قسمت ۳ - تجزیه و تحلیل کاربردی بدافزارها

راهنمای جامع مهندسی معکوس، تجزیه و تحلیل بدافزارها،
باج‌افزارها، جاسوس‌افزارها، روت‌کیت‌ها و بوتکیت‌های رایانه‌ای

آزمایشگاه امنیت کی‌پاد

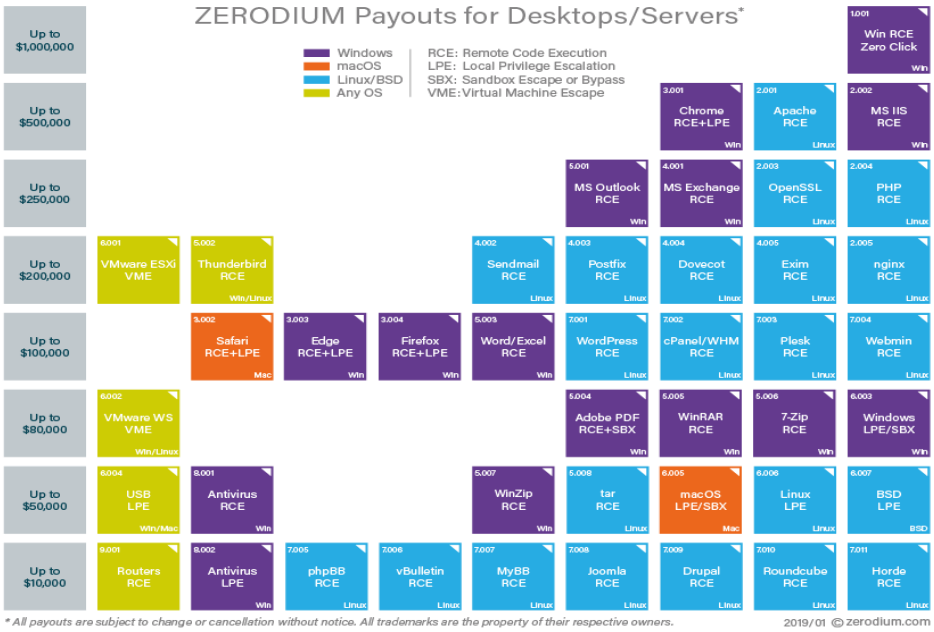
پیکربندی ماشین‌مجازی برای تحلیل بدافزار

قبل از این‌که بدافزاری را به منظور تجزیه و تحلیل دینامیک اجرا کنید، باید یک محیط ایمن راه‌اندازی کرده باشید. بدافزارهای جدید می‌توانند شامل موارد حیرت‌انگیزی باشند و اگر شما این نوع بدافزارها را در یک محیط غیر امین اجرا کنید، آن‌ها می‌توانند با استفاده از یک سری روش‌های خاص و اکسپلویت‌های 0day یا 1Day به سرعت خود را به سامانه‌های دیگر درون شبکه گسترش دهند و در آن موقع حذف آن‌ها یک کار خیلی دشوار خواهد شد. به هر صورت، یک محیط ایمن این اجازه را به شما می‌دهد، بدون آنکه سامانه خود و دیگر سامانه‌های درون شبکه را در معرض خطر قرار بدهید، بدافزارها را تجزیه و تحلیل کنید.

نکته : عموما اکسپلویت‌هایی را 0day یا 1day می‌خوانند که آسیب‌پذیری که آن‌ها مورد بهره‌برداری قرار می‌دهند کشف نشده باشد و هویت آن‌ها برای متخصصین امنیت مخفی بوده باشد.

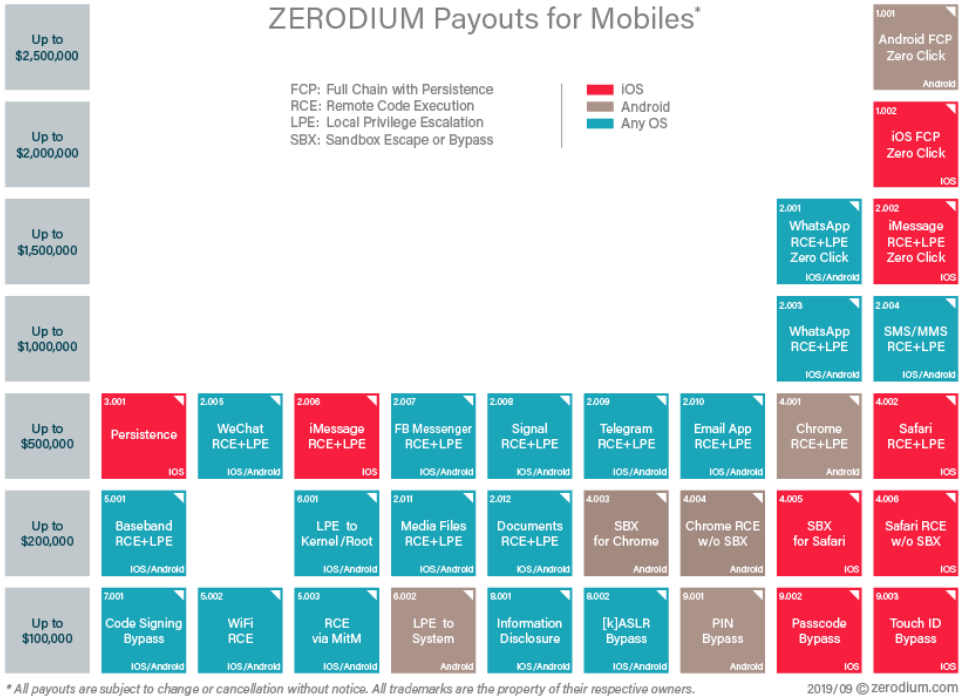
اکسپلویت‌های 0day بسیار گران قیمت هستند و اغلب برای موارد خیلی خاص توسط دولت‌ها مورد استفاده قرار می‌گیرند. در این مورد وب‌گاه‌هایی وجود دارند مانند وب‌سایت مشهور www.zerodayinitiative.com یا سایت www.zerodium.com که برای سامانه‌های گوناگون اکسپلویت 0day خریداری می‌کنند.

در تصویر ۱، لیست قیمت خریداری اکسپلویت‌های روز صفر یا 0day برای نرم افزارهای دسکتاپ و سرور مشاهده می‌کنید که متناسب با نوع پلتفرم آسیب‌پذیری و همچنین نوع اکسپلویت (افزایش سطح دسترسی یا اجرای کد از راه دور) تنوع قیمت زیادی دارند.



تصویر ۱: لیست قیمت آسیب‌پذیری‌های دسکتاپ و سرور

و در تصویر ۲ لیست قیمت خریداری اکسپلویت‌های روز صفر برای نرم‌افزارهای موبایل / تبلت را در وب‌سایت زیرودیوم مشاهده می‌کنید که آن ها همچنین متناسب نوعی که دارند، قیمت متفاوتی دارند.



تصویر ۲: قیمت آسیب‌پذیری‌های موبایل و تبلت

شایان ذکر است بدافزارها می‌توانند در ماشین‌های فیزیکی که از شبکه ایرگپ استفاده می‌کنند، مورد تجزیه و تحلیل قرار گیرند. در اصطلاح به این نوع شبکه رایانه‌ای ایزوله گویند، زیرا باعث می‌شود ماشین‌های فیزیکی به منظور ممانعت از گسترش بدافزارها نتوانند به اینترنت یا دیگر شبکه‌های رایانه‌ای لوکال دسترسی داشته باشند. در نتیجه شما می‌توانید از ماشین‌های فیزیکی یا ماشین‌های مجازی برای مطالعه ایمن روی بدافزارها استفاده کنید.

شبکه‌های ایرگپ به شما اجازه می‌دهند بدون این‌که دیگر رایانه‌ها را در معرض خطر قرار بدهید، بدافزارها را در یک محیط کاملا واقعی اجرا کنید. اما از آنجاییکه بیشتر قسمت‌های یک بدافزار به عنوان مثال برای به‌روزرسانی، کنترل و فرمان‌دهی و دیگر مزیت‌های تعبیه شده درون خود نیاز دارند به اینترنت دسترسی داشته باشند، یکی از عیب‌های اساسی استفاده از این روش عدم اتصال ماشین فیزیکی به اینترنت است.

همچنین یکی دیگر از معایب تجزیه و تحلیل بدافزار در یک ماشین فیزیکی نسبت به یک ماشین‌مجازی این است که بدافزار به سختی ممکن است حذف شود. به منظور ممانعت از این مشکل در تجزیه و تحلیل بدافزارهای رایانه‌ای درون سامانه‌های فیزیکی، اکثریت متخصصین از برنامه Norton Ghost استفاده می‌کردند. آنها با استفاده از این نرم‌افزار می‌توانستند از سامانه خود نسخه پشتیبان بگیرند و پس از به اتمام رساندن تحلیل بدافزارها، سامانه را به حالت اولیه خود بازگردانند.

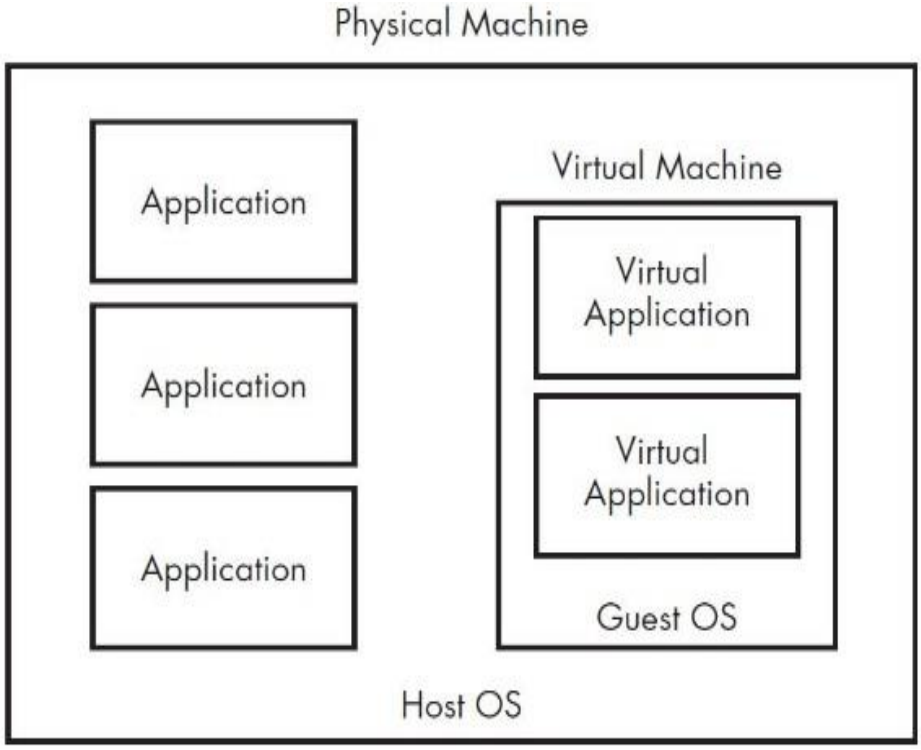
با این حال، اصلی‌ترین مزئیت استفاده از این روش در تجزیه و تحلیل بدافزارها این است که بدافزارها می‌تواند گاهی اوقات در سامانه‌های مجازی متفاوت عمل کنند. به عنوان مثال، اگر شما درحال تجزیه و تحلیل یک بدافزار روی ماشین‌مجازی باشید، برخی از بدافزارها می‌توانند این موضوع را شناسایی کنند و در نتیجه یک رفتار غیرمتعارف به منظور ممانعت از تجزیه و تحلیل نشان دهند.

اما از آنجاییکه خطرات و معایب زیادی در استفاده از ماشین‌های فیزیکی وجود دارد، بیشتر متخصصین تجزیه و تحلیل بدافزار از ماشین‌های مجازی (با مقداری سفارشی‌سازی) برای تحلیل دینامیک بدافزارها استفاده می‌کنند. به همین دلیل ما در این فصل خواهیم آموخت چگونه یک محیط مجازی برای تحلیل بدافزارها راه‌اندازی کنیم.

ساختار ماشین‌مجازی

همان‌طور که در تصویر ۳ نمایش داده شده است، در واقع ماشین‌های مجازی یک ماشین درون یک ماشین دیگر هستند. در این ساختار یک سامانه‌عامل مهمان[1] درون یک سامانه‌عامل میزبان[2] در یک ماشین‌مجازی نصب می‌شود، و سامانه‌عامل در حال اجرا روی ماشین‌مجازی از سامانه‌عامل میزبان مجزا نگهداری می‌شود.

در این حالت اگر بدافزار آسیبی به سامانه‌عامل ماشین‌مجازی برساند، می‌توانید به راحتی آن سامانه‌عامل را دوباره نصب کنید یا ماشین‌مجازی را به حالت درست خود برگردانید. (با قابلیت Snapshot که در Vmware و همچنین VirtualBox تعبیه شده است، این ویژگی به زودی تشریح خواهد شد.)



تصویر ۳: برنامه‌های کاربردی سامانه اصلی درتصویرسمت چپ نمایش داده شده‌اند و سامانه‌عامل مهمان درون ماشین‌مجازی و برنامه‌های کاربردی آن درون سامانه‌عامل مهمان نمایش داده شده‌اند.

[1] Guest OS
[2] Host OS

مجموعه نرم‌افزاری VMware مشهورترین گزینه در زمینه مجازی‌سازی سامانه‌عامل‌های رایانه‌ای است که می‌تواند در تجزیه و تحلیل بدافزارها روی ماشین‌های مجازی مورد استفاده قرار گیرد. همچنین نرم‌افزار VMware Player یک برنامه رایگان از مجموعه نرم‌افزاری شرکت VMware است که می‌تواند برای راه‌اندازی ماشین‌مجازی مورد استفاده قرار گیرد. اما فاقد برخی از قابلیت‌های ضروری است که نرم‌افزار VMware Workstation برای تجزیه و تحلیل بدافزارها به متخصصین ارائه می‌دهد.

علاوه بر این‌ها نرم‌افزار VMware Workstation شامل قابلیت‌های بسیاری از جمله Snapshot است که اجازه می‌دهد حالت جاری ماشین‌مجازی را ذخیره کنید و در مواقع مورد نیاز ماشین‌مجازی را به حالت ذخیره شده برگردانید. قابل ذکر است، تعداد بسیار زیادی برنامه جایگزین برای نرم‌افزار VMware وجود دارد. از قبیل نرم‌افزارهای VirtualBox، نرم‌افزار Parallels، نرم‌افزار Microsoft Hyper-V و موارد دیگر که ما در این فصل از سلسله مقالات تحلیل بدافزار فقط روی استفاده از VMware Workstation متمرکز خواهیم بود.

ایجاد ماشین تجزیه و تحلیل بدافزار

البته، قبل از این‌که بتوانید از یک ماشین‌مجازی برای تجزیه و تحلیل بدافزارها استفاده کنید، نیاز دارید یکی از آنها را ایجاد کنید. قابل ذکر است، این فصل از سلسله مقالات تجزیه و تحلیل بدافزار مخصوص مجازی‌سازی نیست. بنابراین تمامی مباحث مجازی‌سازی در آن مطرح نخواهد شد. با این حال هنگام نمایش گزینه‌ها، اگر نمی‌دانید چه گزینه‌ای را انتخاب کنید، آن‌ها را به صورت پیش‌فرض رها کنید.

نرم‌افزار VMware Workstation هوشمند است و از فضای دیسک سخت هوشمندانه استفاده می‌کند و به صورت پویا فضای دیسک مجازی را تعیین می‌کند. به عنوان مثال، اگر شما ۴۰ گیگابایت فضای دیسک سخت برای ماشین‌مجازی در نظر بگیرید، ولی فقط از ۱۰ گیگابایت آن استفاده کنید، برنامه VMware آن فضا را به صورت خودکار تغییر می‌دهد و به اندازه مورد استفاده شما از فضای دیسک سخت بهره‌مند می‌شود. در ضمن برای شروع مقدار ۴۰ گیگابایت برای ماشین‌مجازی مناسب است. زیرا این مقدار برای سامانه‌عامل مهمان و هر ابزاری که شما به آن برای تجزیه و تحلیل بدافزار نیاز دارید کافی است.

پس از مشخص‌سازی فضای مورد نیاز برای ماشین‌مجازی در گام بعد شما باید سامانه‌عامل و برنامه‌های کاربردی را روی آن نصب کنید. بیشتر بدافزارها و ابزارهای تجزیه و تحلیل در سامانه‌عامل ویندوز اجرا می‌شوند، بنابراین باید سامانه‌عامل ویندوز را روی ماشین‌مجازی خود نصب کنید.

