راهنمای پویش آسیب‌پذیری و تست نفوذ با

Nessus

مهندس احسان نیک‌آور

انتشارات پندار پارس

سرشناسه : نیک‌آور، احسان، ۱۳۶۶ -
عنوان و نام پدیدآور : راهنمای پویش آسیب‌پذیری و تست نفوذ با Nessus
مشخصات نشر : تهران : پندار پارس ۱۳۹۴.
مشخصات ظاهری : ۱۹۲ ص.: مصور، جدول .
شابک : 978-600-6529-84-4: ۱۵۰۰۰۰ ریال
وضعیت فهرست نویسی : فیپای مختصر
یادداشت : فهرستنویسی کامل این اثر در نشانی: http://opac.nlai.ir قابل دسترسی است
یادداشت : کتابنامه .
شماره کتابشناسی ملی : ۳۸۷۲۰۶۳

انتشارات پندارپارس

دفتر فروش: انقلاب، ابتدای کارگرجنوبی، کوی رشتچی، شماره ۱٤، واحد ۱٦ **www.pendarepars.com**

تلفن: ٦٦٥٧٢٣٣٥ - تلفکس: ٦٦٩٢٦٥٧٨همراه: ۰۹۱۲۲٤٥۲۳٤۸ **info@pendarepars.com**

نام کتاب : راهنمای پویش آسیب‌پذیری و تست نفوذ با Nessus
ناشر : انتشارات پندار پارس
ترجمه و تالیف : احسان نیک‌آور
چاپ نخست : مرداد ۹٤
شمارگان : ۵۰۰ نسخه
طرح جلد و صفحه‌آرایی : سارا یعسوبی
چاپ، صحافی : روز
قیمت : ۱۵۰۰۰ تومان **شابک : ٤-۸٤-٦٥۲۹-٦۰۰-۹۷۸**

فهرست

پیش‌گفتار

امروزه فناوری اطلاعات در تمامی سازمان‌ها و شرکت‌ها رشد چشمگیری را به خود دیده است. استفاده از این فناوری و استفاده از شبکه‌های رایانه‌ای در بخش‌های گوناگون سازمان موجب پیشرفت قابل توجه سازمان در نحوه ارائه خدمات و همچنین افزایش کارایی سازمان گردیده است. استفاده از این امکانات بدون رعایت نکات امنیتی و استفاده شایسته از ابزارهای موجود، همواره با مخاطرات بسیاری همراه می‌باشد. امنیت، یکی از مهمترین اجزای مرتبط با فناوری اطلاعات می‌باشد و عدم رعایت موارد امنیت می‌تواند صدمات جبران ناپذیری را به سازمان مطبوع شما وارد نماید.

در این کتاب قصد ما بر این است که شما را با ابزاری به نام Nessus آشنا کنیم که این ابزار قادر به کشف آسیب‌پذیری‌های موجود در سیستم‌های موجود در سازمان یا شرکت شما خواهد بود. با استفاده از این ابزار می‌توانید امنیت خود را به چالش کشیده و همچنین آن را مورد ارزیابی قرار دهید. گفتنی است، مطالب موجود در این کتاب برگرفته از منابع اصلی این ابزار و شرکت ارائه دهنده‌ی آن یعنی Tenable می‌باشد.

مدیران، کارشناسان امنیت و همچنین تمامی علاقمندان حوزه‌ی امنیت شبکه و اطلاعات می‌توانند از این کتاب استفاده کنند و با توجه به اینکه کتاب پیش رو توسط اعضای کوچکی از کارشناسان امنیت فراهم گردیده است لذا خالی از اشکال نیست. به همین منظور از تمامی عزیزانی که در حوزه‌ی امنیت مشغول هستند، صمیمانه خواهشمندیم تا انتقادها، نظرها و پیشنهادهای خود را به آدرس info@esecurity.ir ارسال نمایند. البته دوستان عزیزی که پس از مطالعه‌ی این کتاب پرسشی در باره‌ی موضوعات آن دارند نیز می‌توانند با همین آدرس پست الکترونیکی ارتباط برقرار نمایند. در پایان نیز امیدوارم مطالب موجود در این کتاب برای شما خواننده‌ی عزیز مفید واقع گردد.

