tenable™

Nessus NM™ Manager

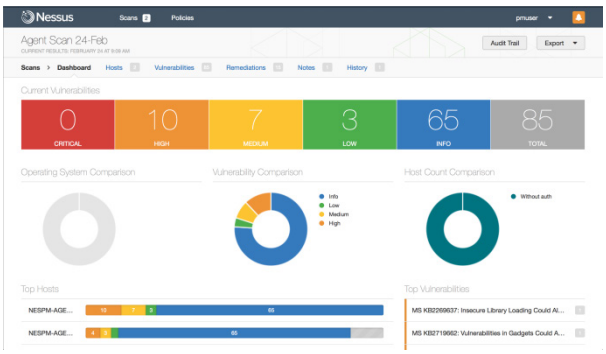
Nessus Manager met la puissance de Nessus à la disposition des équipes de sécurité et d'audit, avec des scans distribués gérés de façon centralisée

La gestion des vulnérabilités pour les équipes

Nessus® Manager combine les puissantes fonctions de détection, d'analyse et d'audit de Nessus, le scanner de vulnérabilité le plus déployé au monde, avec de nombreuses fonctions de collaboration et de gestion pour réduire votre surface d'attaque.

Nessus Manager permet le partage de ressources, dont les scanners Nessus, les programmes de scan, les politiques et les résultats de scan entre plusieurs utilisateurs ou groupes. Les utilisateurs peuvent exploiter et partager les ressources et les responsabilités avec leurs collègues, les propriétaires des systèmes, les auditeurs internes, les membres des équipes risque et conformité, les administrateurs informatiques, les administrateurs réseau et les analystes de sécurité. Ces fonctions de collaboration réduisent le temps et le coût des scans de sécurité et des audits de conformité en simplifiant non seulement les scans, mais également les processus de découverte et de correction des malwares et des mauvaises configurations.

Nessus Manager protège les environnements physiques, virtuels, mobiles et cloud. Nessus Manager est disponible pour un déploiement sur site. Tenable.io Vulnerability Management est à la disposition des organisations qui recherchent une solution hébergée dans le cloud. Nessus Manager prend en charge la plus grande gamme de systèmes, d'appareils et d'actifs, et grâce à des options de déploiement sans agent ou avec Nessus Agent, s'étend facilement aux environnements mobiles, transitoires et difficiles d'accès.



Assistance multi-scan

Nessus Manager permet le contrôle de plusieurs scanners Nessus, ce qui permet d'étendre facilement les scans dans des réseaux complexes, dans des déploiements cloud et entre des sites géographiques différents. Les utilisateurs peuvent planifier les scans, mettre en œuvre les politiques et afficher les résultats en provenance de divers scanners sur une seule console centrale.

Intégration

Nessus Manager s'intègre aux solutions de gestion de correctifs d'IBM, de Microsoft, de Red Hat et de Dell pour assurer l'application des mises à jour logiciel dans les systèmes et les actifs en fonction de leur importance pour l'organisation.

Nessus Manager s'intègre également avec les solutions de gestion d'appareils mobiles (MDM) de Microsoft, Apple, Good, MobileIron et AirWatch pour permettre aux organisations d'ajouter des appareils mobiles au programme de gestion des vulnérabilités.

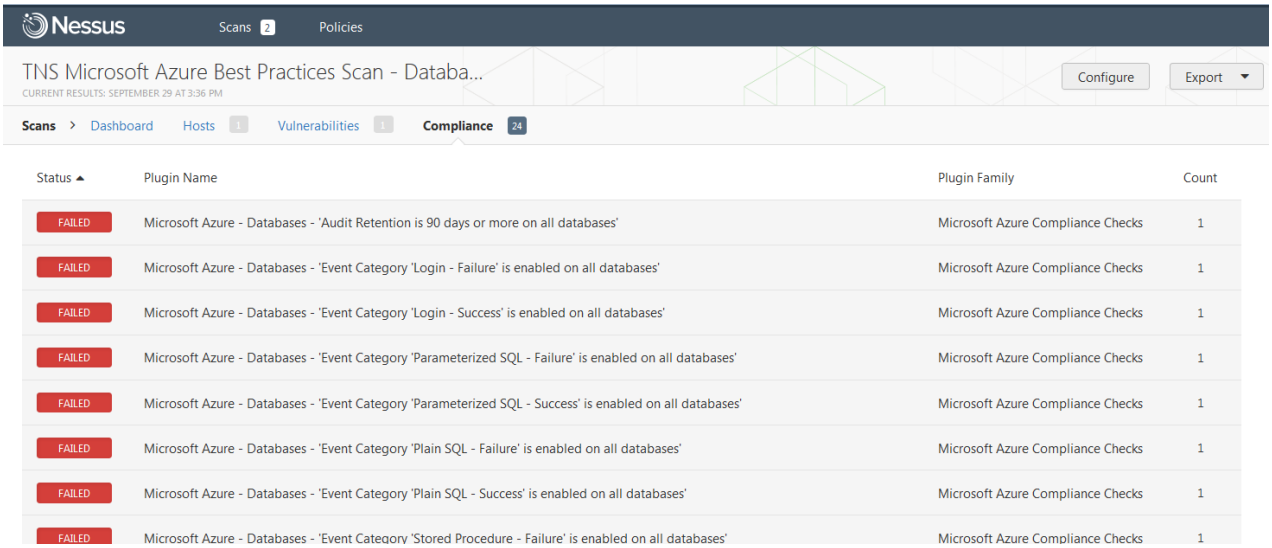
L'intégration de la gestion des mots de passe avec CyberArk facilite la gestion des données d'identification pour les organisations qui utilisent cette solution.

