Analisis dokumen-dokumen berbahaya – Bagian 01 – Pendahuluan dan Mesin Virtual (VM)

Pendahuluan

Kursus (singkat) ini ditujukan untuk para penggemar dan praktisi keamanan digital (dukungan teknis, fasilitator, penanggap pertama, dll.) yang ingin mempelajari lebih lanjut tentang dokumen berbahaya serta cara mengidentifikasinya. Dokumen-dokumen ini dapat berupa lampiran surel, berkas di diska lepas, atau unduhan dari situs web tertentu. Tujuan utamanya adalah:

- Mempelajari dasar-dasar bagaimana cara kerja format dokumen umum dan bagaimana format tersebut dapat digunakan sebagai senjata, dengan penekanan khusus pada berkas Portable Document Format (PDF) dan dokumen Microsoft Office (setidaknya dari MS Word, Excel, dan PowerPoint).
- Memperkenalkan beberapa alat yang mungkin membantu mengidentifikasitanda-tanda dokumen berbahaya atau memastikan bahwa dokumen tersebut aman untuk dibuka.
- Menyediakan beberapa saran keamanan serta mengklarifikasi keraguan umum tentang penanganan berkas mencurigakan.

Kursus ini menggunakan format beberapa bacaan singkat dan kuis di sebagian besar konten yang dibahas, yang mana tergantungpada materinya, akan diperlukan untuk menjalankan beberapa alat. Hal ini akan dibahas di bagian Lingkungan kerja segera setelah pendahuluan, persyaratan umumnya adalah:

- Untuk menyelesaikan latihan yang diajukan:
    - Kapasitas dalam menjalankan 1) mesin virtualdi komputer menggunakan Virtualbox atau perangkat lunak serupa, atau 2) skrip python (hanya untuk menganalisis berkas kursus, bukan untuk menganalisis sampel yang sebenarnya).
- Waktu untuk membahas materi (sekitar 2 jam)

Kursus ini mengambil materi yang tersedia di beberapa referensi lain, dan hanya menggunakan alat-alat yang tersedia secara gratis. Sebagian besar kontennya terinspirasi oleh karya Didier Stevens dari waktu ke waktu, khususnya untuk SANS, serta beberapa referensi lain, daftar pendeknya mungkin adalah:

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

Struktur

Penafian
Beberapa pertimbangan pemodelan ancaman
Untuk setiap jenis format berkas (PDF, MS Office)
    Bagaimana mereka disusun (dengan cara yang lebih teknis)
    Bagaimana mereka bisa dijadikan senjata
    Bagaimana kita bisa melakukan analisis pendahuluan
    Beberapa kesimpulan/fakta tentang format berkas
Beberapa saran umum terhadap ancaman terkait
Apa selanjutnya

Berikut ini adalah beberapa penafian yang berguna sebelum memulai materi ini

Penafian

Mengingat sifat tugas yang akan dilakukan setelahmenguasai konten yang disediakan (menganalisis berkas berbahaya), serta kompleksitas topiknya (yang dilihat sebagai pendahuluan analisis perangkat lunak berbahaya), kami sangat menyarankan untuk membaca bagian ini dan menyetujui semua poin-poin sebelum melanjutkan.

Kursus ini bersifat sebagai pendahuluan: ia dirancang untuk orang-orang yang belum memiliki pengalaman sebelumnya dalam menganalisis dokumen yang mencurigakan. Di bagian Langkah berikutnya, kami menyertakan daftar sumber daya untuk bacaan dan referensi lebih lanjut.
Kursus ini tidak membahas banyak teknik tingkat lanjut: ada banyak ancaman spesifik yang kompleksitasnya berada di luar cakupan materi ini, juga, seperti segala hal yang berhubungan dengan keamanan informasi, mungkin ada ancaman yang menunggu untuk ditemukan yang tidak akan dibahas dalam kursus ini. Kami sarankanuntuk mencari bantuan jika ada dugaan bahwa kita melihat ancaman tingkat lanjut atau tidak dikenal dalam sebuah berkas atau

artefak lainnya, yang akan dibahas di bagian selanjutnya. Meskipun demikian, kursus ini akan membantu kita memahami dengan lebih baik seperti apa biasanya tampilan berkas yang tidak berbahaya tersebut, alih-alih seperti apa tiap dokumen berbahaya disusun.

Ambil tindakan pencegahan saat menganalisis berkas di kondisi nyata: sampel yang digunakan dalam kursus ini tidak berbahaya, walaupun begitu, mengulang alur kerja yang disajikan ke dalam sampel yang sebenarnya tanpa masing-masing keamanan yang terukur, kemungkinan besar akan menyebabkan peranti Anda terinfeksi. Jangan menjalankan berkas mencurigakan apa pun di komputer utama Anda; gunakan mesin virtual, peranti khusus, atau lingkungan lain yang dapat Anda gunakan untuk menganalisis properti berkas tersebut tanpa mengeksekusi berkasnya di mesin Anda.

