الأكاديمية العربية الدولية
Arab International Academy

شبكات الحاسب 2

Introduction to databases

م. خليل المحمد

كلية العلوم – بكالوريوس تقنية المعلومات

الأكاديمية العربية الدولية
Arab International Academy

المحاور

1. التطبيقات العملية لنماذج الشبكات
2. تصميم الشبكات المحلية واللاسلكية
3. التوجيه العملي للبيانات
4. أمن الشبكات – الجزء المتقدم
5. خدمات الشبكة الأساسية
6. إدارة الشبكات باستخدام أدوات متقدمة

المخرجات المتوقعة من المحاضرة

المخرجات المتوقعة من هذه المحاضرة يمكن تلخيصها في النقاط التالية:

1. فهم وتحليل نموذج OSI عمليًا
2. تحديد أسباب الأعطال في طبقات الشبكة المختلفة
3. مقارنة بين نماذج OSI وTCP/IP
4. تصميم شبكة محلية LAN وشبكة لاسلكية WLAN
5. تنفيذ وإدارة التوجيه في الشبكات
6. تطبيق إجراءات أمنية متقدمة على الشبكات
7. إعداد وتشغيل خدمات الشبكة الأساسية

1. التطبيقات العملية لنماذج الشبكات

تعريف نماذج الشبكات وأهميتها:

نموذج الشبكات هو إطار يساعد في فهم كيفية انتقال البيانات بين الأجهزة عبر الشبكة. النموذجان الأشهر هما OSIوTCP/IP، حيث يسهلان تصميم الشبكات وتوحيد البروتوكولات المستخدمة بين مختلف الأجهزة.

دور النماذج في التطبيق العملي:

تُستخدم هذه النماذج لتشخيص المشكلات التقنية عبر تحديد الطبقة التي يحدث فيها العطل بدقة، مما يسرع عملية الحل. كما تُساعد في تطوير الشبكات وصيانتها بشكل فعال خاصة في الشبكات الكبيرة والمعقدة.

أدوات التحليل:

مثل أداة Wireshark التي تتيح مراقبة حركة الحزم أثناء انتقالها، مع عرض تفاصيل كل طبقة، وهذا يمكّن مهندسي الشبكات من فحص البيانات بدقة ومعرفة أين تكمن المشكلة.

1. التطبيقات العملية لنماذج الشبكات

1.1 تحليل طبقات نموذج OSI عمليًا باستخدام أدوات تحليل الحزم

مقدمة لنموذج OSI:

نموذج OSI هو إطار معياري يتكون من سبع طبقات تساعد على فهم كيفية انتقال البيانات عبر الشبكة من المرسل إلى المستقبل.

الطبقات ومهامها: تبدأ الطبقة الفيزيائية بنقل الإشارات الكهربائية أو الضوئية، ثم تأتي طبقة ارتباط البيانات التي تنظم نقل البيانات بين الأجهزة على نفس الشبكة المحلية.

أدوات تحليل الحزم: تُستخدم أدوات مثل Wireshark لتحليل حركة البيانات وفهم كيفية عمل كل طبقة من طبقات OSI.

مراقبة الحزم:

Wireshark يعرض تفاصيل الحزم ويتيح رؤية العناوين والبروتوكولات المستخدمة في كل طبقة، مما يسهل فهم آلية عمل الشبكة وتحليل المشكلات.

1. التطبيقات العملية لنماذج الشبكات

1.1 تحليل طبقات نموذج OSI عمليًا باستخدام أدوات تحليل الحزم

تفاصيل الطبقات في Wireshark:

يمكن رؤية عناوين MAC في طبقة ارتباط البيانات، وعناوين IP في طبقة الشبكة، بالإضافة إلى بروتوكولات النقل مثل TCP وUDP

رؤية بيانات التطبيقات:

في الطبقة العليا تظهر البيانات المتعلقة ببروتوكولات التطبيقات مثل HTTP وDNS، التي تتحكم في خدمات الشبكة.

أهمية التحليل العملي:

فهم كيفية تغليف البيانات Encapsulation وفك تغليفها Decapsulation من خلال كل طبقة يساعد في تشخيص الأعطال بدقة.

الفوائد:

يساعد التحليل في تحسين أداء الشبكة، ضمان الأمان، وتسهيل صيانة الشبكات الكبيرة.

1. التطبيقات العملية لنماذج الشبكات

1.2 تتبع انتقال البيانات بين الطبقات Data Encapsulation/Decapsulation

مفهوم التغليف Encapsulation :

عند إرسال البيانات، تضيف كل طبقة في نموذج OSIرأسًا Header خاصًا بها يحتوي معلومات التحكم، مما يُسهل معالجة البيانات عبر الشبكة.

أهمية التغليف:

التغليف يضمن أن البيانات تنتقل بشكل صحيح وآمن من المصدر إلى الوجهة، حيث تضاف بيانات مثل عناوين IPوأرقام المنافذ في طبقات مختلفة.

