Sicherheitslücken gezielt auf der Spur

Workshop Sicherheitslücken und Schwachstellen von IT-Infrastrukturen lassen sich mit dem Werkzeug Nessus überprüfen. Der Autor zeigt das Vorgehen Schritt für Schritt auf und schlägt Gegenmassnahmen vor.

Christoph Baumgartner*

Es existieren verschiedene Vorgehensmodelle für die Durchführung von IT Verwundbarkeitstests. Eine bekannte Methode wird im «Open Source Security Testing Methodology Manual» (OSSTMM) des Institute for Security and Open Methodologies (ISECOM) erläutert. Dieses umfangreiche und kostenlose Werk besteht aus diversen Checklisten, Formularen und Empfehlungen, welche bei der Durchführung eines IT Verwundbarkeitstests mit Untersuchungsobjekt DMZ (De-Militarisierte-Zone, dieser Ausdruck wird für den Bereich hinter der Firewall, aber nicht im LAN benutzt. In der DMZ stehen beispielsweise die Web-, Mail- und DNS-Server) sehr hilfreich sein können.

Rechtlicher Exkurs

Dieser Artikel ist nicht als Ermunterung zum Hacken gedacht. Er soll lediglich zeigen, dass Unberechtigte selbst ohne Spezialwissen mittels leistungsfähigen und im Internet frei verfügbaren Tools, an sensitive Informationen kommen und per Knopfdruck grossen Schaden anrichten können. Hacking oder Cracking ist in der Schweiz eine Straftat, falls man für diese Aktivität nicht die ausdrückliche Genehmigung des Eigentümers und des Betreibers des zu untersuchenden Systems hat. Es ist also nicht empfehlenswert, den Webserver einer bekannten Firma ohne deren ausdrückliche Genehmigung zu «testen».

Protokolle und Dienste

Die meisten Sicherheits-Tools nutzen Netzwerkprotokolle. TCP/IP (Transmission Control Protocol/Internet Protocol) ist die am weitesten verbreitete Sammlung von Kommunikationsprotokollen, welche es unterschiedlichen Systemen ermöglicht, miteinander zu interagieren. Die Adressierung der Systeme besteht aus vier Zahlenblöcken, welche mit Punkten separiert werden (z.B. 195.129.94.193). Damit die Systeme miteinander kommunizieren können, muss die Adressierung (im LAN, WAN und Internet) eineindeutig sein. Vergleichbar ist dies mit den Hausnummern einer Strasse in einer Ortschaft in einem Land. TCP/IP besteht aus verschiedenen Protokollen, welche unterschiedliche Merkmale besitzen. TCP ist ein verbindungorientiertes Protokoll, welches den Transport von Daten zwischen Systemen ermöglicht. Vor dem eigentlichen Datenaustausch wird eine Verbindung ausgehandelt. Danach findet der Datenaustausch kontrolliert statt. Das heisst, falls der Empfang eines Paketes vom Empfänger nicht bestätigt wurde, wird es vom Sender erneut übermittelt. Diese Methode minimiert die Netzwerkbelastung. UDP (User Datagram Protocol) ist im Gegensatz zu TCP ein verbindungsloses Protokoll. Der Sender verschickt die Pakete auf gut Glück.

Die Funktionalitäten in Netzwerken basieren auf TCP/IP und werden Dienste genannt. Damit pro Adresse verschiedene Dienste unterschieden werden können, wurden jeweils 65 535 Ports auf TCP und UDP definiert, was in etwa mit den verschiedenen Wohnungen in einem Mehrfamilienhaus verglichen werden kann. Manche Dienste sind auf vordefinierten Ports zu finden, andere können den Ports frei zugewiesen werden. Zu den bekanntesten Diensten gehören HTTP (Darstellung und Anzeigen von Webseiten) und SMTP (E-Mail). Aus Benutzersicht weniger bekannte Dienste stellen die Kommunikation im Netzwerk und zwischen (unterschiedlichen) Programmen sicher.

