Erste Schritte: Start der Überwachung

Einführung in Sicherheitsüberwachungen

Mit Hilfe der Netzwerküberwachung (Sicherheits-Audit) können Administratoren potenzielle Sicherheitslücken in einem Netzwerk aufdecken. Eine manuelle Überprüfung ist sehr zeitaufwändig, da sich viele Arbeitschritte und Aufgaben wiederholen und für jeden einzelnen Netzwerk-Rechner durchgeführt werden müssen. Mit GFI LANguard N.S.S. lassen sich Sicherheitskontrollen Ihres Netzwerks automatisch durchführen, und Ihr Netzwerk wird schnell und effektiv auf gängige Schwachstellen überprüft.

Hinweis: Werden in Ihrem Unternehmen IDS-Produkte eingesetzt, löst der Scan-Vorgang des GFI LANguard Network Security Scanner sämtliche Alarme dieser Produkte aus. Sind Sie nicht mit der Administration des IDS-Systems betraut, sollten Sie daher den zuständigen Administrator über einen bevorstehenden Scan informieren.

Neben den von den Scans verursachten IDS-Alarmen sollten Sie auch beachten, dass viele der Scans auch in Protokolldateien verzeichnet werden. UNIX-Logs, Web-Server usw. zeigen die Zugriffsversuche des Rechners an, von dem der N.S.S. gestartet wird. Gibt es mehrere Netzwerk-Administratoren in Ihrem Unternehmen, sollten Sie Ihre Kollegen über bevorstehende Scans informieren.

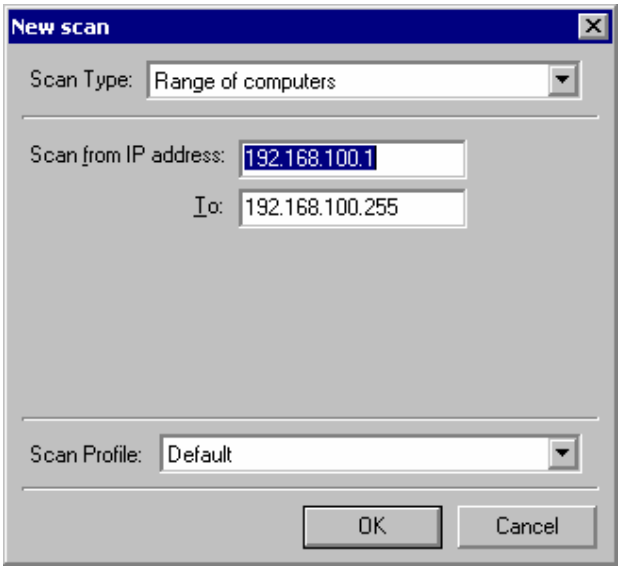
Durchführung eines Scan-Vorgangs

Der erste Schritt zu Beginn eines Netzwerk-Audits besteht darin, einen Scan der aktiven Netzwerk-Rechner und -Geräte durchzuführen.

So starten Sie einen Netzwerk-Scan:

1. Klicken Sie auf “File“ > “New“.
2. Wählen Sie die zu scannenden Bereiche aus. Zur Auswahl stehen:
    a. Scan one Computer – Hierdurch wird ein einzelner Rechner gescannt.
    b. Scan Range of Computers – Hierdurch wird ein bestimmter IP-Bereich gescannt.
    c. Scan List of Computers – Hierdurch werden verschiedene, von Ihnen aufgelistete Rechner gescannt. Rechner können dieser Liste hinzugefügt werden, indem Sie sie aus einer Übersicht der verfügbaren Rechner auswählen, sie einzeln eingeben oder über eine txt-Datei importieren.
    d. Scan a Domain – Hierdurch wird eine vollständige Windows-Domäne gescannt.

3. Je nachdem, welche Scan-Funktion Sie wählen, müssen Sie die Anfangs- und End-Adresse des zu überprüfenden Bereichs angeben.
4. Klicken Sie auf “Start Scan“.



