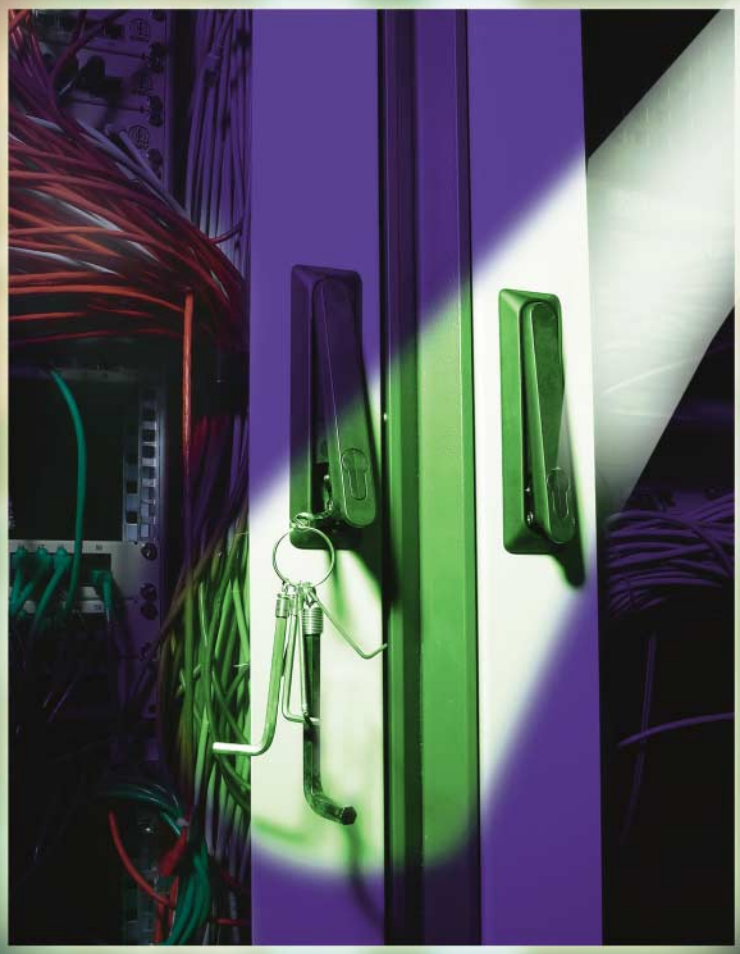
Mit Schwachstellenscannern Sicherheitslücken finden

Schlupflöcher

Christoph Puppe

Schritt eins bei der Absicherung des Firmennetzes gegen unbefugte Zugriffe ist das Aufspüren und Stopfen bekannter Schwachstellen. Für diesen „Basis-Check" bietet der IT-Markt zahlreiche allgemeine sowie auf spezielle Server zugeschnittene Scanwerkzeuge.

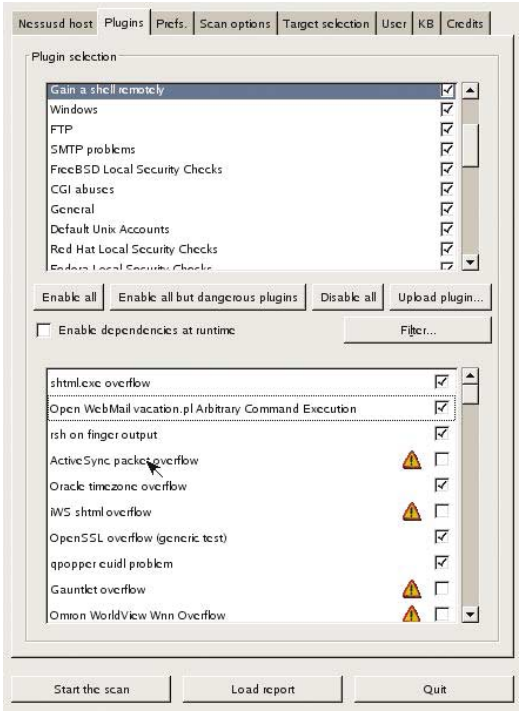


Wenn ein gewisses weibliches Halb-Mensch/Halb-Maschinenwesen einer berühmten Science-Fiction-Serie die Sensorenphalanx neu kalibriert, um nach Signaturen zu scannen, wird nach etwas gesucht, was entweder das Sternenflottenraumschiff Voyager gefährden könnte oder neue Erkenntnisse verspricht. Nach Gefährdungen suchen auch die in dieser Produktübersicht vorgestellten Schwachstellenabtaster, neudeutsch Vulnerability Scanner (siehe Übersichtstabelle „Schwachstellenscanner für Unternehmensnetze"). Analog zur Voyager durchforsten sie das Netzwerk nach Signaturen von bekannten sicherheitsrelevanten Schwachstellen.

