

GS224-2



أمن المعلومات
Google Classroom code:

56ypzw5

IT-GS224 أمن المعلومات

[Copy invite link](#)

أهمية أمن المعلومات



الاهداف :-

- التعريف بأمن المعلومات.
- توضيح الحاجة إلى أمن المعلومات، وأنها ضرورة ملحة، وليست حلولاً اختيارية.
- التعرف إلى تهديدات أنظمة أمن المعلومات، كأحد الأسباب الرئيسة للحاجة إلى أمن المعلومات.
- التعرف إلى الهجمات الإلكترونية وخطورتها على المعلومات والأنظمة المعالجة لها، مع إبراز الحاجة إلى أمن المعلومات لمجابهتها.

1- أمن المعلومات

إن علم أمن المعلومات هو العلم الذي يُعنى بحماية المعلومات من المخاطر التي قد تتعرض لها. ويمكن تعريف أمن المعلومات بشكل مختصر بأنه: " **حماية المعلومات وعناصرها المهمة (بما في ذلك الأنظمة و الأجهزة التي تستخدم هذه المعلومات و تخزينها و ترسلها) من الوصول غير المسموح "**. ويمكن تعريفه بتفصيل أكثر بأنه: " المفاهيم و التقنيات و التدابير التقنية و الإدارية المستخدمة لحماية أصول المعلومات من الوصول غير المأذون به عمداً أو سهواً أو حيازتها أو الاضرار بها، أو كشفها، أو التلاعب بها، أو تعديلها، أو فقدانها أو إساءة استخدامها ".

► 3

2- محاور مفهوم أمن المعلومات

1. حماية المعلومات من الضرر بأشكاله كافة، سواء أكان مصدره أشخاص (كالمخترقين)، أم برمجيات (كفيروسات الحاسب الآلي)، وسواء أكان متعمداً أم عن طريق الخطأ.
2. حماية المعلومات من الوصول غير المصرح به، أو السرقة، أو الالتقاط، أو التغيير، أو إعادة التوجيه، أو سوء الاستخدام.
3. حماية قدرة المؤسسة على الاستمرار وأداء أعمالها على أحسن وجه.
4. تمكين أنظمة تقنية المعلومات والبرامج التطبيقية لدى المؤسسة من العمل بشكل آمن.

►



3- موجبات أمن المعلومات

1- الأصول المعلوماتية الحرجة: إذ لا تقوم تقنية المعلومات المؤسسة، ولا الخدمات التي تقدمها تلك المؤسسة، إلا على أصول معلوماتية مهمة ودرجة يجب حمايتها من أي أخطار تهددها، ويجب المحافظة على استمراريتها وبقائها متاحة متوافرة في جميع الأوقات. فالحاجة لحماية هذه الأصول تأتي من وجهين: الوجه الأول أنه لا يمكن للمؤسسة أن تستمر دون بقاء هذه الأصول عاملة متاحة آمنة، والوجه الآخر أن توفير هذه الأصول كلف مبالغ وجهودا كبيرة تستحق أن يبذل من أجلها الوقت والجهد والمال لحمايتها، ومن الأمثلة على الأصول المعلوماتية الحرجة ما يلي:

- مراكز البيانات
- قواعد البيانات
- أجهزة الخوادم الرئيسية
- شبكات المحلية و المترامية
- أنظمة التشغيل
- البرامج التطبيقية
- أجهزة تخزين المعلومات
- المواقع الإلكترونية

3- موجبات أمن المعلومات

2- حاجة أعمال المؤسسات وأنشطتها إلى ذلك: حيث أصبحت المعلومات تشكل ثروة حقيقية

للمؤسسات وموردا مهما من مواردها، بل إن المعلومات في بعض المؤسسات هي مصدر الدخل الأول لها، ويقوم عليها نشاط المؤسسة الأساسي، والتجارة الإلكترونية خير مثال لذلك.

3- حاجة المستخدمين من الخدمات الإلكترونية إلى ذلك: ومعنى ذلك أن المستخدمين

من الخدمات الإلكترونية بحاجة إلى حماية معلوماتهم من كل ما يضر بها.

4- انتشار الخدمات الإلكترونية عن بعد: مثل خدمات الحكومات الإلكترونية والتعليم عن

بعد، لدرجة أن المواطن يستطيع أن ينهي جل أو جميع إجراءاته، وأن يحصل على درجته العلمية المناسبة من منزله.

3- موجبات أمن المعلومات

5- الحاجة إلى معرفة إمكانيات المؤسسات ومدى قدرتها على حماية معلوماتها ومعرفة التهديدات التي تواجهها: فلكي نكون أمناء، فلا بد أن نعرف أنفسنا، ونعرف التهديدات التي تواجهنا.

6- كثرة التهديدات المعلوماتية وتنوعها، وتعدد مصادرها: والخطورة ذلك أنه قد توجد لجملة من التهديدات داخل المؤسسة، في أنظمتها المعلوماتية أوفي موظفيها، إذا لم يحتاط لها فقد تضرر بالمعلومات.

7- انتشار الهجمات الإلكترونية: ما انفكت وسائل الإعلام -على اختلاف أنواعها- تطالعنا من حين إلى آخر بالمزيد من أخبار الهجمات الإلكترونية، واختراق الشبكات، وتدمير و تخريب الأنظمة، وظهور فيروسات الحاسوبية.

► 7

4- تهديدات المعلومات و انظمتها

التهديدات المحيطة بالمعلومات والأنظمة والتجهيزات التي تتعامل معها، إما بتخزين أو معالجة أو نقل. فهناك تهديدات كثيرة تحيط بأنظمة المعلومات شأنها في ذلك شأن أي نظام مفتوح يمكن الوصول إليه بعدة طرق، ومن قبل أشخاص مختلفين وفي أوقات مختلفة.

1. **التهديدات الفنية** : الناجمة عن القصور والاختفاء الفنية في مختلف أنظمة المعلومات والتي يغلب عليها الطابع الفني او تكون بسبب كارثة طبيعية ، وتشمل:
 - تهديدات عيوب التصنيع و التشغيل : عيوب التصميم في الاجهزة و البرامج و الشبكات و ادوات الربط و التخزين او أى مكون اخر من مكونات أنظمة المعلومات .
 - تهديد تشتت المعلومات : تشتت معلومات المنشأة على أماكن متعددة و يجرى التعامل معها من خلال شبكات متعددة مما يحتم تطبيق أنظمة معلومات متعددة – حسب الاماكن- مما يتسبب في ضعف منظومة الامن و زيادة تكلفتها .

►



4- تهديدات المعلومات و انظمتها

- 2.** **التهديدات البشرية :** الناجمة عن العنصر البشرى مباشرة , فقد يتسبب العنصر البشرى – عمدا او خطأ – فى الضرر او الوصول الى المعلومات و الاطلاع عليها دون ان يكون له صلاحية فى ذلك أو اتلافها او اطلاعها لجهات خارجية، ومنها :
- المستخدم الشرعى الفاسد
 - موظف المرفق الفاسد
 - المستخدم و الموظف الغير واعيين للمخاطر الامنية
 - المؤسسات التجارية المنحرفة
 - المنظمات الارهابية
 - موردو الاجهزة و البرمجيات
 - المهندسون و المبرمجون و فنيو الصيانة و الدعم الفنى الخارجيون
- 3.** **التهديدات الطبيعية :** ويقصد بها الكوارث الطبيعية التى ليس للانسان و التجهيزات الفنية دخل في حدوثها ، كالزلازل و البراكين و الفيضانات و الحرائق و غيرها .



