مقدمة في الأمن السيبراني

الجزء الثالث: الهجمات

أ. د. أسامة حسام الدين

مارس 2018

المحتوى العام

- الجزء الأول: المستخدم.
- الجزء الثاني: القراصنة.
- **الجزء الثالث: الهجمات.**
- الجزء الرابع: طرق الحماية.

الهجمات

أنواع البرمجيات الخبيثة

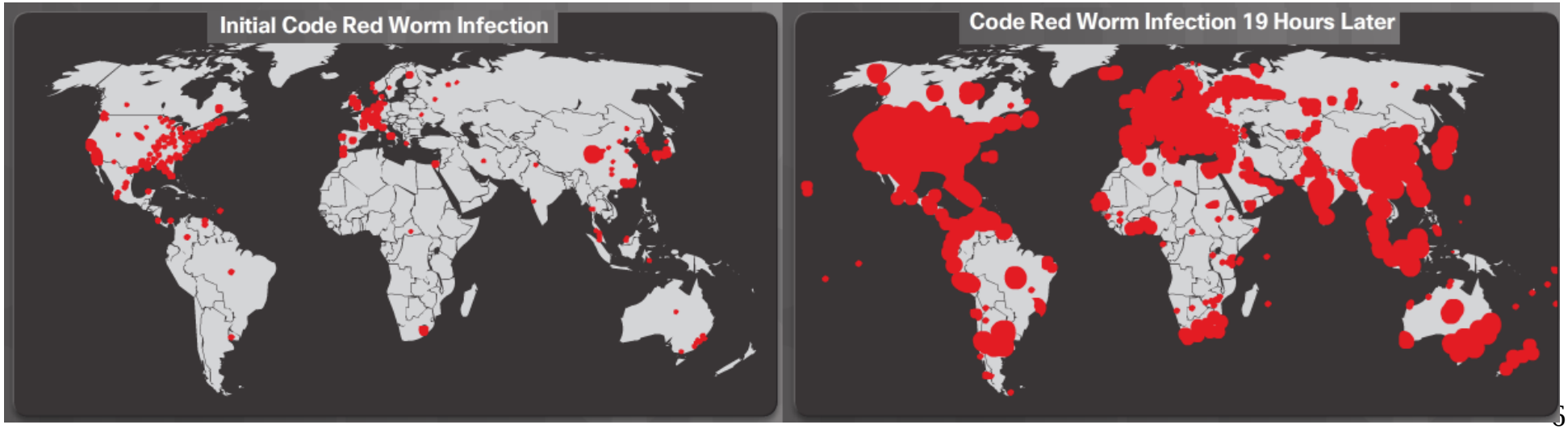
- برمجيات الدعاية والإعلان Adware.
- برمجيات التجسس Spyware.
- برمجيات الفدية Ransomware.
- برمجيات الذعر Scareware.
- **الفيروس:** يحتاج إلى عائل وسيط.
- **حصان طروادة Trojan Horse:** يدخل النظام متخفيا.
- **الديدان Worms:** تنتقل مستقلة بذاتها وسريعة الانتشار.

