الكلية	**كلية العلوم**
القسم	**قسم التقنيات الاحيائية**
المادة باللغة الانجليزية	Computer
المادة باللغة العربية	**الحاسوب**
المرحلة الدراسية	**الثانية**
اسم التدريسي	**م.م. وسام سعد محمد**
عنوان المحاضرة باللغة الانجليزية	Network Security Basics
عنوان المحاضرة باللغة العربية	**اساسيات أمن الشبكات**
رقم المحاضرة	3
المصادر والمراجع	Graham Brown, David Watson, Cambridge IGCSE Information and Communication Technology, 3rd Edition ٢٠٢٠
	الحضر علي الخضر بحّاث، "أساسيات الحاسوب"، ٢٠١٦.
	الدكتور عادل عبدالنور، "مدخل إلى عالم الذكاء الاصطناعي"، ٢٠٠٥.

اساسيات أمن الشبكات Network Security Basics

أساسيات أمن الشبكات تشير إلى المبادئ والإجراءات المستخدمة لحماية شبكة الكمبيوتر والمعلومات الموجودة فيها من التهديدات والهجمات. الهدف الأساسي من أمن الشبكات هو الحفاظ على سرية، سلامة، وتوافر البيانات. إليك أهم الأساسيات:

١. **التشفير (Encryption):** يتم تشفير البيانات لتحويلها إلى شكل غير مفهوم حتى لا يتمكن المتسللون من قراءتها إلا إذا كان لديهم المفتاح الصحيح لفك التشفير.
٢. **الجدران النارية (Firewalls):** تعمل الجدران النارية كحاجز بين شبكتك الداخلية والشبكات الخارجية غير الموثوق بها (مثل الإنترنت)، وتقوم بتصفية المرور بناءً على مجموعة من القواعد المحددة مسبقاً.
٣. **أنظمة الكشف والتصدي:** هذه الأنظمة تقوم بمراقبة حركة البيانات عبر الشبكة لاكتشاف أي نشاط مشبوه أو محاولات للاختراق، وتقوم بإصدار إنذارات أو اتخاذ إجراءات لمنع الهجمات.
٤. **التحكم في الوصول (Access Control):** يتضمن التحكم في من يمكنه الوصول إلى الشبكة ومواردها، ويستخدم بروتوكولات مثل المصادقة الثنائية (Two-Factor Authentication) لتأمين الوصول.
٥. **البرمجيات المضادة للفيروسات (Antivirus Software):** تكتشف البرمجيات المضادة للفيروسات وتحذف البرمجيات الضارة (Malware) التي يمكن أن تصيب الأجهزة وتلحق الضرر بالنظام.
٦. **تجزئة الشبكة (Network Segmentation):** تقسيم الشبكة إلى أقسام أصغر يعزز الأمان من خلال الحد من انتشار الهجمات داخل الشبكة.
٧. **تأمين نقاط النهاية (Endpoint Security):** حماية الأجهزة مثل الهواتف الذكية والحواسيب المحمولة التي تتصل بالشبكة لضمان أنها لا تشكل نقطة دخول للتهديدات.
٨. **بروتوكولات الأمان (Security Protocols):** هناك العديد من البروتوكولات المستخدمة لضمان أمان البيانات مثل SSL/TLS لحماية الاتصالات عبر الإنترنت وIPSec لتأمين اتصالات الشبكات.

كل هذه الإجراءات تعمل معًا لإنشاء بيئة شبكية آمنة تساعد في حماية البيانات والحفاظ على سلامة الشبكة.

فهم تهديدات الشبكات Understanding Network Threats

فهم تهديدات الشبكات يشير إلى التعرف على الأنواع المختلفة من الهجمات والمخاطر التي تهدد أمان الشبكة وأنظمة المعلومات. فهم هذه التهديدات يساعد في تصميم وتنفيذ استراتيجيات أمنية فعّالة. فيما يلي بعض الأنواع الشائعة من تهديدات الشبكات:

١. **البرمجيات الخبيثة (Malware):** البرمجيات الخبيثة هي برامج مصممة لإلحاق الضرر أو تعطيل الأنظمة أو سرقة البيانات. تشمل الأنواع المختلفة من البرمجيات الخبيثة الفيروسات (Viruses)، وبرامج التجسس (Spyware)، وبرامج الفدية (Ransomware)، والدودات (Worms).

٢. **الهجمات ذات الرفض الخدمي (Denial of Service - DoS):**في هذا النوع من الهجمات، يتم إغراق الخادم أو الشبكة بعدد كبير جدًا من الطلبات في وقت واحد مما يؤدي إلى إبطاء أو تعطل النظام تمامًا.

٣. **التصيد الاحتيالي (Phishing):** هجمات التصيد الاحتيالي تعتمد على إرسال رسائل بريد إلكتروني أو مواقع زائفة تخدع المستخدمين للكشف عن معلوماتهم الشخصية مثل كلمات المرور أو أرقام بطاقات الائتمان.

٤. **الهجمات الوسطية (Man-in-the-Middle - MITM):** في هذه الهجمات، يقوم المهاجم بالتسلل بين طرفين في الاتصال ويعترض الرسائل المتبادلة أو يغيرها دون علم الأطراف المتورطة.

