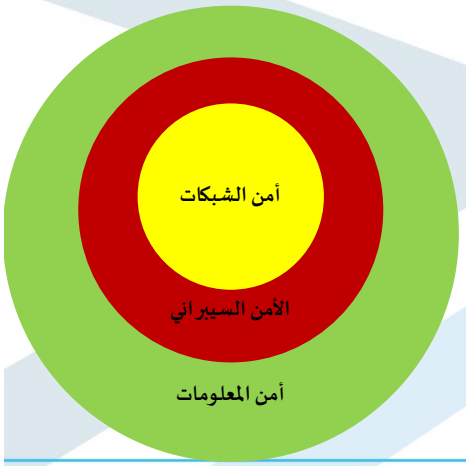
الأمن السيبراني (Cybersecurity) هو فئة من أمن المعلومات

- **يغطي أمن المعلومات:**
  - ✓ الأمن الفيزيائي
  - ✓ أمن الطرفيات
  - ✓ تشفير البيانات
  - ✓ أمن الشبكات
  - ✓ الحماية من كل التهديدات

- **يختص الأمن السيبراني :**

منع أو تخفيف الهجمات المتعلقة بالتقنيات (كالفيروسات ، البرامج الخبيثة ..)

ما الفرق بين مفهومي أمن المعلومات و الأمن السيبراني؟(2 / 2)



أمن المعلومات(Information security) :حماية المعلومات نفسها بغض النظر عن شكلها أو مكان وجودها.
(المجال الواسع)

الأمن السيبراني (Cybersecurity) :حماية الأنظمة الرقمية والشبكات من الهجمات الالكترونية
(المجال الأضيق)

مقارنة عملية بين أمن المعلومات والأمن السيبراني

السيناريو: شركة لديها بيانات عملاء حساسة

إجراءات أمن المعلومات	إجراءات الأمن السيبراني
تشفير البيانات في قواعد البيانات (سرية)	الجدران النارية لحماية الشبكة (Firewalls)
نسخ احتياطي يومي (تو افرية)	أنظمة كشف الاختراق (IDS/IPS)
التوقيعات الرقمية للتأكد من صحة المستندات (تكاملية)	حماية الطرفيات (مكافحة الفيروسات)
تدمير الأوراق السرية بآلات التقطيع (معلومات مادية)	إدارة التصحيحات الأمنية للبرامج (تحديثات)
تدريب الموظفين على عدم مناقشة معلومات سرية في الأماكن العامة (معلومات شفهية)	حماية من هجمات DOS/DDOS حجب الخدمة/حجب الخدمة الموزع

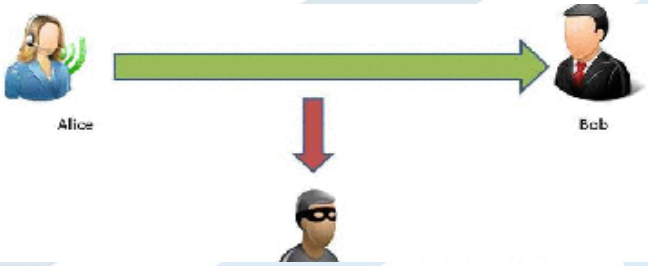
IDS (Intrusion Detection System): نظام كشف التسلل (يكشف وينبه)
IPS (Intrusion Prevention System): نظام منع التسلل (يكشف ويتصرف)

الهجمات ضد الأمن (1/4)

- الهجوم هو الاعتداء على أمن النظام ، هذا الهجوم قد يكون بـ:

1. الاعتراض (Interception):

✓ أن يستطيع المهاجم الوصول إلى جزء من مكونات النظام غير مسموح له الوصول إليه.



