All-Purpose-Schwachstellen-Scanner im Test

Löchersuche

Christoph Puppe

Wer Einbrechern keine Chance lassen möchte, durchsucht sein Netz regelmäßig nach sicherheitsrelevanten Schwachstellen. Scanner dafür gibt es reichlich – wie viel sie taugen, zeigte ein Test.

Im *iX*-Test standen zehn Soft- sowie Hardware-Schwachstellen-Scanner (Appliances) auf dem Prüfstand, die Firmen NetIQ, Ncircle und Symantec stellten keine Testsoftware zur Verfügung. Alle Produkte mussten sich in einem Testnetz von 19 Systemen mit Betriebssystemen verschiedener Hersteller von 1996 bis heute und unterschiedlichster Hardware bewähren.

Scannt man ein Netz nach Schwachstellen und Sicherheitsproblemen, gewinnt man nicht nur Erkenntnisse über dessen Zustand. Vielmehr benutzt der Systemverantwortliche die anfallenden Daten für darauf aufbauende Anwendungen wie Patch- und Risikomanagement, Problembehandlung et cetera, die somit entscheidend von der Qualität der Ergebnisse beeinflusst werden.

Einige der Produkte enthalten neben dem Scannen gleich weitere Funktionen des Schwachstellenmanagements, etwa das Erfassen des Systembestandes, das Patchmanagement oder das ticketbasierte Problemmanagement. Der Test konzentrierte sich allerdings ausschließlich auf die Hauptfunktion, das Finden und Beschreiben von Verwundbarkeiten.

In erster Linie suchten die Testkandidaten über das Netz nach offenen Ports und den darauf laufenden Diensten. Zusätzlich durften sie sich – sofern sie dazu in der Lage waren – auf einigen Systemen anmelden und lokale Untersuchungen durchführen.

Das Testnetz bestand aus einem Intranet mit 19 Rechnern. 13 davon liefen auf einer Maschine mit 3-GHz-Prozessor und 4 GByte RAM als virtuelle Rechner. Alle wurden mit einem Switch verbunden und über einen Router mit NAT (Network Adress Translation) ans Internet angeschlossen. Sämtliche Softwarescanner wurden jeweils in einer eigenen virtuellen Maschine installiert. Im Nachhinein erwies sich die Testumgebung als nicht ideal, alle Scanner hatten jedoch die selben Voraussetzungen.

Kompatible Daten sind von Vorteil

Die Scan-Ergebnisse sind auch für Intrusion-Prevention- und Intrusion-Detection-Systeme (IPS und IDS) relevant. Zudem sind in größeren Netzen häufig mehrere Scanner im Einsatz, deren Ergebnisse der Administrator vergleichen will. Aus diesen Gründen ist die Auslieferung der Daten in einem standardisierten Format wünschenswert. Leider hat jeder Scanner seine eigenen Formate und benötigt damit eine „Übersetzung“.

Zwei Standardisierungsgremien für XML-Schema bieten hier Lösungen an: OASIS veröffentlichte 2003 die mittlerweile nicht mehr weiterentwickelte „Application Vulnerability Description Language“ (AVDL; www.avdl.org), ein Jahr zuvor bot MITRE mit der „Open Vulnerability and Assessment Language“ (OVAL; oval.mitre.org) ein XML-Schema für die Beschreibung von Schwachstellen, Patches, Erfüllungsvorgaben, Datenerhebung und Ergebnissen an. Die Organisation hat schon den bekanntesten Schwachstellenstandard für die einheitliche Benennung beziehungsweise Nummerierung der bekannten Verwundbarkeiten, die „Common Vulnerabilities and Exposures“ (CVE; cve.mitre.org) definiert.

Ein weiterer Mangel an Kompatibilität betrifft die Gewichtung der Schwachstellen: Jeder Scanner klassifiziert das Risikolevel (hochkritisch, mittel, niedrig) anders als die anderen – was nicht nur die Einschätzung gefundener Schwachstellen erschwert, sondern auch einen Vergleich der Scanner. Mit Vorsicht sollte der Administrator Ergebnisse behandeln, die den

Löwenanteil der gefundenen Schwachstellen ganz oben oder ganz unten in der Gefährdungsskala ansiedeln. Realistisch wären ungefähr 20 Prozent hochkritische, 50 Prozent mittlere und 30 Prozent weniger kritische Schwachstellen.

Der „National Infrastructure Advisory Council" (NIAC) versucht seit kurzem, mit seinem „Common Vulnerability Scoring System" (CVSS; www.first.org/cvss/) standardisierte Maßeinheiten für die Schwere und Dringlichkeit von Schwachstellen zu etablieren.

Jeder Scanner erhielt zwei Chancen, sein Können unter Beweis zu stellen. Der erste Durchgang erfolgte mit den Standard-Einstellungen für einen schnellen Lauf, der alle Tests ausführt, die das Ziel-System nicht beschädigen. Für den zweiten Lauf wurde jeder Scanner manuell mit allen verfügbaren Optionen gestartet. Dazu gehörte ein vollständiger Scan aller Ports. Überdies erhielt der Scanner, soweit möglich, ein Passwort: Aufgrund von Sicherheitsaspekten meldet er sich auf Unix-Systemen als normaler Benutzer an, Windows-Systeme hingegen erfordern einen Administrator-Zugang, um bestimmte Funktionen wie das Auslesen der Registry zu erlauben. Auf den Ergebnissen des zweiten Durchlaufs basieren die vorliegenden Bewertungen.

Die Anzahl der erzeugten Meldungen ist nicht zwangsläufig ein Qualitätsmerkmal für einen guten Scanner. Beispielsweise lieferte die Saintbox vergleichsweise wenige Meldungen, die jedoch viele Probleme und ihre CVE-Nummern enthalten, und schneidet daher bei der Auswertung nach CVE-Nummern recht gut ab.