٥. **الاستغلالات الأمنية (Exploits):** تعتمد الهجمات القائمة على الاستغلالات على ثغرات في البرمجيات أو الأجهزة. بمجرد اكتشاف الثغرة، يمكن للمهاجم استخدامها للحصول على وصول غير مصرح به إلى النظام أو سرقة البيانات.

٦. **الهجمات القائمة على كلمات المرور (Password Attacks):** تشمل هذه الهجمات محاولة الوصول إلى النظام من خلال اختراق كلمات المرور. قد يتم ذلك عن طريق تقنيات التخمين (Brute Force) أو جمع المعلومات باستخدام الهندسة الاجتماعية.

٧. **الهندسة الاجتماعية (Social Engineering):** هذا النوع من التهديدات يعتمد على استغلال النفس البشرية لجعل الأفراد يكشفون معلومات حساسة أو يقومون بأعمال تساعد المهاجمين في الوصول إلى الشبكات.

٨. **الهجمات الداخلية (Insider Threats):** تهديد داخلي يحدث عندما يقوم شخص داخل المؤسسة (مثل موظف) بتنفيذ هجمات أو تسريب معلومات سرية. قد تكون هذه الهجمات متعمدة أو غير مقصودة.

٩. **التنصت (Eavesdropping):** هي محاولة للاستماع إلى الاتصالات الحساسة في الشبكة دون علم المرسل أو المستقبل. قد يتضمن ذلك اعتراض البيانات المرسلة عبر الشبكة مثل كلمات المرور أو الرسائل الخاصة.

فهم هذه التهديدات يساعد المتخصصين في الأمن السيبراني على تطبيق التدابير الوقائية اللازمة لضمان حماية الشبكات والأجهزة المتصلة بها.

استكشاف الاخطاء واصلاحها Troubleshooting

استكشاف أخطاء الشبكة وإصلاحها هو عملية تحديد وتحليل المشكلات التي تحدث في الشبكة والعمل على حلها. الهدف من هذه العملية هو استعادة الاتصال أو الأداء الطبيعي للشبكة والتأكد من أن جميع المكونات تعمل بشكل صحيح. يُعد استكشاف أخطاء الشبكة جزءًا أساسيًا من إدارة الشبكات، لأنه يساعد في حل المشاكل التي قد تؤدي إلى توقف الخدمة أو ضعف الأداء.

خطوات أساسية في عملية Network troubleshooting:

١. **تحديد المشكلة (Identify the Problem):** الخطوة الأولى هي جمع المعلومات المتعلقة بالمشكلة. يجب على مسؤول الشبكة أن يستفسر عن أعراض المشكلة وما إذا كانت تؤثر على جميع الأجهزة أو عدد محدود منها، وأيضًا ما إذا كانت المشكلة تتعلق بالاتصال أو سرعة الشبكة أو شيء آخر.

٢. **التأكد من الأساسيات (Check the Basics):** قبل البدء في استكشاف أعطال معقدة، يتم التحقق من الأمور الأساسية مثل الكابلات، الطاقة، حالة الأجهزة (مثل أجهزة التوجيه والمفاتيح)، والتأكد من أن الأجهزة متصلة بشكل صحيح.

٣. **استخدام أدوات الفحص (Use Troubleshooting Tools):** هناك العديد من الأدوات التي تساعد في استكشاف أخطاء الشبكة مثل:

- Ping: لاختبار الاتصال بين جهازين.
- Traceroute: لتتبع المسار الذي تسلكه الحزم عبر الشبكة وتحديد مكان الانقطاع.
- NSLookup: لفحص وحل مشاكل DNS.
- Netstat: لعرض الاتصالات النشطة على جهاز معين.

٤. **تحديد نطاق المشكلة (Narrow Down the Problem):** تحديد ما إذا كانت المشكلة تحدث في جهاز معين أو في شبكة فرعية محددة أو في جزء معين من الشبكة. هذا يساعد في تقليص النطاق وتحديد السبب المحتمل.

٥. **التحقق من مكونات الشبكة (Check Network Components):** يتم التحقق من الأجهزة مثل أجهزة التوجيه (Routers)، المفاتيح (Switches)، ونقاط الوصول (Access Points)، والتأكد من أنها تعمل بشكل صحيح وأن الإعدادات صحيحة.
٦. **التحقق من إعدادات التهيئة (Verify Configuration Settings):** أحياناً قد تكون المشكلة ناتجة عن إعدادات خاطئة في تكوين الشبكة مثل إعدادات IP، DNS، أو التوجيه (Routing). يتم فحص هذه الإعدادات والتأكد من صحتها.
٧. **التحقق من برمجيات الشبكة (Check Network Software):** التأكد من أن البرمجيات التي تدير الشبكة (مثل الجدران النارية والبرامج الأمنية) محدثة ولا تتسبب في حظر حركة المرور أو التأثير على الأداء.
٨. **إعادة التشغيل (Reboot Devices):** في بعض الأحيان، قد يكون حل المشكلة بسيطًا مثل إعادة تشغيل الأجهزة التي تتسبب في العطل، مثل أجهزة التوجيه أو نقاط الوصول.

الهدف الأساسي هو استعادة الشبكة إلى حالتها الطبيعية وتحسين الأداء، وذلك من خلال تحديد السبب الجذري للمشكلة وتطبيق الحلول المناسبة بسرعة وكفاءة.