1

محاضرات مادة مهارات الحاسوب2
الفصل الاول

كلية العلوم للبنات ـ قسم علوم الحياة
المرحلة الثانية

Network

م.م. آمنة هيثم عبد اللطيف
م.م ليلى مرتضى محمد علي

الباب الخامس :- Network

(Network)

تتكون الشبكة من جهازين كمبيوتر أو أكثر مرتبطين بهدف مشاركة الموارد (مثل الطابعات والأقراص المضغوطة)، أو تبادل الملفات، أو السماح بالاتصالات الإلكترونية. وقد تكون أجهزة الكمبيوتر على الشبكة مرتبطة من خلال السلاك، أو خطوط الهاتف، أو الموجات الراديوية، أو الأقمار الصناعية.

➢ هناك نوعان شائعان جدًا من الشبكات:

1. الشبكة المحلية (LAN: local area network)
2. الشبكة الواسعة (WAN :wide area network)

1. الشبكة المحلية (LAN)

الشبكة المحلية (LAN) هي شبكة تقتصر على منطقة صغيرة نسبيًا. وهي تقتصر عمومًا على منطقة جغرافية مثل مختبر، مدرسة او مبنى.

2. شبكة المنطقة الواسعة (WANs)

تربط شبكات المنطقة الواسعة (WANs) الشبكات في مناطق جغرافية أكبر، مثل فلوريدا أو الولايات المتحدة أوالعالم. يمكن استخدام الاسلاك المخصصة عبر المحيطات أو الروابط عبر الأقمار الصناعية لتوصيل هذا النوع من الشبكات العالمية.

باستخدام شبكة WAN، يمكن للمدارس في فلوريدا التواصل مع أماكن مثل طوكيو في غضون ثوانٍ، دون دفع فواتير هاتفية ضخمة. يمكن لمستخدمي على بعد نصف الكرة الأرضية مع محطات عمل مجهزة بمذياع وكاميرا ويب عقد مؤتمرات هاتفية في الوقت الفعلي. شبكة WAN معقدة اكثر من الشبكة المحلية. تستخدم أجهزة الإرسال المتعددة والجسور والموجهات لتوصيل الشبكات المحلية بشبكات الاتصالات العالمية مثل الإنترنت. ومع ذلك، بالنسبة للمستخدمين، لن تبدو شبكة WAN مختلفة كثيرًا عن شبكة LAN.

➢ مكونات الشبكة:

تصنف أجهزة الكمبيوتر المتصلة بالشبكة على نطاق واسع على أنها:

- خوادم
- محطات عمل

لا يستخدم البشر الخوادم بشكل مباشر عمومًا، بل تعمل بشكل مستمر لتوفير "خدمات" لأجهزة الكمبيوتر الأخرى (ومستخدميها من البشر) على الشبكة. يمكن أن تشمل الخدمات المقدمة الطباعة والفاكس، واستضافة

البرامج، و تخزين الملفات ومشاركتها، والمراسلة، وتخزين البيانات واسترجاعها، والتحكم الكامل في الوصول (الأمان) لموارد الشبكة، والعديد من الخدمات الأخرى.

تُسمى محطات العمل بهذا الاسم لأنها تحتوي عادةً على مستخدم بشري يتفاعل مع الشبكة من خلالها. كانت حاسبات المكتبية تعتبر محطات العمل سابقا، و تتكون من حاسبة ولوحة مفاتيح وشاشة وفأرة، أو حاسوب محمول مزود بلوحة مفاتيح وشاشة ولوحة لمس مدمجة. مع ظهور الحواسيب اللوحية وأجهزة شاشات اللمس مثل iPad وiPhone، تتطور تعريف محطة العمل ليشمل تلك الأجهزة، نظرًا لقدرتها على التفاعل مع الشبكة والاستفادة من خدمات الشبكة.

تميل الخوادم إلى أن تكون أقوى من محطات العمل، على الرغم من أن التكوينات تسترشد بالاحتياجات. على سبيل المثال، قد توجد مجموعة من الخوادم في منطقة آمنة، بعيدًا عن البشر، ولا يمكن الوصول إليها إلا من خلال الشبكة. في مثل هذه الحالات، سيكون من الشائع أن تعمل الخوادم بدون شاشة أو لوحة مفاتيح مخصصة. ومع ذلك، قد يزيد حجم وسرعة معالج(ات) الخادم والقرص الصلب والذاكرة الرئيسية بشكل كبير من تكلفة النظام. من ناحية أخرى، قد لا تحتاج محطة العمل إلى قدر كبير من التخزين أو الذاكرة العاملة، ولكنها قد تتطلب شاشة باهظة الثمن لتلبية احتياجات مستخدميها.