5- التحديات التي تواجه نظم امن المعلومات

- (1) **خصم ذكي قادر على التكيف:** في حين أن معظم العلوم تعتمد على الطبيعة غير متقلبة أو متغيرة، فإن أمن المعلومات يواجه خصماً ذكياً ونشطاً يتعلم ويتكيف، وغالباً ما تكون دوافعه مالية.
- (2) **لا توجد قواعد أو قيود:** لا يلتزم المهاجمون بأي قواعد للعب، بينما يتبع المدافعون عادةً بروتوكولات ونظم، ومواصفات ارتباط، ومعايير واعراف.
- (3) **عدم التماثل بين المدافع والمهاجم:** يحتاج المهاجمون إلى العثور على حلقة ضعيفة واحدة فقط لاستغلالها في النظام المستهدف، بينما يجب على المدافعين الدفاع عن جميع نقاط الهجوم المحتملة.
- (4) **حجم الهجوم:** تتيح الإنترنت هجمات واسعة النطاق وبتكلفة زهيدة، حيث يمكن بسهولة إعادة تكوين وتهيئة الاتصالات الإلكترونية وتضخيمها، بزيادة في عرض النطاق الترددي والقدرة الحاسوبية في كل مرة.
- (5) **الترباط العالمي:** مع ازدياد أعداد الأجهزة المتصلة الإنترنت عالمياً والمزودة بإمكانية ترأسل بحزم متعددة الأشكال و الأحجام ، شجع ذلك المهاجمين المتباعدين جغرافياً على تنفيذ هجومات منسقة وقوية (من خلال تدنى إمكانية التتبع والمخاطر المباشرة).



5- التحديات التي تواجه نظم امن المعلومات

- (6) **وتيرة تطور التقنية:** الابتكار التقني السريع يعني التغيير المستمر في الأجهزة والأنظمة البرمجية، وترقيات وتحديثات مستمرة للبرمجيات.
- (7) **تعقيد البرمجيات:** يتزايد حجم وتعقيد المنصات البرمجية الحديثة بشكل مستمر، كما هو الحال مع عالم واسع من البرمجيات التطبيقية. وقد تنمو عيوب البرامج أيضًا بشكل أكثر من خطي مع زيادة عدد أسطر التعليمات البرمجية.
- (8) **تدريب المطورين وأدواتهم:** العديد من مطوري البرامج لديهم القليل من التدريب الأمني أو لا يحصلون على أي تدريب على الإطلاق؛ كذلك من الصعب إنشاء واستخدام الأدوات المؤتمتة/الآلية لتحسين أمان البرمجيات.
- (9) **قابلية التشغيل البيئي والتوافق مع الإصدارات السابقة:** تؤدي متطلبات قابلية التشغيل البيئي لمجموعة متنوعة من الأجهزة والبرامج والأنظمة القديمة إلى تأخير وتعقيد نشر ترقيات الأمان، مما يؤدي إلى ثغرات أمنية مستمرة حتى في حالة توفر التحديثات التصحيحية.



5- التحديات التي تواجه نظم امن المعلومات

- (10) **السياسات الاقتصادية للأسواق ومالكي المؤسسة:** غالبًا ما تعرقل قوى السوق التخصيصات التي تعمل على تحسين الأمان، فعلى سبيل المثال، قد لا يكون المالكون الذين هم في وضع يسمح لهم بتحسين وتطوير الأمان، أو الذين سيتحملون تكلفة نشر التحسينات الأمنية، هم أنفسهم الذين سيحصلون على الفائدة المادية.
- (11) **الميزات تتغلب على الأمان:** من المعروف جيدًا أن التعقيد هو عدو الأمان، ولكن لا يوجد سوى سوقًا قليلة للمنتجات البسيطة ذات الوظائف المحدودة.
- (12) **التكلفة المنخفضة تتغلب على الجودة:** التكلفة المنخفضة والأمن المنخفض يفوزان في سيناريوهات "السوق المفتوح"، حيث بالنسبة للمشتريين، لا يمكن تمييز البرامج عالية الجودة عن البرامج المنخفضة (بخلاف التكلفة الأعلى)؛ كذلك عندما يتم بيع البرنامج، لا يتم تحمل أي مسؤولية عن الأضرار اللاحقة.
- (13) **السياق المفقود لمؤشرات المخاطر والخسائر:** يفتقر الفضاء الإلكتروني إلى إشارات ومؤشرات للمخاطر في الواقع الحقيقي وذلك لتوجيه سلوك المستخدم، وغالبًا ما تكون عواقب الاختراقات الأمنية غير مرئية فورًا وغير مرتبطة بالأسباب (أي الاختراق نفسه).
- (14) **إدارة الأسرار أمر صعب ومكلف:** تعتمد آليات الأمان الأساسية في كثير من الأحيان على الأسرار (على سبيل المثال، مفاتيح التشفير وكلمات المرور)، والتي تعتبر إدارتها السليمة صعبة ومكلفة للغاية، وذلك بسبب طبيعة الأنظمة البرمجية والعوامل البشرية.



5- التحديات التي تواجه نظم امن المعلومات

- 15) عدم امتثال المستخدمين (العوامل البشرية):** يخالف المستخدمون أو يقوضون آليات أمن المعلومات التي تفرض إزعاجات دون فوائد مباشرة مرئية (في المقابل: أقفال الأبواب المادية غير مريح أيضاً، ولكن فوائده مفهومة وواضحة).
- 16) التصميم المسبب للخطأ (العوامل البشرية):** من الصعب تصميم آليات أمنية تكون واجهاتها بديهية للتعلم وسهلة التعامل، ويمكن تمييزها عن الواجهات التي يقدمها المهاجمون، وتحفز الأفعال البشرية المرغوبة للأمن، وتقاوم الهندسة الاجتماعية.
- 17) مستخدمون مغفلين (العوامل البشرية):** في حين أن مستخدمي الحواسيب الأوائل كانوا خبراء تقنيين أو تلقوا تدريباً متخصصاً بموجب سياسات المؤسسة، فإن الكثير منهم اليوم غير خبراء وبدون تدريب رسمي أو أي خلفية تقنية عن الحاسوب.
- 18) الأمان تصميمه لاحق (غير متكامل):** لم يكن الأمان هدف التصميم الأصلي للإنترنت أو الحواسيب بشكل عام، كما أن تعديله مميزة إضافية يعد أمراً مكلفاً وغالباً ما يكون مستحيلاً دون إعادة تصميم كبيرة.
- 19) بزوخ ثغرات جديدة:** قد يؤدي نشر آلية الحماية في حد ذاته إلى ظهور نقاط ضعف جديدة أو ناقلات هجوم.
- 20) العقوبات الحكومية:** رغبة الحكومة في الوصول إلى المعلومات وتبيان الاتصالات (على سبيل المثال، مراقبة المجرمين، أو التجسس على المواطنين والدول الأخرى)، والسياسات الناتجة عن ذلك، تعيق ممارسات الحماية العملية للأمن مثل التشفير القوي.