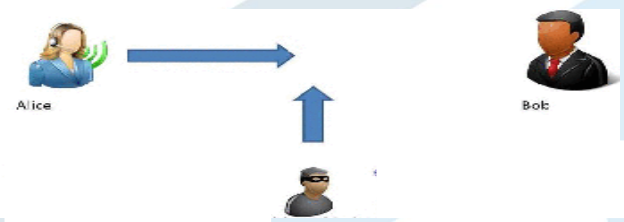
✓ مثلاً هجوم التنصت على الاتصال اللاسلكي

✓ يهدد الموثوقية (Confidentiality)

الهجمات ضد الأمن (2/4)

2. الانقطاع (Interruption):

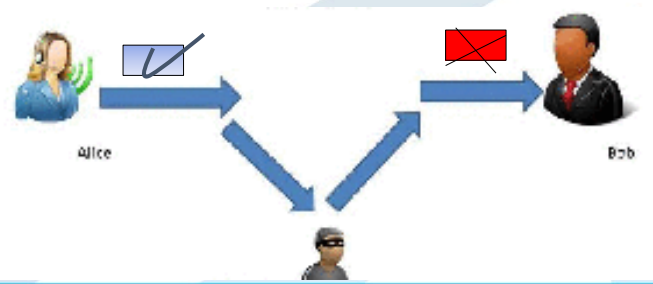
- ✓ أن يدمر المهاجم أحد مكونات النظام بحيث يصبح غير متوفر أو خارج الخدمة .
- ✓ مثلاً قطع الاتصال السلكي ، التشويش على الاتصال اللاسلكي ، إسقاط الرزم.
- ✓ يهدد التوافرية (Availability)



الهجمات ضد الأمن (3/4)

3. التعديل (Modification):

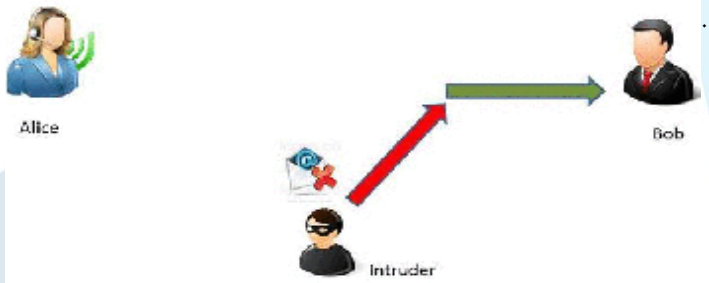
- ✓ أن يستطيع المهاجم الوصول إلى جزء من مكونات النظام غير مسموح له الوصول إليه ويعبث بهذا الجزء.
- ✓ يهدد تكاملية المعلومات (Data integrity)



الهجمات ضد الأمن (4/4)

4. التزييف (Fabrication):

- ✓ أن يحشر المهاجم معلومات مزيفة (أهداف مزيفة) ضمن النظام.
- ✓ مثلاً هجوم تزييف العنوان (IP Spoofing) .
- ✓ يهدد المصادقة (Authentication)



تصنيف كنت للهجمات ضد الأمن
Kent's classification

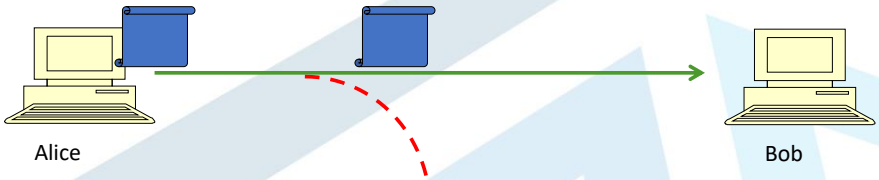
- هجمات فعّالة (Active Attacks)
  - هدفها: الحصول على المعلومات المنقولة و/مع الإضرار بالنظام
- هجمات سلبية (Passive Attacks)
  - هدفها: الحصول على المعلومات المنقولة دون الإضرار بالنظام

الهجمات السلبية (1/2)

❖ هي الهجمات التي تتضمن عملية التنصت و مراقبة الإرسال

✓يوجد نوعان:

١. الحصول على محتوى الرسالة (release of message content)

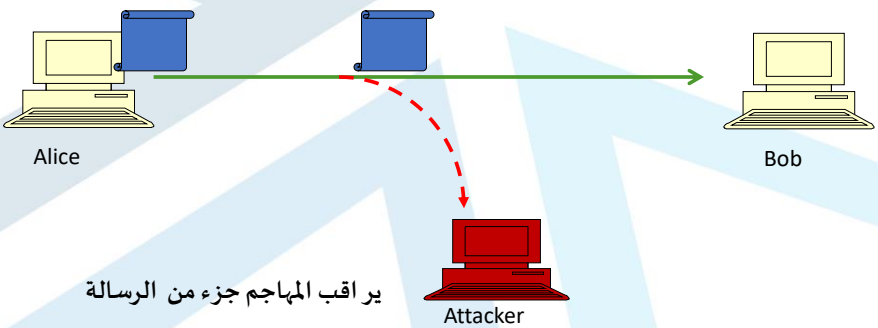


هجوم يتم فيه **الوصول غير المصرح به إلى محتوى الرسائل** السرية والاطلاع عليها

يقرأ المهاجم محتوى الرسالة

الهجمات السلبية (2/2)

٢. تحليل حركة المعلومات (Traffic analysis)



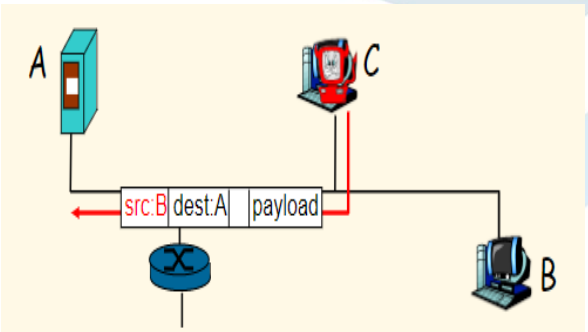
يراقب المهاجم جزء من الرسالة

الهجمات الفعالة (1/5)

❖ هي الهجمات التي تتضمن إجراء تعديلات على تدفق المعلومات أو إنشاء رسائل كاذبة

✓ تتضمن أربعة أنواع:

١.التخفي (spoofing-Masquerading) سرقة الهوية



مثال1 :انتحال عنوان الـ IP (IP Spoofing)

يرسل المهاجم رسالة بعنوان IP لعقدة أخرى

مثال : ترسل العقدة C المهاجمة إلى العقدة A على أنها العقدة B

مثال2: الاحتيال على البريد الالكتروني (e-mail Spoofing)

مهاجم

زبون

Bob@yourcompany.com

المسؤول المالي

Alice@yourcompany.com

ينشىء المهاجم بريداً الكترونياً قريباً من البريد الشرعي للمسؤول المالي

البريد الشرعي Alice@yourcompany.com

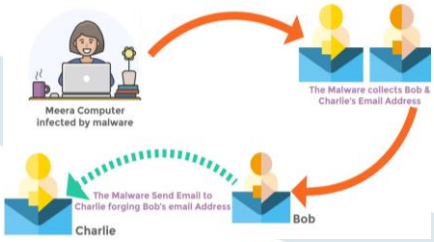
البريد المزور Alice@yourdomain.com

From: Alice@yourdomain.com
To: Bob@yourcompany.com
Subject: عاجل جداً
يترتب عليك تحويل مبلغ ٥٠٠٠٠ $ إلى الحساب الآتي ١٢١١٢١٢قبل نهاية اليوم أو تتوقف جميع المعاملات التجارية الجارية حالياً لصالحك.

