عمل طلاب الفرع التكنولوجي (ذكور شويكة الثانوية)- طولكرم

مالك نعالوه – عمران شرفا – محمد كنوح

تلخيص وحدة السيرفرات وحماية البيانات –اتصالات-

***ملاحظات على التلخيص**

التلخيص لا يشمل الانشطة واسئلة الدروس والوحدة _سؤال وجواب من الدروس

الحواسيب ذات الاداء العالي

الحاسوب ذو الاداء العالي : جهاز ذو قدرة حساوبية عالية يستطيع العمل لسنوات دون توقف له مواصفات تقنية مميزة تمكنه من اداء عمل المؤسسات بسرعة هائلة ومالجة كميات كبيرة من البيانات

الاسباب التي تحول دون قدرة الحواسيب الشخصية على القيام باعمال السيرفرات

1_يعتمد الحاسوب الشخصي على مصدر طاقة واحد للتغذية

2_وجود معالج واحد فقط يحوي 4 او 8 انوية

3_عدد الاقراص الصلبة تالداخلية قليل

4_عدد محدود من المنافذ

5_الحد الاقصى الذي يدعمه الحاسوب الشخصي من الذاكرة محدود

6_التبريد الداخلي في الحاسوب الشخصي غير كافي

7_الحاسوب الشخصي يتعامل مع عدد محدود من الاشخاص

8_لا يدعم استخدام الالياف الضوئية

التركيب البارد : عملية تركيب وتبديل االقطع بعد ايقاف الشتغيل (الحاسوب الشخصي)

التركيب الساخن: عملية تركيب وتبديل القطع دون ايقاف تشغيل الجهاز(السيرفرات)

---

*تسمى طريقة العمل لمدة 24 ساعة يوميا لمدة 7 ايام اسبوعيا لمدة 365 يوما سنويا وهذا الشرط يسمى استمرارية العمل وتختصر (24*7*365)

---

* الاقراص الصلبة لا تتلف بسرعة من عمليات القراءة والكتابة المستمرة وتعمل لمدة تصل الى 50 الف ساعة ما يقارب ال 6 سنوات

*تستخدم الاقراص من نوع sata في الحواسيب البسيطة والشخصية وتستخدم في السيرفرات الاقراص من نوع Scsiالتي تلفظ سكازي

*الاقراص من نوع SAS ذات سرعة واداء افضل من scsi لكن ثمنها اعلى بكثير

مقارنة:

نوع القرص	sata	scsi
سرعة القراءة والكتابة	بطيء	سريع
ضياع البيانات	يحدث	لا يحدث
ساعات العمل	عدة ايام بدون توقف	عدة سنوات دون توقف
التكلفة المادية	رخيص نسبيا	باهظ جدا

برامج فحص الاقراص الصلبة

hddscan_1

deskcheckup_2

dlgdiag_3

macrorit_4

Raid: تقنية تستخدم لضمان عدم ضياع البيانات على الاقراص الصلبة

قرص فيزيائي: قرص مستقل بذاته وغير مرتبط بغيره

القرص المنطقي: مجموعة من الاقراص الصلبة تشكل قرصا واحدا

*هناك انواع مختلفة من تقنية raid حسب درجة الحماية المطلوبة

علل تلف قرص صلب واحد في المجموعة لايوثر على ضياع البيانات

لان الاقراص الصلبة الباقية تقوم بالعمل كوحدة واحدة في حفظ البيانات

*يجب تبديل القرص الصلب التالف بسرعة

*يسترجع النظام المعلومات على القرص الجديد من خلال المعلومات المخزنة على باقي الاقراص من خلال خوارزميات رقمية تعتمد على عملية xor

---

التقنية	Raid1	Raid 5
استرجاع البيانات	ممكن ولكن ببطئ	ممكن بشكل سريع
عدد الاقراص اللازمة	على الاقل 2	على الاقل 3
المساحة الكلية المستخدمة	%50	1/n
التكلفة المادية	مرتفع	متوسط نسبيا

