العطاء الرقمي
Attaa Digital

# الهجمات الالكترونية و أمن شبكات الحاسب

فتحي نورالدين الفقي
أستاذ مساعد
كلية الحاسب
جامعة القصيم

العطاء الرقمي
Attaa Digital

بسم الله الرحمن الرحيم

# مقدمة

أصبحت شبكة المعلومات الإلكترونية المتصلة جزءًا لا يتجزأ من حياتنا اليومية.
تستخدم جميع أنواع المؤسسات، مثل المؤسسات الطبية والمالية والتعليمية، هذه الشبكة للعمل بفعالية.
وتستخدم الشبكة عن طريق جمع كميات كبيرة من المعلومات الرقمية ومعالجتها وتخزينها ومشاركتها.
لذلك أصبحت حماية هذه المعلومات أكثر حيوية لأمننا القومي واستقرارنا الاقتصادي.
بعد الانتشار الكبير للأنترنت والأجهزة الذكية والأجهزة المحمولة، أصبح من الضروري الانتباه للأمن السيبراني وكيفية حماية أنفسنا في الفضاء الرقمي، ابتداءً من المنزل إلى العمل وعلى مستوى الدولة ككل

# الثغرات الأمنية

**الثغرة الأمنية** هو مصطلح يطلق على مناطق ضعيفة في أنظمة تشغيل الحاسب، هذه المناطق الضعيفة يمكن التسلل عبرها إلى داخل نظام التشغيل، ومن ثم يتم التعديل فيه لتدميره نهائيا مثلا، أو للتجسس على المعلومات الخاصة لصاحب الحاسب الالي المخترق، أو ما يعرف بجهاز الضحية.

يعتبر الاستغلال مصطلح يستخدم لوصف برنامج مكتوب للاستفادة من ثغرة معروفة.

يشار الى فعل استغلال الثغرة الأمنية إلى أنه هجوم.

هدف الهجوم هو الحصول على إمكانية الوصول إلى النظام، أو البيانات التي يستضيفها أو الوصول إلى مورد معين

# البرامج الضارة

البرامج الضارة هي مصطلح شامل لكل أنواع البرامج المصممة بقصد خبيث.
غالبًا ما تكون هذه النية الخبيثة سرقة لمعلوماتك الخاصة أو إنشاء باب خلفي لجهاز الكمبيوتر الخاص بك حتى يتمكن شخص ما من الوصول إليها دون إذن منك.
البرنامج الضار هو أي شفرة يمكن استخدامها لسرقة البيانات أو تجاوز عناصر التحكم في الوصول أو إلحاق الضرر بالنظام أو تعريضه للخطر

# أنواع البرامج الضارة

**برامج التجسس**

صممت بهدف التجسس والتتبع وجمع البيانات عن المستخدم.

غالبًا ما تتضمن برامج التجسس برامج تعقب النشاطات، وجمع تفاصيل الضغط على لوحة المفاتيح وجمع البيانات. في محاولة للتغلب على الإجراءات الأمنية، تقوم برامج التجسس بتعديل إعدادات الأمان.

غالبًا ما تجمع برامج التجسس نفسها مع البرامج الشرعية أو مع فيروس حصان طروادة

# أنواع البرامج الضارة

**برامج الإعلانات المتسللة**

هي برامج ضارة صممت بهدف تقديم الإعلانات تلقائياً.

غالباً ما يتم تثبيت برامج الإعلانات المتسللة ببعض إصدارات البرامج.

بعض هذه البرامج تكون هدفها الدعاية الاعلانية فقط وبعضها يكون غطاءً مناسبًا لبرامج التجسس

# أنواع البرامج الضارة

**روبوت أو بوت**

**bot** تم اشتقاقها من كلمة robot

فهي في حقيقة الأمر برامج ضارة صممت لتقوم بتنفيذ إجراء معين بشكل أوتوماتيكي عادة عبر الإنترنت.

