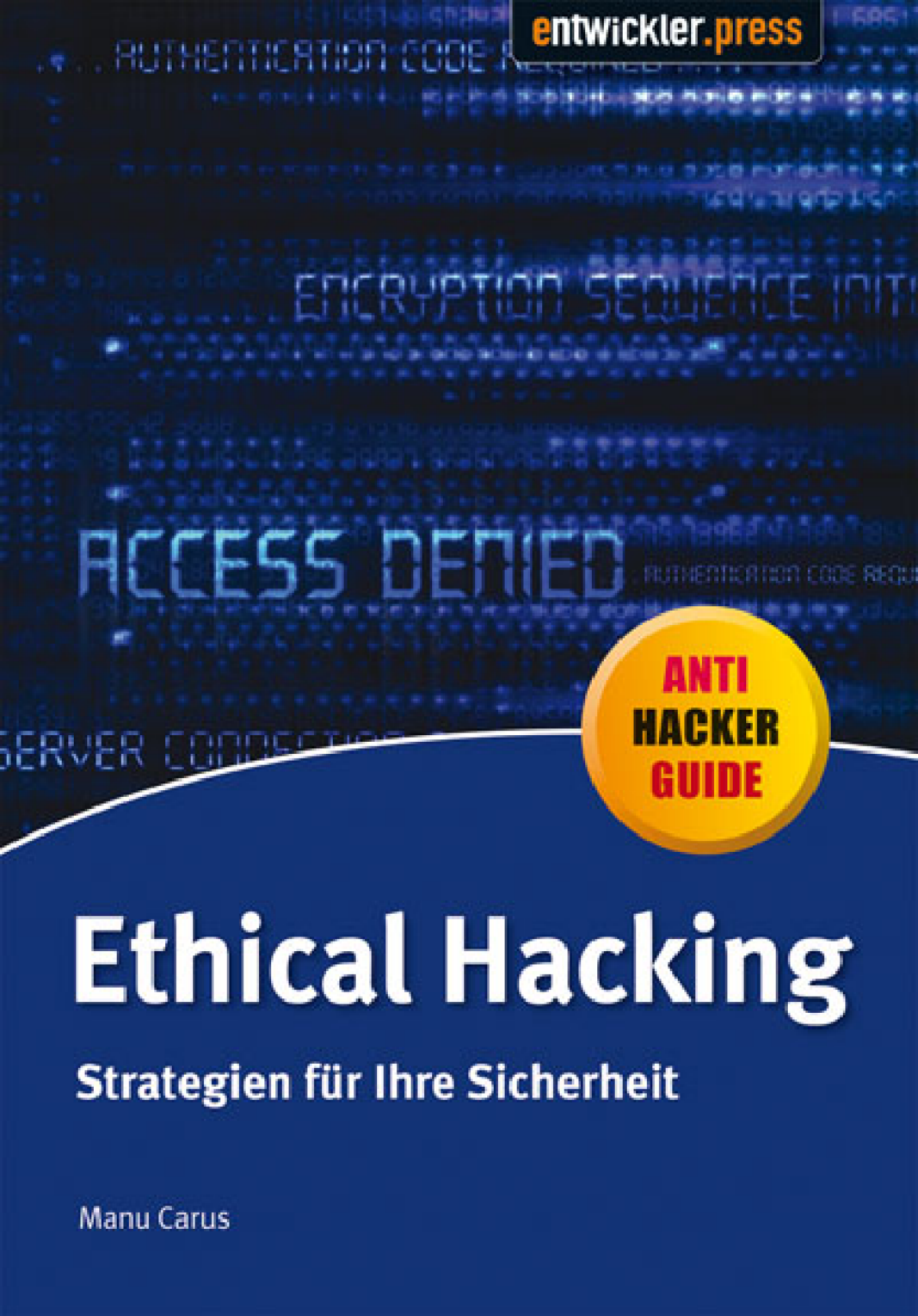


Ethical Hacking

Strategien für Ihre Sicherheit

Manu Carus

Manu Carus

Ethical Hacking

Manu Carus

Ethical Hacking

Strategien für Ihre Sicherheit

entwickler.press

Manu Carus: Ethical Hacking
Strategien für Ihre Sicherheit
ISBN: 978-3-939084-22-8

© 2008 entwickler.press
Ein Imprint der Software & Support Verlag GmbH

Bibliografische Information Der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.ddb.de abrufbar.

Ihr Kontakt zum Verlag und Lektorat:
Software & Support Verlag GmbH
entwickler.press
Hauptstr. 8b
82008 Unterhaching
Tel: +49 (0)89 66 55 76 10
Fax: +49 (0)89 66 55 76-11
http://www.entwickler-press.de

Korrektorat: mediaService, Siegen
Satz: mediaService, Siegen
Umschlaggestaltung: Caroline Butz, Maria Rudi
Belichtung, Druck & Bindung: M.P. Media-Print Informationstechnologie GmbH, Paderborn

Alle Rechte, auch für Übersetzungen, sind vorbehalten. Reproduktion jeglicher Art (Fotokopie, Nachdruck, Mikrofilm, Erfassung auf elektronischen Datenträgern oder andere Verfahren) nur mit schriftlicher Genehmigung des Verlags. Jegliche Haftung für die Richtigkeit des gesamten Werks kann, trotz sorgfältiger Prüfung durch Autor und Verlag, nicht übernommen werden. Die im Buch genannten Produkte, Warenzeichen und Firmennamen sind in der Regel durch deren Inhaber geschützt.

Inhaltsverzeichnis

Vorwort **9**
Über die Notwendigkeit des ethischen Hackers 9
Über den Inhalt dieses Buchs 10
An wen sich dieses Buch wendet 11
Was zum Verständnis dieses Buchs benötigt wird 12
Wie dieses Buch strukturiert ist 12
Danksagung 14
Widmung 14
Über den Autor 15

1 Die Welt ist schlecht! **17**
1.1 Rechtsprechung und Ethik 17
Aus dem Strafgesetzbuch 18
Computer-Ethik 20
1.2 Hacker 21
Black Hats 22
White Hats 22
Gray Hats 22
1.3 Ethical Hacker 22
1.4 Spion gegen Spion 24
1.5 Das Internet braucht eine Revolution ... 24
Die Geschichte des Internet 24
Internet-Protokolle 25
Sicherheit im Internet 26
Anonymität im Internet 29
Das Leben im „Hier und Jetzt“ 34

2 Opfer, Täter, Vorgehensweisen **37**
2.1 Opfer 39
Private Anwender und Unternehmen 39
Systeme und Technologien 44
2.2 Täter 46
2.3 Vorgehensweisen 47
Trojaner 48
Spam 56

	Phishing	61
	Viren	64
	Würmer	67
	Spyware	69
2.4	Goldene Regeln für jeden Internet-User	73
3	**Professioneller Einbruch**	**77**
3.1	Vorgehensmodell	77
3.2	Phase 1: Auskundschaften	78
3.3	Phase 2: Abtasten	83
	Network Scanning	83
	Port Scanning	84
	Vulnerability Scanning	87
3.4	Phase 3: Angreifen	87
3.5	Phase 4: Festsetzen	90
3.6	Phase 5: Tarnen	91
3.7	Ausblick	92
4	**Auskundschaften**	**93**
4.1	Entdecken und entdeckt werden	93
	„Harmlose“ Quellen	93
	Informationsbeschaffung	97
	Verdeckte Ermittlung	98
4.2	Passives Auskundschaften	102
	Wer bist du?	104
	Wo bist du?	123
4.3	Aktives Auskundschaften	125
	Wer bist du?	125
	Wo bist du?	128
4.4	Gegenmaßnahmen	132
5	**Abtasten**	**137**
5.1	Scanning	138
	Methoden	139
	Vorgehensweise	140
5.2	Network Scanning	140
	NMAP	141
	NetScan Tools Pro	150
	SuperScan4	153
5.3	Port Scanning	155
	Ports	155
	TCP	159
	Techniken	162
	Port Scanner	169

