



# Whitepaper

## Penetrationstests

**Version 1.6**

**2008-01-17**

Tobias Glemser  
Reto Lorenz

Tele-Consulting  
security | networking | training GmbH  
Siedlerstraße 22 - 24  
71126 Gäufelden

Telefon	(0 70 32) 9 75 80
Fax	(0 70 32) 7 47 50
eMail	info@tele-consulting.com
Internet	www.tele-consulting.com




## Gliederung

1	Einleitung	1
1.1	Über dieses Dokument	1
1.2	Aufgabenstellung	2
1.2.1	Black-Box-Penetrationstests	2
1.2.2	White-Box-Penetrationstests	3
1.2.3	Ergebnis-Ermittlung der Black-Box- und White-Box-Penetrationstests	3
2	Notwendige Informationen und Festlegungen	4
3	Hinweise zur angewendeten Methodik	5
3.1	Sonderfall Webanwendungen und Webservices	5
3.2	Methodik eines Black-Box-Penetrationstests	6
3.3	Methodik eines White-Box-Penetrationstests	7
4	Technische Vorgehensweise	9
4.1	Mögliche Werkzeuge (Softwaretools)	9
4.2	Abhängigkeiten	10
4.3	Integration in vorhandene Prozesse	11
4.4	Auswirkungen auf den laufenden Betrieb	11
4.5	Berichtsstruktur	12

# 1 Einleitung

## 1.1 Über dieses Dokument

Das Whitepaper zu Penetrationstests der Tele-Consulting GmbH gibt dem Leser zum einen einen prinzipiellen Einblick in die Abläufe und Mechanismen bei einer netzbasierten Sicherheitsüberprüfung (Vulnerability-Scan) von Systemen.

Die zunächst generische Vorgehensweise wird an einzelnen Stellen unternehmensspezifisch verfeinert und gibt so potentiellen Kunden einen Einblick über die Dienstleistungen, die sie von uns erwarten können. Unternehmensspezifische Teile werden durch das Logo der Tele-Consulting GmbH  eindeutig hervorgehoben. Somit bleibt der generische Charakter des Dokuments erhalten.

Das Dokument wurde erstmalig im Jahr 2002 veröffentlicht und seither stets weiterentwickelt.

Folgende Internetseiten möchten wir Ihnen zur weitergehenden Lektüre und Informationsgewinnung empfehlen:

- Homepage der Tele-Consulting GmbH  
<http://www.tele-consulting.com>
- „Grenzen toolgestützter Penetrationstests“ – Vortrag von Reto Lorenz  
<http://pentest.tele-consulting.com>
- „Vorteile, Chancen und Risiken von Penetrationstests“ – Vortrag von Tobias Glemser  
<http://pentest.tele-consulting.com>
- „Glossar Penetrationstests“ – PDF Download  
<http://www.tele-consulting.com>
- Studie des Bundesamtes für Sicherheit in der Informationstechnik "Durchführungskonzept für Penetrationstests"  
<http://www.bsi.bund.de/literat/studien/pentest/>
- Open-Source Security Testing Methodology Manual  
<http://www.isecom.org/osstmm/>
- Wikipedia Eintrag zu Penetrationstests  
<http://de.wikipedia.org/wiki/Penetrationstest>

Das Whitepaper unterliegt dem Copyright der Tele-Consulting security networking training GmbH. Kopien jeglicher Form, auch in Auszügen, bedürfen schriftlicher Genehmigung.

**Sollen Sie Fragen, Anregungen, Kritik oder Hinweise haben, schreiben Sie uns!**  
[pentest@tele-consulting.com](mailto:pentest@tele-consulting.com)

## 1.2 Aufgabenstellung

Durch netzbasierte Penetrationstests werden die aus einem Quellnetz (Internet, WAN, LAN) erreichbaren IT-Komponenten (z.B. Router, Firewallsysteme, Mailserver, DMZ-Systeme, Webserver, Datenbankserver, aber auch Clientsysteme) eines IT-Verbundes auf technische Sicherheitslücken hin untersucht. Die Penetrationstests stellen daher eine netzbasierte Überprüfung dar, wobei grundsätzlich zwischen unterschiedlichen Angriffsquellen und daher auch zwischen verschiedenen -Charakteristiken unterschieden wird. Zwei wesentliche Unterschiede in der Vorgehensweise werden durch die Begriffe „Black-Box-“, bzw. „White-Box-Penetrationstests“ widergespiegelt. Die mit den Begriffen verbundenen Charakteristiken werden in den folgenden Unterkapiteln beschrieben.