در هنگام نوشتن این سلسله مقالات، ویندوز 7 مشهورترین سامانه‌عامل و قربانی برای بدافزارها بوده است. به همین دلیل در این سلسله مقالات ما روی این سامانه‌عامل متمرکز خواهیم شد. پس از نصب سامانه‌عامل ویندوز 7، می‌توانید برنامه کاربردی مورد نیازتان برای تجزیه و تحلیل بدافزار را روی سامانه‌عامل نصب و راه‌اندازی کنید.

در گام بعد، شما باید ابزارهای VMware را روی سامانه‌عامل مجازی نصب کنید. بدین منظور از منو برنامه VMware گزینه VM را انتخاب کرده و روی Install VMware Tools کلیک کنید، تا فرایند نصب ابزارها روی سامانه‌عامل مجازی آغاز شود. اگرچه در نسخه‌های اخیر Vmware Workstation این عمل به صورت خوکار بر روی ماشین مجازی صورت می‌گیرد و دیگر نیاز نیست به صورت دستی عمل نصب را انجام بدهید.

ابزارهای VMware قابلیت‌های تعامل کاربر با ماشین‌مجازی را بهبود می‌بخشد و این امکان را می‌دهد که شما بتوانید از سامانه اصلی با سامانه مجازی خود برای انجام برخی کارها به صورت خیلی ساده ارتباط برقرار کنید.

همچنین به شما اجازه می‌دهد به یک پوشه اشتراکی[1]، انتقال فایل با کشیدن و رها کردن (Drag and Drop) به سامانه مجازی[2] و دیگر قابلیت‌های مفید مختلف دسترسی داشته باشید. در این قسمت از سلسله مقالات تحلیل بدافزار در مورد این ویژگی‌ها بحث خواهیم کرد.

پیکربندی نرم‌افزار VMware

بیشتر بدافزارها شامل کاربردهای شبکه‌ای هستند. به عنوان مثال، یک کرم[3] می‌تواند حملات مبتنی بر شبکه بر علیه دیگر ماشین‌های درون شبکه قربانی انجام داده و خود را گسترش دهد. اما شما نمی‌خواهید به یک

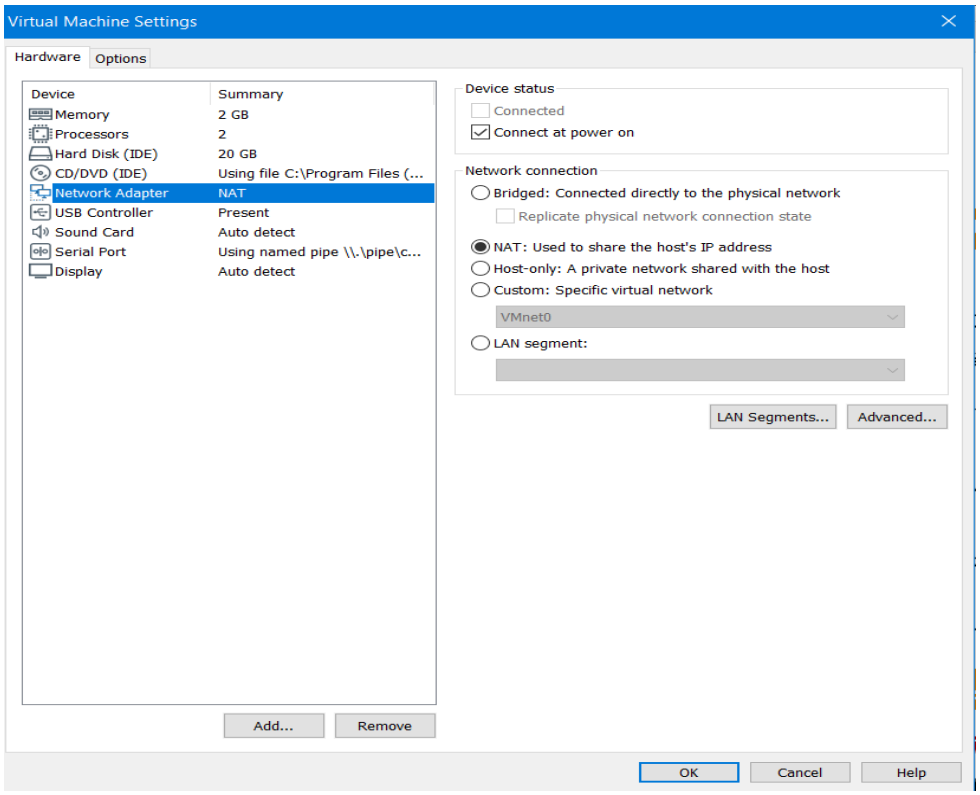
[1] Shared folders
[2] Drag-and-drop file transfer
[3] Worms

کرم این اجازه را بدهید که به شبکه شما دسترسی داشته باشد و بتواند خودش را به دیگر سامانه‌ها گسترش دهد.

هنگامی‌که در حال تحلیل بدافزار هستید، به احتمال زیاد بخواهید فعالیت‌های شبکه بدافزار را مشاهده کنید تا مقصود توسعه‌دهنده بدافزار را از ساخت این بدافزار دریابید، یا برای ممانعت از گسترش آن، یک سیگنیچر جامعه سطح شبکه و سامانه میزبان ایجاد کنید. گزینه‌هایی که می‌توانیم به منظور معماری شبکه ماشین مجازی در VMWare و حتی دیگر نرم‌افزارهای مجازی‌سازی انتخاب کنیم، به شرح زیر است:

- شبکه Host-Only
- شبکه Bridge
- شبکه NAT

همانطور که درتصویر ۴ نمایش داده شده است، برنامه VMware از این گزینه‌ها برای پیکربندی شبکه ماشین‌مجازی پشتیبانی می‌کند. این گزینه‌ها در ادامه این بخش مورد بررسی قرار خواهند گرفت.



تصویر ۴: گزینه‌های پیکربندی شبکه ماشین‌مجازی برای یک آداپتور شبکه

قطع ارتباط شبکه[1]

اگر چه شما می‌توانید یک ماشین‌مجازی پیکربندی کنید که هیچ دسترسی به شبکه نداشته باشد، اما قطع ارتباط با شبکه در حالت کلی فکر خوبی نیست، زیرا شما نمی‌توانید در حالتی که ماشین‌مجازی دسترسی به شبکه ندارد فعالیت‌های شبکه‌ای بدافزار را تحلیل کنید. با این حال قطع ارتباط ماشین‌مجازی با شبکه می‌تواند در برخی شرایط خاص برای تجزیه و تحلیل بدافزار مفید واقع شود.

همچنین در نظر داشته باشید، اگر دلیلی مبنی بر قطع ارتباط ماشین‌مجازی با شبکه داشتید، می‌توانید با حذف آداپتور شبکه از قسمت تنظیمات VMware یا با رفتن به قسمت removable از منوی VM و Disconnect کردن Network Adaptor ارتباط ماشین‌مجازی را با اینترنت قطع کنید.

همچنین می‌توانید کنترل کنید که یک آداپتور شبکه به صورت خودکار در زمان روشن شدن ماشین‌مجازی به شبکه متصل شود. بدین منظور کافی است تیک گزینه Connect at power on را در قسمت تنظیمات آداپتور شبکه فعال کنید. در تصویر ۴ آن را می‌توانید مشاهده کنید.

تنظیم شبکه روی Host-Only

گزینه Host-only networking، قابلیتی است که یک شبکه محلی مجزا میان سامانه‌عامل میزبان و سامانه‌عامل مهمان ایجاد می‌کند. شایان ذکر است، این نوع شبکه‌بندی در تجزیه و تحلیل بدافزارها بسیار رایج است. یک شبکه محلی Host-Only به اینترنت متصل نمی‌شود، این بدین معناست که بدافزار درون ماشین‌مجازی فقط می تواند برخی از فعالیت‌های شبکه را انجام دهد.

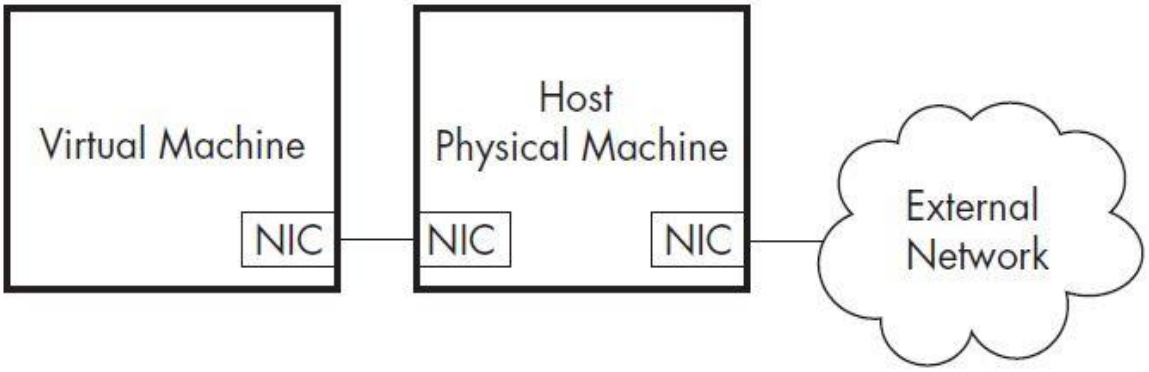
نکته: هنگامی‌که در حال پیکربندی رایانه میزبان هستید، اطمینان حاصل کنید که کاملا ایمن باشد. همچنین برای ممانعت از گسترش بدافزار این فکر خوبی است که در سامانه میزبان یک دیوارآتش به منظور محدودسازی ماشین‌مجازی پیکربندی شود تا از گسترش بدافزار به سامانه میزبان محافظت شود. دیوارآتش سامانه‌عامل‌های مایکروسافت که با ویندوز XP و دیگر سامانه‌عامل‌های این

---

[1] Disconnecting the Network

شرکت ارائه می‌شوند به خوبی مستندسازی شده‌اند و مکانیزم‌های محافظتی خوبی را به ما ارائه می‌دهند. اما با این حال، حتی اگر سامانه شما کاملا وصله و ایمن شده باشد، بدافزارها می‌توانند با استفاده از Zero-Dayها خود را به سادگی به سامانه میزبان و دیگر سامانه‌ها گسترش دهند.

تصویر ۵ پیکربندی شبکه Host-Only را میان دو سامانه نمایش می‌دهد. هنگامی‌که شبکه Host-Only فعال می‌شود، برنامه VMware یک آداپتور شبکه مجازی در ماشین‌های مجازی و میزبان ایجاد می‌کند و سپس بدون آنکه آداپتور شبکه اصلی سامانه میزبان را مورد استفاده قرار بدهد، آن دو سامانه را به همدیگر متصل می‌کند.

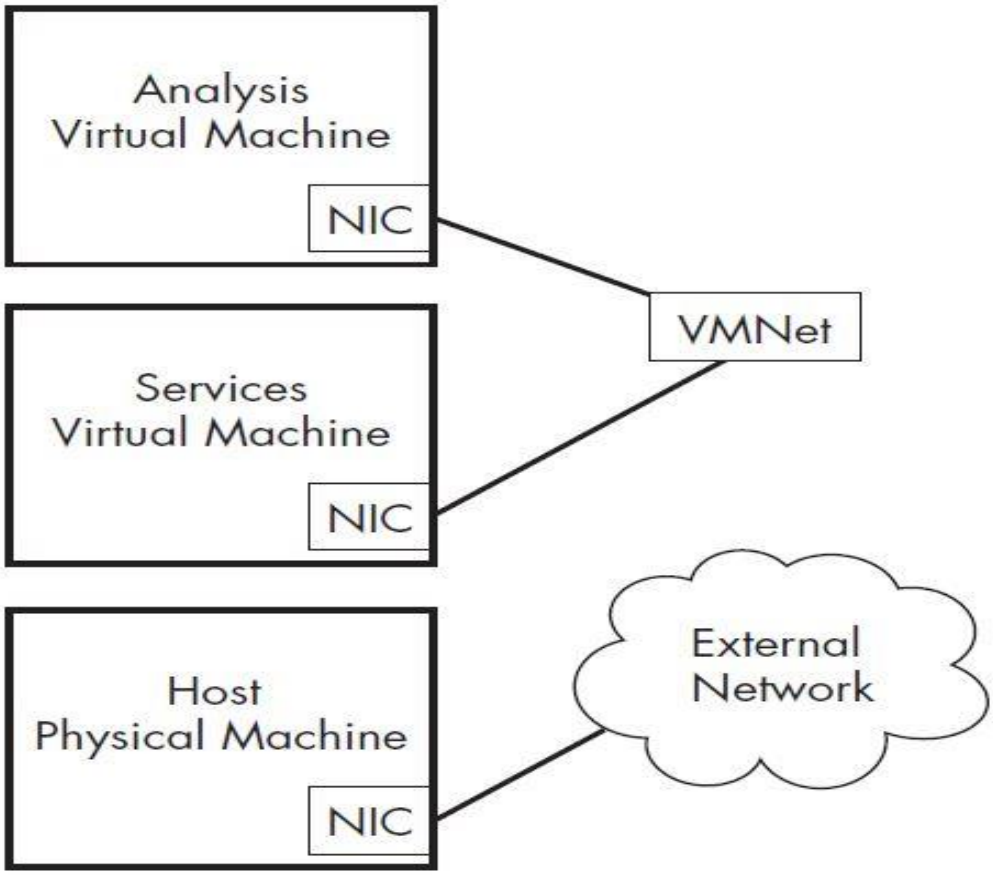


تصویر ۵: شبکه Host-Only در برنامه VMware

استفاده از چندین ماشین‌مجازی

آخرین پیکربندی تمامی گزینه‌های خوب را با همدیگر ترکیب می‌کند. بدین منظور نیاز به چندین ماشین‌مجازی داریم که به یک دیگر توسط شبکه محلی متصل شده باشند. همچنین این سامانه‌ها نباید به اینترنت و ماشین میزبان دسترسی داشته باشند. زیرا برخی از بدافزارها برای اعمال عملیات باید به شبکه متصل شوند این مهم است که سامانه‌ها با همدیگر از طریق یک شبکه محلی در ارتباط باشند، اما نکته حائز اهمیت در این قسمت برای ما این است که شبکه نباید به مورد مهمی (مانند اینترنت و سامانه میزبان) متصل شود.

تصویر ۶ پیکربندی پیشفرض میان دو ماشین‌مجازی که به همدیگر متصل هستند را نمایش می‌دهد. در این پیکربندی، یک ماشین‌مجازی برای تحلیل بدافزار و دیگری برای ارائه سرویس راه‌اندازی شده‌اند. ماشین‌های مجازی به یک سوئیچ مجازی برنامه VMware که Vmnet نامیده می‌شوند، متصل هستند. در این حالت، ماشین میزبان هنوز به شبکه خارجی متصل است، اما ماشینی که از آن برای تجزیه و تحلیل بدافزار استفاده می‌شود دیگر به شبکه خارجی (اینترنت) دسترسی ندارد.



تصویر ۶: شبکه‌های سفارشی در VMware

استفاده از ماشین‌مجازی تجزیه و تحلیل بدافزار

به منظور تمرین مهارت مد نظر خود یعنی تجزیه و تحلیل بدافزار تا جایی که ممکن است، شما باید تمامی سرویس‌های شبکه‌ای را که بدافزار به آن‌ها متکی می‌باشد، شبیه‌سازی کنید. به عنوان مثال بدافزارها عموما

به منظور دانلود دیگر کدهای مخرب خود به یک سرور Http متصل می‌شوند، تا بتوانند تعاملات شبکه خود را انجام بدهند.

حال به منظور مشاهده این فعالیت، باید برای پاسخگویی به درخواست‌های ارسالی بدافزار، اجازه دسترسی به سرور DNS و همچنین سرور Http را صادر کنید. با پیکربندی شبکه سفارشی که به تازگی تشریح شد، ماشین‌ها سرویس‌هایی ارائه می‌کنند که باید در ماشین اجرا شوند زیرا بدافزار برای برقراری ارتباط به آن‌ها نیاز دارد.

اتصال بدافزار به اینترنت

گاهی اوقات به منظور فراهم کردن یک محیط واقعی تجزیه و تحلیل بدافزار، علیرغم خطر واضح آن باید به ماشین تجزیه و تحلیل بدافزار اجازه دسترسی به اینترنت بدهید. بزرگترین خطر، البته این است که رایانه شما یک فعالیت مخربانه انجام خواهد داد.

از قبیل، گسترش بدافزار به دیگر میزبان‌ها، تبدیل شدن به یک گره برای اعمال حملات تکذیب سرویس[1] که هدف از قسمت فرماندهی بدافزار مشخص می‌گردد و از سامانه شما به عنوان یک زامبی یا (Zombie) استفاده می‌شود. یک خطر دیگر این است که نویسنده بدافزار می‌تواند به سادگی متوجه شود که شما به منظور تجزیه و تحلیل بدافزار به سرور آن متصل شده‌اید.