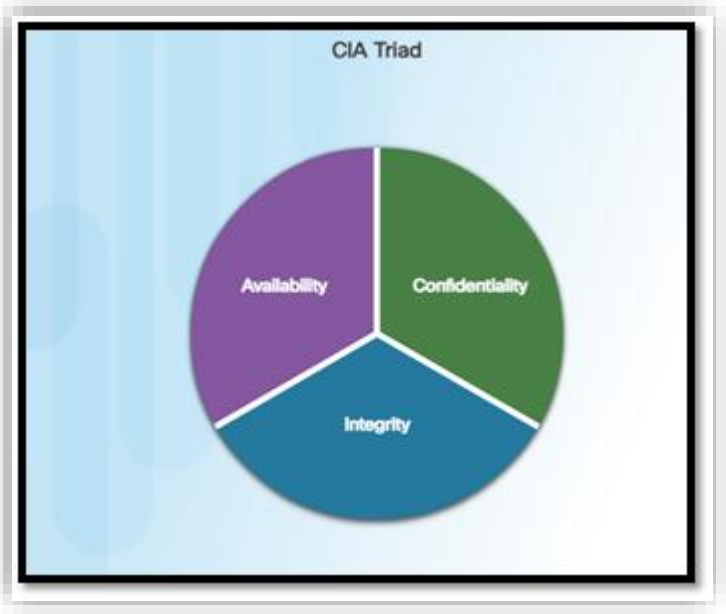
على شبكة LAN واحدة، يمكن توصيل أجهزة الكمبيوتر والخوادم بالاسلاك أو لاسلكيًا. يتم إتاحة الوصول اللاسلكي إلى شبكة سلكية من خلال نقاط الوصول اللاسلكية (WAPs). توفر أجهزة WAP هذه جسرًا بين أجهزة الكمبيوتر والشبكات. قد يكون لنقطة الوصول اللاسلكية النموذجية القدرة النظرية على توصيل مئات أو حتى آلاف المستخدمين اللاسلكيين بشبكة، على الرغم من أن القدرة العملية قد تكون أقل بكثير.

ستكون الخوادم متصلة دائمًا تقريبًا بالكابلات بالشبكة، لأن اتصالات الكابل تظل الأسرع. عادةً ما تكون محطات العمل الثابتة (أجهزة الكمبيوتر المكتبية) متصلة أيضًا بكابل بالشبكة، على الرغم من أن تكلفة المحولات اللاسلكية انخفضت إلى الحد الذي يجعل من الأسهل والأقل تكلفة استخدام اللاسلكي للحواسيب المكتبية عند تثبيت محطات العمل.

➢ ما هو أمان الشبكة ؟

يعرف أمان الشبكات بأنه عملية إنشاء نهج دفاعي استراتيجي يؤمن بيانات الشركة و مواردها عبر شبكتها. يحمي المنظمة من أي شكل من أشكال التهديد المحتمل أو الوصول غير المصرح به. بغض النظر عن حجم المؤسسة أو صناعتها او بنيتها التحتية. فان حلول أمان الشبكة تحميها من التهديد المتطور باستمرار للهجمات الإلكترونية.

يشمل أمن الشبكات على مجموعة واسعة من التقنيات و الأجهزة والعمليات. يشير الى مجموعة من القواعد و التكوينات المصممة بشكل فريد لحماية شبكات الكمبيوتر و بياناتها. يتم الحفاظ على سلامة وسرية و امكانية الوصول الى أجهزة الكمبيوتر هذه من خلال أمان الشبكة و تقنيات البرامج والأجهزة.



تعتبر شبكة آمنة فقط عندما تتكون من ثلاثة مكونات رئيسية:

السرية (confidentiality)

و النزاهة (integrity)

و التوافر(availability).

هذا المزيج، المسمى ثالوث CIA، هو معيار معروف يستخدم أثناء إنشاء سياسات أمن الشبكات لأي مؤسسة.

في عالم يكون فيه انترنت الأشياء (IoT) هو الوضع الطبيعي الجديد,تزداد بنية الشبكة تعقيدا. يتعرض هذا النظام باستمرار لتهديد من المتسللين الذين يتطورون و يجدون باستمرار طرقا لاكتشاف نقاط الضعف و استغلالها. توجد نقاط ضعف في العديد من المجالات مثل الأجهزة و البيانات و التطبيقات والمستخدمين و المواقع و غيرها. حتى مع اقصر فترة توقف، يمكن أن تكون الخسائر هائلة.

➢ انواع الثغرات الأمنية للشبكة:

قبل فحص أنواع مختلفة من الهجمات الأمنية و كيف يساعد أمن الشبكات في تجنبها، فإن فهم مكان ضعف الشبكة هو المفتاح تمنح أي ثغرة امنية المتسللين القدرة على الوصول الى البنية التحتية و تثبيت البرامج الضارة و حتى سرقة البيانات و تعديلها، إن لم يكن تدميرها أو محوها.