Kuis bagian penafian

Pertanyaan 1:Saya memahami risiko menganalisis berkas yang mencurigakan, potensi konsekuensi saat menjalankan perangkat lunak berbahaya baik secara sengaja atau tidak sengaja, saya membaca konten dari halaman/bagian ini, dan saya memahami strategi paling umum untuk mengatasi potensi ancaman-ancaman tersebut.

Pertanyaan 2:Manakah dari pilihan-pilihan berikut yang paling menggambarkan apa saja yang perlu kita lakukan saat menganalisis berkas yang benar-benar mencurigakan?

1. Kita harus memulai mesin virtual (VM) atau komputer khusus untuk menganalisis berkas tersebut dan memberikannya akses sesedikit mungkin kemesin hos kita dan seluruh jaringan

Benar – Jika berkas yang mencurigakan itu memang terinfeksi, segala kerusakan akan terjadi di tempat yang aman; selain memutuskan sambungan mesin dari lingkungan yang sebenarnya, rekomendasi lainnya adalah menyiapkan cara untuk mengembalikansistem operasi ke kondisi aman sebelumnya, memiliki alat pemantauan apabila kita ingin mengetahui perubahan apa saja yang dibuat selama potensi infeksi, serta menggunakan Sistem Operasi yang berbeda antara sistem hos dan tamu (guest system) untuk mengurangi infeksi yang tidak disengaja.

2. Kita dapatmenganalisis berkas tersebut di komputer/lingkungan kita sendiri tetapi tanpa memiliki akses ke internet

Salah – Bahkan meskipun memutuskan sambungan dari internet merupakan praktik yang direkomendasikan saat menganalisis berkas, berkas yang terinfeksi masih dapat menyalahgunakan komputer/sistem operasi utama Anda, atau membiarkannya lebih

siap merusak saat konektivitas kembali pulih.

3. Kita harus menganalisis berkas di komputer atau mesin virtual (VM) dengan Sistem Operasi yang kurang umum seperti Linux atau macOS

Salah – Bahkan ketika sebagian besar perangkat lunak berbahaya yang terkenal dirancang untuk Windows, ada juga kode berbahaya yang dirancang untuk sistem lain, dan hal terpenting ketika menganalisis berkas yang mencurigakan adalah menghindari infeksi di lingkungan utama kita, terlepas dari apa pun Sistem Operasinya. Meskipun saran ini dapat membantu mengurangi dampak negatif dari eksekusi perangkat lunak berbahaya yang tidak disengaja, tidaklah cukup tanpa serangkaian tindakan lain. Saran ini dianggap opsional dan tidak memberikan dampak besar jika kita memiliki lingkungan pengujian yang kuat.

Tentangmodel-model ancaman

Saat mencari saran tentang cara menangani berkas-berkas yang mencurigakan, biasanya pendekatan yang diajukan adalah menghindari interaksi apa pun dengan berkas tersebut, misalnya:

- Jangan membuka berkas yang tidak dikenal.
- Jangan berinteraksi dengan berkas yang mencurigakan.
- Jangan melakukan kontak mata denganberkas mencurigakan apa pun.

Atau, kita dapat menemukan jenis saran lain yang, meskipun cukup bagi kebanyakan orang, dapat menyesatkan pengguna yang sensitif seperti aktivis Hak Asasi Manusia atau jurnalis yang bekerja di lingkungan berbahaya, atau jelas-jelas kontraproduktif,misalnya:

- Menggunakan Antivirus sudah cukup untuk melindungi Anda dari berkas berbahaya.
- Hanya dokumen Microsoft Office dengan perintah makro yang berbahaya, jadi Anda dapat menangani jenis berkas lain tanpa terlalu khawatir.
- Hapus surel apapun yang berisi lampiran yang mencurigakan. Hal inimenjadi perhatian khusus dalam beberapa skenario karena jika kita menghapus surel dan lampiran tersebut dari kotak masuk, kita kehilangan bukti penting yang dapat membantu kita menilai apakah artefak tersebut memang berbahaya atau ditargetkan, yang bisa jadi merupakan informasi yang sangat berharga.

Dalam praktiknya,saat kita bekerja dengan komunitas yang menjadi target (terutama jurnalis), tidak berinteraksi dengan berkas bukanlah suatu pilihan. Banyak organisasi, kelompok, dan individu perlu membuka berkas yang berpotensi berbahaya sebagai bagian dari pekerjaan mereka, dan mereka akan melakukannya meskipun mengetahui

risikonya, beberapa contohnya:

- Jurnalis menerima undangan konferensi pers.
- Aktivis menerima dokumen pendukung sebagai alat bukti dalam kasus pelanggaran HAM atau sebagai pembocor.
- Lembaga yang berseteru di pengadilan mengirimkan dokumen yang harus ditinjau dan ditangani.