Zu erwarten war eine Steigerung der Ergebnisse des zweiten gegenüber dem ersten Lauf. Teilweise, weil die Scanner nun mehr Ports überprüften, hauptsächlich aber, da die meisten sich auch auf den Systemen anmelden und damit mehr und genauere Ergebnisse liefern können. Wenn es keine Steigerung gibt, lässt dies daraus schließen, dass kaum lokale Tests durchgeführt wurden. Teils, weil der Scanner dieses Feature nicht unterstützt, teils, weil es nicht funktionierte.

Wahr, falsch und fehlend

Die wichtigste Auswertung der im Test gesammelten Daten ist die Analyse auf Richtigkeit und Vollständigkeit der Meldungen. Das Maß ist die Zahl der gefundenen CVE-Nummern: erstens die wahren, das heißt alle gefundenen Schwachstellen, die tatsächlich Schwachstellen sind, zweitens die falschen, also solche, die fälschlicherweise als Schwachstelle klassifiziert wurden und drittens die fehlenden, nicht erkannten Schwachstellen.

Letztere resultieren aus der Differenz zwischen den vom jeweiligen Scanner und den von allen gefundenen CVE-Nummern. Auf diese Art lässt sich mit vertretbarem Aufwand eine aussagekräftige Annäherung an die Quote der fehlenden Meldungen erhalten.

Kenntnis der CVE-Nummern wünschenswert

Im vorliegenden Test war die Ausgabe der CVE-Nummern ein wichtiges Kriterium für die Beurteilung der Qualität der Scanner. Zwar muss ein Scanner, der das nicht leistet, nicht zwangsläufig Probleme übersehen, es kann sich jedoch nachteilig auswirken. Als Beispiel nehme man eine alte Version eines Webservers, die viele Schwachstellen enthält. Für jede von ihnen existiert eine CVE-Nummer. Dem Administrator genügt es, wenn er lediglich eine Meldung erhält, die ihm sagt, dass die Version veraltet ist und ein Risiko darstellt. Für einen Penetrationstest oder andere Versuche, die Schwere des Risikos genau einzuschätzen, ist es dagegen notwendig, die CVE-Nummer zu kennen.

iX-TRACT

- Ein guter Schwachstellen-Scanner zeichnet sich nicht nur durch eine hohe Quote an gefundenen Schwachstellen aus, ebenso wichtig ist der möglichst geringe Anteil an falsch positiven Meldungen.
- Für die heterogene Unternehmens-IT sollte ein Scanner zufriedenstellende Ergebnisse für alle gängigen Betriebssysteme liefern und sich in eventuell vorhandene Schwachstellenmanagementsysteme einbinden lassen.
- Sinnvoll sind solche Scans zur Steigerung der Sicherheit im Firmennetz allemal – jegliche Angriffe ausschließen kann man mit ihnen allerdings nicht.

Daher schneiden Scanner mit vielen wahren CVE-Meldungen in der Gegenüberstellung besser ab. Nicht vergleichen kann man nach dieser Methode die Scanner, die keine CVE-Nummern verwenden – von den getesteten betraf das lediglich denjenigen von GFI.

Je mehr CVEs ein Scanner meldet, desto höher ist zwar das Risiko, dass Falschmeldungen dabei sind, umso größer ist aber auch die Chance, dass er alle existierenden CVEs liefert. Im Test untersuchte ein Skript die XML-Versionen der Ergebnisberichte auf CVE-Nummern. Insgesamt 1745 unterschiedliche CVE-/Zielsystem-Kombinationen konnte es aus den 4414 von den Scannern berichteten CVEs extrahieren. Jede dieser Kombinationen steht für ein spezifisches Problem auf einem System.

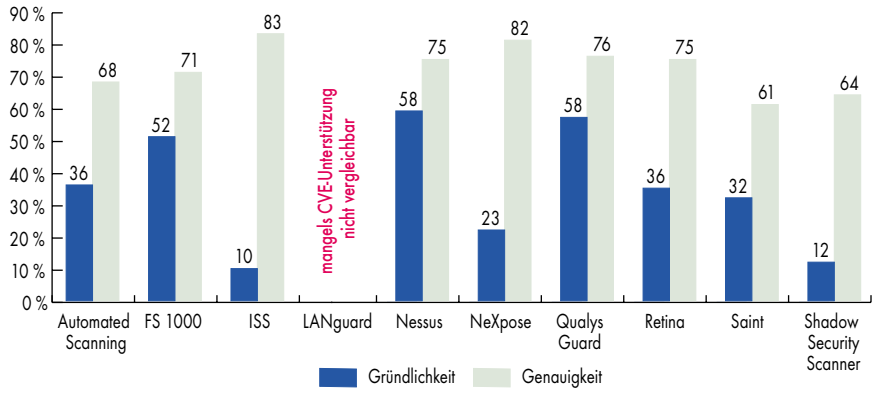
Bei allen Kombinationen musste bewertet werden, ob es sich um einen „echten" Fund oder eine Fehlermeldung handelt. Als Grundlage für die jeweils einzeln getroffenen Entscheidungen diente das Ausprobieren der Exploits, die Recherche in der Verwundbarkeits-Datenbank von Securityfocus.com sowie in den Advisories der Hersteller. Auf diese Weise kristallisierten sich insgesamt 787 richtige und 509 falsche CVEs heraus. 449 ließen sich nicht eindeutig als richtig oder falsch zuordnen. Mit den cirka 1300 verifizierten, sicher bestimmbaren CVE-Nummern ließen sich schließlich die Ergebnisse der einzelnen Scanner vergleichen (s. Abb. 1).