5.4	Fingerprinting	178
	Banner Grabbing	178
	Stack Fingerprinting	180
5.5	Vulnerability Scanning	187
	Schwachstellen	188
	Kataloge	194
	Vulnerability Scanner	201
5.6	Gegenmaßnahmen	228
6	**Angreifen**	**231**
6.1	Enumeration	234
	Strategien	234
	Tools	237
6.2	Passwörter	249
	Cracking	249
	Sniffing	257
	Tools	258
6.3	Rechte	269
	Vorgehensweise	269
	Tools	270
6.4	Gegenmaßnahmen	272
	Sicherheitsrichtlinien	272
	Passwort Saver	278
7	**Festsetzen**	**281**
7.1	Hintertüren	281
	Privater Sektor	281
	Unternehmensnetzwerke	284
7.2	Client/Server-Architektur	285
	Server	286
	Client	289
7.3	Tools	291
	NetCat	291
	PsExec	295
7.4	Gegenmaßnahmen	299
8	**Tarnen**	**301**
8.1	Verschleiern	301
	Dateien angleichen	301
	Dateien binden	305
8.2	Verstecken	305
	Dateien, Verzeichnisse und Dateisysteme	306
	Steganographie	312
	Rootkits	318

8.3	Verwischen	323
8.4	Entdecken	323
	Checksums	323
	ADS	326
	Steganographie	327
	Rootkits	328
9	**Schöne neue Welt ...**	**331**
9.1	Zertifikate	331
9.2	Signaturen	333
9.3	Authentifikation	334
	Client-Authentifikation	334
	Server-Authentifizierung	336
9.4	Public-Key-Infrastruktur	338
	Asymmetrische Verschlüsselungsverfahren	339
	Ein Ausflug in die Komplexitätstheorie ...	339
9.5	Ausblick	344
10	**Epilog**	**347**
A	**Anhang**	**351**
A.1	Tools	351
	Reconnaissance	351
	Scanner	353
	Enumeration	354
	Angriffswerkzeuge	355
	Tarnwerkzeuge	356
	Sniffer	357
	Administrationswerkzeuge	357
	Weitere Werkzeuge	358
A.2	Abkürzungsverzeichnis	359
	Stichwortverzeichnis	**363**

Vorwort

Über die Notwendigkeit des ethischen Hackers

Internetsicherheit ist ein Thema, das man inzwischen nicht mehr auf ein „Firewall einschalten und dann kann eigentlich nicht mehr viel passieren" reduzieren kann. Es ist ein ernstes Problem, das nicht nur Unternehmen in ihrer Existenz bedrohen kann, sondern auch Privatpersonen (existentiell) betrifft. Auch wenn die Gefahren bereits seit vielen Jahren bekannt sind und ausführlich thematisiert wurden, jeder Administrator entsprechend sensibilisiert ist und jede Menge zuverlässiger Schutzmechanismen in allen Preisklassen zur Verfügung stehen, gibt es seit einiger Zeit eine neue, beunruhigende Komponente: Die Dimension der Bedrohung und deren Intensität. Bestand die Bedrohung vor Jahren noch aus E-Mail-Viren, die „nur" Dateien löschten, Trojanern, die Hintertüren für weitere Angriffe öffneten, oder eher sporadischen Einbrüchen von „Hackern", ist die Bedrohung heutzutage kaum noch sichtbar, da die Attacken immer raffinierter und zielgerichteter durchgeführt werden. War bei den „Hackern der 1. Generation" oft die technische Herausforderung die Motivation für das Überwinden von Firewalls und das Ausspionieren von Passwörtern durch „Social Engineering", steht hinter den Angriffen in den letzten Jahren immer mehr die organisierte Kriminalität. Alleine das Phishing, vor ein paar Jahren noch eine eher kuriose Randerscheinung im Internet, verursachte 2007 in Deutschland einen Schaden von mehreren Millionen Euro. Heutige Angriffe zeichnen sich dadurch aus, dass sie unauffällig sind und das „Wirtssystem" nicht schädigen. Harmloser sind sie dadurch nicht geworden, im Gegenteil.

Internetsicherheit ist daher ein Thema, das uns alle angeht, und das man nicht alleine den Sicherheitsexperten überlassen darf, von denen es nach wie vor viel zu wenige gibt. Wir brauchen vor allem mehr „ethische Hacker", die Schwachstellen in Systemen aufdecken, dafür sorgen, dass sie gar nicht erst auftreten, und Firmen, aber auch Privatanwender bei der Frage beraten, wie Sie sich am wirkungsvollsten vor den Gefahren aus dem Internet schützen können. Das Buch „Ethical Hacking" von Manu Carus beschreibt keinen neuen Modetrend oder ein Thema, das nur für technikverliebte IT-Spezialisten eine Bedeutung haben könnte. Es dreht sich um ein Thema, das uns alle angeht. Vor allem (ausnahmslos) jene, zu deren Aufgabe es gehört, ein Netzwerk zu betreuen und damit sicher zu machen. Wie so oft bei globalen Gefahren setzt ein wirkungsvoller Schutz voraus, dass man sowohl über die Gefahren als auch über mögliche Abwehrmöglichkeiten und Gegenmaßnahmen sachlich und objektiv informiert ist. Oder mit den Worten des Autors: „Wer sein Netzwerk vor Hackern schützen möchte, muss wie ein Hacker denken." Das Besondere an dem Buch ist, dass es nicht nur auf eine überaus verständliche Art und Weise die technischen Hintergründe schildert und Techniken wie Scanning oder Footprinting erläutert und die wichtigsten Werkzeuge vorstellt, sondern Administratoren und Systembetreuern Hilfsmittel an die Hand gibt, die sie einsetzen können, ohne einen tiefergehenden technischen Background besitzen zu müssen. Hilfe

zur Selbsthilfe in einem Bereich, in dem es geradezu sträflich fahrlässig wäre zu glauben, man sei von der realen Bedrohung durch kriminelle Hacker nicht betroffen.

Ich kenne den Autor seit vielen Jahren und habe sein technisches Verständnis, vor allem aber die Fähigkeit, sich an speziellen technischen Probleme gerade festbeißen zu können und dabei nicht eher locker zu lassen, bis das Problem gelöst ist, mehr als einmal zu schätzen gelernt. Der Autor versteht sich aber nicht nur als Informatiker, IT-Spezialist und Autor mit der Gabe, technisch komplizierte Vorgänge anschaulich zu erklären, sondern er ist selber ein (zertifizierter) ethischer Hacker. Eine bessere Kombination kann es für dieses Thema nicht geben.

Ich wünsche Ihnen eine genauso anregende wie informative Lektüre und bin mir sicher, dass Sie es nicht beiseite legen werden, ohne Ihr Unternehmensnetzwerk anhand der vorgestellten Methoden noch einmal gründlich zu checken. Und sollten Sie sich zum ersten Mal mit dem Thema beschäftigen: Einen besseren Einstieg kann es nicht geben.

