nessus professional

DATENBLATT

NESSUS PROFESSIONAL

DER BRANCHENSTANDARD FÜR SCHWACHSTELLEN-BEWERTUNG

Knappe Ressourcen, begrenzte Zeit, eine sich ständig verändernde Angriffsoberfläche – für Sicherheitsfachkräfte ist es eine Herausforderung, mit Angreifern Schritt zu halten. Es wird eine schnelle und unkomplizierte Methode benötigt, um Schwachstellen proaktiv erkennen und beheben zu können.

Nessus® Professional automatisiert Point-in-Time-Schwachstellenbewertungen zur schnelleren Erkennung und Behebung von Schwachstellen, einschließlich Softwarefehlern, fehlenden Patches, Malware und Fehlkonfigurationen, für eine Vielzahl von Betriebssystemen, Geräten und Applikationen.

NESSUS – DIE NUMMER EINS BEI DER SCHWACHSTELLEN-BEWERTUNG

Nummer Eins bei Genauigkeit

Nessus hat die niedrigste False-Positive-Rate der Branche mit Six-Sigma-Genauigkeit (0,32 Defekte pro 1 Million Scans).

Nummer Eins bei Abdeckung

Nessus bietet die tiefste und umfassendste Abdeckung – mit über 62.000 CVEs und mehr als 100 neuen Plugins, die wöchentlich innerhalb von 24 Stunden nach Aufdeckung einer Schwachstelle veröffentlicht werden.

Nummer Eins bei Akzeptanz

Mehr als 30.000 Unternehmen weltweit setzen auf Nessus – 2 Millionen Downloads sprechen für sich. 50 % der Fortune 500-Unternehmen und über 30 % der Global 2000 schenken Nessus-Technologie ihr Vertrauen.

REICHWEITE DER ABDECKUNG

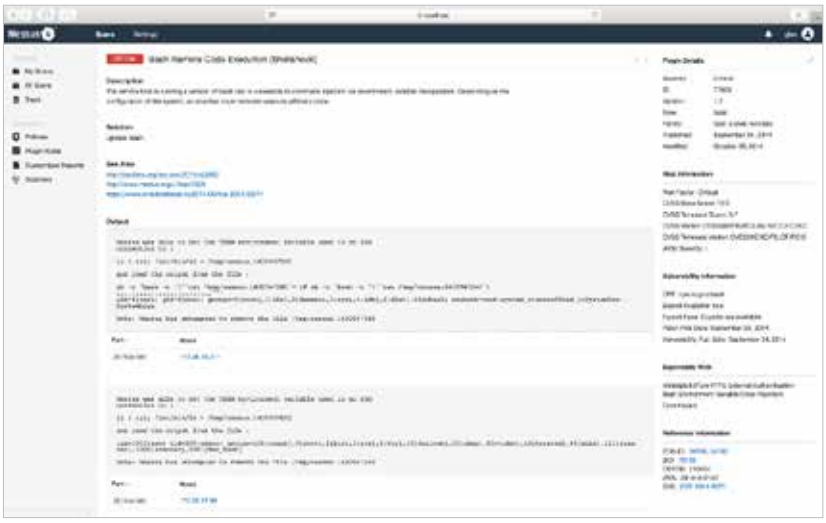
Tenable Research arbeitet eng mit der Security-Community zusammen, um neue Schwachstellen aufzudecken und Erkenntnisse bereitzustellen, mit denen Unternehmen ihre Verfahren zur Schwachstellenbewertung optimieren können. Das Zero-Day-Team von Tenable hat in den letzten drei Jahren mehr als 100 Zero-Day-Schwachstellen aufgedeckt.

DYNAMISCHE UND AUTOMATISCHE PLUGIN-UPDATES REDUZIEREN ZEITAUFWAND FÜR BEWERTUNG UND BEHEBUNG

Mit über 157.000 Plugins, die in Echtzeit aktualisiert werden, lässt sich mit Nessus wertvolle Zeit bei der Bewertung, Untersuchung und Behebung von Problemen sparen.

Um Effizienz und Genauigkeit zu gewährleisten, werden Plugins dynamisch kompiliert. Dies senkt den Speicherplatzbedarf der Nessus Plugin-Datenbank um bis zu 75 % und steigert zugleich die Scan-Performance.