تشمل الثغرات الأمنية :

1. **ثغرات برمجية Software vulnerabilities**
2. **ثغرات في الاجهزة Hardware vulnerabilities**

➢ انواع المهاجمين Attacker

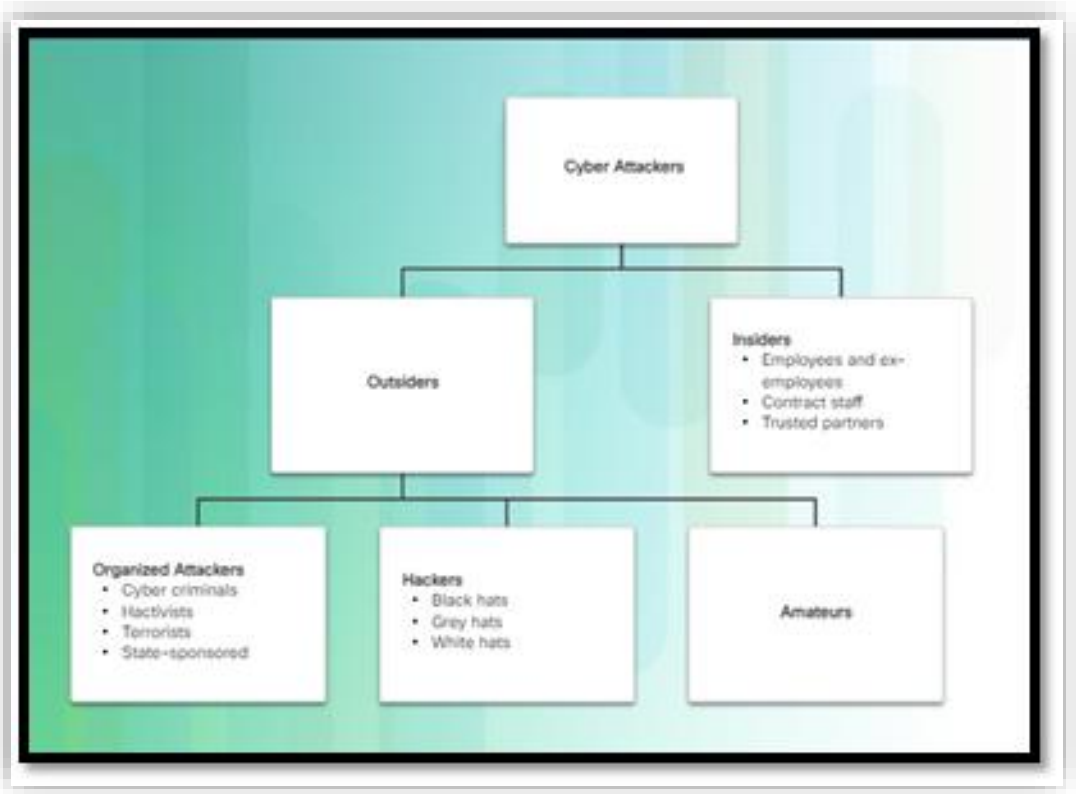
1. **الهواة Amateurs :-** يُطلق على هؤلاء الأشخاص أحيانًا اسم Script Kiddies. وهم عادةً مهاجمون لا يمتلكون مهارات تذكر، وغالبًا ما يستخدمون أدوات أو تعليمات موجودة على الإنترنت لشن الهجمات

2. **القراصنة Hackers:** تقوم هذه المجموعة من المهاجمين باختراق أجهزة الكمبيوتر أو الشبكات للوصول إليها. واعتمادًا على نية الاختراق، يتم تصنيف هؤلاء المهاجمين على أنهم من ذوي القبعات البيضاء أو الرمادية أو السوداء.

- يقوم المهاجمون ذوو القبعات البيضاء باختراق الشبكات أو أنظمة الكمبيوتر لاكتشاف نقاط الضعف حتى يمكن تحسين أمان هذه الأنظمة. تتم عمليات الاختراق هذه بإذن مسبق ويتم الإبلاغ عن أي نتائج إلى المالك.
- من ناحية أخرى، يستغل المهاجمون ذوو القبعات السوداء أي ثغرة لتحقيق مكاسب شخصية أو مالية أو سياسية غير قانونية.
- يقع المهاجمون ذوو القبعات الرمادية في مكان ما بين المهاجمين ذوي القبعات البيضاء والسوداء. قد يجد المهاجمون ذوو القبعات الرمادية ثغرة في النظام. قد يبلغ المتسللون ذوو القبعات الرمادية أصحاب النظام بالثغرة إذا تزامن هذا الإجراء مع أجندتهم. ينشر بعض المتسللين ذوي القبعات الرمادية الحقائق حول الثغرة على الإنترنت حتى يتمكن المهاجمون الآخرون من استغلالها.

3. القراصنة المنظمين Organized Hackers :

تشمل هذه المجموعات من القراصنة منظمات المجرمين الإلكترونيين، والناشطين في مجال القرصنة، والإرهابيين، والقراصنة الذين ترعاهم الدولة. وعادة ما يكون مجرمو الإنترنت عبارة عن مجموعات من المجرمين المحترفين الذين يركزون على السيطرة والسلطة والثروة.