Peter Monadjemi

Autor, Trainer und Chefredakteur des dot.net magazin

Über den Inhalt dieses Buchs

Dieses Buch ist „anders“.

Der Leser findet in diesem Buch keine Schritt-für-Schritt-Anleitung zur Absicherung seines Computersystems oder seines Netzwerks. Auch wird in diesem Buch nicht die neueste Sicherheitssoftware vorgestellt. Dieses Buch stellt des Weiteren keine APIs oder Frameworks vor, mit deren Hilfe bestimmte Sicherheitsmechanismen implementiert werden können.

Das Ziel dieses Buches besteht darin, zum „Anders-Denken“ anzuregen.

Die erfolgreichsten Angriffsstrategien sind das Ergebnis intelligenter Analysen. Dabei sucht der Angreifer nach „unkonventionellen“ Wegen, um einen Benutzer oder ein System zu „überrumpeln“. Einfache Fragestellungen zeigen dem Angreifer mögliche Wege auf, um unbemerkt einbrechen zu können:

- Wie verhält sich ein System in einer bestimmten Fehlersituation?
- Wie antwortet das System auf zufällig generierte Eingaben?
- Wie geht das System mit Massendaten um?
- Welche Erkenntnisse können durch Dekompilierung[1] gewonnen werden?
- Wie nutzt der normale Anwender das System?
- Was passiert, wenn man sich nicht an die vorgegebenen Abläufe hält?

1. Dekompilierung beschreibt den Vorgang, aus einer Maschinensprache oder „Intermediate Language“ wieder lesbaren Quellcode in einer Hochsprache zu gewinnen, beispielsweise in Java oder C#.

- Welche Informationen sind „da draußen“ verfügbar, mit denen Erkenntnisse über ein System und seine Benutzer gewonnen werden können?
- Welche Schwachstellen haben andere Angreifer gefunden, und wie können deren Angriffsstrategien modifiziert und verbessert werden?

Aus den gewonnenen Erkenntnissen können Verfahren und Tools abgeleitet werden, die Angreifern die Kontrolle über fremde Rechner ermöglichen.

Der Schutz eines Computersystems oder eines Netzwerks besteht nicht allein in der Installation geeigneter Sicherheitssoftware. Vielmehr liegt die Verantwortung für die Absicherung eines Systems bei dem Besitzer selbst. Wie aber kann sich dieser über die Sicherheitssoftware von Experten-Firmen hinaus absichern? Die Antwort ist ganz einfach: „Anders denken“! Und genau hier fängt dieses Buch an: sich in die Rolle eines Angreifers versetzen, um mit den so gewonnenen Ideen und Erkenntnissen geeignete Absicherungsmaßnahmen einleiten zu können!

Dieses Buch stellt die Vorgehensweisen professioneller Angreifer vor. Es zeigt, mit welch einfachen Mitteln sowohl gewöhnliche Computeranwender als auch geschulte Systemadministratoren überrumpelt werden können. Aus den dargestellten Verfahren werden geeignete Gegenmaßnahmen abgeleitet. Vor allem aber zielt der Inhalt dieses Buches darauf ab, den Leser aufzurütteln, aufzuwecken und misstrauischer werden zu lassen. Erst mit dieser Grundeinstellung ist nach heutigem Stand ein nachhaltiger Schutz vor professionellen, methodisch ausgeführten Angriffen möglich.

An wen sich dieses Buch wendet

Sicherheit betrifft jeden, der Computer und Netzwerke zum Austausch von Information nutzt: Unternehmen, Privatanwender, Software- und Hardware-Hersteller, Organisationen und viele mehr.

Nicht nur aus diesem Grund richtet sich dieses Buch an Entwickler, technische Designer, Projektleiter, Tester und Administratoren aller Systeme und Hersteller; an Berater, Freiberufler und Angestellte; an interessierte Privatanwender sowie an professionelle Sicherheitsexperten.

Vielmehr sind die dargestellten Ideen und Verfahren für jeden interessant, der mit Software, Rechnern und Netzwerken zu tun hat. Sie helfen, die Architektur von Rechnern und Netzwerken zu verstehen, Schwächen in der Spezifikation von Protokollen nachzuvollziehen und zu lernen, in welch frühem Fortschrittsstadium der Sicherheitstechnologie sich die IT-Branche zum aktuellen Zeitpunkt befindet.

Was zum Verständnis dieses Buchs benötigt wird

Der Autor hat sich alle Mühe gegeben, die teilweise sehr komplexen Zusammenhänge von Protokollen, Angriffsstrategien und Architekturen allgemein verständlich darzustellen. Der Leser erfährt über den grundlegenden Aufbau des Internets und seiner Komponenten, lernt Netzwerkprotokolle, DNS-Server und Proxy-Server kennen und wird bis in die tiefsten Ebenen des TCP-Protokolls eingeführt.

Dennoch reicht ein grundlegendes Interesse an IT-Sicherheit für das Verständnis dieses Buches vollkommen aus. Wer also die Begriffe *IP-Adresse*, *TCP/IP*, *Trojaner* und *Passwort-Richtlinien* einordnen kann, ist bestens gerüstet und lernt nicht nur die wichtigsten Hacker-Tools kennen, sondern versteht auch die Schwächen der heutigen Internet-Architektur und blickt bis hinter die Kulissen der Theoretischen Informatik, die sich mittels moderner Verschlüsselungsmethoden der Verbesserung der Sicherheitsinfrastruktur verschreibt.

Wie dieses Buch strukturiert ist

Dieses Buch führt den Leser in die Welt des Hackings ein. Mit schrittweise steigender Komplexität werden die gängigen Angriffsstrategien und die dabei eingesetzten Werkzeuge vorgestellt. Der umfangreichste Teil dieses Buches beschreibt den methodischen, professionellen Einbruch in die Netzwerke und Computersysteme vermeintlich gut geschützter Unternehmen.

Kapitel 1 wirft einen Blick auf die kriminelle (Miss-)Nutzung des Internets und klärt über die beteiligten Personen und die geltende Rechtsprechung auf. Der Leser lernt die Bedeutung gängiger Fachbegriffe und kann den Begriff des „Ethical Hackings" einordnen und abgrenzen. Das Kapitel beleuchtet, warum ein Zielsystem so einfach, schnell und unbemerkt angegriffen werden kann. Dabei werden die im Internet eingesetzten Protokolle untersucht und grundlegende Architekturschwächen analysiert. Abschließend wird am Beispiel einer Spam-Mail der Versuch unternommen, den Absender zurückzuverfolgen, um anschließend zu der Erkenntnis zu gelangen, dass die Anonymität seiner Benutzer eines der grundlegendsten Probleme des Internets ist.

Kapitel 2 beleuchtet die Auseinandersetzung zwischen Hackern und Sicherheitsverantwortlichen. Der Leser erfährt, wer angegriffen wird, was angegriffen wird, welcher Schaden dabei entsteht und wie Hacker vorgehen. Dabei wird auf die Opfer-Rolle von Privatanwendern und Unternehmen eingegangen sowie die Täter-Rolle der Angreifer untersucht. Im Detail wird beschrieben, mit welchen Mitteln und Werkzeugen Privatanwender „gehackt" werden. Der Leser erfährt, wie Trojaner erstellt werden, wie Spam-Mails verteilt werden, wie Phishing-Sites entstehen, wie Viren und Würmer in Umlauf geraten und wie Spyware zum Ausspionieren eingesetzt wird. Obwohl dieses Buch den Schwerpunkt auf professionelle Einbrüche in Unternehmensnetzwerke setzt, werden einfache Gegenmaßnahmen vorgestellt, mit denen sich Privatanwender wirksam vor solchen Gefahren schützen können.

