GFI LANguard

Network Security Scanner

Netwerk beveiliging door Security scanning en patch management

De GFI LANguard Network Security Scanner (N.S.S.) controleert uw netwerk op alle potentiële methoden die een hacker zou kunnen gebruiken voor een aanval. GFI LANguard N.S.S. identificeert mogelijke beveiligingslekken door het besturingssysteem en lopende applicaties op uw netwerk te analyseren. Met andere woorden, GFI LANguard N.S.S. speelt advocaat van de duivel en maakt u attent op zwakheden voordat een hacker ze kan vinden. Zo kunt u deze problemen oplossen voordat een hacker ze kan uitbuiten.

GFI LANguard N.S.S. scant uw gehele netwerk, IP voor IP, en verschaft informatie zoals het service pack niveau van de machine, ontbrekende security patches, wireless access points, USB-apparatuur, open shares, open poorten, actieve diensten/applicaties, belangrijke registry entries, zwakke wachtwoorden, gebruikers en groepen, en meer. Scanresultaten kunnen gemakkelijk worden geanalyseerd door middel van filters en rapporten zodat u op proactieve wijze uw netwerk kunt beveiligen - bijvoorbeeld door overbodige poorten af te sluiten, shares te sluiten, service packs en hotfixes te installeren, etc.

GFI LANguard N.S.S. biedt tevens patch management. Als GFI LANguard N.S.S. eenmaal uw netwerk heeft gescand en heeft vastgesteld welke patches en service packs ontbreken - zowel in het besturingssysteem als in de applicaties - kan het deze service packs en patches op het gehele netwerk installeren. De GFI LANguard N.S.S. kan ook aangepaste software plaatsen op het gehele netwerk.

Identificeert beveiligingsproblemen en vertelt u wat u eraan kunt doen

Zodra GFI LANguard N.S.S. klaar is met het scannen van een computer categoriseert hij de beveiligingsproblemen en reikt hij oplossingen aan. Waar mogelijk wordt verdere informatie of een link betreffende het probleem bijgevoegd, bijvoorbeeld een BugTraq ID of het nummer van een artikel uit de Microsoft Knowledge Base.

Voordelen

Waarom GFI LANguard N.S.S.?

- Controleer uw netwerk op beveiligings problemen (Windows en Linux)
- Detecteer onnodige shares, open poorten en ongebruikte gebruikers accounts op werkstations
- Installeer ontbrekende security patches en service packs in OS en Office
- Detectie van draadloze nodes en links en scanning van USB-apparatuur
- #1 Windows security scanner (volgens NMAP-gebruikers; reeds meer dan 200.000 exemplaren verkocht).

Snel scannen van TCP/UDP-poorten en service fingerprint identificatie

De GFI LANguard N.S.S. beschikt over een snelle scanner voor TCP/IP- and UDP-poorten waarmee u uw netwerk kunt controleren op onnodige open poorten. Tijdens het identificeren van belangrijke open poorten (zoals www, FTP, Telnet, SMTP) aan de hand van bannercontrole controleert GFI LANguard N.S.S. ook de dienst achter de gedetecteerde open poorten om te zien of er geen poorten gekaapt zijn.

Netwerkwijd beheer van patches en service packs

U kunt ontbrekende service packs en patches in één keer op het gehele netwerk plaatsen zonder dat gebruikers er iets voor hoeven te doen. Met GFI LANguard N.S.S. kunt u zien of Microsoft SUS naar behoren werkt en bovendien taken uitvoeren waartoe SUS niet in staat is, zoals het plaatsen van Microsoft Office patches en aangepaste software patches, patchrapportage en onmiddellijke plaatsing van high alert patches.

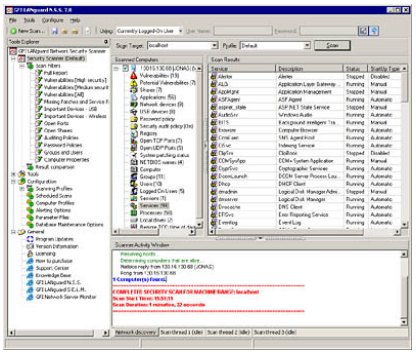
Patchondersteuning voor meertalige besturingssystemen

GFI LANguard N.S.S. ondersteunt de detectie van ontbrekende Microsoft security updates en de plaatsing daarvan op zowel Engelstalige als niet-Engelstalige Windows besturingssystemen.