► 13

6- مصطلحات أمن المعلومات

- **مورد النظام (الأصول):** البيانات المخزنة بنظام المعلومات ؛ أو خدمة التي يقدمها النظام ؛ أو قدرات النظام مثل المعالجة أو عرض نطاق الاتصالات ؛ أو عنصر من معدات النظام (أشياء لها قيمة مادية أو معنوية) . (مثال ، أحد مكونات النظام -الأجهزة أو البرمجيات الثابتة أو الوثائق ؛ أو المنشأة تضم عمليات ومعدات النظام) .
- **التحديات :** حدث أو كائن قد يسبب انتهاك محتمل للأمن ، والذي يحدث عندما يكون هناك ظرف أو قدرة أو إجراء أو حدث يمكن أن ينتهك الأمن ويسبب ضرراً. أي أن التهديد هو خطر محتمل مستغلاً إحدى نقاط الضعف.
- **الخصم (عامل التهديد):** كيان مهاجم أو من يمثله له القدرة علي تنفيذ تهديد ما.
- **الثغرات :** خلل أو عيوب في تصميم النظام أو تنفيذه أو تشغيله وإدارته يمكن استغلاله من قبل الخصم لانتهاك أو تجاوز أمن النظام .
- **المخاطر:** توقع ضرر أو خسارة ما بحيث يتم التعبير عنها باحتمال أن يستغل خصم تهديد معين ثغرة أمنية معينة و يستفيد من الوهن الناتج مما ينتج عنه ضرر ما. (عالي، متوسط، منخفض). لا يمكن تجاهله.

►

6- مصطلحات أمن المعلومات

الهجوم :

اعتداء على أمن النظام نابع من تهديد ذكي ؛ وهو عمل ذكي في محاولة متعمدة (بمعنى كطريقة أو تقنية) للتهرب من الخدمات الأمنية وانتهاك السياسة الأمنية للنظام.

الإجراء المضاد :

إجراء أو تقنية تقلل من تهديد أو ثغرة أو هجوم أمني عن طريق التخلص منه أو منعه ، التقليل من الضرر الذي يمكن أن يسببه ، أو عن طريق اكتشافه والإبلاغ عنه بحيث يمكن اتخاذ إجراءات تصحيحية.

السياسة الأمنية :

مجموعة من القواعد والممارسات التي تحدد أو تنظم كيفية قيام نظام أو مؤسسة بتقديم خدمات الأمان لحماية موارد النظام الحساسة والحرية.



6- مصطلحات أمن المعلومات

المصطلح	المثال في الشكل	المثال في امن المعلومات
الأصول	الدراجة النارية	بيانات المستخدمين
التهديد	فقدان الدراجة النارية	سرقه البيانات
الخصم	الخصم	مهاجم ، فيروس
الثغرات	ثقب في السياج	عيب برمجي
الهجوم	المرور او القفز عبر الثقب في السياج	ارسال فيروس الى خادم بيانات غير محمي
المخاطر	ترحل لشركة التامين (قيمة التامين)	ثقة المستخدمين وثقتهم

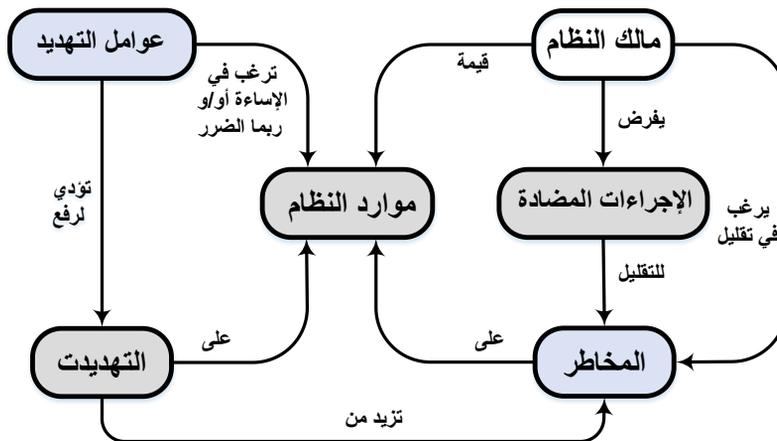


7- نموذج نظام أمن المعلومات

- ▶ موارد النظام
- ▶ الكيان المادي، البرمجيات (نظم التشغيل، التطبيقات)، البيانات (المستخدمين، النظام، قاعدة البيانات)، الشبكات و وسائل الاتصال (الموجهات، الجسور، الشبكة المحلية)
- ▶ قابلية الإصابة و ضعف موارد النظام : فساد ، عدم توفر الخدمة أو تسرب البيانات .
- ▶ التهديدات التي تستغل قابلية الإصابة أو الثغرات
- ▶ الهجوم هو التنفيذ الفعلي لتهديد ما
- ▶ نشط أو سلبي ، من الداخل أو من الخارج
- ▶ الإجراءات المضادة : الاعمال المتخذة لمنع، كشف، استرداد و تقليل المخاطر



مفاهيم وعلاقات الأمن



8- التهديدات و الهجمات

1. الكشف غير مصرح به (Unauthorized disclosure) : تهديد للسرية
 - التعرض: بيانات حساسة تم الإفصاح عنها مباشرة لجهة غير مرخص لها
 - الاعتراض: جهة غير مرخص لها تتواصل مباشرة مع بيانات حساسة أثناء الانتقال.
 - الاستدلال: يصل كيان غير مصرح به بشكل غير مباشر إلى بيانات حساسة من خلال الاستدلال على خصائص أو منتجات ثانوية للاتصالات.
 - التطفل: كيان غير مصرح به يقوم بالتحايل على تدابير الحماية الأمنية للنظام.
2. الخداع (Deception): تهديدًا لسلامة النظام أو نزاهة البيانات
 - التكرار: كيان غير مصرح له يتظاهر بأنه كيان مرخص له.
 - التزوير: بيانات كاذبة تخدع الجهة مرخص لها.
 - التنصت: كيان يخدع شخصًا آخر بإنكار المسؤولية عن فعل ما.
3. الاخلال (Disruption) : تهديدًا للتوافر أو النزاهة
 - العجز: منع / مقاطعة تشغيل النظام عن طريق تعطيل أحد مكونات النظام
 - الفساد: التعديل السلبي لوظائف أو بيانات النظام
 - العوائق: مقاطعة تقديم خدمات النظام عن طريق إعاقة تشغيل النظام.
4. الاغتصاب (Usurpation) : تهديد لسلامة النظام
 - الاختلاس: التحكم المنطقي أو المادي غير المصرح به لمورد النظام (سرقة الخدمة).
 - سوء الاستخدام: يتسبب في قيام النظام بأداء وظيفة أو خدمة تضر بالأمن.



9- الهجمات الالكترونية

تشكّل المعلومات في عصرنا الحاضر رافدًا مهمًا في حياة الدول والشعوب. وكغيرها من الروافد المهمة، فإنّه يحيط بها عدد من المخاطر أو الأعداء يجب حمايتها منهم، وكلّ خطر أو عدوّ من هؤلاء الأعداء لديه طرقه وأساليبه التي يستخدمها للوصول إلى هذه المعلومات، وبمجرّد النفاذ إلى المعلومات، فإنّه يمكن له نسخ أو تعديل أو حذف أو إساءة استخدامها، أو إلحاق الضرر بها بأيّ شكل من الأشكال، ومع تطوّر وسائل التقنية الحديثة أصبحت المعلومات معرضة للخطر أكثر من السابق، وظهرت الحاجة الماسة إلى علم أمن المعلومات.