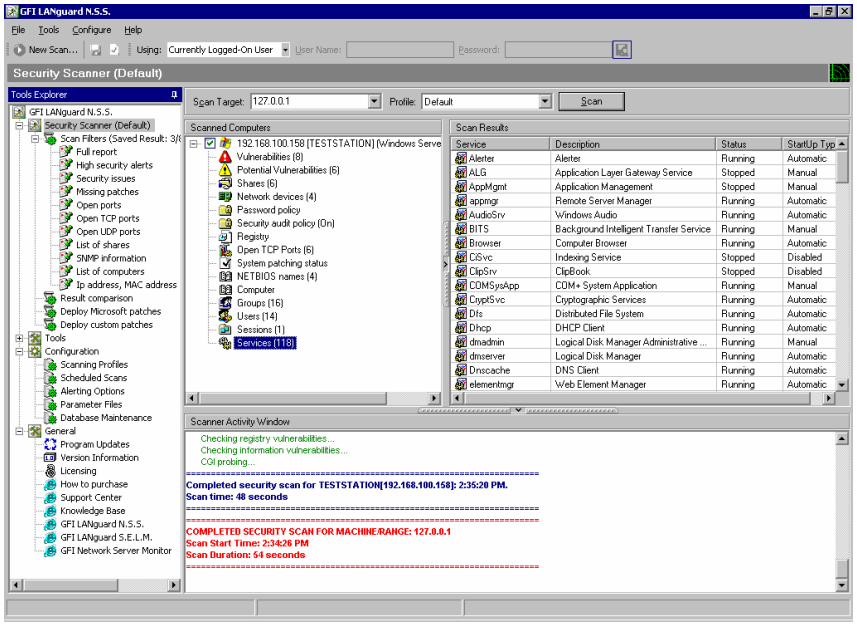
Durchführung eines Scan-Vorgangs

GFI LANguard N.S.S. führt nun den gewünschten Scan durch. Zunächst werden sämtliche aktiven Hosts/Computer aufgelistet und nur diese gescannt. Hierfür werden NetBIOS-Probes, ICMP-Ping und SNMP-Anfragen eingesetzt.

Reagiert ein Gerät auf einen dieser Tests nicht, geht der N.S.S. davon aus, dass es zum Zeitpunkt der Überprüfung unter keiner bestimmten IP-Adresse erreichbar oder gerade deaktiviert ist.

Hinweis: Wenn ein Scan auch auf jeden Fall für Geräte durchgeführt werden soll, die zunächst nicht antworten, finden Sie die hierfür notwendigen Einstellungen im Kapitel “Konfigurierung der Scan-Optionen“.

Analyse der Scan-Ergebnisse



Analyse der Scan-Ergebnisse

Nach jedem Scan-Vorgang sind unter allen vom N.S.S. gefundenen Rechnern verschiedene Knoten aufgeführt. Im linken Fenster werden sämtliche Rechner und Netzwerk-Geräte aufgelistet. Werden diese erweitert, erscheinen weitere Unterknoten mit allen Informationen, die zum jeweiligen Rechner oder dem Netzwerk-Gerät gesammelt werden konnten. Durch einen Mausklick auf einen dieser Knoten werden die Scan-Ergebnisse im rechten Fenster angezeigt.

Während eines Netzwerk-Scans findet der N.S.S. alle aktiven Netzwerk-Geräte. Eine genaue Identifizierung der Geräte durch den N.S.S. und die Art der abrufbaren Informationen sind abhängig vom Gerätetyp und dem Anfragetyp, auf den das Gerät reagiert.

Ist die Überprüfung des Rechners/Geräts/Netzwerks abgeschlossen, werden folgende Informationen angezeigt:

IP, Rechnername, Betriebssystem und installierte Service Packs

Die IP-Adresse des Rechners/Geräts wird angegeben. Danach folgt der NetBIOS-/DNS-Name, je nach Gerätetyp. Zudem zeigt der N.S.S. an, welches Betriebssystem auf den überprüften Rechnern läuft. Bei Windows NT/2000/XSP/2003 erhalten Sie zudem Informationen zu den installierten Service Packs.

