

GFI LANguard

Hálózati biztonságelemző, sérülékenységvizsgáló és patch-menedzsment megoldás

Az adminisztrátorok és üzemeltetők a hálózat sérülékenységeinek felméréséhez, a biztonsági auditok elkészítéséhez vagy a javítócsomagok menedzsmentjéhez gyakran többféle szoftvert is kénytelenek használni. A GFI LanGuard Network Security Scanner (NSS) azonban mind a három funkciót egyesíti, így bevezetésével olyan komplex megoldáshoz juthat az üzemeltető, amellyel a sérülékenységvizsgáló, az auditriportok elkészítése és a javítócsomagok telepítése is megoldható egyetlen közös felületről.

A folyamatos és szinten tartott hálózati biztonság megvalósítása

A GFI LanGuard NSS a hálózat vagy az eszközök felderítéséhez 15000 sebezhetőségi pontot ellenőriz végig. Az ellenőrzés után nem csak riportot és jelentést készít, de lehetőség van az operációs rendszerek biztonsági hiányosságainak kiküszöbölésére, akár többnyelvű és inhomogén rendszerek esetében is. A GFI LanGuard NSS az operációs rendszer típusának (Microsoft Vista, XP, 2000, 2003, Linux, MacOS) és nyelvének megfelelő szervizcsomagokat telepíti fel, illetve nem csak módosításokat javasol a beállításokban, de el is végzi azokat, bezárva ezzel a biztonsági réseket.

Norman, Kaspersky, BitDefender, McAfee és AVG anti-vírus motorok

Az Nmap felhasználói évek óta a legjobb kereskedelmi forgalomban kapható sérülékenységvizsgáló alkalmazásnak választják. A GFI LanGuard NSS rendelkezik OVAL és SANS minősítéssel, az üzemeltetők és a biztonsági auditorok legkedveltebb alkalmazásaként a hálózati biztonság területének nélkülözhetetlen eszköze.

Hálózati és szoftver audit

Ha már legalább egyszer lefutott az ellenőrzés és telepítve lettek a szükséges javítócsomagok, a GFI LanGuard NSS már ismerni fogja a teljes hálózatot és a rendszerek állapotát, valamint:

- a csatlakoztatott USB eszközöket
- a telepített szoftvereket, mind az engedélyezettteket, mind pedig az illegálisan telepítetteket
- a megosztásokat és a nyitott portokat, valamint a jelszóhasználat tulajdonságait
- a Linux rendszerek biztonsági állapotát.

Automatikus szoftver eltávolítás

A szoftveraudit és a cégstandardként meghatározott szoftverlista alapján a GFI LANguard képes eltávolítani a standardtól eltérő szoftvereket. Ezzel a lehetőséggel csökkenthető a felhasználók által telepített illegális, vagy a standard rendszerekkel inkompatibilis

Sebezhetőség vizsgálat

Miközben IP-ről IP-re végigellenőrzi a hálózatot, 15000-nél is több sebezhetőségi pontot vizsgál végig. Előnyök:

- multi-platform vizsgálat (Windows, Linux, MacOS)
- VMWare, Virtual PC virtualizált környezet felismerése
- a begyűjtött adatok alapján megállapítja a hálózat egészére érvényes állapotot
- felhasználóbarát felület és grafikus indikátor a hálózat vagy az ellenőrzött számítógépek, csoporthoz sebezhetőségéről
- gyárilag szállított, mindenre kiterjedő sebezhetőségi adatbázis, amely megfelel az OVAL-nak és a SANS Top 20-nak
- ellenőrzi a legismertebb antivírus és antispyware szoftvereket, definíciós adatbázisukat és megfelelő működésüket
- bevezetése segít megfelelni a PCI DSS és más elvárások (pl. SOX, stb.) követelményeinek.

Patch-menedzsment

A hálózat és a rendszerek átvizsgálása után az észlelt sebezhetőségeket és biztonsági hiányosságokat ki kell javítani. A GFI LanGuard NSS segítségével:

- telepíthetőek a különféle operációs rendszerek javítócsomagjai, a Microsoft rendszerek esetében 38 nyelv támogatott, köztük természetesen a magyar is,
- saját szervizcsomag repository alakítható ki, és a hiányzó javítócsomagok automatikus letöltésével



jelentős idő takarítható meg,

- Microsoft javítócsomagok és alkalmazások mellett tetszőleges szoftvercsomagok is kitelephetőek a kliensgépekre, például vírusirtók, frissítések, stb.

Részletes és összehasonlítható riportkészítés

A GFI LanGuard NSS erőteljes és részletes riportolási lehetőséget nyújt az üzemeltetők és a menedzsment számára.

Riportolási lehetőségek:

- részletekbe menő, a hálózat pillanatnyi állapotát tükröző riport
- részletes hardverlista (alaplapp, processzor, memória, tároló eszközök, videokártya stb.)
- az aktuális és a korábbi vizsgálatok összehasonlító sábjól származó elemzés, amely pontosan feltünteti és követhetővé teszi a rendszerekben bekövetkező változásokat (új szoftverek, új nyitott portok, stb.)
- tetszőleges, grafikus riportok készítése (pl. a 20 legsebezhetőbb rendszer, sérülékenységi információk, trendanalízis, technikai információk, stb.) a riportolási rendszer tartalmazza az alapértelmezett és a tetszőlegesen összeállítható riportok lehetőségét, a riportkészítés ütemezését és e-mailen keresztüli elküldését, valamint az adat-export lehetőségét a legismertebb dokumentum-formátumokba.

Ütemezett ellenőrzés és kiértékelés

A GFI LanGuard NSS-ben beállítható, hogy az ellenőrzéseket és kiértékeléseket ütemezve és automatikusan végezze el. Képes az utolsó ellenőrzés eredményeit összevetni a korábbiakkal, és különbség esetén figyelmeztetést küld az üzemeltetőnek, aki így azonnal tudomást szerez a rendszer állapotának változásairól – például új megosztások és felhasználók létrehozásáról, új szolgáltatások telepítéséről, új, kinyitott portokról.

További funkciók

- Az automatikusan futó programok ellenőrzése (trójai programok azonosítása)
- Csendes, beavatkozás nélküli telepítés.
- A wireless hálózaton csatlakozó eszközök megkülönböztetése
- Az ellenőrzésekhez használt autentikáció előzetes beállítása
- A jelszóházi rendek ellenőrzése az egész hálózatban, minden rendszeren
- SSH shell script, Python és VBscript alapú egyéni ellenőrzés készítése
- Többszálú ellenőrzés (multi-threading) Hibával lefutó ellenőrzéseknél fejlett, automatikus hibakeresés.

Rendszerkövetelmények

- Windows 2000/2003 SBS, Windows XP
- Microsoft Exchange Server 2000/2003/2007/5.5, Lotus Notes, vagy más SMTP szerver
- Small Business Server alapokon, Exchange Server 2000 esetén SP2, Exchange Server 2003 esetén SP1 telepítés
- .NET Framework 2.0
- Microsoft Messaging Queueing Service
- IIS SMTP service

Az Ön viszonteladója:



Díjak