9- الهجمات الالكترونية

اشهر الهجمات الالكترونية المعاصرة :

1

هجمات البرامج (أو الأكواد) الخبيثة (Malicious Code Attacks)

تشمل هجمات البرامج الخبيثة بشكل أساسي: هجمات فيروسات وديدان الحاسب الآلي، وبرامج أحصنة طروادة، وبرامج الاختراق، وبرامج التجسس الإلكتروني. وقد تسبب هذه البرامج في أضرار كثيرة تتراوح ما بين مجرد الإزعاج، إلى فقد البيانات، ووصولاً إلى سرقة الأموال.

2

هجمات الأبواب الخلفية (Back Door Attacks)

في بعض الأحيان، يترك المصممون أو المبرمجون أو فنيو الصيانة طرقاً خفية، تسمى الأبواب الخفية، للوصول إلى الأجهزة والشبكات من أجل استخدامها لاحقاً لأعمال التطوير والصيانة عن بُعد، ويستغل المهاجمون هذه الطرق عند اكتشافها كأبواب خلفية للدخول إلى الأجهزة والشبكات بطرق غير شرعية.

9- الهجمات الالكترونية

كسر كلمات المرور (Password Crack)

3

نعني بكسر كلمات المرور هنا عملية إعادة حساب كلمات المرور من البصمات الرقمية (Hash

Values) لهذه الكلمات، التي تُحفظ عادة في ملفات خاصة بذلك، ويمكن تنفيذ هذا النوع من الهجوم إما بإعادة حساب البصمة الرقمية لكلمات المرور بطرق رياضية معقدة، أو من خلال الجمع بين هذه الطريقة وهجمات المعجم (Dictionary Attack). وما يتم عمله هو حساب البصمة الرقمية لكل كلمة تنتج من هجوم المعجم، ثم مقارنتها مع البصمة الرقمية المخزنة في النظام المراد الهجوم عليه، وفي حال مطابقة هذه القيم فهذا يعني أنه تم الحصول على كلمة المرور، وأما إذا اختلفت فيجري الانتقال لكلمة المرور التي تليها ... وهكذا.

9- الهجمات الإلكترونية



الهجوم الأعمى (الاستقصائي) (Brute Force Attack)

4

يسمى الهجوم الذي يحدث عن طريق تجريب جميع الاحتمالات الممكنة لكلمات المرور أو الأرقام السرية، أو أي معلومة يحتاج إليها المهاجم في عملية الهجوم بالهجوم الأعمى أو الاستقصائي. وسمي بهذا الاسم لأنه لا يعتمد على أي عملية حسابية، أو أي عملية لتسريع الهجوم أو اختصار الوقت للازم لتنفيذه، وإنما يحصل بمحاولة الدخول مرة تلو الأخرى واستقصاء جميع الاحتمالات الممكنة. عادة ما يستخدم هذا النوع من الهجوم على الحسابات أو أسماء المستخدمين المشهورة التي تُكوّن أثناء تنصيب الأنظمة، مثل حساب مدير النظام (Administrator) أو (Admin)، أو حساب الضيف (Guest). وهنا تبرز أهمية تغيير هذه الحسابات من الأسماء الافتراضية لها المحددة من الشركات المنتجة إلى أسماء أخرى خاصة بالمنشأة، وكذلك أهمية تغيير الإعدادات التلقائية التي يمكن النفاذ من خلالها، مثل إعدادات المشاركة في الملفات والطابعات.



9- الهجمات الإلكترونية



وفي هذا الهجوم يحاول قرصنة الحاسب من خلالها الوصول إلى حساب على النظام المستهدف، وذلك بمحاولة «تخمين» كلمة المرور الصحيحة. وفي العادة تكون هذه العملية آلية وقد تستغرق ساعات لإكمالها. وعلى الرغم من أن إصدارات هذا الهجوم التي «صنعت للعرض على شاشة التلفاز»، والتي يحاول فيها القرصان بعضاً من كلمات المرور وبعد ذلك يتمكن بسهولة من الدخول إلى جهاز الحاسب الآلي، إلا أنها ليست بعيدة جداً عن الحقيقة. إن تحليل 450 ألف كلمة مرور تم تسريبها من خلال هجمة على موقع ياهو، يبرز النقاط الهامة التالية:

- إن كلمة السر 160 حساب على ياهو هي (111111).
- تم استخدام كلمة "password" ككلمة مرور في 780 مرة.
- تم استخدام كلمة "ninja" ككلمة مرور في 333 مرة (لكن المستخدم لم يكن كالنينجا الذي أراد أن يكون مثله).

9- الهجمات الالكترونية



هجمات الرجل في الوسط (Man-in-the-Middle Attacks)

5

يُطلق على هذا الهجوم أيضًا هجوم اختطاف بروتوكول النقل (TCP Hijacking) (TCP Attack). ويحدث في هذا الهجوم التقاط حزم البيانات (Data Packets) المارة في الشبكة، ثم تغييرها، ثم إعادةتها مرة أخرى إلى الشبكة لتكمل مسارها، لكن بمعلومات معدلة، فيمكن من خلال هذا الهجوم تعديل البيانات، أو الحذف منها، أو الزيادة عليها، أو تزويرها، أو تحويلها، أو إعادة توجيهها. ومن أشهر استخدامات هذا الهجوم انتحال هوية جهاز (أو مكوّن) آخر في الشبكة، خاصة عند الهجوم على عملية توزيع مفاتيح التشفير باستخدام الشهادات (Digital Certificates) فيظهر المهاجم كأنه رجل (غير مرئي) في الوسط بين الجهازين اللذين تجري عملية تبادل مفاتيح التشفير بينهما، فينتحل شخصية أحدهما، ثم يتعامل مع الآخر كأنه الجهاز (أو المكوّن) الحقيقي المقابل له، ومن ثم يمكن الحصول على معلومات مفاتيح التشفير، انظر الشكل

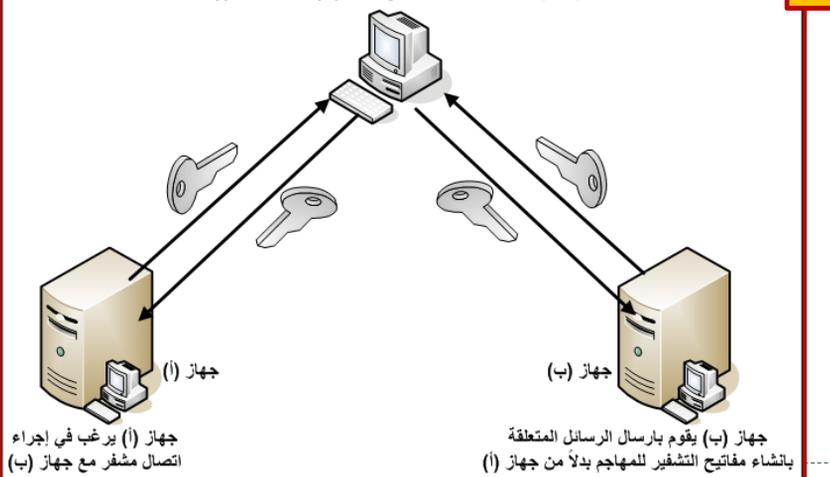
► 25

9- الهجمات الالكترونية



المهاجم (الرجل في الوسط) يقوم باعتراض الاتصال بين جهاز (أ) وجهاز (ب) ثم يقوم بالعمل وكأنه جهاز (ب) ويرسل مفتاح التشفير الخاص به إلى جهاز (أ) ثم يقوم بإنشاء اتصال مشفر مع جهاز (ب) وكأنه جهاز (أ)

