

Security-Audits im Risk Management Process

Detlef Weidenhammer

Whitepaper

Juli 2002

Die Verantwortung für die Bereitstellung einer sicheren IT-Umgebung ist längst nicht mehr allein der IT-Leitung zuzuordnen, neue gesetzliche Vorschriften wie KonTraG (Gesetz zur Kontrolle und Transparenz im Unternehmensbereich) zwingen auch die Geschäftsleitung eines Unternehmens verstärkt, sich dieser Problematik anzunehmen. Sicherheitsüberprüfungen, sog. Security-Audits, gehören dabei zum unverzichtbaren Bestandteil eines umfassenden Security-Managements und liefern für den KonTraG "Risk Management Process" die benötigten Informationen zur Risikoidentifikation. Einige der hierfür verwendeten Techniken werden in diesem Whitepaper dargestellt.

„Der Vorstand hat geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden“ (§ 91 II AktG)

Das KonTraG verpflichtet damit Vorstände von Aktiengesellschaften und nach aktueller Rechtsauffassung auch Geschäftsführer von GmbHs im Rahmen ihrer Sorgfaltspflichten alle erforderlichen Vorkehrungen zur Verhinderung von Vermögensschäden zu treffen. Damit verbunden ist nicht nur die ordnungsgemäße Einrichtung der Unternehmensorganisation, sondern auch der Aufbau eines Überwachungssystems, damit den Fortbestand des Unternehmens gefährdende Entwicklungen frühzeitig erkannt werden können. Obwohl nicht explizit im Gesetz erwähnt, ergibt sich daraus eindeutig die Verpflichtung auch geeignete Maßnahmen zum Schutz der IT-Umgebung aufzusetzen.



Abbildung 1: Regelkreislauf im Risk-Management-Prozess

Zur Einführung und Umsetzung des "Risk Management Process" wird ein Regelkreislauf mit insgesamt 4 Phasen definiert: Die Phase-1 "Strategisches Risk Management" umfasst die Festlegung der Unternehmensziele für die IT-Sicherheit durch Verabschiedung einer entsprechenden Security Policy. Die Phase-2 "Risikoidentifikation" und die Phase-3 "Risikobewertung" umfassen die Sicherheitsüberprüfung einer IT-Umgebung. Die Phase-4 "Risikosteuerung und -kontrolle" schließlich beinhaltet die Konzeption und Umsetzung von Maßnahmen zum sicheren Betrieb. Nachstehend wird genauer auf die in der Phase-2 verwendeten Techniken zur Sicherheitsüberprüfung eingegangen.

Notwendigkeit von Sicherheitsüberprüfungen

Auch bei den besten Sicherheitsmaßnahmen ist niemals von einer völligen Sicherheit auszugehen. Fehler in der Administration oder in der verwendeten System- oder Anwendungssoftware können ebenso die Sicherheit bedrohen wie neue, bisher noch wenig bekannte Angriffsstrategien. Die Bedrohungen kommen dabei sowohl aus internen, aber zunehmend auch aus externen Bereichen wie dem Internet. Hier haben sich in den letzten drei Jahren die (wahr genommenen) Sicherheitsprobleme erschreckend gehäuft. Meldete das CERT/CC in 1999 noch 9.859 Vorfälle (incidents), so waren es in 2001 bereits 52.658. Auch die gemeldeten Schwachstellen (vulnerabilities) stiegen von 417 (1999) auf 2.437 (2001). (siehe http://www.cert.org/stats/cert_stats.html). Eine unlängst vom Security Service Provider Riptech vorgelegte Studie über Angriffe aus dem Internet auf die von ihnen betreuten Kundennetze zeigt ähnliche Tendenzen wie die Zahlen des CERT. Nach Auswertung von 5.5 Milliarden Logeinträgen (Firewalls, IDS) aus den letzten beiden Quartalen 2001 konnten 128.678 Attacken identifiziert werden. Wesentliche Ergebnisse waren:

- Starkes Ansteigen der Angriffe innerhalb der ausgewerteten 6 Monate (um 79%)
- Starkes Ansteigen von Wurm-basierten Attacken (Nimda, Code Red usw.)
- 43% der Unternehmen verzeichneten so gravierende Angriffe, dass eine sofortige Reaktion notwendig war
- 39% der Angriffe waren gezielt gerichtet, hierbei vorwiegend auf Unternehmen aus den Branchen Hochtechnologie, Finanzdienstleistungen, Unterhaltungsmedien und Energieversorger. Dies bedeutet aber auch, dass 61% wahllos innerhalb von globalen Aktionen das Ziel von Angriffen wurden, es kann sich also niemand in Sicherheit wiegen.
- siehe auch <http://www.riptide.com/pdfs/Security Threat Report.pdf>

Wegen dieser ständig zunehmenden Bedrohungen ist die Überprüfung der Sicherheit aller eingesetzten IT-Systeme von besonderer Bedeutung. Um fortlaufend eine sichere Umgebung zu gewährleisten, sind Maßnahmen auf unterschiedlichen Ebenen notwendig.

- Review zur Analyse und Bewertung von Sicherheitspolitik, Sicherheitskonzepten und allen eingesetzten technischen und organisatorischen Sicherheitsmaßnahmen
- Revision zur Überprüfung der korrekten Umsetzung von vorgegebener Sicherheitspolitik und Sicherheitskonzepten
- Schwachstellenanalyse in Form von Einbruchs- und Störversuchen durch Scan- und Penetration-Tests

Da es zumeist nicht sinnvoll ist, die eigenen Administratoren mit der Durchführung von Überprüfungsmaßnahmen zu betrauen (Gefahr der Betriebsblindheit, fehlende Fachkenntnis), empfiehlt sich der Einsatz externer Fachleute. Ebenfalls nicht trivial ist die Auswertung der erzielten Ergebnisse. Insbesondere Security-Scanner liefern häufig Fehlinterpretationen („false positives“), die bei unsachgemäßer Prüfung zu unnötigen und aufwendigen Reaktionen führen können.

Sicherheits-Review der IT-Umgebung

Vor dem Einsatz von überprüfenden Security-Tools sollte immer ein Sicherheits-Review erfolgen. Nur durch diese Form der Analyse lässt sich ein umfassender Überblick auch über Schwachstellen gewinnen, die nicht toolgestützt zu ermitteln sind. Dies betrifft z.B. fast alle Formen der Sicherheitsorganisation und die Umsetzung von Maßnahmen, die bei Scan- und Penetration-Tests nicht untersucht werden.

Im Rahmen des Review wird zusammen mit den hierfür benannten Mitarbeitern des Unternehmens die vorhandene IT-Umgebung analysiert. Dies kann durch Workshops, Interviews und/oder durch Fragebögen realisiert werden. Soweit möglich wird auch auf vorhandene Unterlagen wie Security Policies und Fachkonzepte zurückgegriffen. Die Dokumentationen aller Sicherheitskomponenten, insbesondere die Netzpläne, werden bewertet, die gegenwärtigen und die geplanten Kommunikationsbeziehungen werden einer Risiko-Analyse unterzogen und die Auswirkungen auf Administratoren und Benutzer untersucht.

Ergebnis des Sicherheits-Reviews sind eine abschließende Bewertung der IT-Umgebung und die Empfehlung von Maßnahmen zur Verbesserung des Sicherheitsniveaus. Die nachfolgend dargestellten Scan- und Penetration-Tests sollten immer begleitend durchgeführt werden, da sie wertvolle zusätzliche Erkenntnisse über vorhandene Schwachstellen liefern.

Revision - Prüfung der Sicherheitsorganisation

Die Revision sollte in Form einer Systemprüfung durchgeführt werden, bei der die korrekte Umsetzung der vorhandenen Sicherheitspolitik und Sicherheitskonzeption im Vordergrund steht. Eine generelle Einzelfallprüfung, bei der jede konkrete Dienstenutzung nachvollzogen wird, ist hier nicht sinnvoll. Jedoch sollte stichprobenartig untersucht werden, ob die Sicherheitsvorkehrungen ausreichend sind.

Der erste Teil der Systemprüfung umfasst die **Vollständigkeit und Aktualität** der schriftlich fixierten Ordnung als Teil der Gesamtdokumentation. In dieser Ordnung muss festgelegt sein, welche Art der Dienstenutzung für welche Personen erlaubt ist oder nicht. Neben der Security Policy als Basisdokument muss die Systemdokumentation auch Regelungen darüber enthalten, wie die Systemverwalter den sicheren Betrieb gewährleisten. Das Ergebnis des ersten Teils der Systemprüfung ist eine Aussage zur Aktualität und Angemessenheit der Security Policy und der Betriebsdokumentation.

