بسمه تعالی

تهدیدات و آسیب‌پذیری‌ها در محیط‌های مجازی‌سازی (بخش دوم)

فهرست مطالب

۱ مقدمه

مجازی‌سازی یکی از سریع‌ترین فناوری‌های در حال گسترش در صنعت فناوری اطلاعات است که موجب صرفه‌جویی در هزینه و سهولت در مدیریت استقرار می‌شود. با وجود مزایای زیاد این فناوری، جنبه‌های تاریکی نیز وجود دارند که باعث نگرانی‌های امنیتی می‌شوند. محیط مجازی‌سازی یک سکوی[۱] مناسب برای بسیاری از تهدیدات و آسیب‌پذیری‌های بالقوه است که باید مورد توجه قرار گیرد. مجازی‌سازی چالش‌های امنیتی زیادی را ایجاد می‌کند. امنیت مجازی‌سازی باید این شکاف‌های بالقوه را، به‌منظور کاهش هزینه‌ها و پیچیدگی، مدیریت کند. بنابراین شناسایی این چالش‌ها و تهدیدات امنیتی نقش مهمی را در این زمینه ایفا می کند. در این گزارش رایج‌ترین تهدیدات در مجازی‌سازی ارائه شده است. لازم به ذکر است که بیشتر بر تهدیداتی تمرکز شده است که مجازی‌سازی را هدف قرار می دهند.

۲ تهدیدات محیط مجازی‌سازی

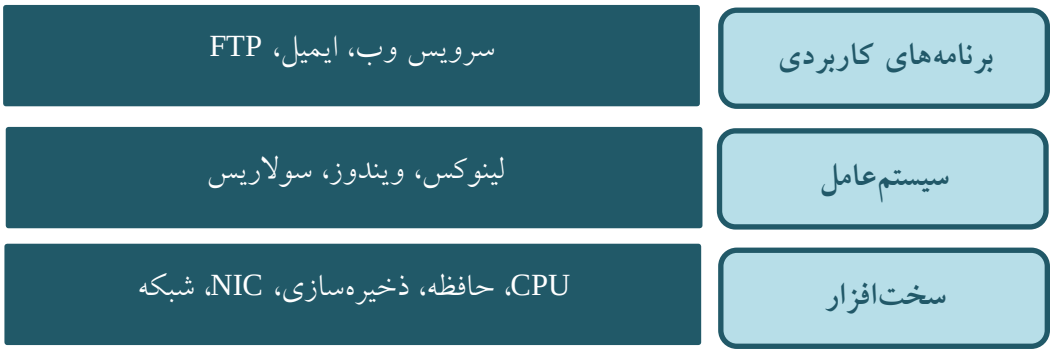
تمام محیط‌های فناوری اطلاعات با تهدیدات امنیتی متنوعی مواجه هستند. این تهدیدات شامل تهدیدات ذاتاً تصادفی (مانند اشتباهات کارمندان)، ویروس‌هایی که به دنبال دزدیدن اطلاعات هستند، و مهاجمان خارجی که تلاش می‌کنند تا به محیط آسیب برسانند، می‌باشند. محیط‌های مجازی نیز مانند محیط‌های فیزیکی با انواع متنوعی از تهدیدات مواجه هستند، با این تفاوت که در محیط‌های مجازی، به دلیل وجود مؤلفه‌های مجازی‌سازی، تهدیدات می‌توانند به روش‌های متنوع‌تری وجود داشته باشند. همان‌طور که در شکل ۱ نشان داده شده است محیط‌های مجازی، علاوه بر مؤلفه‌های محیط‌های فیزیکی، دارای مؤلفه‌ی ابرناظر[۲] هستند. بدیهی است که با اضافه‌شدن این مؤلفه یک سطح حمله‌ی متناظر با آن نیز به حملات محیط اضافه می‌شود.

نگرانی‌ها و تهدیدات امنیتی جدیدی که مجازی‌سازی به وجود می‌آورد، بیشتر مرتبط با به‌اشتراک‌گذاری منابع میان ماشین‌های مجازی و آسیب‌پذیری‌های خود ابرناظر است. حملاتی که بر علیه ابرناظر انجام می‌شوند تأثیر

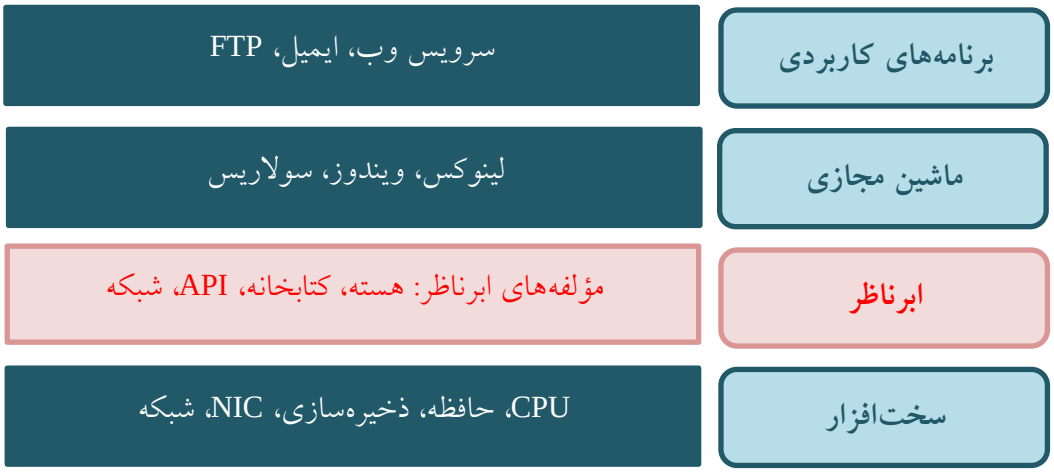
[۱] Platform

[۲] Hypervisor

زیادی بر محیط مجازی دارند، زیرا به مهاجم اجازه می‌دهند که کنترل تمام ماشین‌های مجازی که بر روی آن ابرناظر وجود دارند، را در دست بگیرد.



(الف)



(ب)

شکل ۱ (الف) محیط فیزیکی، (ب) محیط مجازی

در ادبیات امنیت، طبقه‌بندی امنیتی که برای حملات استفاده می‌شود، براساس تأثیرات آن بر سیستم از نظر ویژگی‌های امنیتی است. این طبقه‌بندی به صورت زیر است:

- حمله به صحت: حملاتی که داده‌های غیرمجاز را نوشته یا تغییر می‌دهند.
- حمله به محرمانگی: حملاتی که اجازه خواندن داده‌های غیرمجاز را می‌دهند.
- حمله به دسترس‌پذیری: حملاتی که عملکرد عادی سیستم را مختل می‌سازند.

در این گزارش ما به ارائه‌ی یک طبقه‌بندی برای انواع حملات و تهدیدات موجود در محیط‌های مجازی می‌پردازیم. در این طبقه‌بندی تهدیدات محیط مجازی‌سازی را، بر اساس نوع مؤلفه‌ای که مورد هدف قرار می‌گیرد، به سه گروه زیر تقسیم می‌کنیم:

- تهدیدات ماشین‌های مجازی: مستقیماً ماشین مجازی را هدف قرار می‌دهند.
- تهدیدات ابرناظر: ابرناظر را هدف قرار می‌دهند. این گروه از تهدیدات بسیار خطرناک هستند زیرا مهاجم می‌تواند با حمله به ابرناظر تمام ماشین‌های مجازی روی آن را مورد تهدید قرار دهد.
- تهدیدات شبکه مجازی: این گروه از تهدیدات کل شبکه مجازی که می‌تواند شامل چندین ابرناظر باشد را هدف قرار می‌دهند.

۲-۱ تهدیدات ماشین‌های مجازی

برای یک مهاجم تشخیص این‌که یک سیستم به صورت مجازی اجرا می‌شود بسیار مفید است زیرا می‌تواند روش‌های جدیدی را برای حمله به سیستم به وجود آورد. با تشخیص مجازی‌بودن محیط مهاجم می‌تواند، علاوه بر حملات مربوط به سیستم‌عامل و برنامه‌های کاربردی، بر روی حملات خاص محیط مجازی تمرکز کند که ممکن است سریع‌تر و آسان‌تر باشند.

۲-۱-۱ حمله Cross-VM

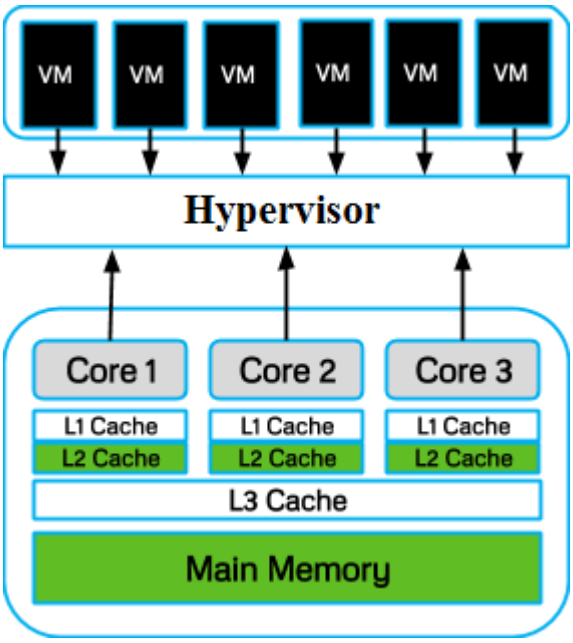
در این حمله مهاجم تلاش می‌کند که یک ماشین مجازی دیگر در میزبان مشابه را مورد حمله قرار دهد. نمونه هایی از چنین حملاتی محدودکردن دسترسی ماشین‌های مجازی یا بازیابی اطلاعات حساس از آن‌ها است. حملات نوع دوم یعنی بازیابی اطلاعات حساس از ماشین‌های مجازی توسط یک ماشین مجازی مهاجم در میزبان مشابه، معمولاً با استفاده از کانال‌های جانبی[۳] مختلف مانند کانال‌های پنهان حافظه نهان، مبتنی بر شبکه (مانند علامت‌گذاری شبکه[٤] و اثر انگشت[٥]) و یا مبتنی بر حافظه (کانال‌های پنهان گذرگاه حافظه)، قابل انجام است. در حقیقت، از آنجایی که ماشین‌های مجازی از منابع سخت‌افزاری مشترک مانند CPU، حافظه و شبکه

[۳] Side channels

[٤] Network watermarking

[٥] Fingerprinting

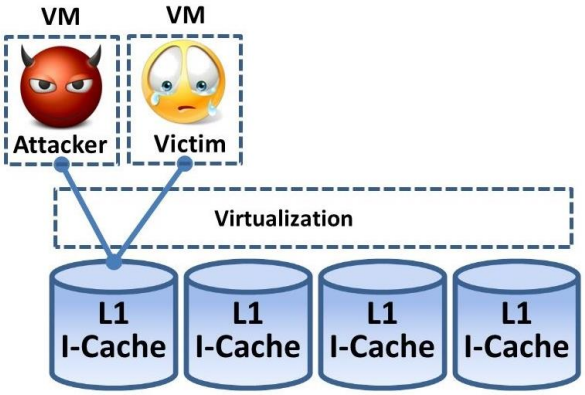
استفاده می‌کنند (شکل ۲) یک ماشین مجازی نفوذی می‌تواند اطلاعاتی را از دیگر ماشین‌های مجازی به دست آورد. مهاجم ابتدا سعی می‌کند مکان ماشین مجازی مورد نظر را شناسایی کرده و سپس ماشین مجازی خود را بر روی همان میزبان قرار می‌دهد.