5



9- الهجمات الإلكترونية



6

هجوم تعطيل الخدمة (Denial of Service (DoS) Attack)

في هذا النوع من الهجوم يُرسل عدد هائل من طلبات الاتصال أو أوامر بروتوكولات الشبكات، مثل أمر (ping) إلى الجهاز الضحية من أجل إغراقه في معالجة هذا الطلبات، وتحمله أكثر من طاقته حتى وصوله لدرجة عدم الاستجابة، ومن ثم عدم قدرته على القيام بمهامه المعتادة، وقد تصل درجة الإغراق في بعض الأحيان إلى تعطيل الهدف نهائياً وخروجه من الخدمة. وهناك نوع خطير من هذه الهجمات يسمّى هجوم تعطيل الخدمة الموزع (Distributed Denial of Service (DDoS) Attack)، والذي يتم فيه توزيع البرامج المصدرة لسلسلة من طلبات و أوامر الإغراق عبر عدد كبير من الأجهزة الموزعة في أماكن مختلفة التي تعمل عن بُعد، ومن ثم برمجة جميع هذه الأجهزة للهجوم معاً على الجهاز الضحية، ومن ثم إغراقه وتعطيله وإخراجه من الخدمة في وقت قصير. ويُعد هذا النوع من الهجمات من أعتى الهجمات وأكثرها ضراوة، حيث لا توجد له حلول مباشرة مخصصة له، وإنما تتم مكافحته بتكاتف عدد من الحلول.

9- الهجمات الإلكترونية



7

هجمات الخداع (Spoofing Attacks)

هي طريقة للتمكّن من الوصول إلى الأجهزة بطريقة غير شرعية عن طريق خداع هذه الأجهزة، بإرسال رسائل مخادعة تحتوي عنوان إنترنت (IP) يجعل الرسالة تبدو كأنها قادمة من جهة موثوقة. وإتمام هذا النوع من الهجوم فلا بدّ للمهاجم من استخدام طُرق وأدوات الحصول على عنوان الإنترنت (IP) المناسب الذي يستطيع من خلاله خداع الجهاز الضحية، وكذلك الحصول على برامج يستطيع من خلالها تغيير المعلومات الموجودة في جزء الرأس من حزم البيانات (Packet Header) لتظهر هذه الحزم كأنها قادمة من جهة موثوقة ومعروفة لدى الجهاز الضحية. وهنا تبرز الحاجة لأنظمة أمن المعلومات التي تستطيع كشف ذلك ومجابهته، خاصّة على مستوى الموجهات وجدران الحماية.



9- الهجمات الإلكترونية



8

الرسائل غير المرغوب فيها (أو المزعجة) (Spam)

يُرَدُّ إلى صناديق البريد الإلكتروني كثير من الرسائل (المزعجة) غير المرغوب فيها. ويُعدُّ كثير من الناس أنَّ هذه الرسائل لا تُعدُّ هجمات إلكترونية، لكن واقع الحال يقول إن كثيراً منها يحتوي ملفات بها برامج أو أكواد خبيثة. ويمكن التخلص من هذا النوع من الرسائل بتفعيل عمليات التنقيح والفلتره الموجودة في خوادم البريد الإلكتروني وكذلك بتوعية المستخدمين بحذف جميع الرسائل غير المرغوب فيها، وعدم الثقة في هذا النوع من الرسائل، وعدم فتحها.



9- الهجمات الإلكترونية



9

هجمات التشمم أو الالتقاط (Sniffer Attacks)

المتشمم هو برنامج أو جهاز يراقب البيانات المارة عبر الشبكة ويلتقطها، ويمكن أن يكون هناك تشمّم أو التقاط شرعي لمراقبة الشبكة ومتابعتها وإدارتها، ويمكن أن يكون غير شرعي لسرقة البيانات. ويُعدُّ هذا الهجوم خطيراً جداً على الشبكة لأنه يمكن زرع المتشمم في أي مكان في الشبكة، وغالباً لا يمكن كشفه، وهذا ما يجعله محبباً لدى المهاجمين. ويزداد الأمر خطورة إذا كان نقل المعلومات يجري على الشبكة، سواءً أكانت محلية (LAN) أم واسعة (WAN). في شكلها الأصلي غير مشفرة، لأنَّ المتشمم في هذه الحالة يستطيع قراءة كلمات المرور وكذلك محتويات الملفات النصية مثل ملفات معالجة الكلمات. وهنا تبرز أهمية توفير أنظمة الحماية التي تكشف وجود برامج وأجهزة التشمم وتكافحها، وكذلك الأنظمة التي تحول دون الاستفادة من المعلومات المسروقة في حالة نجاح المتشمم في سرقتها، كأن تكون مشفرة مثلاً.



9- الهجمات الإلكترونية



هجمات الهندسة الاجتماعية (Social Engineering Attacks)

10

يخلط هذا النوع من الهجوم بين النواحي الاجتماعية واهتمامات الناس وبين المهارات الفنية في خداع الضحايا وكسب ثقتهم للإدلاء بمعلومات سرية يتم استغلالها لسرقة المعلومات والأموال إلكترونياً (انظر الفصل السابع: موضوع: التهديدات الرقمية لشبكات الحاسب الآلي). وقد انتشر هذا النوع من الهجوم في الآونة الأخيرة انتشاراً كبيراً؛ لأنه لا يعتمد على كسر أنظمة الحماية التقنية التي تطورت مع مرور الوقت، وإنما يعتمد على كسب ثقة الضحايا وإيهامهم بأن من يطلب منهم معلوماتهم السرية (كاسم المستخدم وكلمة المرور وأرقام بطاقات الائتمان) هو جهة موثوقة (مصرف مثلاً) وبعد ذلك يتم استغلال هذه المعلومات وانتحال شخصيات الضحايا ومن ثم سرقتهم إلكترونياً عن طريق دخول يبدو شرعياً لأنظمة الحماية.



