به نام او

# راهنمای کاربردی کالی لینوکس

ساختاری برای تست نفوذ

محمدعلی (ارسلان) الیاسی

انتشارات پندار پارس

سرشناسه : الیاسی، محمدعلی، ۱۳۷۸-
عنوان و نام پدیدآور : راهنمای کاربردی Kali Linux/ [ترجمه و تالیف] محمدعلی الیاسی.
مشخصات نشر : تهران : پندار پارس، ۱۴۰۲.
مشخصات ظاهری : ۴۶۰ ص.: مصور، جدول.
شابک : - - - -
وضعیت فهرست نویسی : فیپا
موضوع : کالی لینوکس
Kali Linux
موضوع : آزمایش نفوذ ( ایمن‌سازی کامپیوتر)
Penetration testing (Computer security)
شبکه‌های کامپیوتری -- تدابیر ایمنی
Computer networks -- Security measures
رده بندی کنگره : QA۷۶/۹
رده بندی دیویی : ۰۰۵/۸
شماره کتابشناسی ملی : ۹۱۶۶۳۱۲
اطلاعات رکورد کتابشناسی : فیپا

***انتشارات پندارپارس***

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

تلفن: ۶۶۵۷۲۳۳۵ - تلفکس: ۶۶۹۲۶۵۷۸ همراه: ۰۹۱۲۲۴۵۲۳۴۸ **info@pendarepars.com**

**نام کتاب : راهنمای کاربردی Kali Linux**

**ناشر : انتشارات پندار پارس**

**ترجمه و تالیف : محمدعلی الیاسی**

**چاپ نخست : اردیبهشت ۱۴۰۲**

**شمارگان : ۱۰۰ نسخه دیجیتال**

**طرح جلد : رامین شکرالهی**

**چاپ، صحافی : روز**

**قیمت : ۳۵۰.۰۰۰ تومان** **شابک : ۶-۱۶-۷۷۸۵-۶۲۲-۹۷۸**

# دیباچه

این کتاب در مورد استفاده از کالی لینوکس در انجام تست‌های نفوذ علیه شبکه‌ها، سیستم‌ها و برنامه‌ها می‌باشد. تست نفوذ، یک حمله را علیه یک شبکه یا یک سیستم توسط یک خارجی یا خودی مخرب شبیه‌سازی می‌کند. برخلاف ارزیابی آسیب‌پذیری، تست نفوذ طوری طراحی شده است که شامل مرحله اکسپلویت (بهره‌برداری) باشد. بنابراین، ثابت می‌کند که بهره‌برداری وجود دارد و اگر برطرف نشود، در سیستم رخنه شده است.

به طور خلاصه، این کتاب شما را در سفری از یک آزمونگر نفوذ با بسیاری از تکنیک‌های اثبات‌شده برای شکست دادن جدیدترین دفاع‌ها در یک شبکه با استفاده از کالی لینوکس راهنمایی می‌کند. از انتخاب مؤثرترین ابزار، رخنه کردن در شبکه تا برجسته کردن تکنیک‌های مورد استفاده برای جلوگیری از شناسایی.

### این کتاب برای چه کسی است

اگر شما یک آزمونگر نفوذ، متخصص فناوری اطلاعات یا مشاور امنیتی هستید که می‌خواهید با استفاده از برخی از ویژگی‌های پیشرفته کالی لینوکس، موفقیت آزمایش شبکه خود را به حداکثر برسانید، این کتاب برای شما مناسب است. آشنایی قبلی با اصول اولیه تست نفوذ/هک قانونمند برای استفاده حداکثری از این کتاب مفید خواهد بود.

باید سیستم‌عامل کالی لینوکس و مجموعه ابزارهای آن را دانلود و پیکربندی کنید. برای اطمینان از به‌روز بودن و داشتن تمام ابزارها، باید به اینترنت دسترسی داشته باشید.

متأسفانه، به همه ابزارهای سیستم کالی لینوکس پرداخته نمی‌شود زیرا تعداد آنها بسیار زیاد است. تمرکز این کتاب این نیست که شما را با همه ابزارها و گزینه‌ها غرق کند، بلکه رویکردی برای تست نفوذ ارائه می‌کند که به شما این امکان را می‌دهد، با بدست آوردن تجربیات و دانش در طول زمان، ابزارهای جدید را یاد بگیرید و ترکیب کنید.

اگرچه بیشتر نمونه‌های این کتاب بر روی مایکروسافت ویندوز متمرکز است، روش‌شناسی و بیشتر ابزارها قابل انتقال به سیستم‌عامل‌های دیگر مانند لینوکس و دیگر مدل‌های یونیکس هستند.

در پایان، این کتاب، کالی‌لینوکس را برای تکمیل زنجیره کشتار سایبری علیه سیستم‌های هدف پیاده‌سازی می‌کند. شما به یک سیستم عامل هدف نیاز دارید. در بسیاری از مثال‌های موجود در کتاب از Microsoft Windows 2016، Windows 10، Ubuntu 14.04 و Windows 2008 R2 استفاده شده است.

***توجه***: مجموعه کتاب‌های زیر توسط انتشارات پندارپارس به چاپ رسیده است که هر کدام در فصل‌های جداگانه در این کتاب استفاده شده است:

| عنوان | تألیف/ترجمه |
|---|---|
| - راهنمای پویش آسیب‌پذیری و تست نفوذ با NESSUS | احسان نیک‌آور |
| - آموزش تست نفوذ با Metasploit Framework | مجید داوری دولت‌آبادی |
| - تزریقSQL ، حمله و دفاع | محسن کجباف |
| - نگاه عمیق به بسته‌های شبکه با استفاده از Wireshark | محسن مصطفی جوکار |
| - تکنیک‌های عملیاتی تست نفوذ مبتنی برRed Team | مجید داوری دولت‌آبادی |

برای دسترسی به بیش از ۳۰ عنوان کتاب هک و امنیت، در سایت pendarepars.com، از دسته‌بندی کتاب‌ها وارد دسته "امنیت" شوید.