Beispiele dafür sind FTP (Austausch von Dateien) oder Telnet (Fernsteuerung von Systemen). Da sich Menschen IP-Adressen nur schwer merken können, wurden Systemnamen eingeführt (z. B. webserver.oneconsult.com). Der Dienst DNS stellt die Zuordnung vom eindeutigen Systemnamen und der zugehörigen IP-Adresse sicher. Manchmal überschneiden sich die Dienste bezüglich ihrer Funktionalität, was einerseits ein gewisses Gefahrenpotenzial birgt, andererseits aber auch Möglichkeiten zur Erhöhung des Sicherheitsniveaus bietet.

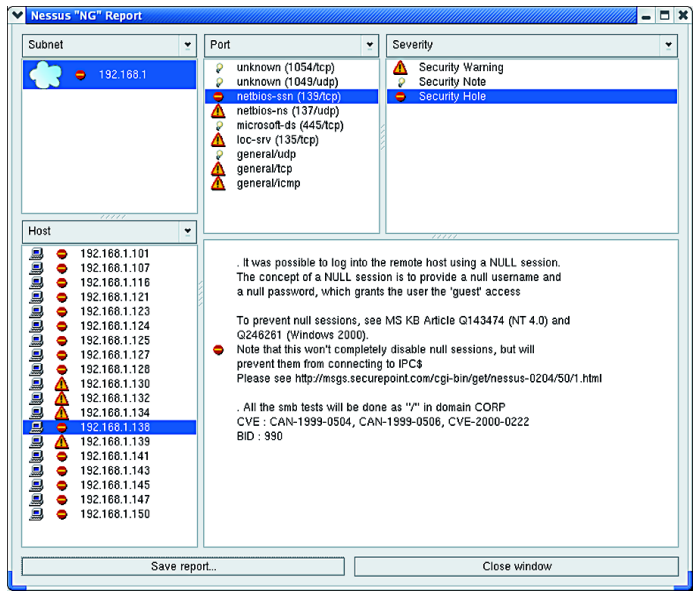
Firewall

Die primäre Aufgabe jeder Firewall ist der Schutz von Systemen vor unberechtigtem Zugriff und/oder unberechtigter Manipulation. Aus diesem Grund kontrollieren die Firewalls den Netzwerkverkehr, welcher ins LAN oder die DMZ hinein und aus dem LAN beziehungsweise der DMZ heraus geht. Die Überprüfung erfolgt anhand so genannter Regeln. Leistungsfähige Firewalls führen eine «Schwarze Liste» von IP-Adressen, welche durch übermässig viele aufgebaute Netzwerkverbindungen oder ungewöhnliches Verhalten (z. B. Paketfragmentierung oder Protokollanomalien) auffallen. Beides sind typische Merkmale eines (schlecht ausgeführten) Hacker/Cracker-Angriffs. Alle Verbindungen, welche von Systemen aufgebaut werden, deren IP-Adressen auf der «Schwarzen Liste» stehen, blockt die Firewall ab oder lässt sie ins Leere laufen. Aus praktischen Gründen wird der IP-Adresseintrag meistens nach 15 bis 30 Minuten aus der «Schwarzen Liste» gelöscht.

Scanner und Nessus

Ein Security-Scanner untersucht ein Netzwerk mitsamt all seiner Komponenten, Protokolle, Dienste, Betriebssysteme, Applikationen usw. auf Sicherheitslücken. Damit kann eruiert werden, ob das Netzwerk ausreichend vor Unberechtigten geschützt ist. Nessus ist ein nach dem Client-Server-Prinzip aufgebauter Security-Scanner. Die Serverkomponente (läuft auf Unix/Linux-Systemen) führt die eigentlichen Tests durch, während die Clientkomponente (läuft auf Unix/Linux- oder Microsoft Windows-Systemen) zur Steuerung der Serverkomponente und der Erstellung der Testreports dient. Nessus ist ein Opensource-Tool und beinhaltet drei Elemente: Security-Scanner, Testscripts (in Form von Plugins programmiert) und sichere Scriptsprache zur Programmierung von Testscripts.