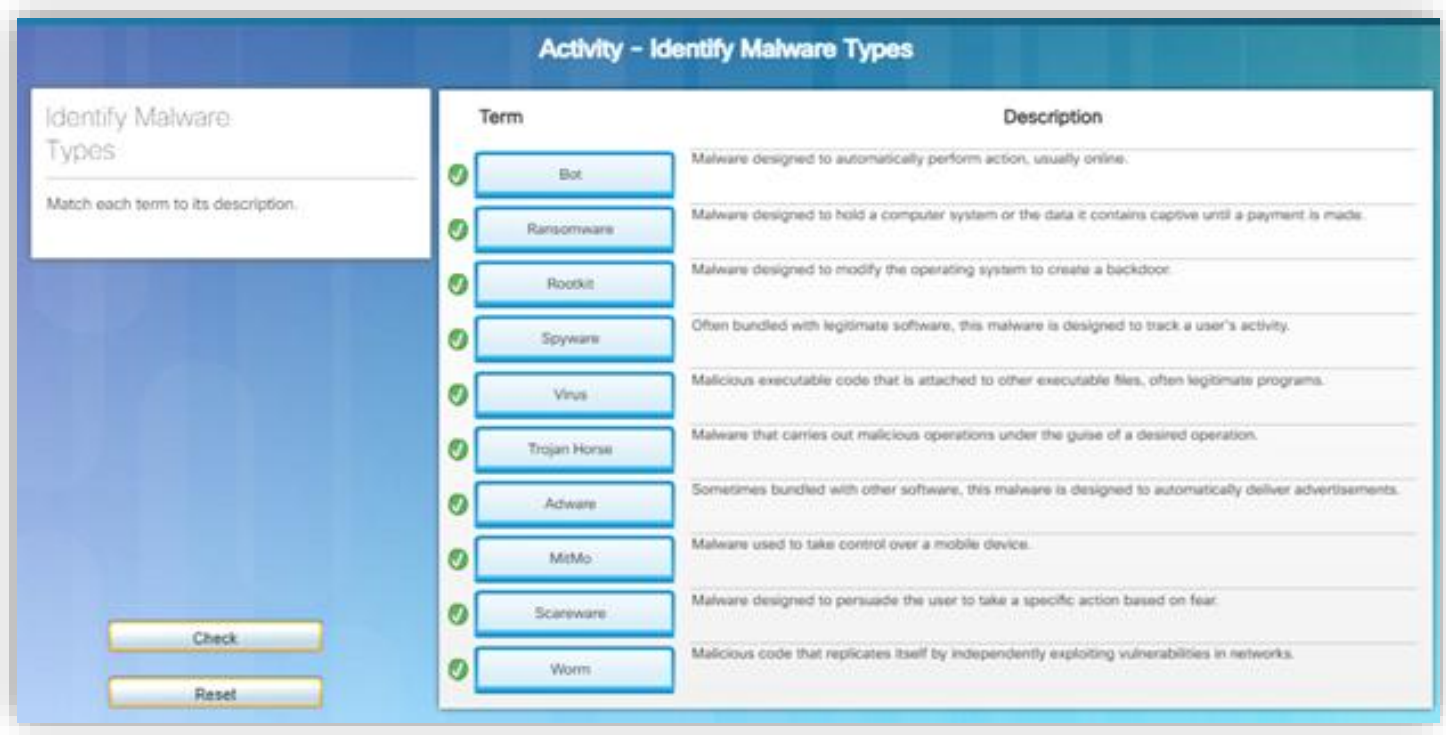
➢ أنواع البرمجيات الخبيثة Malware

1. **برامج التجسس Spyware :** تم تصميم هذا البرنامج الخبيث تتبع المستخدم والتجسس عليه.
2. **برامج إعلانية Adware:** تم تصميم البرامج التي تدعم الإعلانات لتقديم الإعلانات تلقائيًا. غالبًا ما يتم تثبيت البرامج الإعلانية مع بعض إصدارات البرامج. تم تصميم بعض البرامج الإعلانية لتقديم الإعلانات فقط، ولكن من الشائع أيضًا أن تأتي البرامج الإعلانية مع برامج التجسس.
3. **الروبوتات Bot:** من كلمة روبوت، فإن كلمة بوت هي برنامج ضار مصمم لأداء عمل تلقائيًا، وعادة ما يكون ذلك عبر الإنترنت. وفي حين أن معظم الروبوتات غير ضارة، فإن أحد الاستخدامات المتزايدة للروبوتات الضارة هو شبكات الروبوتات. حيث يتم إصابة العديد من أجهزة الكمبيوتر بالروبوتات المبرمجة للانتظار بهدوء للأوامر التي يقدمها المهاجم.
4. **برامج الفدية Ransomware :** تم تصميم هذا البرنامج الخبيث لاحتجاز نظام الكمبيوتر أو البيانات التي يحتوي عليها حتى يتم سداد الدفعة. يعمل برنامج الفدية عادةً عن طريق تشفير البيانات في الكمبيوتر بمفتاح غير معروف للمستخدم.
5. **برنامج مخيف Scareware:** هذا نوع من البرمجيات الخبيثة المصممة لإقناع المستخدم باتخاذ إجراء معين بناءً على الخوف. تقوم البرمجيات الخبيثة بتزوير نوافذ منبثقة تشبه نوافذ حوار نظام التشغيل. تنقل هذه النوافذ رسائل مزيفة تفيد بأن النظام معرض للخطر أو يحتاج إلى تنفيذ برنامج معين للعودة إلى التشغيل الطبيعي. في الواقع، لم يتم تقييم أو اكتشاف أي مشاكل وإذا وافق المستخدم وأزال البرنامج المذكور للتنفيذ، فسوف يصاب نظامه بالبرمجيات الخبيثة.
6. **برامج Rootkit :** تم تصميم هذا البرنامج الخبيث لتعديل نظام التشغيل لإنشاء باب خلفي. ثم يستخدم المهاجمون الباب الخلفي للوصول إلى الكمبيوتر عن بُعد. تستغل معظم Rootkit الثغرات الأمنية في البرامج لاعطاء صلاحيات و امتيازات وتعديل ملفات النظام. ومن الشائع أيضًا أن تقوم Rootkit بتعديل أدوات التحليل الاختراق للنظام والمراقبة، مما يجعل اكتشافها صعبًا للغاية. غالبًا ما يتعين مسح الكمبيوتر المصاب بأداة Rootkit وإعادة تثبيته.