- Mithilfe kundenspezifischer Plugins können spezielle Checks erstellt werden, anhand derer die Sicherheit unternehmensspezifischer Applikationen beurteilt werden kann.
- Kundenspezifische Audit-Dateien unterstützen Sicherheitsteams dabei, die Konfigurationsanforderungen und Compliance-Standards ihres Unternehmens zu verifizieren.



Bei jedem automatischen Plugin-Update werden eine Reihe einfacher Behebungsmaßnahmen angeboten sowie eine schnelle und einfache Möglichkeit, um festzustellen, ob Ihre Systeme gefährdet sind.

Erkenntnisse aus Threat-Intelligence-Feeds

Dank der nahtlosen Integration verschiedener kommerzieller Threat-Intelligence-Feeds erhalten Sie Einblick in potenzielle Malware und Ransomware, die auf Hosts in Ihrer Umgebung ausgeführt wird.

NUTZUNG DER LEISTUNGSSTÄRKE VON PREDICTIVE PRIORITIZATION

Nutzen Sie die Vorteile des Vulnerability Priority Rating (VPR) von Tenable, mit dessen Hilfe Sie sich auf die Schwachstellen konzentrieren können, die das größte Risiko für Ihre spezifische Umgebung darstellen. Das VPR kombiniert von Tenable gesammelte Schwachstellendaten mit Daten zu Schwachstellen und Bedrohungen von Drittanbietern und analysiert diesen Datenbestand mit dem fortschrittlichen datenwissenschaftlichen Algorithmus, der von Tenable Research entwickelt wurde.

Umfassende Sichtbarkeit von Schwachstellen

Jede Bewertung bietet einen umfassenden und tiefgreifenden Einblick in Schwachstellen. Nessus bietet Abdeckung für mehr als 47.000 verschiedenartige IT-Assets. Dazu zählen:

- Netzwerkgeräte (z. B. Cisco, Juniper, HP, F5 und SonicWall)
- MobileIron und VMware AirWatch, um Mobilgeräte anhand von Richtlinien auf Schwachstellen zu prüfen
- Betriebssysteme (z. B. Windows, MacOS und Linux)
- Applikationen – von einfachen Hilfsprogrammen für Treiber-Updates bis hin zu komplexen Office-Suites

„Gut durchdachte Oberfläche, auf der Plugins übersichtlich und strukturiert klassifiziert werden."

– Nessus-Anwender

CONSULTANTS LIEBEN NESSUS

Nessus eignet sich ideal für Security Consultants, da es folgende Vorteile bietet:

- **Unbegrenzte Bewertungen**
  Keine Begrenzung der Anzahl von IPs oder Assessments.
- **Leicht übertragbare Lizenz**
  Lizenzen können schnell und problemlos zwischen Computern übertragen werden. Mit der Nessus on Raspberry Pi-Option profitieren Sie von einem Höchstmaß an Portabilität und Benutzerfreundlichkeit.
- **Konfigurierbare Berichte**
  Berichte lassen sich mühelos mit Kundenname und -logo anpassen und können nach jeder Bewertung direkt per E-Mail an den Kunden gesendet werden.

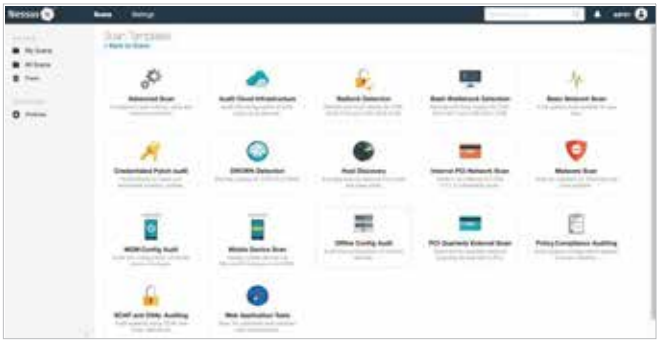
EINFACHE NUTZUNG

Nessus wurde von Sicherheitsexperten für Sicherheitsexperten entwickelt und sorgt durch seine intuitive Benutzerfreundlichkeit für eine schnellere und zuverlässigere Erkennung und Behebung von Schwachstellen.