تنفذ مهمات ضارة، ويمكن استغلالها في الاختراق أو إرسال رسائل عشوائية أو التجسس أو مقاطعة الأعمال أو مهاجمة أي موقع إلكتروني مهما كان حجمه

# أنواع البرامج الضارة

**برامج طلب الفدية**

برامج الفدية هي نوع من البرمجيات الضارة التي يستخدمها المجرمون الإلكترونيون.

إذا تمت إصابة جهاز كمبيوتر ببرنامج فدية، يعمل ذلك الفيروس على حجب الوصول إلى النظام أو يقوم بتشفيرالبيانات الموجودة.

تنتشر برامج طلب الفدية بواسطة ملف تم تنزيله أو بعض ثغرات البرامج

# أنواع البرامج الضارة

**برنامج استغلال الخوف**

هو نوع من البرامج الضارة المصممة لإقناع المستخدم باتخاذ إجراء محدد بناء على الخوف.

يقوم برنامج استغلال الخوف بتكوين إطارات منبثقة تشبه نوافذ حوار نظام التشغيل.

تنقل هذه النوافذ رسائل مزورة تفيد بأن النظام في خطر أو يحتاج إلى تنفيذ برنامج معين للعودة إلى التشغيل العادي.

إذا وافق المستخدم على البرنامج المذكور وتم تنفيذه، فسيتم إصابة نظامه ببرامج ضارة

# أنواع البرامج الضارة

**برنامج – Rootkit**

تم تصميم هذا البرنامج الضار لتعديل نظام التشغيل لإنشاء باب خلفي.

هي نوع من البرمجيات الضارة المصممة لإعطاء المخترقين القدرة على الوصول إلى جهاز مستهدف والتحكم في محتواه.

يستخدم المهاجمون الباب الخلفي للوصول إلى الكمبيوتر عن بُعدتحصل برامج Rootkit على وصول غير مسموح به، وبعدها تفتح الباب أمام المجرمين الإلكترونيين لسرقة البيانات الشخصية والمعلومات المالية، كما تقوم بتثبيت برمجيات ضارة

# أنواع البرامج الضارة

**الفيروسات**

عبارة عن شفرة تنفيذية ضارة متصلة بملفات قابلة للتنفيذ، وغالبًا ما تكون برامج مشروعة.

تتطلب معظم الفيروسات تنشيط المستخدم النهائي

يمكن أن تكون الفيروسات غير ضارة وتعرض صورة ببساطة أو يمكن أن تكون مدمرة، مثل تلك التي تعدل أو تحذف البيانات.

تنتشر معظم الفيروسات الآن بواسطة محركات أقراص USBأو الأقراص الضوئية أو مشاركات الشبكة أو البريد الإلكتروني

# أنواع البرامج الضارة

**فيروس حصان طروادة Trojan horse**

هو برنامج خبيث يقوم بعمليات خبيثة تحت ستار العملية المطلوبة.

يقوم فيروس حصان طروادة بإرفاق نفسه بالملفات التى يتم تحميلها عبر الإنترنت

في كثير من الأحيان، يتم العثور على أحصنة طروادة في ملفات الصور والملفات الصوتية أو الألعاب.

فيروس حصان طروادة قادر على مسح وتعديل البيانات، بالإضافة إلى حجب البيانات ونسخها.

# أنواع البرامج الضارة

## الفيروسات المتنقلة Worms

هي شفرة خبيثة تقوم بتكرار نفسها من خلال استغلال الثغرات في الشبكات بشكل مستقل.

عادة ما تؤدي الفيروسات المتنقلة إلى إبطاء الشبكات.

تعمل الفيروسات المتنقلة ذاتيًا، في حين أن الفيروسات لا تعمل إلا من خلال برنامج مُضيف.

بعد إصابة المُضيف، يمتلك الفيروس المتنقل القدرة على الانتشار بسرعة كبيرة على الشبكة. كما أن لديها القدرة على إيجاد الثغرات.

# أعراض البرامج الضارة

فيما يلي أعراض البرامج الضارة الشائعة بغض النظر عن النوع الذي يصيب النظام:

البطء في سرعة الكمبيوتر.

تجمد الكمبيوتر أو تعطله في أغلب الأحيان.