فيروس شمعون

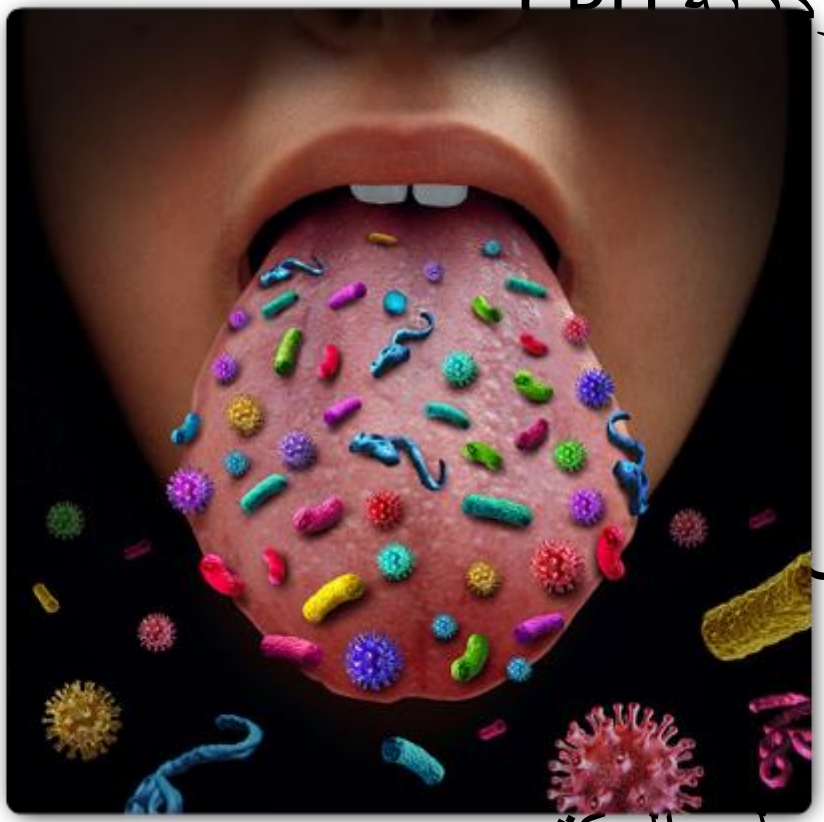
- ظهر في المملكة العربية السعودية في يناير 2017، وقد ظهر قبل ذلك في 2012عندما قام بمهاجمة شركة راس غاز القطرية
- يستهدف فيروس شمعون الحكومة الإلكترونية في المملكة بشكل أساسي بالإضافة لشركة أرامكو وشركات بترول أخرى
- ينتشر الفيروس من خلال الروابط الالكترونية في البريد المشبوه أو عبر ذاكرة الفلاش، وعندما يصل إلى شبكة الشركة أو المؤسسة الحكومية يبحث عن كل المتصلين بها ويصيبهم أيضا
- يستهدف الفيروس تعطيل جهاز الحاسب ومسح محتوياته من خلال استبدال MBR Master Boot Record او ملف الإقلاع الرئيسي بملفات أخرى من شأنها شل الجهاز تماما

دودة الشفرة الحمراء

.الديدان مسئولة عن اكبر الاختراقات على الانترنت ففي سنة 2001م دودة الشفرة الحمراء "Code Red"اصابت ما يقارب 658خادم حول العالم، وفي خلال 19ساعة فقط انتشرت لتصيب اكثر من 300000او ثلاثمائة الف خادم كما نرى في الصورة



أعراض الإصابة بالبرمجيات الخبيثة



- زيادة في استخدام وحدة المعالجة المركزية CPU.
- قلة في سرعة المعالجة لدى الحاسب.
- يتوقف الجهاز وتعطل البرامج فجأة.
- بطء في تصفح الأنترنت.
- مشكلة غامضة مع الاتصال بالأنترنت.
- يتم تعديل الملفات أو حذفها.
- ظهور برامج، ملفات أو رموز على سطح المكتب.
- عمليات غير معروفه يتم تنفيذها.
- يتم غلق البرامج أو يتم تعديل خياراتها تلقائيا.

طرق الهجمات | الهندسة الاجتماعية

- وهي الطرق والوسائل الاجتماعية المختلفة للوصول إلى الشخص وإقناعه في تنفيذ فعل ما أو الإدلاء بمعلومات سرية
- تعتمد الهندسة الاجتماعية على كون الناس بطبيعة الحال ودودين ومساعدين. وأيضا تستغل نقاط ضعفهم وقلة خبرتهم
- على سبيل المثال تتلقى اتصالا هاتفيا من شخص يتظاهر انه موظف بالبنك وأن هناك ضرورة ملحة للدخول إلى حسابك لإجراء بعض الإصلاحات، فتثق به وترسل له معلوماتك الشخصية
- استثارة الغرور لدى الشخص بتفخيمه والتعظيم من شأنه وذكره بما يحب حتى يعطي الثقة
- وأيضا يمكن الدخول من مدخل الطمع لدى الأشخاص في المال

أنواع الهندسة الاجتماعية

.التستر Pretexting: وفيها يتم الاتصال بالضحية والكذب عليه كمحاولة لجلب معلوماته السرية .كمثال المهاجم الذي يتظاهر انه يريد معلومات شخصية أو مالية من الشخص للتأكد من هويته.

.التتبع الظهري :Tailgating وفيه يتم تتبع الأشخاص والسير في ظلالهم ومحاولة الولوج معهم إلى الأنظمة دون تصريح.

.شيء مقابل شيء : Something for Something وفي هذا النوع يطلب المهاجم معلومات شخصية مقابل هدية أو بطاقات خصم على البضائع.