Der dunkelblaue Balken zeigt den prozentualen Anteil der von einem Scanner gefundenen CVE-Nummern an der Gesamtzahl aller wahren CVEs an. Der hellblaue Balken verdeutlicht, wie viel davon wahre Schwachstellen sind. Ein Beispiel: Nessus hat von 787 möglichen 608 CVEs gemeldet, von denen 459 wahr sind. Das entspricht einer Gründlichkeit von 58 Prozent und einer Genauigkeit von 75 Prozent.

Tests oft veraltet

Beide Zahlen sind wichtig und nicht voneinander zu trennen. Ein Scanner ist nur nützlich, wenn er einen hohen Anteil der potenziellen Schwachstellen findet, und die Anzahl der „false positives" möglichst gering ist. Andernfalls werden zu viele Ressourcen für nicht vorhandene Probleme vergeudet.

Die Unstimmigkeiten in den gemeldeten Funden sind bei nahezu allen Scannern gravierend, beispielsweise finden manche eine Verwund-



Gründlichkeit und Genauigkeit in Prozent: „gründlich" steht für den Anteil der durch den jeweiligen Scanner gefundenen CVE-Nummern an der Menge aller richtigen CVEs, „Genauigkeit" steht für die richtigen von den erkannten CVEs. Je höher beide Werte sind, desto besser ist der Scanner (Abb. 1).

barkeit für Linux *rpc.statd* auch auf den BSD-Systemen oder einen NT-4-Exploit auf Windows 2003. Offenbar führen die Scanner selten bis nie eine Plausibilitätskontrolle auf schon bekannte Fakten bei den jeweiligen Systemen durch. Ähnliches gilt für alte Tests, deren Durchführung nach mehreren Jahren kein aussagekräftiges Ergebnis mehr bringt. Aktualisierungen der vorhandenen Tests finden zu selten statt.

Ebenfalls optimieren ließe sich die Funktion, die Resultate von auf einem System durchgeführten Tests auf weitere zu übertragen. Ein Beispiel sind Passwörter: Wenn ein Scanner ein gültiges auf einem System findet, könnte es viel bringen, dieses auch auf anderen Systemen auszuprobieren.

Um die Eignung der Scanner für heterogene IT-Landschaften festzustellen, wurden die Scan-Ergebnisse für die einzelnen Betriebssysteme betrachtet. Kein Scanner fand alle CVE-Nummern auf allen Betriebsystemen. Es zeigte sich außerdem, dass Scanner mit einer hohen Gesamttrefferquote durchaus Schwächen bei einzelnen Betriebssystemen haben. Die Scan-Resultate nach Betriebssystemen untergliedert finden sich in der Tabelle.

Beyond: Automated Scanning Server

Ein erster Scan ist in unter einer Minute gestartet und schnell abgeschlossen. Die Anzeige des Scan-Fortschritts ist detailliert und übersichtlich. Allerdings fand der Schwachstellen-Scanner beim ersten Versuch zwei Systeme nicht.

Der Benutzer kann entscheiden, ob er zuerst einen Vorscan starten möchte, bei dem alle Systeme gesucht werden. Aus diesen kann er die auf Verwundbarkeiten zu testenden auswählen. Bei jedem Scan-Typ und den dazugehörigen Tests lassen sich alle Einstellungen verändern. Außerdem kann der Benutzer einzelne Tests für alle Scans abschalten.

Den nach eigenen Templates erstellten HTML- oder XML-Bericht kann sich der Tester entweder herunterladen oder per E-Mail schicken lassen.

Zwar ist die Liste der gefunden Schwachstellen ziemlich knapp formuliert, sie enthält aber alle wichtigen Informationen und Verweise auf weiterführende Webseiten. Die Empfehlungen zum Beheben des Problems könnten ausführlicher sein – sie sagen nur was zu tun ist, aber nicht wie. Findet der Scanner bei einem Test Details zur Schwachstelle, zeigt er sie mit an.

Ein Nachteil besteht in der begrenzten Zahl der lokalen Tests: Nur auf Windows-Systemen kann sich der Scanner anmelden.

Foundstone: FS1000

Von einer Konsole aus kann man beliebig viele Scanner verwalten. Die Startseite zeigt die gefundenen Probleme nach gewünschtem Kriterium sortiert – etwa nach Systemen oder Risikolevel – in chronologischer Reihenfolge der durchgeführten Scans an. Beim Arbeiten über die HTML-Oberfläche lädt der FS 1000 für fast alle Seiten Applets, was die Prozesse erheblich beschleunigt.

Der Scanner enthält eine Verwaltung der Ziel-Systeme, bei der der Administrator jedes einer Gruppe zuordnen und unterschiedliche Kritikalitätswerte für Gruppen oder Systeme eingeben kann. Darüber hinaus gibt es eine umfangreiche Benutzerverwaltung, die für jeden Benutzer eine Rolle mit Rechten und Pflichten vorsieht.

Jedes gefundene Problem wird im Problemmanagement als Ticket angelegt, wobei es auch möglich ist, diese Tickets in bereits vorhandene Systeme zu exportieren. Wenn Foundstone die Tickets selbst verarbeitet, kann man mit einem Klick den Test wiederholen, um die Problembehebung zu kontrollieren. Diese Funktionen wurden nicht ausführlich getestet, hinterlassen aber einen guten ersten Eindruck.

Eine Besonderheit ist das Threat-Management. Dabei kann der FS 1000 bis zu sechs Verwundbarkeiten in einer grafischen Auswertung zusammenfassen und ihre zeitliche Entwicklung pro Gruppe oder pro Betriebsystem verfolgen.

Die Zahl der Parameter für Scan-Typen ist enorm, aber pro Seite in einen Schieberegler zusammengefasst. Benutzernamen und Passworte für Windows lassen sich angeben. Während des Scans gibt es nur eine Prozentanzeige für den gesamten Vorgang. Die Last auf den Zielsystemen war höher als bei anderen Scannern. Beim ersten Versuch fand der Scanner mehrere Systeme nicht, was sich beim zweiten Durchlauf teilweise wiederholte.

