به‌نام خداوند جان و خرد

پیاده‌سازی آزمایشگاه تحلیل بدافزار در لینوکس و ویندوز

(REMnux Linux, Cuckoo Sandbox, Multi-AV, …)

مهندس مجید داوری دولت آبادی

عضو گروه امنیت GrayHat Hackers

Security Information Assets

انتشارات پندارپارس

سرشناسه	:	داوری دولت‌آبادی، مجید، ۱۳۵۹ -
عنوان و نام پدیدآور	:	پیاده‌سازی آزمایشگاه تحلیل بدافزار در لینوکس و ویندوز (REMnux Linux, Cuckoo Sandbox, Multi-AV, ...)/ مجید داوری‌دولت‌آبادی.
مشخصات نشر	:	تهران : پندارپارس، ۱۳۹۵.
مشخصات ظاهری	:	۲۴۴ ص.: مصور، جدول، نمودار.
شابک	:	978-600-8201-05-2: ۱۸۰۰۰۰ ریال
وضعیت فهرست نویسی	:	فیپا
یادداشت	:	کتابنامه.
موضوع	:	نرم‌افزار بدافزار
موضوع	:	سیستم عامل لینوکس
موضوع	:	سیستم عامل یونیکس
موضوع	:	ویروس‌های کامپیوتر
موضوع	:	کامپیوترها -- ایمنی اطلاعات
رده بندی کنگره	:	۱۳۹۵۷۶/۷۶QA ۱۷۵د۹و/
رده بندی دیویی	:	۰۰۵/۸
شماره کتابشناسی ملی	:	۴۲۰۱۵۰۹

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶ **www.pendarepars.com**

تلفن: ۶۶۵۷۲۳۳۵ – تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۲۱۴۳۷۱۹۶۴ **info@pendarepars.com**

نام کتاب	:	پیاده‌سازی آزمایشگاه تحلیل بدافزار در لینوکس و ویندوز
ناشر	:	**انتشارات پندار پارس**
ترجمه و تالیف	:	مجید داوری دولت آبادی
چاپ نخست	:	**اردیبهشت ۹۵**
شمارگان	:	**۵۰۰ نسخه**
طرح جلد	:	**مصطفی مصباحی**
چاپ، صحافی	:	**روز**
قیمت	:	**۱۸۰۰۰ تومان** **شابک : ۲-۰۵-۸۲۰۱-۶۰۰-۹۷۸**

تقدیم به آنکه

همه زندگیم از آن اوست

تقدیم به همسر عزیزم

فهرست

سخنی با خوانندگان

دنیای بدافزارها و نرم‌افزارهای مُخرب امروزه وسعت بسیاری پیدا کرده است و همه‌ی تجهیزات و منابع اطلاعاتی و ارتباطی را تحت تأثیر خود قرار داده است. این نوع نرم‌افزارها همیشه در علم کامپیوتر و شبکه مطرح بوده و می‌باشند و در همه‌ی دوران‌ها یکی از دقدقه‌های اصلی مدیران سیستم و امنیت شبکه بوده است و هم اینک و در آینده نیز روز به‌روز بر اهمیت آن افزوده می‌شود. اکنون بدافزارها بسیار فعال‌تر از گذشته شده‌اند و از هوشمندی بالایی برخوردار هستند. از این‌رو ممکن است برخی از نرم‌افزارهای ضدویروس نتوانند به سرعت بدافزارها را شناسایی و پاکسازی کنند. در این حوزه همیشه کمبود ابزارهایی افزون بر نرم‌افزارهای ضدویروس، به‌منظور تجزیه و تحلیل بدافزارها و شناسایی رفتار و عملکرد آن‌ها احساس می‌شد، که خوشبختانه چند سالی است محققان و طراحان نرم‌افزارهای امنیتی در این حوزه نیز وارد شده‌اند و ابزارهای متنوعی برای کمک به امر تجزیه و تحلیل بدافزارها، طراحی و پیاده‌سازی نموده‌اند. این ابزارها به‌صورت ساخت‌یافته‌ای و براساس مکانیزم‌های گوناگون تحلیل رفتاری به بررسی و تحلیل انواع نرم‌افزارها و کدهای مُخرب می‌پردازند و در این خصوص کمک شایانی به تحلیلگران در این زمینه می‌کنند. وجود چنین ابزارهایی در آزمایشگاه‌های بررسی بدافزارها و شرکت‌های تولیدکننده ضدویروس، بسیار حیاتی می‌باشند و می‌توانند در امر شناسایی رفتار و تولید پادزهر بدافزارها کمک فراوانی به مختصصان تحلیل و تولید نرم‌افزارهای ضدویروس نمایند.

امروزه در این حوزه، آزمایشگاه‌هایی برپایه تحلیل بدافزار در کنار آزمایشگاه‌های شناسایی بدافزارهای موجود در فضای اینترنت و طراحی نرم‌افزارهای ضدویروس ایجاد شده‌اند که نقش اساسی در تولید ابزارهای ضدویروس برای یک بدافزار خاص و درحالت کلی برای یک نسخه کامل ضدویروس بازی می‌کنند. این نوع آزمایشگاه‌ها نیازمند تجهیزات و امکانات متنوع و صرف هزینه‌های بالا نمی‌باشند و به‌راحتی با کمک نرم‌افزارهای مجازی‌سازی مانند VMware، VirtualBox و غیره می‌توان آن‌ها را بر روی سیستم‌های‌عامل لینوکس و ویندوز پیاده‌سازی کرد که در این‌کار سهم سیستم‌عامل لینوکس به‌واسطه انبوه ابزارهای طراحی شده برای آن در این مقوله، نسبت به ویندوز بیشتر می‌باشد و از کارآیی بیشتری برخوردار است. در این حوزه ابزارهای خاص و قدرتمندی درقالب Sandboxها برای تحلیل بدافزارها طراحی شده‌اند که می‌توان از آن‌ها برای شناسایی رفتار بدافزارهای گوناگون و حتی جدید استفاده کرد. همچنین توزیع‌های لینوکس قدرتمندی نیز براساس این ساختار طراحی و منتشر شده‌اند که به‌صورت پیش‌فرض همه‌ی نرم‌افزارهای مورد نیاز برای تجزیه و تحلیل بدافزارها و پیاده‌سازی یک آزمایشگاه کامل در این

خصوص بر روی آن‌ها نصب و راه‌اندازی شده است و جز در مواردی خاص، به هیچ‌عنوان نیازمندی برای نصب ابزارها به‌منظور تحلیل بدافزارها وجود ندارد.

این کتاب تلاش دارد با بهره‌گیری از ابزارها و توزیع‌های موجود در زمینه تحلیل رفتاری بدافزارها، متخصصان امنیت و یا دانشجویان علم امنیت را با ابزارهای موجود در این حوزه و همچنین چگونگی پیاده‌سازی آزمایشگاه‌های شناسایی بدافزار آشنا سازد، زیرا هم‌اینک مقوله بدافزارها، تغییر مسیر و شیب تندی پیدا کرده است و به‌صورت تدریجی و هوشمند به سمتی هدایت می‌شود که وجود چنین آزمایشگاه‌هایی در هر سازمان و یا مجموعه‌ای که به هر نحوی با کامپیوتر و اینترنت سر و کار دارند، ضروری می‌باشد تا پیش از بُروز رخداد و اختلال در عملکرد شبکه توسط بدافزارها و ایجاد هزینه‌های گزاف برای سازمان مربوطه، متخصصان امنیت سازمان بتوانند پیش از به‌روزرسانی‌ها توسط شرکت‌های تولیدکننده ضدویروس، رفتارهای مشکوک در سطح شبکه خود را شناسایی کنند و در جهت محدودسازی، قرنطینه و پاکسازی موارد مشکوک، گام بر دارند.

شیرازه اصلی این کتاب برگرفته از کتاب‌ها و منابع معتبر و استاندارد شاخه تجزیه و تحلیل رفتاری بدافزارها، اصول پیاده‌سازی آزمایشگاه تحلیل بدافزار، علم شناسایی نرم‌افزارهای مُخرب، ابزارها و توزیع‌های استاندارد پیاده‌سازی آزمایشگاه‌های تحلیل می‌باشد که البته با تجربیات ناچیز اینجانب در این‌باره آمیخته شده است، که به‌فرم کاملا آزاد از مطالب و تجربیات گردآوری و دخل و تصرفی نیز با آن همراه بوده است. اینجانب به‌عنوان عضو کوچکی از خانواده بزرگ امنیت درصدد گردآوری و تألیف کتابی آموزشی برپایه تحلیل بدافزارها به‌منظور افزایش کارایی عملی متخصصان، دانشجویان و مدیران شبکه در این زمینه بودم تا آن‌ها را با اصول فنی، چگونگی پیاده‌سازی یک آزمایشگاه تجزیه و تحلیل بدافزار در محل کار خود آشنا و آگاه سازم (گرچه مدیران و متخصصان امنیت شبکه حُکم اساتید اینجانب را دارند، اما به حُکم وظیفه برخود لازم دانستم که این آگاه‌سازی را انجام دهم). پیشاپیش همه‌ی کاستی‌های آن را می‌پذیرم و ضمن پوزش از اساتید، متخصصان، دانشجویان و مدیران عزیز، انتقادات و راهنمایی‌های دلسوزانه آن‌ها را به دیده منّت پذیرا هستم.