توجه کنید، به عنوان یک متخصص تجزیه و تحلیل بدافزار بهتر است به بدافزار اجازه دسترسی به اینترنت را ندهید، مگر این‌که آن را تجزیه و تحلیل اولیه کرده باشید. زیرا باید در گام اول مشخص سازید که بدافزار پس از متصل شدن به اینترنت ممکن است چه فعالیتی انجام بدهد. پس از آن منطقی است که به بدافزار اجازه دهید به اینترنت متصل شود تا بتوانید فعالیت‌های شبکه آن را تحلیل و گزارش کنید.

با این حال رایج‌ترین راه به منظور متصل ساختن ماشین‌مجازی به اینترنت در نرم‌افزار VMware تنظیم آداپتور شبکه ماشین‌مجازی روی حالت Bridged است. این روش اجازه می‌دهد ماشین‌مجازی به رابط شبکه

[1] denial-of-service attack

مشابه سامانه میزبان فیزیکی متصل گردد. اما راه دیگری هم وجود دارد که ماشین‌مجازی به اینترنت متصل شود. در این روش آداپتور شبکه ماشین‌مجازی روی حالت NAT یا ترجمه آدرس شبکه[1] تنظیم می‌گردد.

در حالت ترجمه آدرس شبکه یا NAT ، آدرس IP ماشین میزبان به اشتراک گذاشته می‌شود. در این حال میزبان مانند یک مسیریاب عمل کرده و تمامی درخواست‌های ماشین‌مجازی را ترجمه می‌کند، به طوریکه فرض می‌شود آن‌ها از آدرس IP میزبان می‌آیند. این روش هنگامی مفید است که سامانه میزبان اصلی به اینترنت متصل باشد.

به عنوان مثال، اگر سامانه میزبان از یک آداپتور بی‌سیم استفاده کند، حالت NAT به راحتی می‌تواند به منظور متصل کردن ماشین‌های مجازی به شبکه مورد استفاده قرار گیرد. حتی اگر در شبکه بی‌سیم مکانیزهای حفاظتی (WEP) و (WPA) فعال باشد. یا اگر آداپتور میزبان به شبکه‌ای متصل شود که فقط اجازه اتصال به برخی از آداپتورهای شبکه را می‌دهد. حالت NAT اجازه می‌دهد ماشین‌های مجازی از طریق میزبان به آن شبکه ها متصل شوند در حالی‌که تنظیمات کنترل دسترسی شبکه ممانعت به عمل می‌آورند.

اتصال و عدم‌اتصال دستگاه‌های جانبی[2]

دستگاه‌های جانبی، از قبیل CD-Romها، حافظه‌های ذخیره‌سازی USB خارجی و... یک مسئله اساسی برای ماشین‌های مجازی هستند. بیشتر دستگاه‌ها می‌توانند به ماشین فیزیکی یا ماشین‌مجازی متصل شوند و امکان متصل شدن به هر دوی آن‌ها را ندارند.

خوشبختانه رابط برنامه VMware اجازه مدیریت دستگاه‌ها را به شما می‌دهد، زیرا که می‌توانید دستگاه‌ها را به ماشین‌مجازی متصل یا قطع ارتباط کنید. اما اگر یک دستگاه را از طریق ارتباط USB به ماشین متصل کنید، در حالی‌که پنجره ماشین‌مجازی فعال است، با توجه به رشد شهرت کرم‌هایی که از طریق دستگاه‌های ذخیره‌سازی USB گسترش پیدا می‌کنند، برنامه VMware دستگاهی که به USB متصل شده است را به ماشین‌مجازی وصل خواهد کرد، نه به ماشین میزبان اصلی و این موضوع می‌تواند برای ما کمی ناخوشایند باشد.

---

[1] Network Address Translation (NAT)
[2] Connecting and Disconnecting Peripheral Devices

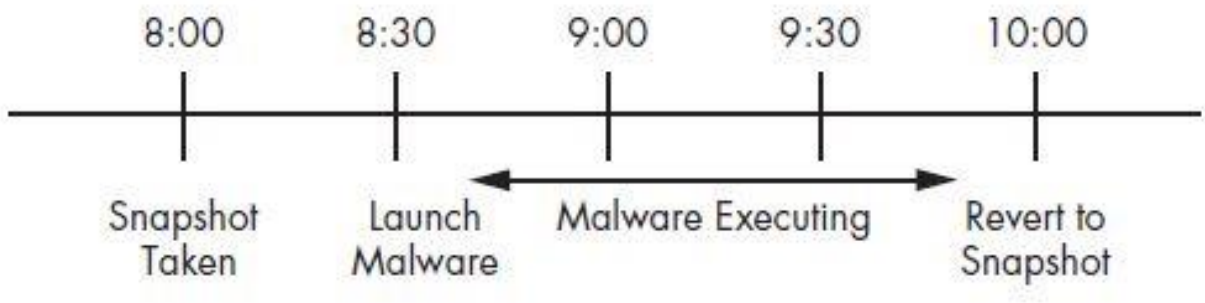
برای تغییر این تنظیمات، به منوی VM بروید و روی گزینه Settings کلیک کنید. سپس در پنجره باز شده روی USB Controller کلیک کنید و سپس در پانل سمت چپ گزینه Automatically connect new USB devices را از حالت انتخاب خارج کنید تا از متصل شدن دستگاه‌های مبتنی بر USB به ماشین‌مجازی ممانعت به عمل آید.

Snapshot گرفتن از ماشین‌های مجازی

Snapshot گرفتن یک واژه منحصربفرد در ماشین‌های مجازی است. Snapshot گرفتن از ماشین‌های مجازی VMware به شما اجازه می‌دهد حالت جاری رایانه را ذخیره کنید و در زمان‌های مورد نیاز آن حالت را برگردانید، Snapshot گرفتن مشابه نقطه بازیابی در سامانه‌عامل ویندوز است.

در جدول زمانی تصویر ۷، چگونگی کارکرد Snapshot نمایش داده شده است. همان‌طور که درتصویرمشاهده می‌کنید، در زمان ۸:۰۰ شما از رایانه یک Snapshot اولیه گرفتید، سپس برای زمان کوتاهی، بدافزار را اجرا کرده و روی آن تحلیل انجام داده‌اید.

در پایان عملیات تحلیل، در زمان ۱۰:۰۰ سامانه را به حالت اولیه برگردانده‌اید. این عمل باعث می‌شود سامانه‌عامل، نرم‌افزارها و دیگر مولفه‌های ماشین به حالت مشابه آن در زمان ۸:۰۰ که از ماشین‌مجازی Snapshot گرفته بودید بازگشت داده شوند.



تصویر ۷: جدول زمانی گرفتن Snapshot

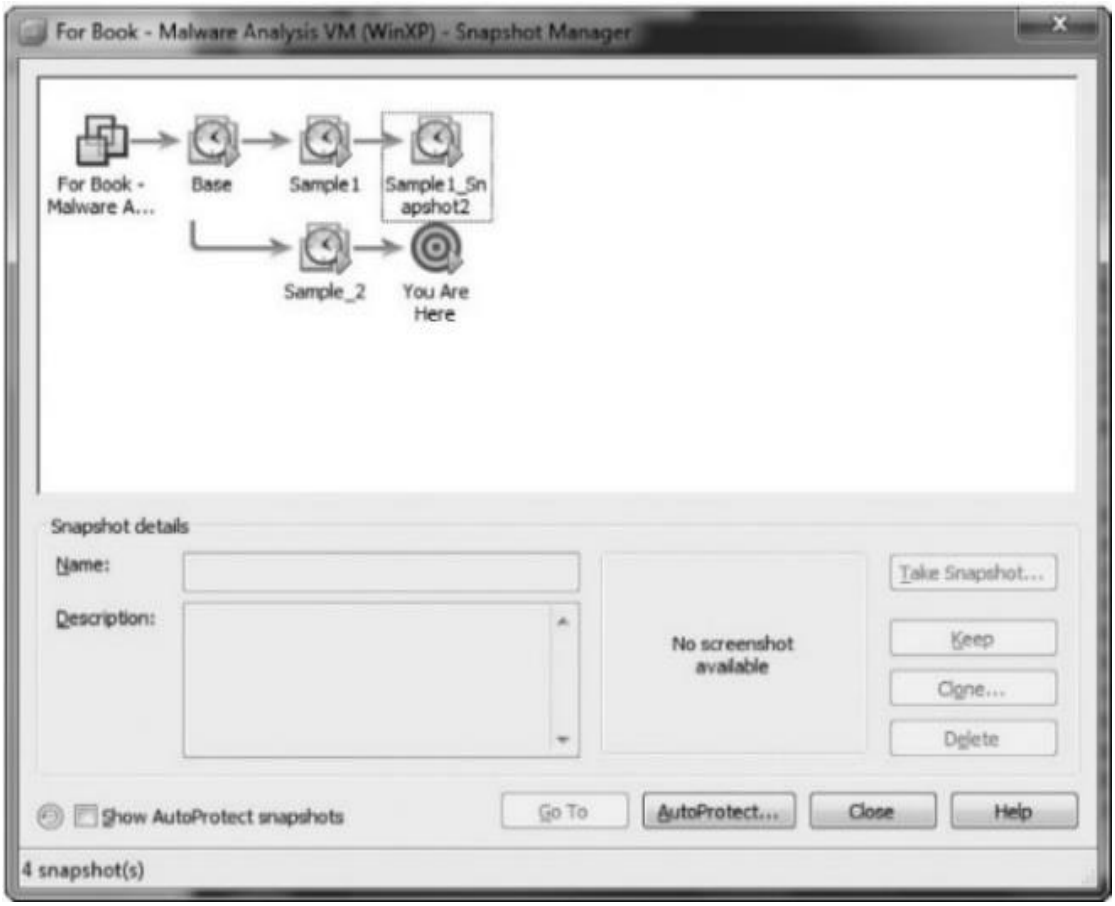
پس از نصب سامانه‌عامل و تمامی ابزارهای مورد نیاز برای تجزیه و تحلیل بدافزار و همچنین پیکربندی شبکه بهتر است از ماشین‌مجازی خود یک Snapshot بگیرید. سپس بدافزار را اجرا کرده و تحلیل خود را کامل

کنید. در پایان سامانه را به حالت پاک و بی‌عیب خود برگردانید. این کار را می‌توانید بار ها انجام بدهید. بدون آنکه نیاز داشته باشید دوباره سامانه‌عامل و ابزارهای مورد نیاز تحلیلگریتان را نصب و راه‌اندازی کنید.

اما اگر شما میان فرایند تجزیه و تحلیل بدافزار بودید و می‌خواستید یک کار متفاوت روی ماشین‌مجازی انجام بدهید بدون آن‌که پیشرفت‌هایی که در فرایند تحلیل بدافزار کرده اید پاک شود، مدیر Snapshot در برنامه VMware به شما اجازه می‌دهد به هر نقطه زمان Snapshot که از ماشین‌مجازی گرفته اید بازگردید. مهم نیست چند بار از حالت‌های ماشین‌مجازی Snapshot گرفته‌اید، مهم این است که شما می‌توانید با استفاده از مدیر Snapshot در نرم‌افزار VMware به هر نقطه که می‌خواهید بروید. حتی می‌توانید Snapshotهای خود از سامانه‌عامل را شاخه‌بندی کرده و پس از آن مسیرهای مختلف را دنبال کنید. بگذارید به ترتیب کار زیر نگاهی بیندازیم:

- هنگامی‌که درحال تجزیه و تحلیل بدافزار شماره ۱ هستید، از تجزیه و تحلیل آن ناامید می‌شوید و می‌خواهید یک بدافزار دیگر را تحلیل کنید.
- از حالت ماشین‌مجازی در تجزیه و تحلیل بدافزار شماره ۱، Snapshot می‌گیرید.
- سپس به حالت اولیه ماشین‌مجازی باز می‌گردید.
- شروع به تحلیل بدافزار شماره ۲ می‌کنید.
- پس از اتمام تجزیه و تحلیل بدافزار شماره ۲، از حالت ماشین‌مجازی یک Snapshot می‌گیرید.

هنگامی‌که شما به ماشین‌مجازی خود باز می‌گردید، می‌توانید به هر یک از Snapshotها از طریق Snapshot Manager دسترسی پیدا کنید. درتصویر ۸ محیط Snapshot Manager نمایش داده شده است. همان‌طور که مشاهده می‌کنید دو حالت ماشین‌مجازی کاملا از هم مجزا هستند. شایان ذکر است، شما می‌توانید به اندازه میزان فضای دیسک هر تعداد که می‌خواهید از ماشین‌مجازی Snapshot بگیرید.



تصویر ۸: محیط مدیر Snapshot های برنامه VMware

انتقال فایل‌ها از یک ماشین‌مجازی

یکی از ضعف‌های موجود در استفاده از Snapshotها این است که همه فایل‌های کاری در ماشین‌مجازی هنگام بازگشت به Snapshot قبلی از دست می‌رود. شما می‌توانید فایل‌های کاری مورد نیاز خود را با قابلیت کشیدن و رها کردن[1] موجود در نرم‌افزار VMware در سامانه‌عامل میزبان (سامانه‌عاملی که ماشین‌مجازی روی آن در حال اجرا است.) ذخیره‌سازی کنید.

[1] Drag and Drop

قابل ذکر است، زمانی از این مزئیت می‌توانید بهره‌مند شوید که ابزارهای VMware روی سامانه‌عامل ماشین‌مجازی نصب شده باشد. در آن زمان می‌توانید با کشیدن و رها کردن[1] فایل‌های کاری خود را ما بین سامانه‌های عامل انتقال بدهید.

این راحترین و ساده‌ترین راه برای انتقال فایل‌ها میان ماشین‌های مجازی و سامانه میزبان است. البته یک راه دیگر هم وجود دارد، آن هم استفاده از پوشه اشتراکی[2] برنامه VMware است. این پوشه اشتراکی از طریق هر دو تا سامانه در دسترس می‌باشد و شما می‌توانید فایل‌های خودتان را مابین آن‌ها به راحتی به اشتراک بگذارید. این پوشه مشابه پوشه‌های اشتراکی ویندوز است.

خطرهای استفاده از برنامه VMware در تحلیل بدافزار

متخصصین تجزیه و تحلیل بدافزار باید توجه داشته باشند که برخی بدافزارها می‌توانند محیطی که در آن اجرا شده‌اند را با استفاده از برخی روش‌ها شناسایی کنند. بدین منظور روش‌های بسیاری تا به الان برای شناسایی محیط های ماشین‌مجازی به اشتراک گذاشته شده است که بدافزارها از آن‌ها برای اعمال مقاصد خود بهره‌مند می‌شوند.

در تصویر ۹ قسمتی از کدهای C را مشاهده می‌کنید که خروجی آن می‌تواند مشخص کند آیا فایل باینری ما در یک محیط مجازی، یا در یک محیط واقعی (Actual) در حال اجراست. زیرا وقتی شما بتوانید تشخیص بدهید، باینری در یک محیط مجازی اجرا شده است، یا در محیط یک دیباگر – دیزاسمبلر اجرا شده است، می‌توانید روند اجرای برنامه مخصوصا اگر ساختار ماژولار داشته باشد، تغییر بدهید و اجازه ندهید، پیلود اصلی بدافزار بر روی سامانه تحلیلگر بارگزاری شود.

به عنوان مثال، اگر در برنامه خود موجودیت رجیستری‌های متعلق به نرم‌افزار را بررسی کنید، وجود رجیستری‌ها می‌توانند گواه وجود یک ماشین مجازی را به شما بدهد یا بررسی پروسه‌هایی که با نام VM* شروع شده‌اند، یا Mac Address که متعلق به ماشین‌های مجازی هستند، پورت‌های باز متعلق به ماشین مجازی، سرویس‌هایی که متعلق به ماشین مجازی هستند و ... تمامی می‌توانند گواه یک ماشین مجازی را بدهند. به

[1] Copy and Paste
[2] Shared Folder

عنوان مثال، لیست رجیستری‌هایی که در قسمت زیر آورده شده‌اند متعلق به ماشین مجازی Vmware هستند:

- **HKLM\SOFTWARE\Vmware Inc.\\\Vmware Tools**
- **SYSTEM\CurrentControlSet\Enum\SCSI\Disk&Ven_VMware_&Prod_VMware_Virtual_S**
- **SYSTEM\CurrentControlSet\Control\CriticalDeviceDatabase\root#vmwvmcihostdev**
- **SYSTEM\CurrentControlSet\Control\VirtualDeviceDrivers**

یا فایل‌های زیر متعلق به ماشین مجازی VirtualBox هستند که وجود این فایل‌ها می‌توانند گواهی دهند ما در یک محیط مجازی هستیم. در ادامه توسعه دهنده بدافزار می‌تواند روند اجرایی بدافزار را متناسب با محیطی که در آن باینری اجرا شده است، تغییر بدهد.