Die netzbasierte Sicht kann grundsätzlich erweitert bzw. in ein umfassenderes Security-Audit einbezogen werden. Die – hier nicht näher ausgeführte – Aufgabenstellung eines Security-Audits kann beispielsweise die Überprüfung von Systemen über direkten Konsolen-Zugriff oder ggf. unter Zuhilfenahme von systembasierten Tools umfassen. Weitere Punkte wären die eingehende Analyse der Sicherheitspolitik, der vorhandenen Sicherheitskonzepte sowie die Überprüfung der praktischen Umsetzung der Sicherheitsmaßnahmen. Während also ein umfassenderes Security-Audit systembasierte, konzeptionelle und organisatorische Anteile umfasst, beschränkten sich die im Folgenden dargestellten Penetrationstests auf die netzbasierte Erkennung und ggf. Ausnutzung von Schwachstellen.

### 1.2.1 Black-Box-Penetrationstests

Durch die Black-Box-Penetrationstests werden eines oder mehrere Zielsysteme auf technische Sicherheitslücken hin untersucht. Dabei wird die Perspektive eines Angreifers vorausgesetzt, der keine Insider-Kenntnisse über die vorliegende Netztopologie und die netztechnische Einbindung der anzugreifenden Zielsysteme in ein organisationsweites Netz hat.

Grundsätzlich werden im Rahmen der Black-Box-Penetrationstests zwischen Angriffsquellen und daher auch zwischen verschiedenen -Charakteristiken unterschieden:

- Die Überprüfung von Zielsystemen aus dem Internet erfolgt in einer Art und Weise, die letztlich jedem Internet-Nutzer zur Verfügung steht. Es wird mit technischen Hilfsmitteln (Scanner-Tools) und mit frei erhältlichen Informationen aus dem Internet versucht, Schwachstellen in der derzeitigen Implementierung der Netzkomponenten und der Zielsysteme zu identifizieren.
- Die Überprüfung aus dem Wide Area Network (WAN) versucht die Schwachstellen zu identifizieren, die durch einen internen Angreifer ausgenutzt werden könnten, der sich Zugang zu einer (beliebigen) Stelle im organisationsweiten WAN verschafft hat. Dieser interne Angreifer hat trotz seiner Stellung jedoch ebenfalls keine nähere Kenntnis der System- und Netzumgebung.
- Die Überprüfung aus dem Local Area Network (LAN) entspricht dem internen Angreifer, der sich Zugang zu den LAN-Strukturen im direkten Umfeld der Zielsysteme verschafft hat. Mit dieser Vorgehensweise wird versucht, Schwachstellen zu identifizieren, die mit Verbindung zum LAN besser gefunden werden können. Für die gefundenen Schwachstellen kann jedoch nicht ausgeschlossen werden, dass diese bei entsprechend großem Zeitaufwand auch aus den anderen Quellnetzen heraus ausgenutzt werden können.

## 1.2.2 White-Box-Penetrationstests

Im Gegensatz zu Black-Box-Penetrationstests werden in diesem Fall die Zielsysteme aus der Sicht eines Insiders, z. B. eines ehemaligen Mitarbeiters oder externen Dienstleisters, auf technische Sicherheitslücken hin untersucht. Hierbei müssen durch den Auftraggeber Informationen über die zu testenden Systeme ausgegeben werden. Der Detailgrad dieser Informationen ist hierbei entscheidend für die Sicht, die der Angreifer einnehmen soll. Dies kann von einem nur kurze Zeit im Unternehmen beschäftigten, über einen mit der Administration von Systemen betrauten bis hin zu einem externen Dienstleister gehen, der Security-, Server-, Client- und/oder Netz-Komponenten installiert und konfiguriert hat. Hierzu werden interne Informationen zum Aufbau der Netzsegmente und zur Konfiguration der Zielsysteme einbezogen. Es kann im Einzelfall auf die Systeme selbst zugegriffen werden, oder – analog zu der Durchführung der Black-Box-Penetrationstests – aus unterschiedlichen Quellnetzen heraus versucht werden, die Schwachstellen der Systeme zu identifizieren. Dies entspricht der Perspektive eines Angreifers, der Kenntnisse über den Aufbau der Netzstrukturen und der relevanten Systeme hat.

Im Rahmen der White-Box-Penetrationstests wird ebenfalls zwischen Angriffsquellen (Internet, WAN, LAN) und daher auch zwischen verschiedenen Charakteristiken unterschieden. Der Unterschied zu den Black-Box-Tests besteht darin, dass für die Durchführung der White-Box-Tests auf interne Informationen zu Technik und Aufbau der Netze und Systeme zurückgegriffen werden kann. Vor dem Hintergrund der internen Informationen wird mit technischen Hilfsmitteln (Scanner-Tools) versucht, aus den jeweiligen Quellnetzen heraus Schwachstellen in der derzeitigen Implementierung der Site zu identifizieren, wobei die Tools hierbei deutlich granularer und gezielter auf die zu überprüfende Systemumgebung angepasst werden können.