مراحل التغليف:

تبدأ البيانات من طبقة التطبيقات ثم تنتقل للأسفل لتُغلف في كل طبقة حتى تصل إلى الطبقة الفيزيائية.

1. التطبيقات العملية لنماذج الشبكات

1.2 تتبع انتقال البيانات بين الطبقات Data Encapsulation/Decapsulation

عملية فك التغليف Decapsulation :

عند استلام البيانات، تتم إزالة رؤوس التحكم طبقة طبقة لاستعادة البيانات الأصلية في طبقة التطبيقات.

دور أدوات التحليل:

تسمح أدوات مثل Wireshark بمراقبة هذه العمليات وعرض كل خطوة من التغليف والفك، مما يساعد المهندسين في تتبع مشاكل النقل.

الأثر العملي:

فهم عملية التغليف والفك يساعد في تحسين جودة نقل البيانات وضمان استقرار الشبكة.

1. التطبيقات العملية لنماذج الشبكات

1.3 حالات دراسية لأعطال في كل طبقة:

الطبقة الفيزيائية:

مشاكل في الكابلات أو التوصيلات تسبب انقطاعًا أو ضعفًا في الإشارة، مما يؤدي لتوقف الاتصال أو تقطعه.

طبقة ارتباط البيانات:

تصادم الحزم أو أخطاء في عناوين MAC تؤدي لفشل الاتصال بين الأجهزة ضمن نفس الشبكة.

أمثلة عملية:

كابل تالف تسبب في انقطاع شبكة كاملة، أو إعداد VLAN خاطئ منع تواصل الأجهزة.

1. التطبيقات العملية لنماذج الشبكات

1.3 حالات دراسية لأعطال في كل طبقة

طبقة الشبكة: أخطاء في تكوين عناوين IP أو جداول التوجيه تمنع وصول البيانات لوجهتها.

طبقة النقل: مشاكل في بروتوكولات TCP أو UDP قد تؤدي لفقدان الاتصال أو بطء في نقل البيانات.

طبقة التطبيقات: أخطاء في بروتوكولات مثل HTTP أو DNSتسبب فشل الخدمات وتأخر تحميل المواقع.

أهمية التشخيص: فهم الأعطال يمكن المهندسين من معالجتها بسرعة وتحسين أداء الشبكة.

1. التطبيقات العملية لنماذج الشبكات

1.4 مقارنة بين OSI و TCP/IP في بيئة حقيقية

نموذج OSI:

يتكون من 7 طبقات، يقدم تقسيمًا دقيقًا للوظائف الشبكية، ويُستخدم كمرجع تعليمي لفهم الشبكات.

نموذج TCP/IP:

يتألف من 4 طبقات، عملي أكثر ويُستخدم فعليًا في معظم الشبكات، خاصة الإنترنت.

الفرق الأساسي:

TCP/IP يدمج بعض الطبقات من OSIلتبسيط النموذج، مما يجعله أكثر كفاءة في التطبيقات الواقعية.

1. التطبيقات العملية لنماذج الشبكات

1.4 مقارنة بين OSI وTCP/IP في بيئة حقيقية

تطبيقات عملية:

في بيئة حقيقية، نستخدم TCP/IP لتوجيه البيانات، بينما OSI يساعد في تحليل وفهم حركة البيانات بالتفصيل.

أدوات التحليل:

Wireshark يعرض طبقات TCP/IP أثناء التشغيل، ويمكننا ربطها بنموذج OSI لفهم أدق.

أهمية المقارنة:

معرفة الفروق تساعد في تشخيص المشاكل وفهم آلية عمل الشبكة بشكل متكامل.

1. التطبيقات العملية لنماذج الشبكات

1.5 تحليل اتصالات باستخدام Wireshark (HTTP, DNS, TCP, UDP)

Wireshark في التحليل: تتيح الأداة التقاط وتحليل حركة الشبكة التفصيلية، مما يساعد على فهم البروتوكولات المختلفة.

تحليل HTTP: رصد طلبات واستجابات صفحات الويب، مما يساعد في فهم تحميل المواقع وتفاعل المستخدم.

تحليل DNS: مراقبة استعلامات ترجمة النطاقات إلى عناوين IP، وهي خطوة أساسية في اتصال الإنترنت.

بروتوكولات TCP و UDP: تحديد طبيعة الاتصال بين الأجهزة، حيث TCP يوفر اتصالًا موثوقًا، و UDP للاتصالات السريعة غير المضمونة.

2. تصميم الشبكات المحلية واللاسلكية

2.1 خطوات تصميم شبكة LAN لمؤسسة صغيرة أو متوسطة

تحديد متطلبات المؤسسة: تحديد عدد المستخدمين، نوع الأجهزة، والخدمات المطلوبة مثل الإنترنت، مشاركة الملفات والطباعة.

تقييم البنية التحتية: دراسة المساحات، توصيلات الكابلات، واحتياجات التوسع المستقبلي.

اختيار نوع الشبكة: تحديد ما إذا كانت شبكة سلكية، لاسلكية، أو مزيج بينهما حسب طبيعة العمل.