Die Reports liefert er als gepackte Archive aus. Der Offline-HTML-Bericht ist der einzige bei den Testkandidaten, in dem sich gut navigieren lässt. Neben Links zu weiterführenden Webseiten enthalten die Empfehlungen oft Schritt-für-Schritt-Anleitungen. Selbst die Ports werden erklärt und mit Tipps für die Konfiguration versehen.

ISS: Internet Scanner

ISS ist der Erfinder des Verwundbarkeitsscans. Die Oberfläche des Scanners erscheint aufgeräumt und funktional, eine Benutzerführung durch Reiter oder eine automatisch startende Update-Funktion gibt es nicht.

Um einen Scan zu beginnen, muss man eine neue Session anlegen und für sie einen Scan-Typ (hier Policy genannt) auswählen. Einen „Alles bis auf DoS"-Scan-Typ, der bei allen anderen

vorhanden ist und im ersten Testdurchgang als Standard diente, sucht man vergeblich. Mit dem Policy Editor kann man eigene Typen erstellen und sich alle Tests nach jedem gewünschten Feld in Gruppen zusammengefasst anzeigen lassen. Für den Test wurde „L5 Max with Fusion“ ausgewählt, diese Policy klang am ehesten nach einer vollständigen Liste aller Tests ohne die DoS-Angriffe. Die kryptischen Bezeichnungen der verschiedenen Scan-Typen erleichtern die Auswahl nicht gerade.

Noch während der Scan läuft, sind die Ergebnisse sukzessive verfügbar. Eines der Ziel-Systeme wurde zwar entdeckt, aber als nicht erreichbar markiert, daher existieren dafür keine Ergebnisse. Nach dem zügig abgeschlossenen Scan bietet ISS die wohl umfangreichste Auswahl an Berichten des gesamten Testfeldes an. Allerdings sind sie für den menschlichen Betrachter nicht unbedingt vorteilhaft formatiert. Bei Port 13 (Zeichengenerator) etwa mehrere Kilobyte Zeichen anzuzeigen ist unschön und verbessert den Gesamteindruck nicht. Die einfache Statistik, wie viele Probleme pro Rechner der Scanner gefunden hat, versteckt sich in einem eigenen Bericht.

Das ISS-Produkt ist der einzige Scanner im Test, der die Zusammenfassung für das Management auf Deutsch erstellt. Die Berichte für die Techniker sind bei diesem Produkt wie bei allen anderen auf Englisch. Wer sich an das Berichtsformat gewöhnt hat, findet dort ausgezeichnete Beschreibungen der Probleme und oft auch Schritt-für-Schritt-Anleitungen zu ihrer Behebung.

GFI: LANguard

Es gibt nur wenige Optionen für die größtenteils sinnvollen Scan-Typen. Der Tester kann eigene Typen anlegen und die Dateien mit den vordefinierten Werten für Passwörter, Benutzernamen sowie Portnummern in einem integrierten Dateieditor bearbeiten. Eine Besonderheit ist der Script-Editor mit Debugger, der es erlaubt, die mitgelieferten Tests zu bearbeiten und neue zu erstellen.

Ebenfalls ungewöhnlich, aber praktisch sind die mitgelieferten Tools. Mit ihnen lassen sich Updates und Software auf den Systemen installieren: eine Maske zur DNS-Abfrage, *traceroute*, *whois*, SNMP-Walk/-Audit, ein Werkzeug zum Erstellen von Benutzerlisten und eins zum Auditieren von SQL-Servern. Der Benutzer benötigt neben dem LANguard keine weitere Software, um zahlreiche Aufgaben bei der Administration von Windows-Netzen zu erledigen.

Nach dem recht flotten Scan ruft das Werkzeug einen der „Scan Filter“ auf, der die Ergebnisse als Bericht darstellt. Eigene Filter, das heißt Berichtsvorlagen, kann man sich aus den vorgegebenen Elementen zusammenstellen.

Die Berichte schließen beim LANguard installierte Updates und Hotfixe ein. Wer zwei Scans miteinander vergleichen möchte, benötigt dafür die XML-Exporte. Leider sind die Berichte recht unübersichtlich und enthalten überdies keine CVE-Nummern. Ein qualitativer Vergleich mit den anderen Testkandidaten war daher nicht möglich.

Nessus

Der einzige Open-Source-Kandidat wartet mit einigen Besonderheiten auf. So ist er der Einzige, der unter Unix läuft und auf einer Client-Server-Architektur mit eigenem Client beruht. Für Windows gibt es seit mehreren Jahren den NessusWX-Client, der noch ein paar neue Features mitbringt. Er speichert etwa alle Ergebnisse sowie Einstellungen der Scans in einer Datenbank und kann auch die Ergebnisse von zwei Scans miteinander vergleichen. Außerdem ermöglicht er den Export in PDF und HTML sowie den Import der nessuseigenen Formate NSR und NBE. Mit NessusWX kann der Tester falsch positive Ergebnisse markieren, damit sie im Bericht nicht auftauchen.

Neuerdings muss der Benutzer die Installation registrieren, damit er Updates herunterladen kann. Eine integrierte Benutzerverwaltung erlaubt es dem Administrator, festzulegen, wer welche IP-Nummern scannen darf. Den Unix-Client kann man von der Kommandozeile oder via GUI unter X starten.

Nessus nutzt optional mehrere andere Open-Source-Programme, die als Plug-ins eingebunden sind: Portscans führt *nmap* durch, das Ausprobieren von Passwörtern übernimmt Hydra und die Webserver-Tests stammen von Whisker. Ein Debugger für die Tests wird mitgeliefert.

