تحليل المستندات الضارة -- الجزء 01 -- مقدمة والأجهزة الظاهرية

مقدمة

تستهدف هذه الدورة التدريبية المصغّرة هواة وممارسي الأمن الرقمي (الدعم الفني والميسرين والمستجيبين الأوائل وما إلى ذلك) الذين يرغبون في معرفة المزيد عن المستندات الضارة وكيفية التعرف عليها. ويمكن أن تكون هذه المستندات مرفقات بريد إلكتروني أو ملفات على محركات أقراص فلاش أو تنزيلات من مواقع ويب محددة، وتتمثل أهدافها الرئيسية فيما يلي:

- التعرّف على أساسيات عمل تنسيقات المستندات الشائعة وكيف يمكن استغلالها لتصبح أسلحة مع التركيز بشكل خاص على ملفات تنسيق المستندات المحمولة (بي دي إف PDF) ومستندات مايكروسوفت أوفيس (Microsoft Office) (من مايكروسوفت وورد (MS Word) وإكسل (Excel) وباوربوينت (PowerPoint) على الأقل).
- التعريف ببعض الأدوات التي قد تساعد في تحديد علامات المستندات الخطرة أو تأكيد أنه من الآمن فتحها.
- تقديم بعض النصائح الأمنية وتوضيح الشكوك الشائعة حول التعامل مع الملفات المشبوهة.

تستخدم هذه الدورة التدريبية تنسيق القراءات القصيرة والاختبارات القصيرة في معظم المحتوى المغطى حيث سيكون من الضروري تشغيل بعض الأدوات حسب المواد. سنغطي ذلك في قسم بيئة العمل بعد فترة وجيزة من المقدمة والمتطلبات العامة هي:

- إكمال التمارين المقترحة:
- إمكانية تشغيل 1) جهاز ظاهري في الكمبيوتر باستخدام فيرتشول بوكس (Virtualbox) أو برنامج مشابه أو 2) نصوص بايثون (فقط لتحليل ملفات الدورة التدريبية وليس لتحليل العينات الحقيقية).
- الوقت اللازم لتغطية المواد (حوالي ساعتين)

تستغرق هذه الدورة المواد المتاحة في مراجع أخرى وتستخدم فقط الأدوات المتاحة مجانًا، ومعظم المحتوى مستوحى من العمل الذي قام به حتى الآن ديدييه ستيفنز (Didier Stevens) وبالأخص سانس (SANS)، بالإضافة إلى المراجع الأخرى التي يمكن أن ترد قائمة مختصرة بها فيما يلي:

- /https://blog.didierstevens.com/2011/05/25/malicious-pdf-analysis-workshop-screencasts
- https://github.com/filipi86/MalwareAnalysis-in-PDF
- /https://www.sentinelone.com/blog/malicious-pdfs-revealing-techniques-behind-attacks
- https://www.youtube.com/watch?v=opdVFQEBCNU

الهيكل

1. بيانات إخلاء المسؤولية
2. بعض اعتبارات نمذجة التهديدات
3. لكل نوع من تنسيقات الملفات (ملفات بي دي إف (PDF) ومايكروسوفت أوفيس (MS Office))
    1. كيفية تنظيمها (بطريقة أكثر تقنية)
    2. كيفية استغلالها لتصبح أسلحة
    3. كيف يمكننا إجراء تحليل تمهيدي
    4. بعض الاستنتاجات/الحقائق حول تنسيق الملف
4. بعض النصائح العامة ضد التهديدات ذات الصلة

5. الخطوات التالية

فيما يلي سلسلة من بيانات إخلاء المسؤولية المفيدة قبل البدء بالمواد

بيانات إخلاء المسؤولية

نظرًا لطبيعة المهمة التي سنؤديها بعد إتقان المحتوى المقدم المتمثل في تحليل الملفات الضارة والخطرة، وتعقيد الموضوع الذي نرى أنه مقدمة لتحليل البرمجيات الضارة نوصي بشدة بقراءة هذا القسم والاتفاق مع جميع العناصر قبل المضي قدمًا.

1. **هذه الدورة تمهيدية:** وهي مصممة للأشخاص الذين ليس لديهم خبرة سابقة في تحليل المستندات المشبوهة، وفي قسم الخطوات التالية قمنا بتضمين قائمة بالموارد لقراءتها والرجوع إليها.
2. **هناك العديد من التقنيات المتقدمة التي لا تغطيها هذه الدورة:** وهناك العديد من التهديدات المحددة التي يتجاوز تعقيدها نطاق هذه المادة كما هو الحال في كل ما يتعلق بأمن المعلومات وقد تكون هناك تهديدات تنتظر اكتشافها ولن تتم تغطيتها في هذه الدورة. نوصي بطلب المساعدة في حالة الاشتباه بأننا نشهد تهديدًا متقدمًا أو غير معروف في ملف أو أي آثار أخرى وسنتحدث عن ذلك أكثر في قسم لاحق. لكن ستساعدنا هذه الدورة على فهم صفات الملف الحميد المعتاد بدلًا من هيكل كل مستند ضار.
3. **اتخذ احتياطاتك عند تحليل الملفات الحقيقية:** العينات المستخدمة في هذه الدورة غير ضارة، ولكن تكرار سير العمل المقدم على عينات حقيقية دون اتخاذ إجراءات الأمان المعنية سيؤدي على الأرجح إلى إصابة جهازك، لذا يرجى عدم تشغيل أي ملف مشبوه على جهاز الكمبيوتر الرئيسي الخاص بك، ونوصي بدلًا من ذلك باستخدام جهاز ظاهري أو جهاز مخصص أو بيئة لا يمكنك فيها تنفيذ الملف على جهازك وإنما فقط تحليل خصائصه.

اختبار إخلاء المسؤولية

السؤال 1: أفهم مخاطر تحليل الملفات المشبوهة، والعواقب المحتملة لتشغيل البرمجيات الضارة عن قصد أو عن طريق الخطأ وقد قرأت محتوى هذه الصفحة/القسم وأتفهم الاستراتيجيات الأكثر شيوعًا لمعالجة هذه التهديدات المحتملة.

السؤال 2: أي من الخيارات التالية تصف بصورة أفضل ما نحتاج إلى القيام به عند تحليل ملف مشبوه حقيقي؟

1. يجب أن نشغل جهازًا ظاهريًا أو كمبيوترًا مخصصًا لتحليل الملف ومنحه أقل قدر ممكن من الوصول إلى الجهاز المضيف وبقية الشبكة.

صحيح -- في حالة كان الملف المشبوه مصابًا بالفعل سيكون الضرر ضمن مساحة آمنة، وإلى جانب فصل الجهاز عن بيئتك الحقيقية هناك توصيات أخرى تحدد طريقة إعادة البيئة إلى حالة آمنة سابقة واستخدام أدوات مراقبة في حالة رغبتنا في معرفة التغييرات التي حصلت خلال الإصابة المحتملة واستخدام أنظمة تشغيل مختلفة بين نظام المضيف والضيف للتخفيف من العدوى العرضية.

2. يمكننا تحليل الملف في جهاز الكمبيوتر/البيئة الخاصة ولكن دون الوصول إلى الإنترنت.

غير صحيح -- حتى عندما يكون قطع الاتصال بالإنترنت ممارسة موصى بها أثناء تحليل الملفات، لا يزال بإمكان الملف المصاب اختراق جهاز الكمبيوتر/البيئة الرئيسية أو تحضيره ليلحق به الضرر به عند عودة الاتصال.

3. يجب علينا تحليل الملف في جهاز كمبيوتر أو جهاز ظاهري مع أنظمة تشغيل أقل شيوعًا مثل لينوكس (Linux) أو ماك أو إس (macOS).

غير صحيح -- بالرغم من تصميم معظم البرمجيات الضارة المعروفة لنظام التشغيل ويندوز هناك أيضًا شفرة ضارة مصممة لأنظمة أخرى، وأهم شيء أيضًا عند تحليل الملفات المشبوهة هو تجنب إصابة بيئتنا الرئيسية بغض النظر عن نظام تشغيلها. في حين قد تساعد في التخفيف من التأثير السلبي لتنفيذ البرمجيات الضارة بصورة عرضية لا تكفي دون استخدام سلسلة تدابير أخرى، وتعد هذه النصيحة اختيارية ولا يترتب عليها سوى تأثير ضئيل إذا كان بيئات الاختبار لدينا قوية.

نبذة عن نماذج التهديد

عند البحث عن المشورة حول كيفية التعامل مع الملفات المشبوهة عادةً ما يكون النهج المقترح هو تجنب أي تفاعل مع الملفات على سبيل المثال:

- لا تفتح ملفات غير معروفة.
- لا تتفاعل مع الملفات المشبوهة.
- لا تنظر بالعين إلى أي ملف مشبوه.

أو يمكننا العثور على نوع آخر من النصائح التي بالرغم من كونها كافية لمعظم الناس يمكن أن تكون مضللة للمستخدمين القادمين من خلفية حساسة مثل نشطاء حقوق الإنسان أو الصحفيين الذين يعملون في بيئات خطرة أو تؤدي إلى نتائج عكسية واضحة مثل:

- يكفي استخدام مضاد فيروسات لحمايتك من الملفات الضارة.
- تُعدّ مستندات مايكروسوفت أوفيس التي تضم تعليمات ماكرو فقط خطيرة ولذلك يمكنك التعامل مع أنواع الملفات الأخرى دون القلق كثيرًا.
- احذف أي بريد إلكتروني يحتوي على مرفقات مشبوهة. يثير هذا الأمر القلق بشكل خاص في بعض السيناريوهات لأننا إذا حذفنا رسائل البريد الإلكتروني والمرفقات من بريدنا الوارد فإننا نفقد الأدلة الرئيسية التي يمكن أن تساعدنا في تقييم ما إذا كانت الآثار ضارة أو مستهدفة بالفعل والتي قد تكون معلومات لا تقدر بثمن.