(m_Davari@TOP-co.ir) (m_Davary@Parshack.zzn.com)

پس از سپاس و ستایش به درگاه پروردگار از همه‌ی دوستان و اساتید عزیزی که مهربانانه دست مرا در انجام اینکار ناچیز فشردند، تشکر می‌کنم. برخود لازم می‌دانم از زحمات بی‌دریغ سرکار خانم مهندس سیده پونه مرتضویان تشکر و قدردانی نمایم. زحمات خاضعانهٔ ایشان سهم بزرگی در تهیه و تدوین این کتاب داشته است. در پایان از مدیریت فرزانه انتشارات پندار پارس جناب آقای مهندس یعسوبی و همه‌ی همکارانشان که زحمت چاپ کتاب را متقبل شده‌اند، صمیمانه قدردانی می‌نمایم.

یارب غم آنچه غیر تو در دل ماست بردار که بی‌حاصلی از حاصل ماست
الحمد که چون تو راهنمایی داریم کز گمشدگانیم که غم، منزل ماست

(مجید داوری دولت آبادی – بهار ۱۳۹۵)

فصل نخست

آغاز کار با ابزار تحلیل‌بدافزار Cuckoo Sandbox

تجزیه و تحلیل نرم‌افزارهای مُخرب، فرآیند شناسایی رفتار مُخرب بدافزارها است که از طریق آن می‌توان درک کرد که یک بدافزار ویژه چه کاری انجام می‌دهد، چه رفتاری دارد، چه اهدافی را دنبال می‌کند و در پایان چگونگی خنثی سازی آن چگونه است. تحلیل بدافزار شامل یک فرآیند پیچیده و فعال است. پزشکی قانونی، مهندسی معکوس، جداسازی قطعات و داده‌ها، اِشکال‌زدایی، فعالیت‌هایی هستند که به‌منظور تحلیل بدافزارها، بر روی آن‌ها انجام می‌شود. هدف از تجزیه و تحلیل نرم‌افزارهای مُخرب به‌دست آوردن درک درستی از چگونگی کار بدافزارها و طریقه مقابله با آن‌ها است. شناسایی رفتار بدافزارها در جلوگیری از وقوع حملات مُخرب برعلیه شبکه‌ها و سیستم‌ها مؤثر است.

روش‌های تجزیه و تحلیل بدافزار

در حالت کلی دو روش معمول در روند تحلیل بدافزارها وجود دارد که به‌طور معمول توسط تحلیلگران بدافزار مورد استفاده قرار می‌گیرند. این دو روش شامل موارد زیر می‌باشند:

- تجزیه و تحلیل استاتیک (تجزیه و تحلیل کد)
- تجزیه و تحلیل پویا (تجزیه و تحلیل رفتار)

این دو تکنیک به تحلیلگران اجازه می‌دهد تا به سرعت به درک کامل و دقیقی از جزییات، خطرات و مقاصد نرم‌افزارهای مُخرب دست یابند. برای انجام عملیات تجزیه و تحلیل استاتیک، کارشناسان، نیازمند درک قوی در مقوله زبان برنامه‌نویسی و مفهوم اسمبلی x86 می‌باشند. در ساختار تجزیه و تحلیل استاتیک به هیچ عنوان نباید بدافزار اجرا شود. در این حالت از کد منبع نمونه‌هایی از بدافزارها

استفاده می‌شود و تحلیل صورت می‌گیرد. به‌منظور جداسازی قطعات کدها و تحلیل آن‌ها برای انجام عملیات مهندسی معکوس موفقیت‌آمیز باید از کد سطح پایین اسمبلی استفاده کرد.

بسیاری از تحلیلگران بدافزارها در مراحل آغازین انجام مکانیزم تجزیه و تحلیل از مکانیزم تحلیل استاتیک در روند کاری خود استفاده می‌کنند، زیرا این روش نسبت به روش پویا امن‌تر می‌باشد. از چالش‌های بزرگ در روش تجزیه و تحلیل استاتیک، پیچیدگی کار با آن در مورد بدافزارهای مدرن است، زیرا در بیشتر موارد بدافزارهای جدید از مکانیزم‌های ضد اِشکال‌زدایی برای جلوگیری از تحلیل قطعه کدها استفاده می‌کنند. تحلیل پویا (تجزیه و تحلیل رفتار)، یک فرآیند تحلیل بدافزار است که در روال کاری آن، بدافزار و نرم‌افزار مُخرب در فضایی مشخص اجرا می‌گردد تا فعالیت و رفتار آن دیده شود. همچنین تغییرات زمانی بدافزار گفته شده در روش اشاره شده هنگام اجرا، دیده می‌شود.

سیستمی که به یک بدافزار جدید آلوده شده باشد، در بستر شبکه بسیار خطرناک خواهد بود، زیرا رفتار آن به‌درستی برای تحلیلگران و نرم‌افزارهای ضد ویروس مشخص نمی‌باشد. حذف فایل‌ها، تغییر متغیرهای رجیستری، تغییر ساختار و محتوای فایل‌ها، سرقت اطلاعات محرمانه و غیره می‌تواند بخشی از رفتار و عملکرد بدافزار مورد نظر باشد. هنگام انجام عملیات تجزیه و تحلیل نرم‌افزارهای مُخرب، نیازمند یک محیط امن در شبکه برای آزمایش بدافزارها می‌باشیم. در مکانیزم تجزیه و تحلیل پویا، آزمایش‌کننده می‌تواند بر روی تغییرات ایجاد شده در سیستم فایل، رجیستری، سرویس‌ها و فرآیندها و شبکه‌های ارتباطی کنترل و نظارت کامل داشته باشد. در حقیقت در این روش می‌توان به درک حقیقی از چگونگی عملکرد و رفتار بدافزار رسید. تحلیلگرهای خودکار بدافزار می‌توانند در بررسی و تحلیل شمار زیادی از بدافزارهای مختلف از جنبه‌های گوناگون کمک به‌سزایی نمایند. تحلیلگرهای خودکار نسبت به روش‌های دستی که توسط کاربر انجام می‌شود، از دقت بالاتری برخوردار می‌باشند. هنگام استفاده از ابزار Cuckoo به‌عنوان یک نرم‌افزار ویژه‌ی تحلیل بدافزار خودکار، در حالت معمول، زمان تجزیه و تحلیل بدافزارها کاهش پیدا می‌کند. البته گفتنی است که برخی مراحل در تحلیل پویای بدافزارها نیازمند زمان زیادی می‌باشند. عملیات تجزیه و تحلیل بدافزار به نظر آسان می‌باشد، اما اگر اقدام به تجزیه و تحلیل چندین بدافزار نماییم، بسیار زمان‌بر خواهد بود.

نظریه اساسی در ساختار Sandbox

ساختارهای Sandbox، تکنولوژی است که با کمک آن‌ها می‌توان، عملیات تجزیه و تحلیل بدافزارها را بدون به خطر افتادن سیستم‌ها انجام داد. این تکنولوژی در میان متخصصان امنیت و

آزمایش‌کنندگان بدافزارها بسیار رایج و معروف می‌باشند. برای کسب اطلاعات بیشتر درباره Sandboxها می‌توان به آدرس URL زیر مراجعه کرد:

http://en.wikipedia.org/wiki/Sandbox_(computer_security)

در حقیقت می‌توان گفت مکانیزم Sandboxing به‌منظور بررسی و اجرای برنامه‌های غیرقابل اعتماد در محیطی مشخص مورد استفاده قرار می‌گیرد. یک مثال عملی در مورد تکنولوژی Sandbox، فضای در نظر گرفته شده برای بازی بچه‌ها در یک مکان تفریحی است که دارای شن و ماسه می‌باشد و بچه‌ها تنها در آن مکان می‌توانند به بازی بپردازند و فضاهای بیرونی مکان تفریحی گفته شده به‌طور کامل پاک و تمیز می‌باشد. مکان در نظر گرفته شده برای بازی بچه‌ها، همانند همان فضایی است که به‌صورت ایزوله در اختیار آزمایش کننده بدافزار قرار می‌گیرد و وی می‌تواند با آسودگی خاطر اقدام به بررسی، پویش و تحلیل بدافزارها نماید. در ابزارهایی مانند Cuckoo که از ساختار Sandbox استفاده می‌کنند، می‌توان چندین قالب Sandbox به‌منظور تجزیه و تحلیل‌های گوناگون پیاده‌سازی و استفاده کرد. این ابزار کدباز است و پشتیبانی مناسبی از آن به عمل می‌آید.