Der Benutzer kann viele Parameter variieren. Als einziger Scanner bietet Nessus die Möglichkeit, riskante Scans auf zwei Arten zu entschärfen: Zum einen kann man bei einigen Tests die Option „Save Checks“ wählen, zum anderen lassen sich alle gefährlichen Tests abschalten. Beide Varianten, die für diesen Test auch gewählt wurden, reduzieren allerdings Zahl und Genauigkeit der Ergebnisse.

Leider ist es nur über Umwege möglich, einen neuen Scan-Typ zu erstellen. Vor Ende eines Durchgangs liefert Nessus keine Ergebnisse. Nach den eher langsamen Scans öffnet sich ein neues Fenster, in dem die Ergebnisse übersichtlich dargestellt sind. Es gibt nur zwei Berichtstypen. Die Beschreibungen der Probleme sind manchmal etwas kurz und die Empfehlungen enthalten wenig konkrete Anleitungen. Sofern verfügbar, finden sich in den Resultaten Verweise auf weiterführende Webseiten.

Weitere auf Nessus basierende Produkte und Add-ons vertreibt das von Nessus-Erfinder Renaud Deraison gegründete Unternehmen Tenable Networks Security.

Rapid7: NeXpose

NeXpose erwies sich als eines der beiden „Problemkinder“ im Test. Zunächst startet der Benutzer in einem Kommandozeilenfenster einen Server, der per HTTPS erreichbar ist. Dieser enthält eine Konsole für wichtige Befehle wie Updates starten, Lizenz-Key anfordern oder Logfiles an den Support schicken. Leider wollte das Pro-

Glossar

Problem: Ein Problem kann mehrere Verwundbarkeiten enthalten, ein Beispiel wäre etwa eine alte Version eines Server-Dienstes, bei dem man im Laufe der Jahre zahlreiche Schwachstellen entdeckt. Jede Schwachstelle wurde mit einer CVE-Nummer versehen. Einem Problem können also viele CVE-Nummern zugeordnet sein.

Schwachstelle: Eine Schwachstelle ist eine Sicherheitslücke in einem System. Findet jemand eine Möglichkeit, eine solche auszunutzen, spricht man von einem **Exploit**.

Verwundbarkeit: gleichbedeutend mit Schwachstelle

dukt solange kein Ziel-System scannen, bis eine der beiden Netzwerkkarten, die die VMware mit dem Testnetz beziehungsweise dem Fileserver verbanden, deaktiviert wurde. Danach funktionierte das Scannen einwandfrei und recht flott. Beim Ausgeben der Berichte gab es jedoch erneut Schwierigkeiten. Es kam zu einer Endlosschleife, nicht aber zu fertigem HTML. Mit zahlreichen Mails an den schnell und kompetent reagierenden Support ließen sich die Probleme teilweise beheben.

Der Administrator muss die Systeme in Gruppen (Sites) einteilen. Für diese Gruppen legt er fest, welcher Scanner sie überprüfen soll und ob die gefunden Schwachstellen mehr oder weniger kritisch bewertet werden sollen.

Jedes Ereignis, zum Beispiel der Start eines Scans oder der Fund eines Problems, kann als Alert per Mail, SNMP oder Syslog versendet werden. Damit ist das Produkt einfach in Verwaltungsstrukturen wie ein Problemmanagement einzubinden.

Ein eigenes Problemmanagement mit vollständiger Benutzerverwaltung auf der Basis von Rollen und Rechten ist im Lieferumfang enthalten. Der Nachteil ist allerdings, dass man die Tickets manuell eröffnen muss. Die Scan-Typen sind nur pro Gruppe veränderbar. Neue einzugeben oder starke Veränderungen an einem vorzunehmen gelang nicht. Man kann einer Vielzahl von Anwendungen Benutzer und Passwörter zuteilen, in diesem Punkt bot das Produkt mehr als die anderen. Da es beim zweiten Durchlauf nicht signifikant mehr Meldungen gab als beim ersten, funktioniert die Testerweiterung entweder nicht oder es sind keine Tests vorhanden, die die Benutzerdaten verwenden.

Während des Scans erhält der Benutzer lediglich über die Konsole Informationen über den Verlauf. Die Berichte sind nüchtern, übersichtlich formatiert und enthalten gute Beschreibungen der Probleme. Die Empfehlungen enthalten teilweise Schritt-für-Schritt-Anleitungen. Dass in den Berichten teils IP-Adressen, teils Rechner-Namen auftauchen, sorgt für unnötige Unübersichtlichkeit.

Qualys: Qualys Guard

Nach Eingabe der Benutzerkennung am Display der Appliance meldet sich der Qualys Guard bei seiner Zentrale in den USA und ist danach einsatzbereit. Qualys bot früher nur den Service, Scans über das Internet ausführen zu lassen. Diese Entwicklungsgeschichte ist wohl auch der Grund für das ungewöhnliche Konzept, dass die Appliance kein eigenes GUI hat, sondern über den Umweg des Herstellerportals angesprochen wird. Firmen, die keine Verbindungen aus ihrem Netz nach außen erlauben, können dieses Gerät nicht einsetzen, denn die Appliance muss sich via HTTPS mit der Zentrale verbinden können. Die Daten der Scans speichert Qualys verschlüsselt in seinen Datenbanken. Dieser Vorgang ist nach Angaben des Herstellers auditiert und genüge höchsten Sicherheitsansprüchen. Gegen Aufpreis kann die Datenhaltung auch innerhalb des eigenen Netzes erfolgen.

Die Startseite des Portals gibt einen ausgezeichneten Überblick über den Stand vergangener Scans und deren Ergebnisse. Über das Portal lassen sich externe Scans und beliebig viele Appliances verwalten. Als Ziel kann man auch Domains angeben, die das Scansystem per Zone Transfer abfragt. Ein erster Scan bindet alle gefundenen Geräte in eine Karte ein, die ein Applet grafisch darstellt. Warum die Karte das Testnetz fälschlicherweise in zwei Teilen anzeigt, ist nicht nachvollziehbar.