7. **فيروس Virus:** الفيروس عبارة عن كود قابل للتنفيذ ضار يتم إرفاقه بملفات قابلة للتنفيذ أخرى، غالبًا ما تكون برامج مشروعة. تتطلب معظم الفيروسات تنشيط المستخدم النهائي ويمكن تنشيطها في وقت أو تاريخ محدد. يمكن أن تكون الفيروسات غير ضارة وتعرض صورة ببساطة أو يمكن أن تكون مدمرة، مثل تلك التي تعدل أو تحذف البيانات. يمكن أيضًا برمجة الفيروسات للتحور لتجنب الكشف عنها. تنتشر معظم الفيروسات الآن من خلال محركات أقراص USB أو الأقراص الضوئية أو مشاركات الشبكة أو البريد الإلكتروني.
8. **البرامج Trojan horse:** حصان طروادة هو برنامج ضار ينفذ عمليات ضارة تحت ستار عملية مرغوبة. يستغل هذا الكود الضار امتيازات المستخدم الذي يقوم بتشغيله. غالبًا ما توجد أحصنة طروادة في ملفات الصور أو الملفات الصوتية أو الألعاب. يختلف حصان طروادة عن الفيروس لأنه يرتبط بملفات غير قابلة للتنفيذ.

9. الفيروس المتنقل Worm: الديدان عبارة عن أكواد خبيثة تتكاثر من خلال استغلال نقاط الضعف في الشبكات بشكل مستقل. وعادة ما تعمل الديدان على إبطاء الشبكات. وفي حين يتطلب الفيروس برنامجًا مضيفًا للعمل، يمكن للديدان أن تعمل من تلقاء نفسها. وبصرف النظر عن العدوى الأولية، فإنها لم تعد تتطلب مشاركة المستخدم. وبعد إصابة المضيف، تصبح الدودة قادرة على الانتشار بسرعة كبيرة عبر الشبكة. وتشترك الديدان في أنماط مماثلة. فكلها لديها ثغرة تمكينية، وطريقة لانتشار نفسها، وكلها تحتوي على حمولة. الديدان مسؤولة عن بعض أكثر الهجمات تدميراً على الإنترنت.

10. رجل في الوسط Man-In-The-Middle (MitM): يتيح MitM للمهاجمين السيطرة على جهاز دون علم المستخدم. وبفضل هذا المستوى من الوصول، يمكن للمهاجم اعتراض معلومات المستخدم والتقاطها قبل نقلها إلى وجهتها المقصودة. تُستخدم هجمات MitM على نطاق واسع لسرقة المعلومات المالية. وهناك العديد من البرامج الضارة والتقنيات التي توفر للمهاجمين قدرات MitM.

11. رجل في الهاتف المحمول Man-In-The-Mobile (MitMo) : MitMo هو نوع من الهجمات يستخدم للسيطرة على جهاز محمول. عند الإصابة، يمكن توجيه الجهاز المحمول لاستخراج معلومات حساسة للمستخدم وإرسالها إلى المهاجمين.



➢ أعراض البرمجيات الخبيثة

بغض النظر عن نوع البرامج الضارة التي أصيب بها النظام، فهذه هي أعراض البرامج الضارة الشائعة:

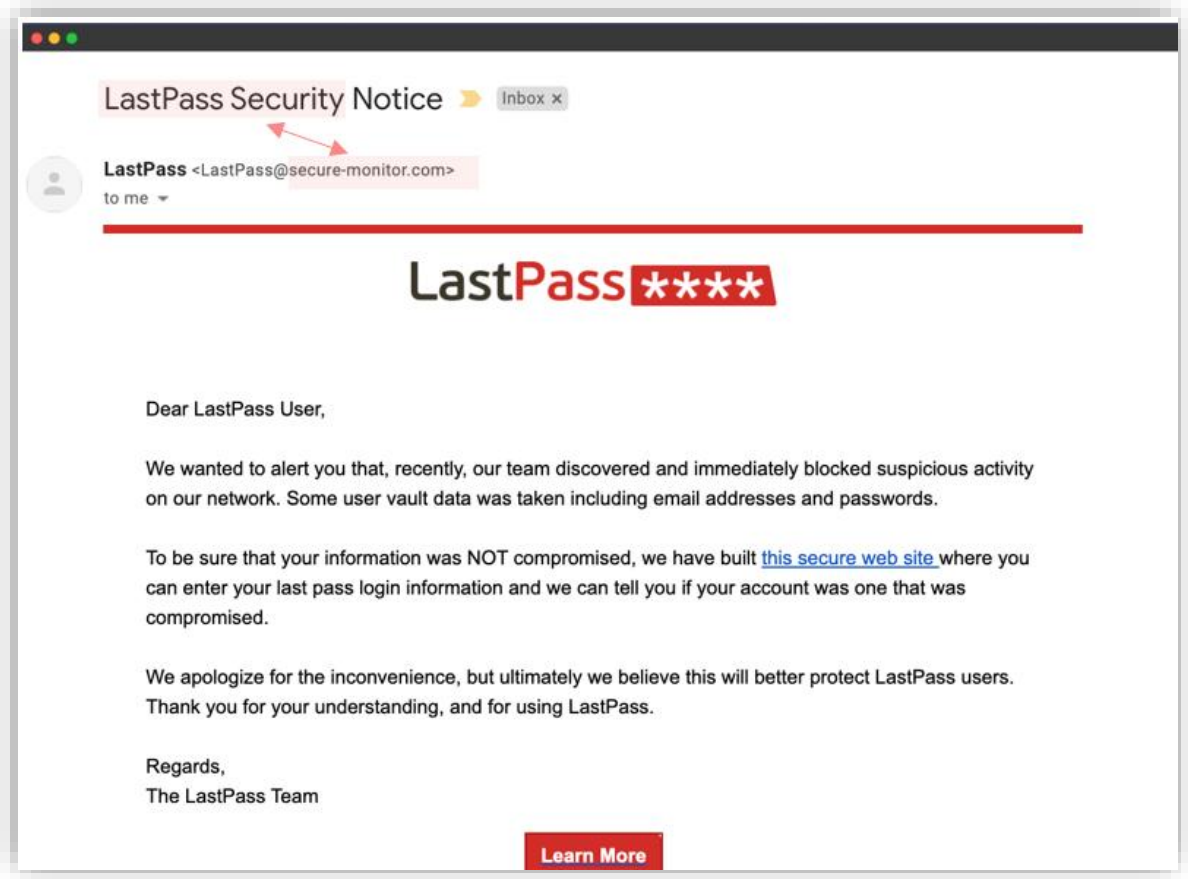
- زيادة استخدام وحدة المعالجة المركزية.
- انخفاض سرعة الكمبيوتر.
- تجميد الكمبيوتر أو تعطله بشكل متكرر.
- انخفاض سرعة تصفح الويب.
- وجود مشاكل غير قابلة للتفسير في اتصالات الشبكة.
- تعديل الملفات.
- حذف الملفات.
- وجود ملفات أو برامج أو أيقونات سطح مكتب غير معروفة.
- وجود عمليات غير معروفة قيد التشغيل.
- إيقاف تشغيل البرامج أو إعادة تكوين نفسها.
- إرسال البريد الإلكتروني دون علم المستخدم أو موافقته.

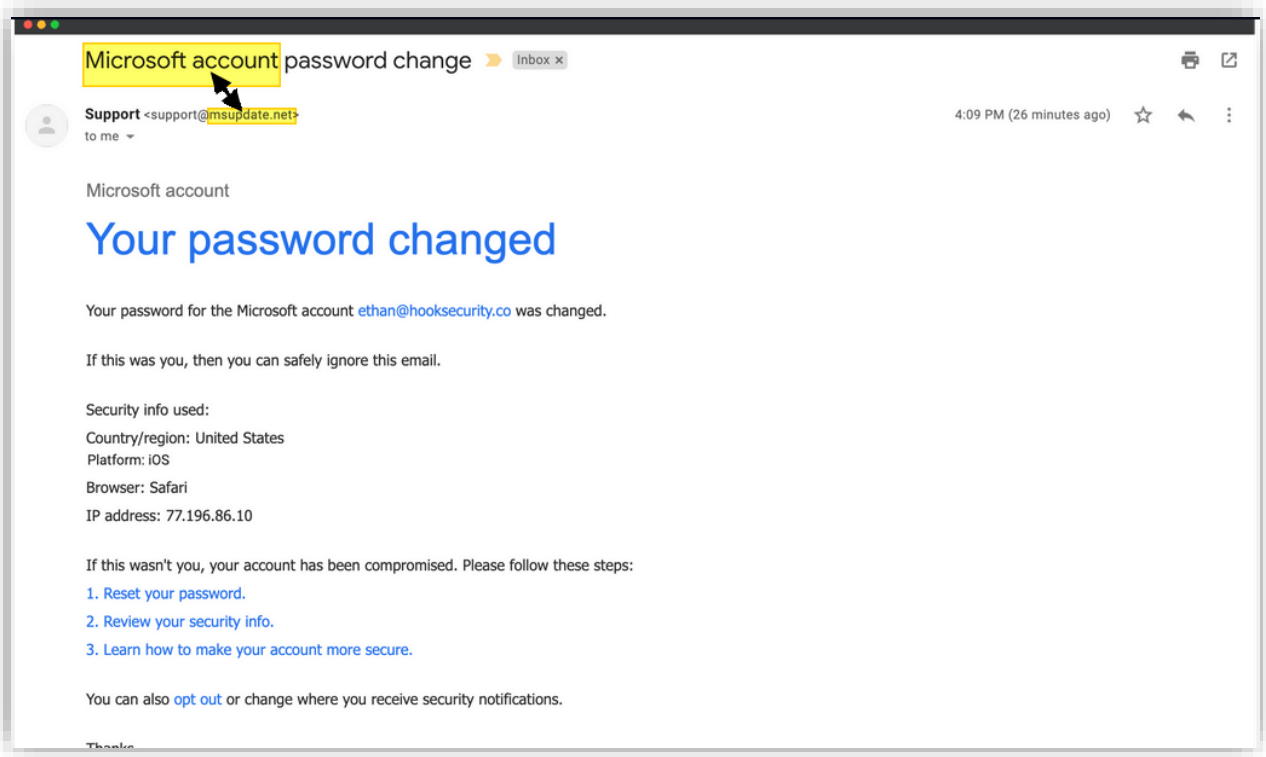
➢ اضافة الى برامج الخبيثة هناك طرق اخرى لاختراق الشبكة :