Der zweite Teil der Systemprüfung besteht aus der Untersuchung der **korrekten Einhaltung** der Security Policy und der Vorgaben der Betriebsdokumentation. Die Sicherheitskomponenten werden dahingehend geprüft, dass ihre Konfiguration mit der Dokumentation im Einklang ist. Diese Konfigurationsprüfung betrifft die Basiskonfiguration sowie die Konfiguration der speziell angebotenen Dienste wie Proxies, Filter oder auch dem Schlüsselmanagement.

Im dritten Teil der Systemprüfung wird die **Wirksamkeit im Betrieb** untersucht. Anhand von Tests und der Sichtung von Protokolldaten wird stichprobenartig untersucht, ob die Sicherheitskomponenten entsprechend den Vorgaben korrekt arbeiten. Darüber hinaus werden alle weiteren Maßnahmen zur Sicherheitsadministration geprüft. Dazu gehört z.B. die regelmäßige Auswertung von Protokolldaten, die Auswertung von Alarmen und evtl. auch das Accounting.

Die Systemprüfung wird (wenn vorhanden) von der internen Revision übernommen, kann sich aber auch externer Fachleute bedienen.

Schwachstellenanalyse mit Scan- und Penetration-Tests

Auch die besten technischen Sicherheitsmaßnahmen können nie von statischer Natur sein. Neu hinzukommende Anwendungen müssen genauso beachtet werden wie die korrekte Einhaltung der Security-Policy („security health check“). Hierzu sind in regelmäßigen Abständen (und zusätzlich bei besonderem Anlass) technische Überprüfungen der Qualität der eingesetzten Schutzmaßnahmen vorzunehmen.

Zum Einsatz hierfür kommen üblicherweise Scan- und Penetration-Tests, die aber jeweils recht unterschiedliche Zielsetzungen haben:

Scan-Tests verfolgen einen breit angelegten Ansatz und versuchen durch umfangreiche Überprüfung der vorgegebenen Zielsysteme eine möglichst detaillierte Schwachstellenanalyse vorzunehmen. Die gefundenen Risiken werden zumeist klassifiziert, zumindest in die Kategorien gering-mittel-hoch, um den Verantwortlichen Prioritäten bei der nachfolgenden Bereinigung zu liefern. Risiken mit der Einstufung "hoch" sollten demnach sofort beseitigt werden, bei den anderen Schwachstellen kann je nach Einschätzung vielleicht sogar bis zum nächsten Update gewartet werden.

Der Einsatz von automatisierten Security-Scannern, die in Form einer Toolbox alle bekannten Schwachstellen „kennen“ und einem Test unterziehen, ist hierzu unabdingbar. Es ist jeweils darauf zu achten, dass nicht nur altbekannte, sondern auch neue Sicherheitsbedrohungen berücksichtigt werden. Die Security-Scanner müssen also ständig aktuell gehalten werden, es gilt damit ähnliches wie für Virenscanner.

Als Startpunkt für das Aufkommen von Security-Scannern kann das Jahr 1994 mit der Freigabe und Verbreitung von SATAN (Security Administration Tool for Analyzing Networks) gelten. Damit stand erstmals ein System zur zentral veranlassten umfassenden Prüfung vernetzter Systeme zur Verfügung. Gute Report-Möglichkeiten verbunden mit Hinweisen zur Behebung der gefundenen Schwachstellen helfen dem Administrator bei der Überprüfung seines Sicherheitsstandes. Kommerzielle Systeme wie z.B. der Internet-Scanner von ISS (Internet Security Systems) kamen bald danach auf den Markt.