Hat der Scanner die Systeme entdeckt und erfasst, kann der Administrator sie in Gruppen zusammenfassen und einzelnen Systemen oder Gruppen je nach ihrer Relevanz und damit Gefährdung in der Firmenarchitektur Multiplikatoren geben. Wenn Qualys Guard eine Verwundbarkeit auf einem solchen System findet, multipliziert er deren Risikostufe mit dem Multiplikator. Bei niedriger Gefährdung kann der Multiplikator auch eine negative Zahl sein. Auf diese Weise soll eine realistische Einschätzung der Gefährdung erreicht werden.

Jedes gefundene Problem lässt sich optional als Ticket in das integrierte Problemmanagement übernehmen. Es ist möglich, diese Daten über eine XML-Schnittstelle in ein eigenes Ticketing-System zu übernehmen. Diese Funktionen wurden keinem gründlichen Test unterzogen, hinterließen aber einen guten ersten Eindruck.

Auch bei diesem Produkt lassen sich neue Scan-Typen konfigurieren, wenngleich die Zahl der Optionen für den Scan nicht so groß ist. Für weitergehende Tests kann man SSH-Keys oder Benutzernamen für Unix und Windows eintragen. Die Beschreibungen in den Berichten sind umfangreich und ausführlich, bieten aber keine Schritt-für-Schritt-Anleitungen zur Behebung. Qualys ist sehr rührig, wenn es um neue Standards geht. CVE wird unterstützt, das Produkt ist OVAL-konform und der Hersteller hat bei der RSA 2005 CVSS-Unterstützung angekündigt.

eEye: Retina Scanner

Der Retina-Scanner startet mit der Erkennung der Systeme. Er zeigt sie sofort in einer Tabelle an und unter dem nächsten Reiter „Audit“ tauchen sie als Zielsysteme auf. In dieser Tabelle werden die Ergebnisse schon während des Scans eingetragen, sodass der Administrator sie ohne Zeitverlust einsehen an.

Nur wenige Optionen stehen zur Verfügung. Es kann je Scan ein Benutzer-Passwort mitgegeben werden. In diesem Test war es das des Windows-Administrators. Vier Scan-Typen sind vordefiniert. Neue Typen anzulegen ist einfach, in den Tests kann man nach Kategorien filtern und nach allen Feldern suchen. Der erste Scan ist schnell abgeschlossen. Nun kann der Administrator die gefundenen Probleme mit Kommentaren versehen und vom Report ausnehmen. Diese Option, die in der Praxis nur dann hilfreich ist, wenn man die Ergebnisse manuell kontrollieren kann, bieten nur dieses Produkt sowie der Nessus-WX-Client. Irritierend ist, dass die Broadcast-Adresse des Netzbereiches als IP-Nummer mit aufgeführt ist.

Die Ergebnisse finden sich unter dem Reiter „Remediation“. Ein IE-Fenster zeigt den entsprechenden Report, den man sich herunterladen kann. Die Darstellung der Probleme enthält alle notwendigen Informationen, gibt Verweise auf weiterführende Informationen und enthält knapp gehaltene Empfehlungen. Unter „Report“ erhält man einen Bericht, der mit teilweise überflüssigen Grafiken und Statistiken überladenen ist. Negativ fällt die ausgesprochen begrenzte Exportfunktion der Berichte auf.

Ein enthaltener Enterprise Manager kann mehrere Retina-Scanner über eine Oberfläche verwalten, mehrere Scans zentral starten sowie Tickets er-

zeugen und weiterbearbeiten. Diese Software war nicht Teil des Tests.

Saintcorporation: Saintbox

Saint liefert eine Appliance mit Linux aus, eine Software-Version ist ebenfalls erhältlich. Man kann einstellen, von welchen IP-Nummern aus das Gerät erreichbar sein soll.

Die Benutzeroberfläche ist übersichtlich. Eine kleine, aber sinnvolle Auswahl von Scan-Typen inklusive SANS-Top-20-Schwachstellen (www.sans.org) steht zur Verfügung. Es lassen sich nur wenige Parameter für die Scans einstellen, einzelne Tests kann man ausschließen. Ein Benutzerpasswort für Windows kann man festlegen, leider keines für Unix.

Das Logfile des Scans ist sehr detailliert, wodurch die Übersichtlichkeit leidet. Die Ergebnisse werden entweder direkt angezeigt, oder durch den Saintwriter in einen Bericht zusammengefasst. Eine Besonderheit ist der Vertrauensbericht: In ihm analysiert Saint, welcher der getesteten Computer welchen anderen vertraut. Das kann DNS, NFS oder andere Protokolle betreffen. So steht zum Beispiel der DNS-Server in diesem Bericht ganz weit oben, da alle Systeme diesen Rechner nutzen. Schwachstellen in solchen Systemen, denen viele Rechner vertrauen, haben folglich mehr Auswirkungen.

Die Beschreibungen der Probleme sind ausführlich und enthalten Links zu weiterführenden Seiten. Die Empfehlungen sind detailliert und klar formuliert. Es werden auch IAVA (Information Assurance Vulnerability Alert)-Nummern der amerikanischen Regierung ausgegeben. Das Produkt ist CVE-zertifiziert.

Safety-Lab: Shadow Security Scanner

Das zweite Problemkind im Test: Der Scanner von Safety-Lab war nicht dazu zu bringen, einen vollständigen Scan aller Ziel-Systeme durchzuführen. Dies führte beinahe zum Ausschluss aus dem Test. Der Hersteller stellte zügig eine neue Version zur Verfügung, mit der das Durchführen der Scans möglich war.