**فهرست**

# فصل ۱
# تست نفوذ هدفمند

جهان، پیوسته در حال تغییر است و ما دائما با فناوری‌های نوین و پیشرفت‌ها طرف هستیم و فعالیت ما در یک دنیای متصل  با فناوری جدید، در دسترس برای کار و زندگی شخصی افراد، بسیار مهم شده است. مطمئناً می‌توانیم این را یک دنیای مجازی بنامیم، جایی که فعالیت‌های محرمانه‌ای که قبلاً در اتاق‌های بسته اتفاق می‌افتاد اکنون از طریق اینترنت انجام می‌شود. این به طور قابل توجهی تعداد تهدیدهای سایبری را حداقل تا پنج برابر افزایش داده است. بازیگران تهدید از این تحول دیجیتالی برای بهره‌برداری از اشتباه‌های کاربران و شرکت‌ها به عنوان نقطه ورود خود برای سود مالی، آسیب رساندن به شهرت یا هر هدف دیگری استفاده می‌کنند. این به شکل باج افزار، فیشینگ و نشت اطلاعات رخ می‌دهد.

برای درک روش‌های کنونی و آینده کار، اجازه دهید با بررسی اهداف یا انگیزه‌های مختلف بازیگران تهدید شروع کنیم. در این فصل، انواع مختلف بازیگران تهدید و اهمیت تست نفوذ هدفمند را با مجموعه‌ای از اهداف مورد بحث قرار خواهیم داد. ما تصورات غلط و اینکه چگونه ممکن است یک اسکن آسیب‌پذیری معمولی، تست نفوذ، و تمرین رد تیم موفقیت آمیز نباشد را بررسی می‌کنیم. این فصل همچنین مروری بر تست امنیتی و راه‌اندازی یک آزمایشگاه با تمرکز بر سفارشی‌سازی کالی برای پشتیبانی از برخی جنبه‌های پیشرفته تست نفوذ خواهد داشت. در پایان این فصل، موارد زیر را پوشش خواهیم داد:

- ✓ انواع مختلف عوامل تهدید
- ✓ مروری بر تست امنیتی
- ✓ تصورات غلط پیرامون اسکن آسیب‌پذیری، تست نفوذ و تمرین‌های رد تیم
- ✓ تاریخچه و هدف کالی لینوکس
- ✓ به‌روز رسانی و سازماندهی کالی
- ✓ نصب Kali در سرویس‌های مختلف (سرویس‌های وب آمازون/ Google Cloud Platform/Android)
- ✓ تنظیم اهداف تعریف شده

بگذارید با انواع بازیگران تهدید که از زیرساخت‌های فناوری بهره‌برداری می‌کنند آغاز کنیم.

## ۱-۱ انواع مختلف بازیگران تهدید

عامل تهدید چیزی نیست جز یک نهاد یا فردی که مسئول یک رویداد یا حادثه‌ای است که نهاد دیگری را تحت تأثیر قرار می‌دهد. این مهم است که انواع مختلف بازیگران تهدید و انگیزه‌های مشترک آنها را درک کنیم، که به ما در درک دیدگاه‌های مختلف در این کتاب کمک می‌کند. جدول زیر، عوامل تهدید رایج، انگیزه‌های آنها و اهداف معمول را نشان می‌دهد.

| بازیگر تهدید | انگیزه مشترک | هدف(ها) |
|---|---|---|
| بازیگران تحت حمایت دولت | برنامه‌های نظامی، سیاسی و فناوری | جاسوسی سایبری، سرقت داده‌ها، یا هر فعالیت دیگری که یک ملت برای منافع اقتصادی به آن مورد، علاقه دارد |
| جرایم سازمان یافته یا مجرمان سایبری | سود مالی | پول و داده‌های ارزشمند |
| هکتیویست‌ها/ افراط گرایان سایبری | اشتراک‌های انگیزشی | تمرکز بر افشای اسرار و ایجاد اختلال در خدمات/سازمان‌هایی که فکر می‌کنند برای جامعه خوب نیستند (هکتیویست‌ها). تمرکز بر ایجاد آسیب و تخریب برای پیشبرد اهداف خود (افراطی‌ها) |
| تهدیدهای داخلی (Insiders) | انتقام | پرداخت باج یا داده یا سبب کاهش درآمد شدن |

**عوامل مختلف تهدید و انگیزه‌های آنها**

اکنون چهار عامل اصلی تهدید و انگیزه‌های آنها را که می‌توانیم در تست نفوذ هدفمند و تمرین‌های رد تیم برای شبیه‌سازی سناریوهای تهدید واقعی استفاده کنیم، خلاصه کرده ایم.

## ۱-۲ نمای کلی مفهومی تست امنیت

اکنون که عوامل مختلف تهدید را درک می‌کنیم بیایید جلو برویم و بفهمیم که سازمان‌ها از چه چیزی و از چه کسی محافظت می‌کنند؟ اگر از ۱۰۰ مشاور امنیتی این سوال را بپرسید که تست امنیتی چیست، به احتمال زیاد ۱۰۰ پاسخ مختلف دریافت خواهید کرد.

در ساده‌ترین شکل، تست امنیتی فرآیندی است برای تعیین اینکه یک دارایی یا سیستم اطلاعاتی محافظت شود و عملکرد آن همانطور که در نظر گرفته شده است حفظ شود.

## ۳-۱ مشکلات رایج ارزیابی آسیب‌پذیری، تست نفوذ، و تمرین‌های رد تیم

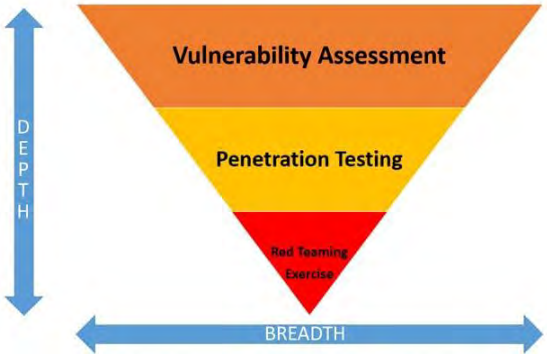
در این بخش، برخی از تصورات نادرست و محدودیت‌های مربوط به اسکن آسیب‌پذیری سنتی/کلاسیک، تست نفوذ و تمرین‌های رد تیم را مورد بحث قرار خواهیم داد. اینک بیایید معنای واقعی این سه موضوع را به زبان ساده و با محدودیت‌های آنها درک کنیم:

- **ارزیابی آسیب‌پذیری (VA)**: فرآیند شناسایی آسیب‌پذیری‌ها یا حفره‌های امنیتی در یک سیستم یا شبکه از طریق یک اسکنر آسیب‌پذیری. یکی از تصورات غلط در مورد VA این است که به شما امکان می‌دهد تمام آسیب‌پذیری‌های شناخته شده را پیدا کنید. خب این درست نیست؛ محدودیت‌های VA شامل این است که فقط آسیب‌پذیری‌های بالقوه یافت شوند و این کاملاً به نوع اسکنر مورد استفاده شما بستگی دارد. همچنین ممکن است شامل تعدادی از موارد مثبت کاذب باشد و برای صاحب کسب و کار، هیچ نشانه روشنی وجود ندارد که کدام یک زمینه‌ساز یک خطر می‌شود و مهاجمان از کدام یک در ابتدا برای دسترسی استفاده خواهند کرد. بزرگترین دام ارزیابی آسیب‌پذیری، حس منفی‌های کاذب است، به این معنی که اسکنر، مشکلی را که سیستم یا برنامه دارد پیدا نکرده است.
- **تست نفوذ (pentesting)**: فرآیند شبیه‌سازی ایمن سناریوهای هک با بهره‌برداری از آسیب‌پذیری‌ها بدون تأثیر زیاد بر شبکه یا تجارت موجود. همچنین تعداد کمتری از موارد مثبت کاذب وجود دارد زیرا آزمایش‌کنندگان سعی می‌کنند آسیب‌پذیری‌ها را تأیید کنند و همچنین تلاش می‌کنند از آنها بهره‌برداری کنند. محدودیتی که در پنتست وجود دارد این است که فقط از اکسپلویت‌های شناخته شده فعلی و در دسترس عموم استفاده می‌کند. بیشتر، این‌ها تمرکزی برای آزمایش پروژه هستند. اغلب در طول یک ارزیابی از مدعیان می‌شنویم، هورا! دسترسی روت گرفتم – اما ما هرگز این سوال را نمی‌شنویم که با آن چه کاری می‌توانید انجام دهید؟ این می‌تواند به دلایل مختلفی مانند محدودیت‌های پروژه، از جمله گزارش مسائل پرخطر بلافاصله به کلاینت باشد، یا اینکه کلاینت فقط به یک بخش از شبکه علاقه‌مند است و فقط می‌خواهد آن قسمت آزمایش شود.

***نکته***: یکی از تصورات غلط در مورد پنتست این است که دید کاملی از شبکه را در اختیار مهاجم قرار می دهد و پس از انجام تست نفوذ شبکه ایمن خواهد بود. وقتی مهاجمان آسیب‌پذیری را در فرآیند تجاری برنامه امن شما پیدا کرده باشند، شبکه دیگر ایمن نخواهد بود.

- **تمرین رد تیم (RTE)**: فرآیندی متمرکز برای ارزیابی اثربخشی یک سازمان برای دفاع در برابر تهدیدهای سایبری و بهبود امنیت آن با هر وسیله ممکن. در طول یک RTE، می‌توانیم راه‌های متعددی را برای دستیابی به اهداف/سناریوها و اهداف پروژه کشف کنیم، مانند پوشش کامل فعالیت‌ها با هدف تعریف‌شده پروژه، از جمله فیشینگ (تغییر قربانی برای وارد کردن اطلاعات حساس یا دانلود محتوای مخرب از طریق ایمیل)، ویشینگ (اغوا کردن قربانی برای ارائه یا انجام برخی اقدامات با هدف مخرب از طریق تماس‌های تلفنی)، "واتس‌اپینگ[1] " (درگیر کردن قربانی از طریق پیام رسان واتس‌اپ با هدف مخرب)، وایرلس، انداختن دیسک[2] (USB و SSD)، و تست نفوذ فیزیکی. محدودیت‌های RTEها سناریوهای از پیش تعریف‌شده، محدود به زمان و یک محیط فرضی و نه واقعی هستند. اغلب، RTE با یک حالت کاملاً نظارت شده برای هر تکنیک اجرا می‌شود و تاکتیک‌ها طبق روال اجرا می‌شوند، اما زمانی که یک مهاجم واقعی بخواهد به هدفی دست یابد، اینطور نیست.

شکل زیر، تفاوت بین هر سه فعالیت را از نظر طول و عرض تمرکز نشان می‌دهد:




**سه روش ارزیابی آسیب‌پذیری سیستم‌ها و وسعت و عمق موفقیت آنها**

اغلب، هر سه روش مختلف تست، به اصطلاح هک یا نشت اشاره می‌کنند. ما شبکه شما را هک خواهیم کرد و نقاط ضعف شما را به شما نشان خواهیم داد. اما صبر کنید، آیا کلاینت یا صاحب کسب و کار تفاوت بین این شرایط را درک می‌کند؟ چگونه آن را می‌سنجیم معیارها چیست؟ و چه زمانی متوجه می‌شویم که هک یا نفوذ کامل شده است؟ همه سؤالات فقط به یک چیز اشاره می‌کنند: هدف از تست نفوذ چیست و هدف اصلی در ذهن چیست.

---

[1] WhatsApping
[2] disk drops

## ۱-۴ تست نفوذ هدفمند

هدف اولیه پنتست / تمرین‌های رد تیم تعیین ریسک واقعی، متمایز کردن رتبه ریسک از اسکنر و دادن ارزش ریسک به کسب و کار برای هر دارایی، همراه با ریسک برای تصویر برند سازمان است. این در مورد میزان ریسک آنها نیست. بلکه هدف این است که چقدر آنها در معرض قرار می‌گیرند و چقدر آسان است که از این قرار گرفتن در معرض آسیب‌پذیری، بهره‌برداری کنیم.

تهدیدی که پیدا شده است گاهی واقعاً یک خطر نیست و نیازی به اثبات ندارد. برای مثال، Cross-Site Scripting (XSS) یک آسیب‌پذیری تزریق اسکریپت است که می‌تواند اطلاعات کاربری کاربران را بدزدد. اگر یک کلاینت که یک شرکت تجاری را اداره می‌کند، وب سایتی بروشور داشته باشد که محتوای ثابت را برای کلاینت‌های خود ارائه می‌دهد، در برابر XSS آسیب‌پذیر باشد، ممکن است تأثیر قابل توجهی بر تجارت نداشته باشد. در این مورد، یک کلاینت ممکن است خطر را بپذیرد و با استفاده از یک فایروال وب اپلیکیشن (WAF) برای جلوگیری از حملات XSS، یک طرح برای کاهش آسیب‌پذیری را در دستور کار قرار دهد. با این حال، اگر همین آسیب‌پذیری در وب‌سایت تجاری اصلی آن‌ها شناسایی شود، آنگاه این یک مشکل مهم است که نیاز دارد در اسرع وقت رسیدگی شود؛ زیرا شرکت در معرض خطر از دست دادن اعتماد مشتریان از طریق مهاجمانی است که اطلاعات آنها را سرقت می‌کنند.

