أمن نظم المعلومات

جلسة العملي الأولى

مدرسة المقرر

د. بشرى علي معلا

التمرين الأول

أجب بـ صح أو خطأ مع التعليل في كلا الحالتين :

1. **تعد برامج الجدران النارية أحد أهم أنواع التحكم الإداري بأمن المعلومات.**

خطأ.بل هو أحد أنواع التحكم المنطقي لأن هذا النوع من التحكم يشمل جميع برمجيات التحكم بالوصول

2. **تو افرية المعطيات هي متطلب الأمن الذي يسمح بضمان وصول البيانات كما أرسلت.**

خطأ. لأن متطلب التوافرية يضمن استمرار الحصول على الخدمة ولا يتعلق بضمان عدم تعديل البيانات

3. **هجوم التعديل هو هجوم إيجابي.**

صح. لأنه يتسبب بأذى للنظام و ليس فقط الحصول على المعلومات.

تابع التمرين الأول

4. يمكن أن يقوم المهاجم بهجوم التعديل عن طريق بإنشاء رسائل جديدة و إرسالها ضمن الشبكة

خطأ. لأن هجوم التعديل هو إجراء تغيير على رسائل موجودة أصلاً و ليس إنشاء رسائل جديدة.

5. **هجوم إعادة الارسال في شبكة مكونة من عقد محدودة الطاقة ينتهك متطلب التو افرية.**

صح. لأن هجوم إعادة الارسال يتسبب بزيادة عمليات الارسال و الاستقبال و بالتالي استهلاك زائد للطاقة و هذا بدوره يسبب إنهاء عمر العقد و خروج الشبكة عن العمل و بالتالي انتهاك متطلب التوافرية.

6. **في تطبيقات التحويلات المصرفية، يعد ضمان متطلب عدم التنصل أمراً غاية في الأهمية.**

صح. لأن في التحويلات المصرفية يضمن متطلب عدم التنصل عدم قدرة الموظف المعني الذي أجرى عملية التحويل من التنصل مما قام به.

التمرين الثاني

اختر الإجابة الصحيحة:

1. يمثل قيام المهاجم بإنشاء رسائل جديدة وإرسالها ضمن الشبكة هجوماً هو هجوم :

A . التعديل B.الانقطاع C. الاعتراض D. التزييف

2.يهدد هجوم الانقطاع متطلب:

A . التكاملية B. الموثوقية C. التوافرية D. عدم التنصل

3.يهدد هجوم التعديل متطلب:

A . التكاملية B. الموثوقية C. التوافرية D. عدم التنصل

حل التمرين الثاني

اختر الإجابة الصحيحة:

1. يمثل قيام المهاجم بإنشاء رسائل جديدة و إرسالها ضمن الشبكة هجوماً هو :

A . التعديل　　B.الانقطاع　　C. الاعتراض　　**D. التزييف**

2.يهدد هجوم الانقطاع متطلب:

A . التكاملية　　B. الموثوقية　　**C. التو افرية**　　D. عدم التنصل

3.يهدد هجوم التعديل متطلب:

A . التكاملية　　B. الموثوقية　　C. التوافرية　　D. عدم التنصل

التمرين الثالث

صنف كل مما يأتي حسب فئة التحكم بأمن المعلومات

1. نسي موظف الحسابات حاسبه قيد العمل و خرج دون أن يغلق باب مكتبه. فدخل أحد الموظفين العابثين وعدل جدول المكافآت. **(إداري)**