شکل ۲ به‌اشتراک‌گذاری سخت‌افزار میزبان بین ماشین‌های مجازی مختلف

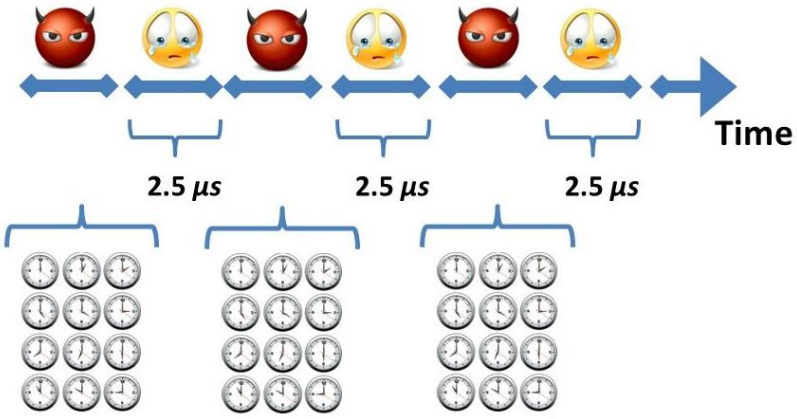
حملات Cross-VM مبتنی بر حافظه نهان در واقع مبتنی بر اطلاعات مربوط به رقابت مهاجم و قربانی برای گرفتن فضا در آن است (شکل ۳). هرگونه سوءاستفاده از حافظه نهان در نتیجه‌ی دسترسی مشترک مهاجم و قربانی به آن است. در واقع مهاجم از روی تغییرات انجام گرفته در حافظه نهان توسط قربانی، حمله خود را انجام می‌دهد. این کار بسیار سخت است، زیرا حافظه نهان کوچک است و به طور معمول هیچ‌کدام از داده های مهاجم برای زمان کافی در حافظه نهان ذخیره نمی‌شود تا اجازه دهد مهاجم در مورد عملیات انجام شده توسط قربانی اطلاعاتی به دست آورد. این حمله نیاز به این دارد که مهاجم بتواند، با به وجود آوردن وقفه‌های زیاد، نرخ تعویض متن[۶] بالایی را در حافظه نهان به وجود آورد.

[۶] Context-switch



شکل ۳ رقابت مهاجم و قربانی برای گرفتن فضا در حافظه نهان

این حمله به این صورت انجام می‌گیرد که مهاجم تلاش می‌کند با ایجاد وقفه‌های متوالی حافظه نهان را در دست بگیرد. به این ترتیب مانع از آن می‌شود که ماشین مجازی قربانی برای زمان مناسبی حافظه نهان را در اختیار داشته باشد و زمان‌هایی که حافظه نهان در اختیار قربانی است بسیار کوتاه می‌شود (شکل ٤). یک مهاجم حرفه‌ای از این طریق می‌تواند یک حمله کانال جانبی انجام داده و اطلاعاتی را از ماشین مجازی قربانی به‌دست آورد. بنابراین، به وجود آوردن وقفه‌های زیاد توسط یک ماشین مجازی می‌تواند یکی از راه‌های شناسایی این حمله باشد.



شکل ٤ گرفتن حافظه نهان از قربانی با ایجاد وقفه‌های متوالی توسط مهاجم

۲-۱-۲ حمله ربودن مهمان

هرگونه حمله به یک ماشین مجازی که باعث شود مهاجم بتواند به فایل‌های خاص ماشین مجازی دسترسی پیدا کرده، آن‌ها را بخواند، و یا دانلود نماید، با عنوان حمله ربودن مهمان[۷] شناخته می‌شود. یکی از شناخته‌شده‌ترین راه‌های انجام این حمله، از طریق حمله پیمایش مسیر[۸] یا پیمایش دایرکتوری[۹] است.

۲-۱-۲-۱ حمله پیمایش مسیر

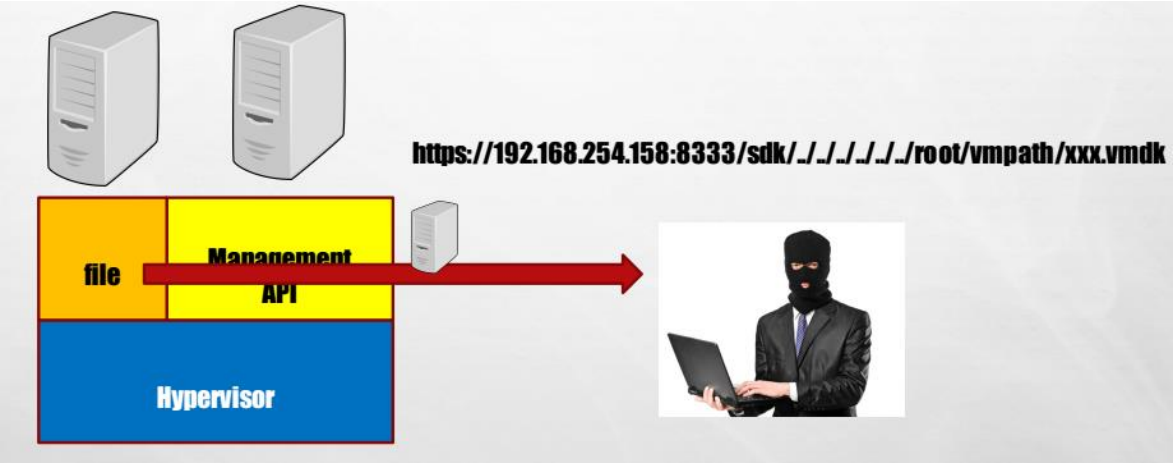
در این حمله کاراکترهایی که برگشت به دایرکتوری والد را نشان می‌دهند (/..) از طریق APIها ارسال می شوند. هدف این حمله این است که از یک برنامه و همچنین اعتبارسنجی ناکافی برای دسترسی به فایل‌ها و پوشه‌ها، سوءاستفاده کرده تا دسترسی غیرمجاز به سیستم‌فایل را به دست آورد. در صورت آسیب‌پذیر بودن ابرناظر به این حمله، مهاجم که با واسط وب ابرناظر اتصال برقرار کرده است می‌تواند با استفاده از کاراکترهای برگشت به دایرکتوری والد از Management API به سیستم‌فایل پرش کند (شکل ۵). در این حالت مهاجم می‌تواند سیستم‌فایل ابرناظر را پیمایش کرده و به فایل پیکربندی ماشین مجازی دسترسی پیدا می‌کند. در نتیجه مهاجم این توانایی را دارد که با خواندن این فایل مسیر دیگر فایل‌ها را نیز پیدا کرده، و همچنین فایل‌ها را دانلود نماید و یا به بیان دیگر سرقت کند (شکل ٦).

[۷] Guest stealing

[۸] Path traversal

[۹] Directory traversal

شکل ۵ پرش مهاجم از Management API به سیستم‌فایل با استفاده از حمله پیمایش مسیر



شکل ٦ پیمایش سیستم‌فایل و دانلود فایل از آن توسط مهاجم

این حمله هوشمندانه و ساده است. در حال حاضر این حمله علیه نسخه‌های قدیمی‌تر VMware Virtual Infrastructure 3.x قابل انجام است. VMware در اواخر سال ۲۰۰۹ و پس از شناسایی این مشکل یک وصله[۱۰] برای این نقص امنیتی منتشر کرد.

۲-۱-۳ حمله VM hyper jumping

حمله VM hyper jumping اجازه می‌دهد تا ترافیک یک ماشین مجازی توسط یک ماشین مجازی مخرب مورد دسترسی قرار گیرد. به عبارت دیگر، این حمله از ضعف یک ماشین مجازی استفاده کرده تا بر علیه دیگر ماشین‌های مجازی در میزبان مشابه حمله انجام دهد. نسخه‌های قدیمی سیستم‌عامل‌ها و سیستم‌عامل‌های ناامن می‌توانند یکی از راه‌های انجام این نوع از حمله‌ها باشند. همچنین سرریز کردن سوئیچ مجازی با انجام حمله MAC سیل‌آسا مهاجم می‌تواند موفق به شنود ترافیک سایر ماشین‌های مجازی قرار گرفته بر روی آن میزبان گردد.

[۱۰] Patch

۲-۱-٤ مشکلات snapshotها

گرفتن تصویر از یک ماشین مجازی با عنوان snapshot شناخته می‌شود. این تصویر اجازه می‌دهد تا در صورت به‌وجودآمدن مشکل، مدیر بتواند بازیابی انجام دهد. این موضوع حائز اهمیت است اما می‌تواند نگرانی‌های امنیتی را نیز به همراه داشته باشد. یک snapshot می‌تواند یک منبع ناامن، که هنگام snapshot گرفتن وجود داشته و پس از آن رفع شده است، مانند یک برنامه‌ی کابردی بدون وصله، را دوباره بر روی ماشین مجازی قرار دهد. مشکل استفاده مجدد از سازوکارهای امنیتی ضعیف یا گذرواژه‌های قدیمی و یا سایر اطلاعات حساس در snapshotها بسیار خطرناک است، زیرا آن‌ها حاوی داده‌های RAM هستند. همچنین در صورت به سرقت‌رفتن snapshotها ممکن است اطلاعات بسیار مهمی در مورد ماشین مجازی افشا شود.