- **C:\\WINDOWS\\system32\\drivers\\VBoxMouse.sys**
- **C:\\WINDOWS\\system32\\drivers\\VBoxGuest.sys**
- **C:\\WINDOWS\\system32\\drivers\\VBoxSF.sys**
- **C:\\WINDOWS\\system32\\drivers\\VBoxVideo.sys**
- **C:\\WINDOWS\\system32\\vboxoglfeedbackspu.dll**
- **C:\\WINDOWS\\system32\\vboxoglpackspu.dll**
- **C:\\WINDOWS\\system32\\vboxoglpassthroughspu.dll**
- **C:\\WINDOWS\\system32\\vboxservice.exe**
- **C:\\WINDOWS\\system32\\vboxtray.exe**
- **C:\\WINDOWS\\system32\\VboxCon**

متاسفانه برنامه VMware نمی‌تواند فرض کند این یک ضعف است و متعاقبا هیچ کاری به منظور جلوگیری از این موضوع نمی‌تواند انجام بدهد. نکته حائز اهمیت این است که برخی بدافزارها هنگامی‌که شناسایی می‌کنند در یک محیط مجازی اجرا شده‌اند یک رفتار غیر متعارف نمایش می‌دهند و حقیقتا زندگی را برای شخص تحلیلگر بدافزار جهنم می‌سازند. (در این مورد، در قسمت‌های بعدی بحث خواهیم کرد، و روش‌های ضدماشین‌مجازی را با جزییات بیشتری بررسی خواهیم کرد).

به عنوان مثال، در تصویر ۹ یک تابع با عنوان VirtualBoxFiles پیاده‌سازی شده است که خروجی آن‌ها True یا False است. اگر این تابع مقدار True را بازگشت بدهد، یعنی باینری در حال اجرا درون یک محیط مجازی است، در غیر این صورت محیط واقعی خواهد بود.

```
BOOL VirtualBoxFiles() {
    BOOL bConditionOfVBox = FALSE;
    const char* ccFilesOfVBox[20] = {
        "C:\\WINDOWS\\system32\\drivers\\VBoxMouse.sys",
        "C:\\WINDOWS\\system32\\drivers\\VBoxGuest.sys",
        "C:\\WINDOWS\\system32\\drivers\\VBoxSF.sys",
        "C:\\WINDOWS\\system32\\drivers\\VBoxVideo.sys",
        "C:\\WINDOWS\\system32\\vboxdisp.dll",
        "C:\\WINDOWS\\system32\\vboxhook.dll",
        "C:\\WINDOWS\\system32\\vboxmrxnp.dll",
        "C:\\WINDOWS\\system32\\vboxogl.dll",
        "C:\\WINDOWS\\system32\\vboxoglarrayspu.dll",
        "C:\\WINDOWS\\system32\\vboxoglcrutil.dll",
        "C:\\WINDOWS\\system32\\vboxoglerrorspu.dll",
        "C:\\WINDOWS\\system32\\vboxoglfeedbackspu.dll",
        "C:\\WINDOWS\\system32\\vboxoglpackspu.dll",
        "C:\\WINDOWS\\system32\\vboxoglpassthroughspu.dll",
        "C:\\WINDOWS\\system32\\vboxservice.exe",
        "C:\\WINDOWS\\system32\\vboxtray.exe",
        "C:\\WINDOWS\\system32\\VBoxControl.exe",
        "C:\\program files\\oracle\\virtualbox guest additions\\"
    };

    for (size_t i = 0; i < sizeof(ccFilesOfVBox) / sizeof(ccFilesOfVBox[0]); i++) {
        if (FileExist(ccFilesOfVBox[i]) != INVALID_FILE_ATTRIBUTES) {
            bConditionOfVBox = TRUE;
            return bConditionOfVBox;
            break;
        }
    }
    return bConditionOfVBox;
}
```

تصویر ۹: تابع شناسایی محیط VirtualBox

همچنین مشابه دیگر نرم‌افزارهای رایانه‌ای، برنامه VMware خود دارای یک سری آسیب‌پذیری است که می‌توانند مورد بهره‌برداری (اکسپلویت) قرار گیرند و موجب شوند سامانه‌عامل ماشین میزبان خراب شود یا روی سامانه عامل میزبان کدهای مخرب اجرا شود.

گرچه مقدار بسیار محدودی ابزار عمومی و همچنین روش‌های مستندسازی شده به منظور اکسپلویت این نوع آسیب‌پذیری‌های در برنامه VMware وجود دارد، اما با این حال، بیشتر ضعف‌های امنیتی که تا به الان پیدا شده‌اند مربوط به ویژگی پوشه اشتراکی و ابزارهایی به منظور اکسپلویت کردن ویژگی کشیدن و رها کردن

(Drag & Drop) این برنامه هستند. لذا همیشه اطمینان حاصل کنید که از نسخه کاملا به‌روز شده VMware استفاده می‌کنید.

و البته، حتی پس از این‌که تمامی گام‌ها را با احتیاط انجام بدهید، برخی از خطرات همواره در حین تجزیه و تحلیل بدافزار وجود خواهند داشت. اگر تجزیه و تحلیل بدافزار را درون یک ماشین‌مجازی انجام می‌دهید؛ باید از انجام تجزیه و تحلیل بدافزار روی ماشین‌های حساس و بحرانی ممانعت کنید.

نکته : برای استفاده از ابزارهای جدید تجزیه و تحلیل بدافزار باید ماشین‌مجازی و ابزارهای موجود در آن را به‌روزرسانی کنید. با استناد به این موضوع شما نیاز خواهید داشت Snapshot اولیه‌ای را که از سامانه‌عامل و ابزارها گرفته بوده‌اید را به‌روز رسانی کنید. بدین منظور کافی است ابزارهای جدید مورد نیاز خودتان را نصب کنید و سپس دوباره از حالت جاری سامانه‌عامل یک Snapshot بگیرید.

جعبه شنی کوکو – تحلیلگر خودکار بدافزار

شایان ذکر است، اکنون که با ماشین مجازی و راه اندازی آن به صورت کلی آشنا شدیم، می توانیم یک ابزار مهم با نام Cuckoo که یک سندباکس است، و تحلیل بدافزار را به صورت خودکار انجام می دهد، مورد بررسی قرار بدهیم.

همانطور که در وب سایت (http://www.cuckoosandbox.org) تشریح شده است، کوکو یک جعبه‌شنی برای بدافزار است که از روش تجزیه و تحلیل پویا به منظور تحلیل بدافزار استفاده می‌کند. با استفاده از این روش، جعبه‌شنی کوکو به سادگی بدافزار را در محیط مجازی اجرا می‌کند و با بدست آوردن PID پروسه باینری بدافزار آن را در سامانه‌عامل مجازی به صورت لحظه به لحظه مورد مانیتورینگ قرار می‌دهد.

به عنوان یک تشریح ساده، کوکو یک سیستم تجزیه و تحلیل کننده خودکار بدافزار است که به شما اجازه می‌دهد تحلیل بدافزار را در یک محیط ایزوله شده انجام بدهید. پروژه کوکو در سال ۲۰۱۰ شروع به توسعه

شد و پس از فعالیت‌های اولیه در تابستان سال ۲۰۱۰ اولین نسخه بتا آن در تاریخ February 5th, 2011 انتشار عمومی یافت.

پروژه کوکو توسط آقای Claudio Guarnieri توسعه و طراحی شده است، ایشان هم اکنون هم توسعه دهنده اصلی این جعبه‌شنی می‌باشد. جعبه‌شنی کوکو در ماه مارس سال ۲۰۱۲، توانست اولین مرحله Magnificent7 که توسط Rapid7 سازماندهی شده بود، را پیروز شود. پس از آن کوکو توسط کمپانی Rapid7 به دلیل رویکرد نوآورانه در تجزیه و تحلیل بدافزارهای سنتی و مبتنی بر موبایل به منظور حمایت مالی انتخاب شد.

کوکو به منظور اجرای خودکار و تجزیه و تحلیل فایل‌ها و جمع آوری نتایج تحلیل، از محیط یک سامانه‌عامل مجازی استفاده می‌کند. همچنین شایان ذکر است، جعبه‌شنی کوکو از انواع فایل آورده شده در لیست زیر می‌تواند برای تجزیه و تحلیل مورد استفاده قرار بگیرد.

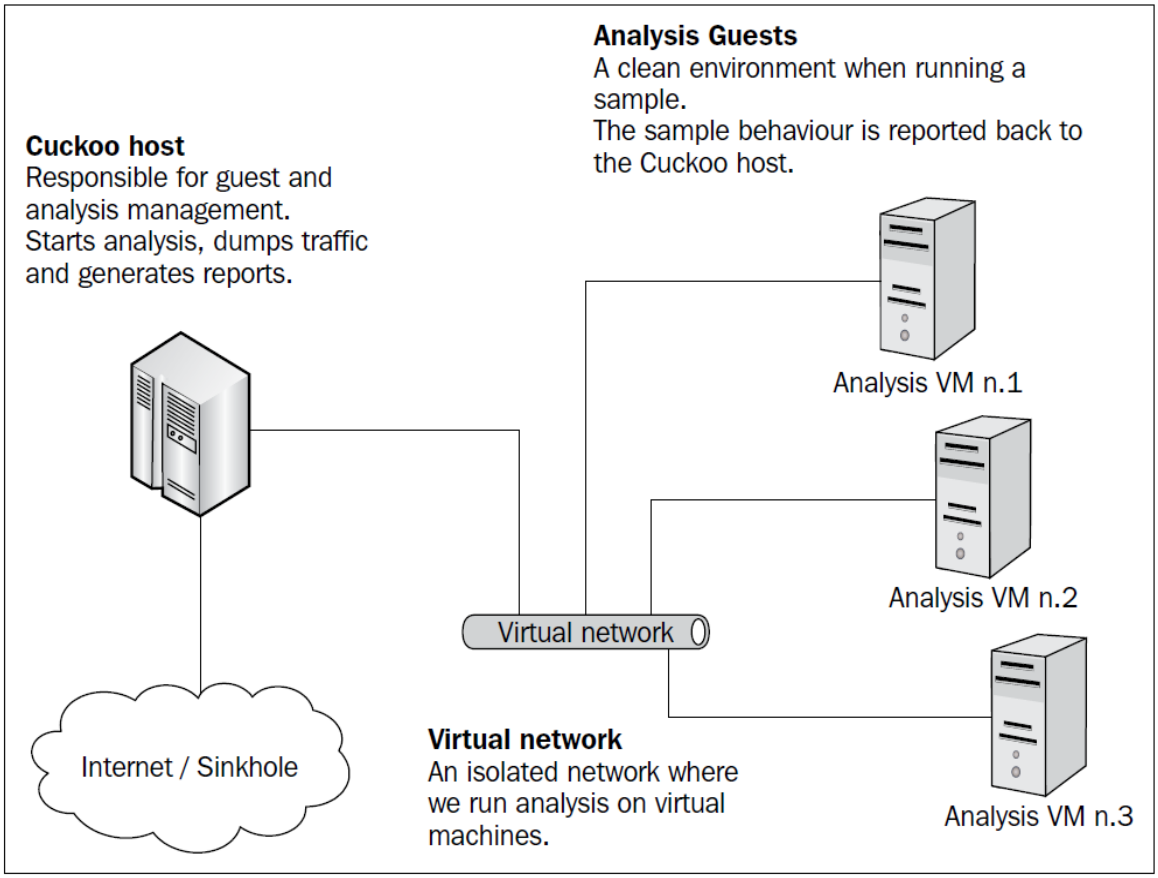
- فایل‌های اجرایی ویندوز
- فایل‌های کتابخانه‌ای پیوندی پویا
- مستندات PDF
- مستندات Microsoft Word
- آدرس‌های اینترنتی
- اسکریپت‌های PHP
- و تقریبا همه چیز

جعبه‌شنی کوکو همچنین می‌تواند جزئیات آورده شده در قسمت زیر را به عنوان خروجی تحلیل تولید کند.

- ردیابی تمامی فراخوانی‌های API انجام شده توسط پروسه بدافزار
- ردیابی تمامی فایل‌های ساخته شده، حذف شده و دانلود شده توسط بدافزار
- استخراج حافظه پروسه بدافزار
- نظارت تعاملات شبکه بدافزار در قالب PCAP
- گرفتن عکس از محیط سامانه‌عامل هنگام اجرای بدافزار
- استخراج حافظه کامل ماشین

جعبه‌شنی کوکو شامل مدیریت مرکزی نرم افزار می‌شود که اجرا و تحلیل بدافزارهای نمونه را کنترل می‌کند. همچنین قابل ذکر است، کوکو تحلیل بدافزارها را در یک ماشین مجازی ایزوله شده انجام می‌دهد. به همین دلیل است که زیرساخت جعبه‌شنی کوکو با یک ماشین میزبان (مدیریت نرم‌افزار) و یک ماشین مهمان (ماشین مجازی برای تحلیل بدافزار) ترکیب شده است.

دلیل اینکه جعبه‌شنی کوکو از دو ماشین استفاده می‌کند این است که تمامی اجزای اصلی آن به صورت مجزا و ایزوله شده کار می‌کنند. به عنوان مثال در معماری کوکو مولفه‌های اصلی جعبه‌شنی که کل فرایند تحلیل بدافزار را مدیریت می‌کنند در ماشین میزبان قرار دارند، در حالیکه ماشین مهمان صرفا فقط یک محیط ایزوله شده است که در آن بدافزار می‌تواند بگونه‌ای ایمن و مطمئن اجرا شود. دیاگرام آورده شده در قسمت زیر، نمایش دهنده معماری این جعبه‌شنی است.



تصویر ۱۰: معماری عملکرد جعبه‌شنی کوکو

قبل از اینکه فرآیند نصب و پیکربندی جعبه‌شنی کوکو را آغاز کنیم، شما نیاز خواهید داشت چند برنامه کاربردی و کتابخانه را بر روی ماشین میزبان خود نصب کنید.

نصب پیش‌نیازهای جعبه‌شنی کوکو

به منظور نصب پایتون در سامانه‌عامل اوبونتو کافیست فرمانی که در قسمت زیر آورده شده‌اند، در ترمینال اجرا کنید، پس از اجرای فرامین مذکور، به صورت خودکار فرایند پیش‌نیازهای نصب کوکو و در نهایت خود جعبه‌شنی آغاز می‌شود.

قبل از اینکه پیش‌نیازهای جعبه‌شنی کوکو را بر روی سامانه‌عامل خود نصب کنید، ابتدا مخزن‌های سامانه‌عامل اوبونتو را به روزرسانی کرده و سپس تمامی بسته‌های نرم‌افزاری را به آخرین نسخه ارتقاع دهید. سپس اقدام به نصب پیش‌نیازهای جعبه‌شنی کوکو بر روی سامانه‌عامل اوبونتو کنید. به منظور به‌روزرسانی مخازن سامانه‌عامل اوبونتو همچنین نصب پیش‌نیازهای جعبه‌شنی کوکو دستورات آورده شده در قسمت زیر را در ترمینال اجرا کنید.

```
Milad@CKL:~$ apt install python python-pip python-dev libffi-dev libssl-dev
Milad@CKL:~$ apt install python-virtualenv python-setuptools
Milad@CKL:~$ apt install libjpeg-dev zlib1g-dev swig
Milad@CKL:~$ apt install mongodb
Milad@CKL:~$ apt install postgresql libpq-dev
```

همچنین در حین استفاده از جعبه‌شنی کوکو به پلاگین Pydeep نیاز خواهید داشت. شایان ذکر است، استفاده از این پلاگین الزامی نیست اما برای کارکرد بهتر کوکو با استفاده از فرمان آورده شده در قسمت زیر می‌توانید بسته نرم‌افزاری Pydeep را نصب کنید. البته پیش از نصب Pydeep باید ssdeep را نصب کرده باشید که راهنمای نصب آن در آدرس (لینک) وجود دارد.

خلاصه تمامی بسته‌های نرم‌افزاری که جعبه‌شنی کوکو به آنها نیاز دارد، را می‌توانید با استفاده از Package Manager دبیان نصب کنید، به جزء بسته نرم‌افزاری ssdeep که باید آن را به صورت مجزا دانلود کرده و بر روی سیستم نصب و پیکربندی کنید.

پس از نصب بسته‌های نرم‌افزاری کوکو که در آدرس (لینک) آورده شده است، می‌توانید اقدام به نصب ssdeep کنید، بدین منظور ابتدا به آدرس (لینک) بروید و فایل tar آن را دانلود کرده و بر روی سیستم

خود ذخیره سازید. سپس آن را از حالت فشرده خارج کنید و با استفاده از فرامین آورده شده در قسمت زیر آن را بر روی سیستم خود نصب کنید.