Kapitel 3 stellt ein gängiges Vorgehensmodell für den professionellen Einbruch in ein Unternehmensnetzwerk vor. Anhand mehrerer Beispiele wird dem Leser illustriert, unter Einsatz welcher Mittel der Angreifer sein Opfer auskundschaftet und abtastet, bevor er den eigentlichen Angriff lanciert und sich auf dem Zielsystem festsetzt. Dabei lernt der Leser grund-

sätzliche Terminologien wie „Network Scanning“, „Port Scanning“ und „Vulnerability Scanning“ kennen und kann diese abgrenzen. Das Kapitel gibt einen Überblick über die eingesetzten Verfahren und Methoden, die in den nachfolgenden Kapiteln erst ausführlich beschrieben werden.

Kapitel 4 widmet sich dem Auskundschaften eines Opfers. Der große Umfang dieses Kapitels wird dem Aufwand gerecht, den ein Angreifer in dieser Vorbereitungsphase betreibt. Der Leser lernt, wo sich Angreifer wertvolle Informationen über ihre Opfer frei beschaffen können und wie sie sich gleichzeitig vor der eigenen Entdeckung schützen. Die dabei eingesetzten Tools werden anhand von Beispielen vorgestellt. Der Leser erfährt die Funktionsweise von whois- und Nameservern, also grundlegender Komponenten des Internets. Durch die beispielhafte Durchmessung von Netzwerkrouten lernt der Leser die Protokolle TCP, UDP und ICMP kennen. Insgesamt ergibt sich dem Leser in diesem Kapitel ein Eindruck, welche Puzzle-Teile zusammengesetzt werden müssen, um sich ein umfassendes Bild von einem Unternehmen und seinem Netzwerk machen zu können. Das Kapitel schließt mit einer Auflistung wirksamer Gegenmaßnahmen ab, die Unternehmen vor der Veröffentlichung zu vieler, sensibler Informationen schützen.

Kapitel 5 stellt die grundlegenden Methoden zum Abtasten eines Zielnetzwerks vor. Der Leser erfährt anhand zahlreicher Beispiele, wie ein Angreifer ein Zielnetzwerk durchleuchten kann und dabei detaillierte Informationen über aktive Geräte, installierte Betriebssysteme und mögliche Schwachstellen erhält. Der Leser lernt Scanning-Tools wie beispielsweise NMAP anwenden und verstehen. Im Detail geht dieses Kapitel auf die Funktionsweise der einzelnen Abtaststrategien ein. Dabei wird das TCP-Protokoll vorgestellt, so dass der Leser unter Kenntnis des Aufbaus von TCP-Paketen die Wirkungsweise spezieller Abtasttechniken nachvollziehen kann. Zahlreiche Beispiele runden das Kapitel ab. Insbesondere wird dieses Kapitel dem hohen Stellenwert des „Vulnerability Scanning“ gerecht: Es werden öffentliche Datenbanken zur Verwaltung bekannter Schwachstellen beschrieben und deren Kataloge untersucht. Anschließend wird die Funktionsweise von Vulnerability Scannern vorgestellt. Ausführliche Fallstudien der relevantesten Werkzeuge und ihres Funktionsumfangs runden das Kapitel ab, ebenso eine Darstellung von Gegenmaßnahmen, mit denen Unternehmen sich vor dem Abtasten sensibler Rechner schützen und eventuelle Angriffsversuche bemerken können.

In *Kapitel 6* erfährt der Leser, wie ein Angriff ausgeführt wird. Es werden verschiedene Verfahren zum „Cracken“ von Passwörtern vorgestellt. Der Leser lernt, wie schnell und effizient einfache Passwörter gebrochen werden können und wie wichtig im Gegenzug die Anwendung von Kennwort-Sicherheitsrichtlinien für den Schutz eines Unternehmens sind. Statistiken zur „Berechnung“ von Passwörtern zeigen die zeitliche Komplexität und den erforderlichen Ressourcenbedarf, denen sich Angreifer ausgesetzt sehen. Als eine der wirksamsten Gegenmaßnahmen vor Angriffen werden dem Leser abschließend Richtlinien und Werkzeuge zur Erstellung und Verwaltung sicherer Passwörter vorgestellt.

Kapitel 7 beschreibt, wie sich der Angreifer nach einem erfolgreichen Angriff in dem Zielsystem festsetzt, um fortan einen leichten und unbehinderten Zugriff zu erhalten. Es wird die grundlegende Architektur einer Backdoor-Applikation vorgestellt und der Source-Code einer Server- und einer Client-Komponente analysiert. Abschließend werden Tools zur Fernsteuerung von Zielsystemen vorgestellt. Der Leser erfährt, wie eine Backdoor installiert wird, wie eine Web-Site verunstaltet wird und wie ein Rechner ferngesteuert werden kann.

Des Weiteren werden Verfahren und Werkzeuge vorgestellt, mit denen Backdoor-Applikationen abgewehrt und aufgedeckt werden können.

Gute Angreifer bleiben unentdeckt. In *Kapitel 8* erfährt der Leser, wie ein Angriff verschleiert wird und die installierten Hacker-Tools im Zielsystem versteckt werden. Es werden gängige Stealth Tools und Rootkits vorgestellt. Nach einem Ausflug in die Steganographie schließt das Kapitel mit der Vorstellung geeigneter Entdeckungs- und Gegenmaßnahmen ab.

Nach dem Durcharbeiten der vorangegangenen Kapitel hat der Leser erfahren, dass die Architektur heutiger Netzwerke und Protokolle keinen grundlegenden Schutz ermöglicht. Neue Sicherheitsmechanismen braucht die Welt! *Kapitel 9* unternimmt einen Ausflug in eine „Schöne neue Welt...". Dabei erfährt der Leser, was eine Public-Key-Infrastruktur ist und wie diese zu einem sicheren Austausch von Informationen beitragen kann. Auf leicht verständliche Weise lernt der Leser die theoretischen Grundlagen moderner Kryptosysteme sowie grundlegende Fragestellungen der Theoretischen Informatik kennen. Das Buch schließt mit einer Empfehlung ab, wie Netzwerke und Computersysteme nachhaltig abgesichert und ihre Benutzer ausreichend geschützt werden können.

Danksagung

Ein Buch über ein solch komplexes und übergreifendes Thema wie das des „Ethical Hackings" zu schreiben erfordert nicht nur die gründliche Arbeit des Autors, sondern insbesondere die Unterstützung einiger wichtiger Menschen, die zu diesem Buch beigetragen haben und bei denen ich mich besonders bedanken möchte.

Ich danke meiner Frau Nina: Du öffnest mir die Augen und zeigst mir den richtigen Weg. Unendlichen Dank für die Unterstützung, die du mir gibst! Ich liebe dich!

Ich danke meinen Söhnen Collin und Miles: Ihr schenkt mir Ablenkung und Aufmerksamkeit, wann immer ich sie brauche. Ihr habt mein Leben um ein Vielfaches bereichert!

