tenable

Nessus NP™ Professional

Nessus a été déployé par plus d'un million d'utilisateurs à travers le monde à des fins d'audit des vulnérabilités, de la configuration et de la conformité.

Scanner de vulnérabilité Nessus Professional

Nessus® Professional, la solution d'audit de la vulnérabilité la plus largement déployée du secteur, vous aide à réduire la surface d'attaque de votre organisation et à garantir la conformité. Nessus dispose entre autres de fonctions de découverte des ressources à grande vitesse, d'audit de la configuration, de profilage des cibles, de détection des malwares et de découverte des données sensibles.

Nessus prend en charge plus de technologies que les solutions concurrentes, en réalisant un scan des systèmes d'exploitation, des dispositifs de réseau, des pare-feux nouvelle génération, des hyperviseurs, des bases de données, des serveurs Web et des infrastructures essentielles à la recherche de vulnérabilités, de menaces et de violations de la conformité.

Fort de sa bibliothèque de contrôles des vulnérabilités et de la configuration (la plus grande bibliothèque au monde de ce type continuellement mise à jour) et de l'assistance de l'équipe d'experts en recherche sur la vulnérabilité de Tenable, Nessus définit la norme en matière de vitesse et de précision de l'analyse des vulnérabilités.

Caractéristiques de Nessus

Rapports et surveillance

- Rapports flexibles : personnaliser les rapports pour les trier par vulnérabilité ou par hôte, créer un résumé analytique ou comparer les résultats des scans pour mettre en évidence les changements
    - Formats natif (XML), PDF (nécessite que Java soit installé sur le serveur Nessus), HTML et CSV
- Notifications ciblées par e-mail des résultats des scans, recommandations de réparations et améliorations de la configuration des scans

Couverture complète des vulnérabilités

- Virtualisation et cloud
- Malwares et botnets
- Audit de configuration
- Applications Web

Principaux avantages

- **Réduction de la surface d'attaque** : prévient les attaques en identifiant les vulnérabilités à traiter
- **Exhaustivité** : respecte le plus large éventail de normes de conformité et de normes réglementaires
- **Évolutivité** : démarrez avec une licence Nessus Professional pour un seul utilisateur, puis passez à Nessus Manager ou Tenable.io lorsque vos besoins en matière de gestion des vulnérabilités augmentent
- **Faible coût total de possession** (TCO) : une solution de scan des vulnérabilités complète pour un moindre coût
- **Mise à jour continue :** ajout continuel de nouveau contenu par l'équipe de recherche de Tenable

SC MAGAZINE

Capacités de scan

- Découverte : découverte des actifs précise et à haut débit
- Scans : scans des vulnérabilités (y compris les réseaux IPv4/IPv6/hybrides)
    - Découverte non accréditée des vulnérabilités
    - Scans accrédités pour la sécurisation renforcée du système et les correctifs manquants
    - Satisfait toutes les exigences de la norme PCI DSS en matière de scan interne de vulnérabilité
- Couverture : couverture des actifs et profilage étendus
    - Périphériques réseau : pare-feux/routeurs/commutateurs (Juniper, Check Point, Cisco, Palo Alto Networks), imprimantes, stockage
    - Audits de configuration des périphériques réseau effectués hors ligne

- Virtualisation VMware ESX, ESXi, vSphere, vCenter, Microsoft, Hyper-V, Citrix Xen Server
- Systèmes d'exploitation : Windows, OS X, Linux, Solaris, FreeBSD, Cisco iOS, IBM iSeries
- Bases de données : Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL, MongoDB
- Applications Web : serveurs Web, services Web, vulnérabilités de l'OWASP
- Cloud : scans de la configuration des applications dans le cloud telles que Salesforce et des instances de cloud comme Amazon Web Services, Microsoft Azure et Rackspace
- Conformité : contribue au respect des exigences gouvernementales, réglementaires et d'entreprise
- Contribue au respect des exigences de la norme PCI DSS en matière de configuration sécurisée, renforcement de la sécurité des systèmes, détection des malwares, scans des applications Web et contrôles d'accès

- Menaces : audits des botnets/programmes malveillants, processus/antivirus
  - Détecte les virus, les malwares, les backdoors, les hôtes communiquant avec des systèmes infectés par des botnets, les procédés connus/inconnus, les services Web reliés à du contenu malveillant
  - Audits de conformité : FFIEC, FISMA, CyberScope, GLBA, HIPAA/HITECH, NERC, SCAP, SOX
  - Audits de configuration : CERT, CIS, COBIT/ITIL, DISA STIG, FDCC, ISO, NIST, NSA, PCI
- Audits des systèmes de contrôle : systèmes SCADA, appareils embarqués et applications ICS
- Audits des contenus sensibles : PII (par exemple, numéros de cartes de crédit, numéros de sécurité sociale)

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

Déploiement et gestion

- Déploiement flexible : logiciels, matériels, dispositifs virtuels déployés sur site ou dans le cloud d'un prestataire de services.
- Options de scan : prise en charge des balayages à distance, certifiés et non certifiés, des recherches locales pour une analyse approfondie et granulaire des ressources en ligne, hors ligne ou à distance.
- Configuration/politiques : politiques et modèles de configuration prêts à l'emploi.
- Scores des risques : classement des vulnérabilités basé sur CVSS, cinq niveaux de gravité (Critique, Élevé, Moyen, Faible, Info), niveaux de gravité personnalisables pour la reclassification du risque.
- Hiérarchisation : corrélation avec les outils de développement et d'exécution d'exploits (Metasploit, Core Impact, Canvas et ExploitHub) et filtrage en fonction de la capacité d'exploitation et de la gravité.
- Évolutivité : prise en charge d'API compatible REST pour l'intégration de Nessus à votre processus de gestion des vulnérabilités.

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