

راهنمای پویش آسیب‌پذیری و تست نفوذ با

# Nessus

مهندس احسان نیکآور  
انتشارات پندار پارس

سرشناسه	- نیکآور، احسان
عنوان و نام پدیدآور	راهنمای پوش آسیب‌پذیری و تست نفوذ با Nessus
مشخصات نشر	مشخصات نشر
مشخصات ظاهری	مشخصات ظاهری
شابک	شابک
وضعیت فهرست نویسی	فیلای مختصر
یادداشت	فهرستنحوی کامل این اثر در نشانی: <a href="http://opac.nlai.ir">http://opac.nlai.ir</a> قابل دسترسی است
یادداشت	کتابنامه.
شماره کتابشناسی ملی	۳۸۷۲۰۶۳

انتشارات پندارپارس



**دفتر فروش: انقلاب، ابتدای کارگر جنوبی، کوی رشتچی، شماره ۱۴، واحد ۱۶**  
**تلفن: ۰۹۱۲۴۵۳۴۸ - تلفکس: ۰۶۶۵۷۶۶۵۷۸ - ایمیل: 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 ۹۴
شمارگان	: ۵۰۰ نسخه
طرح جلد و صفحه‌آرایی	: سارا یعسویی
چاپ، صحافی	: روز

قیمت : ۱۰۰۰ تومان شابک : ۸۴-۴۷۸-۶۰۰-۶۵۲۹\*

## فهرست

۳.....	فصل ۱- آشنایی با مفاهیم و محیط NESSUS
۴ .....	مفاهیم
۵ .....	نمای کلی از واسط کاربری Nessus
۶ .....	Installation
۱۹.....	فصل ۲- آشنایی با ساختار POLICY و مدیریت آن در NESSUS
۱۹.....	سیاست‌ها (Policies)
۲۹ .....	سروریس‌های Cloud
۳۲ .....	Database
۳۴ .....	Host
۳۴ .....	الف- Windows
۴۲ .....	Unix
۴۴ .....	SNMPv3
۴۶ .....	Settings
۴۸ .....	تنظیمات Discovery
۵۸ .....	تنظیمات Assessment
۶۲ .....	Web Applications
۶۹ .....	Report
۷۱ .....	Advanced
۷۴ .....	Mobile Device Management
۷۶ .....	ایجاد یک Scan
۷۶ .....	Plugins and Policy Preferences
۷۷ .....	مدیریت اعتبار در دستگاه‌های تلفن همراه

۸۳	..... مدیریت وصله (Patch Management)
۸۴	..... IBM Tivoli Endpoint Manager (BigFix)
۸۸	..... WSUS
۹۰	..... SCCM
۹۱	..... Red Hat Network Satellite
۹۱	..... Dell KACE K1000
۹۲	..... Symantec Altiris
۹۶	..... اسکن با چندین مدیریت وصله
۹۷	..... مجازی سازی
۹۷	..... VMware
۹۹	..... Red Hat Enterprise Virtualization (RHEV)
۹۹	..... احراز هویت های متفرقه (Miscellaneous Authentication)
۱۰۲	..... احراز هویت پروتکل های Plaintext
۱۰۴	..... اسکن برنامه های تحت وب
۱۱۱	..... Plugins
۱۱۴	..... Compliance Audit Policies
۱۱۷	..... Offline Configuration Audit Policies
۱۱۸	..... PCI Policies
۱۱۹	..... الزامات استاندارد PCI DSS
۱۲۱	..... SCAP Policies
۱۲۵	..... فصل ۳ - اجرای عملیات اسکن
۱۲۵	..... Scan
۱۲۸	..... مثال هایی برای فایل میزبان
۱۳۷	..... فصل ۴ - نتایج اسکن و گزارش ها

۱۳۷.....	نتایج و گزارش‌های اسکن.....
۱۳۸.....	Dashboard
۱۴۵.....	نتایج انطباق.....
۱۴۷.....	محدودسازی‌های گزارش.....
۱۵۴.....	CPE چیست؟.....
۱۵۵.....	CVSS چیست؟.....
۱۵۶.....	CVE چیست؟.....
۱۵۶.....	Bugtraq ID چیست؟.....
۱۵۶.....	CERT Advisory ID
۱۵۷.....	OSVDB ID
۱۵۷.....	Secunia ID
۱۵۷.....	Exploit Database ID
۱۵۷.....	Metasploit Name and Framework
۱۵۸.....	Screenshot های گزارش.....
۱۵۹.....	اسکن یا KB مربوط به اسکن.....
۱۶۲.....	Knowledge Base بارگذاری کردن (Upload) و استخراج (Export) گزارش‌ها.....
۱۶۳.....	سفارشی کردن فرمتهای PDF و HTML
۱۶۴.....	حذف نتایج اسکن.....
۱۶۷.....	<b>پیوست ۱- نصب NESSUS بر روی سیستم عامل ویندوز.....</b>
۱۶۷.....	نصب Nessus در ویندوز (با دسترسی مستقیم به اینترنت)
۱۷۴.....	نصب Nessus در ویندوز (بدون دسترسی مستقیم به اینترنت)
۱۷۷.....	<b>پیوست ۲- نمونه‌ای از اسکن در محیط واقعی .....</b>