Führt man eine solche Suche von Schwachstellen im Firmennetz manuell durch, ist das eine langwierige Prozedur. Wenn die aufgespürten Schwachstellen dann noch ausgenutzt werden, nennt sich das Einbruchs- oder – im gewöhnungsbedürftigen Fachjargon – Penetrationstest. Das automatisierte Durchführen solcher Tests kann zwar nicht grundsätzlich den in der Regel teuren menschlichen Einbruchstester ersetzen, aber dank der zahlreich vorhandenen Werkzeuge kann der Systemadministrator oder Sicherheitsverantwortliche die gröbsten Lücken schon mal finden und stopfen.

Den Grundstein zur Automation legte im Jahr 1989 Dan Farmer mit dem Computer Oracle and Password System (COPS), einer Sammlung von Shell-Skripten, die nach fehlerhaften Konfigurationen auf Unix-Rechnern suchen. Den ersten Scanner, der Verwundbarkeiten über ein Netz aufspürt, schrieb Christopher Klaus 1993. Heraus kam der Internet Security Scanner. Beide Prinzipien wurden seitdem aktiv weiterentwickelt und teilweise in einer Software kombiniert.

Scansoftware gibt es als frei verfügbare Open-Source- und kommerzielle Produkte, außerdem als Hardware-Appliances mit selbstentwickelter Software sowie solche, die auf Open-Source-Scannern – in der Regel Nessus (Abb. 1) – aufbauen. Die letzte Katego-



Üblicherweise sind die von Scannern angebotenen Tests in Gruppen zusammengefasst und können vom Benutzer einzeln an- und ausgeschaltet werden, hier am Beispiel des Open-Source-Scanners Nessus (Abb. 1).

rie ist in der vorliegenden Übersicht nicht enthalten, da sie den Funktionsumfang der eingesetzten Open-Source-Produkte meist nicht wesentlich erweitern. Manche Scanner sind auf einen bestimmten Servertyp spezialisiert, etwa auf Webserver oder Datenbanken. Die größte Gruppe bilden allerdings die für alle Servertypen einsetzbaren so genannten Allzweckscanner, zu denen auch sämtliche Appliances gehören.

In Hinblick auf IT-Haftungsfragen und Vorgaben wie den Sarbanes-Oxley-Act und Basel II ist es für Unternehmen mehr denn je erforderlich, die Risiken in allen (elektronischen) Geschäftsprozessen für Wirtschaftsprüfer nachweisbar zu bemessen und zu minimieren. Dafür ist das Entdecken von Schwachstellen in der IT-Infrastruktur, wie es die genannten Werkzeuge leisten, ein erster wichtiger Schritt. Es existieren über die Marktübersicht hinaus Produkte für das weitere Schwachstellen- und Patchlevel-Management.

Suche nach Bekanntem

So wie bei Star Trek wie auch im richtigen Leben muss man das Gesuchte in der Menge der Daten auch identifizieren können. Das eindeutige Muster zur Erkennung ist die Signatur. Suchen kann ein Scanwerkzeug nur nach bereits bekannt gewordenen Schwachstellen – dort also, wo schon die manuelle Untersuchung einer Anwendung ergeben hat, dass ein Programmierfehler vorliegt oder dass eine bestimmte Art, etwas zu konfigurieren, sich von Bösewichtern ausnutzen lässt.

Der Entdecker eines so genannten Exploit informiert den Hersteller und veröffentlicht nach einer angemessenen Frist seinen Fund, meistens auf den beiden wichtigsten einschlägigen Security-Mailing-Listen (Bugtraq@securityfocus.com und full-disclosure@lists.netsys.com). Ein Gremium des Schwachstellenprojekts CVE (Common Vulnerabilities and Exposures, www.cve.mitre.org/) vergibt für jede eingehende Beschreibung eine eindeutige so genannte CVE-Nummer. Genauso geht Securityfocus vor und vergibt die Bugtraq ID (BID). Da die Daten größtenteils von Securityfocus an das CVE-Gremium geliefert werden, gibt es für jede Schwachstelle eine BID, aber nicht notwendigerweise eine CVE – beispielsweise, wenn es sich bei der Entdeckung um keine echte Schwachstelle handelt.