من الناحية العملية، عندما نعمل مع المجتمعات المستهدفة (وبالأخص الصحفيين) ليس عدم التفاعل مع الملفات خيارًا. تحتاج العديد من المنظمات والمجموعات والأفراد إلى فتح ملفات يحتمل أن تكون خطرة كجزء من عملهم وسيفعلون ذلك حتى مع إدراكهم للمخاطر ومن الأمثلة على ذلك:

- تلقي الصحفيين دعوة لمؤتمر صحفي.

- تلقي النشطاء وثيقة دعم كدليل في قضية أو تسريب متعلق بانتهاكات لحقوق الإنسان.
- إرسال مؤسسة عدائية وثيقة يجب مراجعتها ومعالجتها.

من العوامل الإضافية التي يجب مراعاتها هو تعرض الجهات الفاعلة في المجتمع المدني لتهديدات مستهدفة لا تعرفها برامج مكافحة الفيروسات، وكذلك وبحسب نوع الهجوم قد يتم استغلال تنسيقات الملفات الأخرى لتصبح أسلحة أيضًا. تُعدّ هذه عوامل من الضروري أن ينظر فيها الأشخاص الذين يساعدون الفئات الضعيفة على فهم كيفية استغلال المستندات وتنسيقات الملفات الشائعة الأخرى لتصبح أسلحة، ولأجل تقديم نصائح مفيدة، ولكن أيضًا لمساعدتهم على تحليل ملفات محددة لفهم وتقييم ما إذا كانوا ضحايا للهجمات المستهدفة.

مع مراعاة كل هذه الأمور سنركز على فهم بنية تنسيقات الملفات القياسية وكيفية اكتشاف الهجمات الأكثر شيوعًا التي تستخدمها وكذلك بعض التدابير الدفاعية المحدثة لتجنب وقوع ضحايا لنوع التهديد هذا.

اختبار نموذج التهديد

السؤال 1: بالنسبة لمؤسسة يكثر استهدافها وتتلقى العديد من مستندات مايكروسوفت أوفيس عبر البريد الإلكتروني أي من الخيارات التالية هو صحيح؟ (إجابة واحدة فقط صحيحة.)

1. حتى لو كان برنامج مكافحة الفيروسات يقول إن الملف آمن فقد لا يزال يضم برمجيات ضارة.

صحيح -- من الممكن وبالأخص للضحايا المعرضين لمخاطر عالية أن تستهدفهم برمجيات ضارة ليست مكشوفة لبقية الإنترنت وبالتالي لم تستوفِ محركات مضادات الفيروسات هذه المتطلبات بعد ولا يمكنها اكتشاف أنها ضارة. هناك أيضًا العديد من التقنيات التي تستخدمها الجهات الفاعلة الضارة لإخفاء البرمجيات الضارة بشكل بيانات شرعية تجعل من الصعب في بعض الأحيان على برامج مكافحة الفيروسات اكتشاف التعليمات البرمجية الضارة.

2. عليهم حذف أي مرفقات مشبوهة على الفور لأنه قد يكون من الخطر وجودها في البريد الوارد.

** غير صحيح --** لا تُنفذ المرفقات في البريد الوارد على الكمبيوتر دون إذن صريح من المستخدم (أو على الأقل في الهجمات المعروفة) وبالأخص إذا تم تخزينها في خوادم خارجية. لذلك سيتسبب حذفها على الفور بجعلنا نفقد أدلة قيمة في حال أردنا البحث أكثر عن الملف والبريد الإلكتروني.

3. يجب ألا يفتحوا أي مرفقات من مصادر غير معروفة.

غير صحيح -- حتى عندما يضمن ذلك عدم تنفيذ الملفات الضارة، يجب أن نفهم أن الجماهير المعرضة للخطر تحتاج في معظم الأحيان إلى التفاعل مع المعلومات من مصادر غير موثوق بها لإنجاز مهمتها مما يجعل عدم التعامل نصيحة غير مستدامة في معظم الحالات.

البيئة: اعتبارات عامة

لتنفيذ معظم المهام في هذه الدورة سنستخدم الأدوات الأساسية المكتوبة بلغة برمجة بايثون (Python)، ونظرًا لتوافق بايثون الواسع مع كل نظام تشغيل، هناك طرق لا حصر لها يمكننا من خلالها إعداد بيئة ونقترح واحدة على وجه التحديد، ولكن إذا كنت تعرف بايثون وتحليل البرمجيات الضارة و/أو المحاكاة الظاهرية يمكنك إعداد نوع مختلف يناسبك. يتمثل المطلب القوي الوحيد في وجود بيئة معزولة للتلاعب بالآثار الخطرة وهي في هذه الحالة الملفات، كما توجد اعتبارات أخرى ولكن ربما هذا هو أهمها.

البيئة المعزولة والممارسات الجيدة الأخرى

العينات المستخدمة في هذه الدورة غير ضارة وهي فقط لتوضيح هيكل الملفات وكيفية اكتشاف المؤشرات التي تدق ناقوس الخطر، ولكن إذا كنت تنوي تحليل ملفات حقيقية فمن المحتمل أن تجد ملفًا مصابًا يمكن أن يسبب أنواع مشاكل عديدة مثل إصابة الكمبيوتر الذي تستخدمه أو تعرض معلوماتك للاختراق أو جعل جهازك غير قابل للاستخدام من بين أمور أخرى. لكن من الممارسات الشائعة أن يكون لديك بيئة حصرية لتحليل العينات المشبوهة وتشغيلها بطريقة تخضع فيها للرقابة ولذلك إذا حدث خطأ ما أثناء التلاعب بالعينة فلن يؤثر على جهازك أو المعلومات الواردة فيه.

من الميزات الأخرى لوجود بيئة مخصصة هي أنه بعد العمل على عينات البرمجيات الضارة يمكنك حذف كل شيء والبدء من جديد دون خوف من فقدان الملفات غير ذات الصلة. وهذا يسمح لنا بتخطيط طرق عملية "إعادة ضبط" بيئتنا إلى حالة الاستعداد قبل كل تحليل.

إحدى أكثر الاستراتيجيات استخدامًا لضمان بيئة معزولة هي استخدام الأجهزة الظاهرية والتي تعمل بشكل أساسي على محاكاة جهاز كمبيوتر كامل داخل كمبيوتر آخر يشمل نظام التشغيل والأقراص الصلبة والشاشة وما إلى ذلك. من الأدوات الشائعة لإعداد واستخدام الأجهزة الافتراضية هي فيرتشول بوكس وفي إم وير ووركستيشن بلاير (VMware Workstation Player) من بين أدوات أخرى، ويُعدّ استخدام الأجهزة المخصصة أيضًا خيارًا طالما أنها مؤمنة في حالة الإصابة.

ومن السيئات المحتملة هي حقيقة شمول بعض البرمجيات الضارة على تعليمات برمجية للتحقق مما إذا كان يتم تنفيذها في بيئات معزولة كي تتوقف عن العمل مما يجعل من الصعب تحليلها، ولكن الخطر الكامن في تشغيل البرمجيات الضارة في بيئاتنا اليومية لا يستحق المجازفة به حتى، ولذلك نوصي بالسعي إلى المساعدة والتركيز على التقنيات التي لا تعتمد على تشغيل الملفات المشبوهة، أو الحصول على معلومات حول كيفية إعداد بيئة تبدو وكأنها جهاز حقيقي لعينة برمجيات ضارة. بالنسبة لهذا المورد، لا ينبغي أن يكون هذا مشكلة لأننا لن نقوم بتنفيذ أي تعليمات برمجية من المستندات، ولكن إذا كنت تريد التعلم وإجراء تحليل ديناميكي على الملفات المشبوهة، فسيكون هذا مفيدًا.

اعتبارات أخرى

إلى جانب الممارسة الجيدة المتمثلة في وجود بيئة معزولة توجد ممارسات شائعة أخرى وهي:

- **التأكد من أن الكمبيوتر الذي تستخدمه غير متصل بالإنترنت أو الشبكة المحلية:** بالأخص إذا كنت تفتح ملفات مشبوهة لأن السبب الأكثر شيوعًا للقيام بذلك هو تجنب إطلاق إشارات تُنبّه مشغلي البرمجيات الضارة إلى أن التعليمة البرمجية يتم تنفيذها أو اختبارها وفقًا لبيانات أخرى مثل عنوان بروتوكول الإنترنت أو نوع الجهاز الذي ينفذ البرمجيات الضارة. كما ستحاول

بعض البرمجيات الضارة الانتشار إلى الشبكة المحلية في محاولة لإصابة أجهزة أخرى غير مقصودة، ولذلك من الممارسات الشائعة عزل أجهزة الاختبار ضمن شبكات مادية أو ظاهرية مختلفة (أو شبكات محلية افتراضية). يجب مراعاة أنه في حالة تحليل عينة من خلال تنفيذها من الممكن أن يكتشف البرمجية الضارة أنه يتعذر عليه الوصول إلى الإنترنت وبالتالي يتوقف عن العمل.