9- الهجمات الإلكترونية



10- الهندسة الاجتماعية :

- ▶ جمع المعلومات مباشرة من الأفراد و يعتمد على طبيعة الثقة في الأفراد
- ▶ المناهج النفسية
- ▶ الهدف: إقناع الضحية بتقديم معلومات أو تنفيذ فعل
 - ▶ التملق أو المغازلة
 - ▶ المطابقة
 - ▶ التودد
- ▶ سيطلب المهاجم كميات صغيرة فقط من المعلومات وفي كثير من الأحيان من عدة ضحايا مختلفين
- ▶ يجب أن يكون الطلب قابلاً للتصديق
- ▶ المهاجم "يدفع بالظرف" للحصول على المعلومات: قبل أن يشتبه الضحية في أي شيء
- ▶ قد ينتسم المهاجم ويطلب المساعدة



9- الهجمات الالكترونية

10- الهندسة الاجتماعية :

- ▶ مثال حقيقي لهجوم الهندسة الاجتماعية :
- ▶ اتصل أحد المهاجمين بمكتب الموارد البشرية : طلب وحصل على أسماء الموظفين الرئيسيين
- ▶ اقتربت مجموعة صغيرة من المهاجمين من باب المبنى
 - ▶ يتظاهر بأنه فقد مفتاح
 - ▶ سمح له بالدخول موظف ودود
 - ▶ دخل منطقة مؤمنة
- ▶ علمت مجموعة أن المدير المالي خارج المدينة بسبب رسالة تحية بيريده الصوتي
 - ▶ دخلت مجموعة مكتب المدير المالي
 - ▶ تم جمع المعلومات من جهاز كمبيوتر غير محمي
 - ▶ تفتيش سلة المهملات لاسترداد وثائق مفيدة
- ▶ اتصل أحد الأعضاء بمكتب المساعدة من مكتب المدير المالي يتظاهر بأنه المدير المالي
 - ▶ طلب كلمة المرور على وجه السرعة أعطى مكتب المساعدة كلمة المرور

▶ 33



9- الهجمات الالكترونية

هجوم تصفح الكتف (Shoulder Surfing Attack)

11

يعني هجوم تصفح الكتف أن يطلع المهاجم على المعلومات المهمة والحساسة كما لو كان ينظر إليها من فوق كتف الضحية، ويرى لوحة المفاتيح وما يقوم بضغطه من أزرار وما يعرض على الشاشة من معلومات. ويستخدم هذا الهجوم في الأماكن العامة أو أماكن العمل المشتركة، حيث ينظر المهاجم خلسة إلى شاشة الضحية، ومن ثم يعرف بعض المعلومات السرية، التي يجب أن لا يعرفها. ومن الأمثلة على ذلك: استراق النظر خلسة إلى الأرقام السرية لبطاقات الصرف الآلي وقت إدخال مستخدمها لها، وكذلك معرفة كلمات المرور للحسابات الآلية أو أجهزة الهاتف النقال وقت إدخالها، انظر الشكل .

▶

9- الهجمات الالكترونية

11

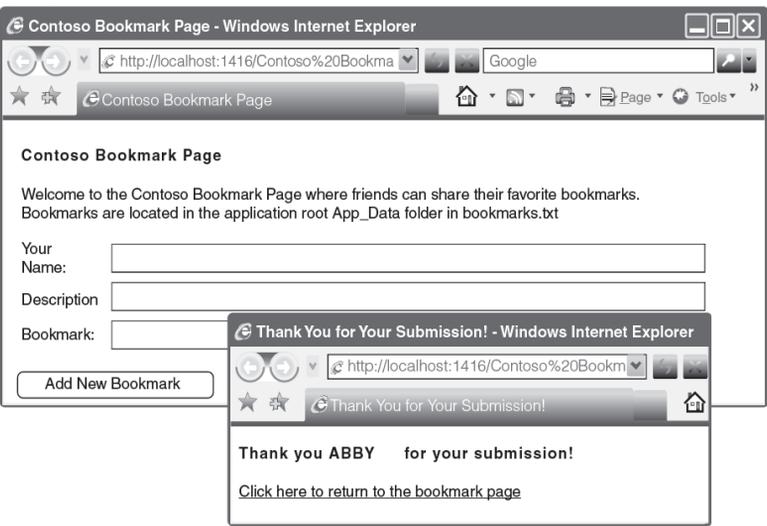
The diagram illustrates various types of cyberattacks. It shows an attacker (المهاجم) targeting an ATM, a computer, a mobile phone (الهاتف الذكي), and a user (مستخدم حاسب الي). The attacker is shown as a silhouette with a red arrow pointing to the target. The targets are labeled: 'المهاجم' (Attacker), 'جهاز الصرف الآلي' (ATM), 'مستخدم حاسب الي' (Computer user), and 'الهاتف الذكي' (Smartphone).

9- الهجمات الالكترونية

12- البرمجة النصية عبر المواقع المشتركة (Cross-Site Scripting (XSS) :

- ▶ البرمجة النصية عبر المواقع : يقوم المهاجم بحقن برنامج نصي من جانب العميل في صفحات الويب التي يعرضها المستخدمون الآخرون. الهدف هو أن المهاجم يدخل البرامج النصية في منطقة يتفاعل معها المستخدمون الآخرون. لذلك عندما ينتقلون إلى هذا الجزء من الموقع ، يتم تنفيذ النص البرمجي للمهاجم ، بدلاً من وظيفة موقع الويب المقصودة. والأهداف الشائعة لهذه الهجمات هي المنتديات على شبكة الإنترنت.
- ▶ إدخال نص برمجي خادم تطبيق الويب : توجيه الهجمات نحو العملاء
- ▶ عندما يزور الضحية موقع ويب محقون بنص برمجي خبيث: يتم إرسال تعليمات ضارة إلى متصفح الضحية
- ▶ لا يستطيع المستعرض التمييز بين التعليمات البرمجية الصالحة والبرامج النصية الضارة المطلوب من موقع الويب المستهدف :
- ▶ يقبل مدخلات المستخدم دون التحقق من صحتها
- ▶ يستخدم المدخلات في الاستجابة بدون تشفير

▶ 36



Contoso Bookmark Page - Windows Internet Explorer

http://localhost:1416/Contoso%20Bookma

Contoso Bookmark Page

Contoso Bookmark Page

Welcome to the Contoso Bookmark Page where friends can share their favorite bookmarks. Bookmarks are located in the application root App_Data folder in bookmarks.txt

Your Name:

Description:

Bookmark:

Add New Bookmark

Thank You for Your Submission! - Windows Internet Explorer

http://localhost:1416/Contoso%20Bookm

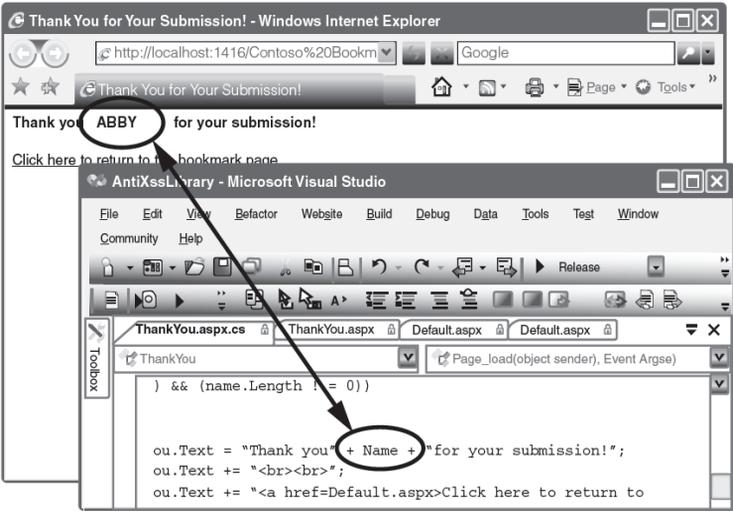
Thank You for Your Submission!

Thank you **ABBY** for your submission!

[Click here to return to the bookmark page](#)

الشكل - صفحة إشارة مرجعية تقبل إدخال المستخدم بدون التحقق من الصحة وتوفر استجابة غير مشفرة

▶ 37



Thank You for Your Submission! - Windows Internet Explorer

http://localhost:1416/Contoso%20Bookm

Thank You for Your Submission!

Thank you **ABBY** for your submission!