سيفترض Bob أن الإيميل شرعي وسيجري التحويل

مهاجم

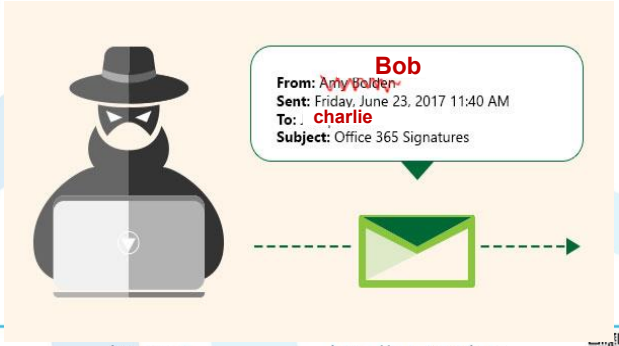
زبون



مثال 3 : الاحتيال على البريد الالكتروني (e-mail Spoofing)

- هذه الطريقة بالهجوم أعقد من المثال السابق
- هناك برامج تسمح للمهاجم أن يضع في جهة المرسل العنوان الذي يريده وليس بالضرورة العنوان الذي يُرسَل منه بشكل فعلي.

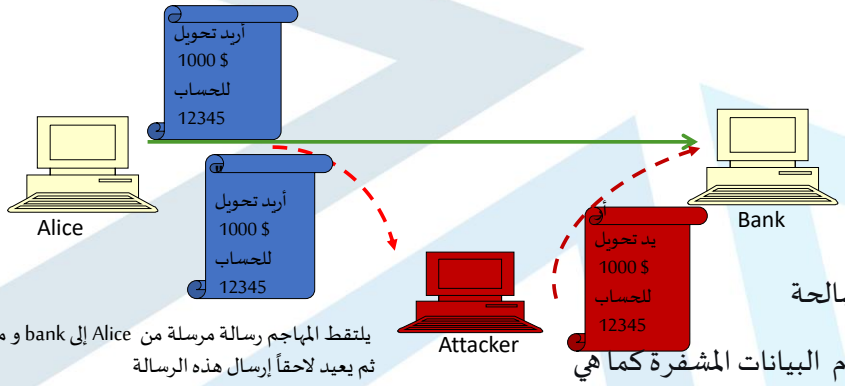
- تعرَّض حاسوب ميرا لهجوم ما
- حصل المهاجم على إيميل كل من بوب و شارلي
- يرسل المهاجم إيميل على أنه بوب إلى شارلي



الهجمات الفعالة (2/5)

٢. إعادة الإرسال (Replay Attack)

هو هجوم يعترض فيه المهاجم **بيانات صالحة** ثم يعيد **إرسالها لاحقاً** لخداع النظام للاعتقاد بأنها طلبات شرعية.



❖ يعد خطيراً لأنه:

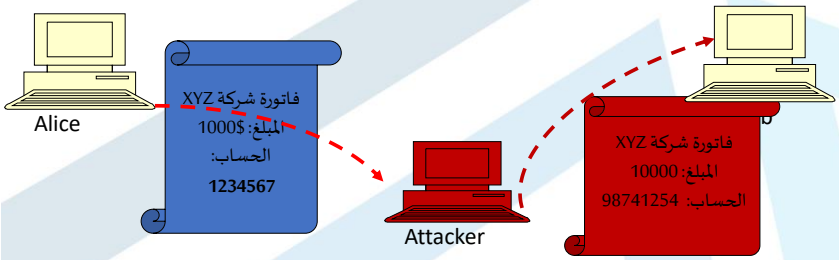
✓ صعب اكتشافه لأنه يرسل بيانات صالحة

✓ لا يحتاج إلى كسر التشفير: يستخدم البيانات المشفرة كما هي

الهجمات الفعالة (3/5)

٣. **تعديل الرسائل (Modification of message)**

هو هجوم يعترض فيه المهاجم **البيانات ويعدلها** قبل وصولها إلى المستلم، بهدف تغيير محتواها أو معناها.