تست نفوذ هدفمند، بسته به مشکل خاصی که یک سازمان با آن مواجه است، مبتنی بر زمان است. مثالی از یک هدف این است: ما بیشتر نگران دزدیده شدن داده‌هایمان و جریمه‌های قانونی ناشی از درز این داده‌ها هستیم. بنابراین، در حال حاضر هدف این است که داده‌ها را با بهره‌برداری از یک نقص در سیستم یا با دستکاری کارکنان از طریق فیشینگ به خطر بیاندازیم. گاهی تعجب‌آور خواهد بود که برخی از داده‌های آنها هم‌اینک در دارک وب موجود است. هر هدفی با تاکتیک‌ها، تکنیک‌ها و رویه‌های خاص خود (TTP) همراه است که از هدف اولیه فعالیت تست نفوذ پشتیبانی می‌کند. تمام این متدولوژی‌های مختلف را در طول این کتاب با استفاده از کالی لینوکس بررسی خواهیم کرد.

## ۱-۵ روش شناسی تست

در روش‌شناسی‌ها این امر مدنظر قرار داده می‌شود که چرا یک تست نفوذ انجام می‌شود یا کدام داده‌ها برای کسب‌وکار حیاتی هستند و نیاز به محافظت دارند. در غیاب این مرحله اولیه حیاتی، تست‌های نفوذ تمرکز خود را از دست می‌دهند.

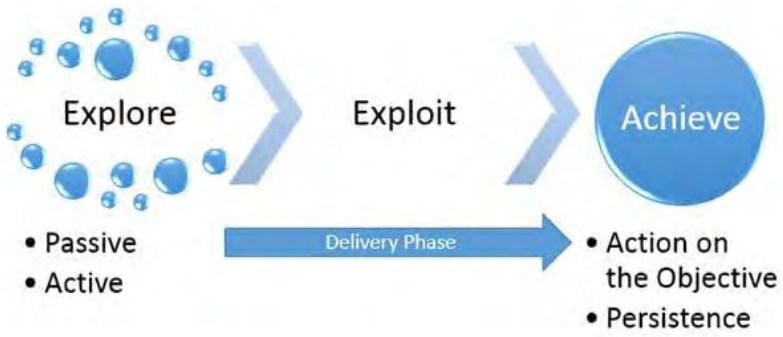
بسیاری از آزمونگرهای نفوذ، تمایلی به پیروی از یک متدولوژی تعریف شده ندارند، زیرا از این می‌ترسند که خلاقیت آنها مانع بهره‌برداری از ضعف امنیتی در شبکه یا برنامه شود. تست نفوذ نمی

تواند فعالیت‌های واقعی یک مهاجم مخرب را منعکس کند. اغلب، کلاینت می‌خواهد ببیند که آیا می‌توانید به یک سیستم خاص دسترسی ادمین داشته باشید (یعنی آیا می‌توانید دسترسی روت بگیرید). با این حال، مهاجم ممکن است بر روی کپی کردن داده‌های حیاتی به روشی متمرکز شود که نیازی به دسترسی روت نداشته باشد یا باعث منع سرویس شود.

برای پرداختن به محدودیت‌های ذاتی در روش‌های تست رسمی، آنها باید در فریم‌ورکی ادغام شوند که شبکه را از منظر یک مهاجم ببیند، معروف به زنجیره کشتار سایبری.

در سال ۲۰۰۹، مایک کلوپرت از لاکهید مارتین CERT مفهومی را معرفی کرد که اکنون به عنوان زنجیره کشتار سایبری شناخته می‌شود. این شامل مراحلی است که از سوی یک دشمن هنگام حمله به یک شبکه انجام می‌شود. همیشه در یک جریان خطی پیش نمی‌رود، زیرا ممکن است برخی از مراحل به صورت موازی رخ دهند. حملات متعدد ممکن است در طول زمان در یک هدف انجام شود و مراحل همپوشانی ممکن است رخ دهد.

در این کتاب، زنجیره کشتار سایبری کلوپرت را اصلاح کرده‌ایم تا با دقت بیشتری نشان دهد که مهاجمان چگونه این مراحل را هنگام بهره‌برداری از شبکه‌ها، برنامه‌ها و سرویس‌های داده اعمال می‌کنند. شکل، یک زنجیره کشتار سایبری معمولی از یک مهاجم را نشان می‌دهد:




**زنجیره کشتار سایبری معمولی که مهاجم ممکن است دنبال کند**

یک زنجیره کشتار سایبری معمولی یک مهاجم را می‌توان به شرح زیر توصیف کرد:

**مرحله کاوش یا شناسایی**: ضرب المثل معروفی که می‌گوید "*در زمان شناسایی هرگز وقت تلف نشود*" و از سوی اکثر سازمان‌های نظامی پذیرفته شده است، اذعان می‌کند که بهتر است پیش از درگیر شدن با دشمن، تا آنجا که ممکن است در مورد آنها اطلاعات کسب کنید. به همین دلیل، مهاجمان پیش از حمله، شناسایی گسترده‌ای از یک هدف را انجام می‌دهند. در واقع تخمین زده

می‌شود که حداقل ۷۰ درصد از تلاش یک تست نفوذ یا حمله صرف انجام عملیات شناسایی می‌شود! به طور کلی، آنها از دو نوع شناسایی استفاده می‌کنند:

- **منفعل**: هیچ تعامل مستقیمی با هدف به صورت خصمانه وجود ندارد. برای مثال، مهاجم وب‌سایت(های) در دسترس عموم را بررسی می‌کند، رسانه‌های آنلاین (به‌ویژه سایت‌های رسانه‌های اجتماعی) را ارزیابی می‌کند و تلاش می‌کند سطح حمله هدف را تعیین کند. یک کار خاص، ایجاد فهرستی از نام‌های کارمندان گذشته و فعلی، یا حتی تحقیق در مورد پایگاه‌های اطلاعاتی درز یافته است که در دسترس عموم قرار دارد.

  این نام‌ها اساس تلاش‌ها برای استفاده از بروت فورس در حدس زدن رمزهای عبور را تشکیل می‌دهند. آنها همچنین در حملات مهندسی اجتماعی کاربرد دارند. تشخیص این نوع شناسایی از رفتار کاربران معمولی اگر نگوییم غیرممکن، دشوار است.

- **فعال**: این نوع شناسایی می‌تواند توسط هدف پی برده شود، اما تشخیص آن از بقیه فعالیت‌هایی که اغلب سازمان‌های آنلاین با ترافیک معمولی مواجه می‌شوند، دشوار است. فعالیت‌هایی که در طول شناسایی فعال رخ می‌دهند شامل بازدیدهای فیزیکی از محل‌های هدف، اسکن پورت، و اسکن آسیب‌پذیری از راه دور است.