Ich danke meinem Freund Peter: Du hast mich lange Zeit zu diesem Buch ermutigt und mich fortlaufend gefordert, Ausdauer, Mühe und Zeit für dieses Projekt aufzubringen. Dabei konnte ich weit über mich hinauswachsen! Vielen Dank für die liebevolle Geduld, die du aufgebracht hast, um mich an diesen Punkt meines Lebens zu führen.

Widmung

Ich widme dieses Buch von ganzem Herzen meiner tapferen Oma Gertrud, die mich vieles gelehrt hat; eines vor allem: den Dingen ein gesundes Maß an Mißtrauen entgegenzubringen.

Über den Autor

Manu Carus, geb. Manuel Lengert, ist als *Certified Ethical Hacker* bei der EC Council in New York registriert. Manu Carus veröffentlicht in regelmäßigen Abständen Fachartikel in den gängigen deutschsprachigen Fachmagazinen und ist Speaker auf verschiedenen Entwickler- und Security-Konferenzen.

Als Sicherheitsspezialist führt er Security-Audits und Penetrationtests für nationale und internationale Kunden durch. Seine Expertise können Sie für Sicherheitsberatung, Reviews, Tests und Audits buchen. Sie erreichen ihn unter *manu.carus@ethical-hacking.de*.

Der Inhalt dieses Buches ist auf einer Audio-CD erschienen! In knapp 50 Minuten Spielzeit wird der Hörer in die Welt des Hackings entführt und erfährt in einem spannenden Vortrag alles Wichtige über Angriffe und Gegenmaßnahmen. Die CD mit dem Titel „Ethical Hacking“ wird von der *Manufaktur IT GmbH* vertrieben und kann unter *www.ethical-hacking.de* bestellt werden.

1 Die Welt ist schlecht!

Als umfassende Informationsquelle dient das Internet nicht nur den „gewöhnlichen" Anwendern. Wer Information sucht, bekommt sie: im Guten wie im Schlechten! Während der unbedarfte Benutzer das Internet zum Recherchieren, Nachschlagen, Einkaufen, Versteigern, Mailen, Chatten und Bloggen nutzt, haben Andere das Internet längst für kriminelle Zwecke pervertiert: für die Ablage und den Austausch von Schadsoftware, für das Ausspionieren und das Fernsteuern fremder Computersysteme, für den Austausch gestohlener digitaler Identitäten.

Hacker regieren das Internet! Sie verteilen Schadsoftware und tarnen diese geschickt als Trojaner. Einmal installiert, richtet sich diese *Malware*, ausgestattet mit den vollen Rechten des betroffenen Eigentümers, als Hintertür für den Hacker auf dem befallenen Rechner ein und wartet auf dessen Befehle. Dem Hacker steht der kompromittierte Rechner unweigerlich zur freien Verfügung. Er kann auf die Systemressourcen des Rechners zugreifen oder den Rechner für Angriffe auf weitere Rechner nutzen.

Dieses Buch gibt einen tiefen Einblick in die Welt des „Hackings" und geht den folgenden Fragen nach:

- Was treiben Hacker im Internet?
- Welcher Schaden entsteht durch ihr Tun?
- Welche Ziele nehmen Hacker ins Visier?
- Warum ist Hacking so einfach?
- Wo liegen die Schwächen des Internets?
- Wie kann man diesen Schwächen wirksam begegnen?

Die einzelnen Kapitel dieses Buchs beschreiben, wie die Rechner von Privatanwendern in die Kontrolle von Hackern übergehen, wie Unternehmensserver gekapert werden und welche Werkzeuge und Verfahrensweisen dabei zum Einsatz kommen. Der Leser nehme bitte dringend die nachfolgenden Ausführungen zur aktuellen Rechtslage und den Gesetzen der Computerethik zur Kenntnis.

1.1 Rechtsprechung und Ethik

Ohne jegliche Programmierkenntnisse lassen sich Phishing-Sites erstellen, Passwörter knacken, Viren, Würmer und Schadsoftware erstellen. Ermöglicht wird dies durch zahlreiche Hacking-Tools, die frei im Internet verfügbar sind. Jeder Skript-Kiddie ist mit Hilfe dieser Werkzeuge in der Lage, immensen Schaden herbeizuführen.

In diesem Buch wird gezeigt, wie Hacker vorgehen und welcher Werkzeuge sie sich bedienen. Die vorgestellten Verfahren sollen dem Computernutzer verdeutlichen, welcher Gefahr er sich aussetzt, sobald er sich mit dem Internet verbindet. Sie zeigen auf, welche Informationen über ihn und seine Systeme im Internet für Dritte verfügbar sind.

> *Der Leser sei sich darüber bewusst, dass die in diesem Buch vorgestellten Werkzeuge und Verfahren nicht ohne die ausdrückliche, schriftliche Genehmigung des Eigentümers und des Betreibers der betroffenen Netzwerke und Computer angewendet werden dürfen!*

Die in diesem Buch beschriebenen Beispiele beziehen sich nicht auf Echtsysteme; stattdessen wurden die in den Abbildungen aufgeführten Hostnamen, IP-Adressen und Benutzerkonten frei erfunden. Eventuelle Übereinstimmungen mit realen Geräten und Angaben wären rein zufällig.

1.1.1 Aus dem Strafgesetzbuch

Hacking ist strafbar. Daher regelt das Deutsche Strafgesetzbuch (StGB) die Konsequenzen illegalen Tuns:

§ 202a: Ausspähen von Daten

(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Daten im Sinne des Absatzes 1 sind nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

§ 202b: Abfangen von Daten

Wer unbefugt sich oder einem anderen unter Anwendung von technischen Mitteln nicht für ihn bestimmte Daten (§ 202a Abs. 2) aus einer nichtöffentlichen Datenübermittlung oder aus der elektromagnetischen Abstrahlung einer Datenverarbeitungsanlage verschafft, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft, wenn die Tat nicht in anderen Vorschriften mit schwererer Strafe bedroht ist.

§ 202c Vorbereiten des Ausspähens und Abfangens von Daten

(1) Wer eine Straftat nach § 202a oder § 202b vorbereitet, indem er

1. Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten (§ 202a Abs. 2) ermöglichen, oder

   Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.

(2) § 149 Abs. 2 und 3 gilt entsprechend.

§ 303a: Datenveränderung

(1) Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

(3) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 303b: Computersabotage

(1) Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, dadurch erheblich stört, dass er

1. eine Tat nach § 303a Abs. 1 begeht,
2. Daten (§ 202a Abs. 2) in der Absicht, einem anderen Nachteil zuzufügen, eingibt oder übermittelt oder
3. eine Datenverarbeitungsanlage oder einen Datenträger zerstört, beschädigt, unbrauchbar macht, beseitigt oder verändert,

wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Handelt es sich um eine Datenverarbeitung, die für einen fremden Betrieb, ein fremdes Unternehmen oder eine Behörde von wesentlicher Bedeutung ist, ist die Strafe Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe.

(3) Der Versuch ist strafbar.

(4) In besonders schweren Fällen des Absatzes 2 ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. Ein besonders schwerer Fall liegt in der Regel vor, wenn der Täter

1. einen Vermögensverlust großen Ausmaßes herbeiführt,
2. gewerbsmäßig oder als Mitglied einer Bande handelt, die sich zur fortgesetzten Begehung von Computersabotage verbunden hat,
3. durch die Tat die Versorgung der Bevölkerung mit lebenswichtigen Gütern oder Dienstleistungen oder die Sicherheit der Bundesrepublik Deutschland beeinträchtigt.