## 1.2.3 Ergebnis-Ermittlung der Black-Box- und White-Box-Penetrationstests

Durch die Vorgehensweise werden mit Hilfe der eingesetzten Werkzeuge Schwachstellen identifiziert, ohne diese in gesonderten Schritten auszunutzen. Angriffe auf identifizierte Schwachstellen sind mit einem sehr hohen Zeitbedarf verbunden, so dass für die Black-Box- und White-Box-Penetrationstests verstärkt auf den Einsatz von Scanner-Tools zurückgegriffen wird. Dieser Ansatz ermöglicht es, ein breites Spektrum an Angriffsmöglichkeiten abzudecken. Die Schwächen der einzelnen Tools werden durch den Einsatz unterschiedlicher Scanner-Software minimiert.

Im Zuge der Penetrationstests aus dem WAN und dem LAN werden die Zielsysteme im Dialog festgelegt. Ein Angreifer aus diesen Quellnetzen würde sich jedoch nicht auf einzelne Zielsysteme beschränken, sondern jede greifbare Information einbeziehen. Daher werden – soweit dies in der verfügbaren Zeit möglich ist – Informationen von Intranet-Servern und anderen erreichbaren Systemen mit einbezogen.

Die Ergebnisse der netztechnischen Sicherheitsüberprüfung werden entsprechend dem Ablauf und der gefundenen Ergebnisse dokumentiert.

## 2 Notwendige Informationen und Festlegungen

Die hier genannten Informationen werden für die Vorbereitung und Durchführung der Sicherheitsüberprüfung herangezogen, um eine gezielte Vorgehensweise zu ermöglichen. Die folgende Aufstellung nennt stichwortartig die Informationen, die grundsätzlich bzw. abhängig vom eingesetzten System zu einer hinreichenden Eingrenzung der Zielsysteme beitragen.

### Grundsätzlich:

- Festlegung der zu überprüfenden Zielsysteme bzw. des damit verbundenen Adressbereichs (IP-Adress-Range) oder Nennung der zu überprüfenden Domain (DNS/Domainnamen)
- Festlegung der berechtigten und verantwortlichen Ansprechpartner
- Dauer und Umfang der Penetrationstests

### Optional:

- Festlegung von Zeitfenstern zur Durchführung
- Ausdrückliche Vereinbarung über Angriffe mittels sog. Social Engineering, schädigender Software (Viren, Trojaner, Würmer), Denial of Service, Buffer Overflow-Attacken
- Ausdrückliche Vereinbarung über die explizite Ausnutzung von möglichen Schwachstellen
- ist ggf. ein Betriebsrat zu informieren (Ergebnisse eines Penetrationstest sind grundsätzlich potentiell zur Überwachung oder Beurteilung von Mitarbeitern geeignet, insbesondere bei Social-Engineering)
- ist ein „ständiger Begleiter“, der die angegriffenen Systeme während der gesamten Testdauer von Nöten, um eventuelle Auswirkungen auf die Systeme frühzeitig zu erkennen

Die entstehenden Aufwände sind abhängig von Dauer und Umfang der Testmaßnahmen, Anzahl der zu prüfenden Systeme, Verfolgung der Schwachstellen, explizite Ausnutzung derselben etc.

Der individuelle Leistungsumfang wird jeweils im Dialog festgelegt.

Sollten outgesourcte Dienste, wie z.B. Webservices auditiert werden, so müssen die externen Dienstleister durch den Auftraggeber entsprechend über anstehende Tests informiert werden. Dies gilt in gleicher Form für Carrier bzw. Provider, über die die externen Netzübergänge realisiert werden, sofern diese Bestandteil der Überprüfung sind.

### 3 Hinweise zur angewendeten Methodik

Die folgenden Hinweise zeigen auf, welche Methodik für die Durchführung der netztechnischen Sicherheitsüberprüfung zugrunde gelegt wird. Soweit möglich und sinnvoll werden die Werkzeuge genannt, die dazu herangezogen werden.



Die Tele-Consulting GmbH bietet mit dem Security-Scanner **fajanas** ein Produkt an, mit dem der Kunde kostengünstig Penetrationstests toolgestützt durchführen lassen kann. Hierbei unter der Nutzung etablierter Security- und Portscanner ein Scan auf das Zielsystem angestoßen und ein Ergebnisbericht produziert. Diese recht „globale“ Vorgehensweise empfiehlt sich zunächst für Black-Box-Penetrationstests.

Sofern jedoch nicht die Alarmierungsmechanismen von Netzsicherungselementen wie Intrusion-Detection-Systemen im Vordergrund stehen, können diese automatisierten Tests eine für den Kunden sehr kosteneffizient Möglichkeit der Prüfung darstellen. Im Falle eines White-Box-Tests wäre dies ein möglicher erster Schritt.