2. ثبت سامي حاسبه المحمول على الطاولة باستخدام قفل الحاسب. **(فيزيائي)**

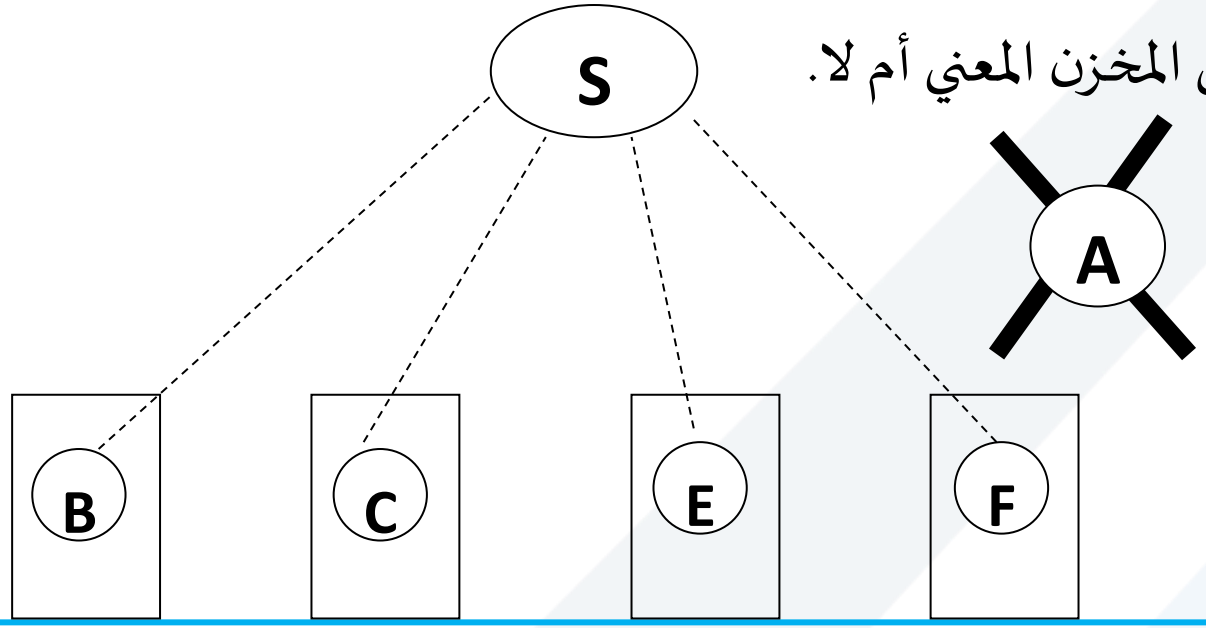
3. تستخدم شركة كاشفات الحركة لرصد التحركات بعد انتهاء الدوام. **(فيزيائي)**

4. يحرص يوسف على تحديث برنامج مضاد الفيروسات الذي يستخدمه . **(منطقي)**

التمرين الرابع

إذا كان لدينا شبكة مكونة من عقد حساسات لاسلكية قادرة على قياس درجة الحرارة . هذه الشبكة موزعة ضمن بناء مكون من أربعة مخازن .الهدف الأساسي لهذه الشبكة هوالإنذار ضد الحريق و يكون ذلك عن طريق مراقبة درجة الحرارة و إرسال رسالة تتضمن درجة الحرارة كل 5 دقائق لتصل الرسائل إلى مركز المراقبة S الذي يقارن درجات الحرارة الواصلة إليه مع العتبة $T_{thershold} = 35^{o}C$

لتحديد وجوب إطلاق إنذارالحريق و تشغيل رذاذ إطفاء الحريق في المخزن المعني أم لا.



إذا كان لدينا العقدة المهاجمة A مجهزة بمجال تغطية يجعلها قادرة على الاستماع إلى الرسائل المتبادلة بين العقد B,C,E,F, و بين مركزالمراقبة S، و المطلوب:

اتصال لاسلكي

تابع للتمرين الرابع

1. في البداية قامت العقدة A بالاستماع إلى الرسائل المرسلة و لم تقم باي إجراء. ماذا نسمي هذا الهجوم؟ و ما نوعه و لماذا؟
2. في حال أرسلت العقدة A الرسالة $\{ID_C, ID_S, T = 45^O C\}$ ماذا نسمي هذا الهجوم؟ و ما نوعه و لماذا؟
3. في حال أرسلت العقدة C رسالة تتضمن $\{ID_C, ID_S, T = 15^O C\}$

وقامت العقدة A بمقاطعة الرسالة و بإعادة إرسال الرسالة كالآتي: $\{ID_C, ID_S, T = 50^o c\}$

ما اسم هذا الهجوم ؟ و ما المتطلب الذي انتهك و لماذا؟

4. نشب حريق ضمن المخزن E، تحسس الحساس الحريق فأرسلت الرسالة الآتية: $\{ID_E, ID_S, T = 40^O C\}$

لكن العقدة A شوشت عليها مما أعاق وصولها إلى المركز S، و بالنتيجة لم يتخذ المركز S أي إجراء. ماذا نسمي هذا الهجوم؟ و ما هو متطلب الأمن الذي انتهك و لماذا ؟

حل التمرين الرابع

1. في البداية قامت العقدة A بالاستماع إلى الرسائل المرسلة و لم تقم بأي إجراء. ماذا نسمي هذا الهجوم؟ و ما نوعه و لماذا؟

هجوم التنصت(الحصول على محتوى الرسالة)،نوعه: هجوم سلبي لأنها حصلت على المعلومات المنقولة دون الإضرار بالنظام .

2. في حال قامت العقدة A بإرسال الرسالة $\{ID_C, ID_S, T = 45^O C\}$ ماذ نسمي هذا الهجوم؟ و ما نوعه و لماذا؟

هجوم التخفي (سرقة الهوية)، نوعه: هجوم فعال لأن تسبب الاضرار بالنظام من خلال إرسال رسالة مزيفة تؤدي إلى اتخاذ قرار خاطئ مثل تشغيل الرذاذ.