(5) Für die Vorbereitung einer Straftat nach Absatz 1 gilt § 202c entsprechend.

§ 303c: Strafantrag

In den Fällen der §§ 303, 303a Abs. 1 und 2 sowie § 303b Abs. 1 bis 3 wird die Tat nur auf Antrag verfolgt, es sei denn, dass die Strafverfolgungsbehörde wegen des besonderen öffentlichen Interesses an der Strafverfolgung ein Einschreiten von Amts wegen für geboten hält.

Problematik in der geltenden Rechtsprechung

Die besondere Problematik der aktuellen Rechtssituation wird in § 303c des StGB ausgedrückt: Eine kriminelle Tat im Internet wird nur auf Strafantrag verfolgt. Das heißt, ein Hacker, der Daten unbefugt gelesen, abgefangen, geändert oder gelöscht hat, muss auf

frischer Tat ertappt werden. Darin unterscheidet sich die Rechtsprechung zwar nicht grundsätzlich gegenüber der herkömmlichen Kriminalität. Aber die Mittel, mit denen digitale Spurensicherer, die sog. *IT-Forensiker*, ausgerüstet sind, stellt sie vor eine fast unmögliche Aufgabe:

- Das Internet gestattet jedem Benutzer einen weitgehend anonymen Zugriff auf alle bereitgestellten Ressourcen. Somit erscheint es fast unmöglich, Einbrüche und Diebstähle bis zu ihrem Verursacher zurückzuverfolgen.
- Die in Netzwerken eingesetzten Standard-Protokolle zwingen die an einer Kommunikation beteiligten Parteien nicht zur Authentifikation. Zwar melden sich die Benutzer an einem POP3-, SMTP- oder FTP-Dienst mit einem Benutzernamen und einem Passwort an. Jedoch werden diese Angaben erstens im Klartext an den Server übertragen, und zweitens können die Benutzer aufgrund von Hacker-Angriffen nicht absolut sicher sein, dass sie wirklich mit dem gewünschten Server kommunizieren. Andere Protokoll-Erweiterungen wie beispielsweise HTTPS verschlüsseln die übertragenen Inhalte, erzwingen aber nicht die Authentizität der an einer Kommunikationsverbindung beteiligten Parteien. Der Benutzer muss keinen Benutzernamen und kein Passwort angeben, um eine HTTPS-Verbindung herzustellen, und der adressierte Server muss sich seinerseits auch nicht bei dem Benutzer ausweisen. Zwar repräsentiert ein SSL-Zertifikat die Authentizität des Servers. Wer jedoch glaubt, damit ausreichend abgesichert zu sein, möge einen aufmerksamen Blick in das Kapitel 2 dieses Buches werfen.
- Für die existierenden Standardsysteme, zum Beispiel Mail-Server, FTP-Server und Web-Server, gibt es keine gesetzlichen Vorgaben für die Protokollierung der durchgeführten Kommunikation. Der mangelnde Zwang führt in der Praxis dazu, dass es kaum möglich ist, den Verlauf eines Internet-Pakets posthum von seinem Empfänger zu seinem Absender zurückzuverfolgen.
- Die geltenden Datenschutzbestimmungen zwingen die Telekommunikationsunternehmen darüber hinaus, ihre Log-Files in regelmäßigen Abständen zu löschen. Die meisten Provider löschen ihre Aufzeichnungen aufgrund der entstehenden Datenmasse in sehr schnellen Abständen, teilweise wöchentlich. Da der Einbruch eines Hackers jedoch meist Monate später, wenn überhaupt, entdeckt wird, besteht eine hohe Wahrscheinlichkeit, dass Forensiker nicht mehr auf die Log-Dateien der Unternehmenssysteme zugreifen können. Der Hacker bleibt unerkannt, der Einbruch ohne Rechtsfolgen ...

1.1.2 Computer-Ethik

Über die geltende Rechtsprechung hinaus hat jeder Computernutzer eine ethische Verantwortung für sich und sein Umfeld zu tragen. Der Autor appelliert daher dringend an den Leser, die vom *Computer Ethics Institute*[1] festgeschriebenen „Gebote der Computer-Ethik“ strikt einzuhalten.

1. Computer Ethics Institute: *http://www.brook.edu/its/cei/cei_hp.htm*

Achtung

Die „Zehn Gebote der Computer-Ethik“:

1. Du sollst einen Rechner nicht benutzen, um anderen zu schaden.
2. Du sollst die elektronische Arbeit anderer nicht beeinträchtigen.
3. Du sollst nicht in den Dateien anderer herumschnüffeln.
4. Du sollst einen Computer nicht benutzen, um zu stehlen.
5. Du sollst einen Computer nicht benutzen, um falsches Zeugnis abzulegen.
6. Du sollst proprietäre Software, für die du nicht bezahlt hast, nicht benutzen oder kopieren.
7. Du sollst die Computer-Ressourcen anderer nicht ohne Erlaubnis oder angemessenes Entgelt einsetzen.
8. Du sollst dir nicht die intellektuellen Arbeitsergebnisse anderer unbefugt aneignen.
9. Du sollst dir über die sozialen Konsequenzen des Programms, das du schreibst, oder der Software, die du gestaltest, im Klaren sein.
10. Du sollst einen Computer stets mit Rücksicht auf und mit Respekt für andere Menschen benutzen.

1.2 Hacker

Die Bezeichnung „Hacker“ wird meist missverstanden. Was in der allgemeinen Sprache negativ klingt, meint eigentlich hochversierte Computerfreaks. Menschen, die sich mit Computersystemen beschäftigen und besonders neugierig sind; Menschen, die Herausforderungen lieben und gerne Neues erlernen. Einen Hacker zeichnet es aus, kreativ zu sein: eigene Ideen zu entwickeln, Neues zu schaffen und die eigenen Fertigkeiten möglichst einfallsreich einsetzen zu können. Hacker nehmen gerne harte Arbeit in Kauf, um ihre Ziele zu erreichen und teilen ihr Wissen und ihre Meinung mit ihresgleichen. Alles in allem durchaus positive Attribute, die sich so manches Unternehmen von ehrbaren Mitarbeitern wünscht ...

Eine spezielle Gruppierung unter Hackern stellt die Gruppe der kriminellen *Cracker* dar: diejenigen Freaks, die dem Begriff „Hacker“ heute ein besonders negatives Image bescheren. Sie brechen in Netzwerke und Computersysteme ein, spionieren Daten aus und „knacken“ Passwörter.

Abbildung 1.1 ordnet Hacker den jeweiligen Gruppen zu:

Abbildung 1.1: Hacker

1.2.1 Black Hats

Black Hats nutzen ihre Fähigkeiten mit krimineller oder destruktiver Absicht. Sie stehlen vertrauliche Daten und bereichern sich daran. Sie verändern fremde Software, um einen Kopierschutz aufzuheben oder unbemerkt eine Schadsoftware anzuhängen. Sie modifizieren Web-Sites, um deren Vertrauenswürdigkeit zu beeinträchtigen. Sie stehlen digitale Identitäten, um sich im Namen anderer Vorteile zu verschaffen. Sie stören die Verfügbarkeit von Diensten mittels Denial-of-Services-Angriffen.

1.2.2 White Hats

White Hats nutzen ihre Fähigkeiten ausschließlich für defensive Zwecke. Meist handelt es sich um unabhängige Security-Consultants, die die Sicherheit in der Infrastruktur eines Unternehmens analysieren und unterstützende Maßnahmen einrichten.