Momentan befinden wir uns im Übergang zu einer neuen Generation von Security-Scannern. Diese zeichnen sich neben verbesserten Reports und Informations-Datenbanken vor allem durch die Kombination von Sicherheitstests aus. Idee dabei ist, das Verhalten von Eindringlingen nachzuahmen, deren Vorgehen zumeist durch das kombinierte Ausnutzen mehrerer Schwachstellen gekennzeichnet ist. Die ebenfalls neue Fähigkeit durch „Auto-Reaktion“ gefundene Probleme automatisch beseitigen zu lassen ist jedoch noch vorsichtig und nur in eindeutig geklärten Fällen (z.B. File-Protections) einzusetzen

Penetration-Tests haben anders als Scan-Tests nicht das primäre Ziel einen möglichst umfassenden Überblick zu Schwachstellen zu liefern, sondern sollen aufzeigen, wie tief ein Angreifer in vermeintlich geschützte Systembereiche eindringen kann. Im Gegensatz zum Scan-Test ist dabei das Vorgehen mehrstufig, d.h. es werden zwar ebenfalls Schwachstellen ermittelt, diese dann aber direkt ausgenutzt, um Systemzugang zu erhalten. Ist dieser Zugang nur mit wenigen Privilegien ausgestattet, wird die nächste Aktion das Erlangen von weiteren Privilegien sein bis man seine Zielsetzung erreicht hat.

Vorgehen bei einem BlackBox-Test

Nachfolgend wird der typische Ablauf der Sicherheitsüberprüfung bei einem sog. BlackBox-Tests gezeigt, wobei eine Kombination von Scan- und Penetration-Tests eingesetzt wird. Es soll die Angreifbarkeit eines Unternehmens demonstriert werden, wobei nur minimale Informationen zur Verfügung gestellt werden. Im Gegensatz zu einem WhiteBox-Test, bei dem die Ziele genau benannt werden, muss der BlackBox-Test allein mit der Benennung des zu untersuchenden Unternehmens auskommen. Dies simuliert genau den Fall des anonymen Angreifers, der nicht mehr Basisinformationen besitzt. Das weitere Vorgehen lässt sich dann in insgesamt vier Phasen von der reinen Informationsbeschaffung bis hin zur finalen Penetration gliedern.

Phase-1: InfoSeek

Die erste Phase dient der reinen Informationsbeschaffung unter Nutzung öffentlich zugänglicher Quellen. Mit dem Namen des Unternehmens können z.B. über Search-Engines (www.google.com) und den (wenn vorhandenen) Webserver des Unternehmens erste Informationen gesammelt werden. Besonders interessant sind Hinweise auf Unternehmensstrukturen, die sich z.B. aus Geschäftsberichten ergeben. Zur Ermittlung von Domain-Namen, IP-Adressbereichen und Public-Servern steht eine Vielzahl von weiteren Recherchemöglichkeiten zur Verfügung. Hierzu gehören öffentliche Server wie die RIPE-Datenbank (www.ripe.net), IP Index (www.ipindex.net) oder auch Tools wie nslookup, dig, whois, finger usw. Nette Hinweise liefert auch www.netcraft.com, wer selber sammelt schon wie dieser Server Statistiken über die Uptime seines eigenen Webserver? Interessant aber sind z.B. die verwendeten Webserver und Betriebssysteme.

Sites with longest running systems at Internet connection of the Federal Republic of Germany						
Internet connection of the Federal Republic of Germany The departments will offer public information. Bonn						
Note: Uptime - the time since last reboot is explained in the FAQ					Generated on 20-Feb-2002 15:10:39	
Rank	Site	Average	Max	Latest	OS	Server
1	bund.de	170	174	174	Solaris 8	Apache/1.3.20 (Unix) ServletExecAS/3.1
2	www.bund.de	133	183	176	Solaris 8	Apache/1.3.20 (Unix) ServletExecAS/3.1
3	www.bva.bund.de	81	250	120	Linux	Apache/1.3.12 (Unix) PHP/4.0.2
4	www.bsi.bund.de	44	70	70	Solaris 8	Apache/1.3.12 (Unix)
5	www.bsi.de	30	68	69	Solaris 8	Apache/1.3.12 (Unix)
6	www.bundesarchiv.de	5	10	11	Linux	Apache/1.3.20 (Unix) PHP/4.0.6
7	www.bvvg.de	-	-	-	NT4/Windows 98	Lotus-Domino/5.0.9