آزمایشگاه تحلیل بدافزار

اکنون باید ببینیم آزمایشگاه تحلیل بدافزار چیست و چرا باید یک آزمایشگاه تحلیل بدافزار در سازمان خود ایجاد کرد. همان‌طور که گفته شد، آزمایشگاه تحلیل بدافزار، محیطی امن برای تجزیه و تحلیل انواع نرم‌افزارهای مُخرب می‌باشد. در حقیقت این آزمایشگاه، یک محیط ایزوله شده و امن می‌باشد که با دارا بودن بسیاری از ابزارهای مفید برای تحلیلگران نرم‌افزارهای مُخرب، کمک می‌کنند تا تجزیه و تحلیل نرم‌افزارهای مُخرب به سادگی و با اطمینان کامل انجام شوند. وجود یک آزمایشگاه بدافزار برای هر سازمان و شرکتی جزو ملزومات امنیتی و حفاظتی آن شرکت و سازمان می‌باشد و می‌توان برای ورود امن فایل‌ها به داخل شرکت و یا سازمان از آن استفاده کرد. در مدل‌های تشخیص پیشرفته، پیش از استفاده از یک ضدویروس مشخص برای پویش فایل مشکوک، از روش تحلیل بدافزار در آزمایشگاه استفاده می‌شود. حوزه آزمایشگاه تحلیل بدافزار با بررسی فرآیندها در روند تحلیل بدافزار آغاز می‌شود.

تجزیه و تحلیل ایستا شامل جداسازی قطعه‌های کد و مهندسی معکوس کدهای بدافزار می‌باشد. در این حالت نیازی به ایجاد تنظیمات پیچیده برای محیط آزمایشگاه نیست و باید نرم‌افزار مُخرب را اجرا کرد و رفتار آن‌را مشاهده نمود. در حالت گفته شده آزمایشگاه تنها برای حفاظت از اجرای تصادفی کدهای باینری و اجرایی بدافزارها هنگام انجام عملیات تجزیه و تحلیل ایجاد می‌شود. در حالت پویا، نیازمند راه‌اندازی یک آزمایشگاه پیچیده‌تر می‌باشیم. نرم‌افزارهای مُخرب بسته به نوع سیستم عامل رفتارهای گوناگونی در هنگام اجرا از خود نشان می‌دهند. راه‌اندازی یک آزمایشگاه

تحلیل بدافزار بسیار ساده است و نیازمند کم‌ترین‌ها از دیدگاه سخت‌افزاری می‌باشد. جداسازی این آزمایشگاه از شبکه شرکت و یا سازمان کافی نیست و حتی باید این محیط از فضای اینترنت نیز جدا باشد، زیرا داده‌ها و بسته‌های در حال تبادل در سطح شبکه اینترنت ممکن است در روند تحلیل یک بدافزار ویژه اختلال ایجاد نماید و موجب به دست آمدن خروجی‌های گوناگونی شود. این نکته بسیار مهم است، زیرا گاهی نرم‌افزارهای مُخرب نیازمند برقرار ارتباط با سرور نویسنده بدافزار می‌باشند، مانند Botnetها که باید با سرور فرماندهی و کنترل در تماس باشند.

دو گزینه در ایجاد یک آزمایشگاه تجزیه و تحلیل بدافزار وجود دارد که شامل محیط فیزیکی و محیط مجازی می‌باشند. این دو محیط باید در این نوع آزمایشگاه در نظر گرفته شود. همان‌طور که پیش‌تر گفتیم، هر دو روش مزایا و معایب خود را دارند. پیاده‌سازی یک آزمایشگاه از نوع فیزیکی نیازمند زمان و هزینه برای سازمان و یا شرکت خواهد بود، در این حالت پیشنهاد می‌شود از ساختارهای مجازی برای ایجاد یک آزمایشگاه تحلیل بدافزار استفاده شود تا در زمان و هزینه صرفه‌جویی شود. در حالت مجازی می‌توان در هر مرحله‌ای از تحلیل، عملیات انجام شده را در وضعیت موجود ذخیره کرد. در این حالت با استفاده از این ویژگی، می‌توان یک محیط مجازی که شامل یک سیستم عامل با یک مجموعه کامل از ابزارهای ویژه‌ی تجزیه و تحلیل ایستا و پویا در اختیار داشت و در هر مرحله اقدام به ذخیره‌سازی اقدامات انجام شده کرد.

پس از پایان عملیات تجزیه و تحلیل بدافزار، می‌توان ذخیره‌سازی را در موقعیت‌های گوناگون انجام داد تا بتوان به مراحل پیش و پس از تحلیل مراجعه کرد. با استفاده از این ویژگی می‌توان نرم‌افزارهای مُخربی که بر روی سیستم عامل موقتی و مجازی نصب شده است را بررسی کرد و به راحتی به حالت پیش از نصب بدافزار منتقل شد. در این ساختار از مکانیزم مجازی‌سازی با ساختار ESX استفاده می‌شود و براساس آن می‌توان هر نوع سیستم عاملی به‌عنوان قالب کار و برای پیاده‌سازی آزمایشگاه نصب از آن استفاده کرد. استفاده از فناوری مجازی‌سازی در پیاده‌سازی آزمایشگاه تحلیل بدافزار، بسیار مفید است و کمک به‌سزایی در انجام آزمایشات تحلیلگر می‌کند و از نظر منابع و هزینه‌های سخت‌افزاری، صرفه‌جویی قابل توجهی را شامل می‌شود. می‌توان یک سیستم عامل را بر روی ساختار مجازی نصب کرد و همه‌ی بدافزارها و نرم‌افزارهای مخُرب را به‌منظور یافتن و شناسایی رفتارهای مشکوک و خطرناک آن‌ها بر روی آن سیستم عامل اجرا کرد تا در فضایی امن به تجزیه و تحلیل بدافزار پرداخت و بر روی فعالیت آن‌ها نظارت کامل داشت.

اِشکالاتی در پیاده‌سازی و اجرای خودکار عملیات تحلیل بدافزار وجود دارد که می‌تواند به‌راحتی توسط نویسندگان نرم‌افزارهای مُخرب تشخیص داده شوند و بیشتر با استفاده از تکنیک‌های فرار مانند مکانیزم‌های ضداِشکال‌زدایی، بسته‌بندی و ایزوله‌سازی کدها، رمزگذاری، مخفی‌سازی کدها و غیره از این اِشکالات سوء استفاده می‌شود. البته می‌توان با کمک تکنیک‌های مجازی‌سازی اِشکالات

موجود را پنهان نمود. هم‌اینک اطلاعات گوناگونی در فضای اینترنت در مورد روش‌ها و تکنیک‌های تشخیص و مقابله با تجزیه و تحلیل بدافزارها درقالب مجازی‌سازی ارائه شده است.

ابزار Cuckoo Sandbox

این ابزار به‌عنوان یک Sandbox مطرح در زمینه تجزیه و تحلیل پویای بدافزارها و انواع نرم‌افزارهای مُخرب شناخته می‌شود. در حقیقت، این ابزار به‌جای استفاده از مکانیزم تجزیه و تحلیل آماری، فایل اجرایی بدافزار را اجرا کرده و در شرایط حقیقی اقدام به نظارت و تحلیل آن بدافزار می‌کند. به‌عنوان یک توضیح ساده می‌توان گفت، ابزار Cuckoo یک سیستم تجزیه و تحلیل بدافزار به‌صورت خودکار و کدباز است که بر اساس مکانیزم و ساختار Sandbox عملیات تجزیه و تحلیل نرم‌افزارهای مُخرب را در شرایط حقیقی انجام می‌دهد. نسخه جدید این ابزار دارای یک واسط کاربری تحت وب مبتنی بر چارچوب جنگو (چارچوب طراحی وب مبتنی بر Python) و پایگاه‌داده MongoDB است. این ابزار همانند سایت وب تحلیل بدافزار Malwr.com عمل می‌کند و می‌توان همه‌ی فایل‌های مشکوک را به‌منظور تحلیل به‌عنوان ورودی به ابزار داد و اطلاعات و جزئیاتی کامل در مورد اجرا و موارد تخریب آن فایل را دریافت نمود. این ابزار برای تجزیه و تحلیل انواع فایل‌ها با ساختارهای زیر طراحی شده است:

- فایل‌های اجرایی سیستم عامل ویندوز
- فایل‌های نوع DLL
- اسناد و فایل‌هایی از جنس PDF
- اسناد مربوط به برنامه کاربردی MS Office
- آدرس‌های URL مشکوک
- اسکریپت‌های PHP و به‌طور تقریبی هر فایل دیگری

همچنین از این ابزار می‌توان داده‌های مفید بسیاری را دریافت نمود که از آن جمله می‌توان به موارد زیر اشاره کرد:

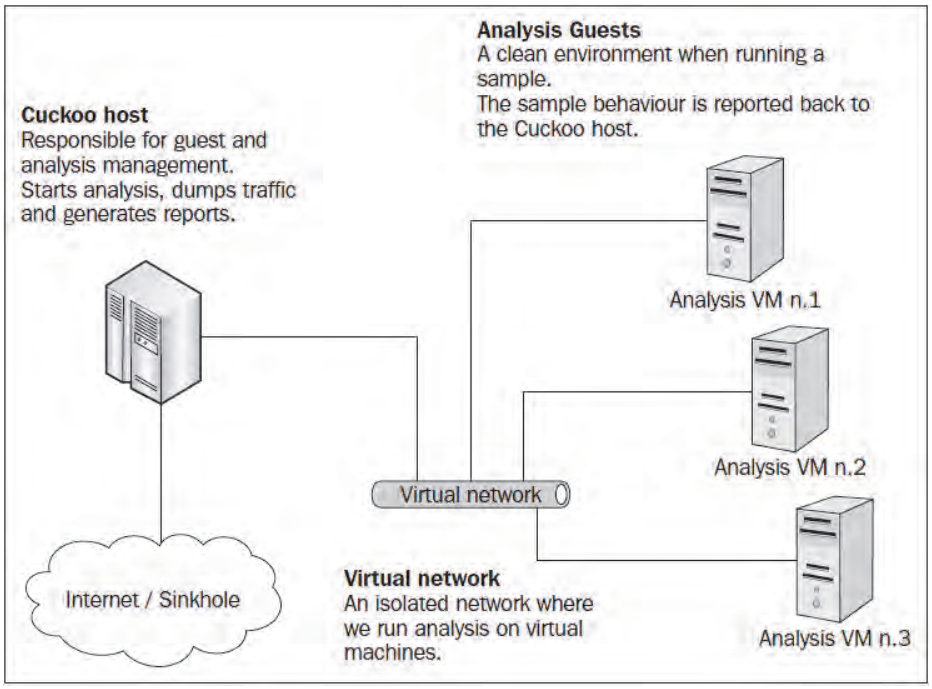
- توابع و APIهای سیستم عامل ویندوز که به هر نحوی توسط بدافزار مورد نظر در فرآیندهای گوناگون فراخوانی شده است.
- تهیه گزارشی در مورد فایل‌هایی که توسط بدافزار در سیستم‌فایل ایجاد، حذف یا اجرا شده‌اند.
- نمونه‌برداری از بخشی از حافظه که مربوط به فرآیندهای انتخابی توسط بدافزار می‌باشد.

- ردیابی ترافیک شبکه سیستمی که عملیات تحلیل بدافزار بر روی آن با فرمت PCAP در حال انجام است.
- نمونه‌برداری کامل از حافظه سیستمی که در حال بررسی و تحلیل است.
- ایجاد تصاویری از صفحه کاری یا Desktop کاربر، در زمانی‌که ابزار تحلیل بدافزار در حال اجرا است.

این ابزار قادر است خروجی‌های مفید خود را به‌صورت گزارش در قالب‌های گوناگونی مانند MongoDB ، HTML، JSON HPFeeds و MAEC ایجاد و ارائه کند. ابزار Cuckoo Sandbox، مبتنی بر یک طراحی رویه‌ای است و کاربر می‌تواند مراحل گزارش‌گیری و فرآیند اصلی تحلیل را شخصی‌سازی کند. این ابزار از طریق سایت اصلی آن به آدرس URL زیر قابل دسترس می‌باشد:

http://www.cuckoosandbox.org

ابزار Cuckoo Sandbox متشکل از یک نرم‌افزار مدیریت مرکزی است که نمونه‌های اجرایی را برای تجزیه و تحلیل دریافت و اجرا می‌کند. هر تجزیه و تحلیلی در یک ماشین مجازی جدید و ایزوله راه‌اندازی و اجرا می‌شود. در حالت کلی زیرساخت این ابزار از یک ماشین میزبان (نرم‌افزار مدیریت) و تعدادی ماشین مهمان (ماشین‌های مجازی برای تجزیه و تحلیل) تشکیل شده است. ماشین میزبان جزء اصلی ابزار محسوب می‌شود که کار مدیریت کل فرآیندها را برای تجزیه و تحلیل برعهده دارد. ماشین‌های مهمان نیز شامل محیط‌های ایزوله‌ای هستند که در قالب آن‌ها با خیالی آسوده عملیات تجزیه و تحلیل نرم‌افزاهای مُخرب انجام می‌شود. شکل (۱-۱) شمایی کلی از معماری این ابزار را نشان می‌دهد.



شکل (۱-۱) شمایی کلی از معماری ابزار Cuckoo Sandbox

نصب و راه‌اندازی ابزار Cuckoo Sandbox

اکنون در آغاز این مرحله باید اجزای مهم در هنگام نصب ابزار Cuckoo Sandbox را مورد بررسی قرار دهیم.

نیازمندی‌های سخت‌افزاری

کمترین نیازمندی‌های سخت‌افزاری برای راه‌اندازی ابزار Cuckoo Sandbox بر روی ماشین مجازی شامل موارد زیر می‌باشند:

- دست‌کم ۲ گیگابایت فضای حافظه RAM
- مقدار ۴۰ گیگابایت فضای دیسک‌سخت که بر روی سیستم مجازی ایجاد می‌شود.

گفتنی است در این کتاب مبنای نیازمندی‌های سخت‌افزاری به فرم زیر در نظر گرفته شده است.
نیازمندی برای Host OS:

- Quad Core CPU
- 4 GB RAM
- 320 GB HDD

آماده‌سازی Host OS

از لحاظ تئوری و کلی، این ابزار می‌تواند بر روی هر سیستم عامل لینوکسی نصب و اجرا شود، اما در این کتاب مبنای همه‌ی دستورات در سیستم عامل میزبان بر اساس لینوکس Ubuntu 12.04 می‌باشد. پیش از ادامه دادن به فرآیند نصب و پیکربندی ابزار Cuckoo Sandbox، باید برخی برنامه‌ها و کتابخانه‌های پیش‌نیاز بر روی سیستم میزبان نصب و راه‌اندازی شود.

نصب و راه‌اندازی Python در Ubuntu

برای نصب Python نیازمند وارد کردن دستور زیر در محیط پوسته فرمان لینوکس Ubuntu می‌باشیم:

```
$ sudo apt-get install python
```

همچنین ابزار Cuckoo نیازمند نصب برنامه کاربردی SqlAlchemy به‌عنوان ابزار پایگاه‌داده برای Python است. بنابراین نیاز دارید تا این ابزار را با کمک دستور زیر در محیط پوسته فرمان لینوکس Ubuntu نصب کنید:

```
$ sudo apt-get install python-sqlalchemy
```

همچنین می‌توانید با کمک دستور pip اقدام به نصب ابزار SqlAlchemy نمایید. Pip ابزاری است که برای نصب و مدیریت بسته‌های نرم‌افزاری Python مورد استفاده قرار می‌گیرد:

```
$ sudo pip install sqlalchemy
```

بسته‌های وابسته دیگر به‌طور تقریبی اختیاری می‌باشند که بیشتر توسط ماژول‌ها و ابزارهای دیگر استفاده می‌شوند. فایل‌های کتابخانه‌ای زیر چندان مورد نیاز نمی‌باشد، اما باید برای تضمین اجرای ابزار Cuckoo Sandbox در محیط خود اجرا شوند:

- dpkt: این کتابخانه برای استخراج اطلاعات موجود در فایل‌های از جنس PCAP توصیه می‌شود.
- jinja2: این کتابخانه برای ارائه گزارش‌های HTML و واسط وب مورد استفاده قرار می‌گیرد.

- magic: این کتابخانه اختیاری است و برای شناسایی فرمت‌های فایل استفاده شده به‌کار می‌رود (وگرنه استفاده از ابزارهای ویژه‌ی فایل خط فرمان پیشنهاد می‌شود).
- ssdeep: این کتابخانه نیز اختیاری می‌باشد و برای محاسبه Hash یا فایل‌های فازی استفاده می‌شود.
- pydeep: این کتابخانه نیز اختیاری است و برای محاسبه فایل Hash فازی ssdeep مورد استفاده قرار می‌گیرد.
- pymongo: این کتابخانه نیز اختیاری است و برای ذخیره‌سازی نتایج در یک پایگاه‌داده MongoDB استفاده می‌شود.
- yara and yara python: این کتابخانه اختیاری است و برای تطبیق امضاهای Yara (استفاده از نسخه svn) مورد استفاده قرار می‌گیرد.
- libvirt: این کتابخانه نیز اختیاری است و از آن برای مدیریت دستگاه‌های KVM استفاده می‌شود.
- bottlepy: این کتابخانه اختیاری است و از آن در ابزارهای web.py و api.py استفاده می‌شود.
- pefile: این کتابخانه نیز اختیاری است و برای تجزیه و تحلیل ایستا از نوع باینری PE32 استفاده می‌شود.

