Rootkits (User Mode)

ماهي ال Rootkit :

عندما يقوم الHacker باختراق جهاز ما سيبدأ بجمع المعلومات عن الهدف و المكان الذي يتواجد فيه الهدف و نوع نظام التشغيل وبعدها يبدأ بفحص منافذ الجهاز ليحدد المنافذ المفتوحة او المغلقة والخدمات Services التي تعمل على هذه المنافذ ,عندها تبدأ مرحلة الحصول على الShell (في أنظمة Windows يكون الهدف الحصول على CMD اما أنظمة Unix يكون الهدف هو الحصول على الShell) وتتم هذه المرحلة بعدة طرق: اما من خلال استغلال ثغرة (ضمن الServices العاملة على جهاز الهدف او نظام التشغيل نفسه) او من خلال الهندسة الاجتماعية حيث يتحايل المهاجم على الهدف لإيصال الBackdoor وتنفيذه ضمن نظام الهدف او من خلال هجوم Brute Force .

وعندما يتم تشغيل الBackdoor بإحدى الطرق السابقة ويحصل المهاجم على صلاحيات معينة ضمن النظام الهدف ,عندها يكون الBackdoor معرض للكشف من خلال Antivirus والتحديثات المستمرة التي يتلقاها او في حال كان الهدف(المستخدم) خبير نوعا ما ووجد Process مريبة تعمل بالخلفية عندها سيتم تحليل هذا Backdoor ويتم الوصول لعنوان المهاجم والقاء القبض عليه او ببساطة سيتم التخلص من الBackdoor ,وبالتالي قد يكون هذا الاختراق كلف المهاجم ساعات بل أيام من التخطيط والمحاولات للوصول للنظام فضلا عن الخوف من تعقب عنوان الIP والوصول اليه , هنا تكمن أهمية الRootkit في تثبيت ال Backdoor ضمن النظام وجعله مخفيا من خلال استخدام API نظام التشغيل والاستفادة منها لتضليل أنظمة الحماية والمستخدم ولتخدم بقاء وتثبيت الBackdoor ضمن النظام لأطول فترة ممكنة.

الRootkit : هي مجموعة من الأدوات (*tools: scripts, configuration files, binaries*) والتي تسمح للمهاجم إخفاء نشاطاته على جهاز الهدف وبتالي اصبح بإمكان المهاجم التحكم ومتابعة العمليات ضمن جهاز الهدف, ان الRootkit المصمم بشكل متقن وصحيح سيمنع انهيار النظام والتضاربات التي قد تحدث نتيجة الاستخدام الخاطئ لدوال النظام.

ان تنزيل وتنصيب الRootkit يأتي مباشرة بعد الحصول على Shell.

الRootkit ليست تكنولوجيا خبيثة بحد ذاتها لكن يمكن استخدامها من قبل البرامج الخبيثة.

ان فهم تقنية Rootkit أمر حساس وبالغ الأهمية للدفاع ضد الهجمات الحديثة .

Rootkit تزود بوظيفتين أساسيتين :

- اصدار الأوامر وتنفيذها : يمكن أن تتضمن التحكم بالملفات ، والوصول إلى موجه الأوامر .
- التنصت: على سبيل المثال التقاط الرزم وضربات المفاتيح وقراءة البريد الإلكتروني .

يمكن للمهاجم أن يستخدم هذه التقنيات لالتقاط كلمات المرور وفك تشفير الملفات .

الاستخدامات المشروعة لRootkit:

يمكن استخدام الRootkit لأغراض مشروعة ،على سبيل المثال يمكن استخدامها من قبل الهيئات القانونية والمنظمات لجمع الأدلة وعمليات الحفاظ على الامن من التهديدات المحتملة .

يمكن أيضاً استخدام الRootkit لمكافحة الحروب والتخفيف من أضرارها ، فالدول وجيوشها تعتمد بشكل كبير على الحواسيب في عملها ,وإذا فشلت هذه الحواسيب فإن ذلك سيؤثر على قرارات وعمليات الدولة العدو .