Abbildung 2: Beispiel: Infos von Netcraft über Webserver des Bundes

```
domain: bund.de
descr: Bundesministerium des Innern
descr: Informationstechnik in der Bundesverwaltung (KBSt)
descr: Graurheindorferstr. 198
descr: 53117 Bonn
descr: Germany
nserver: nserver.bund.de 194.95.179.193
nserver: nuernberg.bund.de 194.95.179.196
nserver: deneb.dfn.de
status: connect
changed: lastchange@denic.de 20011022
source: DENIC

[admin-c][tech-c][zone-c]
Type: PERSON
Name: Egon Troles
Address: Bundesministerium des Innern
Address: Graurheindorferstr. 198
City: Bonn
Pcode: 53117
Country: DE
Phone: +49 1888 681 3394
Fax: +49 1888 681 53394
Email: troles@kbst.bund400.de
Email: egon.troles@bmi.bund.de
Changed: lastchange@denic.de 20011022
Source: DENIC

[tech-c][zone-c]
Type: PERSON
Name: Jens Claessens
Address: Telekom
Address: CC IVBB
Address: Bonner Talweg 100
City: Bonn
Pcode: 53113
Country: DE
Phone: +49 1888 9900 99
Fax: +49 1888 9900 98
Email: uhd@bund400.de
Changed: lastchange@denic.de 20011022
Source: DENIC
```

Abbildung 3: Beispiel: Öffentlich zugängliche Informationen in der Ripe Whois Database

Nach diesen Recherchen sind die dem Unternehmen zuzurechnenden IP-Adressbereiche bestimmt, DNS-, Mail- und Webserver bekannt und zumeist auch noch die Namen (Adressen, Telefonnummern) der administrativen und technischen Ansprechpartner im Unternehmen.

Beim InfoSeek werden keinerlei invasive Methoden verwendet, so dass die Aktivitäten dieser Phase für das zu überprüfende Unternehmen nicht bemerkbar sind.

Phase-2: ConnectScan

Die Ergebnisse der ersten Phase liefern den Input für den sog. ConnectScan, bei dem die zuvor ermittelten IP-Adressbereiche auf wirklich erreichbare Zielsysteme untersucht werden. Üblicherweise sind die IP-Ranges nur dünn belegt, so dass man zumeist nur mit einer geringen Zahl solcher Systeme rechnen kann. Häufig werden auch bestimmte Tastversuche wie Ping-Sweeps unterbunden, so dass auch andere Techniken wie TCP SYN Scans auf ausgewählte IP-Dienste oder Banner-Tests zum Einsatz kommen.

Beim ConnectScan werden einfache Tastversuche unternommen, die einem aufmerksamen Administrator nicht verborgen bleiben sollten. Es werden in dieser Phase aber noch keine Sicherheitsuntersuchungen durchgeführt.