تصميم الهيكل التنظيمي: توزيع الأجهزة والمعدات بطريقة تقلل الازدحام وتزيد من سرعة الاتصال.

تخطيط عناوين IP: تخصيص عناوين IP وتحديد شبكات فرعية Subnetting لتحسين الأداء والتنظيم.

توثيق التصميم: إعداد خرائط ومخططات تفصيلية تشمل توصيلات الأجهزة والعناوين المستخدمة.

2. تصميم الشبكات المحلية واللاسلكية

2.2 اختيار المكونات Switches، Routers، Access Points

المبدلات Switches : اختيار عدد المنافذ وسرعة النقل المناسبة، مع تفضيل المبدلات المدارة للمرونة في الإعدادات.

أجهزة التوجيه Routers : اختيار أجهزة ذات قدرة معالجة عالية تدعم البروتوكولات المطلوبة وأمان الشبكة.

نقاط الوصول اللاسلكية Access Points : تحديد عددها بناءً على حجم التغطية وعدد المستخدمين المتوقعين.

الوسائط والكابلات: اختيار الكابلات مثل Cat5e أو Cat6 لضمان سرعة واستقرار الاتصال.

التوافق والموثوقية:

التأكد من توافق جميع المكونات مع بعضها وضمان جودة الأداء.

2. تصميم الشبكات المحلية واللاسلكية

2.3 تخطيط شبكة WLAN ومناطق التغطية

دراسة البيئة المادية: معرفة توزيع المستخدمين والعوائق مثل الجدران أو الأجهزة التي تؤثر على انتشار الإشارة.

تحديد عدد نقاط الوصول: توزيع نقاط الوصول لتغطية كاملة مع تجنب التداخل بين الإشارات.

اختيار قنوات التشغيل: تعيين قنوات مختلفة لنقاط الوصول القريبة لتقليل التداخل.

تقدير سعة المستخدمين: تحديد عدد المستخدمين المتوقع لكل نقطة وصول لتوزيع الحمل بشكل مناسب.

التشفير والأمان: تطبيق تشفير WPA3 وسياسات وصول صارمة لضمان أمن الشبكة اللاسلكية.

2. تصميم الشبكات المحلية واللاسلكية

2.4 اعتبارات الأداء والأمان في التصميم

تحسين الأداء: استخدام مكونات ذات جودة عالية، تقسيم الشبكة إلى طبقات Access, Distribution, Core .

إدارة حركة البيانات: استخدام VLANs و QoS لضمان أولوية حركة البيانات المهمة مثل الصوت والفيديو.

الأمان: تطبيق جدران حماية، أنظمة كشف التسلل، تشفير البيانات اللاسلكية.

التحديث والصيانة: تحديث الأجهزة والبرمجيات بانتظام لسد الثغرات وتحسين الأداء.

التخطيط للتوسعة: تصميم الشبكة مع إمكانية التوسع المستقبلي بسهولة دون تأثير على الأداء.

2. تصميم الشبكات المحلية واللاسلكية

2.5 رسم خرائط الشبكة باستخدام أدوات مثل Draw.io

أهمية رسم الخرائط: توثيق البنية التحتية للشبكة بطريقة مرئية تسهل الفهم والإدارة.

أدوات الرسم: Draw.io أداة مجانية وسهلة الاستخدام تدعم رموز الشبكات المختلفة.

طريقة الرسم: تمثيل الأجهزة Switches, Routers, Access Points باستخدام الرموز المناسبة وربطها بخطوط توضح الاتصالات.

التسمية: إضافة أسماء الأجهزة، عناوين IP، وأرقام المنافذ لتسهيل التعرف عليها.

التحديث المستمر: مراجعة وتحديث الخرائط بانتظام لتتوافق مع تغييرات الشبكة.

2. تصميم الشبكات المحلية واللاسلكية

2.6 دراسة حالة: تصميم شبكة مكتبية مع WLAN

المتطلبات: تصميم شبكة لمكتب يضم 50 موظفًا مع توفير شبكة سلكية ولاسلكية.

اختيار الأجهزة: استخدام مبدلات Gigabit Routers متقدمة، ونقاط وصول لاسلكية تغطي كل مناطق العمل.

توزيع نقاط الوصول: تحديد مواقع استراتيجية لضمان تغطية كاملة مع تقليل التداخل.

الأمان: تطبيق تشفير WPA3، جدار ناري مركزي، وأنظمة مراقبة الشبكة.

التوثيق والاختبار: إعداد خرائط الشبكة باستخدام Draw.io واختبار الأداء قبل التشغيل.

الأكاديمية العربية الدولية
Arab International Academy

اسئلة

السؤال 1: ما هو دور نموذج OSI في تشخيص أعطال الشبكة؟

السؤال 2: كيف تساعد أدوات مثل Wireshark في تحليل حركة البيانات داخل الشبكة؟

السؤال 3: ما هي الخطوات الأساسية لتصميم شبكة LAN لمؤسسة صغيرة أو متوسطة؟

السؤال 4: ما أهمية تخطيط شبكة WLAN بشكل صحيح؟

السؤال 5: لماذا يعتبر رسم خرائط الشبكة باستخدام أدوات مثل Draw.io مهماً في إدارة الشبكات؟

الأكاديمية العربية الدولية
Arab International Academy

الأجوبة

الجواب 1: يساعد نموذج OSIفي تحديد الطبقة التي يقع بها العطل بدقة، مما يسهل على مهندسي الشبكات تشخيص المشكلة وإيجاد الحل المناسب بسرعة.