Nessus wurde 1998 von Renaud Deraison entwickelt und wird seither von ihm und einigen Helfern konsequent weiter entwickelt. Wann immer eine neue Verwundbarkeit (Exploit) bekannt wird, dauert es oft nur wenige Tage, bis das entsprechende Testskript, welches die Verwundbarkeit aufspürt und geeignete Gegenmassnahmen vorschlägt, als Plugin zum Download bereit steht. Die Aktualisierung der Plugin-Datenbank lässt sich automatisieren. Da die Software im Quellcode vorliegt, kann die genaue Funktionalität überprüft werden. Die Summe dieser Vorteile und die Präzision in der Erkennung von Verwundbarkeiten hat massgeblich zur weltweiten Verbreitung von Nessus beigetragen. Nessus steht den kommerziellen Security-Scannern lediglich in der optischen Aufmachung der zum Schluss generierten Reports nach.



Nessus kommentiert Sicherheitslücken und schlägt Gegenmassnahmen vor. Bild: Autor

Vorbereitende Schritte

Als erstes wird das Untersuchungsobjekt (Zielsystem) definiert. Weil wir im Beispiel die DMZ untersuchen wollen, benötigen wir die externen (vom Internet her sichtbaren) IP-Adressen aller in der DMZ stehenden Systeme (z. B. Web-, Mail- und DNS-Server). Während des IT Verwundbarkeitstests kann es zu Performance-Einbussen im Netzwerk und im Extremfall zu Systemausfällen kommen. Deshalb sollten sämtliche involvierten Stellen über die geplante Durchführung des Verwundbarkeitstests informiert und Backups der Daten erstellt werden. Falls die Verfügbarkeit der IT Infrastruktur nicht gefährdet werden darf, sollte an einem anderen Zielsystem geübt werden.

Bevor mit dem Verwundbarkeitstest begonnen werden kann, muss das Testsystem aufgesetzt werden. Dazu reicht ein Linux/Unix-basierter Computer aus mit Pentium-III-Prozessor, mindestens 128 MByte RAM und Netzwerkanschluss. Damit die grafische Version von Nessus eingesetzt werden kann, muss KDE oder Gnome installiert sein. Des Weiteren wird Nmap (gehört zum Lieferumfang vieler Linux-Distributionen) und Nessus benötigt. Zusätzlich sollte ein Sniffer (z. B. ethereal oder tcpdump) installiert werden. Eine deutschsprachige Installations- und Schnellanleitung für Nmap und Nessus steht unter http://www.oneconsult.com/downloads/downloads.html zum Download bereit. Die Server- und die Clientkomponente von Nessus sollte auf dem gleichen Computer installiert werden. Für den Test benötigt man direkten, ungefilterten Zugriff auf das Internet, das heisst, es darf keine Firewall zwischen dem Testsystem und dem Internet stehen.

Konfiguration von Nessus

Nessus und Nmap sind nun auf dem Testsystem installiert. Falls ein Sniffer installiert wurde, kann dieser jetzt gestartet werden, um den von und zu dem Testsystem generierten Netzwerkverkehr anzuzeigen. Als erstes wird die Plugin-Datenbank von Nessus aktualisiert. Dazu öffnet man eine Konsole und gibt den Befehl «nessus-update-plugins» ein. Daraufhin nimmt Nessus Verbindung zur Website www.nessus.org auf und aktualisiert die Plugin-Datenbank (was der allenfalls laufende Sniffer am Monitor anzeigt). Als nächstes startet man die Serverkomponente von Nessus. Zu diesem Zweck wird in der Konsole der Befehl «nessusd -D» eingegeben. Das System ist jetzt einige Sekunden beschäftigt. Sobald die Eingabeaufforderung erscheint, wird die Clientkomponente mit der Eingabe «nessus» gestartet.