الفوائد من استخدام الحاسوب للهجوم يتضمن كلفة الهجوم ستكون أقل و الحفاظ على الجنود بعيداً عن الخطر فهو يسبب القليل من الأضرار الجانبية .

كيف تعمل الRootkit:

الRootkit معدة لكي تقوم بإخفاء الملفات والعمليات (processes) ومدخلات الRegistry والاتصالات الشبكية وامور أخرى عن المستخدم . ولكي يتم ذلك يجب على الRootkit ان تعدل الCode الخاص ببرنامج ما او مكتبة نظام (System Library) لكي يعيدوا نتائج خاطئة على سبيل المثال (قائمة العمليات (Processes List) المعادة من برنامج ال Task Manager التي تخفي عدد من الprocesses) .

في هذه الدراسة سنتناول الRootkit المخصصة لUser Mode (Ring3) ولن نتطرق الى Kernel Mode (Ring0) كون الإصدارات الحديثة من نظام ويندوز (10 – 8.1) جعلت من المستحيل عمليا التعديل على بنية النواة .

مكونات الRootkit:

وبعكس المتوقع فأن بنية الRootkit بسيطة ,حيث تتكون من برنامج يقوم بالتعديل الCode لProcess أخرى ويقوم بمتابعة الProcesses المنشأة حديثا .

وتحوي على مجموعة من دوال النظام للتعديل واستبدال الدوال الاصلية للنظام .

بعض الأمثلة عن Rootkit:

- **Blue pill** : من اكثر الRootkit تعقيدا وتقدما تستفيد من تقنية الVirtualization ومن الصعب جدا كشفها
(مستخدما تقنية AMD Virtualization Technology Pacifica) .

- **Fu Rootkit:** Rootkit من نمط Kernel Mode تعتمد على تقنية DKOM(Direct Kernel Object Manipulation) .

- **Vanquish Rootkit**: من نمط User Mode تعتمد على تقنية حقن المكتبات (DLL Injection) و API Hooking .*(هذا النمط الذي سيتم دراسته خلال المشروع)*

متطلبات المشروع:

كل البرامج والأكواد ستكون بلغة C++ (لسهولتها ومرونتها في التعامل مع الدوال المنخفضة المستوى Low Level Functions) .

بعض المعرفة بأساسيات لغة Assembly و دوال نظام التشغيل الأساسية (WinAPI 32).

وسيتم تجريب كل وظيفة من وظائف الRootkit على حدا على نظام " Windows 7 32bit".

سيتم في هذا المشروع مناقشة :

1. اهم وظائف الRootkit وكيفية عملها :
   - إخفاء العمليات (Hiding Process).
   - إخفاء الملفات والمجلدات (Hiding files and directories).
   - إخفاء مدخلات الRegistry(Hiding registry entries).
   - انشاء Backdoor و Key Logger .
   - انشاء وحدة تحكم عن بعد (Remote console)
   - تخطي الجدار الناري (Bypassing the Firewall)
2. مميزات الأمان في أنظمة Windows .
3. انشاء تطبيقات غير قابلة للكشف من قبل مضادات الفايروس(Undetectable application).
4. كيفية كشف الRootkits والحماية منها .

اهم المراجع :

الكتب :

- "Rootkits: Subverting the Windows Kernel": Greg Hoglund, James Butler.
- "Windows NT/2000 Native API Reference": Gary Nebbett.

المدونات :

- https://www.malwaretech.com/2013/09/ring3-ring0-rootkit-hook-detection-12.html
- https://arvanaghi.com/blog/dll-injection-using-loadlibrary-in-C/
- https://www.codeproject.com/Articles/11777/InjLib-A-Library-that-implements-remote-code-injec
- https://www.codeproject.com/Articles/32744/Driver-to-Hide-Processes-and-Files