الجواب2 : تتيح Wiresharkمراقبة الحزم التي تنتقل عبر الشبكة وعرض تفاصيل كل طبقة في نموذج OSI، مما يمكّن المهندسين من فهم كيفية تغليف البيانات وفك تغليفها وتشخيص المشكلات.

الجواب3 : تبدأ بتحديد متطلبات المؤسسة وعدد المستخدمين، تقييم البنية التحتية، اختيار نوع الشبكة (سلكية أو لاسلكية)، تصميم الهيكل التنظيمي، تخطيط عناوين IP، ثم توثيق التصميم.

الجواب4 : يضمن تخطيط شبكة WLANبشكل صحيح توزيع نقاط الوصول لتغطية كاملة بدون تداخل، وتحقيق أداء مستقر، بالإضافة إلى تطبيق تشفير وأمان قوي لحماية الشبكة اللاسلكية.

الجواب5 : يساعد رسم الخرائط في توثيق مكونات الشبكة وعلاقاتها بشكل مرئي، مما يسهل إدارة الشبكة، صيانتها، وتخطيط التوسعات المستقبلية بفعالية.

3. التوجيه العملي للبيانات

3.1 إعداد التوجيه الثابت يدويًا Static Routing Configuration

تعريف التوجيه الثابت: التوجيه الثابت هو تكوين يدوي لمسارات الشبكة في أجهزة التوجيه، حيث يحدد المسؤول بشكل صريح مسارات الحزم إلى الشبكات الوجهة.

أهمية التوجيه الثابت: مناسب للشبكات الصغيرة أو التي لا تتغير كثيرًا، ويمنح تحكمًا دقيقًا في مسار البيانات.

طريقة الإعداد: يتم إدخال أوامر التوجيه في الراوتر مثل تحديد الشبكة الوجهة وقناع الشبكة وعنوان الخطوة التالية أو واجهة الخروج.

مزايا وعيوب:

التوجيه الثابت بسيط وموثوق، لكنه غير عملي في الشبكات الكبيرة لأنه يتطلب تحديثات يدوية مستمرة.

3. التوجيه العملي للبيانات

3.2 إعداد بروتوكولات التوجيه الديناميكي (OSPF كمثال)

مفهوم التوجيه الديناميكي: بروتوكولات التوجيه الديناميكي تسمح لأجهزة التوجيه بتبادل المعلومات وتحديث جداول التوجيه تلقائيًا عند حدوث تغييرات.

لماذا OSPF؟ OSPF هو بروتوكول توجيه داخلي يعتمد على خوارزمية الحالة الرابطية، سريع الاستجابة ويدعم تقسيم الشبكة إلى مناطق.

خطوات الإعداد: تمكين OSPF، تعريف الشبكات المشاركة، وتحديد المناطق Areas في أجهزة التوجيه.

مزايا OSPF: تحديث سريع للمسارات، دعم التوسع، وتحسين توزيع حركة المرور عبر الشبكة.

3. التوجيه العملي للبيانات

3.3 فهم جداول التوجيه وتحليلها

ما هي جداول التوجيه؟

جداول التوجيه هي قواعد تحدد أفضل المسارات التي تسلكها الحزم للوصول إلى وجهتها.

محتويات الجدول: تشمل عناوين الشبكات الوجهة، القناع الشبكي، عنوان الخطوة التالية، وواجهة الخروج.

مصادر بناء الجدول: إما عبر التوجيه الثابت أو بروتوكولات التوجيه الديناميكي.

أهمية التحليل:

فهم جداول التوجيه يساعد في تشخيص مشاكل الشبكة وتحسين الأداء.

3. التوجيه العملي للبيانات

3.4 مقارنة بين بروتوكولات RIP و OSPF وBGP

RIP : بروتوكول توجيه داخلي بسيط يعتمد على عدد القفزات، مناسب للشبكات الصغيرة، لكن محدود في الحجم والمرونة.

OSPF : بروتوكول ديناميكي داخلي يعتمد على خوارزمية الحالة الرابطية، يدعم الشبكات المتوسطة والكبيرة بفعالية.

BGP : بروتوكول توجيه خارجي يستخدم لتبادل المعلومات بين أنظمة الشبكات المختلفة، مثالي للإنترنت.

مقارنة سريعة: RIP بسيط وبطيء، OSPF سريع ومعقد، BGP معقد ويستخدم للشبكات الكبرى.