1. **الهندسة الاجتماعية Social Engineering:** الهندسة الاجتماعية هي هجوم الوصول الذي يحاول التلاعب بالأفراد لحملهم على القيام بأفعال أو الكشف عن معلومات سرية. يعتمد المهندسون الاجتماعيون غالبًا على رغبة الأشخاص في المساعدة ولكنهم أيضًا يستغلون نقاط ضعف الأشخاص. على سبيل المثال، يمكن للمهاجم الاتصال بموظف مرخص له بمشكلة عاجلة تتطلب الوصول الفوري إلى الشبكة. يمكن للمهاجم أن يستغل غرور الموظف، أو يستدعي السلطة باستخدام تقنيات ذكر الأسماء، أو يستغل جشع الموظف.

2. **اختراق كلمة المرور:** كسر كلمة مرور شبكة Wi-Fi هي عملية اكتشاف كلمة المرور المستخدمة لحماية شبكة لاسلكية.

3. **التصيد الاحتيالي Phishing:** التصيد الاحتيالي هو عندما يرسل طرف ضار بريدًا إلكترونيًا احتياليًا متنكرًا على أنه من مصدر شرعي وموثوق. والغرض من الرسالة هو خداع المتلقي لتثبيت برامج ضارة على جهازه، أو لمشاركة معلومات شخصية أو مالية. ومن أمثلة التصيد الاحتيالي إرسال بريد إلكتروني مزور ليبدو وكأنه مرسل من متجر بيع بالتجزئة يطلب من المستخدم النقر فوق رابط للمطالبة بجائزة. قد يؤدي الرابط إلى موقع مزيف يطلب معلومات شخصية، أو قد يقوم بتثبيت فيروس.