Knoten für Sicherheitslücken ("Vulnerabilities")

Der Knoten für Sicherheitslücken ("Vulnerabilities") informiert Sie über bekannte Sicherheitsprobleme und gibt Tipps, wie diese zu beseitigen sind. Zu diesen Sicherheitsgefahren zählen fehlende Patches und Service Packs, HTTP-Schwachstellen, NetBIOS- und Konfigurationsprobleme etc.

Sicherheitslücken werden in folgende Kategorien eingeteilt: Fehlende Service Packs ("Missing Service Packs"), fehlende Patches ("Missing

Patches“), kritische Sicherheitslücken (“High Security Vulnerabilities“), wichtige Sicherheitslücken (“Medium security vulnerabilities“) und kleinere Sicherheitslücken (“Low security vulnerabilities“).

Unter jeder der Kategorien für kritische/wichtige/kleinere Sicherheitslücken erfolgt eine weitere Klassifizierung der gefundenen Probleme in: CGI-Missbrauch, Schwachstellen aus den Bereichen FTP, DNS, E-Mail, RPC, Dienste, Registry und sonstigen Bereichen.

Missing patches: GFI LANguard N.S.S: sucht nach fehlenden Patches, indem überprüft wird, welche Patches für ein bestimmtes Produkt bereits installiert und welche zusätzlich verfügbar sind. Fehlen Patches, sieht die entsprechende Warnmeldung in etwa wie folgt aus:

Als Erstes erscheint die Meldung, für welches Produkt ein Patch fehlt. Mit einem Klick auf das Produkt erfahren Sie dann, welcher Patch im Einzelnen fehlt. Über den angegebenen Link können Sie diesen Patch dann herunterladen.

CGI Abuses informiert Sie über Probleme bei Apache-, Netscape-, IIS- und anderen Web-Servern.

FTP Vulnerabilities, DNS Vulnerabilities, Mail Vulnerabilities, RPC Vulnerabilities und **Miscellaneous Vulnerabilities** bieten Links zu Bugtraq oder anderen Sicherheits-Sites, wo Sie weitere Informationen zu den vom N.S.S. gefundenen Problemen finden.

Service Vulnerabilities können verschiedenste Bereiche betreffen: Sie können sich auf aktuelle Dienste beziehen, die auf dem untersuchten Gerät laufen sind, oder auch auf bisher ungenutzte Rechner-Konten.

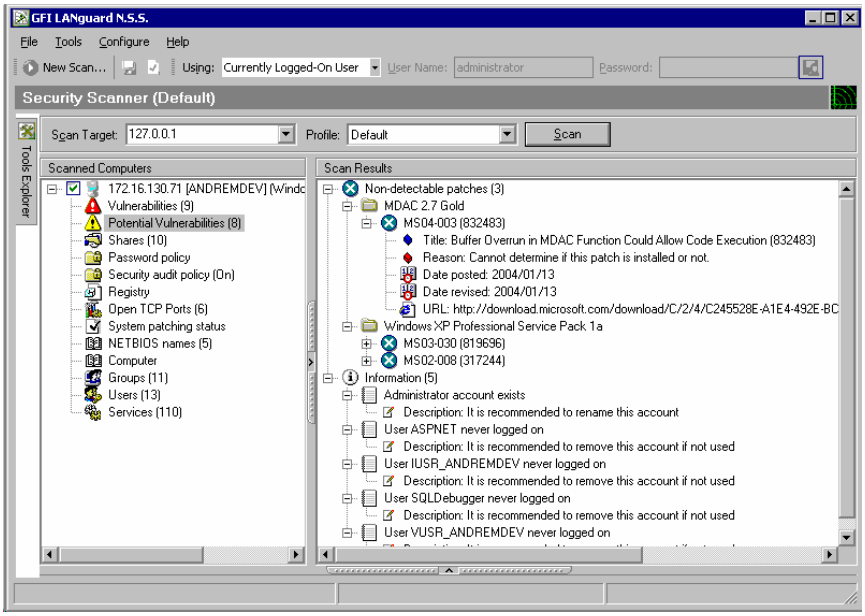
Registry Vulnerabilities werden für Schwachstellen ausgegeben, die zu Beginn des Scans in der Registrierdatenbank eines Windows-Rechners gefunden werden. Hierbei können über entsprechende Links zur Microsoft-Site oder anderen Security-Sites nähere Informationen abgerufen werden, warum die betreffenden Registry-Einträge geändert werden sollten.