3. التوجيه العملي للبيانات

3.4 مقارنة بين بروتوكولات RIP و OSPF وBGP

المقارنة	RIP	OSPF	BGP
النوع	بروتوكول توجيه داخلي بسيط	بروتوكول توجيه داخلي متقدم	بروتوكول توجيه خارجي
المعيار المستخدم	عدد القفزات(Hop Count)	تكلفة الربط(Link Cost)	السياسات(Policies)
الأداء	بطيء نسبيًا	سريع ودقيق	معقد ويعتمد على السياسة
التكوين	بسيط وسهل	متوسط التعقيد	معقد ويتطلب خبرة
الدعم والموارد	خفيف على الموارد	متوسط استهلاك الموارد	عالي الاستهلاك، يحتاج موارد قوية
الأمان	لا يحتوي على خصائص أمان متقدمة	يدعم المصادقة	حساس جدًا للضبط الخاطئ وقد يؤثر على الإنترنت
الملاءمة	شبكات صغيرة	شبكات متوسطة	شبكات كبيرة، بين مزودي خدمات
الانتشار	نادر في الاستخدامات الحديثة	شائع في المؤسسات	أساسي في البنية التحتية للإنترنت
المرونة	محدودة	مرن وديناميكي	عالي جدًا وقابل للتخصيص
التوصية	للشبكات التعليمية أو البسيطة	للشبكات المؤسسية	للبنية التحتية الواسعة بين منظمات أو مزودين

3. التوجيه العملي للبيانات

3.5 استخدام Packet Tracer لمحاكاة بيئة توجيه متكاملة

أهمية Packet Tracer:

أداة محاكاة من Cisco تمكن المهندسين والطلاب من تصميم وتجربة شبكات افتراضية قبل التنفيذ الفعلي.

خطوات المحاكاة: إنشاء شبكة افتراضية، توصيل الأجهزة، إعداد عناوين IP، وتكوين التوجيه الثابت والديناميكي.

التحقق والاختبار: استخدام أوامر مثل ping وtracert لفحص الاتصال وتحليل جداول التوجيه.

فوائد المحاكاة:

تساعد في التدريب العملي، تقليل الأخطاء، وفهم عميق لآلية التوجيه.

3. التوجيه العملي للبيانات

3.6 مشروع صغير: تنفيذ شبكة تحتوي على مسارات متعددة

هدف المشروع: تصميم شبكة تحتوي على مسارات توجيه متعددة لضمان التكرار والموثوقية.

مكونات الشبكة: عدة أجهزة توجيه متصلة بمسارات بديلة تربط بين الشبكات المختلفة.

إعداد التوجيه الديناميكي: تفعيل بروتوكولات مثل OSPF أو EIGRP لدعم تعدد المسارات.

اختبار التكرار: محاكاة انقطاع أحد المسارات والتأكد من استمرارية البيانات عبر المسار البديل.

الفائدة العملية: تعزيز استقرار الشبكة وتحسين الأداء من خلال توزيع الحمل وتكرار المسارات.

4. أمن الشبكات

4.1 الجدران النارية العملية pfSense, Cisco ASA

تعريف الجدران النارية: الجدار الناري هو نظام أمني يتحكم في حركة مرور البيانات بين الشبكات، بهدف منع الدخول غير المصرح به وحماية الشبكة من الهجمات.

أنواع الجدران النارية:

- جدران نارية تقليدية تعتمد على تصفية الحزم Packet Filtering .
- الجدران النارية من الجيل التالي التي توفر فحصاً عميقاً للحزم Deep Packet Inspection وأنظمة كشف التسلل.

وظائف الجدار الناري: توفير الحماية، التحكم في الوصول، دعم شبكات VPN، ورصد حركة المرور لتأمين الشبكة بفعالية.

4. أمن الشبكات

4.1 الجدران النارية العملية pfSense, Cisco ASA

نظام pfSense:

نظام تشغيل مفتوح المصدر مبني على FreeBSD، يقدم حلاً متكاملاً لجدار ناري متقدم.

ميزات رئيسية: إدارة سهلة عبر واجهة ويب، دعم VPN، مراقبة وتحليل حركة المرور، وقابلية التوسع.

مناسب للمؤسسات الصغيرة والمتوسطة التي تبحث عن حلول مرنة ومجانية.

جهاز Cisco ASA:

جهاز أمني متكامل يُستخدم في المؤسسات الكبيرة.

يجمع بين وظائف الجدار الناري، VPN، وأنظمة كشف ومنع التسلل IDS/IPS .

يقدم أداء عالي مع دعم متقدم لإدارة السياسة الأمنية.

4. أمن الشبكات

4.2 إعداد ومراقبة IDS/IPS مثل Snort

مفهوم أنظمة كشف ومنع التسلل IDS/IPS :

أنظمة كشف التسلل IDS تعمل على مراقبة حركة المرور داخل الشبكة بحثًا عن أي نشاط غير طبيعي أو محاولات اختراق قد تهدد سلامة الشبكة والبيانات. تقوم هذه الأنظمة بتحليل الحزم واستخدام قواعد توقيع محددة للتعرف على الهجمات المحتملة، ثم تنبيه المسؤولين لاتخاذ الإجراءات المناسبة.