القواعد العامة لاستعمال تقنية raid

raid1_1 تحتاج عدد زوجي من الاقراص

2_يجب استخدام قرص صلب اضافي في اي تقنية raid ويسمى spare ويحل محل التالف

3_تتشابه تقنيات raid 4 و raid5(والاخير هي الافضل)

4_الحد الادنى من الاقراص الفيزيائية فيraid5 هو3 حيث تحتسب عملية parity

5_الحد الادنى من الاقراص في raid6 هو 4 حيث يحتسب عملية parity للحماية

6_تعد تقنيات raid2 /raid3 ضعيفة ولا تستعمل حاليا

7_التقنيات المتطورة مثل raid10/raid50/raid60 تعني النوع الاساسي متكرر مرتين

(تقنية raid50 تعني تقنية raid5 متكررة مرتين)

---

*السيرفر يستطيع استيعاب عدد cpus اكبر بكثير من الحساوب الشخصي

*معالج السيرفر يحتوي على انوية اعلى بكثير من الحاسوب الشخصي

(في السيرفر يحوي 8 معالجات كل معالج 24 نواة اي ينفذ مهامه على 192 نواة اما الحساوب الشخصي كحد اعلى 16 نواة)

برامج فحص المعالج

1_ intel processor identification utility(لفحص نوع المعالج)

2_qwik mark(لفحص القدرة الحاسوبية)

المعاير المستخدمة للمقارنة بين انظمة الشتغيل

1_البرمجيات والادوات

2_الخدمات التي تقدمها

3_ قدرتها على التعامل مع التقنيات الحديثة

امثلة على انظمة تشغيل windows server

1_windows server core:ابسط الانواع يحوي المكونات الاساسية فقط ويتعامل من خلال اوامر مكتوبة ولا يحوي واجهات رسومية

2_windows server standerd:يحتوي على ما تحتاجه الشركات الصغيرة من برامج وادوات

3_windows server interprise: خاص بالمؤسسات والشركات الكبرى ويدعم تقنيات عالية جدا

4_windows server data center: النظام الاعلى والاغلى ومخصص للشركات العملاقة التي تحتاج لمراكز معلومات خاصة

الاتصال مع العالم الخارجي : يتصل السيرفر مع العالم الخارجي من خلال منافذ عدة

*يمكن استخدام الاسلاك النحاسية في الاتصال التي تدعم سرعات مثل 10 غيغابايت او الالياف الضوئية

*يوجد للسيرفر 4 منافذ للاتصال مع الشبكة

الطاقة الكهربائية: السيرفر له امكانيات وعدد قطع كبيرة لذا يجب استخدام اكثر من مصدر طاقة وقد يصل عددها الى 6 تعمل معا دون توقف

التبريد: ينبعث من السيرفر حرارة مرتفعة جدا من القطع الداخلية ومن اجل تشتيت الحرارة من الداخل الى الخارج من اجل تبريد جميع القطع يحتاج الى عدد كبير من المراوح للتبريد بجانب الاقراص والمعالجات والذاكرة

*غالبا ما يتم تركيب السيرفرات في خزانة خاصة تسمى الكابينات

*الكابينة قد يصل ارتفاعها الى 2متر

مقارنة

الجهاز	حاسوب شخصي	منصة عمل	سيرفر
خاصية التبديل الساخن	لا يدعم	بشكل بسيط (او شفيق)	نعم بشكل متقدم جدا
عدد القطع الداخلية	بسيط وقليل	متوسط و متقدم	كبير وتقنيات متقدمة
دعم الرسومات	بسيط	متقدم جدا	لا يلزم او بسيط
التكلفة	قليل	متوسط	عالي
عدد المستخدمين	قليل	متوسط	كبير جدا
التبريد	بسيط	متوسط	تقنيات عالية جدا
سرعة الاتصال مع الخارج	محدود	متوسط	عالية جدا