Nessus Manager réduit la surface d'attaque et favorise la conformité en analysant les déploiements dans le cloud tels que Microsoft Azure, AWS et Rackspace, et en conduisant des audits sur eux.

Principaux avantages

- Des scans exacts, avérés et pleinement pris en charge : basés sur le scanner de vulnérabilités Nessus
- Partagez les ressources pour améliorer l'efficacité de l'équipe : affectez les scanners, les politiques et les programmes, puis communiquez l'accès à plusieurs utilisateurs ou groupes
- Étendez la portée des scans : utilisez Nessus Agents pour analyser des appareils transitoires comme des ordinateurs portables ou d'autres actifs pour lesquels vous ne disposez pas de données d'identification d'hôte
- Améliorez l'analyse des risques : ajoutez le contexte à partir des cadres d'infrastructure et de partenaire existants
- Assurez l'intégration aux technologies de base : Nessus Manager vous permet de tirer parti de votre investissement dans des technologies complémentaires, telles que les solutions de gestion de correctifs et d'appareils mobiles

SC MAGAZINE



Nessus Manager inclut divers audits de configuration pour les clouds tels que Microsoft Azure, Amazon Web Services, Rackspace et d'autres.

Niveaux d'utilisateur fondés sur les rôles

Nessus Manager permet d'ajouter plusieurs utilisateurs et propose quatre rôles d'utilisateur : administrateur système, administrateur, standard et lecture seule. Chaque utilisateur peut recevoir plusieurs niveaux d'accès aux ressources en fonction de la personne ou du groupe auquel elle appartient. L'administrateur système et l'administrateur ont l'autorité requise pour gérer les utilisateurs et les groupes. En fonction de vos besoins précis, vous pouvez créer des groupes selon les services, les fonctions, les tâches ou responsabilités et l'emplacement géographique.

Équipe de recherche

Compte tenu de l'apparition constante de nouvelles vulnérabilités et menaces, l'équipe de recherche Tenable met fréquemment à jour Nessus Manager pour aider les organisations à combattre les menaces les plus complexes et les vulnérabilités zero day, et pour prendre en charge les nouvelles configurations de conformité réglementaires.

L'avantage Nessus

Les clients optent pour Nessus en raison des avantages suivants :

- Scans à grande exactitude avec faible quantité de faux positifs
- Fonctionnalités d'analyse complètes
- Évolutivité sur des centaines de milliers de systèmes
- Facilité de déploiement et de maintenance
- Faible coût d'administration et d'exploitation

Agents Nessus

Nessus Agents, qui est disponible avec Tenable.io et Nessus Manager, élimine les ennuis liés aux scans de réseau traditionnels, tels que l'obtention des données d'identification nécessaires, tout en facilitant l'analyse d'une plus grande gamme d'actifs, y compris les actifs hors ligne.

La plupart des organisations utilisent une combinaison de scans avec et sans agent dans leur environnement Nessus. Nessus Agents est une option attrayante dans certains cas de figure, tels que :

- **Appareils transitoires** : scans d'ordinateurs portables ou d'autres appareils transitoires qui ne sont pas connectés en permanence au réseau local.
- **Scans sans données d'identification d'hôte** : actifs que vous souhaitez ou devez analyser sans données d'identification.
- **Scans rapides** : lorsque déployés, les agents utilisent les ressources hôtes locales pour les scans et utilisent les ressources du réseau uniquement pour renvoyer les résultats à Nessus Manager, ce qui vous permet d'analyser rapidement un grand nombre d'actifs.

Formation

Tenable propose des formations aux débutants et à ceux qui souhaitent disposer des connaissances et du savoir-faire requis pour maximiser leur utilisation de Nessus, ainsi que des formations spécialisées pour les utilisateurs plus avancés, par exemple pour des thèmes tels que les audits de conformité. Les cours sont disponibles à la demande sur le site Web de Tenable.

tenable™

Pour en savoir plus : visitez tenable.com
Nous contacter : envoyez-nous un e-mail à l'adresse subscriptionsales@tenable.com ou contactez-nous via tenable.com/contact