احسان نیک‌آور

تابستان ۹۴

فصل ۱

آشنایی با مفاهیم و محیط Nessus

از ابزار Nessus به‌منظور کشف آسیب‌پذیری در سطح شبکه استفاده می‌شود. در آزمون‌های نفوذ-پذیری، دو روش جعبه سفید و جعبه سیاه وجود دارد که Nessus قادر است بر پایه‌ی این دو آزمون عمل کند. در آزمون جعبه سیاه شما هیچ اطلاعاتی از هدف ندارید و تنها به آدرس IP و نوع سیستم عامل بسنده می‌کنید ولی در آزمون جعبه سفید شما اطلاعات کافی از هدف مورد نظر را در دست دارید. در آزمون جعبه سفید اطلاعاتی مانند نام‌های کاربری و گذرواژه‌ها یا اعتبارهای لازم را به Nessus داده و با دسترسی مدیر، اقدام به تست آسیب‌پذیری می‌کنید تا مشکلاتی که در حالت جعبه سیاه قادر به کشف آن نیستید توسط این روش به آنها دست یابید. Nessus از انواع ساختارهای مختلف به‌منظور اسکن پشتیبانی می‌کند. این ساختارها شامل سیستم‌عامل‌های مختلف، انواع مجازی سازها و پروتکل‌های شبکه می‌باشد.

هسته‌ی اصلی Nessus، پلاگین‌های آن هستند. در واقع هر یک از پلاگین‌ها بیانگر یک آسیب‌پذیری است که Nessus آنها را در دسته‌بندی مشخصی قرار داده است و می‌توان در هنگام اسکن، آنها را به‌کار گرفت. باید برای افزایش سرعت تست خود، پلاگین‌هایی را که مربوط به هدفتان نیست غیر فعال نمایید. برای نمونه، زمانی که سیستم عامل هدف ویندوز است، باید پلاگین‌هایی که به سیستم عامل ویندوز مربوط نمی‌باشد را غیرفعال نموده تا هم سرعت تست افزایش یابد و هم از ارسال اطلاعات اضافی به هدف خودداری شود.

Nessus شامل دو بخش اصلی اسکن و سیاست (Policy) می‌باشد. در بخش سیاست، روالی که در طی اسکن مدنظرتان است را مشخص می‌نمایید. این روال شامل مشخصات اولیه، نحوه‌ی شناسایی پورت‌ها، تنظیمات گزارش، تعیین پلاگین‌های مورد نیاز، تعریف اعتبار یا نام‌های کاربری و گذرواژه‌ها برای آزمون جبعه سفید می‌باشد. البته سیاست‌های از پیش تعریف شده‌ای هم برای موارد خاص در Nessus وجود دارد که می‌توان از آنها نیز استفاده نمود.

پس از تعریف سیاست، نوبت به انجام اسکن هدف می‌رسد. در این بخش می‌توانید با استفاده از سیاست تعریف شده در مرحله‌ی پیشین و تنظیماتی مانند زمان‌بندی اسکن و مشخصات هدف، اقدام

به اسکن آن نمایید. در پایان نیز اطلاعات به دست آمده از اسکن در قالب یک گزارش قابل دسترس بوده و می‌توانید آن را در یک فایل HTML و یا قالب‌های دیگر ذخیره نمایید.

در این کتاب می‌خواهیم این موارد را به صورت کامل شرح دهیم.

مفاهیم

Nessus در واقع یک برنامه اسکن آسیب‌پذیری بوده و محیط کاربری آن به صورت Web Base می‌باشد.

آخرین نسخه‌ای که هم اکنون از Nessus موجود می‌باشد نسخه ٦.٣ آن است. محصولاتی که در این نسخه ارائه شده است به شرح زیر است:

Nessus ®

Nessus Home

Nessus Professional

Nessus Manager

Nessus Scanner

Nessus Enterprise Cloud

Nessus Agent

می‌توانید پرسش‌های خود را درباره‌ی استفاده از Nessus و مشکلاتی که برای شما بوجود می‌آید به آدرس پست الکترونیکی support@tenable.com ارسال نمایید.

آپدیت‌های ویژگی

برخی از ویژگی‌های Nessus 6.3 در زیر بیان شده است.

- مدل جدیدی از Licensing که شامل Nessus Windows Agent است و می‌تواند در محیط ویندوز داخلی (Local) اجرا شده و اسکن‌ها را کنترل و اجرا نماید.
- داشبوردهای اسکن که آسیب‌پذیری‌ها و نماهای کلی موارد انجام شده را نمایش می‌دهد.
- مدیریت اسکنرها توسط Nessus Manager مرکزی برای گسترش سیاست‌ها (Deploy Policy)، اسکن‌ها، پلاگین‌ها و برنامه‌ی به‌روزرسانی‌ها

نمای کلی از واسط کاربری Nessus

Description

واسط کاربری Nessus یک واسط کاربری تحت وب بوده که شامل یک سرور HTTP ساده و یک وب کلاینت می‌باشد و نیازی به نصب برنامه مجزایی از سرور Nessus نخواهد داشت. ویژگی‌های اصلی آن به شرح زیر است:

- تولید فایلی با پسوند nessus. که محصولات شرکت Tenable از این استاندارد برای سیاستهای اسکن و داده مربوط به آسیب‌پذیری‌ها از آن استفاده می‌کند.
- یک نشست Policy، لیستی از Targetها و نتایج چندین اسکن است و همه آنها می‌تواند در یک فایل با پسوند nessus. ذخیره شده که به آسانی قابل استخراج می‌باشد. برای اطلاعات بیشتر در این مورد می‌توانید به فایل راهنمای"Nessus v2 File Format" مراجعه نمایید.
- به منظور اسکن Targetها می‌توان از چندین فرمت استفاده نمود: IPv4، IPv6، hostname و نماد CIDR
- پشتیبانی از LDAP به صورتی که حسابهای واسط کاربری Nessus قادر به احراز هویت در یک سرور از راه دور باشند.
- نمایش نتایج اسکن به صورت آنی (Real Time)؛ بدین منظور که شما مجبور نباشید منتظر بمانید اسکن کامل شود، سپس نتیجه اسکن را ملاحظه نمایید.
- ایجاد یک واسط متحد برای اسکنر Nessus ورای از نوع Platform و توابع یکسان موجود در ویندوز، لینوکس و Mac OS
- هنگامی که اسکن اجرا شد، حتی چنانچه واسط کاربری به هر دلیلی قطع شود، اسکن ادامه پیدا خواهد کرد.
- خروجی‌ها و گزارشهای مربوط به اسکن‌ها می‌تواند در واسط کاربری Nessus آپلود شده و با دیگر گزارش‌ها مقایسه شود.
- داشبوردهای اسکن که آسیب‌پذیری‌ها و نمای کلی موارد انجام شده را نشان می‌دهد، به شما این امکان را می‌دهد تا از تمامی اسکن‌های انجام شده، اسکن مورد نظر خود را انتخاب نمایید.
- Wizard مربوط به policy به شما کمک می‌کند تا به سرعت Policy مورد نظر خود را برای اسکن و ارزیابی شبکه خود به دست آورید.

- یکی از قابلیت‌های Nessus این است که می‌توان یک اسکنر را به عنوان اصلی در نظر گرفت و دیگری را به عنوان فرعی در نظر گرفت، در این حالت می‌توان آنها را با یک واسط کاربری مدیریت نمایید که این مورد برای مدیریت اسکن‌ها در مقیاس بزرگ به کار می‌رود.
- یک سیستم گروه‌بندی و کاربری وسیع که قادر به مجوزدهی برای هر کدام از منابع اشتراکی شامل اسکنرها، سیاست‌ها، زمانبندی‌ها و نتایج اسکن می‌باشد.

پلتفرم‌های پشتیبانی شده

از آنجا که واسط کاربری Nessus تحت وب می‌باشد، می‌تواند در هر پلتفرم با یک مرورگر وب پیشرفته اجرا شود.

این واسط کاربری با بیشتر مرورگرها سازگاری دارد که از جمله آنها می‌توان به IE10، Mozilla Firefox32، Google Chrome 37، Opera 24 و Safari 7.1 بر روی دسکتاپ و Chrome 29 در اندروید، اشاره نمود.

Installation

روش نصب نسوس به‌شکل کامل در پیوست کتاب آمده است. این نرم‌افزار را می‌توان از طریق ارتباط با اینترنت و هم بدون استفاده از اینترنت نصب نمود که توضیحات مربوط به هر دو بخش در پیوست موجود است.

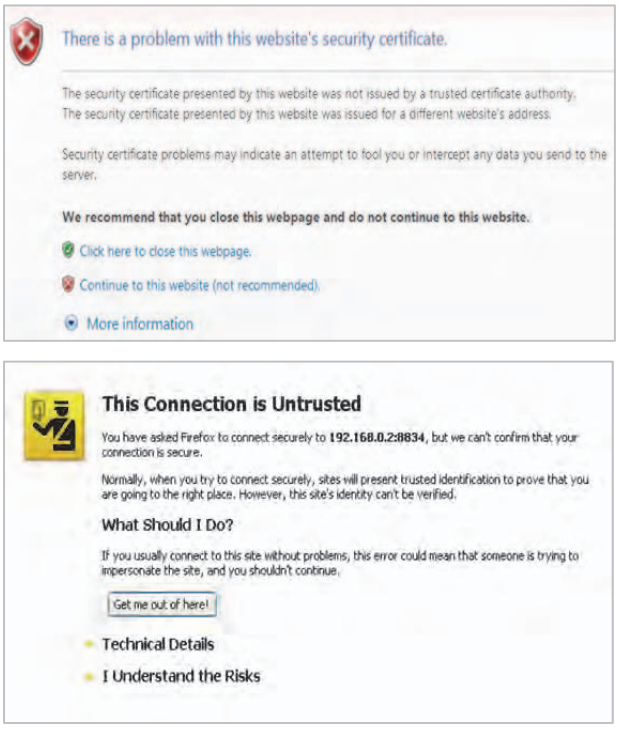
واسط کاربری Nessus

واسط کاربری در Nessus از طریق پروتکل HTTPS با شماره پورت ۸۸۳٤ قابل دسترسی خواهد بود. هر کاربر باید دارای یک نام کاربری و گذرواژه‌ی یکتا باشد.