Alle Systeme werden in jedem Fall manuell entsprechend Ihrer Systemspezifika geprüft. Dies ist besonders für exponierte Systeme wie Webserver oder RAS-Lösungen (Einwahlserver, VPN), ebenso wie für Anwendungen empfehlenswert.

Weitere Informationen finden Sie unter

<http://pentest.tele-consulting.com>

#### 3.1 Sonderfall Webanwendungen und Webservices

Noch bis vor einigen Jahren waren Webseiten wenig umfangreich und wenig interaktiv. Die Sensibilität der in Webdiensten bereitgestellten Informationen steigt dabei stetig an. Es hat sich gezeigt, dass Webanwendungen und Webservices (z. B. SOAP) immer häufiger eingesetzt und deutlich verstärkt in den Fokus von Angreifern gerückt sind. Mittlerweile besteht eine Vielzahl von Schwachstellen, die aktiv von Angreifern ausgenutzt werden.

Die vollumfängliche Prüfung von Webanwendungen und Webservices ist daher in jedem Fall mit spezialisierten Tools zu unterstützen.



Die Prüfungen von Webanwendungen und Webservices ist aus unserer Sicht nur noch sehr bedingt in einem akzeptablen Zeitraum und hoher Testtiefe mit frei erhältlichen Tools möglich. Daher hat sich Tele-Consulting security networking GmbH dazu entschlossen, ein internes Auswahlverfahren zu kommerziellen Web-Vulnerability-Scannern durchzuführen. Der ausgewählte Scanner **acunetix** (Informationen unter [www.acunetix.com](http://www.acunetix.com)) ermöglicht es, komplexe und interaktive Webseiten mit einer hohen Prüftiefe zu testen. Dabei werden neben Cross-Site-Scripting und SQL-Injection auch AJAX-Technologien und Java-Script auf Schwachstellen hin untersucht.

Darüber hinaus bietet die aktuelle Version auch spezielle Tests für Webservices wie z. B. SOAP.

## 3.2 Methodik eines Black-Box-Penetrationstests

Die prinzipielle Methodik der netztechnischen Sicherheitsüberprüfung ist nachstehend aufgeführt. Hierzu werden - nach Absprache - im Einzelfall zusätzliche Tools eingesetzt, soweit dies sinnvoll erscheint. Das nachstehende Schema zeigt beispielhaft das Vorgehen aus dem Internet.

- **Aufklären**
  - Spurensuche im Internet  
Abfrage von offiziellen Verzeichnissen (DENIC, InterNIC, RIPE, ARIN) via whois, nslookup, Browser. Recherche über die Organisation und über deren Mitarbeiter, z.B. in Online-Foren<sup>1</sup>, (z.B. USENET, irc), elektronischen Telefonverzeichnissen, Archiven, Mailing-Lists, Newsletters via (Meta-) Suchmaschinen (z.B. google.com, dogpile.com, altavista.com, alltheweb.com, vivisimo.com etc.)
  - Netzwerktopologie (Aufklärung der sichtbaren Netzstruktur<sup>2</sup>)  
Domain Name Service (DNS) Abfrage mit Zone Transfer (falls möglich), Mail Exchange (MX) records, tracerouting, Einsatz eines Network Analyzers
- **Abtasten**

Zur Netzwerkanalyse gibt es eine Vielzahl von Hilfsprogrammen. Dies reicht von einfachen Skripten bis zum vollautomatischen Scannertool. Nachfolgend aufgeführte Methoden können – je nach eingesetztem Software-Tool – sowohl manuell gesteuert als auch teil- bzw. vollautomatisiert durchgeführt werden.

Neben den gängigen Befehlen und Tools auf TCP/IP-Basis können hierbei Scanner-Tools wie nmap, nessus, LANguard, Stealth, Saint, ISS Internet Scanner sowie Retina eingesetzt werden. Im Zuge des Einsatzes der genannten Scanner-Tools wird zunächst ein erstes Bild der Zielobjekte gewonnen und danach die Parametrisierung stufenweise angepasst.

Mittels der nessus und nmap-Software können erste Ergebnisse ermittelt werden, wobei die eingesetzten Scanning-Techniken nicht immer fein steuerbar sind. Überwiegend wird aber (z.B. bei der Software ISS Internet Scanner und Retina) über sog. Module gesteuert, mit welchen Scanning-Methoden die Zielsysteme auf Schwachstellen hin untersucht werden.