متطلبات الحواسيب ذات الاداء العالي (سيرفر)

1_ عدد المستخدمين المتصلين

2_حجم البيانات المنقولة

3_نوع البرامج وعددها

حماية البيانات :الاجراءات اللازم اتخاذها لحماية الشبكة لمنع الوصول اليها من اشخاص غير مخولين بتقنيات خاصة برمجية او مادية

التهديدات الرقمية التي توثر على حماية الشبكة

1_قراصنة الانترنت

2_الفايروسات

3_سرقة المعلومات من شركات منافسة

4_التجسس بين الدول

---

*المستوى السابع هو مستوى التطبيقات والبرمجيات تستخدم كلمات المرور لحمايته

*الطبقة الفيزيائية الاولى يتم حمايتها من خلال ارسال البيانات بطريقة مشفرة

L0PTH CRACK:برنامج لتخمين كلمة المرور

وسائل الهجوم الالكتروني :الوصول الى بيانات الاخرين بطريقة غير شرعية

الهجوم الالكتروني:عملية الوصول الى المعلومات الالكترونية وسرقتها واتلافها

خوارزمية التشفير : تحويل النص الى صيغة اوشيفرة لا معنى لها للانسان

متطلبات خوارزميات الحماية
1_ان تكون مخرجاتها بعيدة عن البشري

2_تحتاج الى وقت طويل جدا لفكها

*التشفير يعتمد على الخوارزميات التي تعتمد كليا على الرياضيات ويسمى العلم الخاص بها "علم الشتفير" CRYPTOGRAPHY

*يمكن تطبيق التشفير على المستوى الثالث والرابع باستخدام بروتوكولات مختلفة SSH2,IPSECوعند التصفح الامن نستخدم بروتوكول HTTPS

اهم الوسائل المستعملة في حماية البيانات

1_التحكم بالوصول الى الشبكة

2_برامج الحماية من الفايروسات

3_حماية البيانات

4_ تحليل سلوك التطبيقات والمستخدمين

5_منع تسريب البيانات

6_حماية البريد الالكتروني

7_الجدار الناري

8_ نظام منع الاقتحام

9_حماية الشبكة اللاسلكية

10_تقسيم الشبكة لاجزاء منفصلة

11_ادارة المعلومات الامنية

12_الشبكات الخاصة الافتراضية

13_حماية التصفح

البرمجيات الخبيثة

1_حصان طروادة

2_دودة الشبكة

3_برامج التجسس

4_برامج طلب الفدية

برمجية SPAM: برمجيات تقوم بسرقة البيانات الشخصية مثل عناوين البريد الالكتروني لارسال اعلانات تجارية لالاف الاشخاص

وضح مبدا عمل برمجية طلب الفدية

يقوم المهاجم بزرع هذه البرمجيات في جهاز ما وتقوم البرمجية بمنع وصول صاحب البيانات الى ملفاته من خلال تشفيرها واخفائها ويقوم المهاجم بمطالبة الضحية بفع مبلغ من المال مقابل استرجاع الملفات

اهم الانشطة المريبة الخاصة بالبرمجيات الخبيثة

1_ قيام الفايروس بنسخ نفسه في العديد من الملفات

2_احتكار موارد الجهاز

3_تغير اسم ومحتوى ملفات نظام التشغيل

---

*حماية التطبيقات باستخدام كلمات المرور ولكن قد يوجد ثغرة امنية "VULNERABILITY" ويتم تصحيحها من خلال الحصول على التحديثات UPDATE