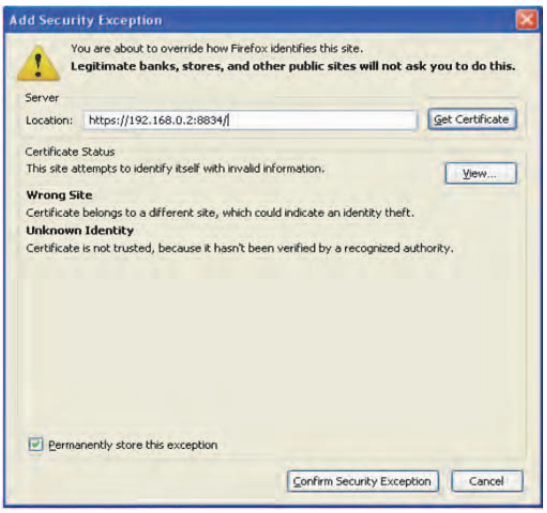
برای اتصال به واسط کاربری Nessus در آغاز باید مرورگر خود را باز کرده و سپس آدرس https:// [server IP]:8834/ را در نوار آدرس خود تایپ کرده و کلید Enter را فشار دهید.

مطمئن باشید که به وسیله پروتکل HTTPS متصل شده‌اید. پروتکل HTTP در این ارتباط پشتیبانی نمی گردد.

نخستین باری که تلاش می‌کنید به واسط کاربری Nessus متصل شوید، بیشتر مرورگرهای وب هشداری مشابه تصویر زیر را نمایش می‌دهند که سایت، مورد اطمینان نیست. (Nessus یک گواهینامه SSL به صورت Self-Signed تولید می‌کند.)



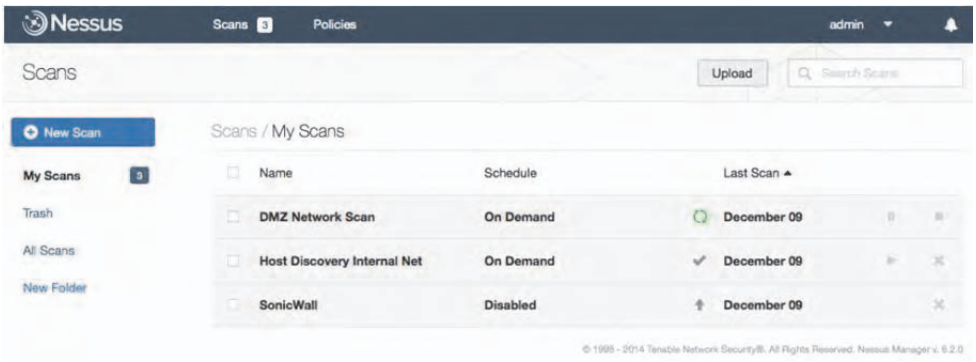
کاربران مرورگر IE می‌توانند بر روی پیوند "Continue to this website (not recommended)" کلیک کنند تا واسط کاربری Nessus بارگذاری شود. کاربران مرورگر Firefox نیز می‌توانند با کلیک بر روی "I Understand the Risks" و سپس انتخاب "... Add Exception" سایت استثناء شده را در صفحه باز شده تایید کنید.



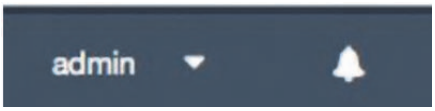
در این بخش باید آدرسی را که در کادر Location قرار دارد را کنترل نمایید و سپس بر روی دکمه‌ی "Confirm Security Exception" کلیک نمایید. پس از انجام مراحل مذکور، صفحه نخست Nessus به شما نمایش داده می‌شود که به شکل زیر خواهد بود و نام کاربری و گذر واژه‌ای که در مراحل نصب وارد کردید را از شما درخواست می‌کند.

نکته: در قسمت پیوست در پایان کتاب مراحل نصب Nessus در ویندوز به صورت کامل توضیح داده شده است.

پس از ورود می‌توانید مرروگر خود را برای به‌خاطرسپاری نام کاربری و گذرواژه تنظیم نمایید. باید به این نکته توجه داشته باشید که ذخیره‌سازی نام کاربری و گذرواژه را تنها در سیستمی که در یک محل امن قرار دارد انجام دهید. پس از احراز هویت موفق، واسط کاربری، منوهای مربوط به مدیریت Policyها و اسکن‌ها را نمایش می‌دهد. البته کاربران در سطح مدیر می‌توانند بخش مربوط به مدیریت کاربران و بخش مربوط به پیکربندی اسکنر Nessus را نیز مشاهده نمایند. هنگامی که وارد برنامه می‌شوید، بخش "Scans" در واسط کاربری به شکل زیر است.

