tenable network security

Nessus® professional

Skaner podatności Nessus Professional

Nessus jest najpowszechniej stosowanym w branży skanerem podatności, który pomaga zmniejszyć obszar ataku i zapewnia zgodność w środowiskach fizycznym, wirtualnym, mobilnym i chmur. Nessus zapewnia szybkie badanie zasobów, audytowanie konfiguracji, profilowanie celów, wykrywanie złośliwego oprogramowania, danych wrażliwych i wiele innych.

Nessus wspiera więcej technologii niż konkurencyjne rozwiązania, skanuje systemy operacyjne, urządzenia sieciowe, hipernadzorców, bazy danych, serwery webowe i wrażliwą infrastrukturę pod kątem podatności, zagrożeń i naruszeń zasad zgodności.

Dzięki największej na świecie, ciągle uaktualnianej bibliotece podatności i testów konfiguracji oraz wsparciu przez zespół ekspertów firmy Tenable ds. badania podatności, Nessus stanowi standard szybkości i precyzji w skanowaniu podatności.

Nessus umożliwia użytkownikowi sortowanie i filtrowanie wyników za pomocą ponad 20 różnych kryteriów. Rankingi dotkliwości podatności mogą być dostosowywane wg potrzeb, podsumowanie zalecanych działań zapobiegawczych może posłużyć jako materiał dowodowy przy różnego rodzaju sporach.

Zalety Nessus

Raportowanie i monitorowanie

- Elastyczność raportowania: dostosowanie raportów wg podatności lub urządzenia, możliwość wygenerowania streszczenia dla zarządu lub porównania wyników różnych skanów w celu wyróżnienia zmian.
  - Standardowy (XML), PDF (wymagana jest instalacja Java na serwerze Nessus), formaty HTML i CSV.
- Celowane powiadomienia o wynikach skanowania wysyłane e-mailem, zalecenia działań naprawczych i usprawnień dot. konfiguracji skanów.

Nessus jest najbardziej zaufanym produktem do analizy bezpieczeństwa i zgodności, którego używa ponad 20 000 klientów na całym świecie.

Pełne pokrycie podatności:

- wirtualizacja i chmury
- szkodliwe oprogramowanie i botnety
- audyty konfiguracji
- aplikacje webowe

Kluczowe korzyści:

- **Zmniejsza liczbę miejsc potencjalnego ataku**: zapobiega atakom identyfikując podatności, które powinny zostać zlikwidowane
- **Wszechstronny**: odpowiada standardom regulatorów i wymogom zgodności w najszerszym zakresie
- **Skalowalny**: począwszy od pojedynczej licencji dla użytkownika Nessus Professional do Nessus Manager albo Nessus Cloud, jeśli tego wymagają zwiększające się potrzeby zarządzania podatnościmi
- **Niski całkowity koszt posiadania** (TCO): kompletne rozwiązanie do skanowania podatności przy niskich kosztach
- **Stale uaktualnianie**: zespół badawczy Tenable ciągle udostępnia aktualizacje
- **Łatwy dostęp:** dostęp przez przeglądarkę o dowolnej porze i w dowolnym miejscu

SC MAGAZINE

Zalety Nessus

Możliwości skanowania

- Wykrywanie: precyzyjne, wysoka szybkość wykrywania zasobów
- Skanowanie: skanowanie podatności (w tym IPv4/IPv6/sieci hybrydowe)
  - Wykrywanie podatności bez uwierzytelnienia
  - Skanowanie z uwierzytelnieniem w celu uszczelniania systemów i wykrycia braków poprawek
- Zakres: szeroki zakres zasobów i możliwości profilowania
  - Urządzenia sieciowe: firewalle/routery/switche (Juniper, Check Point, Cisco, Palo Alto Networks), drukarki, dyski sieciowe
  - Konfiguracja offline audytów urządzeń sieciowych
  - Wirtualizacja: VMware ESX, ESXi, vSphere, vCenter, Microsoft, Hyper-V, i Citrix Xen Server
  - Systemy operacyjne: Windows, OS X, Linux, Solaris, FreeBSD, Cisco iOS, IBM iSeries
  - Bazy danych: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL, MongoDB
  - Aplikacje webowe: serwery i serwisy web, podatności OWASP
  - Chmura: skanowanie konfiguracji aplikacji i instancji w chmurach takich jak Salesforce i AWS
  - Zgodność: uwzględnia wymogi urzędów państwowych oraz wymogi korporacyjne
  - Pomaga spełniać wymogi PCI DSS poprzez możliwość konfiguracji audytu i skanowanie aplikacji webowych
- Zagrożenia: botnety/szkodliwe procesy/audyt systemów antywirusowych
  - Znajdowanie wirusów, szkodliwego oprogramowania, luk w zabezpieczeniach, komunikacji urządzeń z zainfekowanymi systemami, znanych/nieznanych procesów, serwisów web powiązanych ze szkodliwą zawartością
  - Audyt zgodności z: FFIEC, FISMA, CyberScope, GLBA, HIPAA/HITECH, NERC, PCI, SCAP, SOX, GIODO (opracowane przez OpenBIZ)
  - Konfiguracja audytu: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA
- Audyt systemów automatyki przemysłowej: systemy SCADA, urządzenia wbudowane i aplikacje ICS
- Audyt zawartości wrażliwych: dane osobowe (np. numery kart płatniczych, PESEL itd.)