Anhand der Beschreibung der Schwachstelle entwickelt der Hersteller

iX-TRACT

- Um eine erste Schwachstellenanalyse der IT-Infrastruktur durchzuführen, stehen Systemverantwortlichen zahlreiche Scanwerkzeuge zur Verfügung.
- Die auf verschiedene Servertypen spezialisierten Scanner dringen unterschiedlich tief in Systeme ein. Für den Tester bedeutet das ein Abwägen zwischen Risiko und Scangenauigkeit.
- Automatisierte Schwachstellenscans sind nützlich, ersetzen aber manuelle Einbruchstests durch Spezialisten nicht – zumal Bösewichter mit denselben Methoden vorgehen.

des Scanners eine Signatur, die die verwundbare Version dieses Programms möglichst genau identifiziert und bei der Suche nach Sicherheitslücken eingesetzt wird. Je nach Art des Scanners ist die Signatur für ein und dasselbe Problem unterschiedlich. Bei einem lokal auf dem Rechner arbeitenden Scanner besteht sie meist aus der Versionsnummer des installierten Pakets, dem Namen des Patches oder der Versionsnummer, die das Programm selbst auf Anfrage ausgibt. Bei einem Netzscanner kann die Signatur beispielsweise die in den Antworten des Servers enthaltene Versionsnummer sein. Oder eine bestimmte Zeichenfolge, die exakt so nur bei dieser Version vorkommt.

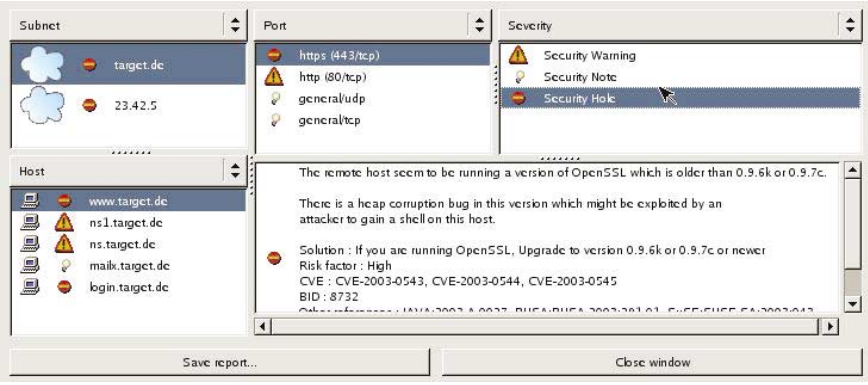
Wenn es ein solches eindeutiges Unterscheidungsmerkmal nicht gibt, kann man das Verhalten des Servers bei speziellen Anfragen untersuchen. Alternativ kann man eine Anfrage stellen, die die Schwachstelle ausnutzt, aber keinen Schaden anrichtet, sondern nur eine Datei anlegt oder eine Mail schickt. Eine lokal durchgeführte Untersuchung ist grundsätzlich genauer als eine Untersuchung von Servern über das Netz. Beide haben allerdings Schwierigkeiten mit der Erkennung, wenn der Hersteller der Software einen Patch herausbringt, ohne die Versionsnummer zu ändern – wobei der lokale Scanner auch hier einen Vorsprung hat, da er nach dem Patch suchen kann.

Scannen via Netz

Vor- und Nachteile lassen sich bei beiden finden. Im Betrieb ist der Netzscanner einfacher, da er nur auf einem System installiert sein muss und von dort alle Systeme in Reichweite überprüfen kann. Es behindern ihn dabei nur Firewalls, die eventuell den Zugang zu den zu testenden Systemen erschweren. Deswegen setzt der Tester üblicherweise einen Scanner pro Segment (beispielsweise je DMZ, je Teil des Intranets) ein, vorausgesetzt, dieser kann aus der Ferne bedient werden – wie beispielsweise die Appliances, Nessus, Saint, Nikto und der VA von Symantec. Andernfalls muss der Tester manuell mit dem Notebook im jeweiligen Segment arbeiten, zumindest wenn der Port nicht erreichbar ist. Für Webscanner hingegen ist das in der Regel keine Einschränkung.

Da die Netzwerkscanner nur über das Netz erreichbare Serverdienste abfragen können, sind ihre Ergebnisse auch auf diese beschränkt. Als Beispiel stelle man sich ein Linux-System vor, das als Web- und FTP-Server dient. Der Netzscanner kann diese beiden Dienste kontaktieren und anhand der Signaturen erkennen, ob die eingesetzte Version des Serverdienstes verwundbar ist. Dass es auf dem Linux-Server überdies einen verwundbaren Kernel gibt, kann der Scanner nur indirekt erkennen, nämlich über die Ausgaben mancher Programme. Hinzu kommt, dass der Scanner nur die Daten auswerten kann, die ihm der Serverdienst liefert. Wenn dieser „lügt“ und ein Apache sich beispielsweise als IIS ausgibt, stimmen viele Scanner ihre weiteren Tests auf diese Information ab und werden wundersamerweise keine der IIS-typischen Probleme auf dem Apache entdecken. Nur eine manuelle Überprüfung würde in diesem Fall zuverlässige Ergebnisse liefern.