۲-۱-۵ تهدیدات سیستم‌عامل مهمان

تهدیدات و آسیب‌پذیری‌های امنیتی مربوط به سیستم‌عامل مهمان یا برنامه‌های کاربردی آن، یکی از انواع تهدیدات محیط‌های مجازی به حساب می‌آیند. یکی از رایج‌ترین انواع این نوع از تهدیدات، تهدیدات مبتنی بر بدافزار است. بدافزارهای آگاه از VM[۱۱] نسل جدیدی از بدافزارها هستند که این توانایی را دارند که تعیین کنند آیا بر روی یک ماشین مجازی در حال اجرا هستند. این کار با ردیابی ویژگی‌های ذاتی مجازی‌سازی مانند نوع آدرس MAC و مکان حافظه قابل انجام است. پس از شناسایی محیط مجازی آن‌ها اغلب سعی می‌کنند که رفتاری متفاوت با محیط فیزیکی از خود نشان ندهند و بنابراین تشخیص خود را مشکل می‌کنند. از آنجایی که بسیاری از متخصصان امنیتی از محیط‌های مجازی برای تحلیل بدافزارها استفاده می‌کنند، این نوع بدافزارها کار را دشوار می‌کنند.

[۱۱] VM-aware

۲-۲ تهدیدات ابرناظر

ماشین میزبان نقطه کنترل و ریشه سیستم مجازی است، که می‌تواند بر برنامه‌هایی که در VM[۱۲]ها اجرا می‌شوند نظارت داشته و با آن‌ها ارتباط برقرار کند. ماشین میزبان، وابسته به نوع فناوری مجازی‌سازی، می‌تواند نقش‌های مختلفی را در تعاملات بین VMها داشته باشد. رایج‌ترین این نقش‌ها عبارتند از:

- میزبان می‌تواند روشن، خاموش، راه‌اندازی مجدد، یا توقف یک VM را انجام دهد.
- میزبان می‌تواند بر منابع VMها نظارت کرده یا آن‌ها را تغییر دهد.
- میزبان می‌تواند داده‌ی ذخیره‌شده روی دیسک مجازی تخصیص داده شده به VM را ببیند، کپی کند، و یا تغییر دهد.

همه‌ی ترافیک شبکه VMها از میزبان عبور می‌کند و بنابراین میزبان قادر است که بر ترافیک شبکه هر VM نظارت داشته باشد. میزبان نقطه کنترل سیستم مجازی است؛ از این رو باید بیشتر از خود VMها و به شدت محافظت شود. جداسازی میزبان باید انجام شود تااجازه ندهد که از آن به‌عنوان دروازه‌ای برای حمله به VMها استفاده شود.

از آنجایی که ابرناظر (که بر روی ماشین میزبان نصب شده است) و کنسول مدیریتی آن نقش مهمی در محیط مجازی‌سازی ایفا می‌کنند. بنابراین ابرناظر هدف جذابی برای مهاجمان در محیط‌های مجازی است. ابرناظر می تواند تبدیل به یک نقطه شکست[۱۳] شود، زیرا هنگامی که یک ابرناظر مورد حمله قرار می‌گیرد می‌توان از آن برای حمله به دیگر VMها در همان میزبان سوءاستفاده کرد.

۱-۲-۲ حمله Hyper-jacking

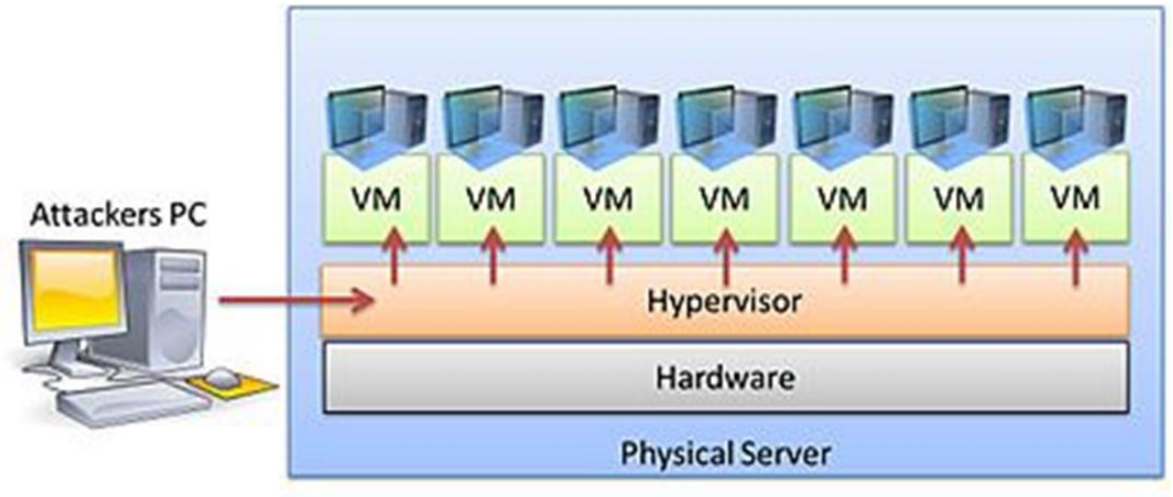
هدف از این کلاس حملات، خراب‌کردن، جاسوسی، سرقت و یا تغییر داده‌های VM به‌وسیله‌ی کدهای مخربی است که در سطح ابرناظر اجرا می‌شود. این کلاس از حملات بر اساس تزریق کد در ابرناظر است. تزریق کد با استفاده از بدافزاری که در سطح ابرناظر اجرا می‌شود قابل انجام است. در حالت کلی نصب یک ابرناظر جعلی و مخرب به منظور در اختیار گرفتن مدیریت کل سیستم سرویس‌دهنده و به دست آوردن کنترل ابرناظر

[۱۲] Virtual Machin

[۱۳] Single point of failure

اصلی یا اجرای یک ابرناظر جعلی تحت ابرناظر موجود را حمله Hyper-jacking می‌گویند (شکل ۷). این حمله‌ی رایجی نیست و نیاز به یک مهاجم بسیار ماهر دارد.

این نوع از حملات از فناوری‌های مجازی‌سازی موجود، مانند AMD-V، Intel VT-x یا Intel VT-d استفاده کرده و تلاش می‌کند تا یک بدافزار (روت‌کیت‌های مبتنی بر ماشین مجازی[۱۴] یا VMBRها) را در یک سطح پایین‌تر از ابرناظر قرار دهد. در واقع یک کلاس از بدافزارها وجود دارند که ابرناظر مخرب را زیر سیستم‌عامل قرار می‌دهند و از مجازی‌سازی استفاده کرده تا خود را غیرقابل شناسایی سازند. به‌عنوان مثال SubVirt، Vitrol و Blue Pill بدافزارهایی برای اثبات این مفهوم هستند.



شکل ۷ به‌دست‌آوردن کنترل ابرناظر توسط مهاجم

این کلاس از حملات بدترین سناریو برای فناوری مجازی‌سازی است زیرا به مهاجم اجازه می‌دهد تا داده‌ها و برنامه‌های غیرمجاز را بخواند یا تغییر دهد. تأثیر چنین حملاتی به خود ماشین مجازی محدود نمی‌شود، بلکه دیگر ماشین‌های مجازی و خود ابرناظر نیز تحت تأثیر قرار می‌گیرند.

به‌عنوان مثال، این حملات می‌توانند به یک مهاجم در سطح ابرناظر اجازه دهند تا کنترل دسترسی ماشین مجازی را تغییر دهد و امتیازات بالاتری را به او بدهد. همچنین، می‌توانند به مهاجم اجازه دهند که به صورت

[۱۴] Virtual Machine Based Rootkits

غیرمحسوس جاسوسی از یک ماشین مجازی دیگر را انجام دهد بدون هیچ‌گونه امکان شناسایی از داخل ماشین مجازی که مورد جاسوسی قرار گرفته است.

۲-۲-۱-۱ روت‌کیت‌های مبتنی بر ماشین مجازی

روت‌کیت‌ها ابزارهای مفیدی برای مهاجمان هستند زیرا آن‌ها خود را پنهان می‌کنند و تشخیص آن‌ها مشکل است. هدف روت‌کیت این است که بر روی هسته سیستم‌عامل اجرا شود (ring0). اگر مهاجم به این هدف دست یابد، می‌تواند کل سیستم را کنترل کند. اگر موفق شود، یک VMBR خواهد بود که تشخیص و حذف آن دشوار است. روت‌کیت‌های مبتنی بر مجازی‌سازی یک نوع خاص از بدافزارها هستند که با وجود کمیاب بودن جزء ابزارهای این حمله محسوب می‌شوند.