1.2.3 Gray Hats

Gray Hats interessieren sich für die Entdeckung und Publizierung von Schwachstellen. Sie vertreten die Ansicht, dass die Software- und Hardware-Hersteller selbst für die Sicherheit ihrer Produkte zuständig sind und überlassen es dem Schicksal, ob die von ihnen veröffentlichten Informationen im Guten oder im Schlechten eingesetzt werden.

1.3 Ethical Hacker

Sei es intellektueller Spieltrieb, Profilierungsdrang oder kriminelle Energie: Hacker sammeln Informationen über die Schwachstellen von Systemen und veröffentlichen diese innerhalb ihrer Community.

Ein Hacker, der sich mit ausdrücklichem Auftrag der Sicherheitsverantwortlichen eines Unternehmens dafür einsetzt, das Unternehmen vor Angriffen zu schützen, wird als *Ethical Hacker* bezeichnet. Ein solcher Hacker verhält sich ethisch korrekt: Er schadet dem Unternehmen nicht und stiehlt auch keine Information. Es ist sein Anliegen, die Integrität und Vertrauenswürdigkeit der Systeme eines Unternehmens zu festigen. Geht er dabei besonders methodisch vor, besteht eine gute Chance, die Auswirkungen bösartiger Angriffe bereits im Testbetrieb auszuwerten, mit dem Ziel, noch vor der Produktivstellung neuer Software oder Änderungen in der Netzwerkkonfiguration einen höheren Sicherheitsgrad zu erreichen.

Ein *Ethical Hacker* wendet die in der Hacker-Community üblichen Methoden und Techniken an. Je nach persönlichem Hintergrund kann es sich um einen *White Hat*, einen *Gray Hat* oder gar einen *Black Hat* handeln, wichtig ist lediglich der gemeinsame Ansatz: die Verwendung gleicher Vorgehensweisen und Denkweisen.

Im Rahmen der Sicherheitsanalyse stellt der ethische Hacker die folgenden Fragen:

- Was kann ein Eindringling auf dem Zielsystem sehen?
- Welche Server und Devices sind für ihn sichtbar?

- Welche dieser Geräte sind für ihn erreichbar?
- Wie kann der Eindringling die gewonnene Information gegen das Unternehmen einsetzen?
- Sind seine Versuche und Erfolge in den Systemen nachvollziehbar?
- Welche Systeme sind im Unternehmen zu schützen?
- Gegen wen oder was muss geschützt werden?
- Welcher Schutz ist jeweils angemessen?
- Welches Budget stellt das Unternehmen für ausreichenden Schutz bereit?

Die Aufgabe des ethischen Hackers besteht darin, die Systeme eines Unternehmens hinsichtlich der bis dato bekannten Hacking-Angriffe abzusichern. Da ein vollständiger Schutz vor neuen Spielarten und Angriffen grundsätzlich nicht möglich ist, bemüht er sich des Weiteren um die Installation von Detect-, Alert- und Log-Mechanismen, um eventuelle Einbrüche bis zum Verursacher zurück nachvollziehen zu können.

Ethical Hacking kann wesentlich zu einem effektiven Schutz des Unternehmens beitragen. Anstatt sich auf die Sicherheitsmechanismen der eingekauften Standardsysteme zu verlassen, bricht der ethische Hacker im Auftrag des Unternehmens in dessen Netzwerke und Computersysteme ein. Mit der gleichen Hartnäckigkeit eines böswilligen Angreifers penetriert der ethische Hacker das Unternehmensnetzwerk und sucht eine Lücke, über die er einbrechen kann. Er tastet alle von außen und innen erreichbaren Geräte ab und versucht die darauf installierten Betriebssysteme und Dienste zu ermitteln. Hat er eine Sicherheitslücke gefunden, verschafft er sich einen Zugriff auf das betroffene System und hinterlässt dort als Beweis für den Auftraggeber eine Nachricht.

Bei diesem als *Penetrationstest* bezeichneten Vorgehen achtet der ethische Hacker besonders darauf, produktiv laufende Dienste nicht zu beeinträchtigen. So werden Angriffe, die auf die Terminierung bestimmter Dienste abzielen, ausschließlich auf Testsystemen durchgeführt. Buffer Overflows, Denial-of-Service-Angriffe und Wurmattacken werden in einem abgeschotteten Testnetzwerk durchgeführt. Um gleiche Produktionsbedingungen zu schaffen, muss die gleiche Hardware und Netzwerkkonfiguration wie auf der Produktionsumgebung eingesetzt werden; dies betrifft Firewalls, Router, Switches, Datenbanken, Web-Server, Mail-Server, FTP-Server u.v.m.

Hacking kann also durchaus ethisch sein!

Was wie ein Widerspruch in sich klingt, ist eine ausgezeichnete Methode, sich gegen bösartige Angriffe abzusichern. Sich nicht auf die Features der eingekauften Systeme zu verlassen, sondern die eigene Infrastruktur zu hinterfragen und ausreichend zu testen, schafft eine solide Basis für mehr Sicherheit. Denn Angreifer interessieren sich in der Regel nicht für das Netzwerk eines bestimmten Unternehmens, auf das sie es abgesehen haben: Sie tasten stattdessen das Internet nach ihnen bekannten Schwachstellen ab und greifen dort an, wo sich ein schneller Erfolg mit wenig Aufwand verspricht!

Wer also sein Netzwerk wirksam vor Hackern schützen möchte, muss selbst wie ein Hacker denken ...

1.4 Spion gegen Spion

Die gegenwärtige Sicherheitspraxis ist für alle Beteiligten unbefriedigend: Auf jede neue Softwareversion antwortet die Hacker-Community mit mindestens einer neuen Schwachstelle. Administratoren spielen Patches ein, und der Kreislauf beginnt von Neuem. Ein Dauerlauf im Hamsterrad, ein ewiges Kräftemessen zwischen *Black Hats* und *White Hats*. Das Aufrüsten zweier Lager, bei dem die eingesetzten Methoden und Werkzeuge immer ausgeklügelter werden ...

Dabei ist das Kräfteverhältnis zwischen den Beteiligten unausgewogen: Während ein *Black Hat* nur eine einzige Sicherheitslücke aufzufinden braucht, um sich einen Zugriff auf das Netzwerk- oder Computersystem zu verschaffen, tragen *White Hats* die Verantwortung, ihre Systeme „rundherum abzudichten".

Wie kann ein Netzwerk grundlegend abgesichert werden? Wie schützt man sich vor Schwachstellen? Wie erreicht man eine sichere Infrastruktur?

Ein Blick auf die Architektur des Internets zeigt, dass das Internet für die Bedürfnisse der modernen Gesellschaft längst nicht mehr geeignet ist ...

1.5 Das Internet braucht eine Revolution ...

1.5.1 Die Geschichte des Internet

Das Internet entstand im Jahre 1969 aus dem *ARPANET*, einem Projekt der *Advanced Research Project Agency* (ARPA) des US-Verteidigungsministeriums. Mit dem vorrangigen Ziel, ein verteiltes Kommunikationssystem für militärische Zwecke zu schaffen, entstand einige Jahre später eine Vernetzung von Universitäten und Forschungseinrichtungen zum Zweck des Austauschs von Dokumenten. Protokolle wie

- TCP/IP (*Transmission Control Protocol / Internet Protocol*)
- Telnet (*Teletype Network*)
- FTP (*File Transfer Protocol*)

haben ihren Ursprung in den Siebziger Jahren; die Protokolle

- SMTP (*Simple Mail Transfer Protocol*)
- HTTP (*HyperText Transfer Protocol*)
- POP (*Post Office Protocol*)
- DNS (*Domain Name System*)

entstammen den Achtziger Jahren.