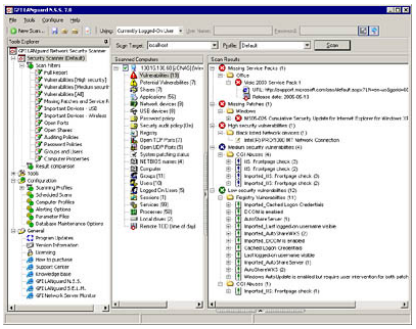
Downloadt automatisch informatie betreffende beveiligingslekken en security patches

Dankzij het auto-updatesysteem beschikt GFI LANguard N.S.S. altijd over de meest recente informatie over nieuwe security updates van Microsoft en nieuwe kwetsbaarheidscontroles van GFI.

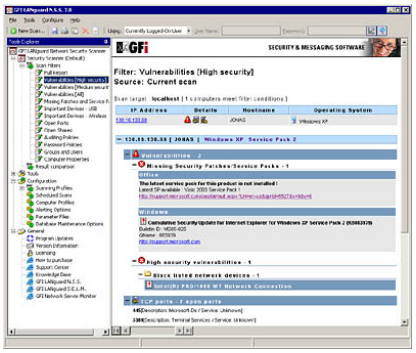
GFI LANguard Network Security Scanner



GFI LANguard Network Security Scanner hoofdscherm

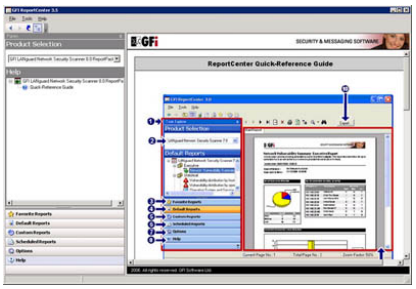


Wijst aangetroffen kwetsbaarheden aan



Uitgebreide HTML veiligheidsrapporten

GFI LANguard Network Security Scanner ReportPack



Quick Reference Guide

Maakt u automatisch attent op nieuwe beveiligingslekken

GFI LANguard N.S.S. kan regelmatig scans uitvoeren (bijvoorbeeld elke dag of elke week) en kan automatisch de resultaten vergelijken met eerdere scans. Als er nieuwe beveiligingslekken op uw netwerk zijn opgedoken of er veranderingen hebben plaatsgevonden, ontvangt u een e-mail. Op deze manier kunt u onder andere nieuwe shares, geïnstalleerde diensten, geïnstalleerde applicaties, nieuwe gebruikers en nieuwe open poorten snel op het spoor komen.

Met de GFI LANguard N.S.S. kunt u er zeker van zijn dat antivirus- en antispamapplicaties van andere fabrikanten optimale bescherming bieden

U kunt controleren of beveiligingsapplicaties zoals antivirus- en antispywaresoftware over de nieuwste definitiebestanden beschikken en naar behoren functioneren. U kunt er bijvoorbeeld voor zorgen dat alle belangrijke functies (zoals realtime scanning) van de ondersteunde beveiligingsapplicaties aan staan.

Breid GFI LANguard N.S.S. uit met efficiënte rapportage

Rapporten die zijn ontworpen met het oog op de eisen van managers en technici bieden een grafisch overzicht van de gezondheidstoestand van uw netwerk. Het GFI LANguard N.S.S. ReportPack biedt op een overzichtelijke manier de informatie die u nodig heeft om te weten hoe veilig uw netwerk is. Het Report Pack is zo eenvoudig in gebruik dat u het kunt installeren en er vervolgens niet meer naar om hoeft te kijken!

Uitgebreide database van zwakke plekken

Bij de GFI LANguard N.S.S. hoort een volledige kwetsbaarheidsdatabase met ondere andere belangrijke SANS-problemen en zwakke plekken in Linux en CGI. De kwetsbaarheidsdatabase wordt regelmatig bijgewerkt met problemen die zijn gerapporteerd aan BugTraq, SANS, CVE en andere bronnen. Nieuwe informatie kan automatisch van de GFI website worden gedownload.

Creëert eenvoudig verschillende soorten scans en kwetsbaarheidstests

Beheerders kunnen scans configureren voor verschillende soorten informatie, zoals open shares op werkstations, audit- en wachtwoordbeleid en machines waarop een bepaalde patch of een bepaald service pack ontbreekt. U kunt scannen op verschillende soorten kwetsbaarheden en de scan kan worden uitgevoerd met gebruik van verschillende identiteiten.

De scanresultaten kunnen gemakkelijk worden gefilterd

U kunt de scanresultaten gemakkelijk analyseren door op één van de default filter nodes te klikken. Zo kunt u bijvoorbeeld zien welke machines met grote beveiligingsproblemen kampen of een bepaald service pack nodig hebben. U kunt gemakkelijk uw eigen filters maken en het is ook eenvoudig om bestaande filters aan te passen. U kunt tevens scanresultaten naar XML exporteren.