Des Weiteren bereiten diejenigen Dienste Schwierigkeiten, die nicht auf dem Port laufen, den sie normalerweise benutzen. Nessus hat als erstes Scanwerkzeug angefangen, jeden offenen Port danach zu befragen, welcher Service dort läuft. So kann etwa ein Webserver erkannt werden, der auf dem FTP-Port lauscht. Mittlerweile enthalten viele Scanner dieses Feature, das in der Tabelle unter dem Stichwort „Diensterkennung“ zu finden ist.



Der Ergebnisbericht bei Nessus kennt drei Abstufungen: gravierende Sicherheitslücke (rotes Zeichen), mittelschwere Schwachstelle (Warndreieck) und Information (Lampe). Im gezeigten Beispiel hat Nessus in einer größeren IT-Umgebung einen verwundbaren HTTPS-Server gefunden (Abb. 2).

Je mehr, je besser

Die Qualität eines Scanwerkzeugs lässt sich an mehreren Eigenschaften bemessen. Der wichtigste Punkt ist jedoch die Aussagekraft und Verwertbarkeit der Ergebnisse: Findet der Scanner nur Schwachstellen, die wirklich vorhanden sind, oder führt er auch nicht vorhandene Fehler auf (false-positive)? Und ist die erste Liste vollständig oder erkennt er einige Probleme nicht (false-negative)? Die Anzahl der Signaturen, auf die ein Scanner testet – in der Tabelle unter „Zahl der Tests“ zu finden –, ist zwar ein erster Hinweis auf die Qualität des Produkts. Für eine angemessene Bewertung müsste jedoch getestet werden, ob die Schwachstellenerkennung anhand dieser Signaturen in der Praxis auch funktioniert.

Ein weiteres wichtiges Kriterium ist die Anzahl der neu hinzugefügten Signaturen und in welchen Abständen der Hersteller Updates zur Verfügung stellt. Jeden Tag entdecken Sicherheitsexperten, Programmierer und andere Interessierte neue Schwachstellen. Wenn niemand den Scanner mit deren Signaturen versorgt, wird er sie auch nicht finden. Die Lizenzmodelle kommerzieller Scanner sehen, vergleichbar den Virenscannern, die Benutzung bei einer definierten Anzahl von Systemen sowie Updates für einen bestimmten Zeitraum vor.

Wer sich für eine Open-Source-Lösung entscheidet, hat zwar keine Lizenzkosten, erhält aber auch nur dann Updates, wenn die Entwicklergemeinde „nachpflegt“. In der Regel sind Benutzer aufgefordert, ihrerseits etwas zum Projekt beizutragen. Ein weiterer großer Pluspunkt der Open Source ist die Erweiterbarkeit. Da die Signaturen offen liegen, kann man eigene ergänzen. Die kommerziellen Produkte zeigen sich hier naturgemäß zugeknöpfter, allerdings bringen die meisten eine Schnittstelle zur Programmierung eigener Signaturen oder gar Module mit.

Teilweise gibt es für einzelne Aufgaben „Spezialisten“. Zum Beispiel *nmap*, das sich als Standard für Portscans durchgesetzt hat, oder *libwhisker*, eine Bibliothek, die auf Scans von Webservern spezialisiert ist. Bis auf eine Ausnahme – AppDetective von AppSec importiert *nmap* – kann keines der kommerziellen Produkte die Ergebnisse von anderen Werkzeugen importieren. Nicht so die beiden Open-Source-Produkte: Nessus nutzt unter anderem *nmap*, *hydra* (Passwort-Brute-Force für viele Dienste) und *libwhisker* als Module, die der Anwender über die GUI konfigurieren kann und deren Ergebnisse der Scanner in seine eigenen Resultate einbaut. Der GPL-Webscanner Nikto bedient sich des Tools *nmap* zur Suche nach Webservern.