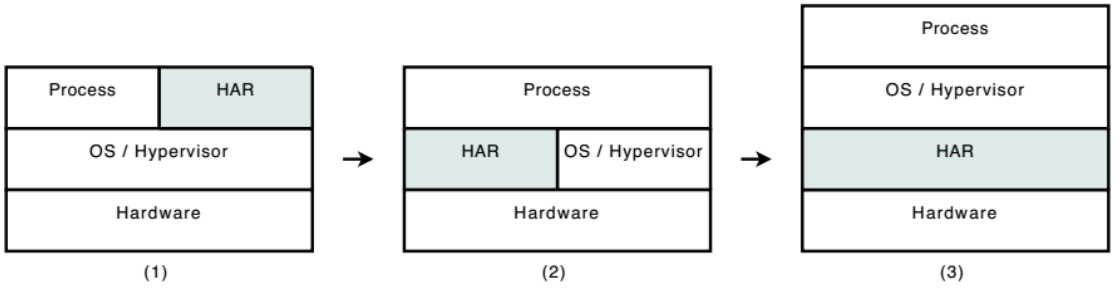
این نوع از حملات می‌توانند سیستم‌عامل یا ابرناظر در حال اجرا را، در زمان اجرا و بدون این‌که توسط آن شناسایی شوند، مجازی‌سازی کنند. این کار باعث می‌شود که یک ابرناظر سایه[۱۵] (ابرناظری که توسط کاربر قابل مشاهده نیست) داشته باشیم که می‌تواند جاسوسی کرده و نیز کنترل تمام ماشین را در دست بگیرد. این نوع از ابرناظرهای جعلی با عنوان روت‌کیت‌های شتاب‌دهنده‌ی سخت‌افزار[۱۶] (HAR) شناخته می‌شوند. این نوع از حملات به روش‌های مختلفی قابل انجام هستند:

۱. ایجاد یک ابرناظر جعلی و جایگزینی ابرناظر اصلی با آن. مراحل زیر نشان می‌دهند که چگونه یک HAR می‌تواند کنترل یک ماشین را در دست بگیرد (این مراحل در شکل ۸ نشان داده شده است):
   أ. HAR به‌وسیله‌ی یک بردار حمله شناخته‌شده شروع به اجرا شدن روی سیستم‌عامل می‌کند.
   ب. HAR محدوده‌ی حافظه‌ی خود را به ابتدای فضای هسته انتقال می‌دهد.
   ت. HAR سیستم‌عامل را، بدون راه‌اندازی مجدد آن، به یک ماشین مجازی مهاجرت می‌دهد.
   اکنون هرگونه عملیاتی در سیستم‌عامل/ابرناظر جدید مجازی‌سازی‌شده توسط HAR قابل کنترل است.

---

[۱۵] Shadow

[۱۶] Hardware Accelerated Rootkits



شکل ۸ مراحل ایجاد یک ابرناظر جعلی و جایگزینی ابرناظر اصلی با آن

۲. تغییر ایستای یک ابرناظر قانونی به منظور انجام عملیات مخرب (مانند تغییر یک ابرناظر کد باز، مثل Xen، به‌منظور جاسوسی کلیدها). انجام این نوع از حملات معمولاً سخت‌تر است.

۳. تغییر پویای یک ابرناظر قانونی در زمان اجرا. این کار با یک دسترسی مستقیم به حافظه[۱۷] (DMA)، یا هر بردار دیگری که اجازه تغییر حافظه را می‌دهد، برای جایگزینی ماژول ابرناظر با یک نسخه‌ی مخرب آن، قابل انجام است. این دسته از حملات سخت‌ترین نوع حملات از نظر شناسایی‌شدن هستند. از نظر سیستم‌عامل، هیچ تغییری در حافظه یا رجیستری CPU در حین یا بعد از مهاجرت[۱۸] (مجازی‌سازی سیستم‌عامل یا ابرناظر قبلی) اتفاق نیفتاده است. این دسته از حملات همچنین سخت‌ترین نوع از نظر قابلیت انجام است.

از لحاظ تئوری امکان تشخیص تمام این حملات با استفاده از معیار تأخیر وجود دارد. انتظار می‌رود که با افزودن یک لایه مجازی‌سازی، زمان اجرای هر عملیات سیستمی افزایش پیدا کند و حتی این افزایش قابل مشاهده باشد. اما، در واقع، تأخیر ناشی از کد مخرب اغلب ناچیز است در مقایسه با زمان تأخیر ابرناظر قانونی. علاوه بر این، تمام مسائل مربوط به مجازی‌سازی را می‌توان به ابرناظر قانونی که تغییر یافته است، مرتبط ساخت، و این قابلیت شناسایی حملات را از دیدگاه VM مشکل می‌سازد.

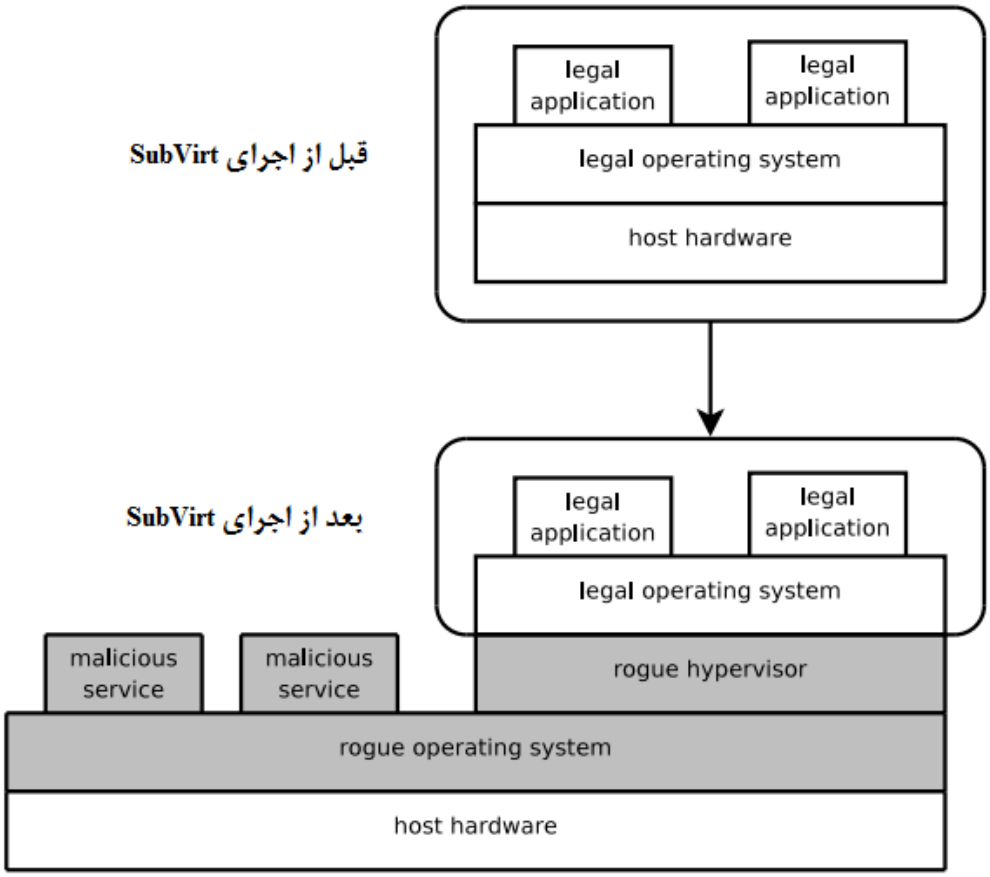
SubVirt روشی برای پیاده‌سازی مجازی‌سازی سایه برای سیستم‌عامل‌های GNU/Linux و Microsoft Windows XP است. هدف این رهیافت، همان‌گونه که در شکل ۹ نشان داده شده است، مجازی‌سازی

[۱۷] Direct Memory Access

[۱۸] Migration

سیستم‌عامل است به‌گونه‌ای که کاربر نهایی متوجه آن نشود. علاوه بر این، این رهیافت اجازه می‌دهد که یک سیستم‌عامل جعلی پایه به‌عنوان یک ابرناظر که سرویس‌های مخرب را مدیریت می‌کند، اجرا شود. سیستم‌عامل جعلی در Virtual PC بر روی Microsoft Windows XP و در VMware بر روی Linux پیاده‌سازی می‌شود. نصب این HAR تنها ٢٤ ثانیه زمان برده و به ٢٢٦ مگابایت فضا نیاز دارد. پس از نصب مجازی‌سازی سایه، سیستم‌عامل تنها ١٩ ثانیه زمان بیشتر برای راه‌اندازی نیاز دارد. با استفاده از این رهیافت، موارد زیر پیاده‌سازی شده‌اند:

- سرویس‌های جعلی مخفی: رله‌های اسپم، زامبی‌های بات‌نت و سرویس‌دهنده‌های وب فیشینگ.
- سرویس‌هایی که داده‌ها و رویدادهایی که از سیستم‌عامل قانونی می‌آیند را مشاهده می‌کنند. این سرویس‌ها می‌توانند به صورت مخفیانه کلیدها و بسته‌های شبکه را ثبت کنند.
- سرویس‌های مخرب که اجرای سیستم‌عامل قانونی (یا برنامه‌های موجود در آن) را در دستورالعمل های دلخواه، به دام می‌اندازند. یکی از این سرویس‌ها هر فراخوانی متد write از سوکت کتابخانه SSL را به دام می‌اندازد که اجازه می‌دهد داده‌های متن آشکار، قبل از رمزگذاری، خوانده شوند.
- سرویس‌هایی که به عمد اجرای سیستم هدف را تغییر می‌دهند. این سرویس‌ها اجازه تغییر ارتباطات شبکه، حذف پیام‌های ایمیل یا تغییر اجرای یک برنامه در سیستم‌عامل قانونی را می‌دهند.



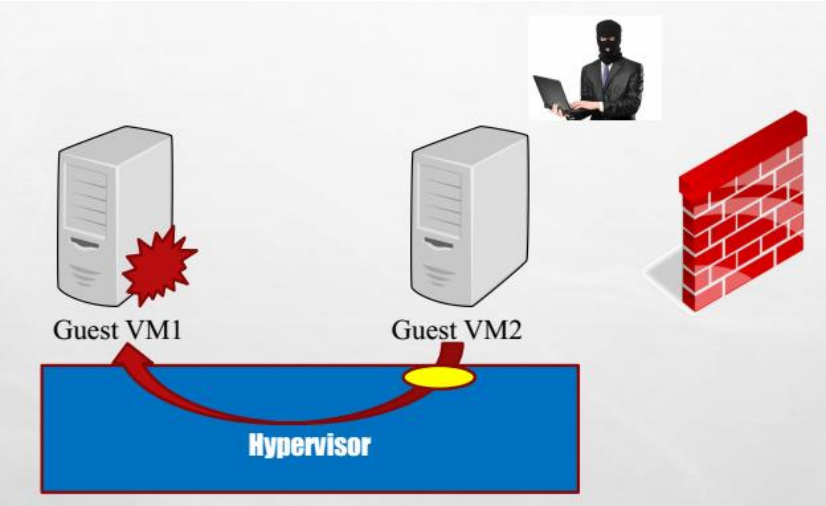
شکل ۹ در دست گرفتن کنترل یک سیستم‌عامل توسط SubVirt

۲-۲-۲ حمله فرار از VM

در حمله فرار از VM[۱۹] مهاجم تلاش دارد از VM خود خارج شده و کنترل ابرناظر را در دست بگیرد. در این هنگام مهاجم می‌تواند هر تابعی، مانند ایجاد VMها، یا مدیریت ورودی/خروجی را فراخوانی کند. به‌عنوان مثال حمله Cloudburst یک سوءاستفاده از فضای حافظه است که VM مهمان را قادر می‌سازد تا کد مخرب را در میزبان اجرا کند و سپس یک تونل اتصال به آن را ایجاد کند. یک حمله متعارف در این دسته حمله پرش از VM[۲۰] است که به مهاجم اجازه می‌دهد که از یک VM به یک VM دیگر در میزبان مشابه حرکت کند (شکل ۱۰).