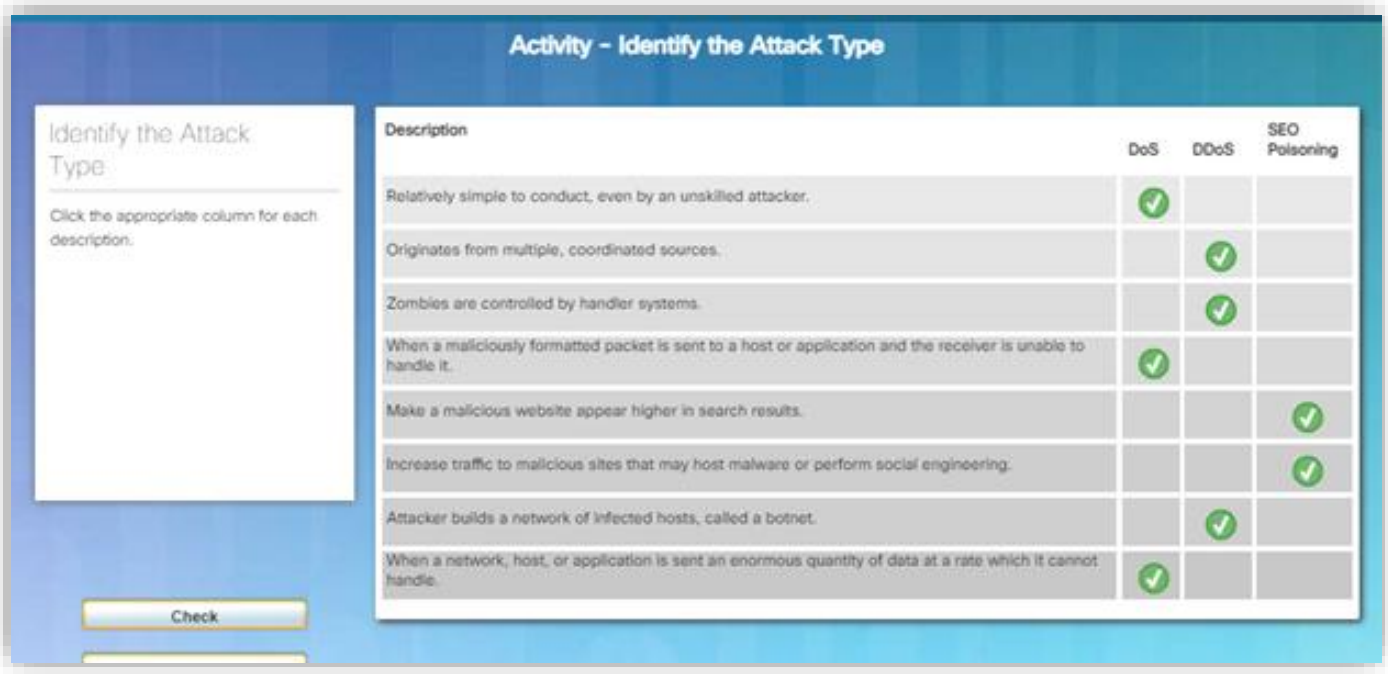




4. **استغلال الثغرات الأمنية:** يعد استغلال الثغرات الأمنية طريقة شائعة أخرى للتسلل. حيث يقوم المهاجمون بمسح أجهزة الكمبيوتر للحصول على معلومات عنها.

5. **هجمات رفض الخدمة (DoS):** هجمات رفض الخدمة (DoS) هي نوع من هجمات الشبكة. تؤدي هجمات رفض الخدمة إلى نوع ما من انقطاع خدمة الشبكة للمستخدمين أو الأجهزة أو التطبيقات.

6. **التسمم بمحركات البحث SEO Poisoning:** تعمل محركات البحث مثل Google على ترتيب الصفحات وتقديم النتائج ذات الصلة بناءً على استعلامات بحث المستخدمين. اعتمادًا على مدى صلة محتوى موقع الويب، قد يظهر أعلى أو أقل في قائمة نتائج البحث. SEO، اختصارًا لـ Search Engine Optimization، هو مجموعة من التقنيات المستخدمة لتحسين ترتيب موقع الويب بواسطة محرك البحث. في حين تتخصص العديد من الشركات المشروعة في تحسين مواقع الويب لتحسين وضعها، يمكن للمستخدم الضار استخدام SEO لجعل موقع الويب الضار يظهر أعلى في نتائج البحث. تسمى هذه التقنية تسميم SEO. الهدف الأكثر شيوعًا لتسميم SEO هو زيادة حركة المرور إلى المواقع الضارة التي قد تستضيف برامج ضارة أو تقوم بالهندسة الاجتماعية. لإجبار موقع ضار على ترتيب أعلى في نتائج البحث، يستغل المهاجمون مصطلحات البحث الشائعة.



➢ احمي بياناتك وحاسوبك:

- إبقاء جدار الحماية قيد التشغيل Firewall
- استخدم برامج مكافحة الفيروسات وبرامج مكافحة التجسس
- إدارة نظام التشغيل والمتصفح الخاص بك
- حماية جميع أجهزتك
- استخدم كلمات مرور فريدة لكل حساب على الإنترنت

➢ نصائح لاختيار كلمة مرور جيدة:

- لا تستخدم كلمات أو أسماء من القاموس بأي لغة
- لا تستخدم الأخطاء الإملائية الشائعة لكلمات القاموس
- لا تستخدم أسماء أجهزة الكمبيوتر أو أسماء الحسابات
- إذا أمكن، استخدم أحرفًا خاصة، مثل ! @ # $ % ^ & * ( )
- استخدم كلمة مرور تتكون من عشرة أحرف أو أكثر

- استخدم عبارة المرور بدلاً من كلمة المرور
  - اختر عبارة ذات معنى بالنسبة لك
  - أضف أحرفًا خاصة، مثل ! @ # $ % ^ & * ( )
  - كلما كانت أطول كان ذلك أفضل
  - تجنب العبارات الشائعة أو الشهيرة، على سبيل المثال، كلمات من أغنية مشهورة

- قوم بتشفير البيانات قبل الارسال
- قم بعمل نسخة احتياطية لبياناتك
- حذف بياناتك بشكل دائم
- المصادقة الثنائية:

• جسم مادي - بطاقة ائتمان أو بطاقة صراف آلي أو هاتف أو سلسلة مفاتيح

• مسح بيومتري - بصمة الإصبع أو بصمة اليد أو التعرف على الوجه أو الصوت

- لا تشارك كثيرًا على وسائل التواصل الاجتماعي

➢ فوائد أمان الشبكة

يعد أمان الشبكة أمرًا حيويًا في حماية بيانات ومعلومات العميل، والحفاظ على أمان البيانات المشتركة وضمان الوصول الموثوق به وأداء الشبكة بالإضافة إلى الحماية من التهديدات السيبرانية .يعمل حل أمان الشبكة المصمم جيدًا على تقليل النفقات العامة وحماية المؤسسات من الخسائر الباهظة التي تحدث نتيجة لخرق البيانات أو أي حادث أمني آخر .إن ضمان الوصول المشروع إلى الأنظمة والتطبيقات والبيانات يمكّن العمليات التجارية وتقديم الخدمات والمنتجات للعملاء.