أما أنظمة منع التسلل IPS فهي تتوسع في هذا الدور لتشمل القدرة على إيقاف الهجمات فور اكتشافها من خلال حظر حركة المرور الضارة تلقائيًا، مما يوفر طبقة إضافية من الحماية الفعالة ضد التهديدات.

أهمية IDS/IPS في بيئة الشبكات:

تعتبر هذه الأنظمة خط الدفاع الثاني بعد الجدران النارية، حيث تكملها في حماية الشبكة من الهجمات المعقدة والمتطورة التي قد لا تكتشفها الجدران النارية التقليدية. فهي تراقب الأنشطة بدقة عالية وتستطيع التعرف على سلوكيات غير طبيعية مثل هجمات حجب الخدمة، محاولات الدخول غير المصرح بها، والبرمجيات الخبيثة.

4. أمن الشبكات

كيف تعمل IDS و IPS؟

تعتمد أنظمة IDS/IPS على قواعد بيانات تحتوي على توقيعات الهجمات المعروفة، وتستخدم خوارزميات سلوك لتحليل البيانات الغير نمطية، مما يمكنها من الكشف عن الهجمات الجديدة والمخفية.

يمكن تشغيلها في وضع المراقبة فقط IDS حيث تقوم بالإبلاغ فقط، أو في وضع الحجب IPS حيث تتدخل لمنع الهجوم.

التحديات والمزايا:

- من التحديات إدارة قواعد التوقيع وتحديثها باستمرار لمواكبة التهديدات الجديدة.
- توفر هذه الأنظمة طبقة حماية متطورة مع إمكانيات التنبيه المبكر وتقليل الأضرار الأمنية.
- تتيح تقارير مفصلة لتحليل الهجمات ودعم اتخاذ القرار الأمني.

4. أمن الشبكات

4.2 إعداد ومراقبة IDS/IPS مثل Snort

نظام Snort:

يُعتبر Snort من أشهر أنظمة كشف ومنع التسلل مفتوحة المصدر، وهو قادر على تحليل حركة مرور الشبكة بشكل مباشر لتحديد الأنشطة المشبوهة والخبيثة.

يعتمد Snort على قواعد توقيع دقيقة تتضمن نماذج مختلفة للهجمات والتهديدات، مما يسمح له بالكشف عن محاولات التسلل والفيروسات والهجمات المتنوعة.

يمكن تشغيل Snort في وضع المراقبة لمجرد التنبيه عند اكتشاف تهديد، أو في وضع منع التسلل الذي يتضمن حظر أو قطع الاتصال مع المصادر الخبيثة.

يتميز Snort بسهولة التكوين والتخصيص، ويتيح للمسؤولين إضافة قواعد جديدة لتغطية التهديدات الحديثة.

4. أمن الشبكات

4.3 إعداد وتشغيل OpenVPN, Ipsec VPN

مفهوم الشبكات الخاصة الافتراضية VPN :

VPNهي تقنية تتيح إنشاء اتصال مشفر وآمن بين شبكتين أو بين مستخدم وشبكة عبر الإنترنت، ما يوفر خصوصية عالية وحماية ضد التنصت والتدخل الخارجي.

يتم استخدام VPN على نطاق واسع لربط الفروع المختلفة للمؤسسات، وتأمين وصول الموظفين عن بعد إلى الموارد الداخلية للشركة.

تتيح تقنية VPN للمستخدمين التصفح والتواصل وكأنهم متصلون مباشرة بشبكة المؤسسة، مما يحسن الأمان والسرعة.

OpenVPN:

هو برنامج VPN مفتوح المصدر يستخدم بروتوكولات SSL/TLS لتأمين الاتصال.

يتميز OpenVPN بمرونة عالية ودعم واسع لأنظمة التشغيل المختلفة مثل Windows، Linux، و MacOS

يدعم خيارات متقدمة مثل المصادقة الثنائية والتشفير المتقدم، مما يجعله خيارًا مثاليًا للشركات والمؤسسات.

4. أمن الشبكات

4.3 إعداد وتشغيل OpenVPN, Ipsec VPN

بروتوكول IPsec:

IPsec هو مجموعة بروتوكولات تستخدم لتأمين حركة البيانات على مستوى طبقة الشبكة.

يوفر IPsec التشفير والتوثيق لضمان سرية البيانات وسلامتها، ويستخدم بشكل واسع في الشبكات المؤسسية وربط الفروع.

يتميز IPsec بمرونته ودعمه لأوضاع تشغيل مختلفة مثل Tunnel Mode لتأمين الشبكات بأكملها و Transport Mode لتأمين الاتصالات بين الأجهزة .

إعداد IPsec يتطلب تبادل مفاتيح وتكوينات دقيقة لضمان توافق الأجهزة والاتصالات بشكل آمن.

4. أمن الشبكات

4.4 تحليل الهجمات: DoSوMITM باستخدام أدوات محاكاة

هجمات حجب الخدمة DoS :

تُعد هجمات DoS من أكثر الهجمات تأثيرًا في عالم الشبكات، حيث تستهدف جعل الخدمات غير متاحة للمستخدمين عبر إغراق الشبكة أو الخوادم بحركة مرور هائلة تتجاوز قدرتها.