Wdrożenie i zarządzanie

- Elastyczność wdrożenia: oprogramowanie, sprzęt, urządzenie wirtualne mogą być uruchomione w siedzibie firmy lub w chmurze dostawcy usług.
- Opcje skanowania: możliwe obydwa rodzaje skanów: zdalne skanowanie bez uwierzytelnienia i z uwierzytelnieniem – lokalne skany dla głębszej i bardziej szczegółowej analizy zasobów, podłączonych do sieci, tymczasowo odłączonych lub dostępnych zdalnie.
- Konfiguracja/ Polityki skanowania: predefiniowane polityki i wzorce konfiguracji.
- Ocena ryzyk: ranking oceny podatności w oparciu o CVSS, pięć poziomów dotkliwości (Krytyczny, Wysoki, Średni, Niski, Informacyjny), dla zmiany perspektywy oceny ryzyka możliwe jest dostosowywanie poziomów ocen dotkliwości.
- Priorytetyzacja: korelacja z danymi z baz exploitów (Metasploit, CoreImpact, Canvas, ExploitHub) i filtrowanie wg prawdopodobieństwa wykorzystania podatności i jej dotkliwości.
- Rozszerzalność: integracja Nessus z już istniejącymi ścieżkami zarządzania podatnościami za pomocą wsparcia RESTful API.

Szkolenia i certyfikacja

Tenable oferuje szkolenia dla nowych użytkowników, którzy chcą posiąść wiedzę i umiejętności, pozwalające maksymalnie wykorzystać zalety produktu. Dla bardziej zaawansowanych użytkowników szkolenia dotyczące konkretnych tematów, np. audytów zgodności. Szkolenia dostępne są na zamówienie poprzez stronę internetową Tenable.

Nessus – poziom wyżej

Dla organizacji, które chcą zarządzać podatnościami zespołowo, dostępne są następujące rozwiązania Nessus:

Nessus Manager

Nessus Manager zapewnia współpracę i scentralizowane zarządzanie poprzez wykorzystanie wielu skanerów. Zaangażowanie w proces zarządzania podatnościami administratorów systemów i sieci, śledczych i grup reagowania na zdarzenia, ryzyka i zgodności oraz wsparcie użytkowników. Najpowszechniej stosowany w przemyśle skaner podatności i oceny konfiguracji zasobów oferuje oparte o role udostępnianie skanerów, polityk, harmonogramów i wyników nieograniczonej liczbie uprawnionych użytkowników.

Nessus Cloud

Udostępniana na serwerach Tenable wersja Nessus Manager pozwala na skanowanie, udostępnianie zasobów i opartą o role kontrolę dostępu dla wielu użytkowników ze zdalnego rozwiązania w chmurze. Nessus Cloud może być również wykorzystywany do spełniania wymogów standardów PCI dot. kwartalnego skanowania sieci, które powinno być wykonywane przez firmę zewnętrzną. Nessus Cloud jest rozwiązaniem certyfikowanym przez PCI jako Approved Scanning Vendor (ASV).

Korzyści Nessus

Klienci wybierają Nessus ze względu na:

- Wysoce precyzyjne skanowanie z rzadkim występowaniem błędnie pozytywnych wyników
- Możliwości i funkcjonalności wszechstronnego skanowania
- Skalowalność do setek tysięcy systemów
- Łatwe wdrożenie i utrzymanie
- Niskie koszty zarządzania i użytkowania

tenable® network security

Więcej szczegółów na stronach tenable.com oraz openbiz.pl.