همه‌ی بسته‌هایی که باید برای ابزار Cuckoo Sandbox بر روی سیستم نصب شوند را می‌توان در یک خط وارد کرد و اقدام به نصب آن‌ها نمود:

```
$ sudo apt-get install python-dpkt python-jinja2 python-magic python-pymongo python-libvirt python-bottle python-pefile ssdeep
```

همچنین می‌توانید همه‌ی بسته‌ها را با کمک ابزار مدیریتی pip به‌صورت زیر بر روی سیستم نصب نمایید (به‌جز python-magic و python-libvirt):

```
$ sudo pip install dpkt jinja2 pymongo bottle pefile
```

pydeep را برای Hash فازی ssdeep نصب می‌کنید، اما پیش از نصب Pydeep، نیازمند نصب بسته‌های وابسته آن می‌باشید. این بسته‌ها که شامل موارد زیر می‌باشند، از طریق محیط پوسته فرمان لینوکس قابل نصب می‌باشند:

```
Build-essential, Git, Libpcre3, Libpcre3-dev, Libpcre++-dev
```

نمونه‌ای از چگونگی نصب این بسته‌ها در قالب لینوکس Ubuntu به فرم زیر می‌باشند:

```
$ sudo apt-get install build-essential git libpcre3 libpcre3-dev libpcre++-dev
```

در ادامه، مراحل زیر را دنبال می‌کنیم (pydeep در دایرکتوری opt/ قرار می‌گیرد):

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

همچنین نیاز دارید yara را در طبقه‌بندی بدافزار نمونه نصب کنید (yara در دایرکتوری opt/ قرار می‌گیرد):

```
$ sudo apt-get install automake –y
$ cd /opt
$ svn checkout http://yara-project.googlecode.com/svn/trunk/yara
$ cd /opt/yara
$ sudo ln -s /usr/bin/aclocal-1.11 /usr/bin/aclocal-1.12
$ ./configure
$ make
$ sudo make install
$ cd yara-python
$ python setup.py build
$ sudo python setup.py install
```

همچنین نیاز دارید ابزار tcpdump را برای گردآوری ترافیک شبکه و تحلیل بر روی لینوکس نصب نمایید:

```
$ sudo apt-get install tcpdump
```

اگر قصد دارید ابزار tcpdump را اجرا کنید، نیازمند داشتن دسترسی root می‌باشید، اما شاید نخواهید ابزار Cuckoo را با دسترسی root یا مدیر سیستم اجرا کنید. باید به مجموعه‌ای از قابلیت‌های لینوکس ویژه‌ای که استفاده می‌کنید، برای اجرای فایل‌های اجرایی آشنایی کامل داشته باشید. دستورات زیر عملیات اجرا را در محیط پوسته فرمان نشان می‌دهد:

```
$ sudo setcap cap_net_raw,cap_net_admin=eip /usr/sbin/tcpdump
```

می‌توانید نتایج به‌دست آمده از آخرین فرمان را با بررسی کامل دریافت کنید:

```
$ getcap /usr/sbin/tcpdump /usr/sbin/tcpdump = cap_net_admin,cap_net_raw+eip
```

اگر ابزار setcap را بر روی لینوکس نصب کرده‌اید، می‌توانید کتابخانه آن‌را به فرم زیر بر روی لینوکس Ubuntu نصب نمایید:

```
$ sudo apt-get install libcap2-bin
```

وگرنه (توصیه نمی‌شود) فرمان زیر را اجرا نمایید:

```
$ sudo chmod +s /usr/sbin/tcpdump
```

همان‌طور که می‌دانید chmod +s به معنی بیت SUID می‌باشد. در ادامه باید مجوز شناسه کاربر (user ID) و شناسه گروه (group ID) را برای یک فایل اضافه کنید. در این مورد منظور tcpdump می‌باشد. چنانچه بیت SUID (s) بر روی tcpdump تنظیم شود، در ادامه کاربران می‌توانند ابزار tcpdump را اجرا کنند و دسترسی مدیر سیستم را به‌دست آورند، به همین دلیل این مرحله توصیه نمی‌شود. پس از پایان راه‌اندازی سیستم عامل میزبان (Host OS)، نیازمند نصب و پیکربندی ابزار تحلیل Cuckoo Sandbox بر روی سیستم عامل میزبان می‌باشیم.

پیکربندی و تنظیم ابزار Cuckoo Sandbox بر روی Host OS

در این بخش قصد داریم چگونگی پیکربندی و تنظیم ابزار Cuckoo Sandbox را بیان کنیم. برای انجام این‌کار باید مراحل زیر را دنبال نمایید:

۱. در آغاز باید ابزار Cuckoo Sandbox را از طریق آدرس URL زیر دریافت کرد:

```
http://www.cuckoosandbox.org/download.html
```

دو روش برای تنظیم و پیکربندی Cuckoo بر روی Host OS وجود دارد. می‌توان نسخه کد منبع این ابزار (Tarball) را دریافت و بر روی سیستم نصب کرد یا با مکانیزم git clone این‌کار را انجام داد.

۲. اگر از مکانیزم git به فرم زیر استفاده شود:

```
$ git clone git://github.com/cuckoobox/cuckoo.git
```

۳. چنانچه بخواهیم از کد منبع با فرمت Tarball برای نصب استفاده شود. برای این‌کار می‌توانید در وب سایت ابزار Cuckoo Sandbox (www.cuckoosandbox.org) بر روی دکمه Download کلیک نمایید.

۴. پس از پایان دریافت فایل با کمک دستور زیر اقدام به استخراج فایل‌های داخل آن در یک دایرکتوری می‌کنیم:

```
$ tar –zxvf cuckoo-current.tar.gz
```

۵. پیش از پیکربندی ابزار Cuckoo بر روی Host OS، نیازمند نصب و راه‌اندازی Guest OS می‌باشیم. در این کتاب برای نصب Guest OS از ابزار VirtualBox استفاده می‌کنیم. برای دریافت این ابزار می‌توانید از آدرس URL زیر استفاده کنید:

https://www.virtualbox.org/wiki/Downloads

در این کتاب از ابزار VirtualBox نسخه 4.2.12 برای میزبان لینوکس استفاده شده است. اگر نسخه 4.2.12 یافت نشد، می‌توانید از نسخه‌های جدیدتر استفاده کنید، اما اگر تمایل به نصب و راه‌اندازی نسخه 4.2.12 داشتید، می‌توانید از آدرس URL زیر برای این منظور استفاده نمایید:

https://www.virtualbox.org/wiki/Download_Old_Builds_4_2

اکنون چندین نسخه از ابزار VirtualBox برای سیستم‌های عامل لینوکس موجود می‌باشند، که می‌توان از آن‌ها برای نصب استفاده کرد. پیش از نصب و پیکربندی Guest OS در ابزار VirtualBox، نیازمند بررسی و نصب درایورهای Vbox هستیم. همچنین نیازمند نصب و پیکربندی vboxdrv پیش از ایجاد Guest OS می‌باشید. برای نصب vboxdrv، نیازمند نصب سرآیند هسته در لینوکس هستیم. سرآیندهای هسته نیازمند کامپایل کردن vboxdrv می‌باشد. اگر بخواهید از نسخه هسته سیستم عامل لینوکس خود اطمینان حاصل کنید، می‌توانید از دستور زیر استفاده کنید:

```
$ uname -a
```

برای نمونه، خروجی دستور اشاره شده به فرم زیر می‌باشد:

```
Linux digit-labs 3.5.0.17-generic #28-ubuntu SMP Tue Oct 9 19:31:23 UTC 2012 x86_64x86_64
x86_64 x86_64 GNU/Linux
```

در این نمونه از نسخه هسته 3.5.0.17 استفاده شده است و نیازمند نصب سرآیند هسته با کمک دستور زیر می‌باشیم:

```
$ apt-get install linux-headers-3.5.0.17-generic
```

پس از پایان نصب سرآیند هسته، می‌توان تنظیمات مربوط به vboxdrv را با کمک دستورات زیر انجام داد:

```
$ sudo /etc/init.d/vboxdrv setup
* Stopping VirtualBox kernel modules [OK]
* Recompiling VirtualBox kernel modules [OK]
* Starting VirtualBox kernel modules [OK]
```

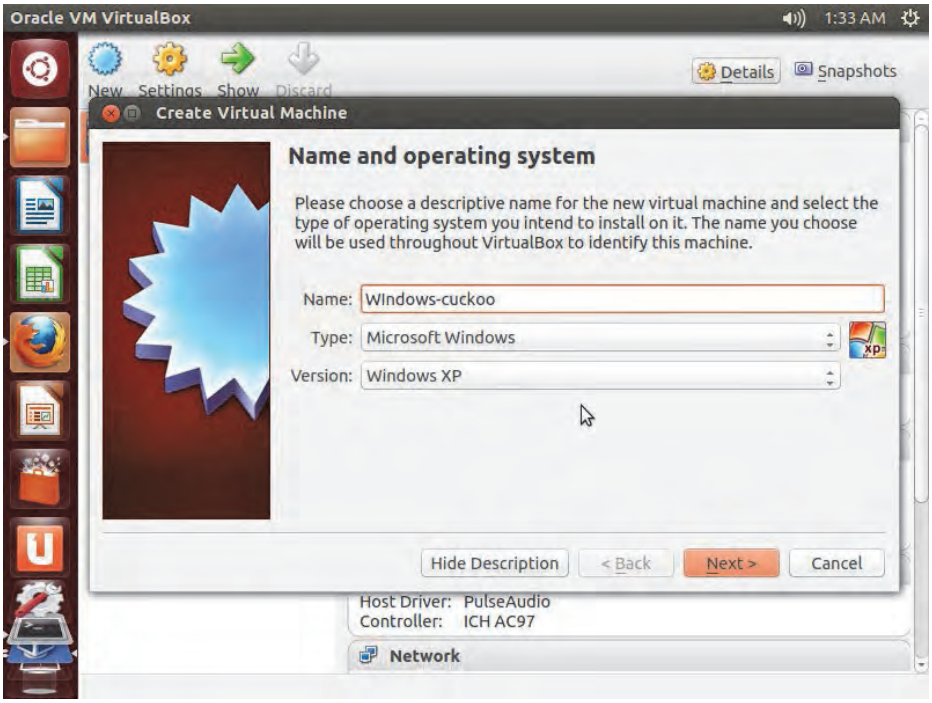
اگر همه‌ی خروجی‌ها OK باشند، می‌توان عملیات نصب و پیکربندی Guest OS را انجام داد.