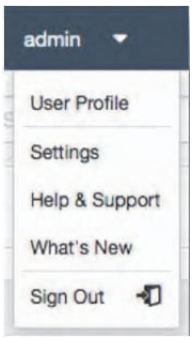


در طول زمانی که از Nessus استفاده می‌نمایید در بخش بالایی و سمت چپ، تنظیمات و منوها نمایش داده می‌شود. بخش "admin" در بالا و سمت چپ قرار دارد که نشان دهنده حساب کاربری وارد شده است. این بخش همچنین دارای زیر شاخه‌هایی نیز هست که به آن اشاره خواهیم کرد. در سمت راست این بخش، آیکن یک زنگ را می‌بینید که آخرین هشدارها و پیام‌ها در آن نمایش داده می‌شود.

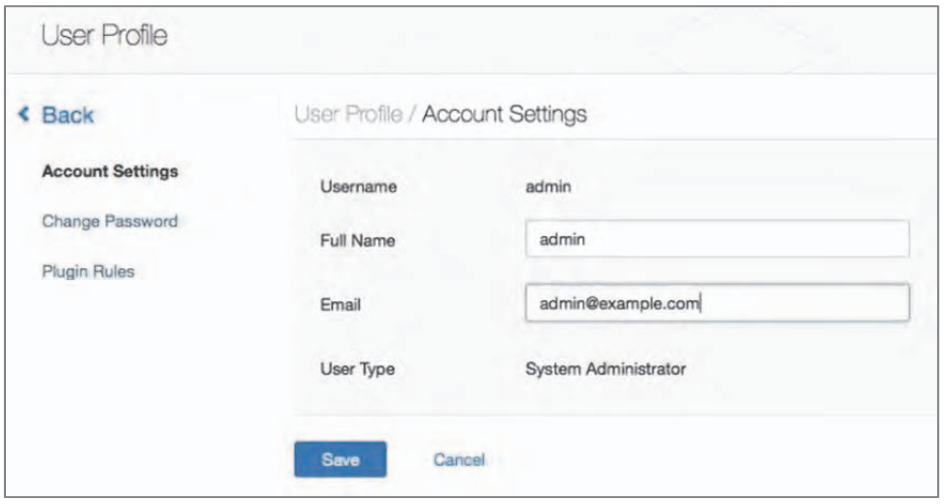


اگر از نسخه Nessus Enterprise Cloud استفاده نمایید، در سمت چپ آیکن زنگ، آدرس ایمیل ثبت شده به عنوان کاربر را مشاهده می‌کنید.

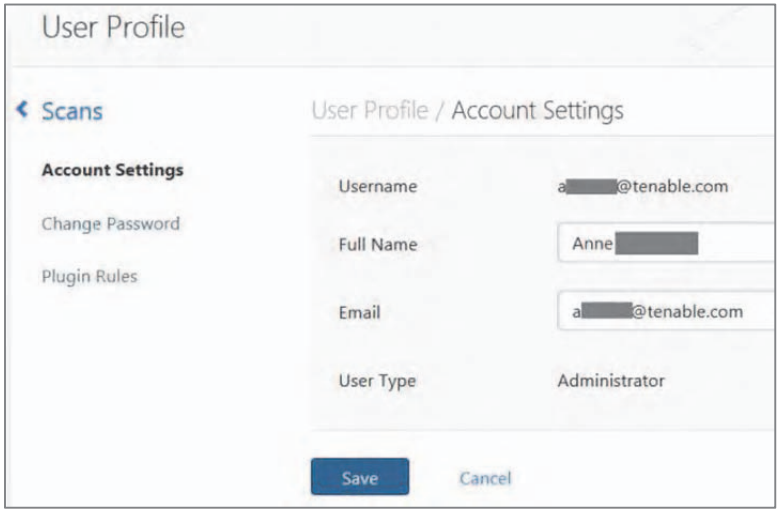
زمانی که بر روی آیکن فلش کنار "admin" کلیک می‌کنید، منویی نمایش داده می‌شود که دسترسی به پروفایل خود، تنظیمات عمومی Nessus، اطلاعات درباره‌ی نصب، بخش help & support، بخش What's New و خروج را برای شما امکان‌پذیر می‌سازد.



با ورود به بخش "User Profile" می‌توان اطلاعات مربوط به کاربر از جمله ایمیل و نام آن را مشاهده و تغییرات دلخواه خود را اعمال نمود. تغییر گذرواژه، مدیریت پوشه‌ها و صفحه مربوط به Plugin Rules نیز بخش‌های دیگری است که در این بخش قرار دارند.