Als Besonderheit bietet der Scanner zwei Entwicklungsumgebungen für eigene Tests. Eine arbeitet als Script-Editor mit Debugger. Die zweite funktioniert mit einem Assistenten, der den Benutzer in sechs Schritten durch alle für den neuen Test notwendigen Felder führt. So kann man URLs, Registry-Keys oder andere Parameter eingeben, auf deren Existenz oder deren Wert der Scanner testen soll. Es ist nur möglich, Benutzer für Windows anzugeben und dies auch nur über den Umweg der Eingabe des Passwortes in eine vom Benutzer zu erstellende Datei.

Vor dem Start eines neuen Scans erfragt ein Assistent alle notwendigen Daten. Wählt man den Typ „Quick-Scan“, ist der Scanner schnell fertig. Der Scan-Typ „Full“, der alle Ports scannt, war auch nach 20 Stunden noch nicht abgeschlossen und musste

All-Purpose-Schwachstellen-Scanner im Vergleich

Produkt	Name	Automated Scanning	FS 1000	Internet Scanner	LANguard
	Version	2.15.80	4.0	7.2	6.0
Angaben	Hersteller	Beyond Security	Foundstone	Internet Security Systems	GFI Software
	Website	www.arrow-marketing.de	www.foundstone.com	www.iss.net	www.gfisoftware.de
	Art/OS	Appliance/Linux	Appliance/Windows	Software/Windows	Software/Windows
	Preis	3000 $[7] plus Appliance (12 000 $)	7306 € + IP-Lizenz	k. A.	850 € [5]
	Zahl der Tests	3019	2150	1427	k. A.
Features	verteilte Scanner/zentrales Management/ zeitgesteuerte Scans	✓/✓ [1]/✓	✓/✓/✓	✓[1]/✓[1]/✓[1]	–/–/✓
	Oberfläche	Web (HTTPS)	Web (HTTPS)	Windows	Windows
	lokale Tests Unix/Windows	–/✓	–/✓	–/–	–/✓
	Asset Gruppen/Tickets	–/–	✓/✓	✓/✓	–/–
Berichtsformate	DOC/HTML/XML/PDF/CHM [2]/MHT [3]	–/✓/✓/✓/–/–/–	–/✓/✓/✓/–/–/–	✓/✓/✓/✓/✓/✓/✓	–/✓/✓/–/–/–/–
Meldungen gesamt	1. Lauf/2. Lauf	599/621	332/672	265/344	152/269
Klassifikationen	hoch/mittel/niedrig	17 %/22 %/61 %	27 %/20 %/53 %	11 %/21 %/68 %	47 %/13 %/39 %
CVE	wahr/falsch/übersehen	284/126/503	407/168/380	77/16/710	n. a.
	% gründlich/% genau	36 %/69 %	52 %/71 %	10 %/83 %	n. a./n. a.
pro Betriebssystem	gesamt wahr/falsch				
AIX	31/38	21/5	23/7	5/0	n. a.
Cisco SIP Phone	3/4	0/0	1/0	0/0	n. a.
FreeBSD	56/55	30/17	37/25	14/2	n. a.
IOS	44/35	13/2	24/6	7/0	n. a.
Irix	23/9	3/1	3/1	6/1	n. a.
Linux	234/151	112/35	124/52	19/5	n. a.
Mac OS X	29/28	10/7	11/8	1/0	n. a.
Novel Netware	30/55	21/23	22/23	1/0	n. a.
Solaris	45/43	32/19	37/20	10/6	n. a.
Windows	301/101	42/17	125/26	14/2	n. a.
iX-Wertung		⊕ eigene Scans ⊕ übersichtliche Bedienung ⊕ versendet Berichte per E-Mail ⊕ markieren von False-Positives ⊖ lokale Tests nicht umfangreich ⊖ wenig Vergleiche	⊕ verwaltet viele Scan Engines ⊕ praktisches Ticket-System ⊕ detaillierte Empfehlungen ⊕ Vergleiche über die Zeit ⊖ einige Fehler bei der Betriebssystemerkennung	⊕ wenig CVEs, aber die meisten Probleme gefunden ⊕ viele Reports ⊕ ausgezeichnete Empfehlungen ⊖ umständliche Bedienung ⊖ ein Rechner nicht gefunden	⊕ Berichte inkl. Hotfixes ⊕ sinnvolle Vergleiche ⊕ praktische zusätzliche Tools ⊖ unübersichtliche Berichte ⊖ keine CVE-Nummern

✓ trifft zu/vorhanden – trifft nicht zu/nicht vorhanden k. A. keine Angabe n. a. nicht anwendbar

[1] Zusatzsoftware erforderlich [2] Compiled HTML Module [3] Message HTML [4] nessuseigenes Berichtsformat [5] unbegrenzte Ziele [6] kostenlos für private Anwender

beendet werden. Deswegen ist der zweite Lauf ebenfalls ein „Quick-Scan“, allerdings mit manuell aktivierten zusätzlichen Ports und dem Administrator-Login.

Die Beschreibungen der Probleme sind kurz, die Empfehlungen, wie sie zu beheben sind, noch kürzer. Wenigstens einen Link zum Hersteller könnte man angeben, wenn dort schon nur steht „Updaten Sie diesen Service“. Zumindest werden die Ergebnisse der Tests mit angezeigt. Teilweise finden sich in den Ergebnissen Verweise auf weiterführende Seiten, dies ist aber eher die Ausnahme.

Fazit

Zwar sind die Trefferquoten der Scanner beim Finden von Schwachstellen für den Einsatz im Firmennetz wichtig, die Wahl eines Produktes sollte aber nicht ausschließlich davon abhängen. Für die ständige Überwachung eines Netzwerks etwa sollte der Scanner darin fest installiert werden können. Alle Produkte mit zwei Ausnahmen bieten das, zwei benötigen dafür allerdings eine zusätzliche Software des Herstellers (siehe Tabelle „verteilte Scanner“). Von Vorteil für die regelmäßige Überwachung ist ebenso die Möglichkeit, zeitgesteuerte Scans durchzuführen, was alle Produkte anbieten.