يعدل المهاجم رسالة مرسلة من Alice إلى Bob

الهجمات الفعالة (4/5)

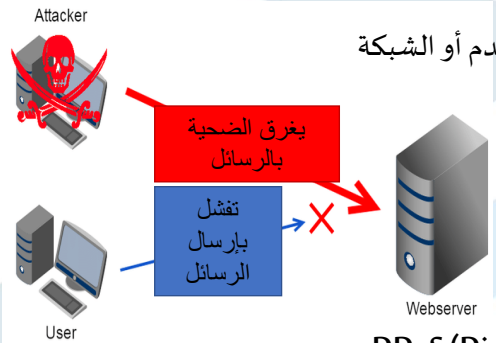
٤. **هجوم حجب الخدمة DoS (Denial of Service)**

هدفه:

جعل الخدمة غير متوفرة من خلال التحميل الزائد(overloading) للمخدم أو الشبكة عن طريق إغراق الشبكة بأعداد كبيرة من الطلبات على الموقع أو الخدمة

من خلال:

- ✓استنفاذ المصادر في الشبكة
- ✓استنفاذ عرض الحزمة
- ✓.....



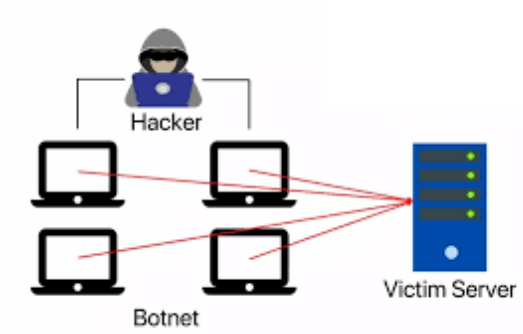
النوع الأخطر منه هو هجوم الخدمة الموزع(DDoS (Distributed Denial of Service

الهجمات الفعالة (5/5)

❖ **تنفيذ هجوم DDoS**

المرحلة1: بناء جيش الأجهزة (Botnet)

- ✓ يقوم المهاجم باختراق آلاف الأجهزة حول العالم
- ✓ يثبت برمجيات خبيثة عليها تصبح تحت سيطرته
- ✓ هذه الأجهزة تسمى "بوتات" أو "زومبي"



حجب الخدمة الموزع DDoS (Distributed Denial of Service)

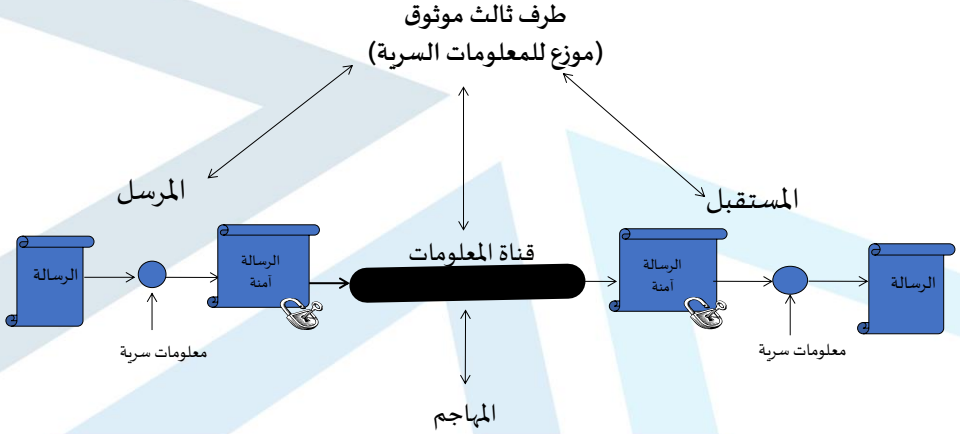
المرحلة 2: إطلاق الهجوم

- ✓ يُصدر المهاجم أمراً واحداً لجميع الأجهزة المخترقة
- ✓ تبدأ جميعها في إرسال طلبات لخدمة الهدف في نفس الوقت