نکته: به منظور نصب بسته نرم‌افزاری ssdeep و پیکربندی آن نیاز دارید که g++ و python-dev را بر روی سامانه‌عامل اوبنتو نصب کرده باشید. برای نصب این کتابخانه‌ها کافیست دستور apt-get install g++ python-dev را اجرا کنید.

```
Milad@CKL:~$ apt-get install g++ python-dev
Milad@CKL:~$ tar zxvf ssdeep-2.4.tar.gz
Milad@CKL:~$ cd ssdeep-2.4
Milad@CKL:/ssdeep-2.4$ ./configure
Milad@CKL:/ssdeep-2.4$ make
Milad@CKL:/ssdeep-2.4$ make install
```

پس از نصب ssdeep می‌توانید بسته نرم‌افزاری pydeep را بر روی سامانه‌عامل نصب کنید. اما قبل از اینکه pydeep را نصب کنید، شما نیاز خواهید داشت، چندین وابستگی این بسته نرم افزاری را بر روی سیستم خود نصب کنید. به منظور نصب وابستگی‌های این بسته نرم‌افزاری فرامین آورده شده در قسمت زیر را در ترمینال اجرا کنید.

```
Milad@CKL:~$ sudo apt install build-essential git libpcre3 libpcre3-dev libpcre++-dev
```

حال می‌توانید بسته نرم‌افزاری pydeep را به ماشین خود clone کنید (pydeep را در پوشه /opt قرار بدهید) و در نهایت آن را نصب و پیکربندی کنید.

```
Milad@CKL:/opt$ git clone https://github.com/kbandla/pydeep.git pydeep
Milad@CKL:/opt$ cd pydeep/
Milad@CKL:/opt/pydeep$ python setup.py build
Milad@CKL:/opt/pydeep$ sudo python setup.py install
```

پس از نصب بسته نرم افزاری pydeep، به منظور دسته‌بندی بدافزارها نیاز به نصب بسته نرم افزاری Yara خواهید داشت. برای نصب این بسته نرم‌افزاری ابتدا به آدرس (لینک) بروید و سپس با کلیک بر روی

Download ZIP این بسته نرم‌افزاری را دانلود کنید یا به جای آن می‌توانید این بسته نرم‌افزاری را بر روی سیستم خود clone کنید.

پس از اینکه این بسته نرم‌افزاری را دانلود کردید، آن را به پوشه /opt انتقال دهید و با استفاده از فرآمین آورده شده در قسمت زیر آن را نصب و پیکربندی کنید. البته قبل از اینکه اقدام به نصب و پیکربندی این ابزار کنید، باید کتابخانه libtool را بر روی سامانه‌عامل خود نصب کرده باشید، تا حین اجرای build.sh با خطا رو به رو نشوید.

```
Milad@CKL:/opt$ sudo apt-get install libtool
Milad@CKL:/opt$ sudo apt-get install automake -y
Milad@CKL:/opt$ git clone https://github.com/plusvic/yara/
Milad@CKL:/opt$ cd yara
Milad@CKL:/opt/yara$ sudo ln -s /usr/bin/aclocal-1.11 /usr/bin/aclocal-1.12
Milad@CKL:/opt/yara$ ./bootstrap.sh
Milad@CKL:/opt/yara$ ./configure
Milad@CKL:/opt/yara$ sudo make
Milad@CKL:/opt/yara$ sudo make install
Milad@CKL:/opt/yara$ cd yara-python
Milad@CKL:/opt/yara/yara-python$ python setup.py build
Milad@CKL:/opt/yara/yara-python$ sudo python setup.py install
```

همچنین برای استخراج ترافیک شبکه که در طی تحلیل بدافزار توسط جعبه‌شنی کوکو صورت می‌گیرد نیاز به نصب بسته نرم‌افزاری tcpdump خواهید داشت. به منظور نصب این بسته نرم‌افزاری می‌توانید از فرمان آورده شده در قسمت زیر استفاده کنید.

```
Milad@CKL:/opt$ sudo apt install tcpdump
```

شایان ذکر است، اگر بخواهید tcpdump را اجرا کنید و مورد استفاده قرار بدهید، نیاز به سطح دسترسی ریشه یا root خواهید داشت. اما از آنجایکه ما نمی‌خواهیم کوکو با سطح دسترسی ریشه اجرا شود، باید این فایل باینری را با یک قابلیت خاص لینوکس تنظیم کنیم، که بدین منظور می‌توانید از فرمان زیر استفاده کنید.

```
Milad@CKL:~$ sudo groupadd pcap
Milad@CKL:~$ sudo usermod -a -G pcap cuckoo
Milad@CKL:~$ sudo chgrp pcap /usr/sbin/tcpdump
Milad@CKL:~$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
```

پس از اجرای فرمان قسمت بالا، می‌توانید نتیجه اجرای آن را با استفاده از فرمان زیر تصدیق کنید.

```
Milad@CKL:~$ getcap /usr/sbin/tcpdump
```

همچنین اگر بر روی سامانه‌عامل خود مجموعه بسته‌های نرم‌افزاری cap را نصب نکرده‌اید، می‌توانید با استفاده از فرمان زیر آن را بر روی سامانه‌عامل خود نصب کنید.

```
Milad@CKL:~$ sudo apt-get install libcap2-bin
```

پس از اینکه نصب و پیکربندی کتابخانه‌ها را در سامانه‌عامل میزبان به اتمام رساندید، نوبت به نصب و پیکربندی جعبه‌شنی کوکو بر روی سامانه‌عامل میزبان می رسد.

راه‌اندازی جعبه‌شنی کوکو در سامانه‌عامل میزبان

در این مرحله ما به نصب و پیکربندی جعبه‌شنی کوکو بر روی سامانه‌عامل میزبان خود خواهیم پرداخت. بدین منظور کافیست گام‌های آورده شده در زیر را دنبال کنید. البته قابل ذکر است، جعبه‌شنی کوکو را می‌توان از طریق دو روش نصب و راه‌اندازی کرد که ما در اینجا هر دو روش را مورد بررسی قرار خواهیم داد.

در روش اول شما نیاز دارید ابتدا بسته نرم‌افزاری جعبه‌شنی کوکو را دانلود کنید، بدین منظور می‌توانید به آدرس (http://www.cuckoosandbox.org/download.html) بروید و پس از اینکه صفحه دانلود جعبه‌شنی کوکو بارگزاری شد، با کلیک بر روی دکمه Download Cuckoo آن را دانلود کنید و سپس فرآیند پیکربندی آن را انجام بدهید.

در روش دوم شما می‌توانید به راحتی با اجرا کردن فرمان git clone و آدرس پروژه cuckoo در github آن را به ماشین خود clone کنید و سپس آن را مورد استفاده قرار بدهید. در این قسمت ما به منظور نصب جعبه‌شنی کوکو از روش اول استفاده خواهیم کرد. پس از اینکه دانلود فایل tar جعبه‌شنی کوکو به اتمام رسید، با استفاده از فرمان زیر می‌توانید آن را از حالت فشرده شده خارج کنید و سپس فرآیند پیکربندی آن را آغاز کنید.

```
Milad@CKL:~$ tar -zxvf cuckoo-current.tar.gz
```

بعد از اینکه جعبه‌شنی کوکو را از حالت فشرده خارج ساختید، قبل از اینکه پیکربندی آن را آغاز کنید، باید سامانه‌عامل مهمان یا محیط اجرایی بدافزارها را بر روی ماشین مجازی نصب و راه‌اندازی کنید. در این قسمت ما به منظور مجازی‌سازی از نرم‌افزار VirtualBox در محیط لینوکس استفاده خواهیم کرد. برای دانلود این نرم افزار می‌توانید به آدرس https://www.virtualbox.org/wiki/Downloads رجوع کنید

و پس از دانلود آن را بر روی سامانه‌عامل خود نصب کنید. پس از اینکه نرم‌افزار مجازی‌ساز VirtualBox را دانلود کردید، با استفاده از فرمان زیر می‌توانید آن را بر روی سامانه‌عامل اوبونتو خود نصب و راه‌اندازی کنید.

```
Milad@CKL:~$ sudo dpkg -i virtualbox-4.3_4.3.12-93733~Ubuntu~raring_i386.deb
Milad@CKL:~$ sudo /etc/init.d/vboxdrv setup
```

بعد از اتمام فرآیند نصب نرم‌افزار Virtualbox، قبل از راه‌اندازی سامانه‌عامل مهمان بر روی آن به عنوان یک سامانه‌عامل مجازی، نیاز خواهید داشت درایور vbox را بر روی سامانه‌عامل لینوکس اوبونتو نصب کنید. برای نصب این درایور، ابتدا باید هدرهای هسته لینوکس خودتان را نصب کنید. چونکه هدرهای هسته لینوکس هنگام کامپایل vboxdrv نیاز هستند. برای نصب هدرهای هسته اوبنتو می‌توانید از فرمان آورده شده در قسمت زیر استفاده کنید.

```
Milad@CKL:~$ apt install linux-headers-$(uname -r)
```

بعد از اینکه نصب هدرهای سامانه‌عامل لینوکس اوبونتو خود را به اتمام رساندید، می‌توانید vboxdrv را با استفاده از فرمان زیر به سادگی نصب کنید.

```
Milad@CKL:~$ sudo /etc/init.d/vboxdrv setup
* Stopping VirtualBox kernel modules            done...
* Recompiling VirtualBox kernel modules         done...
* Starting VirtualBox kernel modules            done...
```

بعد از اجرای فرمان بالا، اگر تمامی خروجی‌ها Done بود، معنی آن این است که نصب درایور vbox به درستی صورت گرفته است.

آماده سازی سامانه‌عامل مهمان

هنگام نصب سامانه‌عامل ویندوز XP که ما در اینجا به عنوان محیط تحلیل بدافزار از آن استفاده خواهیم کرد، باید به نامی که برای این سامانه‌عامل در حین نصب بر روی Virtualbox اختصاص می‌دهید، توجه کنید. چراکه هنگام پیکربندی جعبه‌شنی کوکو، باید نام سامانه‌عامل مجازی خود را در فایل پیکربندی virtualbox.conf ذکر کنید تا جعبه‌شنی کوکو بتواند با آن تعامل برقرار کند.

در گام اول نصب سامانه‌عامل ویندوز XP در Virtualbox، باید نام، نوع و نسخه سامانه‌عامل را مشخص سازیم. در اینجا ما برای نام سامانه‌عامل مجازی از کلمه cuckoo1 استفاده خواهیم کرد و نسخه و نوع سامانه‌عامل را هم بر روی Windows قرار می دهیم. سپس فرآیند نصب را ادامه می دهیم.

تصویر ۱۱: انتخاب نام برای ماشین مجازی

اما قبل از اینکه سامانه‌عامل مهمان خود را بر روی Virtualbox روشن کنید، باید یک رابط شبکه برای ماشین مجازی پیکربندی کنید، بدین منظور گام‌های آورده شده در ادامه این قسمت را دنبال کنید.

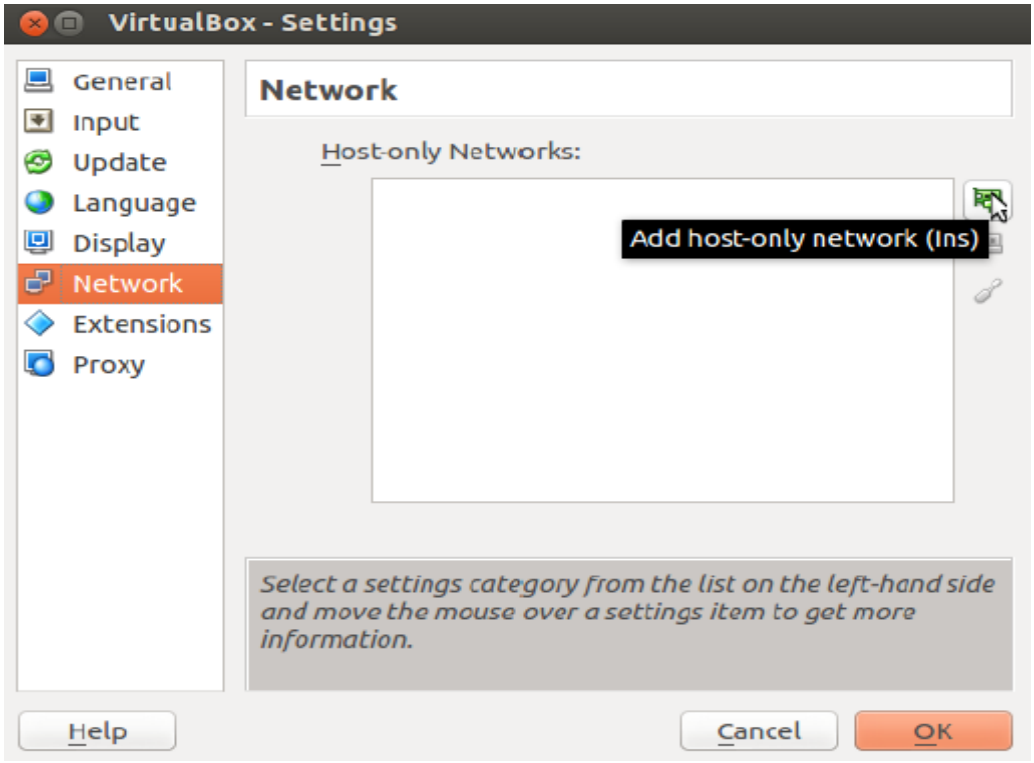
در حالت پایه، نرم‌افزار VirtualBox چندین نوع شبکه‌بندی مانند دیگر مجازی‌سازها دارد که پیش از این در قسمت VMware آن‌ها را بررسی کردیم. این نوع شبکه‌بندی‌ها توسط سامانه‌عامل مهمان می‌تواند مورد استفاده قرار گیرند.

هر کدام از انواع پیکربندی شبکه Virtualbox یک قابلیت مخصوص را به شما ارائه می‌دهد که بر حسب نیاز می‌توانید از آنها بهره‌مند شوید. در اینجا ما قصد بررسی انواع حالت‌های شبکه بندی Virtualbox را نداریم، اما به منظور کسب اطلاعات بیشتر در این زمینه می‌توانید به آدرس http://www.virtualbox.org/manual/ch06.html رجوع کنید.

نکته : شایان ذکر است، برای استفاده از جعبه‌شنی کوکو و آشنایی با قابلیت‌های آن نیاز به دانلود نمونه بدافزارهایی به منظور آزمایش و تحلیل خواهید داشت. به همین منظور به نشانی (aiooo.ir) رجوع کنید، تا نمونه بدافزارهای مورد استفاده قرار گرفته در این سلسله مقالات را دریافت کنید.

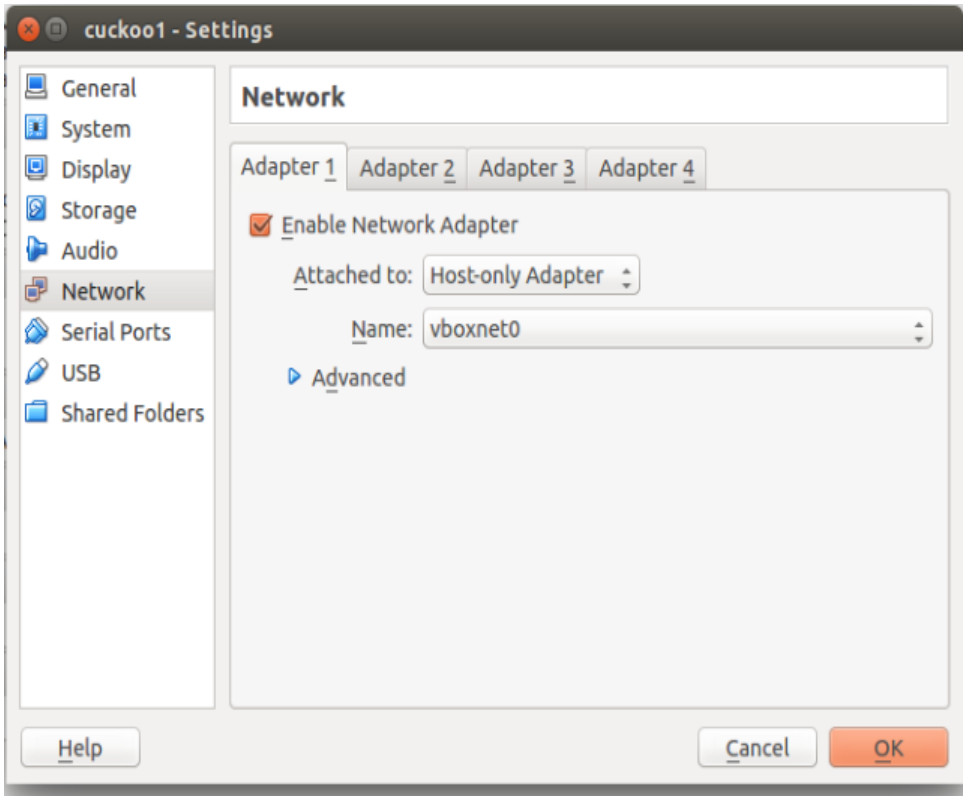
با این اوصاف، ما در استفاده از جعبه‌شنی کوکو و ارتباط برقرار کردن بین ماشین میزبان و سامانه‌عامل مجازی مهمان از نوع شبکه‌بندی Host-Only networking استفاده خواهیم کرد، بدین دلیل که این نوع شبکه‌بندی سامانه‌عامل مهمان را از شبکه خارجی یا اینترنت ایزوله می‌کند. همچنین، با استفاده از این نوع شبکه‌بندی، سامانه‌عامل میزبان و مهمان می‌توانند با یک دیگر به راحتی تعامل بر قرار کنند.