Information Vulnerabilities sind Sicherheitsmitteilungen, die in der Datenbank gespeichert werden und über die der Administrator informiert sein muss; sie beschreiben Sicherheitslücken, die jedoch nur bedingt gefährlich sind.

Knoten für potenzielle Sicherheitslücken (“Potential Vulnerabilities“)

Im Knoten für potenzielle Sicherheitslücken (“Potential Vulnerabilities“) werden mögliche Schwachstellen, wichtige Informationen und einzelne Kontrollen, die nicht durchgeführt werden konnten, angezeigt. Falls z. B. nicht festgestellt werden konnte, ob ein bestimmter Patch installiert ist, wird dieser bei den Scan-Ergebnissen unter dem Knoten “Non-detectable Patches“ aufgeführt. Der

Administrator muss daraufhin die entsprechenden Überprüfungen manuell durchführen.



Knoten für potenzielle Sicherheitslücken

Freigaben (“Shares“)

Der Knoten "Shares" informiert Sie über alle Freigaben auf einem Rechner und welche Anwender darauf Zugriff haben. Sämtliche Netzwerk-Freigaben müssen gesichert werden. Administratoren sollten sicherstellen, dass:

1. kein Benutzer anderen Anwendern Zugriff auf die gesamte Festplatte gewährt.
2. ein anonymer/nicht authentifizierter Zugriff auf Freigaben nicht erlaubt ist.
3. Auto-Start-Ordner oder ähnliche Systemdateien nicht gemeinsam genutzt werden können. Andernfalls hätten Benutzer mit eingeschränkten Zugriffsrechten dennoch die Möglichkeit, Programme/Code auf Zielrechnern zu starten.

Diese Warnungen gelten für alle Rechner, jedoch insbesondere für solche, die wichtig für die Systemintegrität sind, z. B. der Primary Domain Controller (PDC). Wird der Auto-Start-Ordner (oder das Verzeichnis mit dem Auto-Start-Ordner) auf dem PDC vom Administrator für alle Benutzer freigegeben, kann dies schwer wiegende Folgen haben. Mit den entsprechenden Zugriffsrechten können Benutzer problemlos ausführbare Dateien in den Auto-Start-Ordner kopieren, die dann beim nächsten interaktiven Login des Administrators gestartet werden.

Hinweis: Wenn Sie einen Scan durchführen, während Sie als Administrator angemeldet sind, werden auch die administrativen Freigaben angezeigt, z. B. “C$ - Standardfreigabe“. Diese Freigaben stehen normalen Anwendern jedoch nicht zur Verfügung.

Aufgrund der neuartigen Verbreitung des Klez-Virus und anderer neuer Viren über offene Freigaben sollten alle nicht benötigten

Freigaben deaktiviert werden. Alle anderen sollten durch ein Passwort gesichert sein.

Passwort-Richtlinien ("Password Policy")

Mit Hilfe dieses Knotens können Sie kontrollieren, ob die Passwort-Richtlinien genügend Sicherheit bieten. Beispielsweise können Sie die maximale Gültigkeitsdauer festlegen und die Passwort-Protokollierung aktivieren. Die minimale Passwort-Länge sollte 8 Zeichen betragen. Wenn Sie Windows 2000 verwenden, können Sie mit Hilfe eines GPO (Group Policy Object) in Active Directory eine netzwerkweite Richtlinie für sichere Passwörter erstellen.

Registry

Dieser Knoten liefert wichtige Informationen zur Remote-Registry. Klicken Sie auf den Knoten "Run" um herauszufinden, welche Programme beim Booten des Rechners automatisch gestartet werden.