Satu faktor tambahan yang perlu dipertimbangkan adalah bahwa pelaku masyarakat sipil terpapar pada ancaman yang ditargetkan dan tidak diketahui oleh mesin Antivirus. Faktor lainnya tergantung pada jenis serangan; format berkas lain mungkin juga dijadikan senjata. Faktor-faktor ini penting untuk dipertimbangkan oleh orang-orang yang membantu kelompok rentan untuk lebih memahami bagaimana dokumen dan format berkas yang umum lainnya dapat dijadikan senjata, selain untuk memberikan saran yang bermanfaat, namun juga untuk membantu mereka menganalisis berkas tertentu untuk memahami dan menilai apakah mereka menjadi korban dari serangan yang ditargetkan.

Dengan mempertimbangkan semua hal tersebut, kita akan fokus pada pemahaman tentang bagaimana format berkas standar disusun, cara mengenali serangan paling umum yang menggunakannya, serta beberapa tindakan pertahanan terkini agar terhindar menjadi korban ancaman semacam ini.

Kuis bagian model ancaman

Pertanyaan 1: Untuk organisasi yang sangat ditargetkan yang menerima banyak dokumen Microsoft Office melalui surel, manakah dari pilihan berikut yang benar? (Hanya satu yang benar)

1. Meskipun perangkat lunak antivirus (AV) menyatakan bahwa berkas tersebut aman, berkas tersebut bisa jadi masih mengandung perangkat lunak berbahaya.

Benar – Ada kemungkinan (terutama bagi korban berisiko tinggi) untuk menjadi sasaran perangkat lunak berbahaya yang sangat spesifik yang tidak terekspos ke seluruh internet, sehingga mesin AV belum pernah mengenal perangkat lunak tersebut dan tidak dapat mendeteksinya sebagai berbahaya. Selain itu, ada banyak teknik yang digunakan pelaku kejahatan untuk menyamarkan perangkat lunak berbahaya sebagai data sah yang terkadang menyulitkan perangkat lunak AV untuk mendeteksi kode berbahaya.

2. Mereka perlu segera menghapus lampiran apa pun yang mencurigakan karena bisa

berbahaya jika berada di kotak masuk.

Salah – Lampiran di kotak masuk tidak akan dieksekusi di komputer tanpa izin eksplisit dari pengguna (atau setidaknya dalam serangan yang diketahui), terutama jika disimpan di peladen eksternal. Jadi, menghapusnya dengan segera akan membuat kita kehilangan bukti berharga jika kita ingin meneliti lebih lanjut tentang berkas dan surel tersebut.

3. Mereka tidak boleh membuka lampiran apa pun dari sumber yang tidak dikenal.

Salah – Bahkan ketika hal tersebut memastikan bahwa berkas-berkas berbahaya tidak akan dieksekusi, kita harus memahami bahwa audiens yang rentan sering kali perlu berinteraksi dengan informasi dari sumber-sumber yang tidak tepercaya untuk mencapai misi mereka, sehingga ketiadaan interaksi merupakan saran yang tidak dapat dipertahankan dalam kebanyakan kasus.

Lingkungan: Pertimbangan umum

Untuk mengeksekusi sebagian besar tugas pada kursus ini, kita akan menggunakan alat dasar yang ditulis dalam bahasa pemrograman Python. Mengingat kompatibilitas Python yang luas dengan setiap Sistem Operasi, ada banyak cara untuk menyiapkan lingkungan. Kami mengusulkan satu cara khusus, tetapi jika Anda terbiasa denganPython, analisis perangkat lunak berbahaya, dan/atau virtualisasi, Anda dapat menyiapkan versi lain yang sesuai untuk Anda. Satu-satunya permintaan yang kuat adalah agar Anda memiliki lingkungan yang terisolasi untuk memanipulasi artefak berbahaya (dalam hal ini berkas). Ada pertimbangan lain, tetapimungkin ini yang paling penting.

Lingkungan yang terisolasi dan praktik baik lainnya

Sampel yang digunakan dalam kursus ini tidak berbahaya, hanya untuk menunjukkan bagaimana berkas tersebut tersusun dan cara mengenali tanda bahaya. Namun, jika Anda berniat menganalisis berkas yang sebenarnya, kemungkinan besar Anda akan menemukan berkas yang terinfeksi yang dapat menyebabkan berbagai macam masalah, seperti menginfeksi komputer yang Anda gunakan, menyalahgunakan informasi Anda, atau membuat peranti Anda tidak dapat digunakan, dan lain sebagainya. Oleh karena itu, sudah menjadi praktik umum untuk memiliki lingkungan

yang khusus untuk menganalisis dan menjalankan sampel yang mencurigakan dengan cara yang terkendali, sehingga jika terjadi kesalahan saat memanipulasi sampel, ini tidak akan memengaruhi peranti Anda atau informasi yang terkandung di dalamnya.