## 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](mailto: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 به منظور 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 بسته 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 به منظور اسکن پشتیبانی می‌کند. این ساختارها شامل سیستم‌عامل‌های مختلف، انواع مجازی سازها و پروتکل‌های شبکه می‌باشد.

هرسته‌ی 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 به کار گرفت. باید برای افزایش سرعت تست خود، پلاگین‌هایی را که مربوط به هفتان نیست غیرفعال 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، روایی که در طی اسکن مدنظرتان است را مشخص می‌نمایید. این روای شامل مشخصات اولیه، نحوه شناسایی پورت‌ها، تنظیمات گزارش، تعیین پلاگین‌های مورد نیاز، تعریف اعتبار یا نامهای کاربری و گذرواژه‌ها برای آزمون جعبه سفید می‌باشد. البته سیاست‌هایی 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

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 ۶.۳ 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](mailto: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 نمایه‌ای کلی موارد انجام شده را نمایش می‌دهد.
- مدیریت اسکن‌ها توسط Nessus Manager مرکزی برای گسترش سیاست‌ها (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 مجازی 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 می‌توانند 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: hostname، IPv6، IPv4 و CIDR نماد.
- 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 متعدد برای اسکنر Nessus و رای 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 می‌توانند 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 پیشرفت‌های اجرا شود.

این واسط کاربری با بیشتر مرورگرها سازگاری دارد که از جمله آنها می‌توان به Mozilla Firefox 32، Google Chrome 37، Safari 7.1، Opera 24 و IE10 در روی دسکتاپ و 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

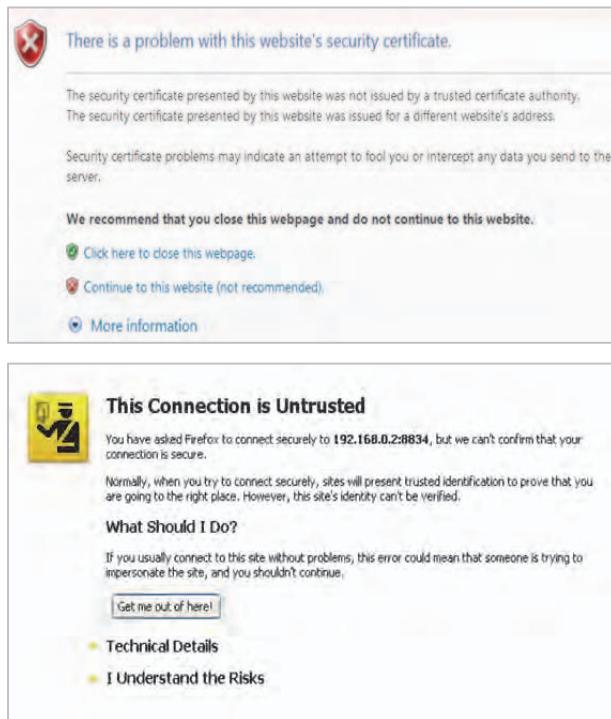
واسط کاربری در Nessus از طریق پروتکل HTTPS با شماره پورت ۸۸۳۴ قابل دسترسی خواهد بود. هر کاربر باید دارای یک نام کاربری و گذرواژه‌ی یکتا باشد.

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 نمی‌گردد.



نخستین باری که تلاش می‌کنید به واسطه کاربری Nessus متصل شوید، بیشتر مرورگرهای وب هشداری مشابه تصویر زیر را نمایش می‌دهند که سایت، مورد اطمینان نیست. (یک 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 واسطه 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 کنند.

## پویش آسیب‌پذیری و تست نفوذ با Nessus

۸



در این بخش باید آدرسی را که در کادر Location قرار دارد را کنترل نمایید و سپس بر روی "کمکی 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 گذر واژه تنظیم نمایید. باید به این نکته توجه داشته باشید که ذخیره‌سازی نام کاربری و گذر واژه را تنها در سیستمی که در یک محل امن قرار دارد انجام دهید. پس از احرار همیت 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.