Ein Vergleich von Ergebnissen verschiedener Scanner ist nur möglich, wenn der Hersteller für die Schwachstellen die CVE-Bezeichnung angibt. Dies erleichtert außerdem die Suche nach Beschreibungen und Lösungen zu dieser Schwachstelle und ist sogar unerlässlich, wenn die Scanergebnisse die Grundlage für eine Verwaltung der Schwachstellen in einem herstellerunabhängigen Vulnerability-Management (VA) bilden sollen. Eine Schnittstelle zu einer solchen VA-Software bringen einige Produkte mit. Die Umsetzung variiert allerdings stark und reicht vom XML-Export über eine direkte Anbindung von Ticketing-Systemen bis hin zur vollständigen Integration in die herstellereigenen Managementsysteme. Wo keine Schnittstelle vorhanden ist, lassen sich die Daten in der Regel mit selbstgeschriebenen Scripts übertragen.

Vergleiche bringen es an den Tag

Das gilt ebenso für den Vergleich von zwei oder mehreren Scans in einem Netzwerk. In einigen Produkten ist dieser bereits vorgesehen, was dem Administrator das Script-Basteln erspart und neue Erkenntnisse beschert. Denn ein Vergleich kann zeigen, ob Systeme, offene Ports oder Schwachstellen neu hinzugekommen oder verschwunden sind. So lassen sich Änderungen in der Systemlandschaft und den derzeit im Netz vorhandenen Risiken schnell aufspüren und beheben.

Wenn man durch den Scan erfahren möchte, was sich im Netz verändert hat, muss der Scanner die neu hinzugekommenen Systeme auch finden. Dazu sollte er Methoden zur Suche nach Rechnern im Ethernet (zum Beispiel per ARP) und im Internet (via DNS) mitbringen. Dies leisten alle Scanner bis auf Nikto, der das aber mit dem Einbinden von *nmap* ausgleicht, den Datenbankscanner von ISS und Sandcat von Syhunt.

Ebenso bedeutend ist die Betriebssystemerkennung auf den zu scannenden Systemen, da der Scanner seine Suche auf Signaturen für das jeweilige Betriebssystem konzentrieren sollte, ohne sich durch eine diesbezüglich falsche Information aus dem Konzept bringen zu lassen. Nur Nikto und ScanDo bringen dieses Feature nicht mit, für auf Webserver spezialisierte Werkzeuge ist es auch nicht relevant.

Hersteller unterscheiden ihre Produkte gerne anhand der „intrusiveness“, also des Grades, mit dem der Scanner in das System eindringt. Eine geringe Eindringtiefe belastet den Server wenig und birgt weniger Risiken, dass es durch den Scan zu Problemen kommt, führt andererseits aber auch zu einer höheren Fehlerrate. Das lässt sich nicht vermeiden, wenn der Scanner an der Oberfläche bleiben soll, trotz gegenteiliger Behauptung mancher Hersteller oder Marketingabteilungen. 100-prozentige Erkennung und keine falschen Meldungen sind Wunschdenken.

Das andere Extrem sind Scanner, die es dem Benutzer erlauben, die gefundenen Schwachstellen auszunutzen. Für einen Penetrationstest kann das ausgesprochen nützlich sein und die Genauigkeit der Bestandsaufnahme deutlich erhöhen. Auf der anderen Seite steigt das Risiko, dass dadurch der jeweilige Dienst gestört wird, Verzeichnisse da angelegt werden, wo keine sein sollten, oder andere unerwünschte Nebeneffekte auftreten.

In welcher Form der Ergebnisreport ausgegeben wird, ist letzten Endes eher eine Frage des Geschmacks oder bestenfalls noch der Weiterverarbeitung der Daten; in der Regel stehen mehrere Ausgabeformate zur Wahl. Wichtiger ist vielmehr, dass das Programm die gefundenen Schwachstellen gewichtet. Denn daraus kann der