طرق الهجمات | محاولات كشف الأسرار

.هجمات التخمين الغاشم Brute-Force attacks: يتم ذلك باستخدام برامج مخصصة لذلك تسمى Dictionary Attack Software

.غربلة الشبكة :وفيها يتم التصنت على المحادثات في الشبكات السلكية واللاسلكية ومن الممكن التقاط كلمات السر ببساطة إن تم تراسل كلمة السر بلا تشفي

.الخداع :**Phishing**وفيها يرسل المهاجم رسالة بريد إلكتروني مدعيا أنها من مصدر موثوق .والرسالة تقنع المستقبل وتكسب ثقته فيتم انزال برنامج خبيث على جهازه

.الخداع الرمحي : **Spear Fishing**هو نوع من الخداع ولكنه مركز على شخص بعينه . ويصل أيضا إلى الضحية عن طريق رسائل البريد الالكتروني .ولكن في هذه الحالة يتم دراسة الشخص ومعرفة ميوله من خلال الشبكات الاجتماعية

هجمات التوسط بين المتصلين

- **هجمات الرجل كوسيط** Man in the Middle attack : وفيها يستطيع المهاجم أن يسيطر على جهاز الحاسب دون علم صاحبه)الضحية (بذلك .ويقوم بالاستيلاء على المراسلات التي يخرجها الضحية من جهازه)كأن يخرج بيانات بطاقة الائتمان لموقع أمازون للشراء .(ثم يأخذ تلك المعلومات ويراسل هو بنفسه المواقع الخاصة بالضحية كحسابه البنكي أو مواقع الشراء ويسحب من رصيد البطاقة الائتمانية الخاصة بالضحية.
- **هجمات الرجل في الجوال** Man in Mobile Attack : وهي نسخة أخرى من هجمات الرجل كوسيط وفيها يتم السيطرة على جهاز جوال بإنزال برامج خبيثة عليه لتراسل المعلومات السرية .كمثال برنامج ZeuS يمكن المهاجمين من التقاط نظام التحقق verification باستخدام الرسائل النصية وإرساله إلى المستخدم.

الهجمات الدائمة المتقدمة

Advanced Persistent Threats

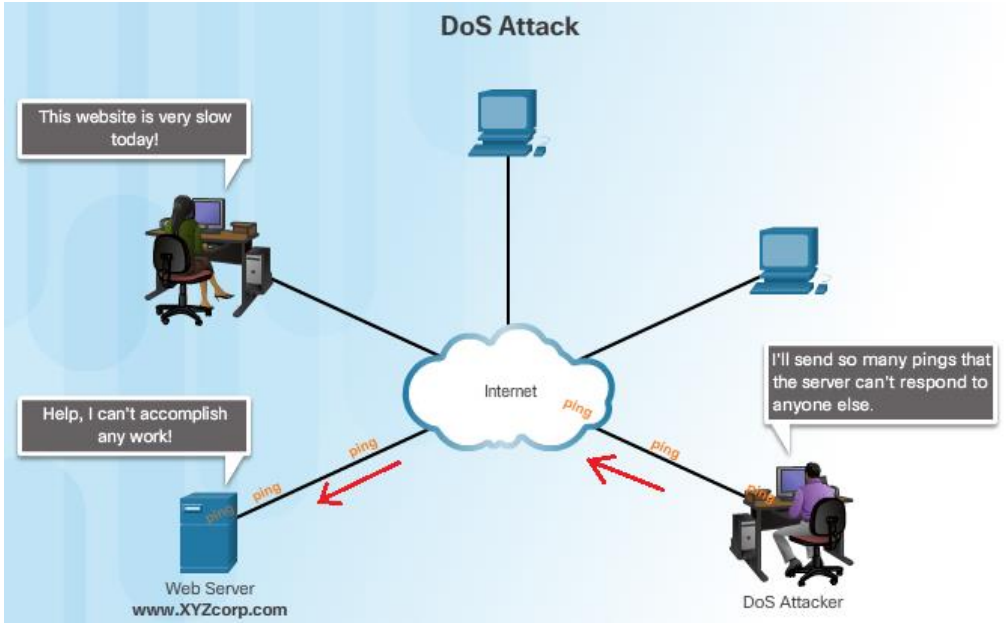
- تتم على أكثر من مرحلة، بخطط طويلة المدى، بشكل خفي، مهاجمة لهدف معين
- نظرا لدرجة التعقيد بها ولارتفاع المستوى المهاري فيها فإنها تكون دائما ممولة من قبل مؤسسات أو حكومات لأهداف سياسية.
- وعادة ما ترتبط الهجمات المتقدمة بالتجسس الشبكي، وفيها يتم نشر برامج خبيثة إلى جهاز أو أكثر بشكل سري.
- لا يمكن أن تكون من قبل فرد واحد وإنما من مجموعة من الأفراد (عصابة)

هجمة قطع الخدمة DoS

نوع من الهجمات الشبكية وينتج عنها تعطيل خدمات الشبكة.