- ** إذا كنت ستتصل بالإنترنت استخدم شبكة ظاهرية خاصة (VPN) أو شيئًا مشابهًا:** حيث إن الفكرة هي إخفاء موقعك الحقيقي في حالة تشغيل البرمجيات الضارة التي نحللها وإرسال إشارات إلى مشغليها. مجددًا لا يوصى عادةً بتنفيذ البرمجيات الضارة دون اتخاذ تدابير لتجنب أي اتصال محتمل مع المشغلين، ولكن قد يكون استخدام الشبكة الظاهرية الخاصة مقياسًا جيدًا في حالة التنفيذ العرضي أو إذا فشلت التكوينات الأخرى في مرحلة ما.
- **رتب عملية لإعادة بيئتك إلى حالتها "النظيفة":** استنادًا إلى ما إذا كنت تستخدم جهازًا ظاهريًا أو جهازًا مخصصًا، هناك بعض الأدوات والميزات المفيدة لإعادة ضبط البيئة، ولذلك في كل مرة تقوم فيها بتحليل عينة، تكون الآلة نظيفة لأن الأجهزة الافتراضية التي تستخدم اللقطات هي مثال جيد وهناك برنامج لإعادة جهاز كمبيوتر فعلي إلى حالة سابقة.
- **الالتزام بتحليل التعليمات البرمجيات بحالتها الثابتة:** يمكننا تقسيم تحليل التعليمات البرمجيات الضارة بشكل عام حسب ما إذا كنا ننفذ العينات أم لا، حيث يحاول تحليل التعليمات البرمجية بحالتها الثابتة تشريح الملفات والآثار الأخرى لجمع أكبر قدر ممكن من الفهم دون تنفيذها، بينما يسمح التحليل الديناميكي بتنفيذ العينات لمعرفة التغييرات في بيئة الاختبار. استنادًا إلى نوع البرمجيات الضارة، قد يكون أحد أنواع التحليل أكثر فائدة من الآخر، ولكن بشكل عام سيتطلب التحليل الديناميكي تدابير حماية إضافية لبيئة الاختبار وللشبكة كي يصبح قادرًا على دعم تنفيذ البرمجيات الضارة الحقيقية وتستعرض هذه الدورة تقنيات التحليل الثابت فقط.
- **عليك الحذر عند نشر عينات أو معلومات أخرى للعينات التي تم يجري تحليلها:** بشكل عام قد ينبّه هذا مشغلي البرمجيات الضارة إلى قيامنا بتحليل حملة البرمجيات الضارة مما يتسبب بإغلاقهم البنية التحتية وتنظيف أي آثار بهدف جعل إمكانية التتبع أكثر صعوبة وما إلى ذلك. ينطبق هذا على أي منصة عامة مثل وسائل التواصل الاجتماعي ومواقع الويب بما في ذلك بعض المنصات العامة التي تسمح لنا بإرسال ملفات لتحليلها على السحابة بحثًا عن مؤشرات من محركات مكافحة الفيروسات ومجتمع أمن المعلومات. بالنسبة للسيناريو الأخير، سنشارك بعض الأمثلة والتقنيات للتحقق من المعلومات التي نحتاجها دون تنبيه أي شخص.

اختبار البيئة

السؤال 1: أي العبارات التالية صحيحة؟

1. سيتطلب تشغيل العينات تدابير أمنية أقل مقارنة بمحاولة تشريح الآثار بحثًا عن معلومات مفيدة.

** غير صحيح --** سيؤدي تنفيذ البرمجيات الضارة إلى إصابة البيئة التي نستخدمها مما يتسبب في أشياء مثل إعلام منشئي المحتوى والبرمجيات الضارة الذين يحاولون إصابة أجهزة أخرى ضمن الشبكة وجعل الجهاز غير قابل للاستخدام. تتطلب هذه العواقب وجود تدابير أمنية أكثر من تحليل العينة دون تنفيذها (تُعرف باسم تحليل التعليمات البرمجية بحالتها الثابتة).

2. سيجعل قطع الوصول إلى الإنترنت من الصعب على عينة البرمجيات الضارة إخطار منشئي المحتوى بأنه قد تم تنفيذه.

** صحيح --** دون الوصول إلى الإنترنت سيتعذر على البرمجيات الضارة التواصل مع الخوادم الخارجية لتنفيذ إجراءات معينة بما في ذلك الإخطار بتنفيذها. من المفيد أن نعرف أيضًا أن بعض البرمجيات الضارة تستخدم الإنترنت لتنزيل أجزاء أخرى من تعليماتها البرمجية، لذلك قد يكون قطع الوصول مشكلة أيضًا لأنه لن يكون لدينا نظرة متعمّقة بكامل الوظيفة دون الحصول على الأجزاء المفقودة، ولكن المخاطر المرتبطة بتشغيل البرمجيات الضارة عن طريق الخطأ تجعل من الأفضل قطع الاتصال لنرى ما إذا كنا نفتقد شيئًا مهمًا أثناء التحليل.

3. أكثر الطرق فعالية لتحليل البرمجيات الضارة هي استخدام الأجهزة الظاهرية لأنه في حالة إصابة الجهاز يمكننا إعادة إنشاؤها مرة أخرى من الصفر.

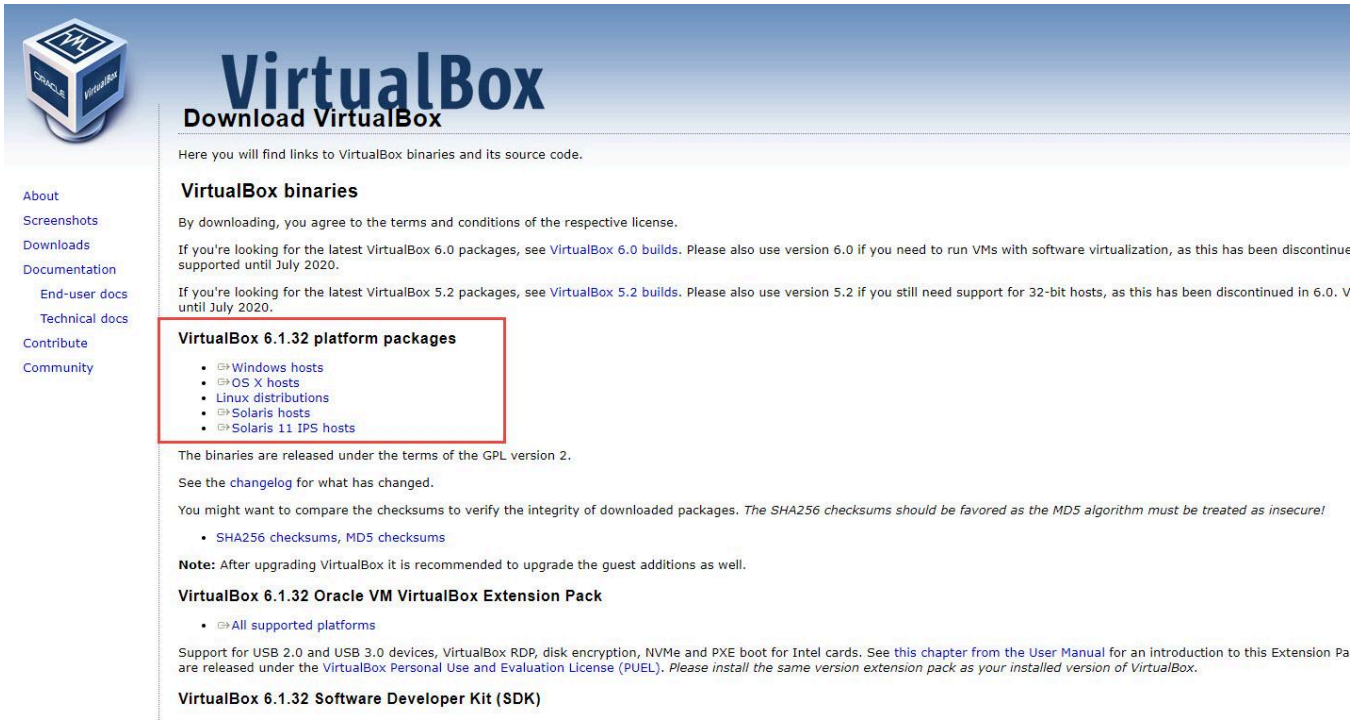
غير صحيح -- ما يجعل الأجهزة الافتراضية أكثر كفاءة من حيث استخدامها لتحليل البرمجيات الضارة هو القدرة على تسجيل "لقطات (snapshots)"، بحيث يصبح بإمكاننا تسجيل لقطة واحدة لحالة الجهاز الافتراضي قبل أن نبدأ التحليل وعند الانتهاء يمكننا إعادة الجهاز الافتراضي إلى تلك اللقطة كي نصبح على استعداد لتحليل العينة التالية بطريقة مضبوطة، مما يسرع أسرع بكثير من إعادة إنشاء الجهاز الافتراضي من الصفر في كل مرة. (لأكون صادقًا كان ذلك أمرًا صعبًا).

