الجذور الخفية ROOTKITS

تعريف Rootkits ؟

هو برنامج خفي يخفي نشاطات المخترق داخل النظام و يسمح للمخترق الدخول الكامل على الخادم او النظام أي وقت في المستقبل

يمكن لبرنامج Rootkits باستبدال برامج النظام الأساسية إلى برامج معدلة تعمل عند تشغيل النظام لتساعد في تشغيل البرمجيات الخبيثة

من الأمثلة عليها : backdoor, DDoS, Packet Sniffers, log-wiping

الجذور الخفية ROOTKITS

يمكن تفعيل Rootkit في النظام عن طريق

- فحص النظام أو الخادم في الويب عن ثغرات
- دمج Rootkits برنامج في لعبة او برنامج عادي مشهور
- تثبيته في الحواسيب بالأماكن العامة عن طريق الهندسة الاجتماعية
- تفعيل Zero Day Attack

أهداف Rootkit في النظام

- فتح قناة اتصال في النظام للدخول الدائم للنظام عبر backdoor
- يخفي نشاطات وتحركات المخترق في النظام
- يجمع بيانات حساسة و نشاطات وسجلات داخل الشبكة من النظام لتفيد المخترق في تسهيل الدخول
- يثبت الكثير من البرمجيات الخبيثة في النظام او الخادم و يحدثها باستمرار

أنواع الجذور الخفية ROOTKITS

Hypervisor Level Rootkits	Hardware/Firmware Rootkits	Kernel Level Rootkits
Boot Loader Level Rootkits	Application Level Rootkits	Library Level Rootkits

عند تشغيل نظام

BIOS

MBR

هنا يمكن ان يتم تثبيت الـ rootkit

عند تشغيل الجهاز لا يتم مسح القرص لأنظر MBR

التعرف على الجذور الخفية ROOTKITS

Integrity-Based Detection	Signature-Based Detection	Heuristic/Behavior Based Detection	Runtime Execution Path Profiling	Cross View-Based Detection
مقارنة ملفات النظام وسجلات التشغيل والذاكرة بملفات نظام موثوق	عملية مقارنة النظام والملفات التشغيلية مع قاعدة بيانات بصمات وتحركات الجذور الخفية	ملاحظة تغير في سلوك النظام.	مقارنة مسارات تشغيل النظام قبل وبعد دخول الـ Rootkits	مقارنة الملفات المعتادة مثل ملفات النظام مع الخوارزميات التي تشغل عادة نفس معطيات ملفات التشغيل

Tools

إخفاء البيانات في الصور

أداة QuickCrypto

تستخدم أداة quickcrypto لإخفاء النصوص في الصور بحيث ان فقط المستخدم لهذه الأداة يستطيع معرفة فك هذه الصورة والتعرف على البيانات السرية المدمجة في الصورة.

QuickCrypto

http://quickcrypto.com/

إخفاء البيانات

Tools:

معنى Steganography (إخفاء المعلومات) ؟

علم اخفاء البيانات علم كتابة رسائل مخفية بطريقة لا يمكن لأحد، عدا المرسل والمستلم المعني، وهو نوع من السرية من خلال الغموض.

مثال:

قد يستخدم شخص ما صورة الكترونية لنقل رسائل نصية (أو حتى صور مخفية) إلى شخص آخر دون أن يعلم أحد. فكل من ينظر من الخارج يظن أن الشخصين يتبادلان صورا، بينما هذه الصور محملة برسائل مخفية غير واضحة.

```
> steghide embed -cf pic.jpg -ef file.txt
```

```
> steghide extract -sf pic.jpg
```

إخفاء البيانات في المستندات

أداة wbStego

تستخدم أداة wbStego لإخفاء النصوص في المستندات بحيث ان فقط المستخدم لهذه الأداة يستطيع معرفة فك هذه المستندات والتعرف على البيانات السرية المدمجة في المستند.

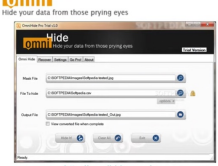
http://wbstego.wbailer.com/

اخفاء البيانات

إخفاء البيانات

برنامج omni Hide يسمح للمستخدم اخفاء البيانات داخل الصور والفيديو والصوتيات والمستندات.

والملف بعد الدمج يكون شكله تماما مثل شكل الملف الاصلي بدون اي اختلاف



http://omnihide.com/

* for android
  - steganography master
  - stegais

linux trick:
add . before any file
> mv Test .Test