الإغراق بالطلبات :وفيها يتم إغراق الخادم بالطلبات)المسموحة (بقصد شغل الخادم وتعطيله عن التجاوب مع المستخدمين الأبرياء

الحزم المعدلة: يقوم المهاجم بتمرير حزم بها أخطاء لا يمكن اكتشافها بالتطبيقات فيحاول التطبيق العثور على الخطأ ويأخذ وقت طويل لمعالجة كمية كبيرة من الحزم لاكتشاف الخطأ،



الهجمة الموزعة لقطع الخدمة DDoS

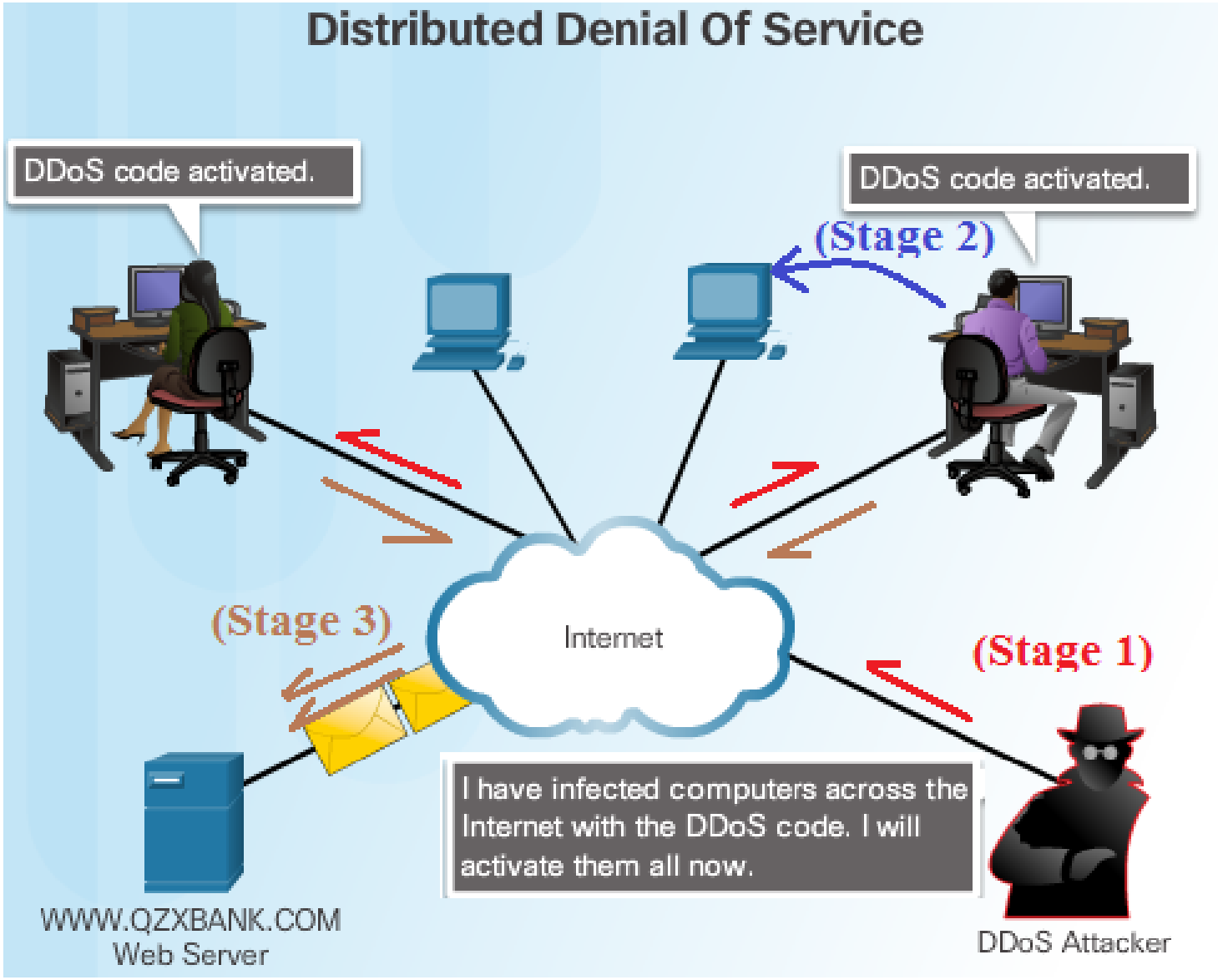
الهجمات الموزعة لقطع الخدمة شبيهة إلى حد ما بهجمات قطع الخدمة العادية إلا أن الموزعة تصدر من أكثر من جهاز موجه نحو الضحية

مرحلة التهيئة :يقوم المهاجم بإنزال برنامج خبيث للهجوم الموزع، يثبته على أكثر من جهاز حول العالم)دون علم أصحابها (ويعمل شبكة تسمى شبكة الروبوت .وتسمى الأجهزة المسخرة في هذه الحالة)**الزومبي** .(ويتم التحكم في الزومبي من خلال جهاز مركزي مثبت عليه البرنامج الرئيسي الذي ينظم الهجمات الموزعة.