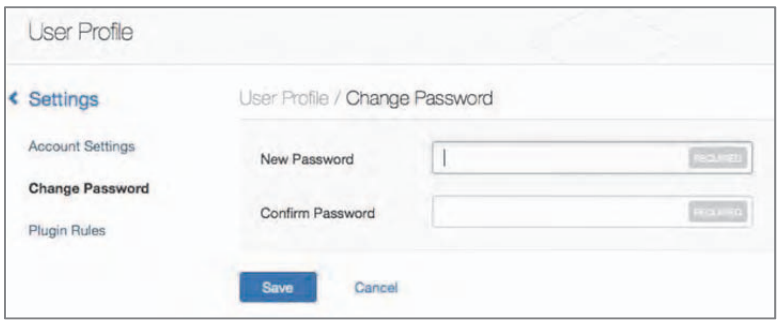


در نسخه Nessus Enterprise Cloud نام کاربری، همان ایمیلی است که به عنوان کاربر ثبت شده است.



در بخش "Account Settings" فیلدهای مربوط به کاربر وارد شده از جمله نام کامل کاربر، آدرس ایمیل و نوع کاربر قرار دارد. نوع کاربر می‌تواند System Administrator، Administrator، Standard و Read Only باشد. به صورت پیش فرض هنگامی که بر روی گزینه "User Profile" کلیک می‌کنید صفحه بالا نمایش داده می‌شود.

گزینه "Change Password" به شما این امکان را می‌دهد تا گذرواژه‌ی خود را تغییر دهید. گفتنی است که گذرواژه‌ی انتخابی می‌بایست برابر با سیاست‌های امنیتی سازمان درباره‌ی ساختار گذرواژه باشد. در بخش تغییر گذرواژه، باید گذرواژه‌ی انتخابی را برای تایید دوباره، وارد نمایید.



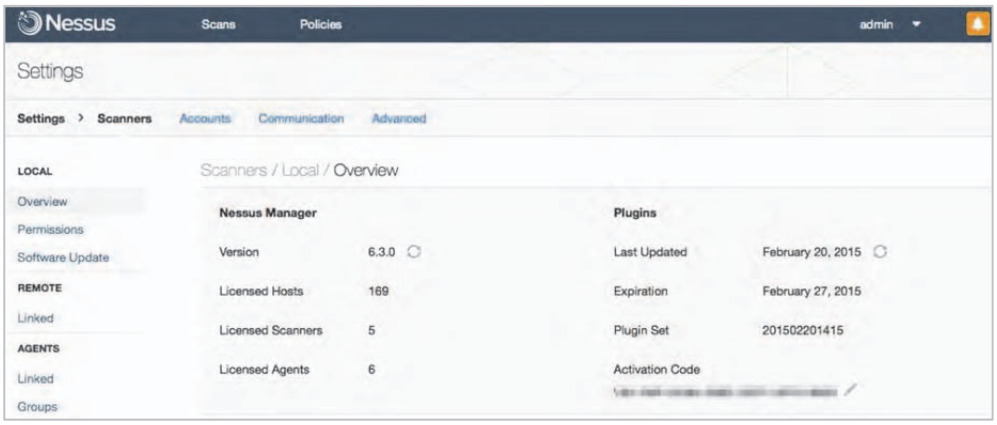
بخش "Plugin Rules" مرکزی است برای ایجاد مجموعه‌ای از قوانین که رفتار پلاگین‌های خاص مربوط به هر اسکن را برای شما فراهم می‌کند. هر Rule را می‌توان بر اساس میزبان یا همه میزبان‌ها، شناسه پلاگین، یک تاریخ انقضای اختیاری و تنظیم یک Severity تنظیم کرد. همان Ruleها

را می‌توان از صفحه نتایج اسکن تنظیم نمود. این به شما اجازه می‌دهد تا شدت نتایج پلاگین‌ها برای محاسبه بهتر استقرار امنیت و پاسخ سازمان را اولویت‌بندی نمایید.