المرحلة 3: إغراق الخدمة

لا يستطيع المخدم معالجة هذا الكم الهائل من الطلبات إذ يستهلك كل موارده (معالج، ذاكرة، اتصال شبكي) ويصبح غير متاح للمستخدمين الحقيقيين

نموذج أمن الشبكة
(Security Network Model)

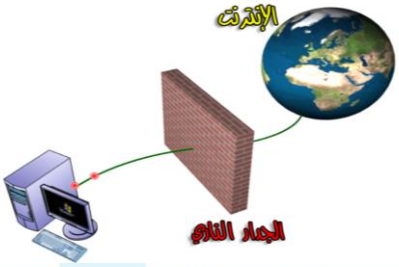


الجدران النارية (الحماية) (1/5)

(Firewalls)

❖ تستخدم لمنع الوصول غير المصرح به من خارج الشبكة إلى داخلها و من داخل الشبكة إلى خارجها.

❖ إنه مصمم ليدفع للأمام ببعض الرزم و يمنع بعضها الآخر.



الجدران النارية (الحماية) (2/5)

(Firewalls)

❖ تكون الجدران النارية إما :

➢ برمجيات (Software)

(Host-based firewall)

- هي الأرخص والأكثر انتشاراً
- سهلة التنزيل عادة تكون موجودة افتراضياً مع نظام windows .
- خاصة بحماية جهاز واحد فقط.
- لكنها قد تستهلك جزء اً كبيراً من موارد النظام
- وقد تتسبب في مشاكل مع برمجيات أخرى موجودة على الجهاز

جامعة المنارة

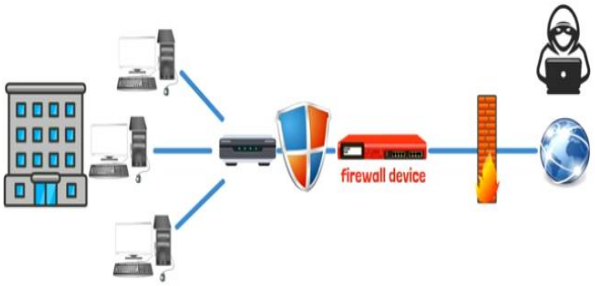
الجدران النارية (الحماية) (3/5)

(Firewalls)

❖ تكون الجدران النارية إما :

✓عتاد صلب (Hardware)

- يستخدم بشكل أكبر في الشركات والمؤسسات الكبيرة
- هو جهاز فيزيائي يوضع بين الموجهات وشبكة الانترنت



جامعة المنارة

الجدران النارية (الحماية) (3/5)

(Firewalls)

❖ تكون الجدران النارية إما :

✓عتاد صلب (Hardware)

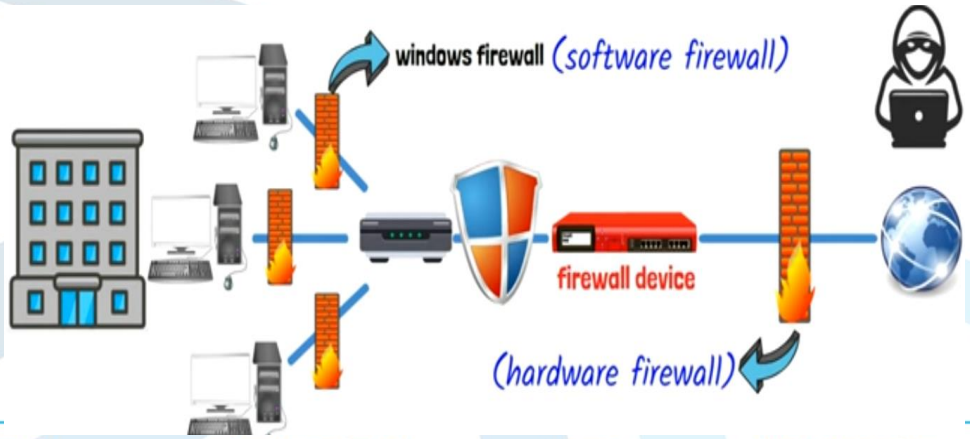
- هي مخصصة من أجل تطبيق وظائف الجدران النارية لذا لا تستهلك من موارد الأجهزة الحاسوبية
- عيبها الأساسي هو الصيانة وذلك لصعوبة تهيئتها وتحديثها بشكل صحيح