البطء في سرعة تصفح مواقع الإنترنت داخل الشبكة.

المشاكل الغامضة المتعلقة بالاتصال بالشبكة.

تعديل الملفات.

حذف الملفات.

تواجد الملفات أو البرامج أو الأيقونات على سطح المكتب غير المعروفة.

هناك تشغيل يحدث لعمليات غير معروفة.

إيقاف البرامج أو إعادة تشغيل نفسها.

إرسال رسائل البريد الإلكتروني دون علم المستخدم أو موافقته.

# الهجوم الوسيط

نوع من الهجمات يقوم فيها الخصم باعتراض المراسلات بينك وبين المتلقي المقصود ثم يدعها تكمل طريقها بعد اعتراضه لها بحيث لا تتمكن أنت أو المتلقي المقصود من معرفة أن هناك "رجلاً (أو جهازاً) دخل في المنتصف بينكما".

يتم هذا الهجوم خاصة عند استخدام الشبكات العامة

يتم استخدام هجوم MitMعلى نطاق واسع لسرقة المعلومات المالية.

# التحايل باستخدام طرق اجتماعية

التحايل بطرق اجتماعية هو عبارة عن هجوم اختراقي يحاول التحكم في الأفراد للقيام بإجراءات معينة أو إفشاء معلومات سرية.
وغالباً ما يعتمد هذا التحايل على قابلية الأشخاص للمساعدة ولكنه أيضًا يستغل نقاط ضعفهم. على سبيل المثال:
قد يتصل المهاجم بموظف مسؤول بخصوص مشكلة عاجلة تتطلب الوصول الفوري إلى الشبكة.
وقد يقنع المهاجم هذا الموظف بأنه عند الرفض سيخفق في مهامه الوظيفية،
وقد يقنعه بأنه من طرف شخص ذي رتبة أعلى وظيفيًا،
أو قد يستغل طمع الموظف

# التلصص على كلمات المرور الخاصة بشبكات Wi-fi

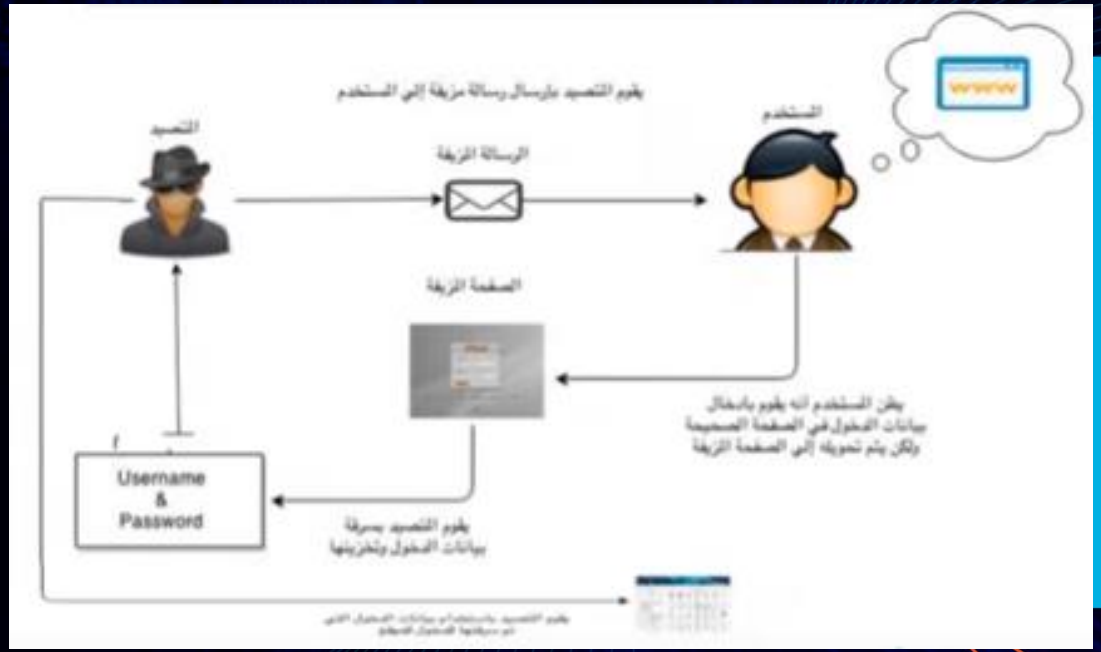
كسر كلمة مرور شبكة Wi-fi هي عملية اكتشاف كلمة المرور المستخدمة لحماية الشبكة اللاسلكية.
وفيما يلي بعض التقنيات المستخدمة في اكتشاف كلمة المرور:
التحايل الاجتماعي وهو تحايل المهاجم على الأشخاص الذين يعرفون كلمة السر للحصول عليها.
هجوم القوة الغاشمة وهو محاولة المهاجم استخدام العديد من كلمات المرور المحتملة بغرض تخمين كلمة المرور.
مراقبة الشبكة عن طريق ترقب الحزم المرسلة عبر الشبكة والتقاطها، عندها يمكن للمهاجم اكتشاف كلمة المرور إذا لم تكن مشفرة (أو بمعنى آخر إذا كانت مكتوبة كنص عادي). وإذا كانت كلمة المرور مشفرة، فقد يتمكن المهاجم من إظهارها باستخدام أداة للتلصص على كلمة مرور.