[Click here to return to the bookmark page](#)

AntiXssLibrary - Microsoft Visual Studio

File Edit View Refactor Website Build Debug Data Tools Test Window

Community Help

ThankYou.aspx.cs ThankYou.aspx Default.aspx Default.aspx

ThankYou Page_load(object sender), EventArgs

```

) && (name.Length != 0)

ou.Text = "Thank you" + Name + "for your submission!";
ou.Text += "<br><br>";
ou.Text += "<a href=Default.aspx>Click here to return to

```

الشكل - يتم استخدام المدخلات في الاستجابة

▶ 31



9- الهجمات الالكترونية

بعض هجمات (XSS) مصممة :

- ▶ انتحال الشخصية.
- ▶ الوصول إلى معلومات حساسة أو معلومات مقيدة.
- ▶ الحصول على وصول مجاني لمحتوى غير مجاني.
- ▶ التجسس على عادات التصفح لمستخدمي الإنترنت.
- ▶ تغيير وظائف المتصفح.
- ▶ التشهير العام بفرد أو بمنظمة.
- ▶ تشويه تطبيقات الإنترنت.
- ▶ هجمات رفض الخدمة.

شكل (6-11): المستوى العالي لهجمات البرمجة النصية للمواقع المشتركة



9- الهجمات الالكترونية

13- حقن استعلام برمجي (SQL Injection) :

- ▶ **حقن استعلام برمجي بلغة (SQL)** : يعتمد هذا الهجوم على تمرير تعليمات لغة الاستعلام البنوية (SQL) إلى تطبيق ويب وجعل هذا الموقع ينفذها. الثغرة هنا هي متعلقة بالتحقق من صحة المدخلات حيث هذه الحالة يتم فيها استخدام مدخلات المستخدم في البرنامج دون التأكد من صحتها. والاستخدام الشائع في حالة البرمجيات و بالأخص برمجيات الانترنت (مواقع الانترنت) هو الوصول للمعلومات من قواعد البيانات. وكما ترى أن هجمات حقن تعليمات الاستعلام البنوية مشابهة إلى حد كبير لهجمات البرمجة النصية عبر المواقع المشتركة (XSS) ، الفرق الأساسي هو أن هجمات (XSS) تنفذ علي الواجهة الأمامية للموقع الإلكتروني في حين أن هجمات حقن تعليمات الاستعلام البنوية تنفذ في الخادم. والمشكلة في كلتا الحالتين أنه لا يتم التحقق من مدخلات المستخدم بالشكل الصحيح.

- ▶ تستهدف خوادم (SQL) عن طريق إدخال الأوامر مباشرة
- ▶ لغة الاستعلام الهيكلية تستخدم لمعالجة البيانات المخزنة في قاعدة البيانات العلائقية (SQL) Structured Query Language : مثال علي بحث علي عنصر يطابق اسم عنصر معين : تُنشئ التعليمات البرمجية التالية بشكل ديناميكي وتنفذ استعلام SQL الذي يبحث عن العناصر المطابقة لاسم محدد.
- ▶ تتم معالجة العبارة المدخلة من قبل قاعدة البيانات



9- الهجمات الالكترونية

13- حقن نص برمجي (SQL Injection) :

```
query = "SELECT * FROM items WHERE itemname = " + ItemName.Text + "";
```

```
// expected user input for ItemName: pencil;
```

```
// actual user input for ItemName: pencil OR 'a'='a';
```

```
// query result is:
```

```
SELECT * FROM items WHERE itemname = pencils OR 'a'='a';
```

```
// which translates to: SELECT * FROM items; the query now returns all entries // stored in the items table, regardless of their specified owner.
```

► 41



9- الهجمات الالكترونية

14 - تحميل/ رفع الملفات غير المقيد :

- يحدث رفع الملفات غير المقيد عندما يتم قبول الملفات من قبل البرمجيات دون التأكد من أن الملف يتبع مواصفات دقيقة. على سبيل المثال، تشجع العديد من مواقع التجارة الالكترونية المستخدمين على رفع صور لاستخدامهم للمنتجات التي تم شراؤها عن طريق الموقع. وإذا كانت تلك المواقع لا تقوم بالتحقق من أن الصور التي تم رفعها هي بالفعل من امتداد (jpg) أو امتداد (gif) أو غيرها من صيغ ملفات الصور المماثلة، فإنه من الممكن للمهاجمين أن يقوموا برفع برمجيات على الموقع بدلاً من رفع الصور. ومن ثم تقوم تلك البرمجيات بمحاولة اختراق الموقع، مثلاً عن طريق سرقة أسماء المستخدمين وكلمات المرور.
- لمنع مثل هذه الهجمات من الحدوث، من المستحسن أن تُعامل جميع الملفات التي يتم رفعها من قبل المستخدمين على أنها ملفات خبيثة، ومن ثم يتم البحث فيها عن رموز الملفات الضارة. وهذا البحث لا يعد عديم الفائدة إذ إن جميع الملفات (كملفات gif) تحتوي على حقول للملاحظات والتي قد يستخدمها المهاجمون لإخفاء الرموز الضارة.

► 42



9- الهجمات الالكترونية

15 – هجمات تجاوز سعة المخزن المؤقت: (Buffer overflow attacks)

- ويقصد بتجاوز سعة المخزن المؤقت الحالة التي يقوم فيها برنامج ما بوضع كمية من كبيرة من البيانات أكثر من سعة المخزن، وهذه واحدة من ثغرات البرمجيات الشائعة. وعادة ستؤدي مثل هذه الحالة إلى تحطم البرمجيات. لكن المهاجم، الذي لديه معرفة تفصيلية عن البرنامج، يستطيع حفن بعض المدخلات الخاصة بحيث تقوم المحتويات الفائضة باختراق جهاز الحاسب الآلي بطرق يمكن توقعها. وإذا كان محتوى الفائض مصمما بشكل جيد فإنه يمكن "خداع" الحاسوب وإقناعه بأن الفائض هو في الواقع جزء من البرنامج ويحتاج إلى تشغيل. ويسمح الاختراق عادة للمهاجمين بالاتصال بجهاز الحاسب الآلي عن بعد ومن ثم سرقة المعلومات.
- يعد تجاوز سعة المخزن المؤقت منتشراً في البرمجيات المكتوبة بلغات غير مُدارة (Unmanaged Language) كلغة (C) أو (C++). وتقوم لغات البرمجة المدارة (Managed Language) مثل (Java) أو (C#) بإدارة الذاكرة والبيانات بحيث يكون تجاوز سعة المخزن المؤقت) غير ممكن في البرمجيات المكتوبة بهذه اللغات. لكن يتم كتابة أكثر البرمجيات (بما في ذلك المتصفحات الحديثة مثل كروم و فايرفوكس) بلغة (C/C++) من أجل تحقيق التوافق عبر المنصات المتعددة. لذلك فإن القضاء على تجاوز سعة المخزن المؤقت في معظم التطبيقات الحديثة يتطلب مهارات برمجة دقيقة للغاية.