SCHWACHSTELLENSCANNER FÜR UNTERNEHMENSNETZE

Hersteller	Eeye	GFI	Harris	Internet Sec. Systems	Nessus	Safety-Lab	Symantec	Symantec	Saintcorporation	Rapid7
Website	www.eeye.com	www.gfisoftware.de	www.stat.harris.com	www.iss.net	www.nessus.org	www.safety-lab.com	www.symantec.de	www.symantec.de	www.saintcorporation.com	www.rapid7.com
Kontakt	info.eu@eeye.com	info@gfisoftware.de	STAT@harris.com	de-info@iss.net		info.eu@safety-lab.com	069/664 10-300	069/664 10-300	austin@saintcorporation.com	alan@rapid7.com
Produkt	Retina Network Security Scanner 5.0	LANGUARD Network Security Scanner 5.0	STAT Scanner Professional Edition	Internet Scanner 7.0	Nessus[1]	Shadow Security Scanner 7.3	Vulnerability Assessment	NetRecon 3.6	SAINT Scanner 5.6	NeXpose V4
Art des Scanners	Allzweckscanner									
Preis (netto)/ Lizenzmodell	je IP, ab 950 €	je IP, ab 295 €, unlimitiert 895 €	je IP, ab 990 USD für 10 IPs	k. A.	GPL	unlimitiert 465 €[2]	Server-Agent 814 €, Workstations ab 123 €	ab 4091 €	je IP, ab 99 US-$	je IP, ab 9360 US-$ für 64 IPs
Produkt verfügbar als SW für .../ HW-Appliance	Win NT 4.0 SP6a, 2000, XP, 2003/ –	Win 2000, XP/ –	Win 2000 und höher/–	Win 2000, XP/ –	Unix, Linux/ –	Win NT, 2000, XP, 2003/–	Win 2000, Solaris, AIX, Linux, HP-UX/–	Win NT 4.0, 2000, XP/–	Unix, Mac OS X, Linux/✓	Windows, Linux/ –
Benutzerinterface	Win GUI und CLI, Web	Win GUI	Win GUI und CLI	Win GUI und CLI	Unix GUI und CLI, Win GUI	Win GUI	Web	Win GUI und CLI	Web	Web
Zahl der Tests	ca. 2500	k. A.	3418	1411	5787	2694	alle von Bugtraq	alle von Bugtraq	>3000	>2600
2004 zugefügt	k. A.	>100	>600	k. A.	k. A.	1053	alle von Bugtraq	alle von Bugtraq	>700	k. A.
Update-Intervall	ca. 12 × pro Monat n. Bedarf	täglich	4 × pro Monat nach Bedarf	täglich	täglich	täglich	2 × pro Monat nach Bedarf	monatlich nach Bedarf	2 × pro Monat und bei Bedarf	12 × pro Monat
Verteilung	Auto-Update	k. A.	Auto-Update	Auto-Update	Auto-Update	k. A.	Auto-Update	Auto-Update	Auto-Update	Auto-Update
CVE-referenziert	✓	–	✓	✓ (optional)	✓ (teilweise nur BID)	✓	✓	✓	✓	✓
zeitgesteuerte Scans	✓	✓	✓	✓ (mit SiteProtector)	✓ (per Cron)	✓	✓	✓	✓	✓
Vergleich der Scans möglich	✓ (nur mit REM)	✓	✓	✓	✓ (mit Win-Client)	–	✓	–	✓	✓
Schnittstelle zu Vuln.-managem.	✓	–	✓ (Patch-Management)	✓ (SiteProtector)	–	✓	✓	✓	✓	✓
Scanziele	keine Einschränkung	Win. NT, 2000, XP, 2003	keine Einschränkungen	keine Einschränkung	keine Einschränkung	keine Einschränkung	keine Einschränkung	keine Einschränkung	keine Einschränkung	keine Einschränkung
Suche per DNS/ICMP/ARP/ B-casts/andere	✓/✓/–/ –/✓	✓/✓/✓/ ✓/–	–/✓/k. A./k. A./✓	✓/✓/✓/ ✓/–	✓/✓/✓/ ✓/✓	✓/✓/–/ –/–	–/k. A.	–/✓/–/ ✓/–	–/–/–/ –/–	✓/–/–/ –/–
Diensterkennung	✓	✓	✓	k. A.	✓	✓	k. A.	k. A.	✓	✓
OS Erkennung	✓ (eigene, nmap, SMB)	✓	✓	✓ (nutzt nmap-DB)	✓ (eigene, nmap-DB)	✓	✓	✓	✓	✓
Schwachstellen ausnutzen	–	–	–	✓	–	✓	–	✓	k. A.	✓
Schwachstellen hinzufügen	✓	✓	–	–	–	✓	✓	–	✓	✓
Scanner erweiterbar/wie	–/eigene API	✓/eig. Module in VB-Script	–	✓/Datenbank- und Systemscanner	✓, Module in NASL oder C	✓/eig. Module in Delphi, VC++	–	–	–	✓/per XML, geg. Aufpreis
mögliche Reportformate	HTML, Word	XML, MS-SQL	Crystal Reports	HTML, PDF, CSV mit SiteProtector	HTML, XML, Tex, NSR	HTML, XML, PDF, CHM	XML, CSV	Crystal Reports	HTML, XML, PDF, CSV, Plain Text, Simple	XML, CSV, PDF, HTML, Database, TXT
Besonderheiten des Produkts	Non-Intrusiveness, hohe Scan geschwindigkeit	k. A.	Common-Criteria-zertifiziert, CVE-Gründungsmitglied, benötigt Login mit Admin-Rechten, da hauptsächlich lokale Tests	integrierbar in die Management-plattform SiteProtector für Intrusion Detection und Prevention	k. A.	k. A.	Host- und Netzwerkagenten ermöglichen Kontrolle auf lokale Verwundbarkeiten	Verknüpfung von Schwachstellen auf unterschiedlichen Systemen	als Software oder Appliance erhältlich	eingebautes Ticketing-System