Stellen Sie sicher, dass die automatisch gestarteten Applikationen keine Trojaner oder sogar erwünschte Programme sind, über die per Fernzugriff auf einen Rechner zugegriffen werden kann (wenn solche Software nicht in Ihrem Netzwerk eingesetzt werden darf). Jede Remote-Access-Software kann sich u. U. als Backdoor-Schwachstelle herausstellen und von Hackern ausgenutzt werden.

Richtlinien für Sicherheitsüberwachungen ("Security Audit Policy")

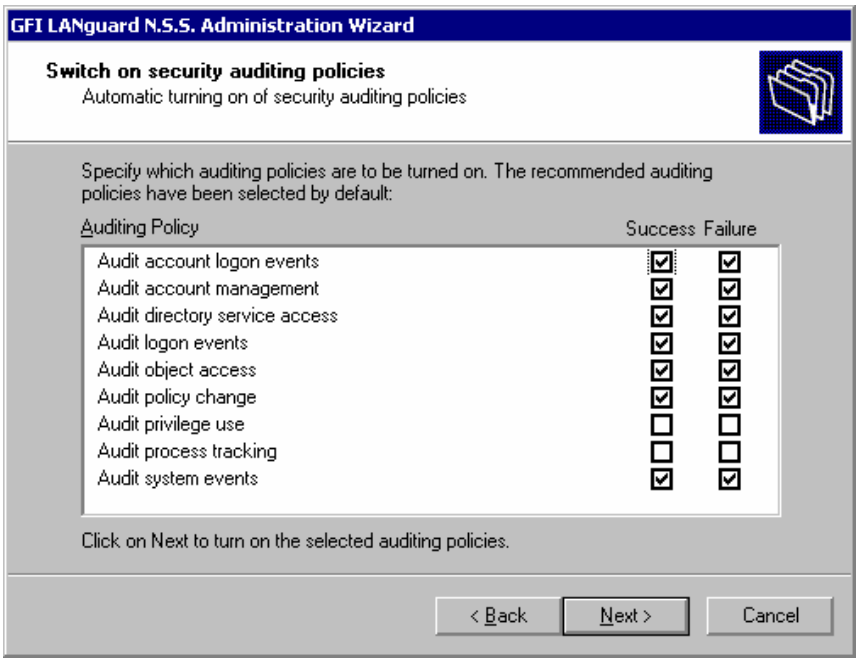
Über diesen Knoten werden Sie informiert, welche verschiedenen Überwachungsrichtlinien auf dem Remote-Rechner aktiviert sind. Folgende Überwachungsrichtlinien sind zu empfehlen:

Überwachungsrichtlinie	Erfolg	Fehler
Anmeldeversuche	Ja	Ja
Kontenverwaltung	Ja	Ja
Active Directory-Zugriff	Ja	Ja
Anmeldeereignisse	Ja	Ja
Objektzugriffsversuch	Ja	Ja
Richtlinienänderungen	Ja	Ja
Rechteverwendung	Nein	Nein
Vorgangsprotokollierung	Nein	Nein
Systemereignisse	Ja	Ja

Die Überwachung kann direkt über GFI LANguard N.S.S. aktiviert werden. Klicken Sie hierfür mit der rechten Maustaste auf einen der Rechner im linken Fenster, und wählen Sie "Enable auditing". Hierdurch wird der Administrations-Assistent für Überwachungsrichtlinien gestartet.