آماده‌سازی Guest OS

سیستم Guest OS نیازمند ویژگی‌های سخت‌افزاری زیر برای راه‌اندازی است:

- 1GB فضای مورد نیاز برای حافظه RAM
- 10GB فضا مورد نیاز دیسک‌سخت
- فرمت VDI برای دیسک مجازی
- اختصاص پویای فضای ذخیره‌سازی
- سیستم عامل ویندوز XP SP3

زمانی‌که Guest OS را نصب می‌کنید، نام Guest OS را برای فایل پیکربندی مربوط به Cuckoo Sandbox VirtualBox ایجاد می‌نمایید. در مرحله نخست، باید یک Guest OS ایجاد شود. نمونه‌ای از مراحل آغازین برای تنظیم نصب Guest OS درقالب ابزار VirtualBox در شکل (۲-۱) نشان داده شده است.



شکل (۲-۱) شمایی از مراحل آغازین جهت تنظیم برای نصب Guest OS درقالب ابزار VirtualBox

پیش از شروع به کار با Guest OS در فضای ابزار VirtualBox، نیازمند پیکربندی شبکه و به اشتراک‌گذاری دایرکتوری میان Host OS و Guest OS و همچنین بهبود قابلیت‌ها در روند تجزیه و تحلیل نرم‌افزارهای مُخرب می‌باشیم.

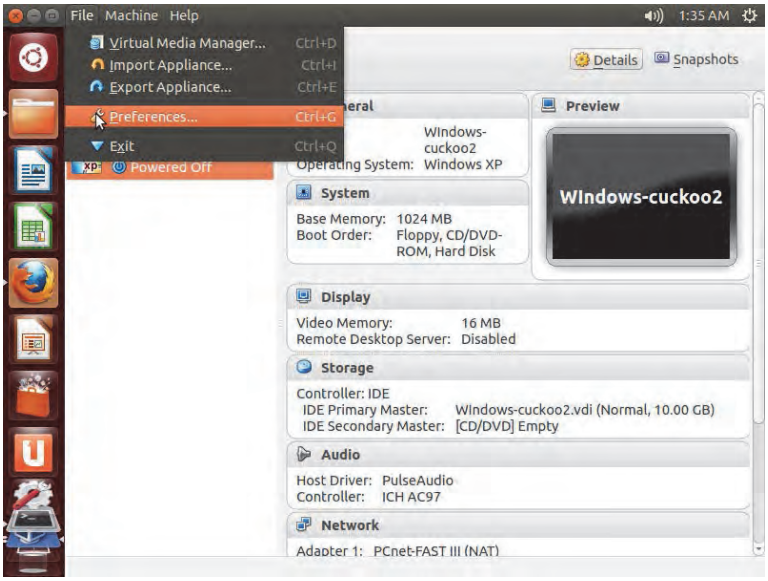
پیکربندی شبکه

ابزار VirtualBox دارای انواع گوناگونی از تنظیمات شبکه است که می‌توان از آن‌ها در سیستم عامل Guest استفاده کرد. هر نوع دارای قابلیت‌های گوناگون براساس نیاز کاربر می‌باشد. برای کسب اطلاعات بیشتر در این باره می‌توانید از آدرس URL زیر استفاده کنید:

www.virtualbox.org/manual/ch06.html

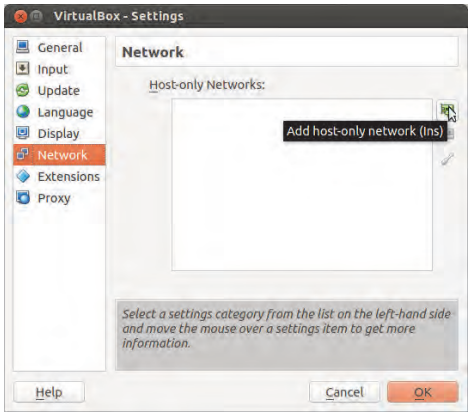
به‌طور استاندارد باید مکانیزم Host-only برای نوع پیکربندی شبکه در ماشین مجازی در نظر گرفته شود، زیرا با این‌کار سیستم به‌طور کامل نسبت به محیط شبکه ایزوله می‌شود و تنها باید Host OS با Guest OS به‌طور محاوره‌ای با یکدیگر در تعامل باشند.

۱. در پنجره اصلی VirtualBox، بر روی دکمه File کلیک کنید و در ادامه گزینه Preferences را انتخاب نمایید. نمونه‌ای از این حالت در شکل (۳-۱) نشان داده شده است.



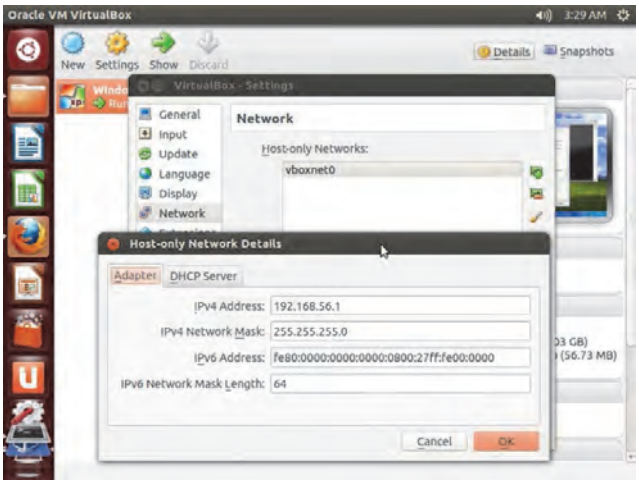
شکل (۳-۱) شمایی از پنجره اصلی ابزار VirtualBox

۲. در ادامه با انتخاب گزینه Network عملیات پیکربندی شبکه در حالت Host-only را انجام می‌دهیم. این‌کار را با کلیک بر روی آیکن سبز رنگ موجود در صفحه Network انجام خواهیم‌داد، که براساس آن قابلیت Host-only به کارت شبکه اضافه می‌شود. شمایی از مراحل تنظیم Host-only در شکل (۴-۱) نشان داده شده است.



شکل (۴-۱) شمایی از مراحل تنظیم Host-only

در ادامه بر روی آخرین آیکن در پنجره سمت راست به‌منظور ویرایش تنظیمات شبکه میزبان کلیک می‌کنیم، تا پیکربندی کنونی شبکه نمایش داده شود. چنانچه سرور DHCP فعال نباشد، نیازمند تنظیم آدرس IP به‌صورت دستی برای Guest OS می‌باشیم. شمایی از پنجره ویژه پیکربندی شبکه در شکل (۵-۱) نشان داده شده است.

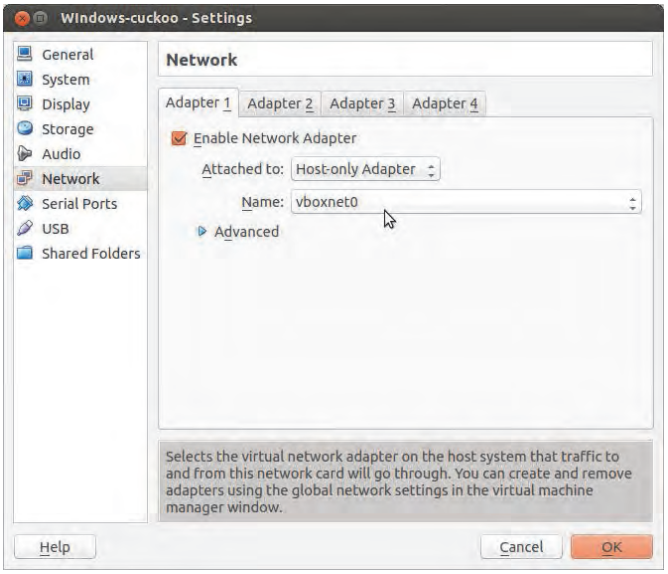


شکل (۵-۱) شمایی از پنجره ویژه‌ی پیکربندی شبکه

سپس نیازمند تنظیم و پیکربندی شبکه Guest OS در حالت Host-only می‌باشیم. برای این منظور نخست ماشین Guest OS را از ابزار VirtualBox انتخاب می‌کنیم و در ادامه، روی گزینه Settings کلیک می‌کنیم. سپس گزینه Network را انتخاب می‌کنیم و عملیات تنظیم شبکه را همانند شکل (۶-۱) انجام می‌دهیم. در این حالت با مراجعه به زبانه Adapter 1 گزینه زیر را تیک می‌زنیم تا بخش مربوط به

شبکه فعال شود. سپس از طریق منوی بازشو، گزینه Host-only Adapter را انتخاب می‌کنیم و در ادامه گزینه vboxnet0 را انتخاب می‌کنیم. Vboxnet0، نام آداپتور شبکه پایه است که هنگام ایجاد ماشین مجازی ایجاد شده است. پس از پایان پیکربندی Guest OS، باید ماشین را برای مراجعه به فرآیند نصب اجرا و در اصطلاح Start نماییم.