Keuntungan lain dari memiliki lingkungan khusus adalah setelah Anda memanipulasi sampel perangkat lunak berbahaya, Anda dapat menghapus semuanya dan memulai kembali tanpa harus takut kehilangan berkas-berkas yang tidak terkait. Hal ini memungkinkan kita untuk merencanakan cara-cara praktis dalam "mengatur ulang" lingkungan kita ke kondisi siap pakai sebelum melakukan tiap analisis.

Salah satu strategi yang paling sering digunakan untuk menjamin lingkungan yang terisolasi adalah dengan menggunakan mesin virtual (VM), yang pada dasarnya meniru komputer lengkap di dalam komputer lain, termasuk Sistem Operasi (OS), diska keras, layar, dll. Alat yang umum untuk menyiapkan dan menggunakan VMadalahVirtualbox dan VMware Workstation Player, di antara yang lainnya. Menggunakan perangkat keras khusus juga menjadi pilihan selama perangkat tersebut aman dari infeksi.

Salah satu potensi kerugian adalah beberapa perangkat lunak berbahaya menyertakan kode untuk memeriksa jika perangkat berbahaya tersebut dieksekusi di lingkungan yang terisolasi dan tidak berjalan, sehingga lebih sulit untuk menganalisisnya. Namun, bahaya yang melekat dari menjalankan perangkat berbahaya di lingkungan kita sehari-hari tidak layak untuk dicoba. Kami sarankan untuk mencari bantuan, yang berfokus pada teknik yang tidak bergantung pada menjalankan berkas yang mencurigakan, atau mendapatkan informasi tentang cara menyiapkan lingkungan yang terlihat seperti mesin yang sebenarnya untuk sampel perangkat berbahaya. Untuk sumber daya ini, seharusnya tidak menjadi masalah karena kita tidak akan mengeksekusi kode apa pun dari dokumen, tetapi jika Anda ingin mempelajari dan melakukan analisis dinamis pada berkas yang mencurigakan, hal ini akan berguna.

Pertimbangan lainnya

Selain praktik yang baik dengan memiliki lingkungan yang terisolasi, praktik umum lainnya adalah:

- **Pastikan komputer yang Anda gunakan tidak terhubung ke internet atau jaringan lokal:** terutama jika Anda membuka berkas yang mencurigakan, alasan yang paling sering dilakukan dalam melakukan hal ini adalah untuk menghindari pemicu sinyal yang akan memperingatkan operator perangkat berbahaya bahwa kode tersebut sedang dieksekusi atau diuji berdasarkan data lain seperti alamat IP, atau jenis peranti yang mengeksekusi perangkat berbahaya tersebut. Selain

itu, beberapa perangkat berbahaya akan mencoba menyebar ke jaringan lokal, mencoba menginfeksi peranti lain yang tidak diinginkan, sehingga sudah menjadi praktik umum untuk mengisolasi peranti pengujian di jaringan fisik atau virtual (atau VLAN) yang berbeda. Perlu diingat bahwa jika sampel dianalisis dengan cara mengeksekusinya, ada kemungkinan perangkat berbahaya tersebut mendeteksi bahwa ia tidak memiliki akses ke Internetsehingga tidak berjalan.

Jika Anda akan terhubung ke internet, gunakan VPN atau sejenisnya: idenya adalah untuk menyembunyikan lokasi Anda yang sebenarnya jika perangkat berbahaya yang kita analisis berjalan dan memberi sinyal kepada operatornya. Sekali lagi, biasanya tidak disarankan untuk mengeksekusi perangkat berbahaya tanpa tindakan-tindakan untuk menghindari potensi komunikasi dengan operator, namun, menggunakan VPN mungkin merupakan tindakan yang baik jika terjadi eksekusi yang tidak disengaja atau jika konfigurasi yang lain gagal di beberapa saat.

Atur proses untuk mengatur ulang lingkungan Anda ke keadaan "bersih": Tergantung pada apakah Anda menggunakan Mesin Virtual atau perangkat keras khusus, ada beberapa alat dan fitur yang berguna untuk mengatur ulang lingkungan sehingga setiap kali Anda menganalisis sampel, mesin akan bersih. Untuk VM yang menggunakan tangkapan kilat adalah contoh yang baik, dan ada perangkat lunak untuk membalikkan komputer fisik ke keadaan sebelumnya.