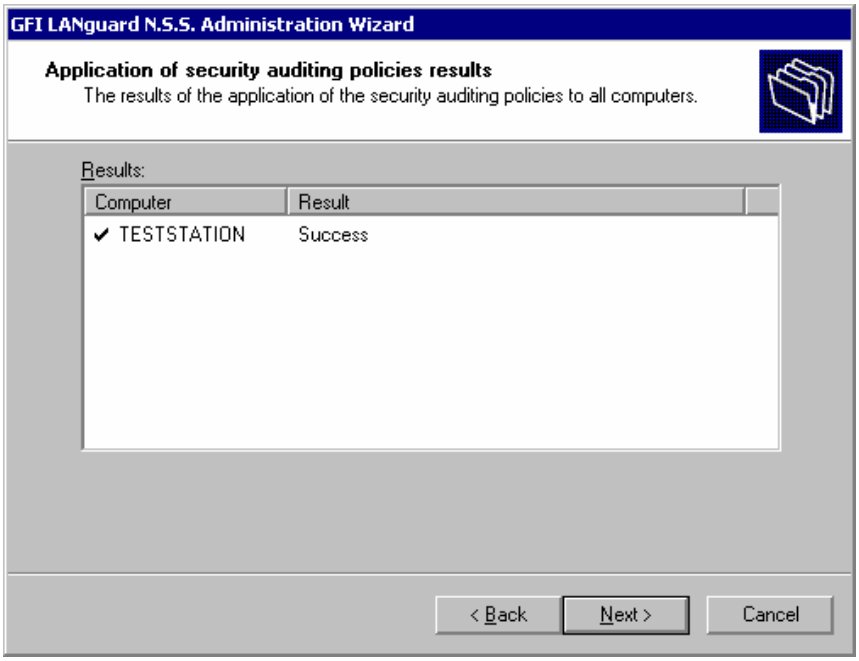
Geben Sie an, welche Audit-Richtlinien aktiviert werden sollen. Unter Windows NT stehen sieben und unter Windows 2000 neun Überwachungsrichtlinien zur Verfügung. Aktivieren Sie die

gewünschten Richtlinien auf den zu überwachenden Rechnern. Klicken Sie hierfür auf “Next“.



Aktivierung von Überwachungsrichtlinien auf Remote-Rechnern

Treten keine Fehler auf, wird der Abschlussdialog angezeigt. Andernfalls erscheint ein Dialogfenster, das Sie darüber informiert, auf welchen Rechnern die Richtlinienaktivierung fehlgeschlagen ist.



Ergebnisdialog im Assistenten für Sicherheitsrichtlinien

Offene Ports

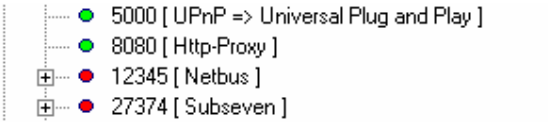
Der Knoten führt alle offenen Ports auf, die auf dem Rechner gefunden wurden (Port-Scan). GFI LANguard N.S.S. führt einen

eingeschränkten Port-Scan durch, d. h., es werden nicht standardmäßig alle 65535 TCP- und 65535 UPD-Ports gescannt, sondern nur solche, die von Ihnen festgelegt wurden. Über die Scan-Optionen lassen sich die zu überprüfenden Ports im Einzelnen festlegen. Weitere Informationen hierzu finden Sie im Kapitel “Konfigurierung von GFI LANguard N.S.S.“

Jeder offene Port steht für einen Dienst/eine Applikation. Ist einer dieser Dienste nur unzureichend vor Missbrauch geschützt, können Hacker ungehindert Zugriff auf diesen Rechner nehmen. Daher ist es wichtig, nicht benötigte Ports zu schließen.

Hinweis: Bei Windows Networks sind die Ports 135, 139 und 445 immer offen.

Der N.S.S. zeigt alle offenen Ports an. Wird ein Port als ein bekannter Trojaner-Port eingestuft, wird er vom Scanner ROT angezeigt. Andernfalls erscheint ein GRÜNER Punkt . Dies zeigt folgender Screenshot:



Hinweis: Selbst wenn ein Port als möglicher Trojaner-Port ROT angezeigt wird, heißt dies jedoch nicht, dass auf dem betreffenden Rechner tatsächlich ein Backdoor-Programm installiert ist. Einige gültige Programme greifen auf dieselben Ports zurück wie verschiedene, bereits bekannte Trojaner. Ein bekanntes Anti-Viren-Programm nutzt beispielsweise denselben Port wie der NetBus Backdoor-Trojaner. Daher sollten Sie immer die angegebenen Banner-Informationen kontrollieren und auf den betreffenden Rechnern weitere Prüfungen durchführen.