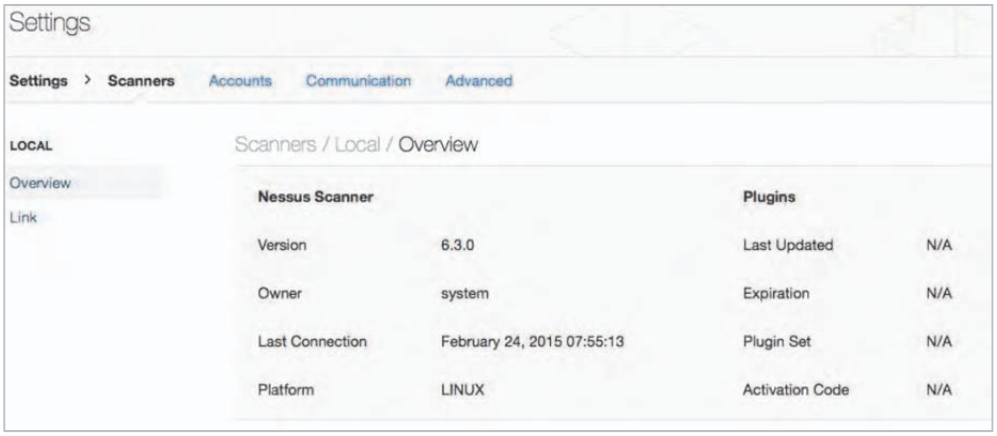
برای ایجاد یک Rule جدید، بر روی دکمه‌ی "New Rule" در بخش بالا سمت راست کلیک کنید. در پنجره باز شده می‌توانید میزبان مورد نظر را انتخاب کنید و اگر این بخش را خالی بگذارید همه میزبان‌ها در نظر گرفته می‌شوند. در بخش Plugin ID می‌توانید شناسه پلاگین مورد نظر خود را قرار دهید. در بخش Expiration Date می‌توانید تاریخ انقضای خود را برای این نقش انتخاب کنید و در بخش Severity، شدت نتیجه که می‌تواند Hide، Info، Low، Medium، High یا Critical باشد را تنظیم نمایید.

تنظیمات

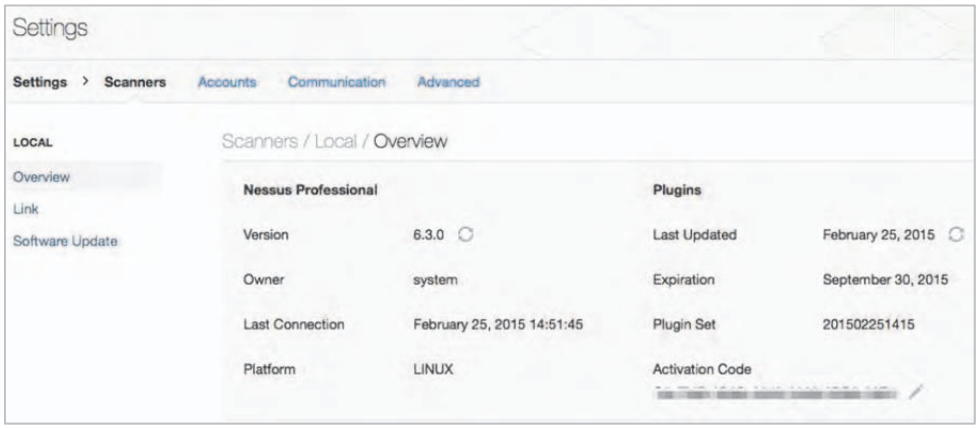
بخش "Settings" برای Nessus Manager دسترسی به صفحه "Overview"، حساب‌ها، ارتباطات با سرورهای میل و پراکسی خارجی، Nessus Agent، اسکنرهای Nessus، و بخش Advanced Scanner (اگر کاربر جاری یک System Administrator باشد) را فراهم می‌کند.



بخش "Settings" برای Nessus Scanner دسترسی به صفحه "Overview"، حساب‌ها، ارتباطات با سرورهای پراکسی و بخش Advanced Scanner (اگر کاربر جاری یک System Administrator باشد) را فراهم می‌کند.



بخش "Settings" برای Nessus Professional دسترسی به صفحه "Overview"، حساب‌ها، ارتباطات با سرورهای میل و پراکسی خارجی و بخش Advanced Scanner (اگر کاربر جاری یک Administrator باشد) را فراهم می‌کند.



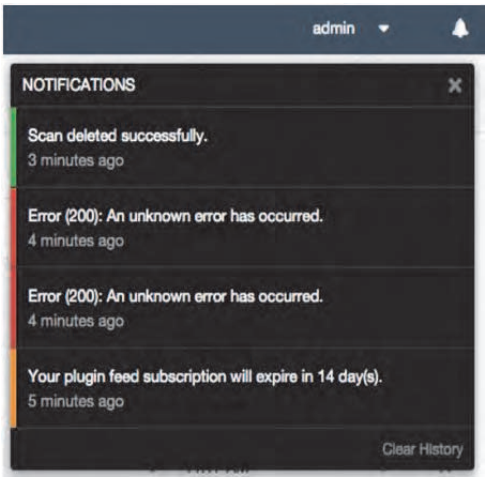
بخش "What's new" لینکی است که به شما ویژگی‌های جدید این نسخه از Nessus را نشان می‌دهد. در تصویر زیر نمونه‌ای از ویژگی‌هایی را که در نسخه ٦.٣ از Nessus ایجاد شده است مشاهده می‌کنید.

