



University of Tripoli Alahila - UTA

Information Technology

Network Security - ITPG407

Fall 2022-2023

Dr. Juma Ibrahim

مقدمه الى امن الشبكات

• ما هو أمن الشبكات ؟What is a Network Security

- أمان الشبكات هو العملية التي يتم من خلالها تأمين الشبكة ضد التهديدات الداخلية والخارجية ذات الأشكال المختلفة.
- وهي تشمل تقنيات W.H وكذلك S.W
- يستهدف انواع متعددة من التهديدات.
- يمنعهم من الدخول والانتشار على الشبكة.
- أمن الشبكة الفعال يدير اليه الوصول الامن إلى الشبكة.

مقدمه الى امن الشبكات

- كيف تعمل الشبكة ؟ How does a Network Security work

- يجمع أمان الشبكة بين طبقات متعددة من الدفاعات على طرف او حافه الشبكة (Network edge) وداخلها. كل طبقة فى الشبكة تنفذ سياسات الامان والضوابط التى تحول دون حصول تهديد او اختراق.

- يحصل المستخدمون المرخصون على حق الوصول إلى موارد الشبكة ، ولكن فى نفس الوقت يتم حظر الجهات الخبيثة من تنفيذ عمليات استغلال الثغرات والقيام بتهديد امن الشبكة.

مقدمه الى امن الشبكات

• أنواع أمن الشبكات Types of Network Security

• جدار الحماية Firewall .

- تضع جدران الحماية حاجزًا بين شبكتك الداخلية الموثوقة والشبكات الخارجية غير الموثوق بها ، مثل الإنترنت. يستخدم جدار الحماية مجموعة من القواعد المحددة للسماح بحركة المرور أو حظرها. يمكن أن يكون جدار الحماية عبارة عن أجهزة أو برامج أو كليهما.

• أمان البريد الإلكتروني Email security .

- بوابات البريد الإلكتروني هي مصدر التهديد الأول لأمن الشبكات. يستخدم المهاجمون المعلومات الشخصية وأساليب الهندسة الاجتماعية لإنشاء حملات تصيد احتيالي معقدة لخداع مستلمي البريد وإرسالهم إلى المواقع التي تقدم برامج ضارة. تحظر تطبيقات أمان البريد الإلكتروني الهجمات الواردة وتتحكم في الرسائل الصادرة لمنع فقدان البيانات الحساسة.

مقدمه الى امن الشبكات

- برامج مكافحة الفيروسات والبرامج الضارة.

Anti-viruses and anti-malware software

- تشير المصطلح "Malware" إلى البرامج الضارة ، بما في ذلك برامج مكافحة الفيروسات والديدان وأحصنة طروادة وبرامج الفدية وبرامج التجسس. في بعض الأحيان ، تصيب البرامج الضارة الشبكة ، لكنها تظل كامنة لأيام أو حتى أسابيع. لا تقوم أفضل برامج مكافحة البرامج الضارة فقط بالبحث عن البرامج الضارة عند الدخول للشبكة، ولكن أيضًا تتابع الملفات باستمرار للعثور على الحالات الشاذة والمشبوهة وإزالة البرامج الضارة وإصلاح الضرر الناتج عنها وتحديث قواعد البيانات الخاصة بها.

مقدمه الى امن الشبكات

- **صلاحيات التحكم والدخول Access Control.**

- يجب أن يكون حق الوصول إلى الشبكة غير مسموح لكل مستخدم. وذلك لمنع المهاجمين المحتملين ، تحتاج إلى التعرف على كل مستخدم وكل جهاز. ثم يمكنك فرض سياسات الأمان الخاصة بك. يمكنك حظر أجهزة النقاط الطرفية غير المتوافقة أو منحها وصولاً محدوداً فقط ، تُعرف هذه العملية بالتحكم في الوصول إلى الشبكة Network Access Control (NAC).

- **أمان التطبيقات Application Security .**

- يجب حماية أي برنامج تستخدمه لإدارة أعمالك ، سواء كان هذا البرنامج من إنتاج وبناء فريق تكنولوجيا المعلومات لديك أو قمت بشرائه. لسوء الحظ ، قد يحتوي أي تطبيق على ثغرات أو نقاط ضعف يمكن للمهاجمين استخدامها للتسلل إلى شبكتك. يشمل أمان التطبيق الأجهزة والبرامج والعملية التي تستخدمها لإغلاق هذه الثغرات.

مقدمه الى امن الشبكات

- منع فقدان البيانات Data loss prevention.
- يجب أن تتأكد المؤسسات من أن موظفيها لا يرسلون معلومات حساسة خارج الشبكة. يمكن لتقنيات منع فقدان البيانات أو DLP منع الأشخاص من تحميل المعلومات المهمة أو إعادة توجيهها أو حتى طباعتها بطريقة غير آمنة.
- أمن الاجهزه المحموله Mobile device's security.
- يستهدف مجرمو الإنترنت بشكل متزايد الأجهزة والتطبيقات المحمولة. في غضون السنوات القليلة الماضية أصبحت الكثير من مؤسسات تكنولوجيا المعلومات تدعم التطبيقات على الأجهزة المحمولة الشخصية. يجب أن تتحكم في الاجهزه المحموله التي يمكنها الوصول إلى شبكتك. ستحتاج أيضًا إلى تصحيح وتهيئه اعدادات اتصالاتهم للحفاظ على خصوصية حركة مرور الشبكة.

مقدمه الى امن الشبكات

- الشبكة الافتراضية الخاصة (VPN) Virtual Privet Network
- تقوم الشبكة الافتراضية الخاصة بتشفير الاتصال من نقطة معينه إلى شبكة ، غالبًا عبر الإنترنت. عادةً ما تستخدم VPN للوصول عن بُعد بروتوكول IPsec أو Secure Socket Layer بروتوكول لمصادقة الاتصال بين الأجهزة والشبكة.
- أمن الويب Web security.
- ستتحكم حلول أمان الويب في استخدام موظفيك للويب، وتحظر التهديدات المستندة وتنتج عن استخدام صفحات الويب الغير امنه، وتمنع الوصول إلى مواقع الويب الضارة. ستحمي بوابة الويب الخاصة بك في الموقع أو في السحابة (Cloud). يشير "أمان الويب" أيضًا إلى الخطوات التي تتخذها لحماية موقع الويب الخاص بك.

مقدمه الى امن الشبكات

- الأمن اللاسلكي Wireless security.

- الشبكة اللاسلكية ليست مؤمنة مثل الشبكات السلكية. بدون إجراءات أمنية صارمة ، يمكن أن يكون تثبيت شبكة لاسلكية مثل وضع منافذ Ethernet في كل مكان بما في ذلك ساحة انتظار السيارات. لمنع حدوث استغلال ، تحتاج إلى منتجات مصممة خصيصًا لحماية الشبكات اللاسلكية.