Benutzer und Gruppen (“Users & Groups“)

Diese beiden Knoten geben Aufschluss über lokale Gruppen und Benutzer, die auf dem Rechner verfügbar sind. Überprüfen Sie die Scan-Ergebnisse auf zusätzliche Benutzerkonten, und kontrollieren Sie, ob das Gastkonto deaktiviert ist. Über diese Konten könnte durch böswillige Benutzer und Gruppen eine Hintertür für den Zugriff auf das Netzwerk geöffnet werden!

Einige Backdoor-Programme aktivieren das Gäste-Konto erneut und versehen es mit Administrator-Rechten. Daher sollten Sie die Angaben des Benutzer-Knotens überprüfen, um einen Überblick über die Aktivitäten aller Konten und ihre Rechte zu erhalten.

Benutzer sollten sich nicht über ein lokales Konto anmelden können, sondern nur in einer Domäne oder über ein Active Directory-Konto.

Zudem ist es auch noch wichtig zu überprüfen, ob Passwörter eventuell bereits zu lange in Gebrauch sind.

Dienste

Sämtliche Dienste, die auf den überprüften Rechnern laufen, werden aufgelistet. Es sollten nur tatsächlich benötigte Dienste aktiv sein. Stellen Sie daher sicher, dass alle anderen Dienste deaktiviert sind.

Jeder Dienst stellt ein potenzielles Sicherheitsrisiko dar und könnte als “Schlupfloch“ für Hacker dienen.

System Patching-Status

Dieser Knoten informiert Sie darüber, welche Patches auf dem Remote-Rechner installiert und registriert sind.

Zusätzliche Ergebnisse

Folgende Knoten und Ergebnisse sollten Sie kontrollieren, nachdem Sie die bereits weiter oben beschriebenen, wichtigeren Scan-Ergebnisse überprüft haben.

NetBIOS names

Mit Hilfe dieses Knotens erfahren Sie im Detail, welche Dienste auf einem Rechner installiert sind.

Computer

MAC gibt die MAC-Adresse der Netzwerk-Karte an.

Username gibt den Namen des aktuell angemeldeten Benutzers oder den Rechnernamen an.

TTL gibt den jedem Gerät eigenen Time To Live-Wert (TTL) an. Die Standardwerte sind 32, 64, 128 und 255. Der TTL-Wert basiert auf diesen Werten und dem tatsächlichen TTL des Datenpakets und informiert über den Abstand (Anzahl der Router-Hops) zwischen dem N.S.S.-Rechner und dem gerade gescannten Computer.

Computer Usage informiert Sie darüber, ob der untersuchte Rechner eine Workstation oder ein Server ist.

Domain informiert Sie über die vertrauenswürdige(n) Domäne(n), wenn der gescannte Rechner Teil einer Domäne ist.

Gehört er zu keiner Domäne, wird die Arbeitsgruppe angezeigt, deren Bestandteil er ist.

LAN manager bietet Angaben zum verwendeten LAN-Manager (und zum Betriebssystem).

Sessions

Zeigt die IP-Adressen der Rechner an, die zum Zeitpunkt des Scan-Vorgangs mit dem Zielrechner verbunden waren. In den meisten Fällen ist dies nur der Rechner, auf dem der N.S.S. eingesetzt wird und der kurz zuvor eine Verbindung aufgebaut hat.

Hinweis: Da sich dieser Wert laufend ändert, wird er nicht im Bericht gespeichert, sondern dient lediglich der allgemeinen Information.

Network Devices

Bietet eine Liste der Netzwerk-Geräte, die auf dem gescannten Rechner zur Verfügung stehen.

Remote TOD

Tageszeit der Gegenstelle. Gibt die Netzwerk-Zeit auf dem gescannten Rechner an, die vom Domänen-Controller bestimmt wird.

Durchführung von On-Site- und Off-Site-Scans

Es ist zu empfehlen, N.S.S.-Scans mit Hilfe zweier Methoden durchzuführen, dem so genannten On-Site- und Off-Site-Scan.

On-Site-Scan

Richten Sie einen Rechner ein, auf dem Sie GFI LANguard N.S.S. installieren. Führen Sie einen Scan Ihres Netzwerks über eine Null-Sitzung durch. Wählen Sie hierfür “Null Session“ aus dem Drop-Down-Listenfeld aus.