The screenshot shows the Nessus Manager web interface. At the top, there's a navigation bar with the Nessus logo, 'Scans 3 Policies', and a dropdown for 'admin'. Below the header is a search bar labeled 'Search Scans' and an 'Upload' button. On the left, there's a sidebar with 'New Scan' (highlighted in blue), 'My Scans' (selected), 'Trash', 'All Scans', and 'New Folder'. The main area is titled 'Scans / My Scans' and lists three scan configurations:

	Name	Schedule	Last Scan
<input type="checkbox"/>	DMZ Network Scan	On Demand	December 09
<input type="checkbox"/>	Host Discovery Internal Net	On Demand	December 09
<input type="checkbox"/>	SonicWall	Disabled	December 09

At the bottom right of the interface, there's a small note: '© 1998 - 2014 Tenable Network Security, Inc. All Rights Reserved. Nessus Manager v. 6.2.0'.

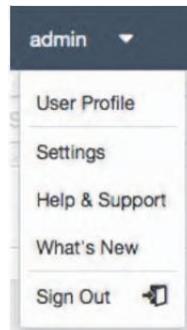
در طول زمانی که از Nessus استفاده می‌نمایید در بخش بالایی و سمت چپ، تنظیمات و منوها نمایش داده می‌شود. بخش "admin" در بالا و سمت چپ قرار دارد که نشان دهنده حساب کاربری وارد شده است. این بخش همچنین دارای زیر شاخه‌هایی نیز هست که به آن اشاره خواهیم کرد. در سمت راست این بخش، آیکن یک زنگ را می‌بینید که آخرین 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 فلاش کنار "admin" کلیک می‌کنید، منویی نمایش داده می‌شود که دسترسی به پروفایل خود، تنظیمات عمومی Nessus، اطلاعات درباره‌ی نصب، بخش help & support 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 پوشش‌ها و صفحه مربوط به Plugin Rules نیز بخش‌های دیگری است که در این بخش قرار دارند.

User Profile / Account Settings		
Account Settings	Username	admin
Change Password	Full Name	admin
Plugin Rules	Email	admin@example.com
	User Type	System Administrator
<input type="button" value="Save"/> <input type="button" value="Cancel"/>		

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

User Profile / Account Settings

Username	a[REDACTED]@tenable.com
Full Name	Anne [REDACTED]
Email	a[REDACTED]@tenable.com
User Type	Administrator

**Scans**

Account Settings  
Change Password  
Plugin Rules

Save Cancel

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 Standard، System Administrator 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.

User Profile / Change Password

New Password	[REDACTED] <small>REQUIRED</small>
Confirm Password	[REDACTED] <small>REQUIRED</small>

**Settings**

Account Settings  
Change Password  
Plugin Rules

Save Cancel

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 Rule

## پویش آسیب‌پذیری و تست نفوذ با Nessus

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 Low Info, Hide, Critical, High, Medium باشد را تنظیم نمایید.

Host	Leave empty for all hosts.
Plugin ID	Nmap
Expiration Date	Options
Severity	Hide this result

Save      Cancel

## تنظیمات

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

The screenshot shows the Nessus Manager interface with the title bar "Nessus" and user "admin". The main menu includes "Scans", "Policies", and a notification icon. The "Settings" tab is selected, followed by "Scanners". The sub-menu shows "Scanners / Local / Overview". The interface displays statistics for LOCAL, REMOTE, and AGENTS sections, including the number of licensed hosts, scanners, and agents, along with version numbers and update information for Nessus Manager and Plugins.

LOCAL		Scanners / Local / Overview	
Overview	Nessus Manager	Plugins	
Permissions	Version 6.3.0	Last Updated February 20, 2015	
Software Update	Licensed Hosts 169	Expiration February 27, 2015	
REMOTE		Licensed Scanners 5	Plugin Set 201502201415
AGENTS		Licensed Agents 6	Activation Code
Linked			
Groups			

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.

The screenshot shows the Nessus Scanner Settings interface with the title bar "Nessus" and user "admin". The main menu includes "Scans", "Policies", and a notification icon. The "Settings" tab is selected, followed by "Scanners". The sub-menu shows "Scanners / Local / Overview". The interface displays statistics for LOCAL section, including the number of licensed hosts, scanners, and agents, along with version numbers and update information for Nessus Scanner and Plugins.