تشمل الهجمات أشكالًا متعددة مثل TCP SYN Flood و UDP Flood، التي تعمل على استنزاف الموارد مثل عرض النطاق الترددي والمعالج.

تؤدي هذه الهجمات إلى توقف الخدمات عن العمل، مما يسبب خسائر مالية وتأثير سلبي على سمعة المؤسسات.

آليات الحماية:

استخدام جدران نارية متطورة وأنظمة كشف ومنع التسلل لمراقبة ومنع حركة المرور الضارة.

تطبيق حلول توزيع الحمل Load Balancing وأنظمة التكرار لتعزيز استمرارية الخدمة.

4. أمن الشبكات

4.4 تحليل الهجمات: DoS و MITM باستخدام أدوات محاكاة

هجمات الرجل في الوسط MITM :

تحدث هجمات MITM عندما يتدخل المهاجم بين طرفين متواصلين لاعتراض أو تعديل البيانات دون علم الطرفين.

تُستخدم تقنيات مثل ARP Spoofing و DNS Spoofing لإعادة توجيه حركة المرور عبر جهاز المهاجم.

تؤدي هذه الهجمات إلى كشف معلومات حساسة مثل كلمات المرور والمعلومات البنكية، مما يشكل تهديدًا جسيمًا لأمان الشبكة.

أدوات المحاكاة:

يستخدم المحللون أدوات مثل Wireshark لمراقبة حركة البيانات واكتشاف التلاعبات.

Kali Linux منصة متقدمة تحتوي على أدوات لاختبار الثغرات وتنفيذ محاكاة الهجمات، مما يساعد في تطوير استراتيجيات الحماية.

4. أمن الشبكات

4.5 التشفير العملي باستخدام OpenSSL و Wireshark

مفهوم التشفير:

التشفير هو تقنية تهدف إلى حماية البيانات بتحويلها إلى صيغة غير قابلة للقراءة دون مفتاح فك التشفير.

يضمن التشفير سرية البيانات ويحميها من التنصت أو التلاعب أثناء انتقالها عبر الشبكة.

يستخدم التشفير في معظم بروتوكولات الأمان الحديثة، مثل HTTPS و VPN

OpenSSL :

هو مكتبة وأداة مفتوحة المصدر تتيح إنشاء مفاتيح التشفير، توليد شهادات SSL، وتنفيذ عمليات التشفير وفك التشفير.

يُستخدم على نطاق واسع في تأمين الاتصالات عبر الإنترنت والتطبيقات المختلفة.

4. أمن الشبكات

4.5 التشفير العملي باستخدام OpenSSL و Wireshark

Wireshark : أداة تحليل شبكي تسمح بمراقبة حركة البيانات وتحديد ما إذا كانت مشفرة.

يمكن عبر Wiresharkرؤية عملية المصافحة Handshake في بروتوكولات SSL/TLS التي تتبادل فيها المفاتيح السرية.

تساعد الأداة في التحقق من سلامة الاتصال وفهم عملية التشفير بشكل عملي، مما يسهم في تحسين أمن الشبكات.

4.6 استجابة الحوادث الأمنية وخطط الطوارئ

مفهوم استجابة الحوادث الأمنية: هي مجموعة إجراءات منهجية تُتخذ فور وقوع حادث أمني لاكتشافه، تقييم خطورته، واحتوائه لمنع تفاقمه.

تشمل الاستجابة مراحل: الكشف، التقييم، الاحتواء، القضاء على التهديد، والاستعادة.

تساعد الاستجابة السريعة على تقليل الخسائر المالية، الفنية، والمعنوية للمؤسسات.

4. أمن الشبكات

4.6 استجابة الحوادث الأمنية وخطط الطوارئ

خطط الطوارئ:

هي استراتيجيات وسياسات تهدف إلى ضمان استمرارية العمل وتقليل الأثر الناتج عن الحوادث الكبيرة مثل الهجمات السيبرانية أو الكوارث الطبيعية.

تشمل: النسخ الاحتياطي الدوري للبيانات، توفير أنظمة تعافي احتياطية، وخطط اتصال فعالة خلال الأزمات.

تدريب الفرق على سيناريوهات مختلفة يعزز جاهزيتهم ويقلل من فرص الأخطاء.

المراجعة الدورية للخطط وتحديثها بناءً على التجارب الواقعية تضمن جاهزية دائمة لمواجهة الأزمات.