برای پیکربندی این نوع شبکه‌بندی ابتدا به منوی فایل بروید و سپس گزینه Preferences... را انتخاب کنید. در نهایت پس از باز شدن صفحه تنظیمات Virtualbox به تب Network بروید و به منظور ایجاد کردن یک رابط شبکه مبتنی بر Host-only بر روی دکمه ای که در تصویر زیر مشخص شده کلیک کنید.



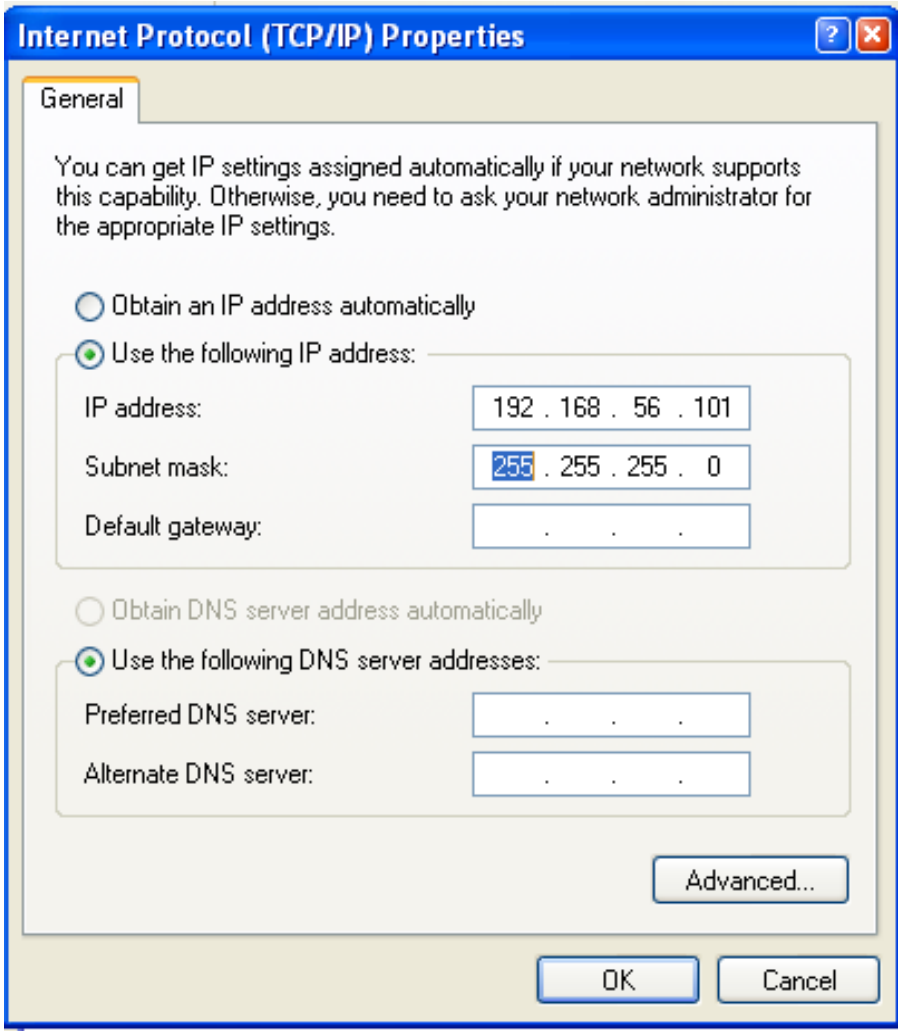
تصویر ۱۲: شبکه‌بندی VirtualBox

در گام دوم؛ شما نیاز خواهید داشت تنظیمات شبکه سامانه‌عامل مهمان را پیکربندی کنید. بدین منظور ابتدا آن را در صفحه اصلی Virtualbox انتخاب کنید، و سپس با کلیک بر روی آیکون Settings وارد پانل تنظیمات سامانه‌عامل مد نظر خود شوید. بعد از آن به تب Network بروید و تنظیمات این قسمت را مطابق تصویر آورده شده در قسمت زیر به روز رسانی کنید.



تصویر ۱۳: تنظیمات آداپتور شبکه

در گام سوم، پس از اینکه پیکربندی شبکه سامانه‌عامل مهمان را بر روی Virtualbox انجام دادید، می‌توانید سامانه‌عامل را روشن کنید. بعد از اینکه سامانه‌عامل را روشن کردید، و سامانه‌عامل با موفقیت راه‌اندازی شد، به Control Panel و سپس Network Connection بروید. پس از آن بر روی آیکون Local Area Connection کلیک کنید و سپس به صورت دستی به آن آدرس 192.168.56.101 را اختصاص بدهید و بر روی OK کلیک کنید.



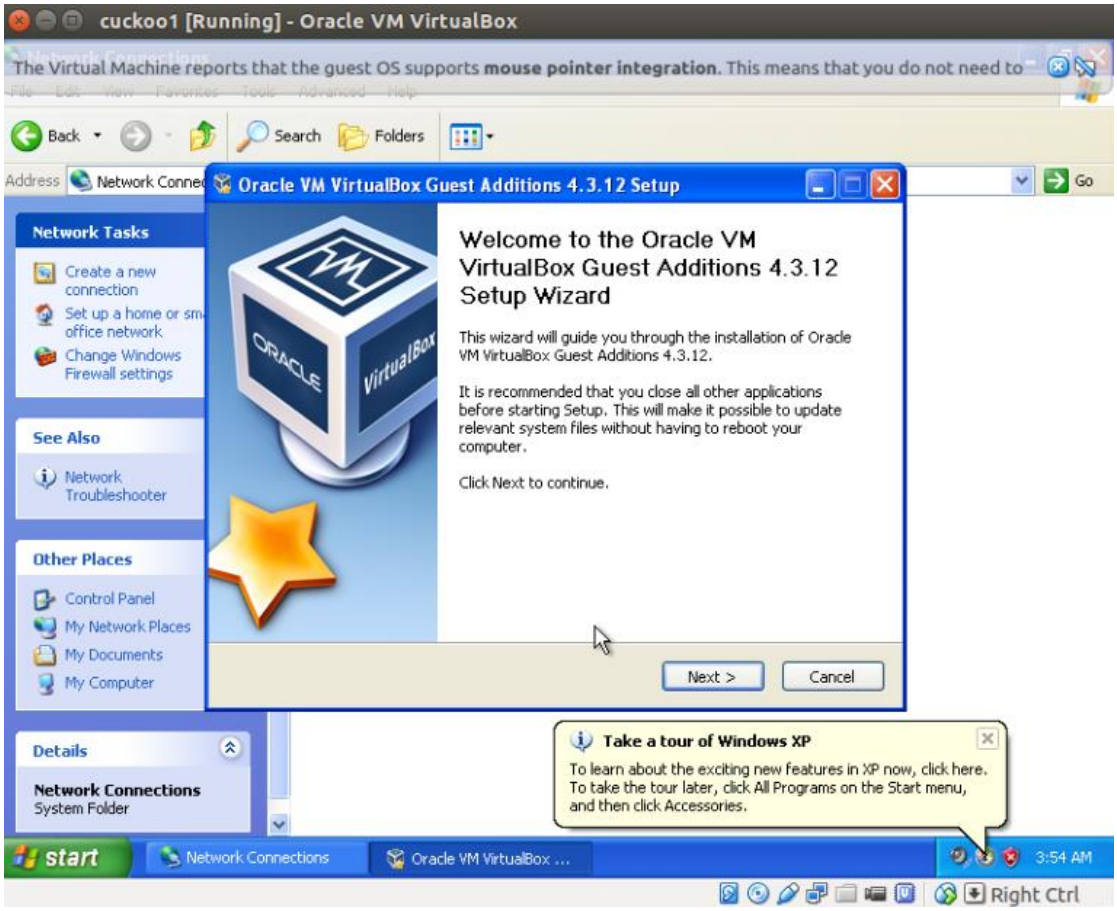
تصویر ۱۴: پیکربندی شبکه ویندوز XP

در گام چهارم شما باید دیوار آتش سامانه‌عامل ویندوز XP را خاموش کنید. برای خاموش کردن دیوار آتش ابتدا به Control Panel بروید و سپس بر روی Windows Firewall کلیک کنید. سپس در پنجره جدید که باز می‌شود، گزینه Off(Not Recommanded) را انتخاب کنید.

بعد از اینکه دیوار آتش سامانه‌عامل را خاموش کردید، از ماشین میزبان با استفاده از دستور Ping آدرس IP که به این ماشین اختصاص دادید را ping کنید تا صحت برقراری ارتباط تصدیق شود. همچنین از داخل ماشین مجازی آدرس IP ماشین میزبان را ping کنید. پس از اینکه هر دو ماشین توانستن هم دیگر را به درستی Ping کنند، می‌توانید به مرحله بعد بروید.

راه‌اندازی یک پوشه اشتراکی بین سامانه‌عامل میزبان و مهمان

به منظور راه‌اندازی یک پوشه اشتراکی بین سامانه‌عامل مهمان و سامانه‌عامل میزبان، ابتدا شما باید سامانه‌عامل مهمان را روشن کنید و سپس از منوی Devices بر روی Install Guest Additions کلیک کنید تا بسته‌های نرم‌افزاری VirtualBox بر روی سامانه‌عامل مهمان نصب شوند تا در نهایت شما بتوانید بین سامانه‌عامل مهمان و میزبان یک پوشه اشتراکی ایجاد کنید.

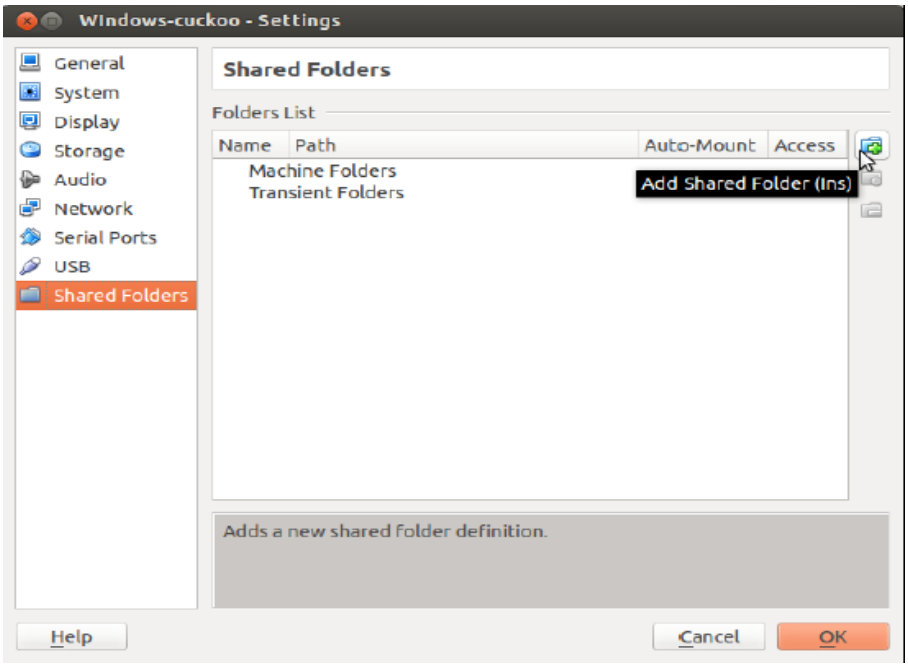


تصویر ۱۵: محیط نصب ابزار VirtualBox

با این حال، پس از اینکه بسته‌های نرم‌افزاری VirtualBox را نصب کردید، به منظور پیکربندی یک پوشه اشتراکی بین سامانه‌عامل مهمان و میزبان می‌توانید گام‌های آورده شده در قسمت زیر را دنبال کنید. در گام اول، پس از اینکه سامانه‌عامل ویندوز XP راه‌اندازی شد، به منوی Devices بروید و به منظور پیکربندی یک پوشه اشتراکی بین ویندوز XP و سامانه‌عامل میزبان (اوبنتو) بر روی Shared Folders کلیک کنید.

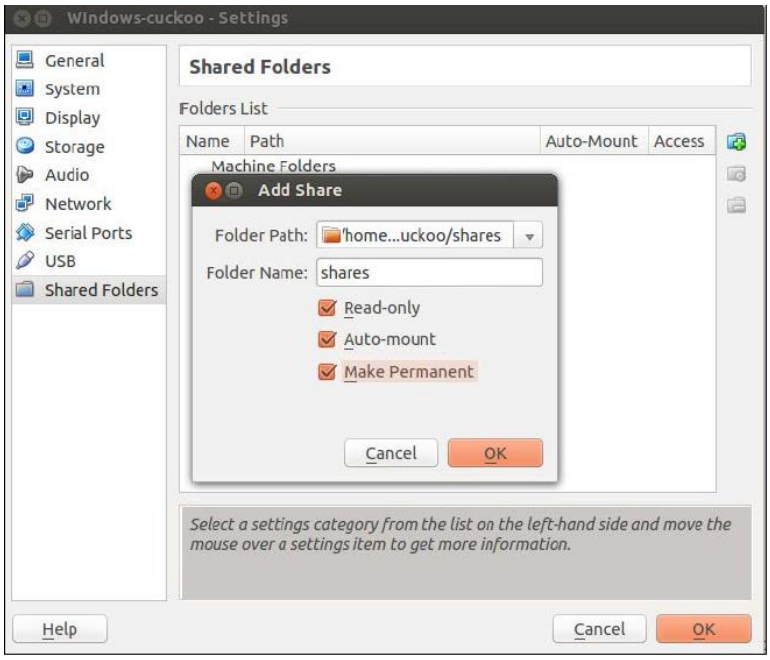
تصویر ۱۶: پیکربندی پوشه اشتراکی

سپس در گام دوم بر روی آیکون Add Shared Folder به صورتی که در تصویر زیر نشان داده شده است کلیک کنید تا پنجره تعریف تنظیمات پوشه اشتراکی باز شود.



تصویر ۱۷: پیکربندی پوشه اشتراکی در VirtualBox

پس از اینکه بر روی Add Shared Folders کلیک کردید، صفحه‌ای به شکل زیر به نمایش در خواهد آمد. در این صفحه شما باید در قسمت Folder Path مسیر پوشه‌ای که می‌خواهید در سامانه‌عامل میزبان به اشتراک بگذارید و در قسمت Folder Name یک نام برای پوشه اشتراکی تنظیم کنید. دیگر گزینه‌های این پنجره را همانند تصویر آورده شده در قسمت زیر تنظیم کنید.