Nun erscheint das Setup-Fenster von Nessus mit diversen Registern. Im Register «Nessusd host» gibt man unter Login den Usernamen und das Passwort ein, welches bei der Installation von Nessus definiert wurde. Anschliessend klickt man auf «Log in». Wenn die Eingaben korrekt sind, erscheint eine Meldung, dass die gefährlichen Plugins deaktiviert sind. Die Grundeinstellungen von Nessus sind schon sehr gut für diese Zwecke geeignet, da die «gefährlichen Plugins» (Tests, welche Systeme zum Stillstand bringen oder deren Konfiguration beeinträchtigen können) deaktiviert sind.

Definition der Register

Zur Sicherheit drückt man erneut auf «Enable all but dangerous plugins», damit Nessus keine Denial-of-Service (DoS)-Attacken ausführt. Ausserdem setzt man noch den Haken vor «Enable dependencies at runtime».

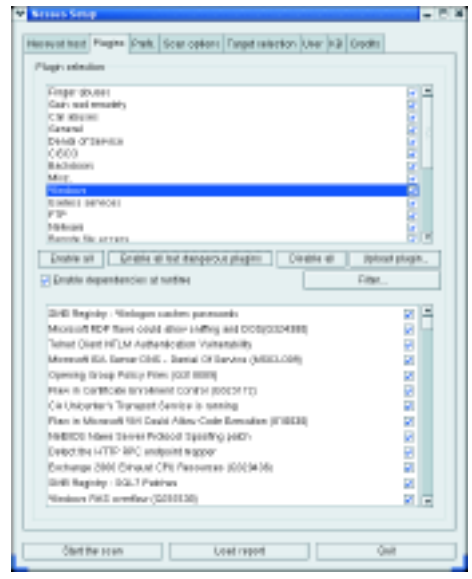
Nun wechselt man zum Register «Prefs.». Da man schlafende Hunde nicht wecken soll, werden die simulierten Hackerangriff der Firewall nicht lautstark angekündigt. Aus diesem Grund setzt man ausschliesslich die Häkchen «SYN Scan» und «Identify the remote OS» im Abschnitt «Nmap». Bei «Port range» wird «User specified range» gewählt. Der Rest bleibt unverändert.

Jetzt kann zum Register «Scan options» gewechselt werden. Hinter «Port range» schreibt man folgende Zeile «20-25,53,67,69,79,80,88,109-119,123,135-139,143,161,162,389,443,445,465,513-515,563,593,636,993,995,1080,1433,1434,1443,2049,2512,2513,2598,2897». Bei «Number of hosts to test at the same time» wird «5» eingegeben und «Number of checks to perform at the same time» erhält den Wert «2». Dies garantiert selbst bei einer langsamen Internetanbindung verlässliche Resultate. Ausserdem sollten die Optionen «Optimize the test» und «Safe checks» aktiviert werden. Im Fenster «Port Scanner» wählt man ausschliesslich «Nmap» und «SYN Scan».

Nun kann zum Register «Target selection» gewechselt werden. Unter «Target(s)» gibt man die IP-Adressen der Systeme in der DMZ ohne die IP-Adresse der Firewall ein. Besonders interessant sind erfahrungsgemäss der Webserver und der Mailserver. Der Rest kann unverändert bleiben. Somit sollte die Firewall während des Tests keine Probleme bereiten und keines der Systeme zum Stillstand gebracht werden. Eine Garantie dafür gibt es allerdings nie.

