GFI LANguard

Network Security Scanner

Schwachstellen-Scans, Patch-Management und Sicherheits-Audits für Netzwerke

GFI LANguard Network Security Scanner (N.S.S.) unterstützt Administratoren mit einer zentralen Konsole beim Aufspüren, Bewerten und Beheben sämtlicher Sicherheitslücken ihres Netzwerks. Als Systemverantwortlicher kennen Sie das Problem: Sicherheitsrelevante Aufgaben wie Schwachstellen-Scans, Patch-Management und Netzwerk-Audits müssen oft getrennt voneinander mit unterschiedlichen Lösungen bewältigt werden. Der mehrfach ausgezeichnete GFI LANguard N.S.S. hingegen vereint diese drei tragenden Elemente des Schwachstellen-Managements in einem Produkt. Dank der leistungsfähigen Reporting-Funktionalität kann zudem schneller und effektiver auf Gefahren reagiert werden.

GFI LANguard N.S.S. greift beim Scannen des Netzwerks auf über 15.000 Schwachstellen-Checks und -bewertungen aus einer leistungsfähigen Datenbank zurück, die auf OVAL (Open Vulnerabilities Assessment Language) und den SANS Top 20 beruht. Benutzerfreundliche Tools unterstützen Sie bei der Kontrolle unterschiedlicher Plattformen in Umgebungen jeder Art. Analysieren Sie den Sicherheitsstatus Ihres Netzwerks, und profitieren Sie von der effektiven Installation und Verwaltung von Patches in verschiedenen Sprachen und für mehrere Betriebssysteme. Dank der einheitlichen Konfigurierung über die gesamte Netzwerkumgebung hinweg wird Ihr System zuverlässig vor Schwachstellen abgesichert.

Die Auszeichnungen sprechen für sich: Bereits zwei Jahre in Folge ist GFI LANguard N.S.S. von Nmap-Anwendern zum besten kommerziellen Netzwerksicherheits-Scanner gewählt worden. Unter den von TechTarget prämierten "Produkten des Jahres 2006" schnitt die Lösung zudem als beste Anwendung in der Kategorie "Patch-Management" ab, ebenso wie bei den "Best of TechEd Awards 2007" in der Kategorie "Sicherheit". GFI LANguard N.S.S. ist die integrierte Rundum-Lösung für Schwachstellen-Management, mit denen Sie Ihre IT-Umgebung kostengünstig vor Hacker-Angriffen und Sicherheitsverletzungen absichern können.

Vorteile

Vorteile von GFI LANguard N.S.S.

- Kontrolliert das gesamte Netzwerk mit über 15.000 Schwachstellen-Checks und -bewertungen
- Sorgt für geringere Betriebskosten durch Zentralisierung von Schwachstellen-Scans, Patch-Management und Netzwerk-Audits
- Bietet anpassbare Berichte zu netzwerkweiten Scans von Anwendungen und Ressourcen
- Unterstützt IT-Administratoren bei einer schnelleren und effektiveren Sicherung ihres Netzwerks
- Verhindert Systemausfälle und Geschäftseinbußen durch ausgenutzte Schwachstellen
- Beliebtester kommerzieller Sicherheits-Scanner für Microsoft Windows (bereits zweimal in Folge Sieger bei Nmap-Anwenderumfrage) und "Best of TechEd"-Gewinner 2007 in der Kategorie "Sicherheit"

Integriertes Schwachstellen-Management

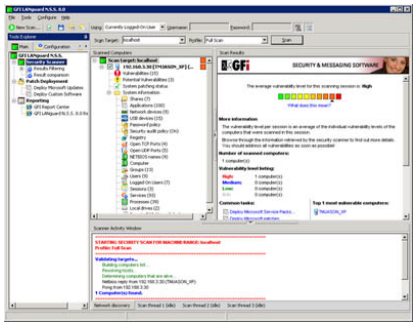
Mit GFI LANguard Network Security Scanner (N.S.S.) lassen sich die drei tragenden Elemente des Schwachstellen-Managements – Schwachstellen-Scans, Patch-Management und Netzwerk-Audits – über eine einzelne integrierte Konsole verwalten. Durch Scans des gesamten Netzwerks werden sämtliche potenziellen Sicherheitsgefahren aufgespürt. Umfassende Reporting-Funktionen zur Berichterstellung bieten darüber hinaus wertvolle Hilfe bei Bewertung und Behebung der ermittelten Schwachstellen.