✓ trifft zu/vorhanden – trifft nicht zu/nicht vorhanden n. a. = nicht anwendbar k. A. = keine Angabe CLI = Command Line Interface [1] alle Angaben vom Hersteller, außer bei den mit [1] gekennzeichneten Produkten

Systemverantwortliche eine Prioritätenliste zur Behebung der Schwachstellen generieren. Die schweren Probleme als Erstes zu beheben, hilft, die Sicherheit im Ganzen schneller zu erhöhen. Wer dazu neigt, sich von A bis Z durchzuarbeiten und nicht erst die größten Risiken zu beseitigen, riskiert, mit viel Aufwand wenig zu erreichen. Diese Funktion ist in den meisten Produkten enthalten, Foundstone erlaubt hier zusätzlich die Angabe von besonders wichtigen Systemen.

Fazit

Um das eigene Netz auf Schwachstellen zu testen, stehen Systemadministratoren oder Sicherheitsverantwortlichen zahlreiche Werkzeuge zur Verfügung. Je nach zu untersuchendem Servertyp und Relevanz der genannten Eigenschaften lässt sich für jedes System der passende Scanner aussuchen. In der Regel sind von allen Produkten Testversionen verfügbar, die man vor dem Kauf erst einmal in der firmeneigenen Infrastruktur testen kann.

Für einen Angreifer, der Böses im Schilde führt, sind die hier vorgestellten Scanner zu „laut“. Die Signaturen der Scanner werden von allen IDS so-