[۱۹] VM Escape

[۲۰] VM Hopping

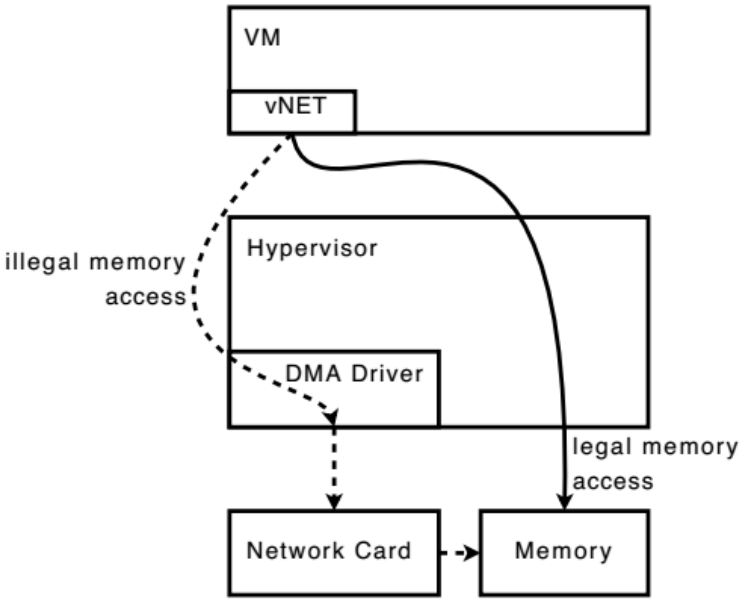


شکل ۱۰ حمله پرش از ماشین مجازی

۲-۲-۲-۱ دسترسی مستقیم به حافظه

برخی درایورها این توانایی را دارند که به سخت‌افزار پایه دسترسی داشته باشند. این کار با استفاده از DMA قابل انجام است. این حمله این امکان را به وجود می‌آورد که کل حافظه فیزیکی خوانده یا نوشته شود. همان‌طور که در شکل ۱۱ نشان داده شده است، در معماری مجازی‌سازی دو راه برای دسترسی به حافظه وجود دارد:

- روش نرمال: هر نوع دسترسی به حافظه توسط ابرناظر کنترل می‌شود تا تضمین کند که یک VM می‌تواند تنها به محدوده‌ی حافظه خود دسترسی داشته باشد.
- روش مخرب: یک مهاجم می‌تواند با استفاده از یک درایور DMA جعلی که بین واسط شبکه مجازی (vNet) و کارت شبکه فیزیکی قرار می‌گیرد، به کل حافظه‌ی فیزیکی دسترسی داشته باشد. کارت شبکه فیزیکی می‌تواند به‌صورت غیرمستقیم از طریق DMA و بدون کنترل ابرناظر به حافظه دسترسی داشته باشد.



شکل ۱۱ دو راه برای دسترسی به حافظه در معماری مجازی‌سازی

با استفاده از این حمله این امکان وجود دارد که هم صحت و هم محرمانگی ابرناظر و تمام VMهای در حال اجرا بر روی حافظه فیزیکی، نقض شود. همچنین، این حمله می‌تواند منجر به جلوگیری از سرویس[۲۱] شود (دسترس‌پذیری)، زیرا می‌تواند اختلال در کار ابرناظر و تمام VMها به‌وجود آورد، به‌عنوان مثال با حذف فضای هسته حافظه یک VM.

۳-۲-۲ حمله جلوگیری از سرویس

حمله جلوگیری از سرویس تلاش دارد که منابع را از دسترس کاربران خارج سازد. این حمله بیشتر از طریق شبکه‌های کامپیوتری انجام می‌شود، ولی به آن محدود نمی‌شود، و همچنین می‌تواند در رابطه با منابعی مانند مدیریت منابع CPU انجام گیرد. این کار را می‌توان با ارسال سیل‌آسای درخواست‌های ارتباط به سیستم انجام داد که منابع آن را مصرف می‌کنند، و باعث می‌شود که توانایی پاسخ‌دادن به ترافیک قانونی را نداشته باشد و یا آن‌قدر آهسته پاسخ داده شود که قابل ارائه نباشد. در مجازی‌سازی به دلیل به‌اشتراک‌گذاری منابع فیزیکی مانند CPU، حافظه و شبکه بین VMها و میزبان، یک VM می‌تواند حمله جلوگیری از سرویس را به سایر VMهای همان میزبان تحمیل کند. این کار با گرفتن و مصرف‌کردن تمام منابع ممکن سیستم قابل انجام است

[۲۱] Denial of Service

که در نتیجه آن‌ها را برای سایر VMها غیرقابل دسترس می‌سازد. بنابراین حمله جلوگیری از سرویس هم در نتیجه‌ی باگ‌های ابرناظر و هم در نتیجه‌ی حملات شبکه‌ای روی می‌دهد، و یک حمله جلوگیری از سرویس روی ابرناظر همه VMها را تحت تأثیر قرار می‌دهد.

با تخصیص محدود منابع به هر VM می‌توان تا اندازه‌ای از این حمله جلوگیری کرد. معمولاً همه فناوری‌های مجازی‌سازی سازوکارهایی را برای محدودکردن تخصیص منابع به یک VM خاص، ارائه می‌دهند.

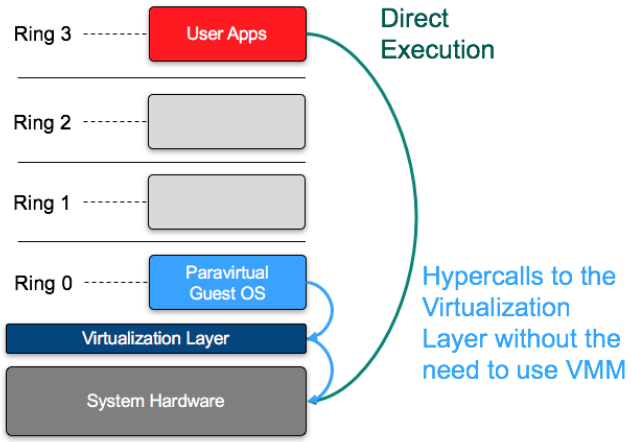
٤-٢-٢ VM Sprawl

مشکل Sprawl در دنیای فناوری اطلاعات جدید نیست. VM Sprawl زمانی اتفاق می‌افتد که منابعی مانند CPU، حافظه و ذخیره‌سازی توسط VMهای بدون استفاده مصرف می‌شوند. این اتفاق در نتیجه‌ی این امر می‌تواند رخ دهد که یک VM به طور غیرضروری و بدون توجیه و تأیید مناسب ایجاد و یا سفارش داده شده باشد. ممکن است این VMها در ابتدا به طور گسترده‌ای مورد استفاده قرار بگیرند و پس از گذشت زمان برای مدت طولانی غیرفعال شوند، و یا این‌که از همان ابتدا با منابع خیلی زیاد (بیش از حد CPU، حافظه یا دیسک) درخواست داده شده باشند. این مسأله در دنیای مجازی‌سازی حادتر است و دلیل آن سهولت و سرعت درخواست ایجاد VM جدید است. به عبارت دیگر، دنیای مجازی‌سازی پیچیدگی‌های دنیای فیزیکی از قبیل درخواست، تأیید، سفارش سیستم، و سایر کارهایی که مستلزم زمان است را ندارد و می‌تواند این روند را به چند دقیقه کاهش دهد.

راه‌حل‌هایی برای sprawl وجود دارد که برخی از آن‌ها استفاده می‌شود و برخی از آن‌ها پیشنهادی و تحت آزمایش هستند. به طور عمده سیاست‌هایی که مدیران را قادر می‌سازد تا کنترل کنند که چه منابعی و از هر منبع چه مقدار را می‌توان مصرف کرد، به جلوگیری از به‌وجودآمدن این مشکل کمک می‌کنند. همچنین سیاست‌هایی مورد نیاز است برای مشخص‌کردن این‌که پس از انقضای یک VM یا زمانی که یک VM دیگر مورد نیاز نیست چه کاری باید انجام شود. در این مرحله VMها CPU یا حافظه مصرف نخواهند کرد، اما برای مدت زمان لازم بایستی بایگانی شوند و بنابراین فضای ذخیره‌سازی را مصرف خواهند کرد. یک سیاست باید مدت زمانی را تعیین کند که این بایگانی باید نگه داشته شود. این مشکل همچنین برای snapshotها وجود دارد زیرا این snapshotها با گذشت زمان رشد می‌کنند و فضای ذخیره‌سازی بیشتری را مصرف می‌کنند. همچنین می‌توان با خودکارسازی فرآیند شناسایی ماشین‌های غیرفعال و رهاشده، تصفیه منابع و استفاده مجدد از آن‌ها را انجام داد، و همچنین تعداد ماشین‌های غیرضروری که منابع زیادی در اختیار گرفته‌اند را کاهش داد.

۵-۲-۲ حمله Hypercall

hypercallها درخواست‌های دوسطحی هستند که در محیط‌های paravirtualization برای ارتباط بین VM مهمان و ابرناظر استفاده می‌شود (شکل ۱۲). در حقیقت از hypercallها برای انجام پردازش و دسترسی به منابع استفاده می‌شود.



