**Linux forensics logs #2**

بسم الله اليوم بتكلم عن فحص logs لنظان لينكس و اليوم بيكون سيناريو واقعي

في البداية بستخدم اداتي المتواضعه [بياكوغان](https://github.com/kira2040k/Byakugan)

**auth.log**

اول شي ببدأ ب ملف auth.log و بفحصه بشوف وش فيه

Table

Description automatically generated

زي ما نلاحظ هنا كل ايبي و كم ريقويست ارسل و هل تم تسجيل دخوله بشكل صحيح ب ssh او لا ناخذ الايبي الاول اللي ارسل 7574 ريقويست و اليوزر اللي يخمن عليه r و هذا شي بفتح auth.log اشيك ممكن تكون مشكله بالاداة

Text, calendar

Description automatically generated

و ماظهر لي اي يوزر في اللوقز ما اعرف وش السبب بس مافيه مشكله نكمل فحص باخذ ايبي 219.150.161.20 و بشوفه باللوقز هل هو قاعد يسوي تخمين على ssh او لا

Graphical user interface, text, application

Description automatically generated

في البداية رتبت الايبيات بناء على الرقم و ضغطت كلك يمين و بحثت عن الايبي و بشوف الوقت من بين كل ريقويست و واضح انه كل ثانيه الى ثانيتين يرسل ف واضح انه تخمين و اصلا كان واضح من يوم شفنا انه ادخل 7574 باس غلط في ssh حلو الحين عرفنا انه تخمين + عرفنا انه ارسل 7574 باس غلط السؤال يقول هل قدر يلقى الباس و يدخل او لا؟

Table

Description automatically generated

استخدم خاصيه البحث مره ثانيه و ارتبها حسب التسجيل الدخول صحيح و نشوف انه قدر يدخل و بيوزر روت! و دخل على نظامنا 4 مرات طيب هل هو الايبي الوحيد اللي دخل عن طريق التخمين؟ نسوي نفس الخطوات على ايبي ثاني

Table

Description automatically generated

هذا الايبي دخل روت بعد و كان يخمن على بورت ssh

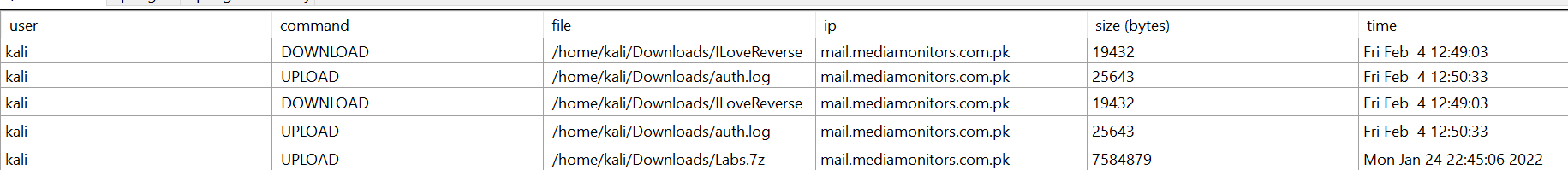
Table

Description automatically generated

و هذا تاريخ دخول احد الايبيات عن طريق ssh و بيوزر روت

**vsftpd.log**

بنشوف ملف vsftpd.log و يمكن نحصل شي



هذي الاشياء اللي صارت من اشياء انرفعت او تحملت

Table

Description automatically generated

و من ناحية محاولات الدخول نفس الشي فيه تخمين كيف عرفت؟ الوقت و الايبي طيب هل قدر يدخل على يوزر الادمن؟

Table

Description automatically generated

الحمد لله ماقدر يدخل ftp حقنا حاول يخمن 605 مره بس ماقدر يدخل بس فيه شي غريب mail.mediamonitors.com.pk هذا وش يبي ليه دخل ftp و بيوزر كالي؟ هذي ممكن ترفقها بالتقرير حقك بس لو طلع سيرفر عادي مصرح له يدخل ف مافيه مشكله لو انه تخمين بيطلع لنا انه خمن بس كل محاولات تسجيل الدخول صحيحة بنسبة 100% ممكن نرجع و نشوف الوقت اللي دخل فيه

Table

Description automatically generated

احد الخصائص الحلوة انك تقدر تحفظ النتايج ك csv عشان تستفيد من كل خصائص excel

A screenshot of a computer

Description automatically generated

**الملخص**

شفنا اللوقز حقت الssh , ftp و شفنا مين من اليوزرات سجل دخول و مين منهم bruteforce و كل من دخل ftp وش سوا بالضبط