Foundstone	Qualys	Ncircle	AppSec Inc.	Internet Sec. Systems	Safety-Lab	Kavado	N-Stalker	CIRT.net	Spidynamics	Syhunt
www.mcafee.de	www.qualys.com	www.ncircle.com	www.appsecinc.com	www.iss.net	www.safety-lab.com	www.kavado.com	www.nstalker.com	www.cirt.net	www.spidynamics.com	www.syhunt.com
info_deutschland@mcafee.com	info-de@qualys.com	+1/415/625 5900	info@appsecinc.com	de-info@iss.net	info.eu@safety-lab.com	info@kavado.com	ob@iQ-Dynamix.de	sullo@cirt.net	info@cirosec.de	sales@syhunt.com
FoundStone Enterprise 4.0	QualysGuard	IP360 Vuln. Management System 6.3	AppDetective 4.1	Database Scanner 4.3	ShadowDatabase-Scanner 7.30	ScanDo Web Application Scanner 2.5	N-Stealth[1]	Nikto 1.34	WebInspect Enterprise Edition 4.0[1]	Sandcat Security Scanner 7.1
Appliance			**Datenbankscanner**			**Webscanner**				
k. A.	je IP, ab 13 995 € für 32 IPs pro Jahr; Appliance Leasing 1000 € pro Jahr	je IP, ab 36 250 US-$	pro Datenbank-instanz ca. 900 € im Jahr	k. A.	unlimitiert 465 €[2]	ab 11 000 US-$ pro Scanserver, per Seat und Mengenrabatte erhältlich	je IP, ab 250 US-$, unlimitiert 799 US-$	GPL	je IP, ab 6000 US-$ pro Server	je IP, als Kauf (unlim. 2312 US-$) oder Subscription (unlim. 1360 US-$)
Win 2000/✓	–/✓	–/✓	Win 2000, XP/–	Win NT, 2000, XP/–	Win NT, 2000, XP, 2003/–	Windows/–	Windows/–	alle OS, Perl erforderlich/–	Win NT4, 2000, XP/–	Win/–
Web, Win GUI	Web	Web	Win GUI und Web	Win GUI	Win GUI	Win GUI	Win GUI	CLI	Win GUI	Win GUI
k. A.	3874	1738	>1000	k. A.	234	k. A.	>31 350	3200	k. A.	26 000
k. A.	800	638	k. A.	k. A.	76	k. A.	k. A.	ca. 470	k. A.	2000
nach Bedarf	täglich	2 × pro Monat nach Bedarf	1 × pro Monat	k. A.	täglich	täglich	täglich	täglich	täglich	monatlich bei Bedarf
Auto-Update	Auto-Update	Auto-Update	Auto-Update	k. A.	k. A.	Auto-Update	Auto-Update	Web-Download	Auto-Update	Auto-Update
✓	✓	✓ (1303 von 1738)	✓	k. A.	k. A.	✓	✓	–	✓	✓
✓	✓	✓	✓	–	✓	✓	–	✓ (Cron)	✓	✓ (mit ext. Tools)
✓	✓	✓	✓	✓	–	✓	–	–	✓ inkl. Trendanalyse	–
✓	✓ zum eigenen System	✓	–	–	✓	–	–	–	k. A.	✓
keine Einschränkung	keine Einschränkung	keine Einschränkung	siehe[3]	MS-SQL 7/2000, Oracle 8/9, Sybase 12./12.5	keine Einschränkung	Webserver	Webserver	Webserver	Webserver	Webserver, inkl.Firewalls und Router
✓/✓/–/–/✓	✓/✓/✓/✓/✓	✓/✓/–/–/✓	–/–/–/–/–	–/–/–/–/–	✓/✓/–/–/–	–/–/–/–/–	–/–/–/–/–	–/–/–/–/–	k. A.	–/–/–/–/–
k. A.	✓	✓	n. a.	n. a.	n. a.	n. a.	n. a.	n. a.	n. a.	n. a.
✓	✓	✓	✓	–	✓	–	✓	–	✓	✓
–	–	✓	✓	✓	✓	✓ optional	✓	–	✓	✓
✓	–	✓	✓	–	k. A.	✓	✓	–	✓	✓
✓/Threat Correlation u. a.	✓/per XML in weiterverarb. Systeme	✓ per XML in weiterverarb. Systeme	–	–	✓/mit Delphi und VC++	eigene Module	–	Perl-Quellcode verfügbar	eigene Module	✓/Web Miner u. a.
HTML, XML, PDF, CSV, Crystal Reports	HTML, XML, PDF, MHT	PDF	HTML, HTML Web Archive, XML, PDF, Plain Text, Crystal Reports	k. A.	HTML, XML, PDF, CHM	HTML, XML, PDF, ADTG	HTML	HTML, CSV, Plain Text	HTML, PDF, Plain Text, RTF,	HTML, XML
eingebunden in Ticketing-Systeme SDK für Signaturen wird mitgeliefert	Korrelation mit Snort, integrierbar in Problem- und Patchmanagement, Rollenmodell für Benutzer	erlaubt es, einen Host als Standard festzulegen und gegen diesen zu vergleichen	untersucht Datenbanken auf Anwendungsebene, optional mit Logins für weiterführende Scans		k. A.	k. A.	IDS Evasion eingebaut, hohe Scangeschwindigkeit	findet auch alte Schwachstellen, IDS Evasion, HTTP-Auth Brute Force	sucht nach Fehlern in Webapplikationen, enthält Tools zum manuellen Pen-Test mit	umfassende Analyse des Servers, der Inhalte, der Logfiles und d. Konfiguration

[2] Herstellerpreis in Tabelle weicht von Preisangaben auf Website ab

[3] MySQL, Oracle, Sybase, IBM DB2 Microsoft SQL Server, Oracle Application Server, Lotus Notes/Domino

fort erkannt. Generell führen diese Werkzeuge zu viele Tests durch, um unbemerkt zu bleiben, denn es soll sich ja dem Sicherheitsverantwortlichen ein vollständiges Bild der Lage des Serverraums erschließen. Der Angreifer, der sich dieser Tools bedient, geht ein hohes Risiko ein, erwischt zu werden. Wahrscheinlicher ist daher, dass er sich vor einem Systemeinbruch mit subtileren, weniger auffälligen Methoden Informationen beschafft (siehe Artikel „Hack the Net“, S. 34) – ähnliche Methoden, wie sie auch ein Einbruchstester anwendet, um eine höhere Genauigkeit der Schwachstellenanalyse zu erreichen, als es mit den Scannern möglich wäre.

Für den Systemadministrator ist das Scannen jedoch eine sehr gute Methode, schnell, effektiv und regelmäßig festzustellen, wo Lücken im Netz sind. Allerdings kann ein automatisierter Scan nicht mit der Kreativität eines Menschen mithalten. Einen Einbruchstest ersetzen diese Produkte ebenso wenig, wie sie 100-prozemtige vor einem Einbruch schützen. (ur)

CHRISTOPH PUPPE

ist Security Consultant bei der Hisolutions AG in Berlin, CISSP und seit mehreren Jahren als Penetrationstester tätig.