مثال على بيئة: ريمنوكس + فيرتشول بوكس

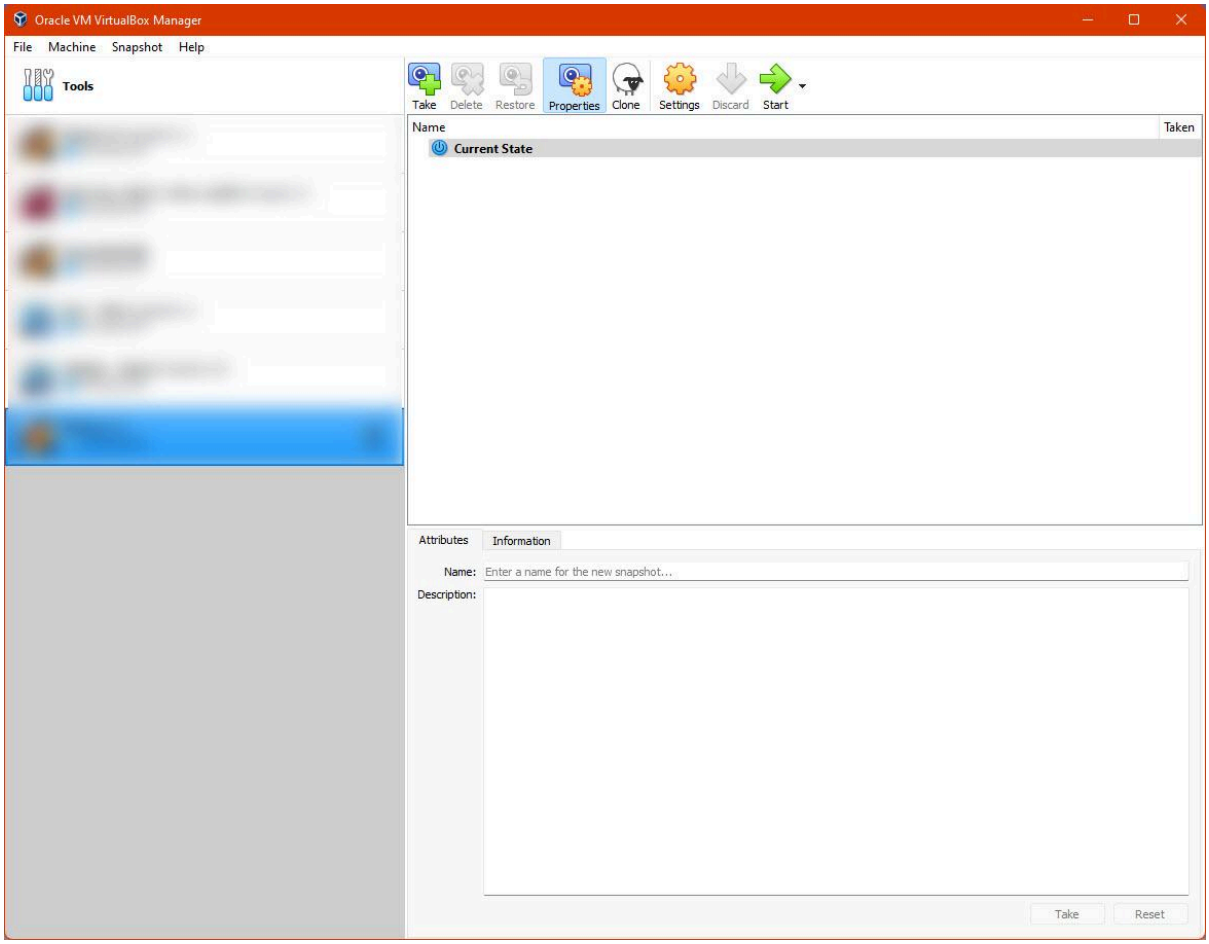
في حال كنت تريد بيئة جاهزة للعمل نوصي باستخدام ريمنوكس وهو جهاز ظاهري قابل للتنزيل تم تكوينه مسبقًا يشمل بعض الأدوات المفيدة لتحليل البرمجيات الضارة. سنستخدم هنا فيرتشول بوكس لتحويل ريمنوكس إلى جهاز ظاهري، لكن إذا كنت تعرف هذه العملية فلا تتردد في الانتقال إلى القسم التالي من الدورة التدريبية.

تثبيت فيرتشول بوكس

سنحتاج أولًا إلى برنامج لإدارة أجهزتنا الافتراضية، وقد اخترنا فيرتشول بوكس لأنه الحل الأكثر استخدامًا والمتوافق مع المنصات الرئيسية الثلاث (ويندوز وماك أو إس ولينوكس)، وهو مجاني. لأجل النسخة المعنية يمكن زيارة https://www.virtualbox.org/ والبحث عن الزر الأزرق الكبير، ثم ابحث عن القسم الذي يحتوي على الحزم حسب المنصة كما هو موضح في الصورة.



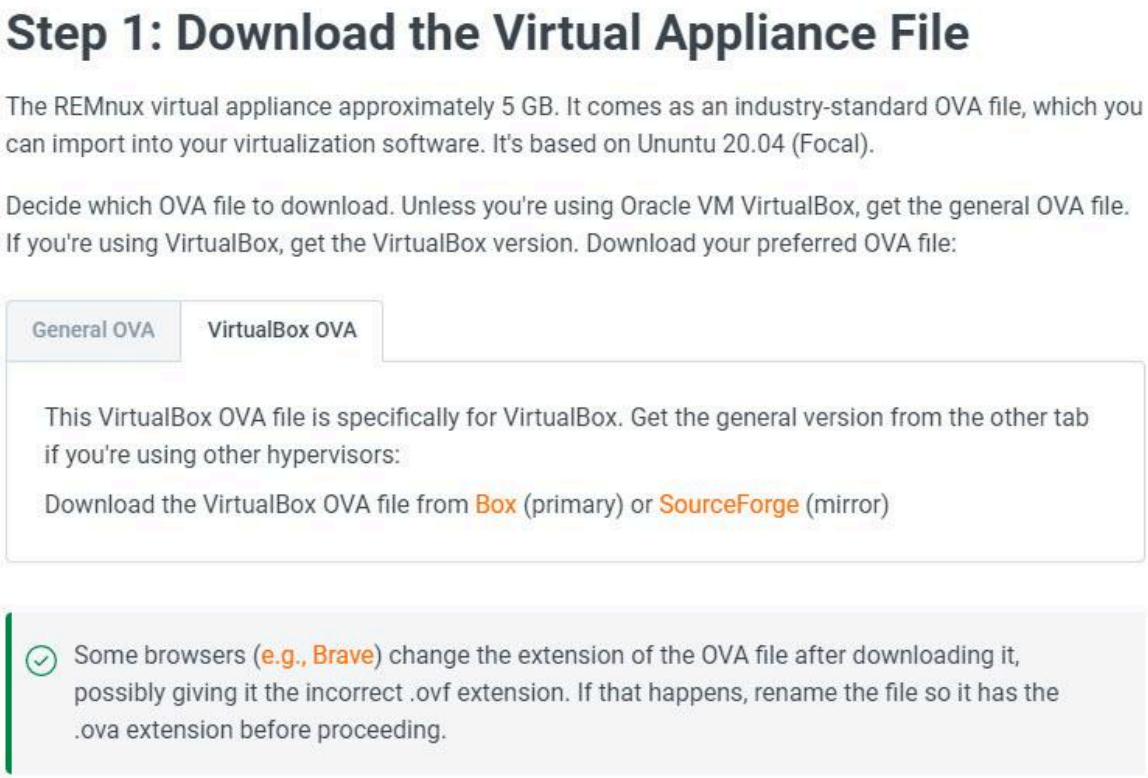
انقر هنا على منصتك واتبع التعليمات، ويمكنك بعدها تشغيل فيرتشول بوكس وسترى نافذة تشبه هذه.



لن يكون هناك شيء في المنطقة غير الواضحة وبالتالي نحن مستعدون لتنزيل وتثبيت ريمنوكس.

تثبيت ريمنوكس

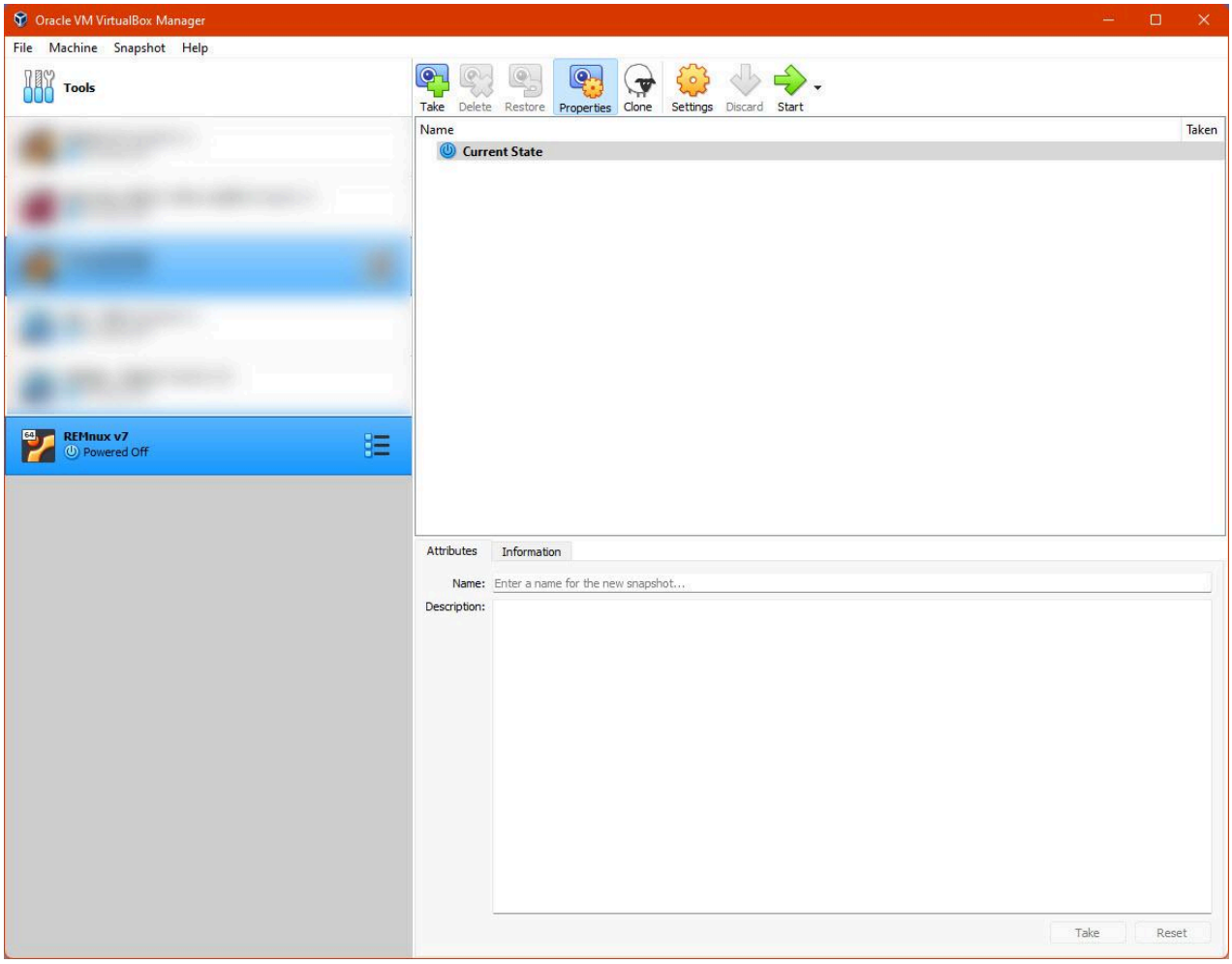
يمكنك الآن الانتقال إلى https://remnux.org/ والنقر على "تنزيل" في القسم المقابل، وقد تتم إعادة توجيهك إلى صفحة أخرى تطلب منك تحديد ما إذا كنت تريد تنزيل ملف General OVA أو Virtualbox OVA، وفي حالتنا الخيار الثاني هو الصحيح.