Je nach Scan-Verlauf können die Module der Scanner-Software in unterschiedlichen Zusammenstellungen oder auch separat für sogenannte Scan-Läufe eingesetzt werden. Die generellen Methoden umfassen im Allgemeinen folgendes:

- Netzwerkanalyse<sup>3</sup>  
ping sweep (ICMP ECHO\_REQUEST, ECHO\_REPLY) TCP ping (TCP ACK, SYN/ACK), traceroute, ICMP query (TIMESTAMP, ADDRESS MASK REQUEST), SNMP InformationPort Scanning<sup>4</sup>  
TCP connect scan, TCP half-open scan / SYN scan, TCP FIN scan, TCP Null scan, UDP scan, RPC scan

---

<sup>1</sup> Online-Foren dienen dem Informationsaustausch zu unterschiedlichsten Themen, oft wird übersehen, dass man hier sehr viele Anhaltspunkte hinterlässt

<sup>2</sup> Zur Netzstruktur zählen unter anderem die Adressen, über welche die Rechner der Organisation bzw. des Unternehmens über das Internet angesprochen werden können, aber auch der populäre Webaufttritt der Firma

<sup>3</sup> Um die aktiven Netzwerkkomponenten eines Systems zu ermitteln.

<sup>4</sup> Rechner stellen über Ports verschiedene Dienste zur Verfügung, die auch missbraucht werden können.

- Betriebssystem/Anwendungen ermitteln<sup>5</sup>  
Aufgrund von herstellerspezifischen Abweichungen der RFC Implementierungen kommt es zu OS und Anwendungsspezifischen Anomalien, die zu einer Eingrenzung bzw. Bestimmung des Betriebssystems verwendet werden können. Dies kann z.B. durch Stack-Fingerprinting, Banner-Grabbing, Untersuchung der Initial Sequence Number oder Analyse der Round-Trip-Time erfolgen.
  - Recherche und Überprüfung spezifischer Schwachstellen der Systeme und Anwendungen:  
In einem zeitlich beschränkten Maße werden spezifische Schwachstellen betreffend der eingesetzten Systeme recherchiert und für die weitere Vorgehensweise genutzt. Für zahlreiche Systeme und verwendete Software im Bereich von Internet-Zugängen bzw. angebotenen Internet-Diensten sind in den Scanner-Tools die Informationen zu möglichen Angriffsvarianten hinterlegt. Dadurch ist die Scanner-Software in der Lage, derartige Schwachstellen aufzudecken, ohne dass dadurch der Angriff tatsächlich durchgeführt wird. Betroffen sind insbesondere Schwachstellen aufgrund des eingesetzten Betriebssystems oder z. B. der Web-Server-Software.
  - Überprüfung auf vorhandene Backdoors  
Durch Programmcode, der – in der Regel unbewusst – auf Zielsystemen in internen Netzen installiert wird (sog. Trojaner), kann es einem Angreifer ermöglicht werden, Informationen auszuspähen oder direkt auf das Systemverhalten Einfluss zu nehmen. Hierfür sind in den Scanner-Tools die bekanntesten Backdoors mit den verwendeten Standard-Parametern hinterlegt.
  - Weitere Maßnahmen  
Je nach „Ausbeute“ können – auf der Basis der bereits gefundenen Ergebnisse – die verfügbaren Dienste abgeprüft werden. Hierzu gehören die Angriffsmethoden Versuch der Kompromittierung, eMail-Fälschung, etc. Für die weiteren Maßnahmen können unter anderem die Scanner-Tools oder – je nach vorheriger Absprache – gesonderte Tools eingesetzt werden.
- **Auswerten**  
Die Ergebnisse werden nach technischen Gesichtspunkten ausgewertet. Entsprechend der erzielten Ergebnisse gehören dazu beispielsweise folgende Aspekte:
    - Auswertung offener Ports und der dahinter verfügbaren Dienste
    - Zusammenstellen von gemeinsam genutzten Ressourcen, wie z.B. Datenbanken, Dateien, aber auch von Druckern, Datenträgern usw.
    - Vergleich von Ergebnissen der unterschiedlichen Tools und Prüfung der Ergebnisse auf Plausibilität und Relevanz der identifizierten Schwachstellen.

### 3.3 Methodik eines White-Box-Penetrationstests

Die nachfolgende Aufstellung orientiert sich hinsichtlich der Struktur an der Methodik des Black-Box-Penetrationstests, zeigt jedoch nur die Erweiterungen bzw. Änderungen für die Methodik des White-Box-Penetrationstests auf.

- **Aufklären**
  - Spurensuche im Internet  
Es erfolgt eine vertiefende Recherche im Internet über die Organisation und über deren Mitarbeiter. Soweit es sinnvoll erscheint, werden hierzu auch Begrifflichkeiten aus den internen Informationen einbezogen.

---

<sup>5</sup> Ist das Betriebssystem eines angegriffenen Rechners bekannt, können später gezielt die Schwachstellen dieses Systems genutzt werden.