Nach diesem ersten Scan ändern Sie die Einstellung über das Listenfeld bitte auf “Currently logged on user“ (wenn Sie administrative Rechte für Ihre Domäne besitzen) oder auf “Alternative credentials“, über die administrative Rechte für die Domäne oder Active Directory zur Verfügung stehen.

Sie sollten die Ergebnisse dieses zweiten Durchgangs als Vergleichswerte speichern.

Mit der Null-Sitzung haben Sie die Möglichkeit herauszufinden, welche Daten den Benutzern zugänglich sind, die eine Verbindung mit Ihrem Netzwerk über eine solche Null-Sitzung herstellen. Der mit Administrator-Rechten durchgeführte Scan informiert Sie über alle Hot Fixes und Patches, die auf dem Rechner fehlen.

Off-Site-Scan

Ist ein Netzwerk-Zugriff per DFÜ möglich oder eine High-Speed-Internet-Anbindung verfügbar, die nicht an Ihr Unternehmen gebunden ist, sollten Sie nun Ihr Netzwerk auch von außen einem Scan unterziehen.

Führen Sie einen Scan Ihres Netzwerks per Null-Sitzung durch. Dadurch erfahren Sie, welche Informationen bei einem über das Internet gestarteten Scan Ihres Netzwerks abrufbar sind. Der Scan kann jedoch durch Firewalls in Ihrem Unternehmen oder bei Ihrem ISP beeinträchtigt werden. Gleiches gilt auch für die Kommunikation über Router, die bestimmte Pakettypen nicht weiterleiten.

Speichern Sie die Ergebnisse, um sie später als Vergleichswerte heranziehen zu können.

Vergleich von On-Site- und Off-Site-Scans

Die von GFI LANguard Network Security Scanner gesammelten Informationen sollten nun genauer analysiert werden.

Sind die Daten des Scans, der per Null-Sitzung aus dem Netzwerk heraus erfolgt ist, mit denen des externen Scans identisch, scheint Ihr Netzwerk keine funktionsfähige Firewall oder andere Sicherheitsfilter zu besitzen. In diesem Fall sollten Sie sich zunächst um diese Sicherheitslücken kümmern.

Überprüfen Sie danach, welche Informationen außerhalb Ihres Netzwerks abrufbar sind. Sie sollten überprüfen, ob z. B. Ihre Domain Controller für alle externen Benutzer sichtbar sind oder ob eine Liste aller Computer-Konten öffentlich zugänglich ist.

Zudem sollten Sie bei Web-Servern, FTP-Zugängen und ähnlichem eigene Sicherheitsprioritäten festlegen. So ist es unter Umständen

erforderlich, beispielsweise nach Patches für Web-Server und FTP-Server zu suchen. Auch die Einstellungen für SMTP-Server sollten überprüft und ggf. geändert werden. Kein Netzwerk gleicht dem anderen. Der N.S.S. hilft Ihnen gezielt bei der Suche nach Netzwerk-Schwachstellen und Sicherheitsproblemen und verweist auf qualifizierte Web-Sites, die Lösungsvorschläge zur Beseitigung dieser Gefahren bieten.

Wenn Sie Dienste finden, die aktiv sind, aber nicht benötigt werden, sollten Sie diese auf jeden Fall deaktivieren. Jeder Dienst stellt ein potenzielles Sicherheitsrisiko dar, das Dritten einen unautorisierten Zugriff auf Ihr Netzwerk ermöglicht. Es werden ständig neue Buffer-Overflow-Techniken und Exploits entwickelt, die Ihr Netzwerk bedrohen. Schutzmaßnahmen, die gegenwärtig als zuverlässig eingestuft werden, können sich sehr schnell als veraltet und somit als Sicherheitsrisiko erweisen.

Daher sollten Sicherheits-Scans in regelmäßigen Abständen durchgeführt werden. Nur so können Sie sicher sein, dass Schwachstellen entdeckt werden, bevor Hacker sich diese zum Eindringen in Ihr Netzwerk zu Nutze machen können.