



GFI LANguard

Network Security Scanner

Skanowanie zagrożeń sieci, zarządzanie poprawkami (łatami) i audyt

GFI LANguard Network Security Scanner (N.S.S.) jest wielokrotnie nagradzonym rozwiązaniem, które pozwala skanować, wykrywać, oceniać i naprawiać wszelkie zagrożenia na jakie wystawiona jest sieć. Jako administrator musisz radzić sobie oddzielnie z problemami bezpieczeństwa, zarządzania poprawkami i audytem sieci, używając czasem różnych narzędzi. GFI LANguard N.S.S. obsługuje te 3 filary bezpieczeństwa sieci jednocześnie. Używając jednej konsoli z rozbudowanymi funkcjami raportowania, dzięki GFI LANguard N.S.S. możesz reagować na zagrożenia szybciej i bardziej efektywnie.

GFI LANguard N.S.S. wykorzystuje supernowoczesne bazy danych zagrożeń oparte na bazach zagrożeń OVAL i SANS, wykonując ponad 15.000 ocen bezpieczeństwa podczas skanowania sieci. GFI LANguard N.S.S. dostarcza Ci informacji i narzędzi do wielopoziomowego skanowania i analizowania bezpieczeństwa i efektywnego instalowania i zarządzania poprawkami we wszystkich komputerach działających w różnych systemach operacyjnych i językach. Dzięki temu, ciągle konfigurowane środowisko jest zabezpieczone przed niebezpieczeństwami płynącymi z sieci.

Wybrany 2 lata z rzędu najlepszym komercyjnym skanerem przez użytkowników Nmap, zwycięzca w kategorii Zarządzania poprawkami na TechTarget's 2006 (Produkt Roku) i w kategorii bezpieczeństwa na Best of TechEd Awards 2007, GFI LANguard N.S.S. jest najpełniejszym rozwiązaniem w dziedzinie zarządzania zagrożeniami sieciowymi zintegrowanym w jednym produkcie. GFI LANguard N.S.S. jest podstawowym, ekonomicznym rozwiązaniem dla biznesu, zapewniającym bezpieczeństwo systemu i sieci przed atakami hakerów i naruszaniem zasad bezpieczeństwa.

Korzyści

Dlaczego stosować GFI LANguard N.S.S.?

Ponad 15.000 ocen bezpieczeństwa Twojej sieci.

Redukcja kosztów przez centralne skanowanie zagrożeń, zarządzanie uaktualnieniami i audyt sieci.

Dostarcza spersonalizowane raporty skanów całej sieci, włącznie z aplikacjami i wszystkimi zasobami.

Pomaga administratorom zabezpieczać sieć jeszcze efektywniej i szybciej.

Zapobiega przestojom i stratom spowodowanym zagrożeniami sieciowymi.

Nr 1 w kategorii komercyjnych skanerów (wybrany przez użytkowników Nmap 2 lata z rzędu) i Best of TechEd 2007 (w kategorii bezpieczeństwo).

Zintegrowane rozwiązanie w zarządzaniu bezpieczeństwem

GFI LANguard Network Security Scanner (N.S.S.) jest wielokrotnie nagradzonym rozwiązaniem obejmującym 3 filary zabezpieczania sieci: skanowanie zagrożeń, zarządzanie uaktualnieniami i audytem sieci zintegrowanym w jednej konsoli. Przez skanowanie całej sieci, definiuje wszystkie potencjalne elementy bezpieczeństwa i dzięki wszechstronnym funkcjom raportowania zapewnia niezbędne narzędzia do wykrywania, oceny i usuwania zagrożeń:

- Skanowanie podatności na zagrożenia
- Zarządzanie uaktualnieniami
- Audyt sieci i oprogramowania

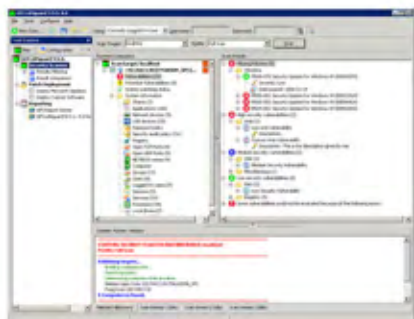
Skanowanie zagrożenia sieci

Podczas audytowania, przeprowadzone jest ponad 15.000 ocen bezpieczeństwa w sieci według adresów IP. GFI LANguard N.S.S. umożliwi wielosystemowe skanowanie (Windows, Mac, Linux) różnych środowisk w celu zanalizowania poziomu bezpieczeństwa z jednego źródła. Zapewnia to zidentyfikowanie i naprawienie błędów zanim zdążą zrobić to hakerzy.