مرحلة العدوى :تقوم حاسبات الزومبي بصفة دورية بمسح وإصابة أجهزة جديدة، لخلق حاسبات زومبي جديدة .وتسيطر على الزومبي الجديد نفس الجهاز المركزي.

مرحلة الهجوم الموزع :عندما يحين الوقت المناسب يقوم المهاجم بإصدار التعليمات للجهاز المركزي بالبدء بالهجوم الموزع فيتبعه جميع حاسبات الزومبي ليكون هجوما ضاريا.

الهجمة الموزعة لقطع الخدمة DDoS



تسمم المتصفح SEO Poisoning

.تعمل محركات البحث مثل جوجل من خلال ترتيب الصفحات حسب أهميتها .فعندما يطلب المستخدم كلمة مفتاحية فإن الصفحات الأعلى أهمية تظهر في بداية نتائج البحث وتظهر الصفحات الأقل أهمية تباعا

.قد يصير الموقع الإلكتروني لشركة ما ذات أهمية بتحسين أهميته وترقيته ليظهر كنتائج أولى عند البحث.

.يتم هذا بشكل شرعي أو يتم بشكل غير شرعي بأن يقوم المهاجم بوضع صفحة ويب خبيثة ويضع فيها الكلمات المفتاحية التي يطلبها الناس أكثر بغرض ظهورها كنتائج أولى في محركات البحث،

.كمثال كلمة "التخسيس "أو كلمة "الجنس "ويسمى

هذا النوع من الهجوم "تسمم نتائج البحث".

الهجمات الخليطة

.هي هجمات منظمة تستخدم اكثر من تقنية لتقويض هدف معين .وبإستخدام أكثر من تقنية للهجوم.

.كثير من الهجمات الخليطة تستخدم رسائل البريد المزعج، رسائل الدردشة، أو حتى مواقع الإنترنت لدمج الروابط بها والتي عند الضغط عليها يتم انزال البرمجيات الخبيثة إلى الحاسوب.

.تستخدم أنواع أخرى من الهجمات المختلطة نظم الهجمات الموزعة لقطع الخدمة (DDoS) مقترنة مع هجمات الخداع برسائل البريد الإلكتروني.

.فعلى سبيل المثال تستخدم الهجمات الموزعة في تعطيل الموقع الإلكتروني للبنك وترسل بريد إلكتروني للعملاء للاعتذار عن الإزعاج بسبب العطل. وتوجه الرسائل الإلكترونية العملاء لموقع مزيف لإدخال معلوماتهم الشخصية فيتم سرقتها على الفور.

الهجمات الخليطة

- الهجمات المدمرة المشهورة مثل نيمدا، CodeRed, BugBear, Kelz كلها هجمات بطابع خليط.
- على سبيل المثال تستخدم ديدان نيمدا خليط من مرفقات البريد الإلكتروني وتحميل الملفات من موقع مهاجم (بفتح الجيم)، أو مشاركات الملفات كطرق للانتشار. ونسخ أخرى من ديدان نيمدا تقوم بتعديل حساب الضيف Guest Account الموجود افتراضيا في ويندوز لتعطي من خلاله صلاحيات أعلى للمهاجم أو للبرمجية الخبيثة.
- من الديدان الحديثة دودة كونفيكر (Conficker) و زيوس (ZeuS/LICAT) وتستخدم ديدان كونفيكر كل الطرق التقليدية في الانتشار.

الحد من الأثر

لا توجد تدابير أمنية محددة تحل المشاكل بنسبة 100%.

<u>بعض المعايير للشركات التي يجب أن تضعها في الاعتبار بخصوص الاختراقات الأمنية</u>

- قم بإخبار الجميع عن الهجوم أو الشك في حدوث الهجوم.
- اعط تفاصيل أكثر، اشرح لماذا حدثت المشكلة وما هو الذي تم تقويضه أو الوصول إليه.
- حاول فهم السبب وراء الهجوم ومن سهل له. وإذا دعت الضرورة قم بتأجير الخبراء في مجال التحاليل الجنائية لتقصي وتحليل المشكلة.

سؤال ؟