شکل ۱۲ Hypercallها در محیط Paravirtualization

حمله hypercall یک تله نرم‌افزاری است که از هسته‌ی یک VM مهمان به ابرناظر انجام می‌شود. hypercallهای مخرب با پارامترهایی که خارج از محدوده و یا غیرمنتظره هستند بارگذاری می‌شوند. این hypercallهای مخرب معمولاً بر روی هدر دادن منابع مشترک ابرناظر در حافظه و CPU تمرکز کنند و به این ترتیب سعی در ایجاد شکست در نرم‌افزار میزبان دارند. پس از انجام یک حمله موفق، میزبان نمی‌تواند از VMهای قانونی پشتیبانی کند و منابع مورد نیاز آن‌ها را تأمین نماید. بنابراین حمله hypercall یک حمله جلوگیری از سرویس است که مبتنی بر ارسال تعداد زیادی بسته نیست.

حمله جلوگیری از سرویس مبتنی بر hypercall توسط یک ماشین مجازی مهمان غیر قابل اعتماد آغاز شده و ابرناظر میزبان را هدف قرار می‌گیرد. این حمله از طریق واسط hypercall انجام می‌شود. به‌طور کلی، هدف حمله جلوگیری از سرویس مبتنی بر hypercall این است که توانایی ابرناظر را کم کند تا ابرناظر نتواند از ماشین‌های مجازی مهمان پشتیبانی کند. این نوع حملات در دو دسته‌ی کلی زیر طبقه‌بندی می‌شوند:

- شکست نرم‌افزاری میزبان
- شکست منابع سیستم

۲-۲-۵-۱ شکست نرم‌افزاری میزبان

حملات شکست نرم‌افزاری به‌وسیله‌ی توالی‌هایی از hypercallها ایجاد می‌شوند که یا تصویر میزبان بارگذاری‌شده را خراب می‌کنند، و یا خطاهای استثنا[۲۲] را در ابرناظر راه‌اندازی می‌کنند. سقوط نرم‌افزاری که از مجازی‌سازی پشتیبانی می‌کند منجر به جلوگیری از سرویس برای ماشین‌های مجازی می‌شود.

مهمان‌ها به طور کامل وابسته به مانیتور ماشین‌های مجازی خود هستند تا بتوانند حافظه، پردازش، شبکه و ذخیره‌سازی را به کار گیرند. ابرناظرها با استفاده از hypercallها و وقفه‌ها با مهمانان ارتباط برقرار می‌کنند تا بتوانند عملیات خود را انجام دهند. هرگونه وقفه در این سرویس‌ها به شکست مهمان منتهی می‌شود. با توجه به میزان وابستگی مهمان‌ها به ابرناظرها برای حفظ عملکردشان، مهاجمان ممکن است صحت تصویر بارگذاری‌شده‌ی میزبان را خراب کنند یا از خطاهای استثنا در کد سیستم استفاده کنند. این حملات توسط ماشین‌های مجازی مخرب با استفاده از واسط hypercall انجام می‌شود.

۲-۲-۵-۲ شکست منابع سیستم

حملات این دسته به‌وسیله‌ی توالی‌های hypercall رخ می‌دهد که حافظه میزبان و/یا تخصیص‌های پردازنده را از بین می‌برد. به این ترتیب مهمان‌ها جلوگیری از سرویس را تجربه خواهند کرد.

دو اصل اصلی در مجازی‌سازی، انتزاع منابع فیزیکی به مجازی و تقسیم منابع مجازی در میان ابرناظر و تمام ماشین‌های مجازی تحت پوشش آن است. سیستم‌عامل میزبان و هر مهمان یک سهم از منابع را دریافت می کنند و نمی‌توانند آن را به بیشتر از منابع تخصیص‌یافته به خود گسترش دهند. این کار، در شرایط عادی، مانع ار تأثیرگذاری عملکرد یک منبع بر دیگران می‌شود. اما مهاجمان روش‌هایی را پیدا کرده‌اند که منابع مجازی اختصاص یافته به میزبان را مصرف می‌کنند. مهاجمان از واسط hypercall به عنوان یک بردار ورودی استفاده می‌کنند، زیرا این واسط امکان دسترسی غیرمستقیم به سخت افزار سیستم را فراهم می‌کند.

[۲۲] Exception errors

۲-۳ تهدیدات شبکه مجازی

تمامی تهدیدات و حملات مربوط به شبکه‌های فیزیکی در شبکه‌های مجازی نیز وجود دارند. از جمله این حملات می‌توان به حملات پویش[۲۳]، شنود[۲۴]، مردی در میانه[۲۵]، جلوگیری از سرویس و غیره اشاره کرد. در ادامه به صورت مختصر در مورد برخی از این حملات در محیط مجازی صحبت می‌کنیم.

۲-۳-۱ شنود ترافیک شبکه

در محیط‌های مجازی هر ماشین مجازی برخی منابع را به اشتراک می‌گذارد که این می‌تواند یک نقطه مناسب برای حمله باشد. لینک‌های فیزیکی ناامن می‌توانند یک سکو برای شنود را ارائه دهند. در محیط مجازی تعامل بین مهمان‌ها با استفاده از هاب یا سوئیچ مجازی انجام می‌شود. اگر هاب پیاده‌سازی شود، مهاجم می‌تواند بسته ها را در ارتباطات شبکه مورد حمله قرار دهد. در مورد استفاده از سوئیچ مجازی نیز می‌تواند از ARPهای جعلی استفاده کند. همان‌گونه که در شکل ۱۳ نشان داده شده است، مهاجم با قرار دادن کارت شبکه سیستم خود در حالت بی‌قاعده[۲۶] می‌تواند یک نسخه از تمام بسته‌هایی که از سوئیچ عبور می‌کنند را دریافت کند و به این ترتیب شنود ترافیک شبکه را انجام دهد. علاوه بر این، برخی سوئیچ‌های مجازی (به‌عنوان مثال سوئیچ‌های مجازی در VMware ESXi) خود حالت بی‌قاعده را پشتیبانی می‌کنند. به این مفهوم که با فعال‌کردن این حالت برای سوئیچ، تمام ترافیک عبوری از آن توسط تمام ماشین‌های مجازی متصل به آن قابل مشاهده می‌باشد. در صورت فعال‌بودن این گزینه شنود ترافیک برای ماشین مجازی مهاجم بسیار آسان است. بنابراین بایستی دقت شود که این گزینه تنها در موارد ضروری فعال شود.

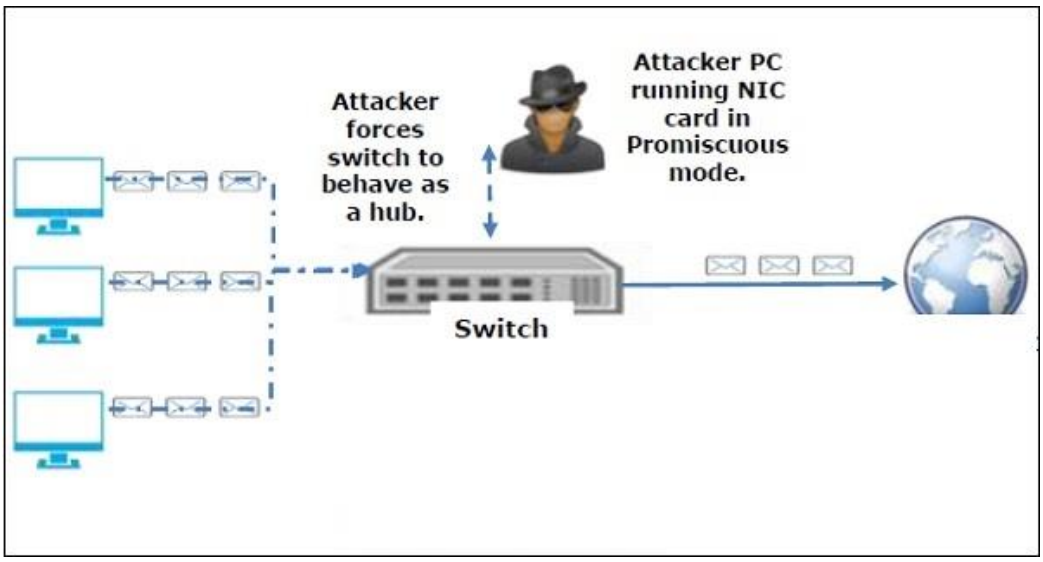
---

[۲۳] Scanning

[۲۴] Sniffing

[۲۵] Man In the Middle

[۲۶] Promiscuous mode



شکل ۱۳ شنود ترافیک شبکه

۲-۳-۲ آسیب‌پذیری‌های مدیریت از راه دور

میزبان‌ها معمولاً یک کنسول مدیریتی دارند که ماشین‌های مجازی را مدیریت می‌کنند. این کنسول به انجام کارهای مدیریتی کمک می‌کند و در عین حال ممکن است هدف حمله قرار گیرد. با مورد حمله قرار گرفتن این کنسول مهاجم به‌آسانی می‌تواند تمام ماشین‌های مجازی را کنترل کند.

۲-۳-۳ حمله مردی در میانه

در این حمله، مانند شبکه‌های فیزیکی، مهاجم در بین ارتباط بین سرویس‌دهنده و سرویس‌گیرنده قرار می‌گیرد و می‌تواند داده‌های جعلی را به ارتباط تزریق کند. در ادامه در مورد دو نوع حمله مردی در میانه در محیط مجازی صحبت می‌کنیم.