Navigation und Nutzungserlebnis wurden durch UX-Updates einfacher und intuitiver gestaltet. Im neuen Nessus-Ressourcencenter haben Nutzer relevante Informationen stets zu Hand. Benutzerspezifische Anleitungen bieten umsetzbare Tipps und Empfehlungen auf der Grundlage der jeweils ausgeführten Vorgänge und Funktionen.

Schnelle Erkennung von Schwachstellen dank vorgefertigter Richtlinien und Vorlagen

Dank sofort einsetzbarer, vorkonfigurierter Vorlagen für mobile und IT-Assets, einschließlich Konfigurationsprüfungen, kann schnell erkannt werden, wo Schwachstellen vorliegen.



Mehr als 450 Compliance- und Konfigurationsvorlagen ermöglichen die Beurteilung der Konfigurationskonformität anhand von CIS-Benchmarks und anderen Best Practices.

Intelligente Schwachstellenbewertung mit Live Results

Mit Live Results wird die Schwachstellenbewertung bei jedem Plugin-Update automatisch im Offlinemodus durchgeführt – ohne dass ein Scan erforderlich ist. Nach dem Einloggen werden die Ergebnisse zu potenziellen Schwachstellen basierend auf dem jeweiligen Scanverlauf angezeigt. Mit nur einem Klick kann ein Scan durchgeführt werden, um das Vorhandensein der Schwachstelle zu bestätigen. Der Prozess für die Bewertung, Priorisierung und Behebung von Schwachstellen gestaltet sich dadurch schneller und effizienter.

Einfache Konfiguration von Berichten

Die Berichterstellung erfolgt auf Grundlage angepasster Ansichten (z. B. bestimmte Arten von Schwachstellen, Schwachstellen nach Host/Plugin oder nach Team/Kunde) in verschiedenen Formaten (HTML, CSV und Nessus XML).

Drilldown und Fehlerbehebung

Netzwerke werden zunehmend differenzierter und komplexer, wodurch sich die Bestimmung von potenziellen Problemen als immer zeitaufwendiger erweist. Die Nessus-Funktion zur Erfassung von Datenpaketen ermöglicht eine leistungsstarke Fehlersuche zur Behebung von Scanning-Problemen.

Präzise Fokussierung dank gruppierter Ansicht

Ähnliche Probleme oder Kategorien von Schwachstellen werden in einer Gruppe zusammengefasst und in einem Thread dargestellt. Mit der Snooze-Funktion können bestimmte Schwachstellen für einen festgelegten Zeitraum aus der Ansicht ausgeblendet werden. Dies erleichtert die Priorisierung, da sich der Nutzer ausschließlich auf die Schwachstellen konzentrieren kann, mit denen er sich gerade befasst.

Portierbar und flexible

Nessus ist ab sofort für Raspberry Pi verfügbar, um Portabilität und Benutzerfreundlichkeit zu gewährleisten. Dies ist insbesondere für Pen Tester, Consultants und andere Personen nützlich, deren Tätigkeit Mobilität zwischen Standorten erfordert.

ADVANCED SUPPORT ERHÄLTLICH

Kunden mit Nessus Professional haben auf Subscription-Basis rund um die Uhr Zugang zur „Advanced"-Stufe des technischen Supports – per E-Mail, Portal, Chat und Telefon. Dies trägt außerdem zu schnelleren Reaktionszeiten und Lösungen bei Fragen und Problemen bei. Sämtliche Informationen zu unseren Support-Plänen finden Sie hier.

ÜBER TENABLE

Tenable®, Inc. ist das Cyber Exposure-Unternehmen. Über 30.000 Unternehmen aus aller Welt verlassen sich auf Tenable, wenn es um die Erkennung und Minimierung von Cyberrisiken geht. Als Erfinder von Nessus® hat Tenable sein Know-how im Bereich des Schwachstellen-Managements erweitert, um die weltweit erste Plattform bereitzustellen, mit der jedes digitale Asset auf jeder beliebigen Computing-Plattform erkannt und abgesichert werden kann. Zu den Kunden von Tenable zählen mehr als die Hälfte der Fortune 500-Unternehmen, mehr als 30 Prozent der Global 2000 sowie große Regierungsbehörden. Weitere Informationen finden Sie unter de.tenable.com.

Weitere Informationen: Besuchen Sie de.tenable.com
Kontakt: Bitte senden Sie eine E-Mail an sales-de@tenable.com oder besuchen Sie de.tenable.com/contact