بخش "Help & Support" لینکی است که پورتال Tenable Support را در یک tab جدید باز می‌کند.

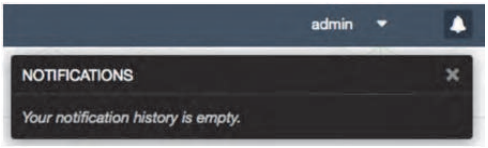
"Sign Out" نشست شما با Nessus را پایان خواهد داد و از برنامه خارج می‌شوید.

همان‌گونه که در بخش‌های پیشین اشاره شد، در بالای صفحه و سمت راست، کنار بخش "admin" آیکن زنگ مشاهده می‌شود. در این بخش هرگونه پیامی مربوط به عملکردهای Nessus شامل هشدارها، پیغام‌های مربوط به نسخه جدید Nessus، رخدادهای مربوط به نشست کنونی و دیگر موارد نمایش داده می‌شود.

این بخش همچنین به عنوان محلی برای فراهم نمودن هر هشدار دیگر یا پیام‌های خطا بوسیله پاپ‌آپ‌هایی که به صورت کم رنگ و کوتاه می‌باشند، به کار گرفته می‌شود. این پیام‌ها تا زمانی که حذف نشوند در حافظه باقی خواهند ماند.



شکل زیر نشان دهنده عدم وجود هرگونه هشدار و پیام خطایی می‌باشد.



کلیدهای میانبر و Shortcutهای واسط کاربری

واسط کاربری که به‌شکل HTML5 می‌باشد امکان استفاده از کلیدهای میانبر گوناگونی را می‌دهد تا به وسیله آنها به سرعت، به بخش‌های گوناگون آن دسترسی پیدا کنید. این کلیدها می‌توانند در هر زمانی و از هر جایی داخل واسط کاربری استفاده شوند.

در بخش اصلی واسط کاربری، کلیدهای میانبر زیر قابل استفاده هستند.

Hot Key	Description
R	Scans
P	Policies
U	Users
C	Settings
G	Groups (Nessus Manager and Nessus Enterprise Cloud only)
M	User Profile

در بخش اصلی از واسط کاربری برای فرآیندهای ایجاد، از کلیدهای میانبر زیر استفاده می‌شود.

Hot Key	Description
Shift + R	New Scan
Shift + F	New Folder (Scan view only)

در بخش "Scans" کلید زیر قابل استفاده می‌باشد.

Hot Key	Description
N	New Scan

در بخش "Policies" کلید زیر قابل استفاده می‌باشد.

Hot Key	Description
N	New Policy

در بخش "Users" کلید زیر قابل استفاده است.

Hot Key	Description
N	New User

در بخش گروه‌های کاربری در Nessus Manager و Nessus Enterprise Cloud کلید زیر قابل استفاده است.

Hot Key	Description
N	New User Group

در بخش "Advanced" و نمایش تنظیمات، کلید زیر قابل استفاده می‌باشد.

Hot Key	Description
N	New Setting

فصل ۲

آشنایی با ساختار Policy و مدیریت آن در Nessus

سیاست‌ها (Policies)

یک Nessus Policy مجموعه‌ای از پیکربندی‌های لازم برای انجام اسکن آسیب‌پذیری است. پیکربندی‌های لازم شامل بخش‌هایی به شرح زیر است:

- پارامترهایی که جنبه‌های گوناگون اسکن را مشخص می‌کند که عبارتند از تعیین شمار میزبان‌ها، انواع اسکنر برای پورت‌ها و مواردی از این دست.
- تنظیم اعتبارات لازم برای اسکن‌های داخلی مانند نام‌های کاربری و گذرواژه‌های مربوط به ویندوز، SSH و ...، احراز هویت در اسکن پایگاه داده اوراکل، احراز هویت پروتکل‌هایی مانند HTTP، FTP، POP، IMAP یا Kerberos
- تعیین اسکن مبتنی بر پلاگین و تنظیمات پلاگینهای لازم.
- کنترل Policyهایی مربوط به پایگاه داده، تنظیم اطلاعات اضافی و کامل در گزارش، تنظیمات مربوط به اسکن شناسایی سرویس‌ها، کنترل بخش‌های مربوط به Unix و موارد دیگر.
- تنظیمات مربوط به بررسی Offline برای دستگاه‌های شبکه، اجازه چک کردن ایمن دستگاه‌های شبکه بدون نیاز به اسکن مستقیم دستگاه‌ها.
- Windows Malware Scan که MD5های فایل‌ها را مقایسه می‌کند و فایل‌های سالم و آلوده را از هم تشخیص می‌دهد.