- **مرحله تحویل**: تحویل عبارت است از انتخاب و توسعه سلاحی که برای تکمیل اکسپلویت در حین حمله استفاده می‌شود. سلاح دقیق انتخاب شده به هدف مهاجم و همچنین مسیر تحویل (به عنوان مثال، در سراسر شبکه، از طریق یک اتصال بی سیم، یا از طریق یک سرویس مبتنی بر وب) بستگی دارد. تأثیر مرحله تحویل به طور مفصل در نیمه دوم این کتاب بررسی خواهد شد.

- **مرحله اکسپلویت**: این مرحله زمانی است که یک اکسپلویت خاص با موفقیت اعمال می‌شود و به مهاجمان اجازه می‌دهد تا جای پایی در سیستم هدف به دست آورند. اکسپلویت ممکن است در یک فاز اتفاق افتاده باشد (به عنوان مثال، یک آسیب‌پذیری شناخته شده سیستم عامل با استفاده از یک سرریز بافر مورد بهره‌برداری قرار گرفته است)، یا ممکن است یک اکسپلویت چند فازی باشد (به عنوان مثال، اگر یک مهاجم بتواند داده‌ها را از اینترنت جست‌وجو و دانلود کند. از منابعی مانند https://haveibeenpwned.com یا موارد مشابه؛ این سایت‌ها معمولاً شامل داده‌های نقض‌شده، از جمله نام‌های کاربری، رمز عبور، شماره تلفن و آدرس‌های ایمیل هستند که به آن‌ها اجازه می‌دهد به راحتی دیکشنری رمزهای عبور را برای دسترسی به نرم‌افزار ایجاد کنند. به عنوان یک سرویس (SaaS) برنامه‌های کاربردی، مانند Microsoft Office 365 یا Outlook Web، سعی می‌کنند مستقیماً به یک VPN شرکتی وارد شوند یا از آدرس‌های ایمیل برای انجام تکنیک‌های فیشینگ ایمیل هدفمند استفاده کنند. مهاجم حتی می‌تواند یک SMS با

لینک‌های مخرب برای تحویل ارسال کند. یک پیلود). هنگامی که یک مهاجم مخرب یک شرکت خاص را هدف قرار می‌دهد، حملات چند مرحله‌ای معمول است.

- **مرحله دستیابی – اقدام بر اساس هدف**: این مرحله اغلب و به اشتباه به عنوان مرحله استخراج[1] نامیده می‌شود زیرا تمرکز بر درک حملات صرفاً به عنوان مسیری برای سرقت داده‌های حساس (مانند اطلاعات ورود به سیستم، اطلاعات شخصی و اطلاعات مالی) است. در واقع معمول است که یک مهاجم هدف متفاوتی داشته باشد. برای مثال، یک مهاجم ممکن است بخواهد یک بسته باج افزار را روی رقبای خود رها کند تا کلاینت‌هایی را به سمت مدنظر خود سوق دهد. پس در این مرحله باید روی بسیاری از اقدامات احتمالی یک مهاجم تمرکز شود. یکی از متداول‌ترین فعالیت‌های بهره‌برداری، زمانی رخ می‌دهد که مهاجمان تلاش می‌کنند تا سطح دسترسی خود را به بالاترین سطح ممکن (افزایش عمودی[2]) بهبود بخشند و تا آنجا که ممکن است حساب‌ها را به خطر بیاندازند (افزایش افقی[3]).
- **مرحله دستیابی - پایدارسازی**: اگر در رخنه کردن در یک شبکه یا سیستم، ارزشی وجود داشته باشد، در صورت دسترسی مداوم، این مقدار احتمالاً ممکن است افزایش یابد. این به مهاجمان اجازه می‌دهد تا ارتباطات خود را با یک سیستم رخنه شده حفظ کنند. از دیدگاه مدافع، این بخشی از زنجیره کشتار سایبری است که معمولاً ساده‌ترین تشخیص است.

زنجیره‌های کشتار سایبری صرفاً مدل‌هایی از رفتار مهاجم در هنگام تلاش برای رخنه کردن در یک شبکه یا یک سیستم داده خاص هستند. به عنوان یک متامدل، می‌تواند هر روش تست نفوذ اختصاصی یا تجاری را در خود جای دهد. با این حال، برخلاف متدولوژی‌ها، تمرکز سطح استراتژیک بر نحوه نزدیک شدن مهاجم به شبکه را تضمین می‌کند. این تمرکز بر فعالیت‌های مهاجم، طرح و محتوای این کتاب را شکل می‌دهد.

## ۱-۶ آشنایی با ویژگی‌های کالی لینوکس

کالی لینوکس (Kali) جانشین پلتفرم تست نفوذ BackTrack است که به طور کلی به عنوان بسته استاندارد واقعی ابزارهایی در نظر گرفته می‌شود که برای تسهیل تست نفوذ برای ایمن‌سازی داده‌ها و شبکه‌های صوتی استفاده می‌شود. توسط Mati Aharoni و Devon Kearns در Offensive Security توسعه داده شده است. این توزیع عمدتاً برای تست نفوذ و جرم شناسی دیجیتال است.

---

[1] Exflitration
[2] vertical escalation
[3] horizontal escalation

در سال ۲۰۲۱، نسخه ۴ کالی به‌روز رسانی شد. آخرین نسخه رولینگ در ۹ دسامبر ۲۰۲۱ با هسته ۵.۱۴.۰ و محیط دسکتاپ Xfce 4.16.3 منتشر شد. افزون بر این، یک به‌روز رسانی جزئی در ۲۳ دسامبر ۲۰۲۱ با نسخه Kali 2021.4a وجود داشت.