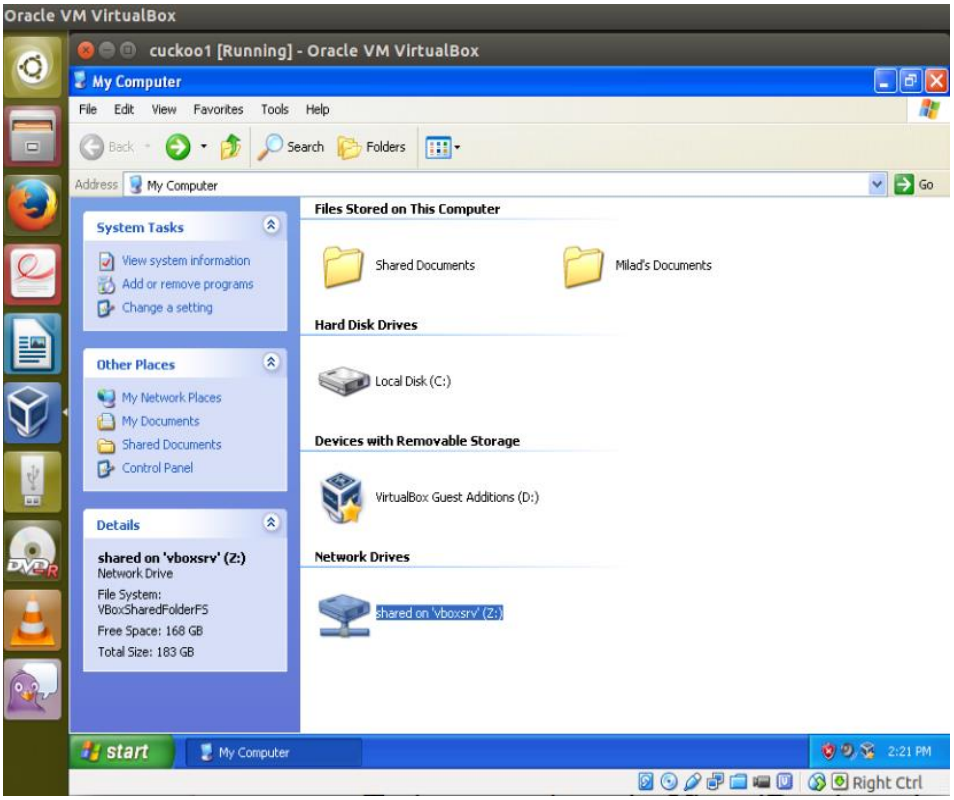


تصویر ۱۸: انتخاب پوشه اشتراکی

در گام بعد، وارد سامانه‌عامل مهمان شوید و بر روی My Computer کلیک راست کنید. سپس در منوی که باز می‌شود گزینه Map network driver... را انتخاب کنید. بعد از اینکه پنجره Map Network Driver باز شد، در منوی بازشوی قسمت Drive یک درایو را به منظور تعامل با پوشه اشتراکی انتخاب کنید و در قسمت Folder مسیر پوشه اشتراکی تحت شبکه را وارد کنید.

به این نکته دقت کنید؛ نامی که به پوشه اشتراکی در قسمت قبل اطلاق کردید، در اینجا باید به درستی ذکر شود تا ارتباط با موفقیت برقرار گردد. از آنجایی که در مرحله قبل برای پوشه اشتراکی نام shares را انتخاب کردم، در این قسمت آدرس آن را به شکل \\vboxsrv\shares وارد کرده و سپس بر روی Finish کلیک می کنم تا ارتباط برقرار شود.

بعد از اینکه بر روی Finish کلیک کنید و به My Computer سامانه‌عامل بروید یک درایو با نام Z مشاهده خواهید کرد که به سامانه‌عامل افزوده شده است. این درایو در اصل یک بستر تعاملی با پوشه اشتراکی است که شما در ماشین میزبان (Ubuntu) آن را به اشتراک گذاشتید. حال از این به بعد به سادگی می‌توانید بین این دو سامانه‌عامل فایل جا به جا کنید.



تصویر ۱۹: پیکربندی نهایی درایو اشتراکی

حال نوبت به پیکربندی سامانه‌عامل مهمان می‌رسد. در این قسمت ما نیاز داریم در سامانه‌عامل مهمان (ویندوز XP) به منظور اجرای اسکریپت‌های پایتون بسته نرم‌افزاری این زبان را نصب کنیم. بدین منظور کافیست به آدرس http://python.org/download بروید و از آنجا نسخه Python 2.7 را برای ویندوز دانلود کنید.

نکته : توجه داشته باشید که حتما نسخه ۲.۷ را دانلود کرده باشید. زیرا اگر دیگر نسخه‌های این زبان را نصب کنید، نمی‌توانید اسکریپت agent.py جعبه‌شنی

کوکو را بر روی سامانه‌عامل ویندوز XP به درستی اجرا کنید.

پس از نصب کتابخانه‌های این زبان، شما باید چندین نرم‌افزار قدیمی را به منظور اجرای بدافزارهای مورد بررسی این کتاب دانلود کنید. لیست این نرم‌افزارها در زیر آورده شده است.

- Microsoft Office 2003/2007
- Acrobat Reader 9.5
- Mozilla Firefox 3.6

سپس در مرحله بعد باید فایل agent.py جعبه‌شنی کوکو را به سامانه‌عامل مهمان منتقل کنید. با استفاده از فرمان زیر می‌توانید این کار را انجام بدهید.

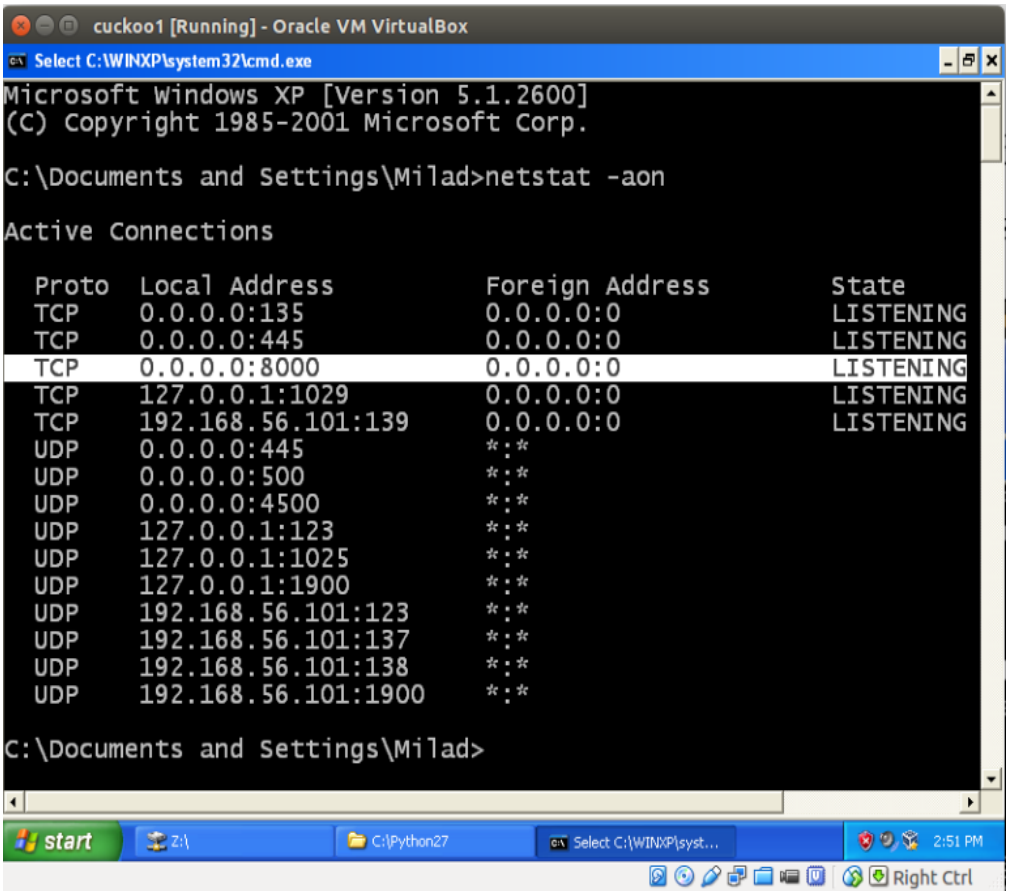
```
Milad@CKL:~$ cp /opt/cuckoo/agent/agent.py ~/Desktop/shares/
```

سپس به سامانه‌عامل مهمان بروید و در آنجا فایل agent.py را به پوشه C:\\Python27 منتقل کنید و نام آن را از agent.py به agent.pyw تغییر بدهید.

نکته : هنگامی که شما پسوند یک فایل پایتون را به pyw تغییر می دهید، بعد از اینکه آن اجرا شود، صفحه کنسول سامانه‌عامل را نمایش نمی‌دهد. به عنوان مثال، اگر شما فایل agent.py را اجرا کنید، یک صفحه کنسول باز خواهد شد که شرح فرآیند اجرای اسکریپت را به شما گزارش می‌دهد، اما اگر آن را به agent.pyw تغییر نام بدهید و اجرا کنید هیچ صفحه کنسولی مشاهده نخواهید کرد.

در گام بعد به منظور اجرای این اسکریپت در Startup به صورت دائمی، فایل agent.pyw را به مسیر C:\Document and settings\c3phalex1n\StartMenu\Programs\Startup انتقال بدهید. سپس هنگامی که این اسکریپت اجرا شود، درگاه 8000 پروتکل TCP در حالت شنود باید قرار بگیرد.

به منظور بررسی اینکه این درگاه به درستی باز شده است، می‌توانید فرمانی که در زیر آورده شده است را در Command Prompt سامانه‌عامل ویندوز XP اجرا کنید تا تمامی درگاه‌های در حال شنود سامانه‌عامل نمایش داده شوند.



تصویر ۲۰: شنود پورت ۸۰۰۰

در تصویر بالا مشاهده می‌کنید که درگاه ۸۰۰۰ بر روی حالت شنود و یا Listening قرار گرفته است. این موضوع حاکی از این است که اسکریپت agent.py توانسته است به درستی اجرا شود. در گام بعد شما نیاز دارید قواعد فیلترگذاری و Ip forwarding یا به عبارتی مسیریابی سامانه‌عامل میزبان را با استفاده از iptables پیکربندی کنید. بدین منظور کافیست فرآمین آورده شده در قسمت زیر را در ترمینال سامانه‌عامل اوبونتو اجرا کنید.

```
Milad@CKL:~$ iptables -A FORWARD -o eth0 -i vboxnet0 -s 192.168.56.0/24 -m conntrack --ctstate NEW -j ACCEPT
```

```
Milad@CKL:~$ iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT
Milad@CKL:~$ iptables -A POSTROUTING -t nat -j MASQUERADE
Milad@CKL:~$ sysctl -w net.ipv4.ip_forward=1
```

حال که تمامی مراحل پیش نیاز استفاده از جعبه‌شنی کوکو را آماده و پیکربندی کردیم، نوبت به پیکربندی خود جعبه‌شنی کوکو می رسد.

ایجاد یک نام کاربری جدید

برای استفاده از جعبه‌شنی cuckoo می‌توانید از نام کاربری اصلی خود یا از یک نام کاربری دیگر استفاده کنید. اما همواره توسیعه می‌شود، برای استفاده از جعبه‌شنی کوکو از یک نام کاربری دیگر عضو گروه vboxusers استفاده کنید. زیرا اگر نام کاربری اصلی خودتان را در این گروه بیفزایید، شناسه کاربری شما از sudoers خارج می‌شود و دیگر نمی‌توانید عملیات های سطح ریشه را در سامانه‌عامل انجام بدهید. به هر حال، به منظور ایجاد یک نام کاربری جدید فرمان آورده شده در قسمت زیر را دنبال کنید.

```
Milad@CKL:~$ sudo adduser cuckoo
```

از آنجاییکه ما از VirtualBox به منظور مجازی‌سازی استفاده می کنیم، باید نام کاربری جدیدی را که افزودیم را به گروه vboxusers بیفزاییم. به منظور انجام این کار می‌توانید از فرمان آورده شده در قسمت زیر استفاده کنید.

```
Milad@CKL:~$ sudo usermod -G vboxusers cuckoo
```

بعد از انجام عملیات‌های آورده شده در قسمت بالا می‌توانید فرآیند نصب کوکو را ادامه بدهید.

نصب کردن جعبه‌شنی کوکو

برای نصب و استفاده از جعبه‌شنی کوکو، نیاز به انجام کار خاصی ندارید. کافیست فقط فایل tar آن را دانلود کنید و سپس در یک مسیر خاصی از سامانه‌عامل لینوکس آن را از حالت فشرده خارج سازید تا بتوانید آن را مورد استفاده قرار بدهید. پیشتر ما نحوه دانلود و خارج‌سازی این جعبه‌شنی را مورد بررسی قرار دادیم. با این حال، ما در اینجا به منظور استفاده از این جعبه‌شنی، آن را در پوشه /opt/ قرار می دهیم و از حالت فشرده خارج می سازیم. اما قبل از اینکه بخواهیم فرآیند استفاده از این جعبه‌شنی را مورد بررسی قرار بدهیم، باید با

فایل های پیکربندی آن آشنایی نسبی داشته باشیم. به همین دلیل در این قسمت به بررسی فایل های پیکربندی این جعبه‌شنی خواهیم پرداخت.

فایل پیکربندی cuckoo.conf

این فایل شامل تنظیمات پیکربندی پایه جعبه‌شنی کوکو می‌شود. به عنوان مثال، شما می‌توانید با تغییر ایجاد کردن در تنظیمات موجود در این فایل، جعبه‌شنی کوکو را مجبور سازید که هر بار اجرا می‌شود، نسخه جاری خودش را بررسی کند. اگر شما از این ویژگی استفاده کنید، جعبه‌شنی کوکو نسخه جدیدش را به صورت خودکار دانلود می‌کند و مورد استفاده قرار می‌دهد. همچنین شما می‌توانید نسخه قدیمی جعبه‌شنی کوکو را پس از به روز رسانی بر روی سیستم نگاه دارید یا حذف کنید. که تمامی این موارد را می‌توانید به سادگی در این فایل پیکربندی تنظیم کنید.

فایل پیکربندی ماشین‌مجازی <machinemanager>.conf

همانطور که پیشتر مورد بررسی قرار گرفت، جعبه‌شنی کوکو قابلیت تعامل با مجازی‌سازهای معروف نظیر VMware، Virtualbox و غیره را دارد و برای هر کدام از این‌ها یک فایل پیکربندی شامل می‌شود که در آن نحوه تعامل جعبه‌شنی کوکو با آن مجازی‌ساز تنظیم می‌شود.

در این قسمت ما از مجازی‌ساز Virtualbox استفاده می‌کنیم، بنابراین فقط نیاز داریم تنظیمات virtualbox.conf را مورد بررسی قرار بدهیم و اگر لازم بود تنظیمات موجود در آن را مورد ویرایش قرار بدهیم. به عنوان مثال، اگر می‌خواهید هنگام استفاده از جعبه‌شنی کوکو، مجازی‌ساز Virtualbox در حالت گرافیکی اجرا شود، کافیست که فقط مقدار mode را در این فایل پیکربندی برابر با gui قرار بدهید یا بالعکس اگر خواستید که Virtualbox در حالت خط فرمان اجرا شود، باید مقدار mode را برابر headless قرار بدهید.

در حالت کلی، فایل virtualbox.conf شامل تنظیمات تعاملی جعبه‌شنی کوکو با Virtualbox می‌شود. همچنین تمامی پارامترهای پیکربندی که در این فایل وجود دارند، به صورت کامل در داخل خود فایل مستندسازی شده‌اند، که شما می‌توانید به سادگی آنها را مورد مطالعه قرار بدهید و با نحوه عملکرد آن پارامترها آشنا شوید.

همچنین، به یاد دارید که در هنگام نصب سامانه‌عامل مهمان در مجازی‌ساز Virtualbox متذکر شدیم، باید به نامی که به سامانه‌عامل مهمان اختصاص می‌دهید، توجه کنید. زیرا در هنگام استفاده از جعبه‌شنی کوکو باید آن را برای کوکو تنظیم کنید.

به عنوان مثال، تصور کنید که ما یک سامانه‌عامل مهمان دیگر با نام WindowsCuckoo نصب و راه‌اندازی کرده ایم. حال می‌خواهیم از این سامانه‌عامل به عنوان سامانه‌عامل مهمان برای جعبه‌شنی کوکو استفاده کنیم. بدین منظور ابتدا فایل پیکربندی virtualbox.conf را با یک ویرایشگر نظیر nano یا vim باز می کنیم و سپس به قسمت شناسه [cuckoo1] می رویم که شناسه ماشین مجازی مورد استفاده توسط جعبه‌شنی کوکو است. سپس در قسمت [cuckoo1] مقدار پارامتر label را با نام WindowsCuckoo که نام سامانه‌عامل مهمان ما هست، تنظیم می‌کنیم. مانند نمونه‌ای که در تصویر ۲۱ آورده شده است.

```
[cuckoo1]
# Specify the label name of the current machine as specified in your
# VirtualBox configuration.
label = cuckoo1
```

تصویر ۲۱: نام ماشین‌مجازی میزبان بدافزار

شایان ذکر است، اگر بخواهیم سامانه‌عامل‌های دیگری هم را به عنوان سامانه‌عامل مهمان به منظور استفاده توسط جعبه‌شنی کوکو نصب و راه‌اندازی کنیم، کافیست به تعداد سامانه‌عاملی که نصب کردیم، در قسمت پارامتر machines به هر کدام یک شناسه اختصاص بدهیم و جزئیات آن را در فایل پیکربندی virtualbox.conf تعریف کنیم.

به عنوان مثال، اگر بخواهیم یک سامانه‌عامل ویندوز هفت را به عنوان سامانه‌عامل مهمان برای جعبه‌شنی کوکو نصب و راه‌اندازی کنیم. ابتدا سامانه‌عامل ویندوز هفت را با نامی مانند Windows7Cuckoo بر روی Virtualbox نصب و راه‌اندازی می کنیم.