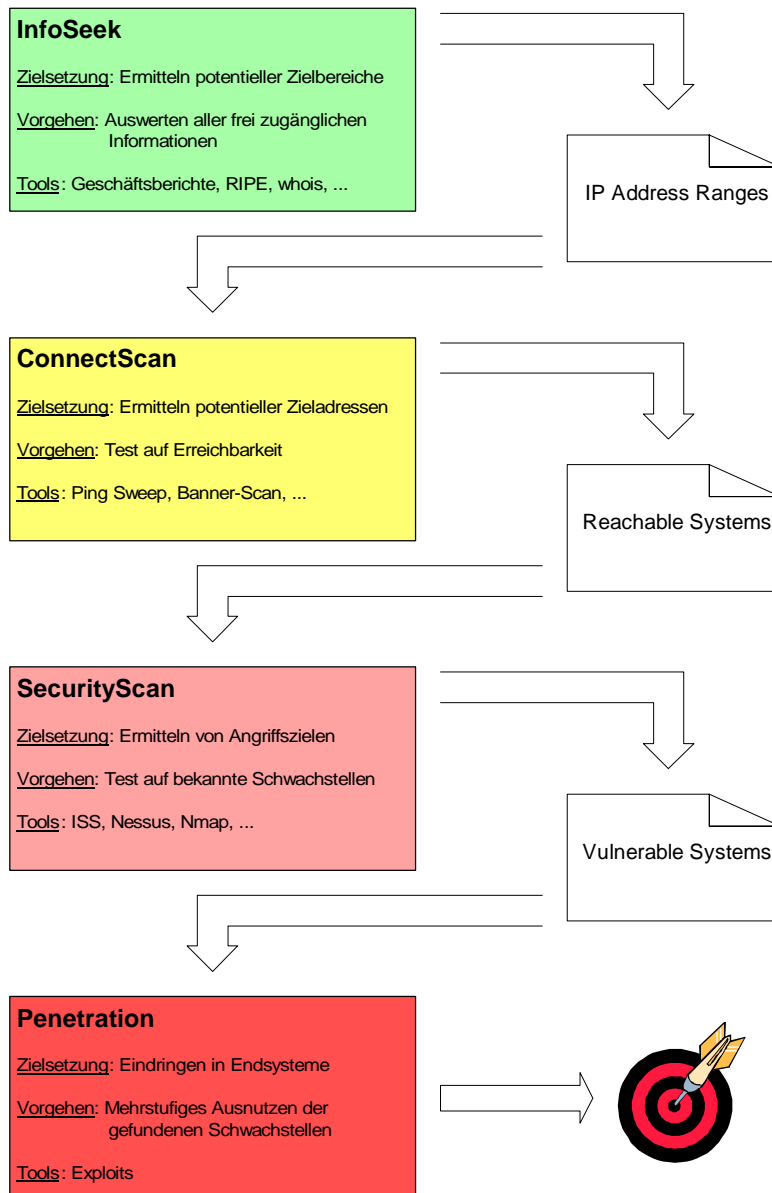


Abbildung 4: Vorgehensmodell beim BlackBox-Test

Phase-3: SecurityScan

Die dritte Phase verwendet die Ergebnisse des ConnectScan, um gezielt nach Schwachstellen zu suchen. Durch den Einsatz von Portscannern, CGI-Tests, OS-Detection, usw. werden genauere Informationen über die auf den Zielsystemen eingesetzte System- und Anwendungssoftware gesammelt. Versionen, bei denen bekannte Schwachstellen vorliegen und für die Programme zum Ausnutzen derselben verfügbar sind („exploits“), werden je nach Gefährdung aufgelistet. Dankbare Objekte hierfür sind zumeist ältere (ungepatchte) Betriebssysteme oder Dienste wie BIND, SSH, MS IIS, SMTP. Häufig gelingt es aber auch schon durch einfaches Raten z.B. Router-Passwörter zu ermitteln, oder mit ungeänderten Initial-Passwörtern wie bei SNMP (Community-String "public" oder "private") einen Schritt weiter zu kommen.

Häufig eingesetzte Tools hierbei sind: kommerzielle Security-Scanner von ISS, NAI, Symantec usw., oder auch OpenSource Varianten wie Nessus, Nmap, WhatsRunning, Idistfp.

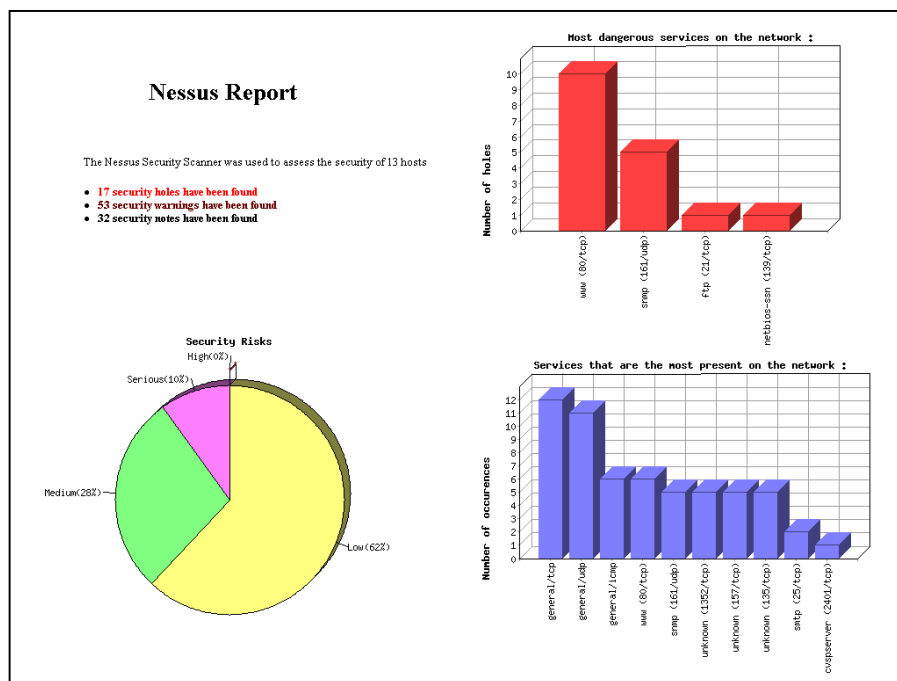


Abbildung 5: Ausgabe des Security-Scanners Nessus

Beim SecurityScan sind typische Angriffsmuster erkennbar, die einem Administrator sofort auffallen sollten. Bestimmte Tests können sogar zum Systemabsturz führen (insbesondere Denial-of-Service Attacken), weshalb diese vorher genau abzustimmen sind und bei Anwendung die ständige Erreichbarkeit des lokalen Administrators erforderlich machen.