# التصيد

التصيد الالكتروني هو نوع من أنواع الجرائم الالكترونية الأكثر إنتشارا.

يعد التصيد الإلكتروني أحد أساليب الإحتيال عبر الإنترنت وذلك للحصول على معلومات شخصية أو مالية عن طريق رسائل البريد الإكتروني أو من خلال مواقع الويب.

# التصيد


يقوم التصيد بإرسال رسالة مزيفة إلى المستخدم
التصيد
الرسالة المزيفة
المستخدم
الصفحة المزيفة
يظن المستخدم انه يقوم بادخال
بيانات الدخول في الصفحة الصحيحة
ولكن يتم تحويله إلى الصفحة المزيفة
Username
&
Password
يقوم التصيد بسرقة
بيانات الدخول وتخزينها

# أخطاء شائعة تمكنك من كشف عمليات التصيد

وجود أخطاء إملائية ونحوية واضحة في رسائل التصيد

رسائل التصيد لا تشير الى المستلم

الرابط الحقيقي سوف يوجه المستخدم الى الموقع المزيف

بريد المرسل تجده مزور

تحتوي الرسالة على تهديدات قد تكون غير منطقية

# التصيد الاحتيالي

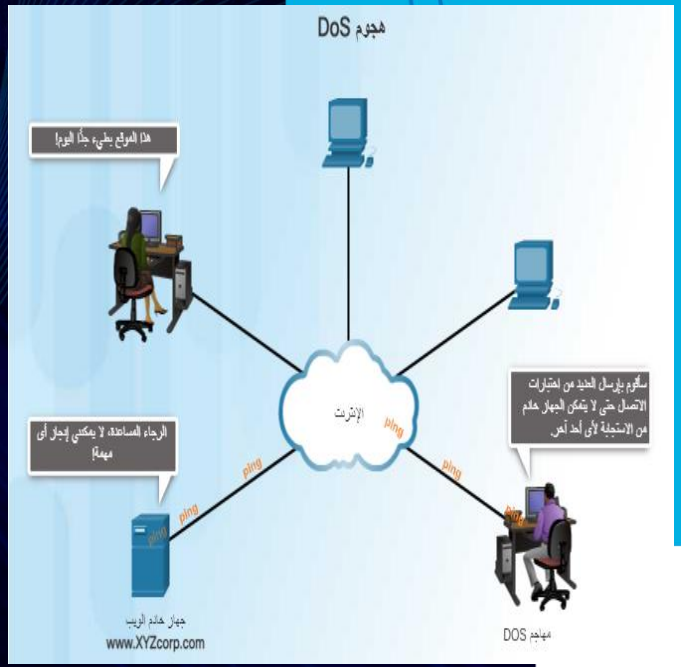
يحدث التصيد الاحتيالي عندما يرسل الطرف الضار بريدًا إلكترونيًا مخادعًا متنكراً على أنه مصدر شرعي وموثوق به.
هدف الرسالة هو خداع المستلم لتثبيت البرامج الضارة على أجهزته أو مشاركة معلومات شخصية أو مالية.
من أمثلة التصيد الاحتيالي تزوير رسائل البريد الإلكتروني لتبدو وكأنها مرسلة من متجر بيع بالتجزئة يطلب من المستخدم النقر فوق الرابط والحصول على جائزة.
وقد ينتقل الرابط إلى موقع مزيف يطلب المعلومات الشخصية، أو قد يقوم بتثبيت الفيروسات.