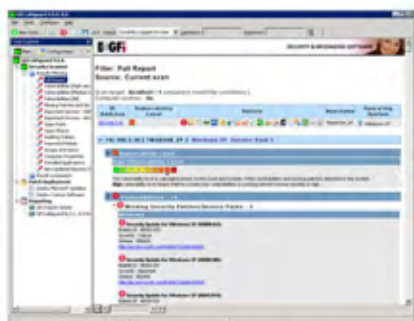
GFI LANguard Network Security Scanner



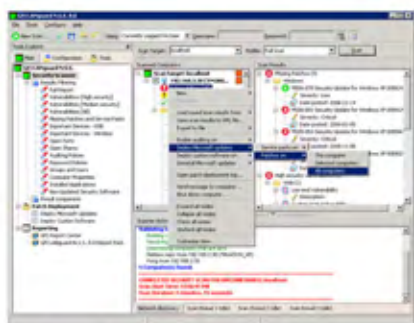
GFI LANguard Network Security Scanner main screen



Indicates vulnerabilities found

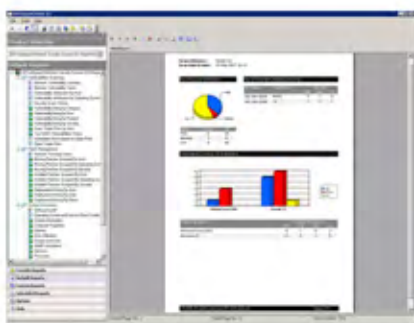


Extensive HTML security reports



Easily deploy patches network-wide

GFI LANguard Network Security Scanner ReportPack



Executive report showing network vulnerability summary

■ Identyfikowanie zagrożeń i podejmowanie działań naprawczych

GFI LANguard N.S.S. skanuje komputery, identyfikuje i kategoryzuje zagrożenia oraz podaje rekomendowane sposoby zniwelowania ich za pomocą dostępnych metod. GFI LANguard N.S.S. wykorzystuje także graficzne wskaźniki poziomu zagrożenia, które dostarczają intuicyjnej, wyważonej oceny zagrożeń dla pojedynczego komputera lub grupy maszyn. Gdziekolwiek jest to możliwe, dostarczany jest link lub informacje dotyczące danego problemu jako BugTraq ID lub ID artykułu w Microsoft Knowledge Base.

■ Rozległa i pojemna baza zagrożeń

GFI LANguard N.S.S. jest dostarczany z kompletną bazą oceny zagrożeń zawierającą takie standardy jak OVAL (ponad 2.000 sprawdzeń) i SANS Top 20. Baza danych jest regularnie uaktualniana informacjami z BugTraq, SANS Corporation, OVAL, CVE i innych. Przez system automatycznych aktualizacji, GFI LANguard N.S.S. jest zawsze na czasie z bieżącymi uaktualnieniami Microsoft'u oraz nowymi testami bezpieczeństwa GFI i innych składnic informacji, takich jak bazy danych OVAL.

■ Dbanie o optymalną wydajność obcych aplikacji zabezpieczających takich jak programy antywirusowe i anty-szpiegowskie

GFI LANguard N.S.S. kontroluje czy obsługiwane aplikacje zabezpieczające, takie jak programy antywirusowe i anty-szpiegowskie posiadają aktualne definicje plików i funkcjonują poprawnie. Na przykład, pozwala sprawdzić czy wszystkie kluczowe funkcje aplikacji (np. skanowanie w czasie rzeczywistym) są włączone.

■ Łatwe tworzenie różnych typów skanowania i testów zagrożeń

W prosty sposób można skonfigurować skanowanie pod kątem różnych typów informacji; takich jak współdzielenie urządzeń, audyt bezpieczeństwa, zarządzanie hasłami oraz komputery, na których brakuje denego uaktualnienia lub service pack'a. Różne zagrożenia mogą być skanowane w celu zidentyfikowania potencjalnych problemów bezpieczeństwa. Między innymi:

- **Otwarte porty:** GFI LANguard N.S.S. skanuje w poszukiwaniu otwartych portów i sprawdza czy nie zachodzi zawłaszczanie portów.
- **Nie używane konta użytkowników lub grupy:** usuwanie i wyłączenie nieużywanych kont użytkowników
- **Czarne listy aplikacji:** identyfikowanie nieautoryzowanego i niebezpiecznego oprogramowania, które ma być powiązane z bardziej aktywnym alarmowaniem zagrożeń
- **Niebezpieczne urządzenia USB, węzły sieci bezprzewodowej i połączenia:** Skanowanie wszystkich urządzeń podłączonych do USB lub sieci bezprzewodowej i alarmowanie o wszystkich podejrzanych działaniach.
- **I wiele więcej!**

■ Ustaw własne skanowanie zagrożeń

GFI LANguard N.S.S. pozwala w łatwy sposób zaprogramować spersonalizowane sprawdzanie zagrożeń dzięki wspomaganym przez kreatora ustawieniom. Dzięki GFI LANguard N.S.S. VBScript można programować skomplikowane sprawdzenia zabezpieczeń. GFI LANguard N.S.S. zawiera edytor i debugger skryptów ułatwiający ich rozbudowę.

■ Z łatwością analizuj i filtruj wyniki skanowania

GFI LANguard N.S.S. pozwala na łatwą analizę i filtrowanie wyników skanowania przez kliknięcie na jedno ze zdefiniowanych kryteriów. Umożliwia to, na przykład, odnajdowanie komputerów o wysokiej podatności na zagrożenia lub tych, które nie posiadają danego service pack'a. Spersonalizowane filtry mogą być łatwo tworzone od podstaw lub dostosowywane. Rezultaty skanowania mogą być eksportowane do plików XML.