Test und Testreport

Nun kann der Test mit dem Button «Start the scan» gestartet werden. In der Folge verschwindet das Setup-Fenster und es erscheint ein Fenster, in dem für jede IP-Adresse des Untersuchungsobjekts zwei Balken angezeigt werden, in welchen der Fortschritt der Tests grafisch dargestellt wird. Die Testdauer ist jeweils von verschiedenen Kriterien abhängig: Anzahl der zu testenden Komponenten und Ports, Art der Portscans, Leistung des Testsystems, Leitungskapazität, Anzahl detektierter Dienste usw. Der Test sollte innert 15 bis 30 Minuten abgeschlossen sein. Umfangreiche und sehr gründliche IT-Verwundbarkeitstests können aber durchaus mehrere Tage dauern.



Der Security-Scanner Nessus stellt über 1000 Plugins zur Verfügung. Bild:Autor

Sobald die Tests abgeschlossen sind, erscheint ein neues Fenster, in welchem die Resultate dargestellt werden. Eine Wolke symbolisiert ein Netzwerk, das Zeichen «verbotene Fahrtrichtung» signalisiert Sicherheitslöcher, ein Warndreieck steht für Sicherheitswarnungen und die Glühbirne symbolisiert eine Sicherheitsinformation. Dieser Report kann mit «Save report...» in andere Dateiformate exportiert werden. Besonders empfehlenswert ist dabei die Option «HTML with pies and graphs». Damit wird ein Report generiert, welcher mittels Browser betrachtet werden kann. Im Report werden Gegenmassnahmen in Form von Sofortmassnahmen (Konfigurationsänderungen oder Updates) zur Schliessung der erkannten Sicherheitslücken aufgezeigt. Als Faustregel bezüglich des Handlungsbedarfs beziehungsweise der Priorisierung gilt: Sicherheitslöcher und Sicherheitslücken der Kategorie «Kritisch/ Hoch» sind sofort zu schliessen. Sicherheitswarnungen und Sicherheitslücken der Kategorie «Ernsthaft/Mittel» sind so bald wie möglich zu schliessen. Sicherheitsinformationen und Sicherheitslücken der Kategorie «Niedrig» müssen nicht zwingend geschlossen werden. Aus sicherheitstechnischer Sicht sollte dennoch über deren Schliessung nachgedacht werden. Sofern die Sofortmassnahmen umgesetzt werden, wird ein höheres Sicherheitsniveau erreicht.

Wer die Firewall überprüfen will, kann diese selbst als Ziel eingeben. Dazu wird im Register «Scan options» hinter «Port range» das Wort «default» eingetippt. So kann festgestellt werden, ob man bei der Firewall auf die «Schwarze Liste» kommt.

Fazit

Möglicherweise hat dieser Artikel dazu beigetragen, Sicherheitslücken aufzuspüren und sie zu schliessen bevor ein Unberechtigter sie ausnutzt. Die Vielzahl der Kombinationsmöglichkeiten bei der Konfiguration von Nessus lässt die Komplexität von IT-Verwundbarkeitstests erkennen. Obwohl Nessus ein ausgezeichneter Security-Scanner ist, ist es nur eins von vielen Sicherheitstools, die in den Werkzeugkoffer eines jeden Security-Testers gehören. Aus diesem Grund sollten IT-Verwundbarkeitstests immer von Leuten durchgeführt werden, welche die Bereiche Netzwerk und Security fachlich beherrschen. Wie bei allen Aspekten des IT-Riskmanagement gilt auch hier die Regel: Es reicht nicht, Massnahmen umzusetzen, wenn deren Wirksamkeit nicht ab und zu überprüft wird.

Info/http://www.cdcit.ch
http://www.oneconsult.com
http://www.osstmm.org
http://www.insecure.org/nmap/nmap_download.html
http://www.nessus.org/nessus_2_0.html
http://www.oneconsult.com/downloads/downloads.html

*Christoph Baumgartner ist Head of IT Consulting bei der CDC IT AG und Geschäftsführer der OneConsult GmbH. Er ist seit 1996 im IT Consulting mit den Schwerpunkten IT Risk Management und IT Strategie tätig.