Vindt ongebruikte lokale gebruikers en groepen

De LANguard N.S.S. maakt een lijst van alle lokale gebruikers en groepen en identificeert gebruikersaccounts die niet meer in gebruik zijn. Vervolgens kunt u deze accounts verwijderen of uitschakelen zodat ze geen veiligheidsrisico meer kunnen vormen voor uw netwerk.

Vindt alle shares op uw netwerk

De GFI LANguard N.S.S. laat u alle shares op uw netwerk zien, inclusief beheer- en printershares (C$, D$, ADMIN$) en geeft aan wie toegang heeft tot welke share. Met deze optie kunt u:

- Controleren of de toegang tot shares op correcte wijze is ingesteld
- Controleren of een gebruiker zijn of haar gehele schijf met andere gebruikers deelt
- Anonieme toegang tot shares voorkomen
- Ervoor zorgen dat startup folders of gelijksoortige systeembestanden niet kunnen worden gedeeld aangezien anders gebruikers met minder rechten code op target machines zouden kunnen uitvoeren.

Detecteert applicaties die op een zwarte lijst zijn gezet

Met de GFI LANguard N.S.S. kunt u een lijst maken van alle applicaties die momenteel op de computers geïnstalleerd zijn. U kunt tevens ongeautoriseerde of gevaarlijke software identificeren door de lijst met te blokkeren applicaties die u als zeer kwetsbaar beschouwt, te specificeren.

Detecteert draadloze nodes en links

De GFI LANguard N.S.S. kan computers of andere apparaten die door middel van een draadloze link met uw netwerk zijn verbonden, detecteren. Draadloze links vormen een groot veilligheidsrisico als ze niet naar behoren zijn beveiligd.

Biedt de mogelijkheid om authentificatiedetails vooraf te bepalen

De GFI LANguard N.S.S. biedt u de mogelijkheid om voor elke computer op uw netwerk aparte authentificatiedetails op te slaan zodat u niet voor iedere scan opnieuw authentificatiedetails hoeft te specificeren. U kunt in een enkele sessie alle computers in uw netwerk auditen, zelfs als ze verschillende authentificatiedetails of -methodes vereisen.

Gebruik van software en patches van andere fabrikanten over het gehele netwerk

Naast patches en service packs kunt u met de GFI LANguard N.S.S. ook gemakkelijk software of patches van andere fabrikanten plaatsen op het gehele netwerk. Met deze optie kunt u onder andere client software plaatsen, aangepaste software of software van andere fabrikanten dan Microsoft updaten en virusupdates installeren. Dankzij de optie voor het plaatsen van aangepaste software wordt Microsoft SMS, dat te complex en te duur is voor kleine en middelgrote netwerken, overbodig.

Scannen op gevaarlijke USB-apparatuur

USB-apparatuur vormt een potentieel veiligheidsprobleem aangezien bijna ieder apparaat aangesloten kan worden. Dit betekent een potentieel veiligheidsrisico en u heeft als beheerder maar weinig controle. De GFI LANguard N.S.S. scant alle apparaten die met de USB-hub verbonden zijn, filtert geautoriseerde USB-apparaten (zoals de muis) en maakt u alleen attent op gevaarlijke of onbekende USB-apparaten.

Scant en vindt OS data uit Linux-systemen

Het is mogelijk om vanop afstand OS data uit Linuxgebaseerde systemen te halen en de scanresultaten op dezelfde manier te bekijken als die voor Windows. Dit betekent dat Linux- en Windowsgebaseerde computers in één keer gescand kunnen worden! De GFI LANguard N.S.S. bevat diverse security checks voor Linux, waaronder rootkitdetectie.

Systeemvereisten

- Besturingssysteem: Windows 2000 (SP4) / XP (SP2) / 2003.
- Internet Explorer 5.1 of hoger.
- Client voor Microsoft Networks component - dit is inbegrepen in Windows 95 en hoger.
- Secure Shell (SSH) - dit is inbegrepen in elk Linux OS distributiepakket.

Onderscheidingen

U kunt de testversie downloaden op http://www.gfi.nl/nl/lannetscan/

GFI Software
Magna House, 18 – 32 London Road
Staines, Middlesex
TW18 4BP
UK
Tel +44 (0) 870 770 5370
Fax +44 (0) 870 770 5377
sales@gfi.co.uk

GFI Software
15300 Weston Parkway
Suite 104
Cary, NC 27513
USA
Tel +1 (888) 243-4329
Fax +1 (919) 379-3402
sales@gfiusa.com

GFI Asia Pacific Pty Ltd
83 King William Road
Unley 5061
South Australia
Tel +61 8 8273 3000
Fax +61 8 8273 3099
sales@gfiap.com

GFI Software
GFI House
San Andrea Street
San Gwann SGN 1612
Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

Microsoft GOLD CERTIFIED Partner

GFI www.gfi.com