Zarządzanie uaktualnieniami

Po zakończeniu skanowania, GFI LANguard N.S.S. daje funkcjonalność i narzędzia, które są potrzebne do efektywnego instalowania i zarządzania uaktualnieniami na wszystkich komputerach działających na różnych systemach operacyjnych w 38 językach. GFI LANguard umożliwia także automatyczne pobieranie aktualizacji, jak i cofanie instalacji poprawki. Spersonalizowane oprogramowanie również może być dystrybuowane. Wszystko to zapewnia stałe konfigurowanie środowiska, aby pozostawało zabezpieczone przed jakimikolwiek zagrożeniami.

■ Automatyczne instalowanie w sieci uaktualnień i service pack-ów

Za pomocą GFI LANguard N.S.S. można z łatwością zainstalować brakujące w sieci uaktualnienia i service pack-i. GFI LANguard N.S.S. jest idealnym narzędziem do monitorowania czy serwis aktualizacyjny Microsoft-u wykonuje poprawnie swoje zadania, takie jak instalowanie uaktualnień Microsoft Office-a i spersonalizowanego oprogramowania. GFI LANguard N.S.S. posiada także nowe dodatkowe cechy takie jak automatyczne pobieranie uaktualnień i rollback (odinstalowanie) uaktualnień. Jest zgodny z Unicode i obsługuje zarządzanie uaktualnieniami dla 38 języków używanych obecnie przez Microsoft.

■ Rozprowadzanie w sieci firmowej uaktualnień innych producentów

Poza dystrybucją uaktualnień i service pack-ów, GFI LANguard N.S.S. pozwala z łatwością instalować oprogramowanie innych producentów w całej sieci. Można w ten sposób dystrybuować w sieci oprogramowanie klienckie, uaktualnienia spersonalizowane oprogramowanie, nie tylko Microsoftu, oraz bazy danych wirusów. Daje to możliwość obycia się bez Microsoft SMS, który jest zbyt skomplikowany i drogi dla małych i średnich sieci.

Audyty sieci i oprogramowania

Funkcje audytowania GFI LANguard N.S.S. dostarczają informacji na temat tego wszystkiego co powinieneś wiedzieć o swojej sieci – jakie urządzenia USB są do niej podłączone, jakie oprogramowanie jest zainstalowane, jakie otwarte porty i słabe hasła są w użyciu. Dogłębne raporty dostarczają ważnych obrazów sieci uzyskanych w czasie rzeczywistym. Rezultaty skanowania mogą być z łatwością analizowane za pomocą filtrów i raportów umożliwiających aktywne zabezpieczanie sieci przez zamykanie portów, usuwanie kont użytkowników i lub grup, które nie są używane lub blokowanie połączeń bezprzewodowych z punktami dostępu.

■ Automatyczne alerty o lukach w zabezpieczeniach

GFI LANguard N.S.S. wykonuje zaplanowane (np. raz dziennie lub raz w tygodniu) i porównuje rezultaty z poprzednimi skanami. Wszystkie nowe luki w zabezpieczeniach lub zmiany w ustawieniach zabezpieczeń wykryte w sieci są przesyłane mailowo do przeanalizowania. Pozwala to na szybkie zidentyfikowanie nowo-zainstalowanych serwisów, aplikacji, użytkowników, nowo-otwartych portów i innych.

■ Skanowanie i odzyskiwanie danych z systemów Linux

Istnieje możliwość zdalnego uzyskiwania danych systemu operacyjnego opartego na Linux-ie a wyniki są przedstawiane w taki sam sposób jak w systemach opartych na Windows-ie. Oznacza to, że komputery pracujące na systemie Windows i Linux mogą być analizowane przy jednej sesji skanowania. GFI LANguard N.S.S. zawiera liczne Linux-owskie testy kontrolne, włącznie z wykrywaniem rootkitów. GFI LANguard N.S.S. może wykorzystywać pliki prywatnych kluczy SSH zamiast konwencjonalnych ciągów haseł uwierzytelniających dla komputerów pracujących w Linux-ie.

Wymagania systemowe

- Systemy operacyjne Windows 2000 (SP4), XP (SP2), 2003, VISTA
- Internet Explorer 5.1 lub nowszy
- Klient komponentów Microsoft Networks – dla system Windows 95 lub nowszego
- Secure Shell (SSH) – zawarty standardowo we wszystkich dystrybucjach Linux-a.

Nagrody



Pobierz wersję testową z <http://www.gfi.com/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

ed&r Polska SP. z o.o.
Biuro Handlowe
ul. Nowy Świat 32/106
Lublin 20 - 418
PL
Tel. +48/ 81/ 534-83-25
Fax. +48/ 81/ 534-83-26
gfi@edr.pl



ed&r
IT Experts Group
GFI
Authorised distributor
SECURITY SPECIALIST