Nessus™ NP Professional

A Nessus-t világszerte több mint egymillió felhasználó alkalmazza a sebezhetőség, a konfiguráció és a megfelelőség értékelésére.

Nessus Professional sérülékenység szkenner

A Nessus® Professional, az iparág legelterjedtebb sérülékenységvizsgáló megoldása, segít csökkenteni a szervezet támadási felületét és biztosítja a megfelelőséget. A Nessus gyors eszközfelfedezést, konfiguráció-ellenőrzést, célpontprofilozást, rosszindulatú programok és érzékeny adatok felderítését és még sok más funkciót kínál.

A Nessus több technológiát támogat, mint a versenytársai. Képes vizsgálni az operációs rendszereket, hálózati eszközöket, új generációs tűzfalakat, virtuális gép kezelőket, adatbázisokat, webkiszolgálókat, valamint kritikus infrastruktúrákat a sebezhetőségek, fenyegetések és megfelelőség szempontjából.

A világ legnagyobb, folyamatosan frissített sérülékenység- és konfiguráció-ellenőrzési könyvtárával, valamint a Tenable szakértő sérülékenység-kutató csapatának támogatásával a Nessus meghatározza a sérülékenységvizsgálat sebességének és pontosságának hatékony módszerét.

Nessus Funkciók

Jelentés és felügyelet

- Rugalmas riportálás: Testreszabhatja a riportokat sebezhetőség vagy hoszt szerint, készíthet összefoglalót vagy összehasonlíthatja a vizsgálati eredményeket a változások kiemelése érdekében.
  - Natív (XML), PDF (Java telepítése szükséges a Nessus szerverre), HTML és CSV formátumban.
- Célzott e-mail értesítések a vizsgálati eredményekről, javítási ajánlásokról és a vizsgálati konfiguráció javításairól

Teljes sérülékenység lefedettség

- Virtualizáció és felhő
- Rosszindulatú programok és botnetek
- Konfiguráció auditálás
- Webes alkalmazások

Legfontosabb előnyök

- **Csökkenti a támadási felületet:** Megelőzi a támadásokat a kezelendő sebezhetőségek azonosításával.
- **Átfogó:** Megfelel a megfelelőségi és szabályozási előírások legszélesebb körének.
- **Skálázható:** Kezdje a Nessus Professional egyfelhasználós licenccel, és térjen át a Nessus Manager vagy a Tenable.io szolgáltatásra, a sebezhetőségek kezelésére vonatkozó igényei növekedésével.
- **Alacsony teljes tulajdonlási költség (TCO):** Teljes körű sérülékenységvizsgálat egyszeri, alacsony költséggel
- **Folyamatos frissítés:** A Tenable kutatócsapata folyamatosan új sérülékenységekkel bővíti az adatbázist.

SC MAGAZINE

Szkennelési képességek

- Felderítés: pontos, nagy sebességű eszközfeltárás
- Szkennelés: sebezhetőségi vizsgálat (beleértve az IPv4/IPv6/hibrid hálózatokat)
  - Nem hitelesített sebezhetőség felderítése
  - Hitelesítő adatokkal ellátott szkennelés a rendszer hardening és a hiányzó javítások érdekében
  - Megfelel a PCI DSS belső sebezhetőségi vizsgálatra vonatkozó követelményeinek
- Lefedettség: Széles körű eszközlefedettség és profilalkotás
  - Hálózati eszközök: tűzfalak/routerek/kapcsolók (Juniper, Check Point, Cisco, Palo Alto Networks), nyomtatók, tárolóeszközök
  - Hálózati eszközök offline konfigurációs ellenőrzése

- Virtualizáció: VMware ESX, ESXi, vSphere, vCenter, Microsoft, Hyper-V, Citrix Xen Server
- Operációs rendszerek: Windows, OS X, Linux, Solaris, FreeBSD, Cisco iOS, IBM iSeries
- Adatbázisok: Oracle, SQL Server, MySQL, DB2, Informix/DRDA, PostgreSQL, MongoDB
- Webes alkalmazások: webkiszolgálók, webszolgáltatások, OWASP sebezhetőségek
- Felhő: A felhőalapú alkalmazások konfigurációjának ellenőrzése (Salesforce, Amazon Web Services, a Microsoft Azure és a Rackspace)
- Megfelelés: Segít megfelelni a kormányzati, szabályozási és vállalati követelményeknek
- Segít a PCI DSS követelményeinek érvényesítésében a biztonságos konfiguráció, a rendszer hardening, a rosszindulatú programok észlelése, a webes alkalmazások ellenőrzése és a hozzáférés-ellenőrzés tekintetében.

- Fenyegetések: Botnet/rosszindulatú, folyamatok/antivírus audit
  - Vírusok felderítése, rosszindulatú programok, backdoor, botnet-fertőzött rendszerekkel kommunikáló hosztok, ismert/ismeretlen folyamatok, rosszindulatú tartalmakra mutató webes szolgáltatások
  - Megfelelőség audit: FFIEC, FISMA, CyberScope, GLBA, HIPAA/ HITECH, NERC, SCAP, SOX
  - Konfiguráció audit: CERT, CIS, COBIT/ITIL, DISA STIGs, FDCC, ISO, NIST, NSA, PCI
- Ellenőrző rendszerek auditálása: SCADA rendszerek, beágyazott eszközök és ICS-alkalmazások
- Érzékeny tartalmak ellenőrzése: PII (pl. hitelkártyaszámok, SSN-ek)

Telepítés és Menedzsment

- Rugalmas telepítés: szoftver, hardver, virtuális eszköz helyben vagy a szolgáltató felhőjében telepítve.
- Szkennelési lehetőségek: Támogatja mind a hitelesítés nélküli távoli szkenneléseket, mind a hitelesített helyi szkenneléseket, amelyek lehetővé teszik a csatlakoztatott (online) és a nem csatlakoztatott vagy távoli (offline) eszközök részletes elemzését.
- Konfiguráció/irányelvek: Kész megoldások és konfigurációs sablonok alapértelmezett irányelvekkel.
- Kockázati pontszámok: A sebezhetőségek rangsorolása a CVSS alapján, öt, testreszabható szinttel (Kritikus, Magas, Közepes, Alacsony, Információ), a kockázat újraértékeléséhez.
- Összekapcsolás keretrendszerekkel (Metasploit, Core Impact, Canvas, ExploitHub) és szűrés a kihasználhatóság valamint kockázat alapján.
- Bővíthető: RESTful API támogatás a Nessus integrálásához a meglévő sérülékenység-kezelési munkafolyamataiba

Oktatás

A Tenable képzéseket kínál azok számára, akik most kezdik a Nessus használatát, és szeretnék elsajátítani azokat az ismereteket és készségeket, amelyek segítségével a terméket maximálisan kihasználhatják, de olyan speciális témákat is érint, mint például a megfelelőségi auditálás a haladó felhasználók számára. A kurzusok a Tenable weboldalán elérhetők, igény szerint.

A Nessus előnyei

Az ügyfelek azért választják a Nessust, mert:

- Nagyon pontos szkennelést nyújt, és kevés a hamis pozitív eredmény.
- Átfogó szkennelési képességekkel és funkciókkal rendelkezik.
- Rendszerérettől független használat.
- Könnyű a telepítése és a karbantartása
- Alacsony adminisztrációs és üzemeltetési költséggel jár.

Az Ön magyarországi partnere:
Nádor Rendszerház Kft. I 1152 Budapest, Telek u. 7-9. I info@nador.hu I +36 1 470-5000