Wer in einem großen Netzwerk den Überblick behalten möchte, benötigt ein Werkzeug, dass sich gut in die betrieblichen Abläufe einfügt. Dafür ist es erforderlich, dass alle Probleme als Tickets in vorhandene Lösungen exportiert werden können. Dies bieten einige Produkte, alle inklusive einer eigenen Verwaltung der Tickets. Unverzichtbar ist ebenso das Remote-Management über eine zentrale Konsole, die in der Lage ist, alle Scanner im Netz zu steuern. Nicht notwendig, aber sinnvoll ist es, die überprüften Systeme in Gruppen einzuteilen und die Ergebnisse in Abhängigkeit zu den Zugehörigkeiten zu diesen Gruppen unterschiedlich zu bewerten und zu melden.

Fast schon eine Selbstverständlichkeit ist der Hinweis, dass selbst nach einem oder mehreren Scans und der Behebung aller gefundenen Probleme ein Netz nicht zwangsläufig sicher sein muss und Angriffe nicht ausgeschlossen werden können. Denn kein Scanner findet alle Schwachstellen, auch sind nicht alle Verwundbarkeiten, die es gibt, bekannt, und schließlich sollte man die Kreativität eines menschlichen Angreifers nie unterschätzen. Dennoch lohnt der Einsatz dieser Programme, denn eine schnelle Erhebung und Beseitigung der Schwachstellen steigert die Sicherheit im Netzwerk signifikant. Und den Angreifern ihre Sache erschweren kann man mit solchen Mitteln allemal. (ur)

CHRISTOPH PUPPE

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

Nessus	**NeXpose**	**Qualys Guard**	**Retina Network Security Scanner**	**Saintbox**	**Shadow Security Scanner**
2.2.3	4.0.8	2.8.35	5.1.2	5.6.8	7.41
Nessus*	Rapid7	Qualys	eEye Digital Security	Saintcorporation	Safety-Lab
www.nessus.org**	www.rapid7.com	www.qualys.com	www.eeye.com	www.saintcorporation.com	www.safety-lab.com
Unix/Windows	Software/Windows	Appliance/k. A.	Software/Windows	Appliance/Linux	Software/Windows
1200 $/Jahr [5, 6]	180 000 € [5]	ab 2995 € pro Jahr	6520 $[7]	2634 $ [7]	1699 $ [7]
7867	> 2600	4207	ca. 2500	1297	294
✓/–/✓	✓/✓/✓	✓/✓/✓	✓[1]/✓[1]/✓	✓/–/✓	–/–/✓
Windows/Unix	Web (HTTPS)	Web (HTTPS)	Windows	Web (HTTPS)	Windows
✓/✓	✓/✓	✓/✓	✓/✓	–/✓	–/✓
–/–	✓/✓	✓/✓	✓/✓	–/–	–/–
–/✓/✓/✓/–/–/ Tex/NBE [4]	–/✓/–/–/–/✓	✓/✓/✓/✓/–/✓	✓/✓/–/–/–/–	–/✓/✓/✓/–/– / CSV	–/✓/✓/✓/✓/–
986/1176	358/403	1136/1448	330/686	153/231	452/446
27 %/28 %/46 %	15 %/66 %/19 %	18 %/34 %/48 %	38 %/43 %/20 %	16 %/14 %/69 %	55 %/38 %/7 %
459/149/328	178/39/609	455/143/332	281/92/506	252/160/535	98/56/689
58 %/75 %	23 %/82 %	58 %/76 %	36 %/75 %	32 %/61 %	12 %/64 %
23/19	3/1	17/8	11/4	14/6	0/11
1/1	0/0	1/3	1/0	1/0	0/0
35/17	7/8	17/6	16/12	12/10	4/9
13/2	17/1	18/20	17/10	4/6	0/1
4/2	1/1	15/4	2/2	4/1	0/0
145/21	79/17	99/32	80/34	102/60	31/19
6/1	14/1	13/4	7/2	21/18	0/0
6/23	13/2	22/10	14/13	15/17	0/10
33/17	10/0	33/17	14/8	22/14	6/1
193/46	34/8	220/39	119/7	57/28	57/5
⊕ Client und Server ⊕ bindet andere Programme ein ⊕ sehr gute lokale Tests ⊖ schlechte Empfehlungen ⊖ kein Speichern von Scan-Typen	⊕ umfangreiches Ticketing ⊕ Logins für viele Dienste möglich ⊕ detaillierte Empfehlungen ⊖ Probleme bei den Berichten ⊖ Probleme beim Scannen	⊕ verwaltet viele Scan Engines ⊕ Vergleiche über die Zeit ⊕ große Berichtsauswahl ⊕ eingebautes Ticketsystem ⊖ benötigt Verbindung zur Zentrale in den USA	⊕ gute lokale Tests ⊕ schöne Reports ⊖ unübersichtliche Berichte ⊖ Broadcast-Adresse taucht im Bericht auf	⊕ Vertrauensbericht hilfreich ⊕ sinnvolle Vergleiche ⊕ viele Ergebnisse bei seltenen Systemen ⊕ zusammengefasste Meldungen zu Problemen ⊖ wenig Parameter für eigene Scans	⊕ mehrere Editoren für eigene Tests ⊕ übersichtlich ⊖ viele Funde als hoch eingestuft ⊖ sehr knappe Empfehlungen ⊖ Probleme beim Scannen

[7] Class C pro Jahr

* Nessus Add-ons bei Tenable Network Security

** bzw. www.tenablesecurity.com