MU-EPP-FM-005 Issue date 17November2025 issue no:1 https://manara.edu.sy

الجدران النارية (الحماية) (3/5)

(Firewalls)

❖ عادة ما يستخدم النوعان السابقان معاً و هذا ما يتنج عنه ما يسمى بـ Network –based firewall

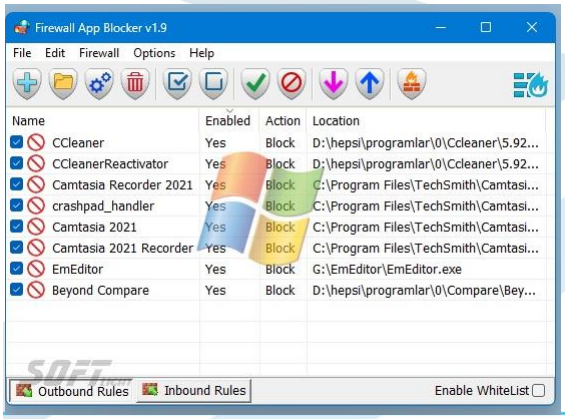


الجدران النارية (4/5)

(Firewalls)

❖ يوجد نوعان للجدران النارية حسب آلية عمله:

١. النوع الأول : يعتمد على أسماء البرامج لتحديد فيما إذا كانت مسموح لها الاتصال بالانترنت أم لا. و هو النوع الأكثر شيوعاً لبساطته.

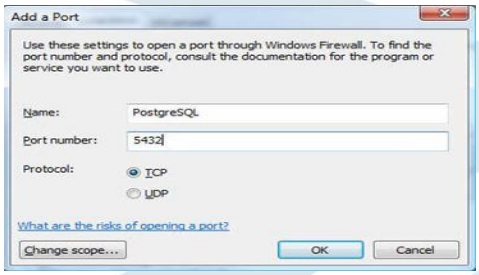


❖ مثال في شركة تمنع استخدام برامج وسائط التواصل الاجتماعي

- ✓ الموظف يحاول فتح البرنامج وليكن (Telegram)
- ✓ الجدار الناري يتفحص قائمة البرامج المسموحة
- ✓ بالنتيجة سيمنع اتصال Telegram

الجدران النارية (5/5)

(Firewalls)



❖ يوجد نوعان للجدران النارية:

٢. النوع الثاني: يعتمد على **أرقام المنافذ** ليحدد فيما إذا كنت تريد السماح بالاتصال عبر هذا المنفذ أم لا.

هذا النوع أقل شيوعاً و ذلك بسبب تعقيده.

مثال : سياسات الجدار الناري - القواعد الأساسية:

قواعد الدخول (Inbound):

- مسموح: المنفذ 80 ⟶ (HTTP)مخدم الويب
- مسموح: المنفذ 443 ⟶ HTTPSمخدم الويب
- مسموح: المنفذ 22 ⟶ (SSH)مخدم الإدارة
- ممنوع: جميع المنافذ الأخرى

قواعد الخروج (Outbound):

- مسموح: المنفذ 80 ⟵ (HTTP) التصفح
- مسموح: المنفذ 443⟵(HTTPS)التصفح الآمن
- مسموح: المنفذ 53 ⟵ (DNS) تحليل أسماء النطاقات
- ممنوع: المنفذ 25 ⟵ (SMTP) منع إرسال بريد غير مصرح