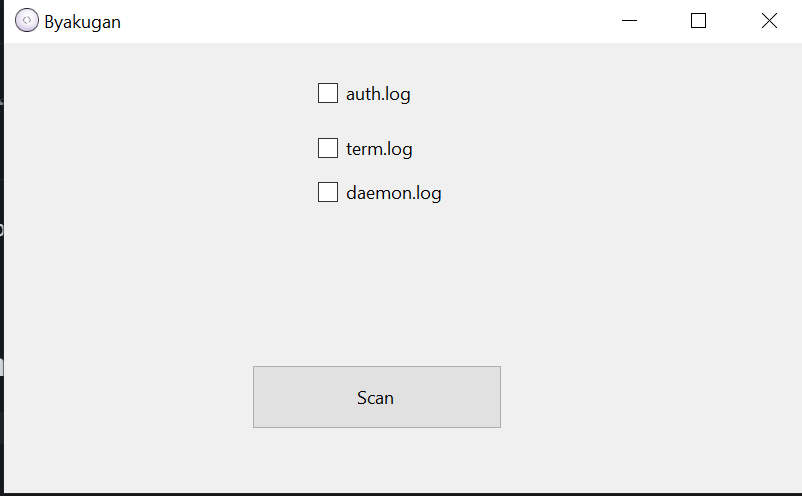
**Linux forensics logs #1**

بسم الله الرحمن الرحيم اليوم بنحلل logs لجهاز نظامة linux و بنسخدم اداة برمجتها انا و وظيفتها مساعدتك بالفحص فقط

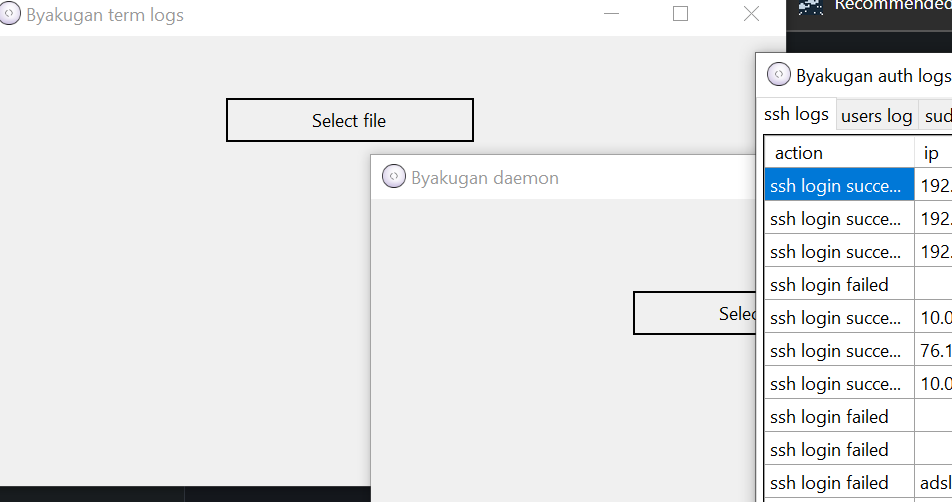
​[لتحميل الاداة](https://github.com/kira2040k/Byakugan) و بنحلل هذي الملفات auth.log و daemon.log و term.log

​

**Byakugan**



اول ما نشغل الاداة بتجينا هذي الواجهة البسيطة حدد نوع الملف اللي تبي تفحصه طبعا حاليا بس فيه 3 انواع و ان شاء الله ازيدها ف بحدد على كل الملفات عشان يفحصها لي



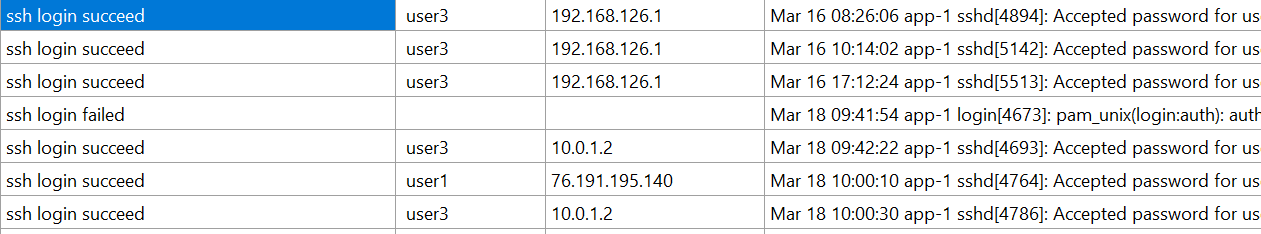
​

بما اني حددت الثلاثة كلهم بيفتح لي 3 نوافذ و عشان تفرق بينهم تشوف العنوان او تقدر تحلل ملف ملف عشان ما تصير زحمة عندك و بيطلب منك تحدد مسار الملف و تقدر تبدأ