برخی از ویژگی‌های این آخرین نسخه کالی شامل موارد زیر است:

بیش از ۵۰۰ ابزار تست نفوذ پیشرفته، جرم شناسی داده و دفاعی. اکثر ابزارهای از پیش نصب شده قدیمی حذف شده و با ابزارهای مشابه جایگزین شده‌اند. آنها پشتیبانی بی‌سیم گسترده‌ای را با چندین سخت‌افزار ارائه می‌کنند تا امکان تزریق بسته مورد نیاز برای برخی از حملات بی‌سیم را فراهم کنند. جدول زیر، تجزیه و تحلیل ابزارها را با توجه به وظیفه خاص آنها از دسامبر ۲۰۲۱ ارائه می‌دهد:

| دسته بندی ابزارها | تعداد ابزارها |
|---|---|
| جمع آوری اطلاعات | ۶۷ |
| تجزیه و تحلیل آسیب‌پذیری | ۲۷ |
| حملات بی سیم | ۵۴ |
| وب اپلیکیشن ها | ۴۳ |
| ابزارهای اکسپلویت | ۲۱ |
| ابزارهای جرم شناسی | ۲۳ |
| اسنیفینگ و اسپوفینگ | ۳۳ |
| حملات رمز عبور | ۳۹ |
| حفظ دسترسی | ۱۷ |
| مهندسی معکوس | ۱۱ |
| هک سخت افزار | ۶ |
| ابزارهای گزارش دهی | ۱۰ |

**تعداد ابزارهای موجود، فهرست شده با توجه به وظایف خاصی که برای آنها استفاده می‌شود**

برخی از ویژگی‌های کلیدی کالی لینوکس عبارتند از:

- پشتیبانی از چندین محیط دسکتاپ مانند KDE، GNOME3، Xfce، MATE، e17، lxde ، و i3wm.021.
- به‌طور پیش‌فرض، کالی لینوکس دارای ابزارهای سازگار با دبیان است که حداقل چهار بار در روز با مخازن دبیان همگام‌سازی می‌شوند و به‌روزرسانی بسته‌ها و اعمال اصلاحات امنیتی را آسان‌تر می‌کنند.
- محیط‌های توسعه ایمن و پکت‌ها و مخازن با امضای GPG وجود دارد.
- پشتیبانی از سفارشی‌سازی ISO وجود دارد که به کاربران امکان می‌دهد نسخه‌های شخصی خود را از Kali با مجموعه محدودی از ابزارها بسازند تا آن را سبک کنند. تابع راه‌اندازی همچنین نصب شبکه سراسری سازمانی را انجام می‌دهد که می‌توانند با استفاده از فایل‌های از پیش نصب شده، خودکار شوند.
- از آنجایی که سیستم‌های مبتنی بر ARM رایج‌تر و ارزان‌تر شده‌اند، پشتیبانی از ARMEL و ARMHF در کالی لینوکس را می‌توان بر روی دستگاه‌هایی مانند rk3306 mk /ss808، Raspberry Pi، ODROID U2/X2، Samsung Chromebook، EfikaMX، Beaglebone Black، CuBox و Galaxy Note 10.1 نصب کرد.
- کالی همچنان یک پروژه منبع باز رایگان است. مهم‌تر از همه اینکه به خوبی با یک جامعه آنلاین فعال پشتیبانی می‌شود.

## ۱-۷ نقش کالی در تاکتیک رد تیم

با اینکه نفوذگران ممکن است هر نوع سیستم عاملی را برای انجام فعالیت مورد نظر خود ترجیح دهند، استفاده از کالی لینوکس صرفه جویی قابل توجهی در زمان می‌کند و از نیاز به جست‌وجوی پکت‌هایی که معمولاً در سایر سیستم‌عامل‌ها موجود نیستند جلوگیری می‌کند. برخی از مزایایی کالی لینوکس در طول تمرین رد تیم دارد و مورد توجه قرار نمی‌گیرد شامل موارد زیر می‌شود:

- یک منبع واحد برای حمله به سیستم عامل‌های مختلف.
- اضافه کردن منابع و نصب پکت‌ها و کتابخانه‌های پشتیبانی کننده (به‌ویژه مواردی که برای ویندوز در دسترس نیستند) سریع است.
- حتی امکان نصب پکت‌های RPM با استفاده از alien وجود دارد.

هدف کالی لینوکس، ایمن‌سازی زیرساخت‌های شبکه، ابر و برنامه‌ها و بسته‌بندی همه ابزارها برای ارائه یک پلتفرم واحد برای آزمونگران نفوذ و تحلیلگران جرم شناسی است.

## ۸-۱ نصب و به‌روز رسانی کالی لینوکس

در این بخش، پایه نصب کالی لینوکس بر روی پلتفرم‌های متداول، همراه با پلتفرم ابری گوگل و یک گوشی اندرویدی روت نشده را بررسی می‌کنیم.

### استفاده به عنوان یک دستگاه قابل حمل

نصب کالی لینوکس بر روی یک دستگاه قابل حمل بسیار ساده است. در برخی شرایط، کلاینت‌ها اجازه استفاده از لپ‌تاپ خارجی را در داخل یک مرکز امن نمی‌دهند. در این موارد، معمولاً یک لپ‌تاپ آزمایشی توسط کلاینت در اختیار نفوذگرها قرار می‌گیرد تا اسکن را انجام دهند. اجرای کالی لینوکس از یک دستگاه قابل حمل مزایای بیشتری در طول پنتست یا RTE دارد:

- می‌تواند در داخل یک جیب، همچون درایو USB یا دستگاه تلفن همراه، جا شود.
- بدون ایجاد هیچ تغییری در سیستم عامل میزبان می‌توان آن را به صورت زنده اجرا کرد.
- می‌توانید ساخت کالی لینوکس را سفارشی کنید و حتی ذخیره‌سازی را پایدار کنید.

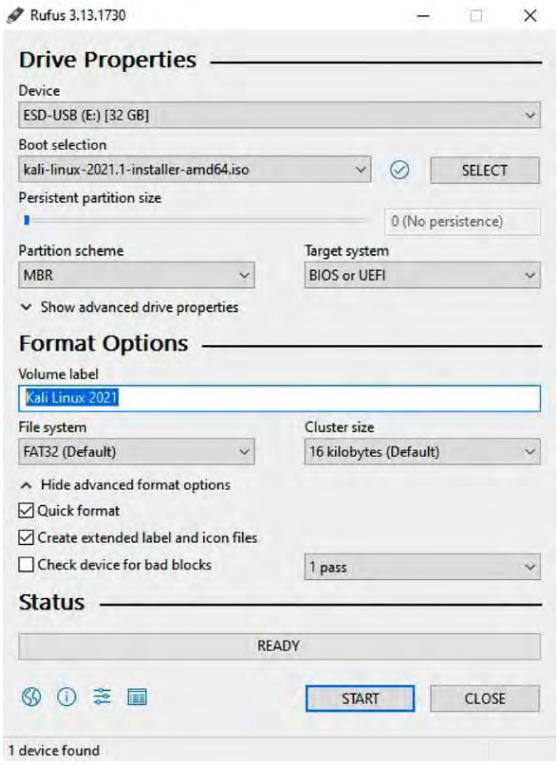
سه مرحله ساده برای تبدیل یک درایو USB به شکل قابل حمل Kali از رایانه شخصی ویندوز وجود دارد:

۱. ایمیج رسمی کالی لینوکس را از آدرس زیر دانلود کنید:

http://docs.kali.org/introduction/download-official-kali-linux-images

۲. از ابزار منبع باز Rufus برای ایجاد یک دیسک قابل بوت استفاده خواهیم کرد. Rufus به ایجاد و فرمت درایوهای قابل بوت کمک می‌کند. جدیدترین Rufus را از https://github.com/ pbatard //rufus/releases دانلود کنید.

