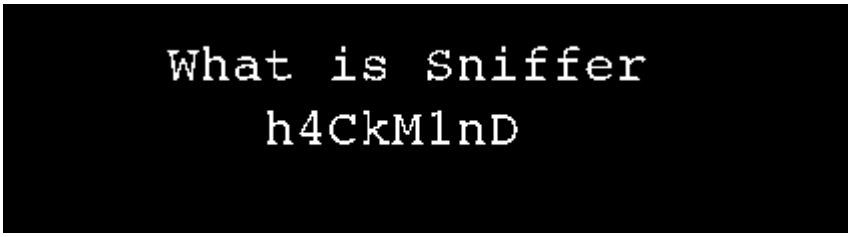


Author : rOCkHuntEr
Title : Introduction Sniffer
Contact : r0ck.hunt3r@gmail.com
Gr33tz : A4s . S4A . h4CkM1nD

ماهو السنايفر

يسمى سنايفر بشكل عام ويسمي Packet Sniffer على وجه الخصوصية

يستخدم السنايفر في بيئة عمل الشبكات ويهتم في جمع والتقاط الحزم ضمن هذه البيئة

وما يميز السنايفر وادواته هية القدرة على تحليل الحزم الممرة داخل الشبكة والقيام بتحليل البروتوكولات المستخدمة مما يجعل بمقدوره عرض هذه الحزم
على شكل مبسط او ما يسمى plan text

وهنالك نقطة مهمة جدا ذكرنا سابقا انه يقوم بعرضها بشكل مبسط ولكن مالم تكن هذه الحزم مشفرة

وقدرة عمل السنايفر ليست محدودة بلاجهزة التي يتم تشغيلها فقط بل هية تشمل جميع الاجهزة التي تعمل على شبكة واحدة ليتم بعد ذلك التقاط اي باكيت يمرر من خلال هذه الاجهزة المترابطة مع بعضها البعض

يعتقد الكثيرون ان السنايفر يستخدم فقط في عملية الهجوم بل ان هنالك اعمال كثيرة من الممكن الاستفادة منها من النواجي الامنية ومن ناحية مدراء الشبكات

بماذا يستخدم السنايفر

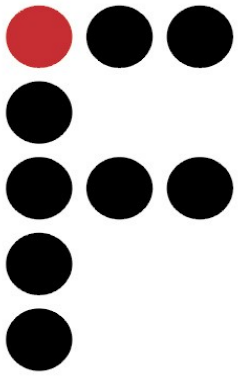
اولا : للحصول على كلمات المرور والبيانات السرية التي تمرر من خلال الشبكة ليتم بعد ذلك تحليلها وعرضها بشكل مبسط

ثانيا : يساعد السنايفر في تحليل وقراءة الحزم الممرة فالحزم قبل تحليلها او قرائتها من خلال اي برنامج لعمل السنايفر تبقى بيانات وهمية ويقوم السنايفر بتحليل هذه البيانات وعرضها بشكل موضح تسمح للمستخدم بفهم هذه البيانات

ثالثا : يساعد السنايفر في حل مشاكل الشبكات ومراقبتها ومعرفة مستوى ادائها عن طريق بعض الحزم المتعلقة بذلك كحزم ICMP/IGMP/SNM تحليل

رابعا : يساعد في الكشف عن محاولات التطفل عن طريق تحليل الحزم ويقصر ذلك على انظمة التطفل التي تعمل تحت بيئة IDC

خامسا : الأطلاع الكامل على سريان البيانات وتناقلها ضمن الشبكة او ما يسمى logging



ماهية طبيعه عمل السنايفر

تبدا العملية بالبدء بعملية هجوم او فحص او اختبار لشبكة ما باستخدام اداة ما تقوم بهذه العملية وعلى سبيل المثال اداة WireSharK

تبدا بأختيار نوع الاتصال المراد الهجوم عليه . وبعد ذلك تبدا بألتقاط الحزم او الباكيت الممر عبر هذه الشبكة نأتي للمرحلة الثانية وهية مرحلة التحليل ليتم على ذلك تحليل هذه الحزم ليتم بعد ذلك فحصها وتنقسم الحزم لطبقات

الأول : الترويسة
الثاني : الايبي
الثالث : هو ال TCP
الرابع : هو ال UDP
خامسا : في هذه المرحلة نصل للبيانات الحقيقة

في الطبقة الأولى او ما يسمى الترويسة تكون كمية البيانات والداتا فيها كثير بشكل كبير جدا وتمشل نوع البروتوكول ومصدر الحزمة وجهتها والمنفذ المستخدم ويمكنك ايضا معرفة النظام المستخدم

بعد ذلك نأتي للنقطة الأخير وهية التي نبحث عنها لأنهاء هذا الهجوم وهية حل رموز حزم البيانات وعرضها بشكل مبسط كما ذكرنا سابقا على شكل Plan Text

ويختلف عنها نوع العرض مشفر او غير مشفر وتختلف كذلك انواع التشفيرات ليتم بعد ذلك المرحلة الاخيرة فك التشفير والحصول على البيانات المطلوبة

rOcKHuntEr