► 43



9- الهجمات الالكترونية

16 – الأذونات الناقصة:

- الأذونات الناقصة: وتحدث ثغرة الأذونات الناقصة عندما يسمح البرنامج للمستخدمين بالوصول إلى أجزاء متميزة من البرنامج دون التحقق من بيانات اعتماد المستخدم. ودائماً يحاول المهاجمون العثور على أجزاء من النظام المالي التي يمكن الوصول إليها دون الحاجة لبيانات الاعتماد. وإذا تم العثور على هذا الجزء، فمن المرجح أن يتم استغلاله لسرقة معلومات مالية حساسة. وفي الواقع فإن العديد من حالات سرقة البيانات الكبيرة التي حدثت هي نتيجة لثغرة الأذونات الناقصة. فعلى سبيل المثال، ووفقاً لنشرة "أخطر 25 خطأ" فإن مئات الآلاف من الحسابات البنكية التابعة الى (Citigroup) قد تعرضت لاختراق في شهر مايو من عام 2011 نتيجة لوجود ثغرة الأذونات الناقصة.

► 44



9- الهجمات الالكترونية

17 - البيانات غير المشفرة:

▶ البيانات غير المشفرة: وتحدث ثغرة البيانات غير المشفرة عندما يتم تخزين بيانات حساسة محلياً أو عندما يتم نقلها عبر الشبكة بدون التشفير السليم. وتشمل البيانات الحساسة بيانات اعتماد المستخدم وغيرها من المعلومات الخاصة. ويمكن قراءة البيانات غير المشفرة والمتدفقة عبر الشبكة بسهولة باستخدام برامج تدعى - الثشم (snifers). ويمكن سرقة البيانات غير المشفرة والمخزنة في قاعدة البيانات إذا سمحت (الأذونات الناقصة) أو (عدم التحقق من صحة المدخلات) للمستخدمين بقراءة البيانات. وتمثل (البيانات غير المشفرة) عنصراً من عناصر سرقة البيانات الرئيسية.



9- الهجمات الالكترونية

18 - الاستغلال الفوري : (Zero-day exploits)

▶ الاستغلال الفوري (Zero-day exploits) : ويتم من خلالها اختراق ثغرة لم تكن معروفة في برمجيات الحاسب الآلي. ويشير المصطلح إلى أن المطورين لديهم (صفر) من الأيام لمعالجة الثغرة التي تم استغلالها. وعلى الرغم من أن المطورين ليس لديهم معرفة بالثغرة التي تم استغلالها وقت وقوع الهجوم، فإن شخصاً ما كان على علم بتلك الثغرة ، و اتاحت له الفرصة لتحديد وسيلة ما لاستغلال الثغرة بنجاح



9- الهجمات الإلكترونية

19 - الزومبي:

▶ الزومبي: وهو جهاز حاسب آلي متصل بالإنترنت تم اختراقه لتنفيذ المهام الضارة بتوجيه من متحكم عن بعد. واسم (زومبي) من الامتثال غير المشروط للتوجيهات عن بعد. وتسمى الزومبي أحياناً بالإنسان الآلي (bots) وعموماً يكون مالكو أجهزة الزومبي غافلين عن الاختراق حتى يتم إعلامهم من قبل مسؤولي الأنظمة. وهذا النوع من التهديدات متوفر بتكلفة معقولة حيث يصل معدل الإيجار الي 100,000 إلى 200,000 زومبي لمدة 24 ساعة ما يقارب من 200 دولار. وبشكل عام تستخدم الزومبي لأداء ثلاثة أنواع من الأنشطة :- إرسال رسائل إلكترونية غير مرغوب فيها، وإطلاق هجمات رفض الخدمة، وتنفيذ هجمات القاموس لكسر كلمات المرور.

▶ 47



9- الهجمات الإلكترونية

20 - تزوير الطلب عبر المواقع الإلكترونية المشتركة: (Cross-site request forgery)

عندما تجلس لاستخدام جهاز الحاسب الآلي هناك احتمال كبير أن تقوم بتسجيل الدخول إلى العديد من المواقع المختلفة مثل الفيسبوك (Facebook)، وشبكة مايكروسوفت (MSN)، والموقع الاخباري سي إن إن (CNN)، وغيرها. والمهاجم الذي يستخدم ثغرة (تزوير الطلب عبر المواقع الإلكترونية المشتركة) يعتمد على هذه الحقيقة لإرسال "طلبات" لخدمات التسجيل في تلك المواقع نيابة عنك. وفي حين أن هجمات (البرمجة النصية عبر المواقع المشتركة) "ترد" حمولة الخادم مرة أخرى إلى العميل فإن هجوم (تزوير الطلب عبر المواقع الإلكترونية المشتركة) يقوم بتنفيذ الأمر على الخادم نيابة عن العميل.

على سبيل المثال، من وراء الكواليس ومن دون علمك قد يقوم المهاجم بإرسال طلب باستخدام "بروتوكول نقل النص المتشعب" (HTTP) إلى الخادم بهذا الشكل:

<http://somesite.com/change-password.php&user=jdoe?new-pwd=ilikepie>

يتلقى خادم الشبكة هذا الطلب، ويؤكد أنه تم تسجيل دخول (jdoe)، ويقوم بتغيير كلمة المرور إلى (ilikepie) .

▶ 48



9- الهجمات الالكترونية

21 – هجمات بيانات الاعتماد الافتراضية (Default credentials attacks)

تأتي الأجهزة مصممة لتكون متصلة عادة من المصنع بكلمة مرور افتراضية. وينطبق هذا الكلام على بعض التطبيقات البرمجية وقواعد البيانات. وتشير هجمات بيانات الاعتماد الافتراضية إلى الحوادث التي يقوم فيها قراصنة الحاسب بالوصول إلى نظام أو إلى برنامج محمي بواسطة اسم مستخدم وكلمة مرور موحدة ومحددة مسبقاً (ومن ثم تكون معروفة على نطاق واسع). وهناك العديد من المواقع الإلكترونية التي تقوم بجمع قوائم كلمات السر الافتراضية. موقع (CIRT.net)، على سبيل المثال، يحتفظ بقاعدة بيانات تتضمن 1973 كلمة مرور افتراضية من 467 شركة مثل مايكروسوفت و فريزون .

وفي شهر يوليو من عام 2012 اكتشف أحد مزودي خدمة الإنترنت الرئيسيين في هولندا أن حسابات العملاء معرضة لاختراق بسبب بيانات الاعتماد الافتراضية؛ إذ جرى إعداد اسم المستخدم ليتكون من الرمز البريدي بالإضافة إلى عنوان الشارع، في حين تم ضبط كلمة المرور الأولية لتكون "welkom01". وعندما جرى القيام بالفحص الأمني على الحسابات تم اكتشاف أن 140 ألف عميل لم يكلفوا أنفسهم عناء تغيير كلمات المرور الافتراضية الأولية.

► 49



9- الهجمات الالكترونية

22 – القرصنة

وفقاً لتقرير اختراق البيانات التابع لنموذج تصنيف الحوادث (VERIS) لعام 2011 فإن 81% من الخروقات في عام 2011 قد تضمنت نوعاً من أعمال القرصنة. وبعض الأساليب المستخدمة للوصول إلى الأجهزة تتم من خلال البرمجيات الخبيثة. والفرق الأساسي بين اختراق القرصنة وبين الإصابة بالبرمجيات الخبيثة هو أن الإصابة بالبرمجيات الخبيثة تنتشر تلقائياً دون تدخل العنصر البشري. وعلى الرغم أن كلا منها قد يستخدم أساليب الاختراق نفسها، فإن اختراق القرصنة هو هجوم موجه من قبل القرصان ويستهدف مجموعة أو مؤسسة معينة.

► 50