- Schwachstellen-Scans
- Patch-Management
- Netzwerk- und Software-Audits

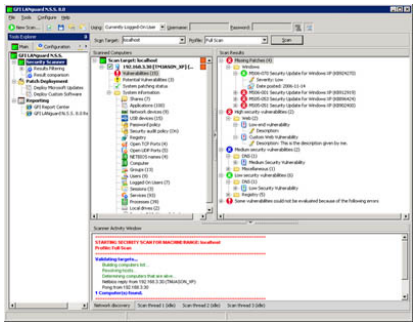
Schwachstellen-Scans

Im Rahmen der Sicherheitsüberprüfungen werden mehr als 15.000 Schwachstellen kontrolliert und bewertet sowie alle IP-Adressen des Netzwerks untersucht. Führen Sie Scans für mehrere Betriebssystem-Plattformen (Windows, Macintosh, Linux) in jeder IT-Umgebung durch, und analysieren Sie den Sicherheitsstatus Ihres Netzwerks anhand von zentral konsolidierten Daten. So lassen sich Lücken aufspüren und schließen, bevor Hacker dadurch eindringen können.

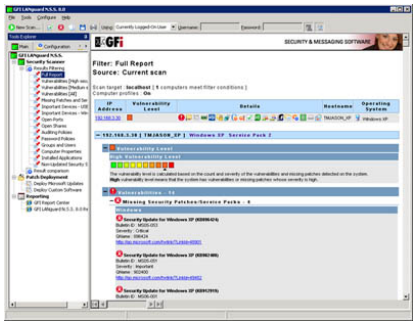
GFI LANguard Network Security Scanner



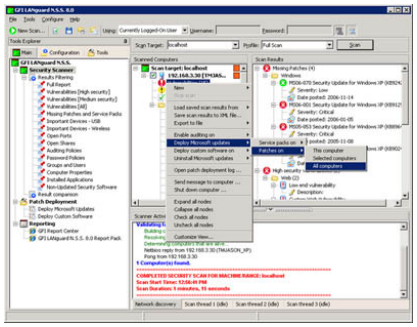
Hauptfenster



Anzeige identifizierter Sicherheitslücken

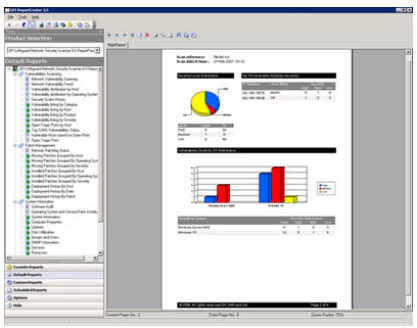


Umfangreiche HTML-Sicherheitsberichte



Einfache, netzwerkweite Installation von Patches

GFI LANguard Network Security Scanner ReportPack



Übersicht zu Netzwerk-Sicherheitslücken (Executive Report)

Unterstützung bei der Einleitung von Gegenmaßnahmen

GFI LANguard N.S.S. scannt alle Netzwerkrechner, schlüsselt identifizierte Sicherheitslücken in verschiedene Gefahrenkategorien auf und bietet Hinweise sowie Tools zur Problembehebung. Eine leicht verständliche grafische Anzeige des Gefährdungsgrads durch Schwachstellen erlaubt die rasche Bewertung des Sicherheitsstatus einzelner Computer oder des gesamten Netzwerks. Gegebenenfalls werden Links oder zusätzliche Informationen bereitgestellt, die beim Schließen einer speziellen Lücke helfen können – z. B. eine BugTraq-ID oder eine Artikel-ID der Microsoft Knowledge Base.