- Netzwerktopologie (Aufklärung der sichtbaren Netzstruktur)  
Aufgrund der über die internen Informationen vorliegenden Hinweise kann an dieser Stelle eine angepasste Vorgehensweise genutzt werden, um evtl. vorhandene Schutzmaßnahmen zu umgehen.
  - Recherche spezifischer Schwachstellen der Systeme und Anwendungen:  
In einem zeitlich beschränkten Maße werden spezifische Schwachstellen betreffend der eingesetzten Systeme recherchiert und für die weitere Vorgehensweise genutzt.
- **Abtasten**  
Die Methodik stellt eine vertiefende Netzwerkanalyse dar, wobei prinzipiell die gleichen Tools angewendet werden, die auch für die Black-Box-Penetrationstests Verwendung finden. Die Tools können hierbei mit Hilfe der internen Informationen gezielter eingesetzt werden.
  - **Auswerten**  
Mit Hilfe der internen Informationen kann die Relevanz identifizierter Schwachstellen besser bewertet werden. Dies kann dazu führen, dass im Rahmen der Black-Box-Tests durch die Scanner-Tools identifizierte Schwachstellen sich als einen „Fehlalarm“ herausstellen, weil die Scanner-Tools die Reaktion eines Systems im Rahmen der gesamten Systemumgebung falsch interpretiert hat.

## 4 Technische Vorgehensweise

Der Einsatz der genannten Methoden und Werkzeuge erfolgt in unterschiedlicher Weise. Während für die Scanner-Tools die Einsatzparameter eine wichtige Rolle spielen, können bei Werkzeugen wie beispielsweise nslookup, telnet, ping oder traceroute wenige oder keine Einstellungen vorgenommen werden.

Die verwendeten Parameter lassen sich nicht bei allen Tools gleichermaßen gut dokumentieren bzw. lesbar darstellen. Die für einzelne Scans verwendeten Parameter können auf Wunsch in jeweils elektronischer Form dokumentiert und zur Verfügung gestellt werden.

### 4.1 Mögliche Werkzeuge (Softwaretools)

Die möglichen Werkzeuge werden nachfolgend ohne Anspruch auf Vollständigkeit oder deren tatsächlichen Einsatz aufgeführt:

- Browser (z.B. Opera, Internet Explorer, Netscape Navigator): Der Browser dient zunächst der Informationsbeschaffung im Internet. Weiterhin kann durch die Manipulation der Adress-Zeile (URL) versucht werden, Informationen von Server-Diensten zu erlangen oder eine Fehlfunktion des Zielsystems herbeizuführen.
- telnet, netcat: für die manuelle Überprüfung von bestimmten Serverdiensten wird mit Hilfe von telnet bzw. netcat versucht, weitergehende Informationen zu erlangen oder vorhandenen Serverdiensten Informationen "unterzuschieben".
- whois, host: Programme zur automatischen Abfrage von Domain Informationen
- nslookup: Informationen von Nameservern werden mit Hilfe von nslookup ermittelt.
- ping: dient zur Überprüfung der Erreichbarkeit einer IP-Adresse.
- traceroute: damit wird versucht, den Kommunikationsweg zu einem Zielsystem zu ermitteln.
- nmap: nmap ist ein gut steuerbarer Portscanner, der zudem für die Methode des OS und Applikation-fingerprinting verwendet wird, um das Betriebssystem und die Typen der Anwendungsprogramme von Zielsystemen zu ermitteln.
- Xprobe: Tool zur Ermittlung des Betriebssystems mittels ICMP-Paketen.
- ISS Internet Scanner: Scanning-Tool, das über eine hinterlegte Datenbank mit zahlreichen Angriffsmustern verfügt. Mit Hilfe dieser Angriffsmuster werden bei den Zielsystemen Schwachstellen identifiziert, indem die Antworten bzw. die Reaktion der Zielsysteme interpretiert wird. Dabei werden die Angriffsmuster nicht für die Durchführung eines tatsächlichen Angriffs verwendet.. Verwendung in Absprache mit dem Kunden, da die Lizenzbedingungen eine konkrete Bindung an explizit genannte IP-Adressen und damit entsprechende Lizenzkosten mit sich bringt
- Retina: Scanning-Tool mit ebenfalls ähnlichen Eigenschaften wie der ISS Internet Scanner. Es wird ebenfalls die Verwendung in Absprache mit dem Kunden festgelegt, da die Lizenzbedingungen eine konkrete Bindung an explizit genannte IP-Adressen und damit entsprechende Lizenzkosten mit sich bringt
- nessus: Open-Source (Version 2.x; in Version 3.x ist die Scanning Engine ClosedSource) Vulnerability-Scanner auf der Basis von Scripten.
- Mitschnitte der Datenströme durch Sniffer-Tools (ethereal, packetyzer, tcpdump, sniffer, hunt, etc.): bestimmte Informationen während der Durchführung von Scan-Läufen sowie spezielle Informationen der Kommunikation zu Serverdiensten werden nicht durch die eingesetzten Scanner-Tools sichtbar, sondern nur durch eine fallweise Analyse des Protokolldatenstroms. Daher sind im Einzelfall und für gezielte Fragestellungen die Mitschnitte dieses Protokolldatenstroms hilfreich.
- Tools für Aufgaben im Bereich von SNMP (z.B. snmpwalk, snmpsniff)
- MGEN, Hping2/3: Tools zum Versenden maßgeschneiderter ICMP/UDP/TCP-Pakete