امثلة على سلوك غير مالوف داخل الشبكة

1_نقل ملفات كبيرة الى خارج الشبكة

2_استخدام كثيف للشبكة خارج اوقات العمل

3_محاولة قراءة البيانات من اشخاص خارج المؤسسة

4_الاتصال مع عناوين شبكة خارجية غير مالوفة

DOS: هجوم الكتروني يسمى هجوم حجب الخدمة يمنع المستخدمين من استخدام الشبكة

المؤشرات على هجوم ال DOS

1_استقرار صعود البيانات على قيمة عالية

2_عدم تمكن المستخدمين من استخدام الشبكة

طرق منع تسريب البيانات

1_مراقبة البريد الالكتروني الصادر

2_مراقبة عملية تحميل الملفات الى الخارج

3_مراقبة طباعة الملفات على ورق لتسريبه

الهندسة الاجتماعية: قيام القراصنة بنسج علاقات مع اشخاص من داخل المؤسسة وتبادل الرسائل الالكترونية معهم وتكون الرسائل تحوي برامج خبيثة لاصطياد معلومات مستخدمي الشبكة

---

*ياتي الجدار الناري كبرمجية "SW" او كجهاز "HW" يعمل كعائق بين داخل الشبكة المحمي وخارجها الغير محمي

مبدأ عمل الجدار الالكتروني

يسمح الجدار الناري للحزم الرقمية الموثوق بها الدخول الى الشبكة اما الهجمات والاتصال الغير امن يتم صده

تبعا لقواعد معينة يحدد بها جهة المرسل والجهة المسموح بالوصول لها ونوع البيانات وعنوان الجهاز المرسل

توضع هذه المعلومات في قوائم التحكم بالوصول "ACL"

اطراف الاتصال بالجدار الناري

1_الداخلي او الخاص وهو الطرف الامن

2_الخارجي او العام وهو غير امن

انواع الحماية التي تدعمها تقنية UTM

1_منع التسلسل الى الشبكة

2_منع البريد الضار

3_منع الفايروسات

4_ تفعيل الجدار الناري

5_الحماية عند تصفح الانترنت

نظام منع الاقتحام IPS:يقوم بفحص البيانات وتحليها للتعرف على اي محاولة تسلل ومنعها من خلال ذكاء اصطناعي تتم برمجته داخل هذه الاجهزة

مبدأ العمل :

يقوم بفحص كميات كبيرة جدا من المعلومات التي تشبه عمليات اقتحام معروفة بالتالى يستطيع النظام التنبؤ بسلوك المقتحم والهدف من الاقتحام ويقوم بوقف الاقتحام من خلال جزء خاص يسمى IDS

مثال على بينات تم تحليلها من هجمة حجب خدمة DOS

1_تاريخ محاولة الهجوم

2_مستوى الخطر

3_مصدر الهجوم

4_البروتوكول المستخدم للهجوم

5_المطلوب فعله من نظام الحماية

6_اسم الهجوم

طرق حماية الاتصال اللاسلكي

1_وضع كلمة مرور صعبة

2_استخدام طرق تشفير حديثة وامنة لنقل البيانات

3_وضع المستخدمين في شبكة لاسلكية مختلفة عن شبكة الضيوف

علل وضع كلمة مرور صعبة

لمنع استخدام الشبكة الا باذن من مسؤول الشبكة

فوائد تقنية VIRTUAL LANS

1_حماية عالية للشبكة

2_اداء وسرعة افضل في نقل البيانات

---

*تستعمل المؤسسات المالية والحكومية انظمة خاصة جدا وباهظة الثمن لحماية معلوماتها وقد تاتي على شكل برمجيات او اجهزة"SIEM"

الشبكات الخاصة VBN:شبكة خاصة افتراضية تربط جهازين بعدين وتعمل على نقل البيانات من خلال الانترنت باستخدام خط محمي وأمن بين الشبكتين

وظائف حماية التصفح في الانترنت

1_مراقبة تصفح الانترنت

2_منع الوصول الى المواقع الضارة

3_منع اي مخاطر من الدخول الى الشبكة

4_حماية موقع المؤسسة والسيرفرات المتصلة بلانترنت