Umfangreiche Datenbank zu Sicherheitsproblemen

Im Lieferumfang von GFI LANguard N.S.S. ist eine vollständige Datenbank mit Schwachstellenkontrollen und -bewertungen enthalten, darunter über 2.000 branchenweit anerkannte OVAL-Checks (Open Vulnerabilities Assessment Language) und Scans zu SANS Top 20-Sicherheitslücken. Diese Datenbank wird regelmäßig mit neuen Informationen von BugTraq, der SANS Corporation, OVAL, CVE und anderen Quellen zur Informationssicherheit aktualisiert. Dank einer automatischen Aktualisierungsfunktion stehen darüber hinaus immer alle aktuellen Informationen zu neu veröffentlichten Sicherheits-Updates von Microsoft sowie zu neuen Schwachstellen-Checks von GFI und anderen Sicherheitsquellen (z. B. OVAL-Datenbank) zur Verfügung.

Funktionskontrolle anderer Sicherheitsanwendungen wie Anti-Virus- und Anti-Spyware-Lösungen

Stellen Sie mit GFI LANguard N.S.S. fest, ob unterstützte Sicherheitsanwendungen wie Anti-Virus- und Anti-Spyware-Programme mit aktuellen Signaturdateien arbeiten und ihre Scans korrekt verrichten. So können beispielsweise die Konfigurationseinstellungen der Security-Produkte kontrolliert werden um zu überprüfen, ob wichtige Funktionen wie Echtzeit-Scans aktiviert sind.

Problemlose Anpassung von Scans und Schwachstellen-Checks

Scans lassen sich mühelos für die Suche nach unterschiedlichen sicherheitsrelevanten Informationen anpassen. Hierzu zählen Freigaben auf Arbeitsplatzrechnern, Richtlinien für Sicherheitsüberwachungen und Passwörter oder auch Computer, auf denen bestimmte Patches oder Service Packs fehlen. Ebenso möglich ist die Suche nach folgenden potenziellen Schwachstellen:

- **Offene Ports:** GFI LANguard N.S.S. sucht nach nicht benötigten offenen Ports und stellt sicher, dass kein Port per Port-Hijacking von Hackern übernommen wurde.
- **Ungenutzte Konten lokaler Benutzer und Gruppen:** Nicht länger verwendete Benutzerkonten sollten aus Sicherheitsgründen gelöscht oder deaktiviert werden.
- **Unerwünschte Anwendungen:** Setzen Sie unautorisierte oder gefährliche Programme auf eine Blacklist. Bei Identifizierung einer unerwünschten Anwendung erfolgt eine entsprechende Warnung.
- **Gefährliche USB-Geräte und Funkverbindungen/-knoten:** Lassen Sie alle per USB oder Funkverbindung angekoppelten Geräte aufspüren und sich bei verdächtigen Aktivitäten benachrichtigen.
- u. v. m.

Definition eigener Schwachstellen-Checks

GFI LANguard N.S.S. erlaubt es Ihnen, mit Hilfe eines einfachen Assistenten zur Erstellung und Konfigurierung von Sicherheits-Checks eigene Schwachstellen zu definieren. Umfangreichere Kontrollen lassen sich zudem per VBScript-kompatible Skript-Engine programmieren. Ein Skript-Editor und -Debugger hilft zusätzlich bei der Skriptentwicklung.

Einfache Analyse und Filterung von Scan-Ergebnissen
Scan-Ergebnisse lassen sich mit nur einem Mausklick auf einen der vorgegebenen Filter-Knoten rasch analysieren. So erfahren Sie z. B., auf welchen Rechnern schwerwiegende Sicherheitslücken geschlossen werden müssen und wo einzelne Service Packs fehlen. Standardmäßige Filter können problemlos an eigene Bedürfnisse angepasst werden – oder erstellen Sie einfach neue Filter nach eigenen Vorgaben. Der Export von Scan-Ergebnissen in XML ist ebenfalls möglich.