Tetap berpegang pada analisis statis: Secara umum, kita dapat membagi analisis perangkat berbahaya tergantung pada apakah kita mengeksekusi sampel atau tidak. Analisis statis mencoba membedah berkas dan artefak lain untuk mengumpulkan sebanyak mungkin wawasan dengan tidak mengeksekusinya, sementara analisis dinamis mengeksekusi sampel untuk melihat perubahan apa yang terjadi di lingkungan pengujian. Tergantung pada jenis perangkat berbahaya, satu jenis analisis mungkin lebih berguna daripada yang lain, tetapi secara umum, analisis dinamis akan memerlukan lebih banyak tindakan untuk melindungi lingkungan pengujian dan jaringan agar dapat mendukung eksekusi perangkat berbahaya yang sebenarnya. Kursus ini hanya menunjukkan teknik analisis statis.

Berhati-hatilah saat memublikasikan sampel atau informasi lain dari sampel yang dianalisis: Secara umum, hal ini bisa jadi memperingatkan operator perangkat berbahaya tentang kita yang sedang menganalisis kampanye perangkat tersebut, membuat mereka dapat mematikan infrastrukturnya, membersihkan jejak apa pun untuk mempersulit atribusi, dll. Hal ini berlaku untuk semua platform publik seperti media sosial dan situs web, termasuk beberapa platform publik tempat kita dapat mengirim berkas untuk dianalisis di awan guna mencari tanda dari mesin Antivirus dan komunitas keamanan informasi. Untuk skenario terakhir, kami akan membagikan beberapa contoh dan teknik untuk memeriksainformasi yang kita butuhkan tanpa memperingatkan siapa pun.

Kuis bagian Lingkungan

Pertanyaan 1: Manakah dari pernyataan berikut yang benar?

1. Menjalankan sampel akan memerlukan lebih sedikit tindakan keamanan dibandingkan mencoba membedah artefak untuk mencari wawasan yang berguna.

Salah – Mengeksekusi perangkat berbahaya akan menginfeksi lingkungan yang kita gunakan; menyebabkan hal-hal seperti pemberitahuan kepada pembuatnya, perangkat berbahaya yang mencoba menginfeksi peranti lain dalam jaringan, serta membuat peranti tidak dapat digunakan. Semua konsekuensi ini memerlukan tindakan-tindakan keamanan yang lebih baik daripada menganalisis sampel tanpa menjalankannya (dikenal sebagai Analisis Statis)

2. Memutus akses ke internet akan mempersulit sampel perangkat berbahaya untuk memberi tahu pembuatnya bahwa perangkat berbahaya tersebut telah dieksekusi.

Benar – Tanpa akses internet, perangkat lunak berbahaya tidak akan dapat berkomunikasi dengan peladen eksternal untuk mengeksekusi tindakan tertentu, termasuk memberi tahu pengeksekusiannya. Perlu diketahui juga bahwa beberapa perangkat berbahaya menggunakan internet untuk mengunduh bagian lain dari kodenya, jadi memutus akses juga bisa menjadi masalah karena kita tidak akan memiliki wawasan tentang keseluruhan fungsi tanpa memperoleh bagian yang hilang. Namun, risiko yang terkait dengan menjalankan perangkat berbahaya secara tidak sengaja, membuatnya lebih baik untuk memutus koneksi dan melihat selama proses analisis apakah kita melewatkan sesuatu yang penting.

3. Cara paling efisien untuk menganalisis perangkat berbahaya adalah dengan menggunakan Mesin Virtual (VM) karena jika mesin terinfeksi, kita dapat membuatnya lagi dari awal.

Salah – Yang membuat VM lebih efisien untuk digunakan dalam analisis perangkat berbahaya adalah kemampuannya untuk mengambil"tangkapan kilat". Jadi kita dapat mengambil satu tangkapan keadaan VM sebelum memulai analisis, dan setelah selesai kita dapat mengembalikan VM ke tangkapan kilat tersebut, sehingga kita sudah siap menganalisis sampel berikutnya dengan cara yang terkendali. Cara ini jauh lebih cepat daripada membuat ulang VM dari awal setiap saat. (Sejujurnya, ini hal yang sulit)

Contoh lingkungan: Remnux + Virtualbox

Jika Anda menginginkan lingkungan fungsional yang siap digunakan, kami sarankan untuk menggunakan Remnux, mesin virtual (VM) yang dapat diunduh dan telah dikonfigurasi sebelumnya dengan beberapa alat yang berguna untuk analisis perangkat berbahaya. Di sini, kita akan menggunakan Virtualbox untuk membuat virtualisasi mesin Remnux. Jika Anda sudah familier dengan proses ini, silakan lanjut ke bagian kursus berikutnya.