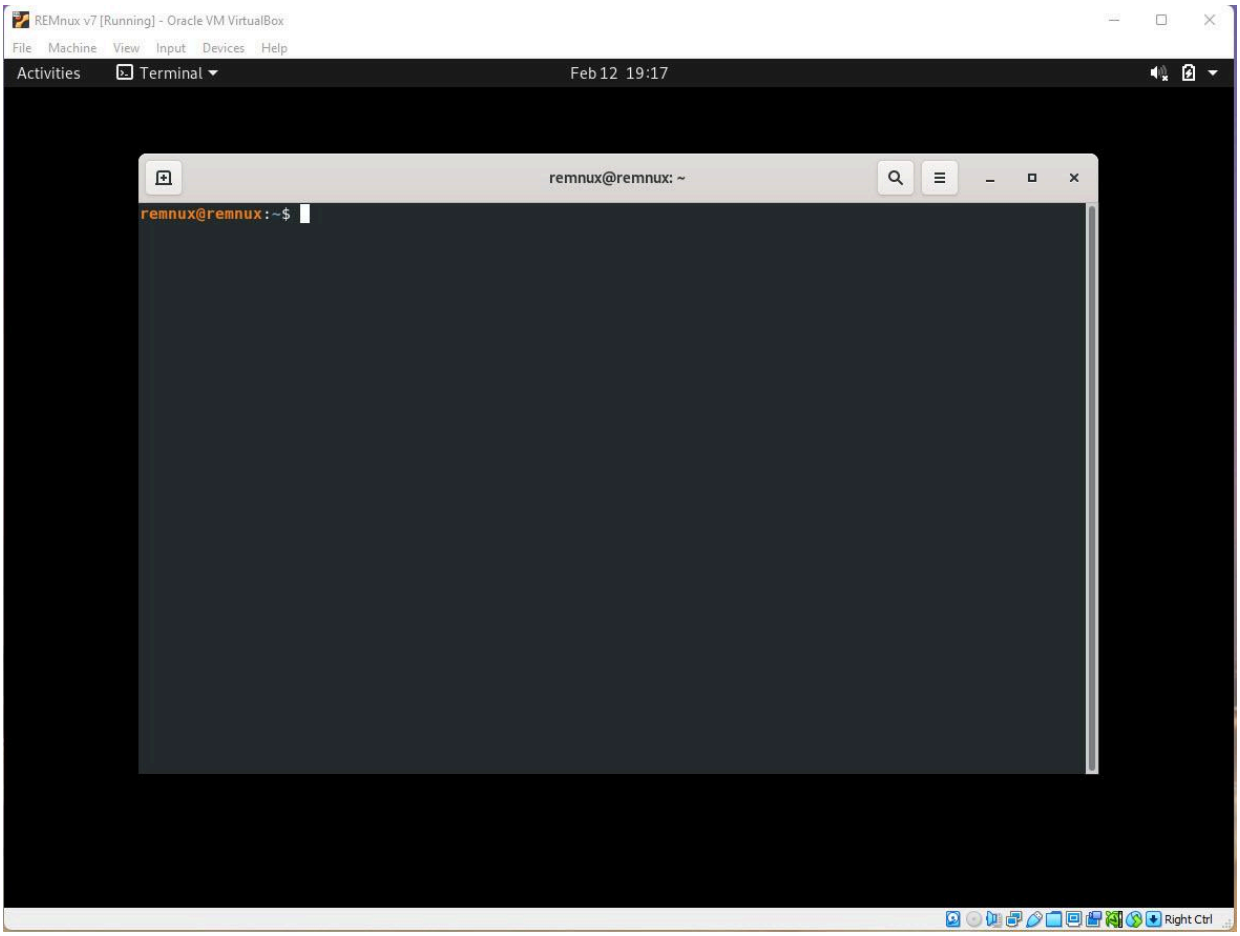


بعد تنزيل الملف، يوصى بالتحقق مما إذا كان الملف قد تم تنزيله بشكل صحيح، ولأجل القيام بذلك نحتاج إلى التحقق من شفرة التجزئة المرتبطة بالملف. تُعدّ شفرات التجزئة موضوعًا عميقًا نشجع على تعلمه وتطبيقه كما أنه يستخدم كثيرًا في تحليل البرمجيات الضارة، ولكن في الوقت الحالي يمكننا تلخيصه على أنه عملية رياضية تحول البيانات مثل نص أو ملف إلى رمز أبجدي رقمي، يجب أن يكون هذا الرمز فريدًا للبيانات التي تقوم بتحليلها، وحتى في التغييرات الصغيرة ستتغير شفرة التجزئة كثيرًا لذا فإن التحقق من أن الملف الذي تم تنزيله يطابق شفرة التجزئة المنشورة ذاتها في موقع ريمنوكس سيدل على أنه تم تنزيل الملف بدون مشاكل، أما إذا كانت التجزئة مختلفة فسيكون ذلك علامة على أن الملف قد تلف بسبب عملية تنزيل خاطئة أو ليس الملف الصحيح لسبب ما. (ربما يكون خطأ من جانبنا في تحديد الإصدار الصحيح أو في حالة سيناريو مستبعد قد يقوم شخص ما بتغيير الملف ليصبح إصدارًا ضارًا، لذا عليك توخي الحذر). يتوفر مرجع سريع حول كيفية التحقق من شفرة التجزئة على https://technastic.com/check-md5-checksum-hash/.

تنزيل الملف

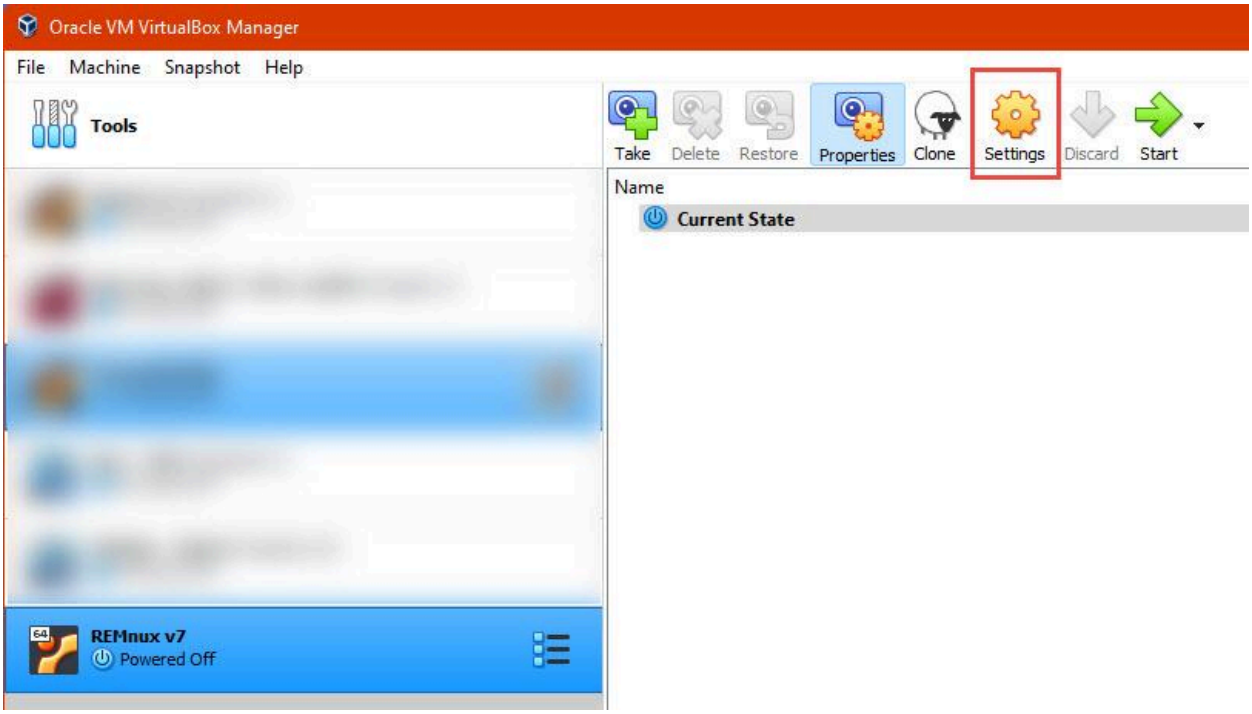
بعد التحقق من أن ملفنا قد تم تنزيله دون مشاكل يمكننا الآن استيراده إلى فيرتشول بوكس، وفي صفحة ريمنوكس حيث قمنا بتنزيل الجهاز الظاهري تتوفر تعليمات، ولكن يكفي النقر نقرًا مزدوجًا على ملف ova. وسيرشدنا المعالج خلال عملية الاستيراد. يمكننا ترك كل شيء كما هو مقترح في التكوين المقترح، وفي النهاية يجب أن نرى آلة ريمنوكس في نافذة فيرتشول بوكس لدينا. سيؤدي النقر على "Start (ابدأ)" إلى تشغيل الجهاز في نافذة منفصلة. هذا جهاز يعمل بنظام لينوكس واسم المستخدم لتسجيل الدخول هو *remnux* وكلمة السر هي *malware*، (لكن من الممكن أن تكون الجلسة مفتوحة دون طلب بيانات الاعتماد).