Enable Network Adapter

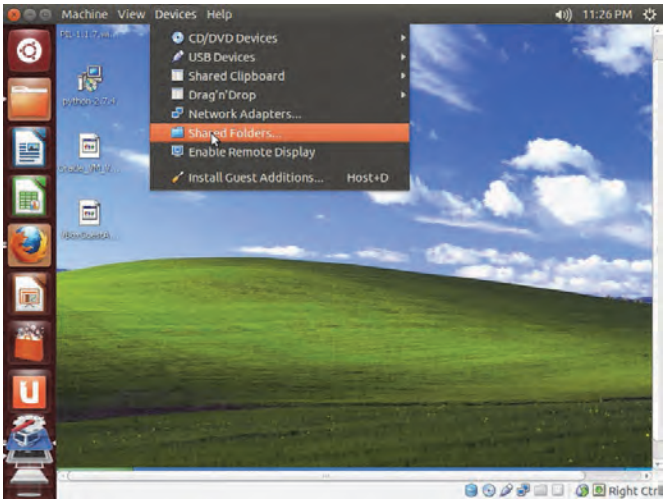


شکل (۶-۱) شمایی از عملیات تنظیم شبکه در Guest OS

پس از پایان عملیات نصب ماشین مجازی، باید در صورت عدم وجود سرور DHCP، در بخش پیکربندی شبکه، اقدام به تنظیم آدرس IP به‌صورت دستی به‌منظور دسترسی به Host OS کنیم. در این مثال آدرس IP سیستم Host OS برابر 192.168.56.1 و آدرس IP سیستم Guest OS برابر 192.168.56.101 می‌باشد.

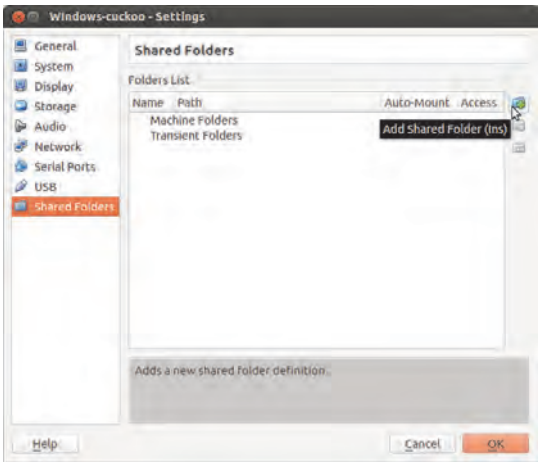
تنظیم دایرکتوری اشتراکی میان Host OS و Guest OS

۱. در پنجره اصلی Guest OS، بر روی گزینه Devices کلیک می‌کنیم و گزینه Shared Folders را همانند شکل (۷-۱) انتخاب می‌نماییم.



شکل (۷-۱) شمایی از پنجره اصلی Guest OS برای انتخاب گزینه ...Shared Folders

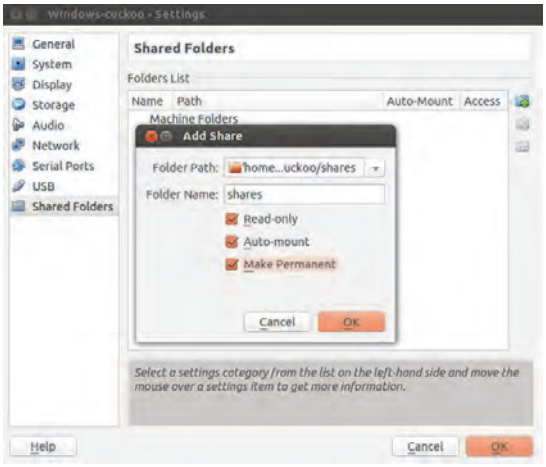
۲. در ادامه از طریق آیکن سبز رنگ در گوشه سمت راست و بالای پنجره اقدام به اضافه کردن دایرکتوری برای اشتراک‌گذاری بین دو سیستم می‌کنیم. شمایی از پنجره ویژه‌ی اضافه کردن دایرکتوری اشتراکی بین دو سیستم عامل در شکل (۸-۱) نشان داده شده است.



شکل (۸-۱) شمایی از پنجره ویژه‌ی اضافه کردن دایرکتوری اشتراکی بین دو سیستم عامل

۳. در مرحله بعدی باید یک دایرکتوری بر روی Host OS به‌منظور به اشتراک‌گذاری فایل‌ها با Guest OS در مسیری دلخواه انتخاب کنید. به‌طور پیش‌فرض سیستم نامی را برای دایرکتوری به

اشتراک گذاشته شده در نظر می‌گیرد. می‌توان نام دایرکتوری را به نام دلخواه خود تغییر داد. در ادامه نیز می‌توان گزینه‌های انتخابی را همانند شکل (۹-۱) تیک زد.



شکل (۹-۱) انتخاب نام و مسیر برای دایرکتوری اشتراکی به همراه تنظیم گزینه‌های انتخابی

۴. اکنون به محیط Guest OS مراجعه کنید و بر روی منوی Start کلیک کنید و در ادامه بر روی گزینه My Computer کلیک راست نمایید و با انتخاب گزینه Map network drive، یک درایو از دایرکتوری به اشتراک گذاشته شده بر روی Host OS ایجاد نمایید. به‌عنوان مثال مسیر مورد نظر می‌تواند عبارت \\vboxsrv\shares باشد.

۵. اکنون می‌توان به پیکربندی Guest OS پرداخت. نخست باید نرم‌افزار Python را از آدرس زیر دریافت و بر روی آن نصب نمود:

https://www.python.org/downloads/

نصب ماژول Python با نام PIL[۱] نیز برای ایجاد تصاویر از صفحه Desktop ضروری می‌باشد. این نرم‌افزار از طریق آدرس URL زیر قابل دریافت می‌باشد:

http://www.pythonware.com/products/pil/

در ادامه دو قابلیت سیستم عامل ویندوز به نام‌های Automatic Windows update و Windows firewall را غیرفعال نمایید. سپس نرم‌افزارهای مورد نیاز را از سایت www.oldapps.com دریافت نمایید و

---

[۱] Python Imaging Library

به‌صورت اختیاری بر روی سیستم نصب نمایید. برخی از این نرم‌افزارها می‌توانند شامل موارد زیر باشند:

Microsoft Office, Acrobat Reader, Mozilla Firefox, …

۶. سپس موتور اصلی نرم‌افزار Python را با کمک دستور زیر در دایرکتوری اشتراکی بر روی Host OS کپی کنید:

```
$ cp /home/digit/cuckoo/agent/agent.py /home/digit/cuckoo/shares/
```

۷. از سیستم عامل ویندوز در Guest OS، فایل agent.py را در دایرکتوری C:\Python27 کپی کنید و نام آن‌را به agent.pyw تغییر دهید. فایل‌های با پسوند pyw اسکریپت‌هایی هستند که بدون نیاز به فراخوانی کنسول ویندوز اجرا می‌شوند. به ویژه اگر برنامه مورد نظر گرافیکی باشد. اگر بر روی فایل agent.py دوبار کلیک کنید، به نظر می‌رسد که یک محیط اِعلان خط فرمان بر روی صفحه نمایش، ظاهر شده است. اگر پسوند فایل را به pyw. تغییر دهید، فایل بدون پنجره pop-up در محیط ویندوز آشکار می‌شود. این حالت شبیه اجرا شدن یک فرآیند در محیط پس‌زمینه در سیستم عامل لینوکس می‌باشد.