حل التمرين الرابع

3. في حال أرسلت العقدة C رسالة تتضمن $\{ID_C, ID_S, T = 15^o C\}$

و قاطعت العقدة A الرسالة و أعادت إرسال الرسالة كالآتي: $\{ID_C, ID_S, T = 50^o c\}$

ما اسم هذا الهجوم ؟ و ما المتطلب الذي انتهك و لماذا؟

هجوم التعديل. المتطلب هو التكاملية. لأن المهاجم عدل على قيمة درجة الحرارة المرسلة

4.نشب حريق ضمن المخزن E،تحسس الحساس الحريق و فأرسلت الرسالة الآتية: $\{ID_E, ID_S, T = 40^o C\}$

لكن العقدة A شوشت عليها مما أعاق وصولها إلى المركز S، و بالنتيجة لم يتخذ المركز S أي إجراء. ماذا نسمي هذا الهجوم؟ و ما هو متطلب الأمن الذي انتهك و لماذا ؟

هجوم حجب الخدمة(التشويش). متطلب الأمن هو التوافرية لأنه منع الوصول إلى الخدمة التي يقدمها المركز وهي تشغيل الرذاذ و إطفاء الحريق

التمرين الخامس

بفرض لدينا شبكة حساسات لاسلكية متجانسة مكونة من العقد محدودة الطاقة ومركز معالجة رئيسي يدعى S متصل مع مركز للإطفاء .الهدف من هذه الشبكة هو مراقبة بستان مشجر للإنذار عن الحريق . إذا علمت أنه هناك عقدة مهاجمة ضمن الشبكة. والمطلوب:

1. إذا توضعت هذه العقدة في موقع سمح لها بمنع وصول أية رسالة موجهة إلى مركز المعالجة الرئيسي للشبكة. ما اسم هذا الهجوم مع التعليل؟ ما نوعه مع التعليل؟

2. أرسلت هذه العقدة رسالة إنذار كاذبة وصلت إلى مركز المعالجة، فأصدر المركز أمراً للإطفاء للتوجه إلى مكان الحريق. ما اسم هذا الهجوم مع التعليل؟ ما نوعه مع التعليل؟

3. استقبلت هذه العقدة رسالة إنذار عن الحريق من إحدى عقد الشبكة في لحظة t1 . فقامت بتمرير هذه الرسالة بشكل طبيعي و احتفظت بنسخة منها. ثم قامت بإرسال هذه الرسالة في اللحظات (t2,t3,t4,t5). ماذا يسمى هذا الهجوم مع التعليل؟ ما نوعه مع التعليل؟

حل التمرين الخامس(1/2)

1. إذا توضعت هذه العقدة في موقع سمح لها بمنع وصول أية رسالة موجهة إلى مركز المعالجة الرئيسي للشبكة. ما اسم هذا الهجوم مع التعليل؟ ما نوعه مع التعليل؟

هجوم حجب الخدمة (DOS). التعليل: لأنه منع وصول الرسائل إلى المركزو بالنتيجة حجب خدمة الإنذارمن الحريق التي تقدمها هذه الشبكة

نوعه: هجوم إيجابي . التعليل : لأنه أدى إلى الإضرار بالنظام.

2. أرسلت هذه العقدة رسالة إنذار كاذبة وصلت إلى مركز المعالجة، فأصدر المركز أمراً للإطفاء للتوجه إلى مكان الحريق. ما اسم هذا الهجوم مع التعليل؟ ما نوعه مع التعليل؟

هجوم التزييف التعليل: لأن العقدة المهاجمة أنشأت رسالة جديدة و أرسلتها.

نوعه: هجوم إيجابي . التعليل : لأنه أدى إلى الإضرار بالنظام.

حل التمرين الخامس(2/2)

3. استقبلت هذه العقدة رسالة إنذار عن الحريق من إحدى عقد الشبكة في لحظة t1 . فمررت هذه الرسالة بشكل طبيعي و احتفظت بنسخة منها. ثم أرسلت هذه الرسالة بعد ذلك في اللحظات المتتالية (t2,t3,t4,t5). ماذا يسمى هذا الهجوم مع التعليل؟ ما نوعه مع التعليل؟

هجوم إعادة الإرسال التعليل: لأن العقدة المهاجمة أعادت إرسال رسالة عدة مرات سبق لها وأن أرسلت ضمن الشبكة.
نوعه: هجوم إيجابي . التعليل : لأنه أدى إلى الإضرار بالنظام لأن العقد محدودة الطاقة.

نهاية الجلسة الأولى