- Firewall: Werkzeug, das mittels modifizierter traceroute-Technik Netztopologie und Filter erkennen kann
- Ettercap/Cain&Abel: Werkzeug für den Einsatz in geschwichten Netzumgebungen, z. B. für ARP-Poisoning, Man-in-the-Middle-Attacken und für Mitschnitte von Kommunikationsverbindungen (z. B. VoIP), etc.
- Metasploit: Toolkit zur aktiven Ausnutzung von Exploits
- NAT: NetBIOS Auditing Tool
- LANguard: NetBIOS-Scanner, Verwendung in Absprache mit dem Kunden, da ggf. Lizenzkosten anfallen.
- Acunetix Scanner: kommerzieller Website-Scanner mit Modulen zur Erkennung von XSS und SQL-Injection sowie Backup-Dateien.
- N-Stealth: kommerzieller Website-Scanner für gezielte URL-Attacken
- Password Cracker: z.B. L0pht Crack, John the Ripper, Cain&Abel, AccessDiver
- THC-Scan, THC-Scan ng: War-Dialer zum Auffinden und Analysieren von Telefon-/FAX-/Modem- und RAS-Zugängen
- Access-Diver: http-Brute Forcer, beispielsweise zum Testen von Authentisierungsschwachstellen auf Web-Servern.
- Kismet, Netstumbler, Wellenreiter: Tools zur Erkundung von WLAN Accesspoints und Stationen, Ausgabe von Informationen wie Netzlast, Verschlüsselung
- WEPcrack, Aircrack-ng, WEPattack: Tools zum Cracken der WEP-Verschlüsselung in WLAN-Verbindungen
- Yersenia zur Prüfung von Schwachstellen im Layer 2 (nur für Angriffe aus dem LAN relevant)

Aufgrund des hochdynamischen Umfelds im IT-Bereich kommen situationsabhängig ständig neue Tools zum Einsatz bzw. vorhandene Tools werden angepasst oder selbst generiert sowie spezielle Exploits manuell durchgeführt.

## 4.2 Abhängigkeiten

Die Durchführung von Sicherheitsüberprüfungen ist von Randbedingungen abhängig, die im Allgemeinen nicht direkt beeinflusst werden können. Hierzu zählen beispielsweise die netztechnischen Gegebenheiten durch die Konfiguration von Netzkomponenten zwischen einem ausgewählten Quellnetz und den festgelegten Zielsystemen. Die Penetrationstests können dadurch z. B. dahingehend beeinflusst werden, dass bestimmte Arten von Paketen nicht in der gewünschten Weise weitergeleitet werden. Soweit derartige Abhängigkeiten festgestellt werden können, erfolgen entsprechende Hinweise darauf in der Ergebnisdokumentation. Durch derartige Effekte können so genannte „false positives“ und „false negatives“ zum Vorschein kommen, d. h. es können dadurch Schwachstellen identifiziert werden, die nicht vorhanden sind oder es werden bestimmte Schwachstellen nicht identifiziert, obwohl diese aus einem anderem Quellnetz heraus ausgenutzt werden könnten.

Werden im Umfeld der internen Firewall-Systeme Angriffs-Erkennungstools (Intrusion-Detection- oder Intrusion-Response-Systeme) eingesetzt, so kann die Durchführung der netzbasierten Überprüfung von Schwachstellen derart beeinflusst werden, dass bestimmte Tests nicht vollständig durchführbar sind und dementsprechend auch die Aussagefähigkeit der Ergebnisse hinsichtlich möglicher Schwachstellen eingeschränkt wird. Stattdessen werden dann die aus unserer Sicht erkennbaren Gründe dafür aufgeführt.

## 4.3 Integration in vorhandene Prozesse



Die Tele-Consulting security networking training GmbH ist sehr bemüht, Testpläne an die internen Prozesse der Kunden anzupassen. So ist es nicht erstrebenswert, z. B. einen Firewall-Audit kurz vor einer Umstellung der Firewall durchzuführen, da sich das Ergebnis schnell überholt hat. Daher ist es erforderlich, alle Tätigkeiten eng mit dem Kunden abzustimmen und auch bei langfristigen Prüfplänen aktuelle interne Projekte und Umstrukturierungen zu berücksichtigen.