۳. فایل اجرایی Rufus را به عنوان ادمین باز کنید. درایو USB را به درگاه USB موجود وصل کنید. به مکانی که ایمیج خود را در آن بارگیری کرده‌اید، بروید. باید آنچه در شکل نشان داده شده است را ببینید. نام درایو مناسب را انتخاب کنید و سپس روی Start کلیک کنید:




**اجرای Rufus برای نوشتن کالی لینوکس بر روی یک دیسک خارجی**

پس از تکمیل، برنامه Rufus را ببندید و با خیال راحت درایو USB را بردارید. اکنون کالی لینوکس به عنوان یک دستگاه قابل حمل برای اتصال به هر لپ‌تاپ و راه‌اندازی آماده است. اگر قصد دارید اطلاعات را هنگام بوت شدن روی یک دیسک زنده ذخیره کنید، مطمئن شوید که اندازه پارتیشن Persistence را برای داشتن حداقل ۴ گیگابایت انتخاب کنید. سپس هنگام بوت کردن کالی لینوکس در دستگاه قابل حمل، Live USB persistence را انتخاب کنید. اگر سیستم عامل میزبان شما لینوکس است، این امر با دو دستور استاندارد قابل دستیابی است:

```
sudo fdisk -l
```

با این کار تمام دیسک‌های نصب شده روی درایو نمایش داده می‌شود. ابزار خط فرمان *dd* تبدیل و کپی را انجام می‌دهد:

```
dd  if=kali linux.iso  of=/dev/nameofthedrive  bs=512k
```

*If* برای فایل ورودی استفاده می‌شود، *of* برای فایل خروجی و *bs* برای اندازه است.

### ۱-۸-۱ نصب کالی روی Raspberry Pi 4

Raspberry Pi یک دستگاه تک بورد است که ماهیت فشرده دارد و می‌تواند درست مانند یک رایانه کاملاً بارگذاری شده با حداقل عملکرد کار کند. این دستگاه‌ها در حین فعالیت‌های RTE و تست نفوذ در محل بسیار مفید هستند. پایه سیستم عامل از کارت SD بارگیری می‌شود، درست مانند هارد دیسک برای رایانه‌های معمولی.

می‌توانید همان مراحلی را که در بخش قبل بیان شد، روی یک کارت SD پرسرعت که به Raspberry Pi وصل می‌شود، انجام دهید. سپس آماده استفاده از سیستم بدون هیچ مشکلی باشید. اگر نصب با موفقیت انجام شود، هنگام بوت شدن Kali Linux از Raspberry Pi ، صفحه زیر را خواهید دید. در این تصویر از Raspberry Pi 4 استفاده شده است و با استفاده از مانیتور به سیستم عامل Pi دسترسی پیدا کرده است:


نصب موفقیت آمیز **Kali Linux بر روی Raspberry Pi 4**

### ۱-۸-۲ نصب کالی در VM

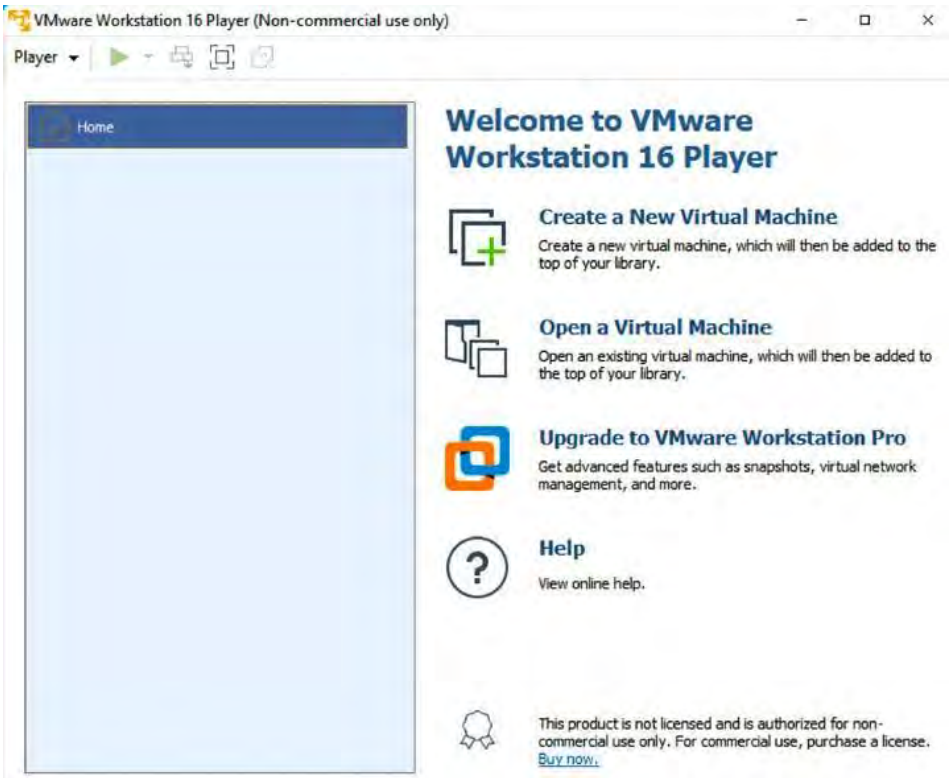
در اینجا روش نصب سریع اشاره می‌شود.