۸. برای اجرای فایل agent.pyw در فرآیند شروع سیستم عامل ویندوز، نیازمند قرار دادن فایل در پوشه Startup می‌باشیم. پس از اجرای فایل agent.pyw یک سوکت جدید بر روی پورت ۸۰۰۰ به فرم 0.0.0.0:8000 به‌صورت فال‌گوش در می‌آید. برای دیدن این وضعیت باید دستور زیر را در محیط خط فرمان سیستم عامل ویندوز اجرا نمایید:

```
C:\>netstat -aon
```

۹. همچنین نیازمند پیکربندی دیوار آتش Host OS برای فرستادن و فیلترسازی با استفاده از Ruleهای زیر در ابزار Iptables می‌باشیم:

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

$ iptables -A FORWARD -m conntrack --ctstate ESTABLISHED,RELATED -j ACCEPT

$ iptables -A POSTROUTING -t nat -j MASQUERADE

$ sysctl -w net.ipv4.ip_forward=1
```

۱۰. گام بعدی، پیکربندی ابزار Cuckoo Sandbox می‌باشد.

ایجاد یک حساب کاربری

می‌توانید ابزار Cuckoo Sandbox را با حساب کاربری خود اجرا کنید، یا اینکه یک حساب کاربری جدید ویژه‌ی این ابزار برای ایمنی بیشتر ایجاد کنید. پیشنهاد می‌شود به‌طور حتم یک حساب کاربری جداگانه ویژه‌ی این ابزار ایجاد کنید و برای اجرای ابزار از آن حساب کاربری استفاده نمایید. مطمئن شوید که حساب کاربری که ایجاد کرده‌اید، به‌طور دقیق همان امکانات و مجوزهای حساب کاربری که ابزار Cuckoo با آن اجرا می‌شود را داشته باشد؛ وگرنه ابزار Cuckoo قادر به اجرا و راه‌اندازی نخواهد بود. برای ایجاد حساب کاربری تنها باید دستور زیر را در محیط خط فرمان اجرا کنید:

```
$ sudo adduser cuckoo
```

اگر از ابزار VirtualBox استفاده می‌کنید، مطمئن شوید که حساب کاربری جدید متعلق به گروه vboxusers باشد یا اینکه گروه استفاده شده در VirtualBox اجرا شود:

```
$ sudo usermod -G vboxusers cuckoo
```

اگر از KVM یا هر ماژول مبتنی بر libvirt دیگر استفاده می‌کنید، مطمئن شوید که حساب کاربری جدید متعلق به گروه libvirtd باشد یا اینکه گروه توزیع لینوکس برای اجرا از libvirt استفاده کند:

```
$ sudo usermod -G libvirtd cuckoo
```

اینک بهترین زمان برای نصب و پیکربندی ابزار Cuckoo Sandbox می‌باشد.

نصب و پیکربندی ابزار Cuckoo Sandbox

در این مرحله نخست باید فایل کد منبع دریافت شده از سایت ابزار Cuckoo را به مسیر مورد نظر منتقل کرد، و آن‌را از حالت فشرده و بایگانی خارج نمود. به‌عنوان مثال، می‌توان مسیر مورد نظر را برابر مسیر زیر قرار داد:

```
/home/username/cuckoo
```

نخستین موردی که نیازمند پیکربندی آن هستیم، فایل ویژه‌ی پیکربندی cuckoo.conf می‌باشد. این فایل جزو فایل‌های اصلی ابزار Cuckoo به شمار می‌آید:

۱. cuckoo.conf: این فایل پیکربندی شامل اطلاعاتی درباره رفتار و گزینه‌های تجزیه و تحلیل عمومی در ابزار Cuckoo Sandbox است.
۲. <machinemanager>.conf: این فایل اطلاعاتی در مورد پیکربندی ماشین مجازی را در خود نگه می‌دارد. نام این فایل بستگی به نام ماشین مجازی دارد که استفاده شده است.
۳. processing.conf: این فایل برای فعال‌سازی و پیکربندی ماژول‌های فرآیندها استفاده می‌شود.

۴. reporting.conf: این فایل شامل اطلاعاتی درباره تکنولوژی‌های گزارش‌گیری می‌باشد.

این فایل به‌طور کامل در ادامه فصل مورد بررسی قرار می‌گیرند.

فایل cuckoo.conf

این فایل شامل اطلاعات پیکربندی عمومی و پایه‌ای ابزار Cuckoo می‌باشد. برای نمونه، می‌توانید با این فایل به بررسی جدیدترین نسخه ابزار در هنگام اجرا بپردازید. چنانچه از این ویژگی استفاده کنید، ابزار Cuckoo جدیدترین نسخه را دریافت می‌کند و می‌توانید آن‌را بر روی نسخه پیشین ذخیره نمایید. این‌کار در متغیر version_check در فایل cuckoo.conf تعریف می‌شود. می‌توانید روش مجازی‌سازی را در فایل cuckoo.conf تعریف و تشریح کنید. به‌عنوان مثال اگر از VirtualBox استفاده می‌کنید، می‌توانید مقدار متغیر زیر را برابر عبارت virtualbox قرار دهید و یا اگر از VMware استفاده می‌کنید می‌توانید مقدار متغیر گفته شده را برابر عبارت vmware قرار دهید:

```
machine_manager= virtualbox
```

همچنین می‌توان مقدار آدرس IP مربوط به Host OS و شماره پورت آن‌را برای استفاده از Cuckoo Sandbox در فایل cuckoo.conf تعریف کرد. به‌صورت پیش‌فرض آدرس IP برای Host OS برابر 192.168.56.1 (زیرا از روش شبکه‌بندی Host-only استفاده می‌کند) و مقدار پورت به‌طور پیش‌فرض برابر 2042 می‌باشد. فراموش نکنید که باید واسط شبکه‌بندی را نیز تعریف نمایید. به‌طور معمول واسط شبکه‌بندی قابل تعریف برای Cuckoo، برابر vboxnet0 می‌باشد.

فایل <machinemanager.conf>

ماژول‌های حوزه مدیریت ماشین، ویژه‌ی تعریف تعامل ابزار Cuckoo با ابزارهای مجازی‌سازی می‌باشند. اگر از VirtualBox استفاده می‌کنید، فایل <machinemanager>.conf به فایل پیکربندی virtualbox.conf برمی‌گردد، اما اگر از ابزار VMware استفاده می‌کنید، فایل ویژه‌ی ماژول‌های مدیریت ماشین یعنی <machinemanager>.conf به فایل vmware.conf برمی‌گردد. در این کتاب از ابزار VirtualBox استفاده شده است، بنابراین تنها نیازمند توجه و دقت به فایل virtualbox.conf می‌باشیم. می‌توان فایل اصلی را برای نیازمندی‌های خود ویرایش کرد. به‌عنوان مثال اگر بخواهید ابزار VirtualBox را در حالت گرافیکی اجرا کنید، باید حالت gui را در فایل گفته شده ویرایش و تنظیم کنید. اکنون اگر با کار کردن با ابزار VirtualBox در وضعیت خط فرمان، راحت‌تر هستید، می‌توانید حالت headless را به فرم زیر در فایل virtualbox.conf تنظیم نمایید.

```
mode = headless
```

به خاطر دارید که در هنگام نصب و راه‌اندازی Guest OS گفته شد که نام‌گذاری سیستم Guest OS باید با دقت انجام شود. اینک اگر بخواهید نام مورد نظر را تغییر دهید، این‌کار با ویرایش فایل پیکربندی Guest OS امکان‌پذیر است. بنابراین در بخش [cuckoo1] می‌توانید نام ویژه‌ای برای Guest OS در نظر بگیرید. اگر نام cuckoo1 را برای Guest OS در نظر گرفته‌اید باید فایل ویژه‌ی پیکربندی Guest OS را به فرم زیر ویرایش کنید:

```
label = cuckoo1
```

گفتنی است که در مثال کتاب نام Guest OS برابر عبارت windows-cuckoo در نظر گرفته شده است. چنانچه از سیستم عامل ویندوز مانند XP برای Guest OS استفاده می‌کنید، باید عبارت platform را در فایل پیکربندی برابر windows قرار دهید.

```
platform = windows
```

فراموش نکنید که آدرس IP مربوط به Guest OS باید تنظیم شود. همان‌طور که گفته شد از ساختار Host-only برای شبکه‌بندی استفاده می‌شود و به‌صورت پیش‌فرض نخستین سیستم عامل، سیستم Guest با آدرس IPایی برابر 192.168.56.101 می‌باشد.

فایل processing.conf

این فایل پیکربندی اجازه می‌دهد تا عملیات فعال، غیرفعال‌سازی و پیکربندی را برای همه‌ی ماژول‌های فرآیند پیاده‌سازی کنید. به‌طور کلی نیازی به تغییر در فایل پیکربندی پیش‌فرض وجود ندارد. اما می‌توانید کلید API مربوط به قابلیت VirusTotal را به آن اضافه کنید. چنانچه حساب کاربری در VirusTotal ندارید، می‌توانید با مراجعه به وب سایت آن یک حساب کاربری ایجاد کنید و کلید را در خط زیر وارد کنید:

```
# Add your VirusTotal API key here. The default API key, kindly
# provided by the VirusTotal team, should enable you with a
# sufficient throughput and while being shared with all our users,
# it should not affect your use.
key = a0283a2c3d55728300d064874239b5346fb991317e8449fe43c902879d758088
```

فایل reporting.conf

این فایل که در مسیر conf/reporting.conf قرار دارد شامل اطلاعاتی در مورد تولید گزارش‌های خودکار است. فایل گفته شده شامل اطلاعاتی در مورد روش‌ها یا انواع گزارش‌هایی است که می‌خواهید پس از پایان فرآیند تجزیه و تحلیل از آن‌ها استفاده کنید. می‌توان روش‌های گزارش‌گیری را فعال یا غیرفعال کنید. پس از پایان عملیات پیکربندی ابزار Cuckoo Sandbox می‌توان برای نخستین