پس از اینکه نصب و راه‌اندازی سامانه‌عامل ویندوز هفت به اتمام رسید به پارامتر machines یک شناسه جدید با نام MiladSample باید بیفزایم. سپس به صورت جداگانه یک قسمت جدید با شناسه

[MiladSample] ایجاد می کنم و در آن به پارامتر label مقدار Windows7Cuckoo که نام سامانه‌عامل مهمان هست را اختصاص می دهیم.

```
# Specify a comma-separated list of available machines to be used. For each
# specified ID you have to define a dedicated section containing the details
# on the respective machine. (E.g. cuckoo1,cuckoo2,cuckoo3)
machines = cuckoo1, MiladSample

[MiladSample]
label = Windows7Cuckoo
```

تصویر ۲۲: نام ماشین‌مجازی Windows 7 میزبان بدافزار

پس از آن می‌توانیم از این سامانه‌عامل هم به عنوان سامانه‌عامل مهمان استفاده کنیم. شایان ذکر است، هر سامانه‌عامل مهمانی که شما راه‌اندازی می‌کنید، باید درگاه 8000 پروتکل TCP طبق پیکربندی تعاملی Cuckoo بر روی آن باز باشد و همچنین IP آدرس آن در فایل پیکربندی کوکو تنظیم شده باشد تا جعبه‌شنی کوکو بتواند به آن متصل شود و رفتار بدافزار را در محیط آن سامانه‌عامل مورد بررسی قرار بدهد.

فایل پیکربندی procssing.conf

این فایل پیکربندی به شما اجازه می‌دهد تمام ماژول‌های پردازشگر جعبه‌شنی کوکو را پیکربندی، فعال و غیر فعال کنید. در حالت معمول نیاز نیست هیچ تغییری در این فایل ایجاد کنید.

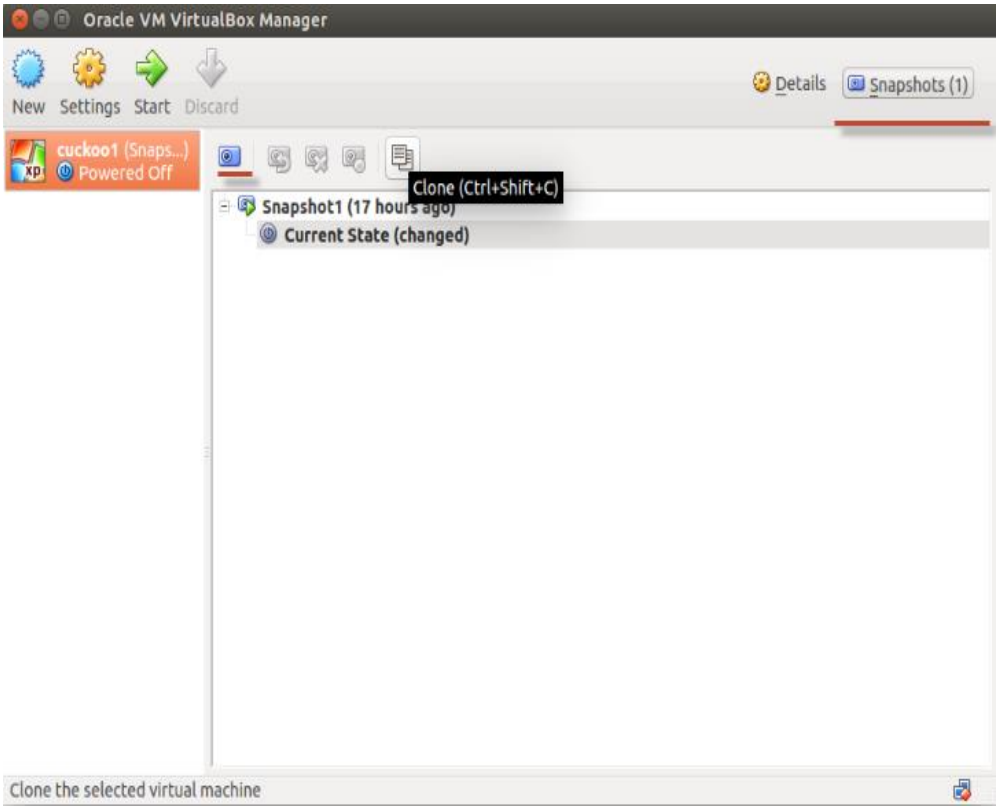
فایل پیکربندی reporting.conf

فایل پیکربندی conf/reporting.conf شامل اطلاعات تولید گزارش خودکار توسط جعبه‌شنی کوکو می‌شود. این فایل شامل روش ها و نوع های گزارشگری می‌شود که شما می‌توانید پس از اتمام تجزیه و تحلیل یک فایل توسط جعبه‌شنی کوکو از آنها استفاده کنید. حال که با تمامی جزئیات و اطلاعات پیکربندی جعبه‌شنی کوکو آشنا شدیم؛ می توانیم تحلیل یک بدافزار را با استفاده از Cuckoo آغاز کنیم. بدین منظور گام های آورده شده در زیر را دنبال کنید.

در گام اول استفاده از جعبه‌شنی کوکو، باید از سامانه‌عامل مهمان یک Snapshot بگیرید. برای Snapshot گرفتن از سامانه‌عامل مهمان، کافیست فرمان آورده شده در قسمت زیر را در ترمینال اجرا کنید تا از سامانه‌عامل مهمان یک Snapshot گرفته شود.

```
Milad@CKL:~$ vboxmanage snapshot "cuckoo1" take "Snapshot1" --pause
```

البته شما می‌توانید علاوه بر خط فرمان؛ این کار را با رفتن به محیط Virtualbox و انتخاب گزینه Snapshot و کلیک بر روی آیکون دوربین انجام بدهید.

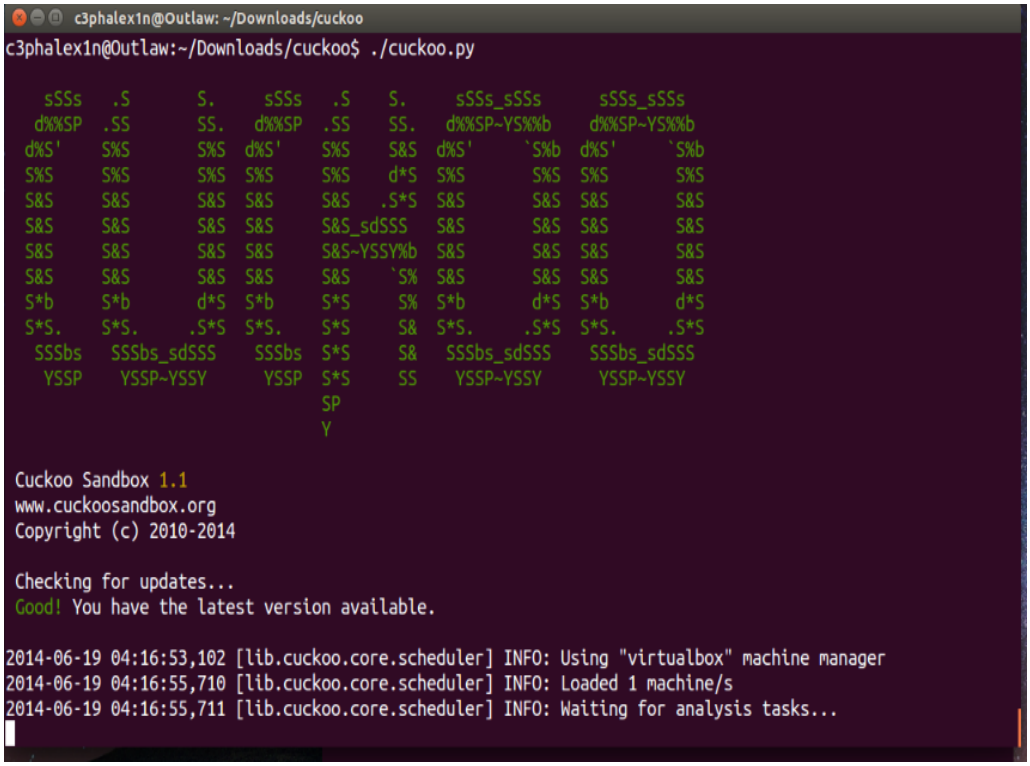


تصویر ۲۳: محیط VirtualBox و گزینه Snapshot

در گام دوم به منظور اجرای جعبه‌شنی کوکو، کافیست به مسیر نصب آن بروید و سپس فرمان آورده شده در قسمت زیر را اجرا کنید تا جعبه‌شنی کوکو اجرا شود و آماده تحلیل بدافزارها گردد.

```
Milad@CKL:~/Downloads/cuckoo$ ./cuckoo.py
```

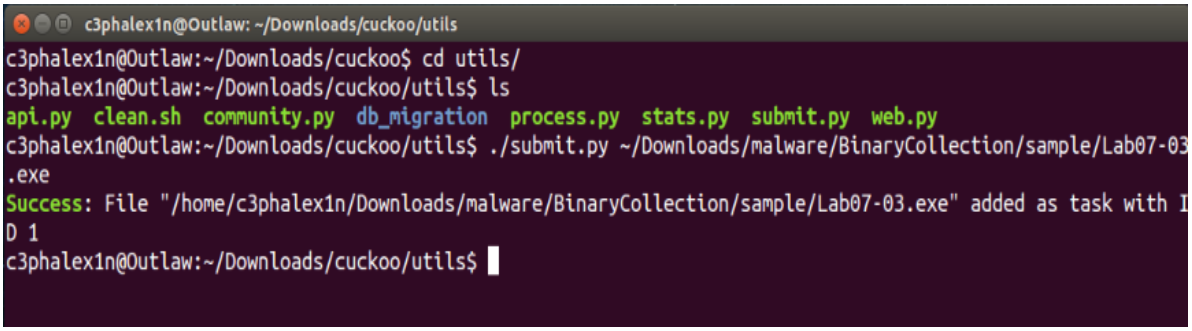
بعد از اینکه فرمان آورده شده در قسمت بالا را اجرا کنید، به صورت خودکار سامانه‌عامل مهمان در Virtualbox به حالت کنترل جعبه‌شنی کوکو می‌رود و بنر جعبه‌شنی کوکو به نمایش در می‌آید و پیام بارگزاری ماشین مجازی (Loaded 1 machine/s) را صادر می‌کند.



تصویر ۲۴: بارگزاری جعبه‌شنی کوکو

درگام سوم، پس از اینکه جعبه‌شنی کوکو با موفقیت اجرا شد و توانست با ماشین مجازی ارتباط برقرار کند، باید بدافزارهایی را که می‌خواهیم مورد تحلیل قرار بدهیم را در جعبه‌شنی کوکو ثبت کنیم، تا جعبه‌شنی کوکو تحلیل آن را در سامانه‌عامل مهمان آغاز کند. با این حال، برای ثبت بدافزارها در کوکو باید از اسکریپت submit.py استفاده کنید که نحو استفاده از آن در زیر نمایش داده شده است.

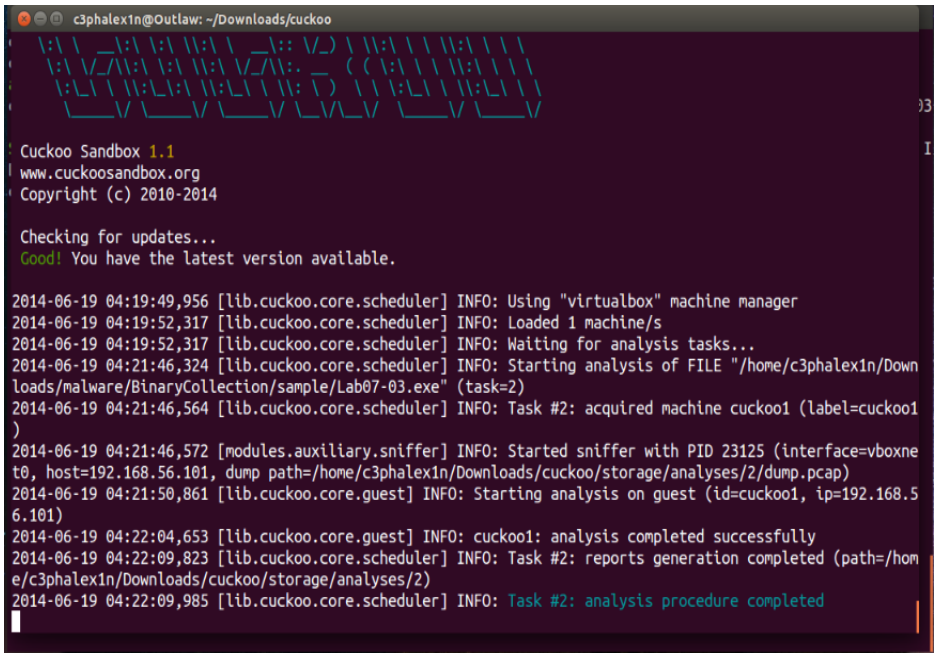
نکته : در این قسمت از یک بدافزار ساده استفاده شده است که نام آن Lab07-03.exe است. به منظور دانلود این بدافزار و دیگر بدافزارهای مورد استفاده قرار گرفته در این مقاله، همانطور که پیشتر گفته شد می‌توانید به آدرس http://aiooo.ir/ رجوع کنید.



تصویر ۲۵: بارگزاری بدافزار در ماشین مجازی

پس از اینکه بدافزار با موفقیت به سامانه‌عامل مهمان منتقل شود، در خروجی پیام Success را مشاهده خواهید کرد. همچنین قابل ذکر است، بعد از اینکه بدافزار به محیط سامانه‌عامل مهمان انتقال پیدا می‌کند به آن یک شناسه تعلق می‌گیرد که می‌توانید از آن شناسه به منظور مطالعه گزارش های تحلیل بدافزار مذکور توسط کوکو استفاده به عمل آورید.

به هر حال، پس از اینکه بدافزار با موفقیت به سامانه‌عامل مهمان منتقل شود، جعبه‌شنی کوکو به صورت خودکار ماشین مجازی را راه‌اندازی می‌کند و تحلیل بدافزار مدنظر شما را در محیط سامانه‌عامل مهمان آغاز می‌کند. شایان ذکر است، نتیجه لحظه به لحظه تحلیل بدافزار توسط کوکو را می‌توانید در cuckoo.py مشاهده کنید.



تصویر ۲۶: آغاز تحلیل بدافزار توسط جعبه‌شنی کوکو

بعد از اینکه فرآیند تحلیل بدافزار توسط کوکو به اتمام برسد، جعبه‌شنی کوکو این موضوع را با یک پیام گزارش می‌دهد. به عنوان مثال در تصویر بالا مشاهده می کنید که بدافزاری با شناسه ۲ تجزیه و تحلیل آن توسط کوکو به اتمام رسیده است.

نتیجه‌گیری

در این قسمت از سلسله مقالات تجزیه و تحلیل بدافزار متوجه شدیم، برای تجزیه و تحلیل بدافزار، نیاز خواهید داشت بدافزار را اجرا کنید تا رفتار آن را بتوانید مورد بررسی قرار بدهید. هنگامی‌که بدافزار اجرا می‌شود، باید دقت کنید که رایانه و یا شبکه شما آلوده نشود.

خوشبختانه نرم‌افزار VMware Workstation یا VirtualBox به شما اجازه می‌دهند، بدافزار را در یک محیط ایمن و قابل کنترل اجرا کنید و با استفاده از ابزارهایی خاص بتوانید پس از به اتمام رساندن فرایند تجزیه و تحلیل بدافزار، به سادگی آسیب‌هایی که ممکن است بدافزار به سامانه برساند را پاکسازی کنید و سامانه را به حالت اولیه و سالم خود بازگردانید.

در ادامه نحوه نصب و پیکربندی جعبه‌شنی کوکو را آموختیم که به ما در حین تحلیل باینری‌های مخرب کمک شایانی می‌کند. این جعبه‌شنی با تحلیل فایل‌های مخرب به صورت خودکار و ارائه گزارش از نحوه عملکرد باینری می‌تواند اطلاعات خوبی برای شروع تحلیل بدافزار ارائه بدهد تا در ادامه تحلیلگر با بررسی جزئیات به شکل عمیق تر متوجه ساختار و نحوه عملکرد آن شود. در نهایت تحلیلگر بدافزار خواهد توانست با ارائه یک سیگنیچر مبتنی بر شبکه و مبتنی بر میزبان از توسعه و رشد آن بدافزار در شبکه جلوگیری کند.

به هر صورت، در طی این سلسله مقالات، ما هنگامی‌که در مورد اجرای بدافزار گفتگو می‌کنیم، فرض خواهیم کرد که شما بدافزار را در ماشین‌مجازی اجرا کردید. شایان ذکر است، قابلیت‌های کلیدی ماشین مجازی VMWare Worksation را در حین کار با بدافزارها و تجزیه و تحلیل آن‌ها مورد بررسی قرار خواهیم داد.