## 4.4 Auswirkungen auf den laufenden Betrieb

Eine maximale Betriebssicherheit während der Durchführung der Sicherheitsüberprüfung wird angestrebt. Hierzu werden die erforderlichen Maßnahmen in drei Kategorien unterteilt:

1. Unkritische Maßnahmen  
Diese beeinträchtigen nach unserem heutigen Kenntnisstand die Betriebssicherheit nicht.
2. Teilkritische Maßnahmen (z.B. Scans mit fragmentierten Paketen, Passwort Brute-Force)  
Diese können unter ungünstigen Randbedingungen zu einer teilweisen Beeinträchtigung des laufenden Betriebs führen.
3. Kritische Maßnahmen (z.B. Überprüfung von Denial-of-Service-Schwachstellen)  
Diese führen möglicherweise zu einer zeitweiligen Beeinträchtigung des laufenden Betriebs.

Ohne erfolgte Abstimmung können zunächst nur die unkritischen Maßnahmen durchgeführt werden. Teilkritische und kritische Maßnahmen bedürfen im Vorfeld der Durchführung einer Abstimmung bzgl. Einsatz, Dauer und flankierender Betriebssicherheitsvorkehrungen.

Die eingesetzten Tools beschränken sich somit zunächst auf die Erkennung von möglichen Schwachstellen. Im Zuge der Sicherheitsüberprüfung werden zudem ggf. weitere Tools eingesetzt, die sich aufgrund der gewonnenen Informationen für die Überprüfung einzelner Schwachstellen eignen. Daher kann nicht ausgeschlossen werden, dass beispielsweise durch Portscanning die Kommunikation behindert oder durch gezielte Denial-of-Service-Überprüfungen die entsprechenden Systeme die vorgesehenen Dienste nicht mehr ohne vorherigen manuellen Eingriff erbringen können.

Sollten sich derartige Vorfälle ereignen, wird in Absprache mit dem Auftraggeber nach Lösungen gesucht, die eine schnelle Minderung oder Beseitigung einer Schwachstelle zulassen. Sollten entsprechende Eskalationsszenarien nicht im Sicherheitskonzept festgelegt sein, so ist die Erstellung der entsprechenden Kapitel dringend empfehlenswert und sollte vor einem Penetrationstest erfolgen. Bei der Erstellung eines Sicherheitskonzepts oder Teilen davon, stehen wir Ihnen ebenfalls gerne zur Verfügung.

Zwei Hinweise sind für die Beurteilung der Ausfallsicherheit elementar:

1. Aufgrund der Komplexität von IT-Systemen kann niemals zu 100% ausgeschlossen werden, dass sich das zu testende System stabil verhält. Selbst ein simpler Port-Scan, der keinerlei Schwachstellen ausnutzt, kann unter Umständen zum Absturz eines Systems oder Teilen davon führen.
2. Entscheidet man sich gegen die Durchführung kritischer Maßnahmen (siehe Punkt 3 oben), limitiert man die Aussagekraft eines Tests. Es ist auch in Produktivumgebungen meist durchaus empfehlenswert, diese Maßnahmen durchzuführen. *Ein realer Angreifer macht vor diesen Maßnahmen auch nicht halt!* Selbstverständlich müssen entsprechende Konzepte vorliegen, die im Falle eines Ausfalls einen schnellen Wiederanlauf der Umgebung ermöglichen.

## 4.5 Berichtsstruktur



Die nachstehende Struktur hat sich bewährt. Individuelle Anpassungen gemäß Kundenwünschen können nach Absprache erfolgen. Der Ergebnisbericht strukturiert sich im Allgemeinen wie folgt:

- Ein Ergebnisbericht zur Darstellung der Randbedingungen, Vorgehensweisen, Methoden, Werkzeuge und der Bewertung der Ergebnisse. Hierbei werden Maßnahmen zur Beseitigung von evtl. gefundenen Schwachstellen enthalten sein. Der Bericht enthält ggf. Verweise auf gesonderte Dokumente im Anhang.
- Exemplarische Verweise auf Auszüge der im Internet gefundenen Informationen, die für die Sicherheitsüberprüfung verwendet wurden.
- Ggf. ein Management-Summary mit der Nennung und Erläuterung der wichtigsten Ergebnisse und deren Auswirkungen.
- Ergebnisse der eingesetzten Software-Tools in Form von Listings, Reports oder Screenshots.

Im Gegensatz zu vielen Wettbewerbern verwenden wir keine Textbausteine sondern passen die Ausführungen an die Bedürfnisse jedes Kunden an. Dies hat Auswirkung auf den Detailgrad und die Formulierungen.

Eine Anpassung auf Kundensicht erhöht den Nutzen für die jeweilige Kundensituation, da angestrebt wird nur relevante Inhalte in der erforderlichen Informationstiefe beschrieben werden und keine Inhaltshülsen zum Generieren von Seitenzahlen im Bericht genutzt werden.