الأكاديمية العربية الدولية
Arab International Academy

أسئلة

السؤال 1: ما الفرق بين التوجيه الثابت والتوجيه الديناميكي؟

السؤال 2: كيف يساهم بروتوكول OSPF في تحسين أداء الشبكة مقارنة ببروتوكول RIP؟

السؤال 3: ما أهمية استخدام أدوات مثل Packet Tracer في تعلم التوجيه؟

السؤال 4: ما هي الفروقات الأساسية بين جهازي الجدار الناري pfSense وCisco ASA؟

السؤال 5: كيف تساعد أنظمة IDS/IPS مثل Snortفي تعزيز أمان الشبكة؟

الأجوبة

الإجابة 1 : التوجيه الثابت هو إعداد يدوي لمسارات الشبكة حيث يتم تحديد المسار يدوياً من قبل المسؤول. أما التوجيه الديناميكي فيستخدم بروتوكولات مثل OSPF لتحديث جداول التوجيه تلقائيًا بناءً على تغيرات الشبكة.

الإجابة 2 : OSPF يستخدم خوارزمية الحالة الرابطية التي توفر تحديثات أسرع وأكثر دقة للمسارات، ويدعم تقسيم الشبكة إلى مناطق لتحسين الكفاءة.

بينما RIP يعتمد على عدد القفزات فقط ولا يتعامل جيداً مع الشبكات الكبيرة أو المعقدة، ويحدث تحديثات أبطأ.

الإجابة 3 : Packet Tracer تتيح محاكاة بيئة شبكية افتراضية تمكن المستخدمين من تصميم الشبكات، إعداد التوجيه الثابت والديناميكي.

الإجابة 4 : pfSense هو نظام مفتوح المصدر يوفر حلاً مرناً وسهل الإدارة موجه للمؤسسات الصغيرة والمتوسطة، بينما Cisco ASA هو جهاز أمني متكامل وذو أداء عالي يستخدم في المؤسسات الكبيرة.

الإجابة 5 : IDS تكشف عن محاولات الاختراق والنشاطات المشبوهة وتنبه المسؤولين، أما IPS فتتدخل مباشرة لمنع الهجمات من خلال حجب حركة المرور الضارة تلقائيًا.

🧰 أدوات محاكاة عملية

- **Cisco Packet Tracer**

أداة محاكاة شبكات من Cisco تتيح لك تصميم واختبار الشبكات: تحميل الأداة

- **GNS3**

أداة محاكاة متقدمة تدعم أجهزة Ciscoالحقيقية: تحميل الأداة

مصادر خارجية

عنوان الفيديو	الرابط
قائمة تشغيل تشرح طبقات نموذج OSI بشكل مبسط باللغة العربية.	https://www.youtube.com/playlist?list=PLLlr6jKKdyK3dM-mtOZfBx6FNTJZ4vgu0
مقدمة سريعة حول استخدام Wireshark لتحليل الشبكات.	https://www.youtube.com/watch?v=ywwFoAcIC-4
شرح مفصل لبروتوكول OSPF وكيفية عمله.	https://www.youtube.com/watch?v=kfvJ8QVJscc

مواقع تعليمية ودورات تدريبية

1. دورات تعليمية باللغة العربية

- **دورة تحليل الشبكات باستخدام Wireshark**

دورة تدريبية باللغة العربية تشرح استخدام Wiresharkلتحليل الشبكات: ابدأ الدورة

- **دورة CCNA 200-301 بالعربي**

دورة تدريبية باللغة العربية تغطي مفاهيم التوجيه والشبكات: ابدأ الدورة

2. دورات تعليمية باللغة الإنجليزية

- **Cisco Packet Tracer Basic Networking - Static Routing using 2 routers**

دورة تدريبية تشرح كيفية إعداد التوجيه الثابت باستخدام Cisco Packet Tracer.

ابدأ الدورةyoutube.com+6youtube.com+6youtube.com+6

- **OSPF Explained | Step by Step**

دورة تدريبية تشرح بروتوكول OSPFبشكل مفصل: ابدأ الدورة

المراجع

- Tanenbaum, Andrew S., and David J. Wetherall. *Computer Networks*. 5th Edition, Pearson, 2011.
- Kurose, James F., and Keith W. Ross. *Computer Networking: A Top-Down Approach*. 7th Edition, Pearson, 2016.
- Stallings, William. *Data and Computer Communications*. 10th Edition, Pearson, 2013.
- Easttom, Chuck. *Network Defense and Countermeasures*. 3rd Edition, Pearson, 2014.
- Cisco Systems, Inc. *Cisco ASA Series Firewall CLI Configuration Guide*, Cisco Press, 2020.
- OpenVPN Technologies, Inc. *OpenVPN User Manual*, 2021.

- الزبيدي، عبد القادر. *مبادئ شبكات الحاسب*. دار اليازوري العلمية للنشر والتوزيع، 2018.
- الحسني، محمد عبد الله. *أساسيات شبكات الحاسوب*. دار الفكر العربي، 2019.
- العلي، خالد محمد. *أمن شبكات الحاسب: الأسس والتطبيقات*. دار وائل للنشر والتوزيع، 2020.
- علي، سامي محمود. *الشبكات المحلية والتوجيه*. مكتبة الأنجلو المصرية، 2017.
- منصور، حسين عبد الكريم. *التوجيه في شبكات الحاسب: مفاهيم وتطبيقات*. دار النهضة العربية، 2021

آمل ان تكونوا قد حققتم الفائدة
شكرا لكم