Oracle VM VirtualBox Manager
File
Machine
Snapshot
Help
Tools
Take
Delete
Restore
Properties
Clone
Settings
Discard
Start
Name
Taken
Current State
REMnux v7
Powered Off
Attributes
Information
Name:
Enter a name for the new snapshot...
Description:
Take
Reset

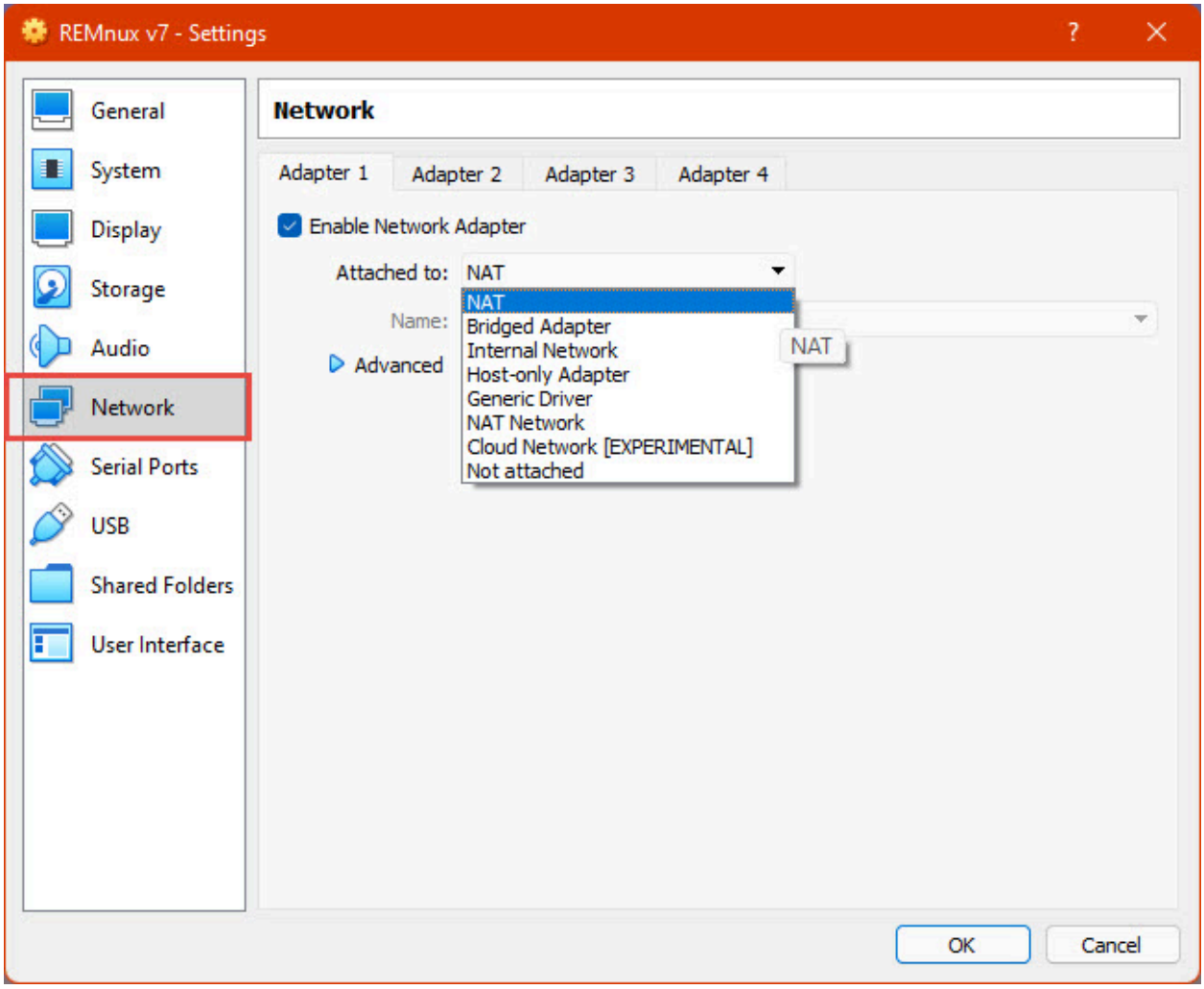


تكوينات إضافية على فيرتشول بوكس -- الشبكة

نظرًا لأننا سنقوم بتحليل ملفات يحتمل أن تكون ضارة فليس من المستحسن تشغيل الجهاز بطريقة تسمح له بالتواصل مع بقية شبكتنا وقد تختلف الاستراتيجية المحددة اعتمادًا على أسلوب المحلل ولكن يتم التكوين في الغالب في شاشة واجهات الجهاز الافتراضي. ولأجل الوصول إليها يمكننا بعد إيقاف تشغيل آلة ريمنوكس الضغط على زر "Settings (الإعدادات)" في شريط الأدوات.



ثم في قسم "Network (الشبكة)"، سيكون لديك سلسلة من الخيارات وأهمها:

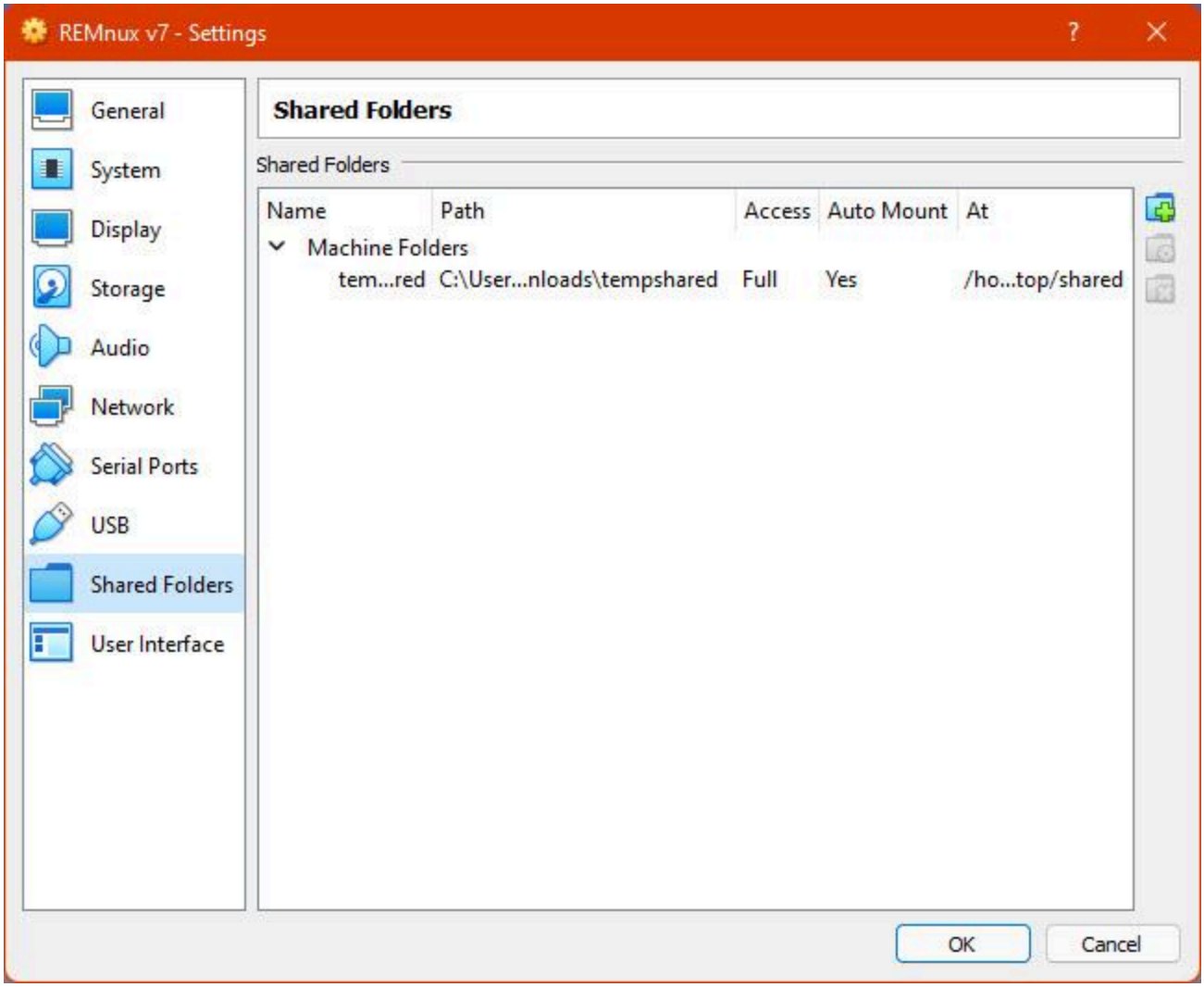


- **تمكين محول الشبكة:** سيؤدي تعطيل هذا إلى إيقاف أي اتصال بين الجهاز الظاهري والأجهزة الأخرى في الشبكة (بما في ذلك جهازنا والذي سنقوم بإدارته باستخدام واجهة الرسم) وسوف يحاكي غياب أجهزة الاتصال بأي شبكات في الجهاز الظاهري.
- **مرفق بـ -- ترجمة عناوين الشبكة (Attached to -- NAT):** هذا هو التكوين الافتراضي ويحاكي شبكة جديدة للجهاز الافتراضي ويسمح له بالوصول إلى الإنترنت ولكن أيضًا إلى الأجهزة الأخرى في شبكتنا وهذا غير موصى به لنوع استخدام الجهاز الافتراضي.
- **مرفق بـ -- محول الجسر (Attached to -- Bridged Adapter):** سيؤدي هذا إلى مشاركة محول الشبكة لجهاز الكمبيوتر المضيف الفعلي الخاص بنا مع الجهاز الافتراضي مما يجعله يظهر مثل أي جهاز آخر على شبكتنا، ولا ينصح بهذا أيضًا لحالة الاستخدام الخاصة بنا.
- **مرفق بـ -- محول المضيف فقط (Attached to -- Host-only Adapter):** يربط ذلك الجهاز الظاهري بشبكة متصلة فقط بجهاز المضيف الخاص بنا والأجهزة الظاهرية الأخرى التي لها التكوين ذاته وفي بعض الحالات قد يكون هذا مفيدًا، ولكن يمكن أن يعرض هذا أيضًا الجهاز لنشاط ضار.
- **مرفق بـ -- الشبكة الداخلية (Attached to -- Internal Network):** على غرار الشبكة الأخيرة، ولكن لا يمكن الوصول إلى الجهاز المضيف الخاص بنا وهذا مفيد عندما نريد أن نرى كيف يتفاعل جهازان أو أكثر مع بعضهما البعض.
- **مرفق بـ -- غير مرفق (Attached to -- Not attached):** يحاكي هذا محول الشبكة دون كابل متصل به.

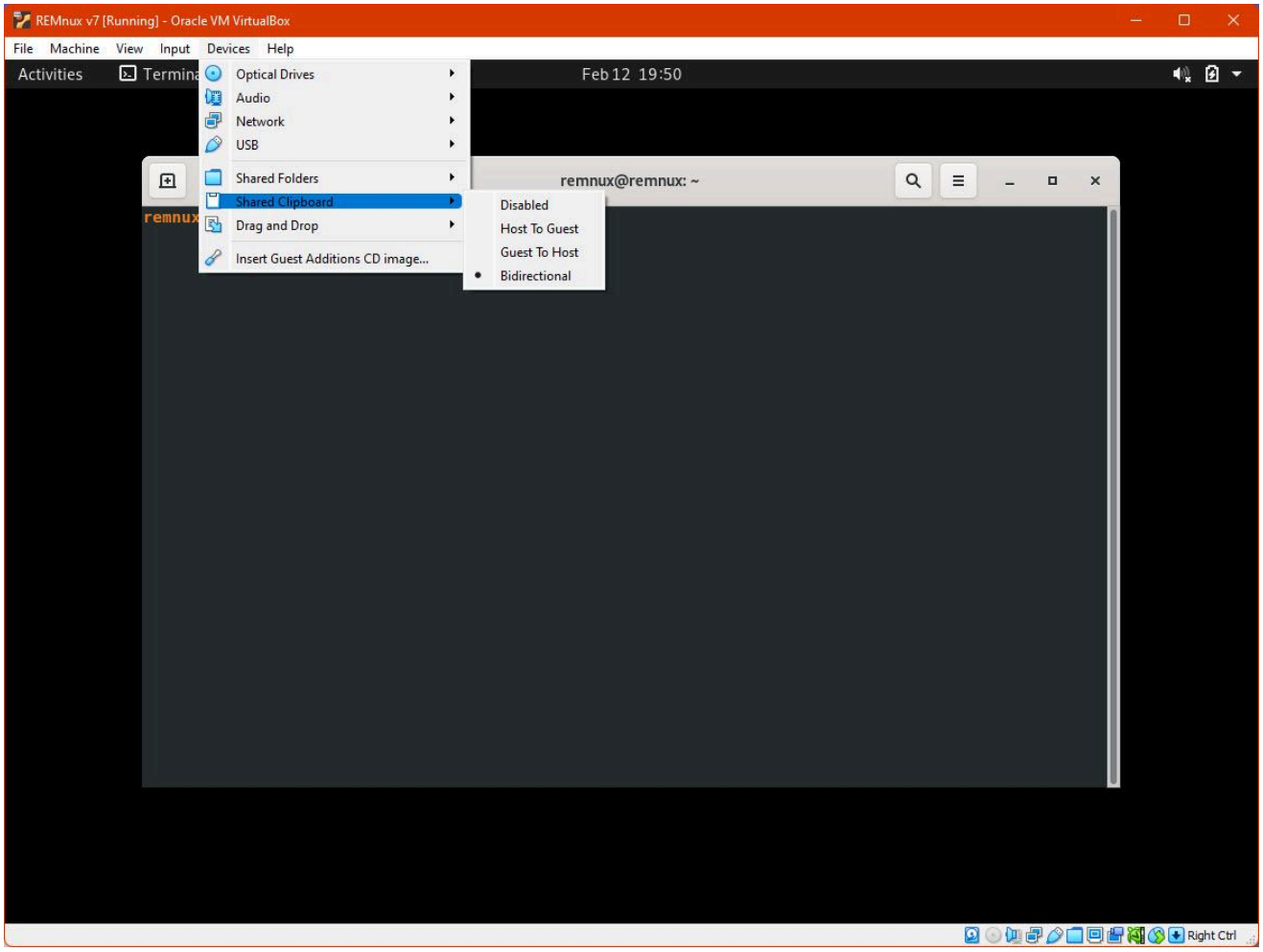
حسب الاستخدام المقصود من جهازنا بالنسبة للتكوين الأولي يمكننا إبقاء ترجمة عناوين الشبكة مفعلة للوصول إلى الإنترنت لتنزيل الأدوات وما إلى ذلك، وقبل بدء تحليلنا يمكننا تغييره إلى غير مرفق أو شبكة داخلية أو تعطيل المحول.

تكوينات إضافية على فيرتشول بوكس -- مشاركة المعلومات مع الجهاز المضيف

من المعتاد جدًا مشاركة الملفات والبيانات الأخرى بين جهاز الكمبيوتر الخاص بنا والجهاز الافتراضي، ومرة أخرى هناك طرق مختلفة يمكننا اعتمادها:**المجلدات المشتركة:** على غرار المجلد المشترك على الشبكة ويمكننا مزامنة مجلد واحد بين النظام المضيف والضيف لدينا (الجهاز الظاهري). لا ينصح دائمًا بذلك لمشاركة عينات البرمجيات الضارة لأنه يفتح مساحة في جهاز الكمبيوتر الخاص بنا يتحكم بها الجهاز الظاهري لدينا والذي يمكن أن يصاب خلال لحظات من تحليلنا. يوجد قسم مخصص في الإعدادات لأجل تكوين المجلدات المشتركة.



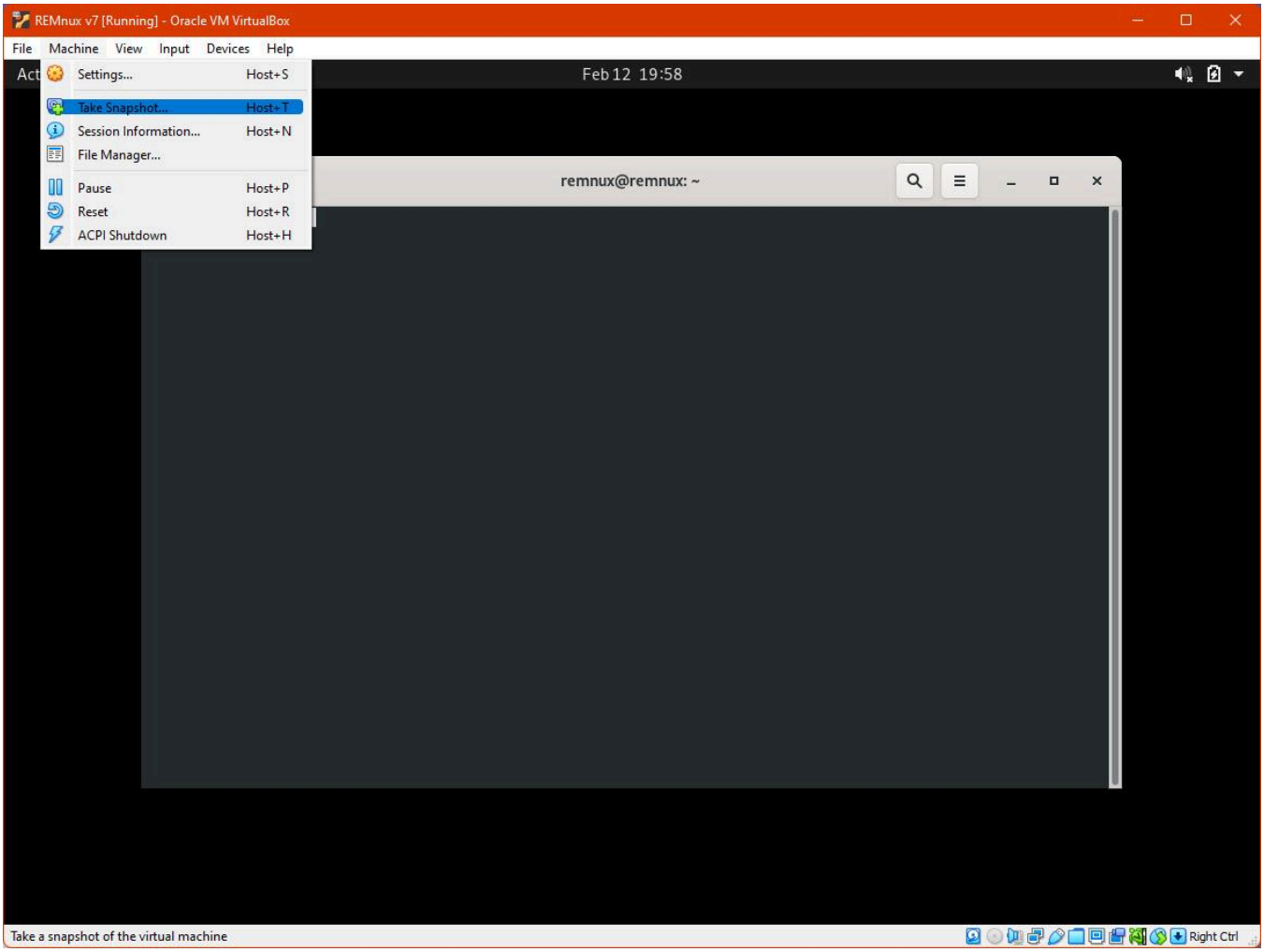
- **الحافظة المشتركة والسحب والإفلات:** سيتيح لنا ذلك مشاركة الحافظة بين جهاز الكمبيوتر الخاص بنا والجهاز الافتراضي ويمكن تعطيلها أو جعلها أحادي الاتجاه أو ثنائية الاتجاه كما هو مقترح في الصورة. تشبه سحب وإفلات الملفات بين أنظمة المضيف والضيف. بالنسبة للبعض فإن تعطيل مشاركة المجلدات وتمكين السحب والإفلات فقط من "المضيف إلى الضيف" هو الخيار الأكثر أمانًا لحماية أجهزة الكمبيوتر المادية على غرار مشاركة الحافظة ولكن قد نحتاج في بعض اللحظات إلى استخراج المعلومات من الجهاز الافتراضي.