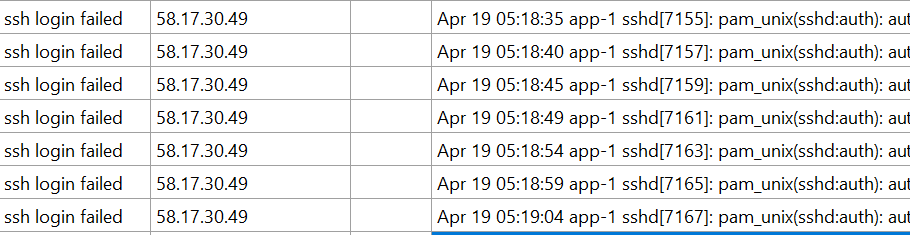
​

**auth.log**

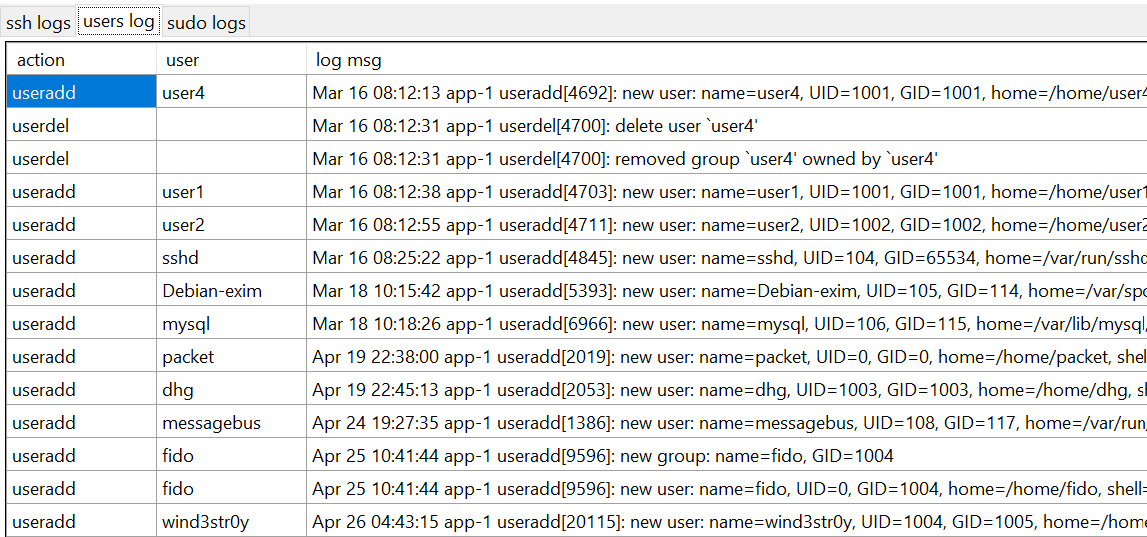
بيكون اول ملف نشيك عليه و نفتحه بالاداة و نشوف وش يجي لنا



بنشوف هنا ان فيه كثير ناس حاولو يتصلو ssh و دخلهم و فيه اكثر من ايبي بنسوي ترتيب حسب الوقت و نشوف



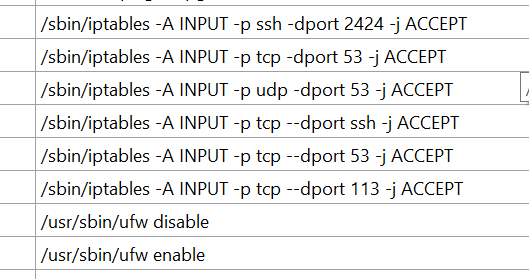
فيه ايبيات قاعدين يحاولون يسوون bruteforce لو تلاحظ الوقت و انه مادخله بتعرف انه يخمن



هنا نشوف اليوزرات اللي انضافت او انحذف و مع الوقت حقها



و هنا بعض الاوامر اللي سوا لها اليوزر sudo و نقدر نشوف اليوزر و الكوماند اللي سواه

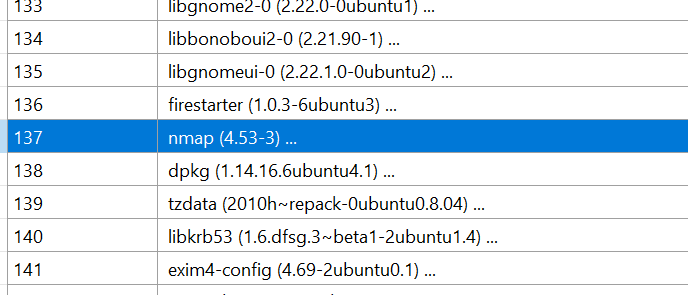


نشوف انه قعد يلعب في firewall

و هذي هي الطريقة تشوف اللقوز و بناء عليها تعرف اذا فيه شي او لا

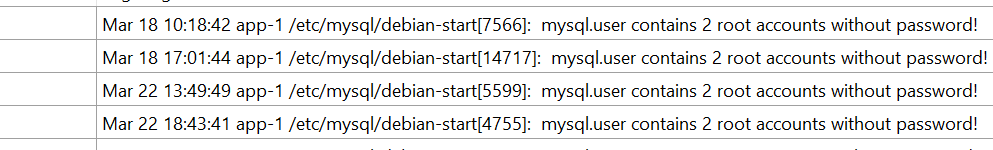
**term.log**

و يكون فيه اشياء حقت apt و اللي انت محملها ف نحط الملف في الاداة و نشوف



ف نشوف ان nmap محمل بالجهاز ممكن يكون شي عادي عندك هذا يعتمد على الشغل اللي كان يصير على الجهاز ف مو شرط يعتبر شي ضار او خطير

**daemon.log**



هذا ملف تلاقي فيه اغلب اشياء services و لو نشوف mysql يعطي انذار ان فيه يوزرين root بدون باسوورد

​

**الملخص**

قدرت تحلل بعض ملفات logs في اللينكس و تعرف وش قاعد يصير بالجهاز طبعا فيه ملفات كثير غيرها و بنفس الملفات فيه اشياء ثانيه بس ماحبيت اطول المقالة اكثر من كذا و ان شاء الله تعجبكم