Patch-Verwaltung

Eine umfangreiche Auswahl an Tools hilft Ihnen bei der effektiven Installation und Verwaltung von Patches auf allen Netzwerkrechnern. Fehlende Patches können per automatischen Download für unterschiedliche Betriebssysteme und in 38 Sprachen installiert werden. Zudem lassen sich Änderungen per Rollback-Funktion leicht rückgängig machen. Die Installation eigener Sicherheitssoftware trägt zusätzlich dazu bei, sich über die gesamte Netzwerkumgebung hinweg zuverlässig vor allen Arten von Schwachstellen absichern zu können.

Automatische netzwerkweite Patch- und Service Pack-Installation und -Verwaltung
Neben der netzwerkweiten Verteilung von Patches unterstützt GFI LANguard N.S.S. auch die Bereitstellung fehlender Service Packs. Darüber hinaus lassen sich die Microsoft WSUS (Windows Server Update Services) überwachen. Zusätzlich können von den WSUS nicht unterstützte Aufgaben, wie die Bereitstellung von Patches für Microsoft Office und Drittanbieter-Software, zuverlässig durchgeführt werden. Funktionen wie der automatische Patch-Download und -Rollback erleichtern die Verwaltung von Sicherheits-Updates. Weitere Vorteile bestehen durch die Unterstützung von Unicode-Standards; Patches können für alle 38 von Microsoft unterstützten Sprachen verwaltet werden.

Netzwerkweite Installation von eigenen und Drittanbieter-Lösungen/-Patches
Lassen Sie GFI LANguard N.S.S. im Handumdrehen eigene oder Drittanbieter-Software und -Patches im gesamten Netzwerk verteilen. Es können unter anderem Client-Software installiert, eigene oder Microsoft-fremde Programme aktualisiert und Anti-Virus-Updates bereitgestellt werden. Der zu komplexe und für kleine bis mittelgroße Netzwerke zu teure Microsoft SMS ist somit nicht länger erforderlich.

Netzwerk- und Software-Audits

Mit der Audit-Funktion von GFI LANguard N.S.S. werden alle sicherheitsrelevanten Netzwerkinformationen erfasst – ob zu angeschlossenen USB-Geräten, installierter Software, Freigaben und offenen Ports oder unsicheren Passwörtern. Detaillierte Berichte geben darüber hinaus wichtigen Aufschluss über den aktuellen Sicherheitsstatus. Sämtliche Scan-Ergebnisse lassen sich anhand von Filtern und Berichten mühelos analysieren. Die Ergebnisse helfen Ihnen, Ihr Netzwerk proaktiv abzusichern, indem Sie beispielsweise nicht benötigte Ports schließen, Benutzer- oder Gruppenkonten löschen oder WLAN-Access-Points deaktivieren.

Automatische Warnmeldungen bei neu entdeckten Sicherheitslücken
GFI LANguard N.S.S. kann regelmäßige Scans durchführen (z. B. täglich oder wöchentlich) und Ergebnisse automatisch mit vorherigen Scan-Resultaten vergleichen. Über neue Schwachstellen im Netzwerk oder sicherheitsrelevante Konfigurationsänderungen werden Sie per E-Mail informiert. So können Sie rasch analysieren, ob beispielsweise neue Freigaben, neu installierte Dienste und Anwendungen, hinzugefügte Anwenderkonten oder zuvor noch nicht geöffnete Ports eine Bedrohung darstellen.

Systemanforderungen

- Microsoft Windows 2000 (SP4)/XP (SP2)/2003/Vista
- Internet Explorer 5.1 oder höher
- Client für Microsoft-Netzwerke – standardmäßig im Lieferumfang von Windows 95 und höher enthalten
- Secure Shell (SSH) – standardmäßig im Lieferumfang jeder Linux-Distribution enthalten

Auszeichnungen

Ihre Testversion steht unter http://www.gfisoftware.de/de/lannetscan/ zum Download bereit!

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