LOCAL		Scanners / Local / Overview	
Overview	Nessus Scanner	Plugins	
Link	Version 6.3.0	Last Updated N/A	
	Owner system	Expiration N/A	
	Last Connection February 24, 2015 07:55:13	Plugin Set N/A	
	Platform LINUX	Activation Code N/A	

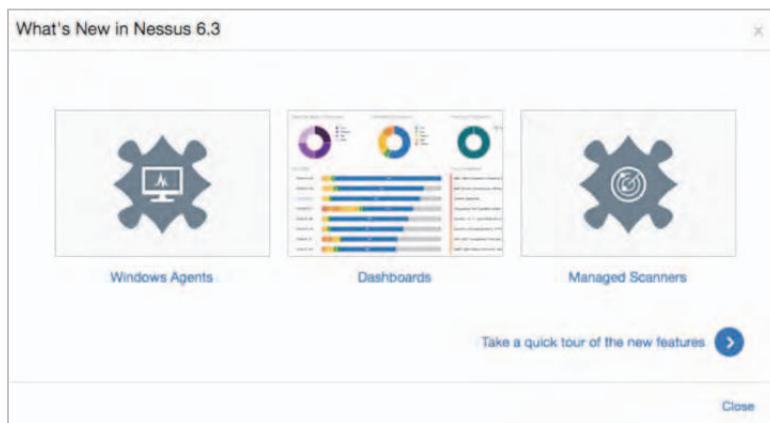
بخش "Settings" برای Nessus Professional دسترسی به صفحه "Overview"، حساب‌ها، ارتباطات با سورورهای میل و پراکسی خارجی و بخش Advanced Scanner (اگر کاربر جاری یک Administrator باشد) را فراهم می‌کند.

Scanners / Local / Overview		
LOCAL	Nessus Professional	Plugins
Overview	Version: 6.3.0	Last Updated: February 25, 2015
Link	Owner: system	Expiration: September 30, 2015
Software Update	Last Connection: February 25, 2015 14:51:45	Plugin Set: 201502251415
	Platform: LINUX	Activation Code: [REDACTED]

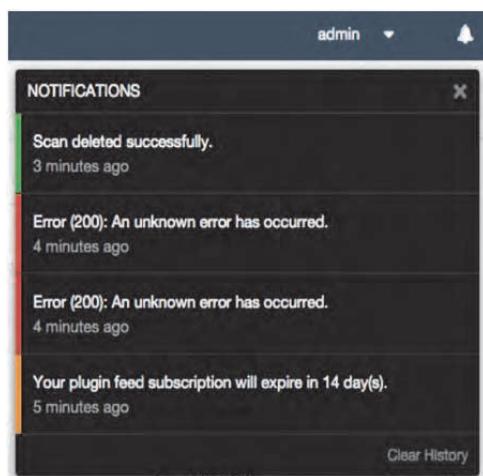
بخش "What's new" لینکی است که به شما ویژگی‌های جدید این نسخه از Nessus را نشان می‌دهد. در تصویر زیر نمونه‌ای از ویژگی‌هایی را که در نسخه ۶.۳ از Nessus ایجاد شده است مشاهده می‌کنید.

بخش "Help & Support" لینکی است که پورتال Tenable Support را در یک tab جدید باز می‌کند. نشست شما با Nessus را پایان خواهد داد و از برنامه خارج می‌شوید.

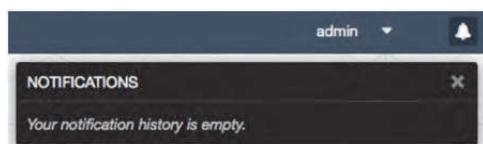
همان‌گونه که در بخش‌های پیشین اشاره شد، در بالای صفحه و سمت راست، کنار بخش "admin" آیکن زنگ مشاهده می‌شود. در این بخش هرگونه پیامی مربوط به عملکردهای Nessus شامل هشدارها، پیغام‌های مربوط به نسخه جدید Nessus، رخدادهای مربوط به نشست کنونی و دیگر موارد نمایش داده می‌شود.



این بخش همچنین به عنوان محلی برای فراهم نمودن هر هشدار دیگر یا پیام‌های خطاب‌بوسیله پاپ‌آپ‌هایی که به صورت کم رنگ و کوتاه می‌باشد، 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 به شکل 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 Enterprise Cloud و Nessus Manager 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 Kerberos یا IMAP، POP، FTP، HTTP
- 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 اینمن دستگاه‌های شبکه بدون نیاز به اسکن مستقیم دستگاه‌ها.
- Windows Malware Scan که MD5‌های فایل‌ها را مقایسه می‌کند و فایل‌های سالم و آلوه را از هم تشخیص می‌دهد.