Phase-4: Penetration

Soll die Überprüfung nicht mit den Ergebnissen des Security-Scans abgeschlossen werden, sondern Angriffe bis zum Erfolg (z.B. Eindringen in lokale Systeme über Netzgrenzen hinweg) durchgeführt werden, kommt der Penetration-Test zum Einsatz. Dieser ist entgegen der Aussage einiger Hersteller von Security-Scannern nur bedingt automatisierbar und erfordert weitgehend manuelles Vorgehen von erfahrenen Fachleuten. Diese müssen insbesondere sehr gut über neue oder noch weitgehend unbekannte Schwachstellen Kenntnis haben, sind also angehalten sich zumindest beobachtend in Hackerkreisen zu bewegen.

Die aus der vorigen Phase ermittelten Schwachstellen liefern die ersten Ansatzpunkte für das weitere Vorgehen. Sind bekannte Schwachstellen ermittelt worden, werden die notwendigen Exploits eingesetzt, um diese auszunutzen. Je nach Art der Schwachstelle ist es möglich Dienste zu unterbinden (DoS-Attacke), Webinhalte zu verändern oder sich Zugang zum gewünschten Zielsystem zu verschaffen.

Eine "typische" Penetration läuft häufig wie folgt ab:

Step-1: Bei einem öffentlich erreichbaren System wurde eine ausnutzbare Schwachstelle festgestellt. Anfällig hierfür sind besonders Web- und DNS-Server, natürlich auch gern gesehen sind vor der Schutzzone platzierte Server für ftp- oder telnet-Zugang.

Step-2: Entweder gelingt es gleich hohe Privilegien zu erlangen, oder es wird als einfacher User jetzt lokal nach weiteren Schwachstellen gesucht. Häufig gelingt es an die Passwort-Datei zu gelangen und diese dann einem Crack-Programm zuzuführen.

Step-3: Privilegiert lassen sich jetzt von diesem Ausgangssystem leicht weitere Aktivitäten starten. Zunächst werden Logeinträge gereinigt und evtl. auch Systemprogramme gegen manipulierte Versionen ausgetauscht. Hierüber oder durch Installation eines Sniffer-Programms lassen sich dann weitere Passwörter ablauschen.

Step-4: Mit etwas Glück findet der Angreifer Vertrauensbeziehungen zu anderen Rechnern oder er kann eine bestehende Session übernehmen („hijacking“). Dagegen bietet selbst die Verwendung von Starker Authentisierung keinen Schutz. Ist diese Session von interner Seite aus initiiert, dann ist sogar ein Eindringen in das interne Netz möglich.

Fazit

Aus praktischer Erfahrung diverser Sicherheitsüberprüfungen läßt sich feststellen, daß man wohl in die meisten Unternehmensnetze eindringen kann, wenn diese zumindest über eine Internetanbindung mit den üblichen Standard-Diensten verfügen. Es sei darauf hingewiesen, dass in den vorstehend dargestellten Szenarien nicht einmal solche überaus Erfolg versprechenden Attacken wie Social-Engineering, Denial-of-Service oder das Einschleusen von manipulierten Email-Attachments berücksichtigt wurden. Je mehr Netzverbindungen zu unterschiedlichen Partnern ein Unternehmen betreibt, desto anfälliger wird es für Angriffe. Da diese internen Verbindungen häufig nur schwach gesichert sind, kann über nur ein einziges schlecht gesichertes Netz der gesamte Verbund attackiert werden. Gleiches gilt für die zunehmende Zahl von Tele-Arbeitsplätzen, die zumeist nur schlecht gesichert angebunden werden. Nur eine umfassende Überprüfung in der vorgestellten Form liefert aussagekräftige Informationen, um Maßnahmen für ein ausreichend gutes Sicherheitsniveau aufzusetzen.