### VMware Workstation Player –

VMware Workstation Player که قبلاً به عنوان VMware Player شناخته می‌شد، برای استفاده شخصی رایگان است و همچنین یک محصول تجاری است که امکان استفاده از VMware را به عنوان یک برنامه دسکتاپ می‌دهد که این امکان را VM فراهم می‌آورد تا در سیستم عامل هاست شما اجرا شود. این نرم‌افزار را می‌توانید از نشانی دانلود کنید:

https://www.vmware.com/uk/products/workstation-player/workstation-player-evaluation.html

ما از نسخه ۱۶.۱ استفاده خواهیم کرد. پس از دانلود نصب کننده، بر اساس سیستم عامل میزبان خود، VMware Player را نصب کنید. اگر نصب کامل شد، باید صفحه‌ای مشابه شکل زیر ببینید:




**نصب موفقیت آمیز VMware Workstation Player**

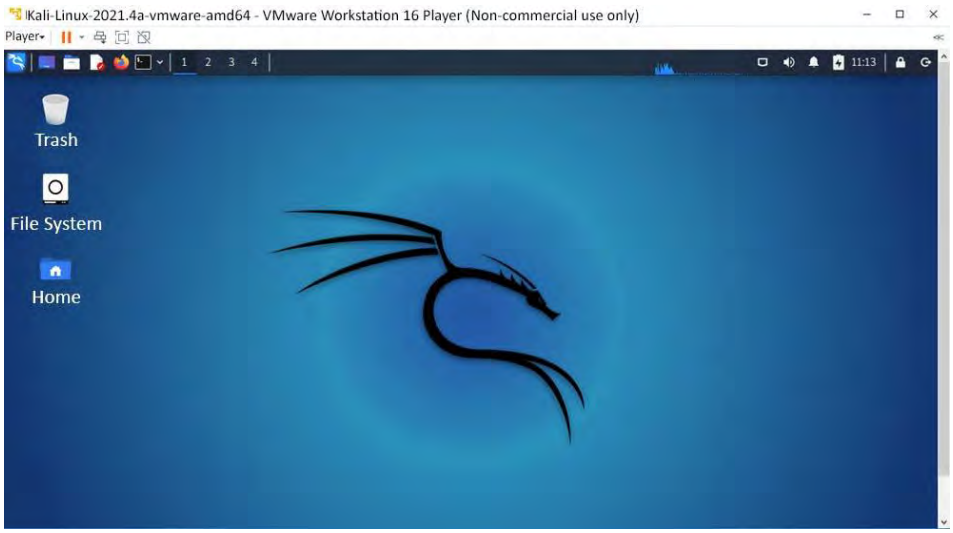
مرحله بعدی برای نصب کالی لینوکس روی VMware این است که بر روی Create a New Virtual Machine کلیک کنید و Installer disc image file (iso) را انتخاب کنید. به فایل ISO خود که دانلود

شده است بروید و سپس روی Next کلیک کنید. اکنون می‌توانید نام دلخواه خود را وارد کنید (مثلا HackBox) و مکان سفارشی را انتخاب کنید که می‌خواهید تصویر VMware خود را در آن ذخیره کنید. روی Next کلیک کنید و ظرفیت دیسک را مشخص کنید. توصیه می‌شود حداقل از ۲ گیگابایت رم استفاده شود و برای اجرای Kali به ۱۵ گیگابایت فضای دیسک نیاز است. روی Next کلیک کنید تا تمام شود.

روش دیگر دانلود مستقیم ایمیج VMware است:

/https://www.offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download

فایل . vmx را باز کنید و I copyed it را انتخاب کنید. این باید کالی لینوکس کاملاً بارگذاری شده در VMware را بوت کند. می‌توانید انتخاب کنید که Kali Linux به عنوان سیستم عامل میزبان نصب شود یا آن را به عنوان یک ایمیج لایو اجرا کنید. پس از اتمام تمام مراحل نصب، آماده راه‌اندازی کالی لینوکس از VMware بدون هیچ مشکلی هستید. شکل زیر، صفحه‌ای را نشان می‌دهد که باید دیده شود:




**وقتی کالی لینوکس با موفقیت بر روی VMware نصب شد، این اسکرین، نشان داده می‌شود**

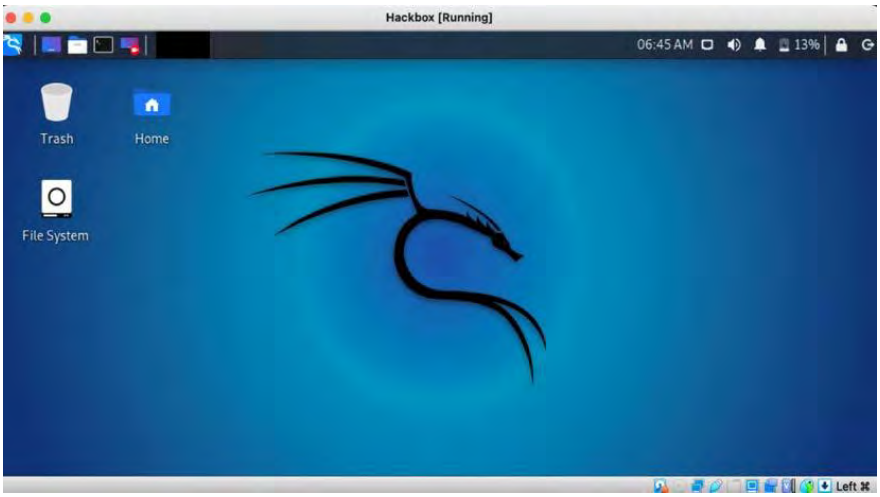
### - VirtualBox

مشابه VMware workstation player، VirtualBox یک Hypervisor است که کاملا متن باز و یک برنامه دسکتاپ رایگان است که می‌توانید هر ماشین مجازی را از سیستم عامل میزبان اجرا کنید. این نرم‌افزار را می‌توانید از https://www.virtualbox.org/wiki/Downloads دانلود کنید.

اکنون پیش می‌رویم و کالی را روی VirtualBox نصب می‌کنیم. مشابه VMware، فقط فایل اجرایی دانلود شده را اجرا می‌کنیم تا زمانی که Oracle VirtualBox با موفقیت نصب شود، همانطور که در شکل نشان داده شده است:


**صفحه نمایش با نصب موفقیت آمیز VM VirtualBox**

در حین نصب، توصیه می‌شود رم را حداقل ۱ یا ۲ گیگابایت قرار دهید و هارد مجازی را با حداقل ۱۵ گیگابایت ایجاد کنید تا مشکلی در عملکرد ایجاد نشود. پس از آخرین مرحله، باید بتوانید کالی لینوکس را در VirtualBox بارگذاری کنید، همانطور که در شکل نشان داده شده است:




**کالی لینوکس، همانطور که در VM VirtualBox نمایش داده می‌شود**

پس از تکمیل این کار، اکنون آماده استفاده از کالی لینوکس از طریق VirtualBox هستیم. با این حال، گزینه‌های مختلف شبکه را در بخش بعدی، شبکه LAB بررسی خواهیم کرد.