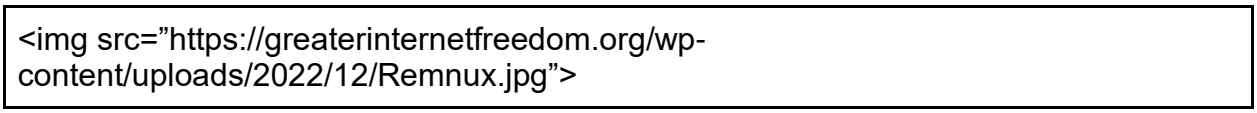
Memasang Virtualbox

Pertama, kita memerlukan program untuk mengelola mesin virtual kita.Kami memilih Virtualbox karena ia merupakan solusi yang paling banyak digunakan dan kompatibel dengan tiga platform utama (Windows, macOS, dan Linux) serta gratis. Untuk mengunduh masing-masing pemasangnya, kunjungi https://www.virtualbox.org/ dan cari tombol biru besar. Kemudian, cari bagian dengan paket berdasarkan platform seperti yang ditunjukkan pada gambar.

Di sini, klik platform Anda, dan ikuti petunjuknya. Setelah itu, Anda dapat menjalankan Virtualbox dan melihat jendela seperti ini

Anda belum memiliki apa pun di area yang kabur, dari sini kita siap mengunduh dan memasang Remnux

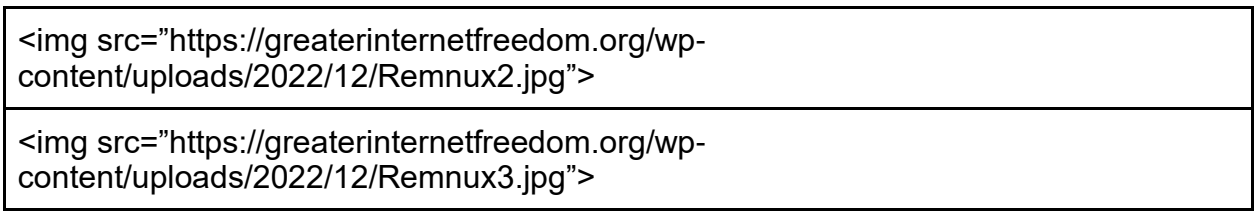
Memasang Remnux
Sekarang, Anda dapat pergi ke https://remnux.org/ klik “Unduh” di bagian yang sesuai.Ada kemungkinan Anda akan diarahkan ke halaman lain yang meminta Anda untuk memilih apakah Anda ingin mengunduh General OVA atau Virtualbox OVA, dalam kasus kita, pilihan yang terakhir adalah yang benar.



Setelah mengunduh berkas tersebut, sebaiknya periksa apakah berkas diunduh dengan benar. Untuk melakukan hal ini, kita perlu memeriksa hash terkait dari berkas tersebut. Hashing adalah topik padat yang kami anjurkan untuk dipelajari dan diterapkan (juga sangat digunakan dalam analisis perangkat berbahaya),tetapi untuk saat ini, kita dapat meringkasnya sebagai proses matematis yang mengubah sepotong data (seperti teks atau berkas) menjadi kode alfanumerik. Kode ini harus unik untuk data yang Anda analisis, bahkan dengan perubahan kecil, hash akan banyak berubah.Jadi, dengan memeriksa apakah berkas yang kita unduh memiliki hash yang sama dengan yang dipublikasikan di situs web Remnux akan memberi tahu kita bahwa berkas tersebut diunduh dengan tanpa masalah. Jika hash-nya berbeda, itu akan menjadi tanda bahwa berkas tersebut rusak karena proses pengunduhanyang salah atau entah bagaimana itu bukan berkas yang benar (mungkin kesalahan di pihak kita saat memilih versi yang tepat, atau sebagai skenario jarak jauh, seseorang telah mengubah berkasnya menjadi versi yang berbahaya, jadi waspadalah). Referensi singkat tentang cara memeriksa hash tersedia dihttps://technastic.com/check-md5-checksum-hash/