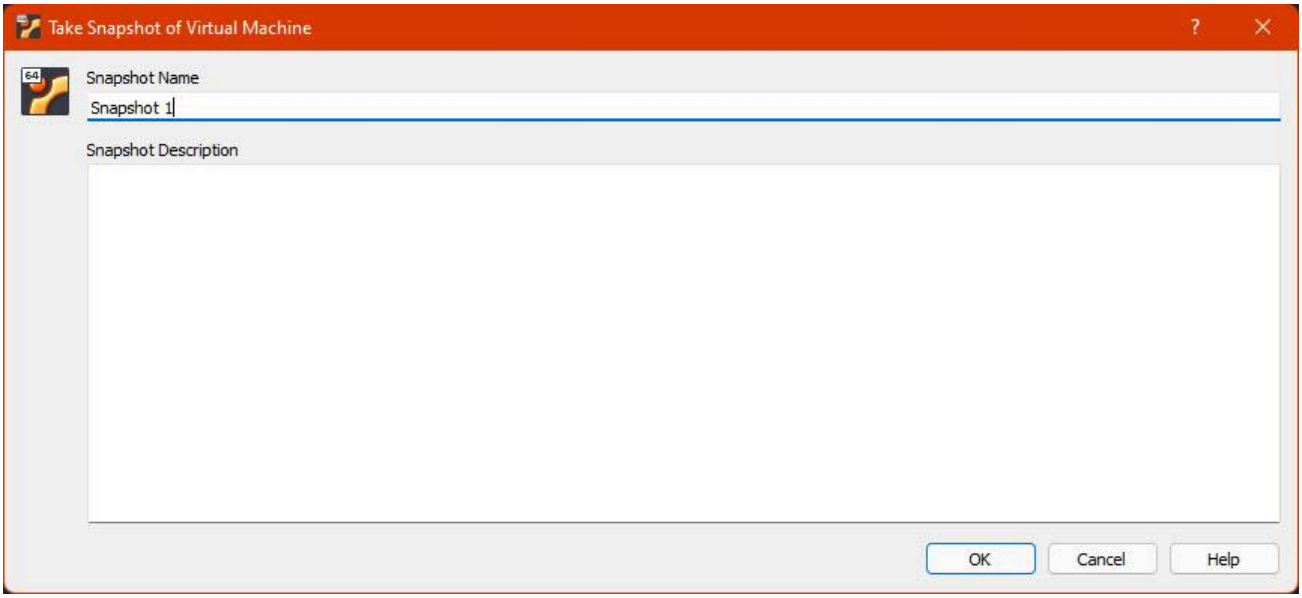
تكوينات إضافية على فيرتشول بوكس -- لقطات

إحدى الميزات المفيدة جدًا في فيرتشول بوكس هي إمكانية حفظ إصدار من الجهاز الظاهري يمكننا الرجوع إليه في أي وقت في المستقبل، وبالتالي إذا قمنا على سبيل المثال بتكوين جهاز ريمنوكس لتحليل البرمجيات الضارة فقد نرغب في حفظ لقطة قبل بدء التحليل وعندما ننتهي يمكننا إعادة الجهاز الظاهري إلى اللقطة المحفوظة للتأكد من أن الجهاز غير مصاب ونحن على استعداد لمواصلة التحليل.

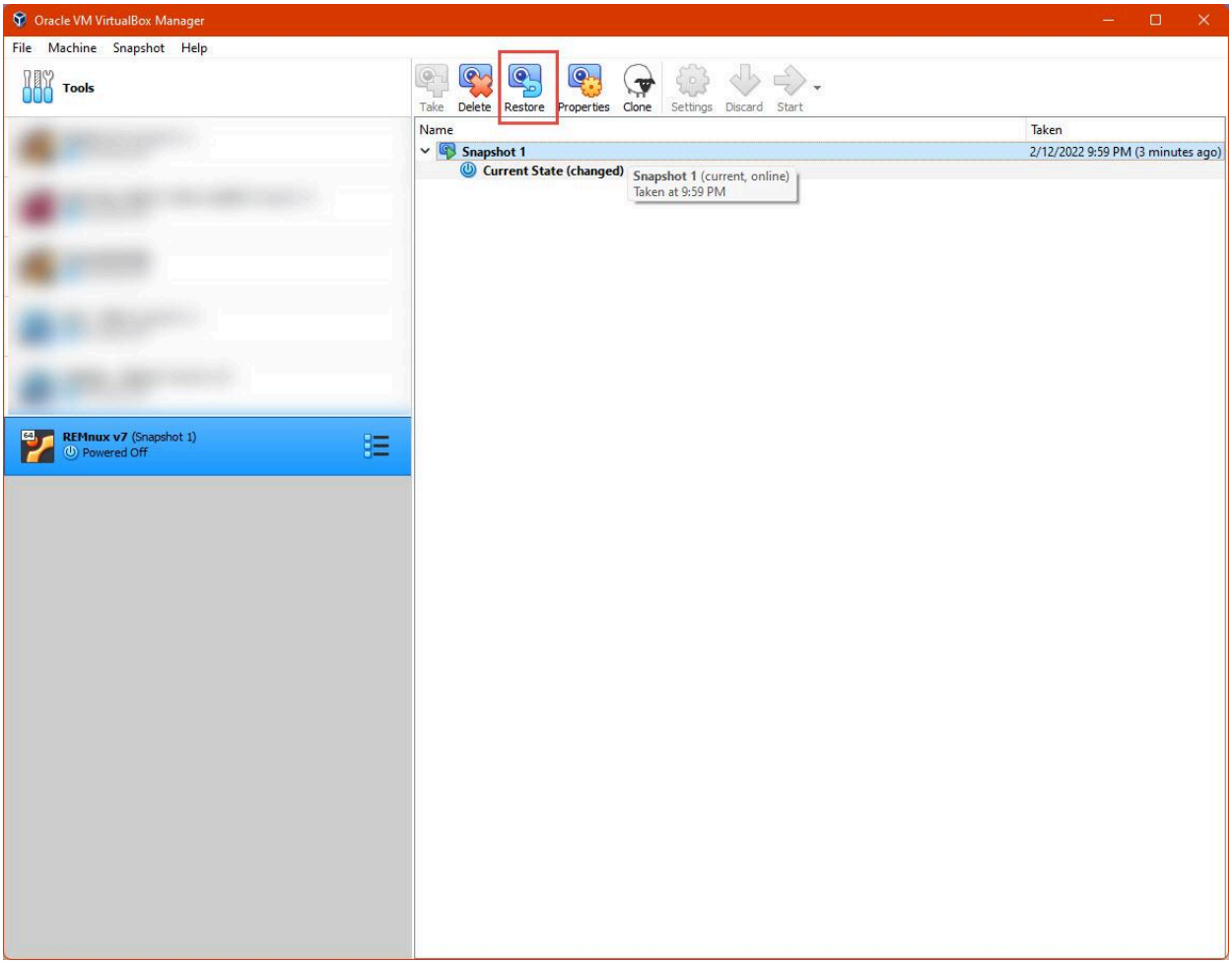
لأجل حفظ اللقطة بعد التأكد من وجود الجهاز في الحالة المطلوبة انقر على "جهاز (Machine)"، ثم "التقاط لقطة (Take Snapshot)"



ثم حدد اسمًا وانقر على "OK (موافق)" وسيستغرق إنشاء اللقطة بعض الوقت وبعدها سيكون متاحًا في قسم اللقطات (Snapshots) على الشاشة الرئيسية لفيرتشول بوكس على جهازنا الافتراضي.



يمكننا استخدام زر "استعادة (Restore)" على الشاشة المعنية.



الخطوات التالية

نظرًا لأنه يمكننا التعامل مع الأساسيات باستخدام فيرتشول بوكس، يمكننا التعرف على ريمنوكس أثناء فهم وتحليل نوع تنسيق الملف الأول وهو ملفات بي دي إف (PDF).