۲-۳-۳-۱ حمله SSL MiTM

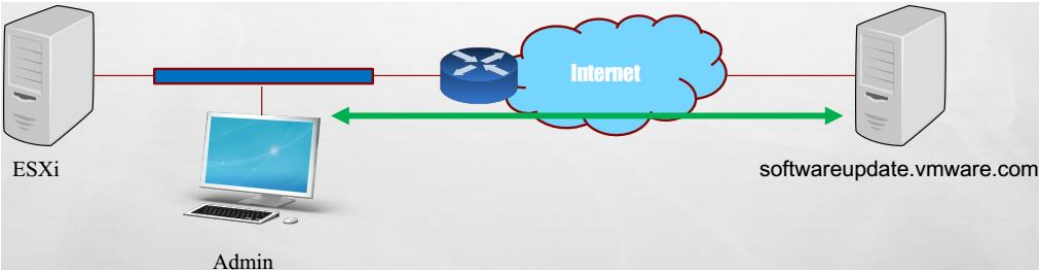
یک حمله تزریق گواهی‌نامه است که در آن مهاجم در یک ارتباط باز بین یک سرویس‌گیرنده و یک سرویس‌دهنده SSL قرار گرفته و گواهینامه خود را، به جای گواهینامه اصلی، به جریان ارتباط تزریق می‌کند (شکل ١٤). این حمله بیش از هر چیز دیگری به نحوه مدیریت محیط مجازی بستگی دارد. اگر محیط مدیریتی در شبکه پخش باشد کنترل این حمله سخت‌تر می‌شود. این حمله یکی از دلایلی است که VMware و دیگر متخصصان امنیتی توصیه می‌کنند که شبکه مدیریتی را کاملاً کنترل کنید و هیچ مدیرتی را خارج از شبکه مدیریتی قرار ندهید. به طور خاص، هر چیزی که اجازه دسترسی مستقیم به ابزار مدیریت مجازی‌سازی از

طریق اینترنت را بدهد خطرناک است. بنابراین توصیه می‌شود که برای مدیریت از راه دور از یک پروکسی محلی استفاده شود.

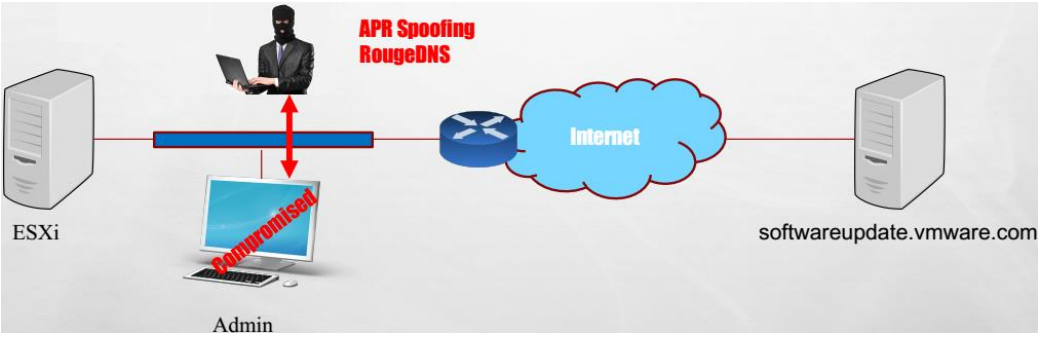
شکل ۱۴ تزریق گواهینامه‌ی جعلی به جای گواهینامه‌ی اصلی با حمله مردی در میانه

۲-۳-۳-۲ به‌روزرسانی جعلی نرم‌افزار مدیریت

هنگامی که یک میزبان قصد دریافت به‌روزرسانی‌های نرم‌افزاری مربوط به ابرناظر را دارد، مهاجم ممکن است در بین ارتباط بین میزبان و سرویس‌دهنده مربوط قرار گرفته و به‌روزرسانی‌های جعلی خود را به ارتباط تزریق نماید (شکل ۱۵).



(الف)



(ب)

شکل ۱۵ به‌روزرسانی نرم‌افزار مدیریت، (الف) حالت اصلی، (ب) حمله مردی در میانه

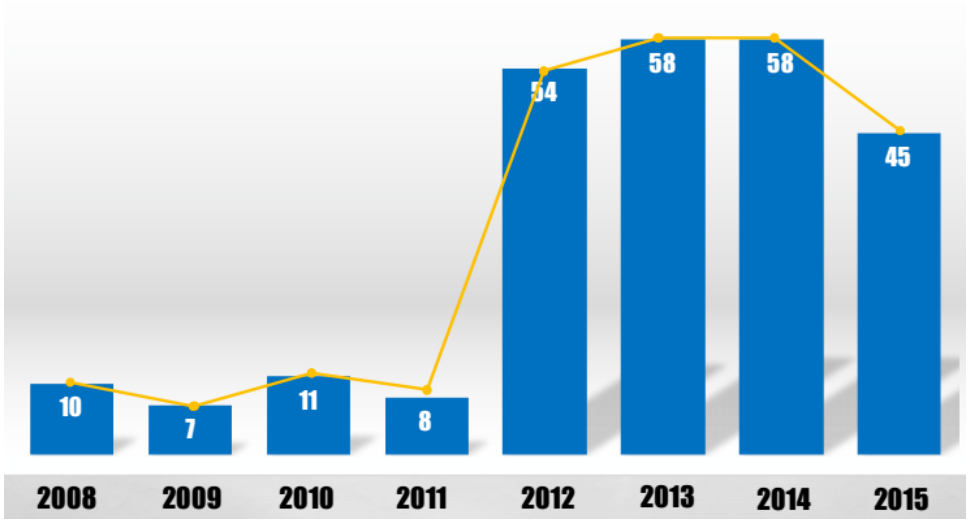
۳ آسیب‌پذیری‌های محیط مجازی

آسیب‌پذیری‌های مختلفی در سکوهای مختلف مجازی‌سازی گزارش شده است که در این میان آسیب‌پذیری های مربوط به VMware اهمیت بیشتری دارند به دلیل این‌که VMware سهم بیشتری از بازار را در اختیار دارد.

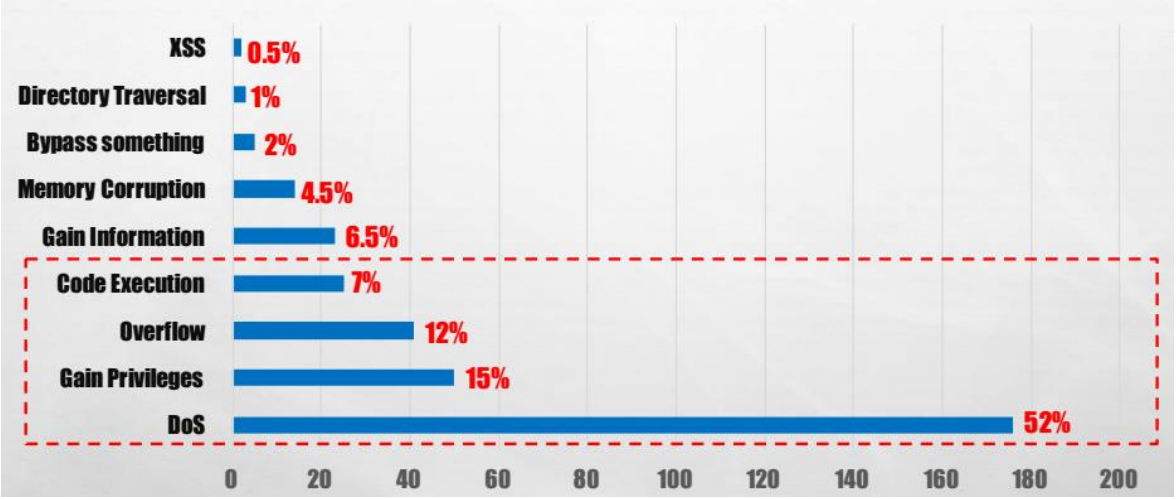
متأسفانه، علیرغم پیشرفت‌هایی که در زمینه‌ی مجازی‌سازی سخت‌افزار و استفاده از عملکردهای مختلف در هسته‌های سیستم‌عامل میزبان به وجود آمده است، ابرناظرهایی مانند Xen و VMware ESXi، کد پایه‌ی زیاد و پیچیده‌ای دارند، و بنابراین سطح حمله بالقوه‌ی گسترده‌ای را دارا می‌باشند. علاوه بر این، در این کدها، چندین مؤلفه نسبتاً پیچیده هستند، مانند مجازی‌سازی حافظه و تقلید دستورالعمل‌های مهمان، که اغلب آسیب‌پذیری‌های مختلف قابل بهره‌برداری را ارائه می‌دهند.

با انتقال‌دادن مکانیزم حفاظت به سطوح پایین‌تر، مهاجمان باید تلاش بیشتری را برای پنهان کردن فعالیت‌های خود انجام دهند. این موضوع برای مهاجمان نیز درست است، به همین دلیل تلاش می‌کنند تا به سطح ابرناظر برسند تا بتوانند همه‌ی ماشین‌های مجازی را کنترل کنند. بنابراین بین مهاجمانی که تلاش برای حمله می‌کنند و محافظانی که تلاش برای حفاظت می‌کنند، یک مسابقه برای حرکت به پایین‌ترین سطح ممکن وجود دارد. فرض اساسی برای قرار دادن یک مکانیزم حفاظتی در ابرناظرها این است که آن‌ها معمولاً بر پایه‌ی کدی هستند که بسیار کوچک‌تر از سیستم‌عامل‌های معمولی است، و دارای اشکالات (آسیب‌پذیری‌های) کمتری هستند و سخت‌تر دچار انحراف می‌شوند.

شکل ۱۶ تعداد آسیب‌پذیری‌های گزارش شده در ابرناظرهای Bare-metal را در بازه‌ی زمانی ۲۰۰۸ تا ۲۰۱۵ میلادی نشان می‌دهد. در شکل ۱۷ این آسیب‌پذیری‌ها بر اساس نوع آسیب‌پذیری تقسیم‌بندی شده‌اند. همان‌گونه که مشاهده می‌شود بیشتر از نیمی از آسیب‌پذیری‌ها منجر به حمله جلوگیری از سرویس می‌شوند. همان‌طور که در بخش قبل توضیح دادیم حملات جلوگیری از سرویس یکی از اصلی‌ترین حملات در محیط‌های مجازی هستند. دلیل این امر این است که علاوه بر روش‌هایی که برای انجام این نوع از حملات در شبکه‌های فیزیکی وجود دارد، که در شبکه‌های مجازی نیز این روش‌ها قابل استفاده هستند، مهاجم به هر طریقی که بتواند به ابرناظر دسترسی پیدا کند و مانع از ارائه سرویس‌های ابرناظر به ماشین‌های مجازی قانونی شود و یا ارائه‌ی سرویس به آن‌ها را با اختلال مواجه کند، یک حمله جلوگیری از سرویس اتفاق افتاده است.