Mengunduh berkas

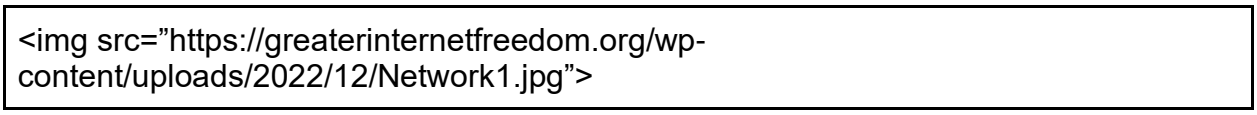
Setelah memeriksa bahwa berkas kita telah diunduh dengan tanpa masalah, sekarang kita dapat mengimpornya ke Virtualbox. Di halaman Remnux tempat kita mengunduh VM, terdapat petunjuk yang tersedia, namun, cukup dengan mengeklik dua kali berkas .ova, dan wisaya akan memandu kita melalui proses impor. Kita dapat membiarkan semuanya seperti yang disarankan dalam konfigurasi yang diajukan. Pada akhirnya, kita akan melihat mesin Remnux di jendela Virtualbox kita. Mengeklik"Mulai" akan menyalakan mesin kita di jendela terpisah. Ini adalah mesin Linux, dan untuk kredensial log masuk pengguna adalah "remnux" serta kata sandinya adalah "malware" (namun, ada kemungkinan bahwa sesi akan terbuka tanpa meminta kredensial).



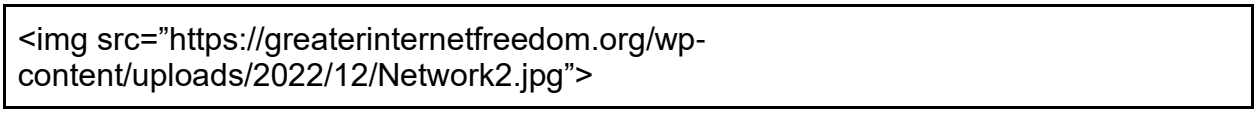
Konfigurasi tambahan pada Virtualbox – Jaringan

Mengingat bahwa kita akan menganalisis berkas yang berpotensi berbahaya,tidak disarankan untuk menjalankan mesin dengan cara yang dapat berkomunikasi dengan jaringan kita yang lain. Strategi spesifik lain mungkin berbeda-beda tergantung pada

gaya analis, namun sebagian besar konfigurasi dilakukan di layar antarmuka VM kita. Dengan mesin Remnux kita dimatikan, kita klik tombol “Pengaturan” di bilah alat.



Kemudian di bagian “Jaringan”, Anda akan memiliki serangkaian opsi, yang paling penting adalah:

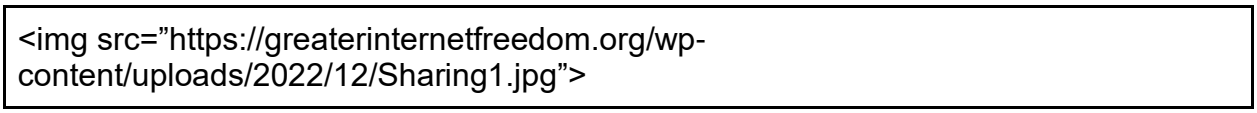


- **Aktifkan Adaptor Jaringan:** menonaktifkan hal tersebut akan menghilangkan konektivitas apa pun antara VM kita dan peranti-peranti lain melalui jaringan (Termasuk milik kita, kita akan mengelolanya menggunakan antarmuka grafis), opsi ini akan meniru ketiadaan perangkat keras untuk terhubung ke jaringan apa pun di VM.
- **Terhubung ke – NAT:** Konfigurasi bawaan, akan meniru jaringan baru untuk VM. Ini memungkinkan VM untuk mengakses internet, tetapi juga peranti-peranti lain dalam jaringan kita. Opsi ini tidak direkomendasikan untuk jenis penggunaan yang akan kita berikan pada VM kita.
- **Terhubung ke – Adaptor Jembatan:** Ini akan membagikan adaptor jaringan komputer hos fisik kita ke VM, menempatkannya seperti peranti lain di jaringan kita. Opsi ini juga tidak direkomendasikan untuk kasus penggunaan kita.
- **Terhubung ke – Adaptor Khusus Hos:** ini akan menghubungkan VM ke jaringan yang hanya terhubungke mesin hos kita dan VM lain dengan konfigurasi yang sama. Dalam beberapa kasus opsi ini mungkin berguna, tetapi, ini juga dapat membuat mesin kita rentan terhadap aktivitas berbahaya.
- **Terhubung ke – Jaringan Internal:** mirip dengan yang terakhir tetapi mesin hos kita tidak dapatdiakses, opsi ini berguna ketika kita ingin melihat bagaimana dua atau lebih mesin berinteraksi satu sama lain.
- **Terhubung ke – Tidak terhubung:** Opsi ini meniru adaptor jaringan tanpa kabel yang terhubung

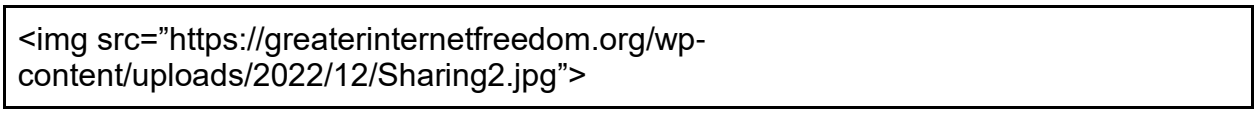
Bergantung pada penggunaan yang akan kita berikan pada mesin kita, untuk konfigurasi awal kita dapat membiarkan NAT tetap aktif untuk mengakses Internet guna mengunduh alat, dll., dan sebelum memulai analisis, kita dapat mengubahnya menjadi Tidak terhubung, Jaringan Internal, atau menonaktifkan adaptor.

