



المقال الأسبوعي لنادي الأمن السيبراني

Wireshark

Wireshark هو برنامج قوي ومفتوح المصدر يُستخدم على نطاق واسع كمحلل بروتوكولات الشبكات، يسمح لمستخدمي الأمن السيبراني ومديري الشبكات والمهتمين بالشبكات بالتقاط وفحص وتحليل حركة الشبكات في الوقت الحقيقي. يوفر فهماً عميقاً للاتصالات الشبكية، مما يساعد في تحديد المشكلات الأمنية وحل مشاكل الشبكة وتحسين أدائها. في هذه المقالة، سنتناول مميزات المميزة، ومزاياه، وعيوبه، وأهميته.

مميزات Wireshark:

- استخلاص الحزم (Packet Capturing): يستطيع Wireshark التقاط وعرض الحزم من مجموعة واسعة من واجهات الشبكة، بما في ذلك الإنترنت، واي فاي، وواجهة الحلقة المحلية (loopback).
- دعم البروتوكولات: يدعم مجموعة واسعة من البروتوكولات الشبكية، مما يجعله قادراً على تحليل حركة الشبكة على مختلف الطبقات الشبكية، من الطبقة الفيزيائية إلى الطبقة التطبيقية.
- فلاتر قوية: يقدم Wireshark قدرات تصفية مرنة للتركيز على الحزم الخاصة بالمواضيع المحددة، مما يوفر الوقت والموارد أثناء التحليل.
- واجهة المستخدم الرسومية (GUI): يتيح واجهة المستخدم السهلة الاستخدام للمستخدمين تصفح وتفسير البيانات الشبكية المعقدة بكفاءة.
- التقاط مباشر وتحليل دون اتصال: يمكن للمستخدمين إجراء التقاط مباشر للحزم أو تحليل ملفات التقاط الحزم المسجلة مسبقاً.
- خيارات عرض متنوعة: يوفر Wireshark تمثيلاً بصرياً متنوعاً، مثل الرسوم البيانية الخطية والرسوم الدائرية، لتصور الإحصائيات.
- دعم فك التشفير: يستطيع فك تشفير حركة الشبكة المشفرة إذا توفرت مفاتيح التشفير المطلوبة.
- مجانية ومفتوحة المصدر: Wireshark متوفر بشكل مجاني، مما يجعله متاحاً لجمهور واسع ويساهم في تشكيل مجتمع قوي من المستخدمين والمساهمين.
- توافق متعدد المنصات: يتوفر Wireshark على أنظمة التشغيل المتعددة، بما في ذلك ويندوز وماك ولينكس، مما يعزز مرونته.
- تحليل شامل: يوفر دعمه لمجموعة واسعة من البروتوكولات تحليلاً مفصلاً لسلوك الشبكة، مما يساعد في اكتشاف الشذوذ والتهديدات الأمنية.
- أداة تعليمية: يعتبر Wireshark أداة تعليمية ممتازة للطلاب وهواة الشبكات لتعلم بروتوكولات الشبكة وسلوكها.
- دعم المجتمع: بفضل مجتمع المستخدمين النشط، يستفيد Wireshark من تحديثات منتظمة وإصلاحات للأخطاء وتحسينات للميزات.



المقال الأسبوعي لنادي الأمن السيبراني

Wireshark

سلبيات Wireshark:

- استهلاك الموارد: تحليل التقاط الحزم الكبير قد يتطلب استهلاك موارد الجهاز والذاكرة الكبير.
- انحدار تعليمي حاد: بالنسبة للمبتدئين، قد يكون فهم وتفسير البيانات الشبكية تحديًا، مما يتطلب وقتًا للتعلم.
- مخاوف الخصوصية: يمكن أن يقوم Wireshark بالتقاط معلومات حساسة، مثل كلمات المرور والبيانات الخاصة، إذا تم استخدامه بدون احتراس أو بشكل غير أخلاقي.
- اعتبارات قانونية وأخلاقية: قد ينتهك التقاط حركة الشبكة بدون ترخيص القوانين الخصوصية والمبادئ الأخلاقية.

أهمية Wireshark:

Wireshark يلعب دورًا حيويًا في أمان الشبكات وحل مشاكلها:

- إصلاح الشبكة: يساعد في تشخيص مشاكل الشبكة، مثل احتكار الشبكة والتأخير وسوء التكوين.
- تحليل البرمجيات الخبيثة: يستخدم Wireshark لتحليل سلوك البرمجيات الخبيثة واكتشاف الأنشطة الضارة وتحديد الأنظمة المصابة.
- كشف الاختراق: من خلال دراسة أنماط حركة الشبكة، يساعد في اكتشاف الأنشطة المشبوهة أو غير المصرح بها.
- التدقيق الأمني: يساعد في إجراء التدقيقات الأمنية لتحديد الثغرات والضعف في بنية الشبكة.
- تطوير وتصحيح البروتوكولات: يساعد مطوري البرمجيات في تصحيح أخطاءهم والتحقق من صحة بروتوكولات الشبكة وتطبيقاتها.