شکل ۱۶ آسیب‌پذیری‌های گزارش شده در ابرناظرهای Bare-metal را در بازه‌ی زمانی ۲۰۰۸ تا ۲۰۱۵ میلادی



شکل ۱۷ آسیب‌پذیری‌های گزارش شده در ابرناظرهای Bare-metal را در بازه‌ی زمانی ۲۰۰۸ تا ۲۰۱۵ میلادی (براساس نوع آسیب‌پذیری)

در بازه‌ی زمانی بین ژانویه ۲۰۱۲ و ژوئن ۲۰۱۵ میلادی، NVD[۲۷] تعداد ۳۸ آسیب‌پذیری با شدت بالاتر از ۷، که در درجه High قرار می‌گیرند، را برای ابرناظرها گزارش داد. آسیب‌پذیری‌های با درجه High از نظر امنیتی بسیار حیاتی هستند. این آسیب‌پذیری‌ها در جدول ۱ نشان داده شده‌اند. همان‌طور که در این جدول مشاهده

[۲۷] National Vulnerability Database

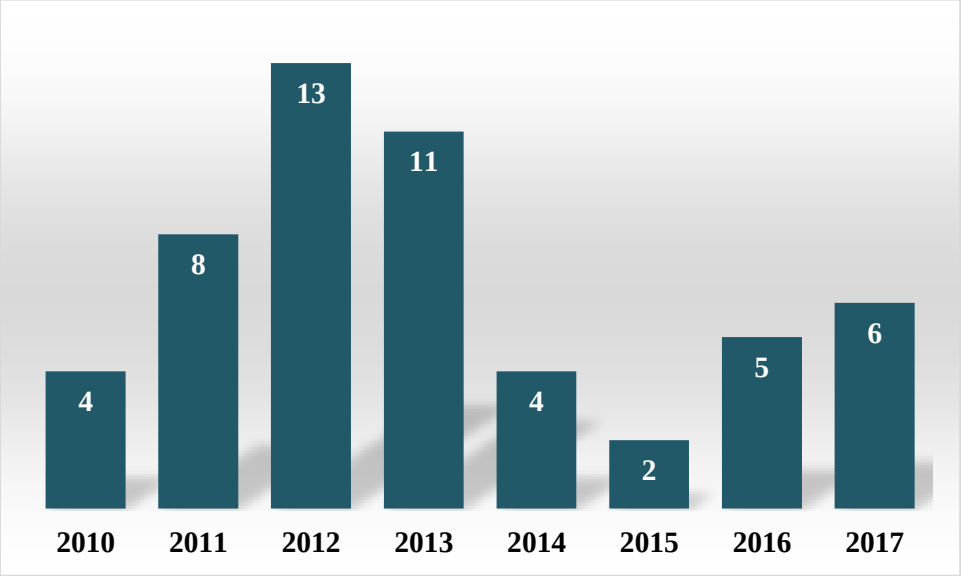
می‌شود، ۱۸ آسیب‌پذیری برای Xen، ۱۸ آسیب‌پذیری برای VMware ESXi، ۱ آسیب‌پذیری برای Hyper-V و ۲ آسیب‌پذیری برای KVM (که یکی از آن‌ها با Xen مشترک است) گزارش شده است. برخی از این آسیب‌پذیری‌ها به مهاجم این امکان را می‌دهند که به صورت مستقیم و به‌عنوان مثال با فرار از یک VM، ابرناظر را مورد تهدید قرار دهد. وقتی که یک ابرناظر مورد حمله قرار گرفت مهاجم می‌تواند کنترل همه VMهای قرار گرفته بر روی این ابرناظر را در دست گرفته و در سرویس‌های آن‌ها اختلال به وجود آورده و یا داده‌های محرمانه هر VM را مورد تهدید قرار دهد. همچنین در جدول ۱ نشان داده شده است که هر یک از آسیب‌پذیری‌ها کدام‌یک از ویژگی‌های محرمانگی، صحت، و دسترس‌پذیری را مورد حمله قرار داده‌اند. مشاهده می‌شود که همه‌ی آسیب‌پذیری‌ها بر ویژگی دسترس‌پذیری تأثیر داشته‌اند.

جدول ۱ آسیب‌پذیری‌های با درجه High در ابرناظرهای مختلف بین سال‌های ۲۰۱۲ تا ۲۰۱۵ میلادی

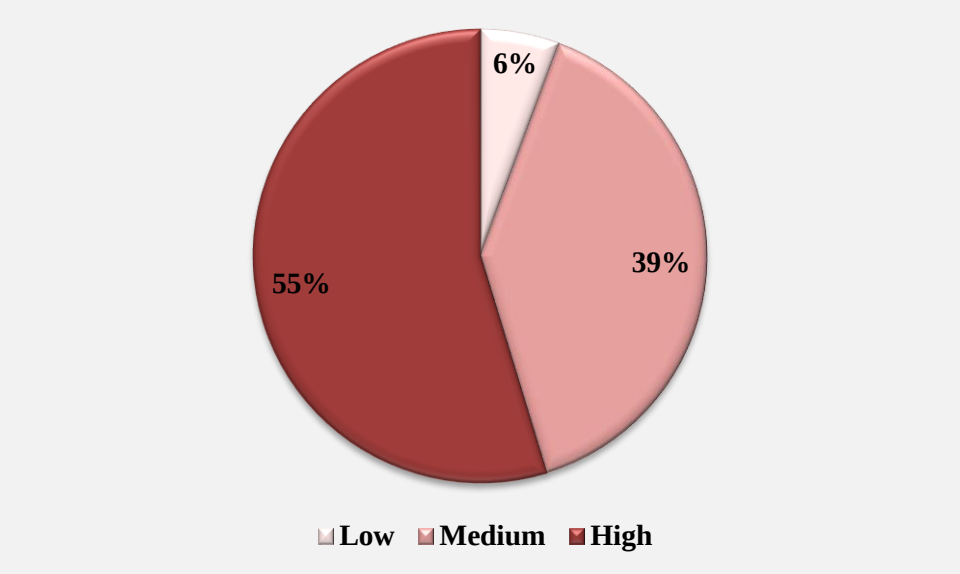
محصول	CVE ID	نوع آسیب‌پذیری	محرمانگی	صحت	دسترس‌پذیری
ESXi	CVE-2013-5970	DoS	_	_	✓
ESXi	CVE-2013-3658	Dir. Trav.	_	✓	✓
ESXi	CVE-2013-3657	DoS Exec Code Overflow	✓	✓	✓
ESXi	CVE-2013-3519	+Priv	✓	✓	✓
ESXi	CVE-2013-1659	DoS Exec Code Mem. Corr.	✓	✓	✓
ESXi	CVE-2013-1406	+Priv	✓	✓	✓
ESXi	CVE-2013-1405	DoS Exec Code Mem. Corr.	✓	✓	✓
ESXi	CVE-2012-3289	DoS	_	_	✓
ESXi	CVE-2012-3288	DoS Exec Code Mem. Corr.	✓	✓	✓
ESXi	CVE-2012-2450	DoS Exec Code	✓	✓	✓
ESXi	CVE-2012-2449	DoS Exec Code Overflow	✓	✓	✓
ESXi	CVE-2012-2448	DoS Exec Code Overflow	✓	✓	✓
ESXi	CVE-2012-1518	+Priv	✓	✓	✓
ESXi	CVE-2012-1517	DoS Exec Code Overflow	✓	✓	✓
ESXi	CVE-2012-1516	DoS Exec Code Overflow	✓	✓	✓
ESXi	CVE-2012-1515	+Priv	✓	✓	✓
ESXi	CVE-2012-1510	Overflow +Priv	✓	✓	✓
ESXi	CVE-2012-1508	DoS +Priv	✓	✓	✓
Xen	CVE-2015-4104	DoS	_	_	✓

✓	✓	✓	DoS Exec Code Overflow	CVE-2015-3456	**Xen**
✓	✓	✓	Exec Code Overflow	CVE-2015-3209	**Xen**
✓	_	_	DoS	CVE-2015-2751	**Xen**
✓	✓	✓	DoS Exec Code Mem. Corr. +Info	CVE-2015-2151	**Xen**
✓	_	_	DoS	CVE-2015-0361	**Xen**
✓	_	_	DoS	CVE-2014-9030	**Xen**
✓	✓	✓	DoS	CVE-2014-7188	**Xen**
✓	✓	✓	+Priv	CVE-2014-3969	**Xen**
✓	✓	✓	DoS +Priv	CVE-2014-1666	**Xen**
✓	✓	✓	DoS +Priv	CVE-2013-6375	**Xen**
✓	✓	✓	Other	CVE-2013-2211	**Xen**
✓	✓	✓	DoS Overflow +Priv Mem. Corr.	CVE-2013-2072	**Xen**
✓	✓	✓	DoS +Priv	CVE-2013-1432	**Xen**
✓	✓	✓	DoS	CVE-2012-6030	**Xen**
✓	✓	✓	+Priv	CVE-2012-3515	**Xen**
✓	✓	✓	Overflow +Priv	CVE-2012-0217	**Xen**
✓	✓	✓	DoS +Priv	CVE-2011-1763	**Xen**
✓	✓	✓	DoS Exec Code Mem. Corr.	CVE-2013-3898	**Hyper-V**
✓	✓	✓	DoS Exec Code Overflow	CVE-2015-3456	**KVM**
✓	✓	✓	DoS Overflow +Priv	CVE-2011-2212	**KVM**

با توجه به اهمیت بیشتر ابرناظر VMware ESXi، به‌دلیل گستردگی استفاده از آن، در شکل ۱۸ تعداد آسیب‌پذیری‌های گزارش شده توسط NVD برای این ابرناظر، در بازه‌ی زمانی ۲۰۱۰ میلادی تا کنون، نشان داده شده است. همچنین شکل ۱۹ درصد این آسیب‌پذیری‌ها را براساس درجه اهمیت آن‌ها (Low، Medium و High) نشان می‌دهد.



شکل ۱۸ آسیب‌پذیری‌های گزارش شده توسط NVD برای ابرناظر VMware ESXi، در بازه‌ی زمانی ۲۰۱۰ میلادی تا کنون



شکل ۱۹ درصد آسیب‌پذیری‌های گزارش شده توسط NVD برای ابرناظر VMware ESXi، در بازه‌ی زمانی ۲۰۱۰ میلادی تا کنون، براساس درجه اهمیت آن‌ها