Konfigurasi tambahan pada Virtualbox – Berbagi informasi denganmesin hos

Berbagi berkas dan data lain antara komputer kita dan VM merupakan hal yang biasa, sekali lagi, ada beberapa pendekatan berbeda yang dapat kita terapkan:**Folder bersama**: mirip dengan folder bersama jaringan, kita dapat menyinkronkan satu folder antara hos dansistem tamu kita (Mesin Virtual). Tidak selalu disarankan untuk berbagi sampel perangkat berbahaya karena akan membuka ruang di komputer kita yang dikendalikan oleh VM kita, yang dapat terinfeksi pada saat kita melakukan analisis. Untuk mengonfigurasi folder bersama, ada bagian khusus dalam pengaturan.



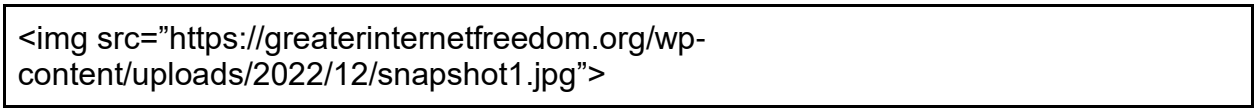
Papan klip bersama dan Seret-Lepas: Hal ini memungkinkan kita berbagi papan klip antara komputer kita dan VM, ia dapat dinonaktifkan, diatur searah, atau dua arah seperti yang disarankan dalam gambar. Mirip untuk seret-lepas berkas antara sistem hos dan tamu. Bagi sebagian orang, menonaktifkan folder bersama dan mengaktifkan seret-lepas hanya dari "Hos ke Tamu" adalah opsipaling aman untuk melindungi komputer fisik kita, mirip dengan papan klip bersama, namun, dalam saat tertentu kita mungkin perlu mengekstrak informasi dari VM.



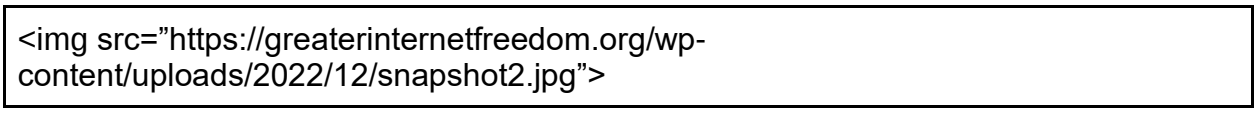
Konfigurasi tambahan pada Virtualbox – Tangkapan kilat

Salah satu fitur Virtualbox yang sangat berguna adalah menyimpan versi VM yang dapat kita kembalikan pada titik tertentu di masa mendatang. Jadi misalnya, jika kita mengonfigurasi mesin Remnux untuk menganalisis perangkat berbahaya, kita mungkin ingin menyimpan Tangkapan kilat sebelum memulai analisis, sehingga ketika kita selesai, kita dapat mengembalikan VM ke tangkapan kilat yang disimpan untuk memastikan mesin tidak terinfeksi, dan kita siap untuk melanjutkan analisis tersebut.

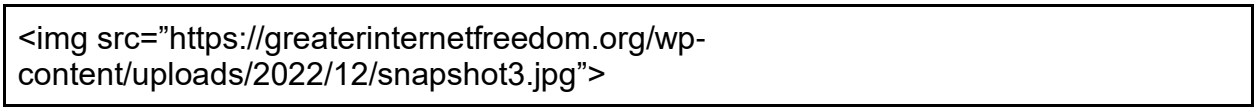
Untuk menyimpan tangkapan kilat, dengan mesin dalam keadaan yang diinginkan, klik “Mesin”,lalu “Ambil Tangkapan kilat



Kemudian pilih nama dan klik “OK”. Ini akan memakan waktu beberapa saat untuk membangun tangkapan kilat dan setelah itu akan tersedia di bagian Tangkapan kilatdi layar utama Virtualbox untuk VM kita.



Kita dapat menggunakan tombol “Pulihkan” pada layar masing-masing



Apa selanjutnya

Mengingat kita dapat menangani cara-cara dasar dengan Virtualbox, kita dapat mempelajari Remnux sambil memahami dan menganalisis format berkas pertama kita: PDF.