# DoS

**هجمات رفض الخدمة ( DoS)** هي نوع من الهجمات التي تتعرض لها الشبكة. وينتج عن هجوم DoS نوعًا من قطع خدمة الشبكة على المستخدمين أو الأجهزة أو التطبيقات.

عادة يتم تحقيق ذلك عن طريق التحميل الزائد على الهدف (غالبًا خادم ويب) بكمية هائلة من التصفح أو عن طريق إرسال طلبات ضارة تتسبب في خلل المورد المستهدف أو تعطيله بالكامل

وتشكل هجمات DoS خطرًا كبيرًا نظرًا لقدرتها على قطع الاتصال بسهولة وعلى إحداث فقد للكثير من الوقت والمال



# DDoS

هجوم رفض الخدمة الموزع ( DDoS) متشابه مع هجوم DoS ولكنه ينشأ من مصادر متعددة منسقة.

تخضع موارد الشبكة، مثل خوادم الويب، لحدود معينة لجهة عدد الطلبات التي يمكن خدمتها في آن واحد. ومتى تجاوز عدد الطلبات حدود قدرة أي مكون من مكونات البنية التحتية، من المحتمل أن يتراجع مستوى الخدمة كما يلي:

ستكون الاستجابة للطلبات أبطأ بكثير من المعتاد.

سيتم تجاهل بعض، أو كل، طلبات المستخدمين تمامًا.

# تسميم SEO

تعمل محركات البحث مثل Googleبتصنيف صفحات الويب وتقديم النتائج ذات الصلة التي تعتمد على استعلامات البحث من المستخدمين.

SEOهو اختصار لما معناه "تحسين محرك البحث"، وهي عبارة عن مجموعة من التقنيات المستخدمة لتحسين رتبة مواقع الويب عن طريق محرك البحث.

بينما تختص العديد من الشركات مصدر الثقة بتحسين مواقع الويب ووضعها في موضع أفضل، يمكن للمستخدم الضار استخدام SEO لجعل مواقع الويب الضارة تظهر أعلى في نتائج البحث. وتسمى هذه التقنية تسميم SEO

الهدف الأكثر شيوعاً من تسميم SEOهو زيادة نسبة استخدام المواقع الضارة التي قد تستضيف البرامج الضارة أو تقوم بالتحايل بطرق اجتماعية.

# التهديدات المستمرة المتقدمة

التهديدات المتواصلة المتقدمة ((APTs، هي من ضمن الطرق التي يتم الاختراق من خلالها. وهي تتكون من عملية متعددة الأنماط طويلة الأمد سرية ومتقدمة على هدف محدد.

نظراً لدرجة تعقيدها ومستوى المهارات المطلوبة، فعادة ما يتم التمويل الجيد لمثل تلك العمليات. وتستهدف APTالمؤسسات أو الدول لأسباب تجارية أو سياسية.

ويعتبر الغرض من APTهو نشر البرامج الضارة المخصصة على نظام واحد أو العديد من أنظمة الهدف والتزام التخفي، فهي غالبًا متعلقة بالتجسس من خلال الشبكة.

لا تركز على نقطة ضعف واحدة في النظام ، والتي يمكن اكتشافها بسهولة ، ولكنها تستخدم سلسلة من نقاط الضعف للوصول إلى المناطق الأمنية العالية داخل الشبكة

العطاء الرقمي
Attaa Digital

# شكراً لكم