In den Neunzigern wurde der erste graphische Webbrowser veröffentlicht, und mit der Freigabe des Netzes durch die *US-National Science Foundation* für kommerzielle Zwecke wurde das *World Wide Web* zu dem, was es auch heute noch ist: zu einem weltweiten Kommunikationsnetz, das zahlreiche geschäftliche und private Anwendungszwecke unterstützt und sich dabei auf veraltete Protokolle stützt!

1.5.2 Internet-Protokolle

Jede Datenübertragung im Internet erfolgt zunächst unverschlüsselt. Das Internet ist in seiner grundlegenden Architektur daher genauso unsicher wie eine Telefonleitung: Einfache „Abhöreinrichtungen“ wie bspw. Netzwerksniffer können ein vollständiges Klartext-Protokoll aller Daten erstellen, die über eine Netzwerkleitung übertragen werden. Abbildung 1.2 zeigt eine typische Netzinfrastruktur, die von einem solchen „Lauschangriff“ betroffen ist, sowie die beteiligten Komponenten und Protokolle.

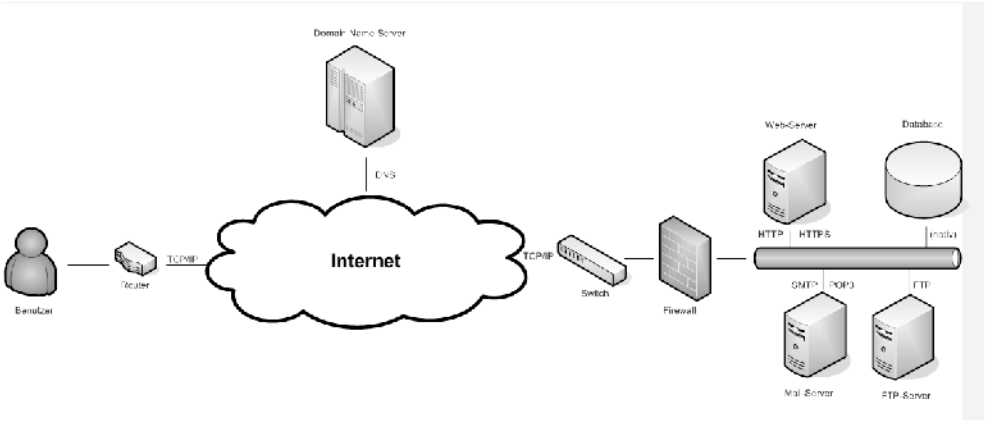


Abbildung 1.2: Internet-Protokolle

Erst 1994, also mit der Einführung des Sicherheitskonzepts *Secure Socket Layer* (SSL), erfuhren die bis dato standardisierten Internet-Protokolle einen Sicherheitsüberbau. Web-Seiten konnten endlich verschlüsselt übertragen werden, und der Versand von E-Mails und der Upload von Dateien erhielten einen optionalen Anmeldemechanismus.

Tabelle 1.1 gibt einen Überblick über die wesentlichen Protokollerweiterungen:

Protokoll	Bezeichnung
HTTPS	HTTP over SSL
Secure FTP	FTP over Secure Shell (SSH)
POP3S	POP3 over SSL
STARTTLS	Secure SMTP over TLS
PGP	Pretty Good Privacy
S/MIME	Secure Multipurpose Internet Mail Extensions

Tabelle 1.1: Sichere Internet-Protokolle

SSL bildet die Basis für sichere Internet-Protokolle. Mittlerweile unter der Bezeichnung *Transport Layer Security* (TLS) weiter entwickelt, spezifiziert SSL ein Verschlüsselungsprotokoll für Datenübertragungen im Internet. SSL wird vor allem in Verbindung mit HTTP eingesetzt (*HTTPS*), um die Übertragung von Web-Seiten und die Eingaben der User zwi-

schen Client und Server zu verschlüsseln. Für das Absenden und das Abfragen von E-Mails wurde gleich eine ganze Reihe von Protokollen angepasst:

- *STARTTLS* erweitert SMTP mit Hilfe von TLS um eine neue Serverantwort STARTTLS. Dabei zeigt der E-Mail-Server dem E-Mail-Client an, dass er die Option „verschlüsselte Kommunikation" anbietet. Der E-Mail-Client kann von dieser Option Gebrauch machen und sich im Laufe der Verbindung mit dem E-Mail-Server darauf verständigen, dass jede weitere Kommunikation in verschlüsselter Form erfolgen soll.
- *POP3 over SSL* bietet die gleiche Funktionalität für das POP3-Protokoll.
- *PGP* basiert nicht auf SSL, sondern implementiert ein PKI-Verfahren zur Verschlüsselung von Daten. PGP ist in der Open-Source-Community sehr beliebt.
- *S/MIME* stützt sich auf X.509v3-Zertifikate und standardisiert die Verschlüsselung und Signatur von E-Mails durch ein asymmetrisches Verschlüsselungsverfahren.
- FTP erhielt mit *Secure Shell* (SSH) einen Sicherheitsüberbau (*Secure FTP*), so dass die Anmeldung an einen FTP-Server nicht mehr im Klartext übertragen werden muss, sondern über eine gesicherte Verbindung transportiert werden kann. Allerdings wurde die Verschlüsselung nur auf das Anmeldeverfahren und nicht auf den Prozess des Datentransfers angewandt, so dass der Upload von Dateien über einen ungesicherten Port abläuft und nach wie vor „abgehört" werden kann.

Diese Protokollerweiterungen ermöglichen zwar jeweils eine Verschlüsselung der ausgetauschten Inhalte, das eigentliche Problem des Internets berücksichtigen sie jedoch nicht, wie der nächste Abschnitt zeigt.

1.5.3 Sicherheit im Internet

Die „neuen" Verschlüsselungsprotokolle haben die Sicherheit im Internet nicht nachhaltig verbessert. Da die alten Standards nicht verworfen und durch einen allumfassenden Sicherheitsansatz ersetzt wurden, basiert die heutige Internet-Sicherheit immer noch auf lückenhaften Altlasten. Die bestehenden Protokolle erhielten lediglich einen optionalen Überbau, der bei Bedarf genutzt werden kann. Somit konnte zwar gewährleistet werden, dass Änderungen an den Internet-Protokollen 100 Prozent kompatibel zu bestehender Hard- und Software bleiben. Das eigentliche Sicherheitsproblem des Internets, die Anonymität aller beteiligten Benutzer, wurde dabei aber nicht berücksichtigt.

Das in der Praxis zunächst bestehende Problem ist, dass die Anwendung der Sicherheitsmechanismen für die Internet-Protokolle optional ist. Es besteht kein Zwang! Aus diesem Grund werden E-Mails auch heute noch unverschlüsselt übertragen, und es ist ein Leichtes, die Benutzernamen und Passwörter bei der Anmeldung eines E-Mail-Clients an einem POP3-Server abzuhören und entsprechenden Missbrauch zu betreiben. Listing 1.1 zeigt eine beispielhafte POP3-Kommunikation, die im Klartext über eine Leitung gesendet wird:

```
(Der Server pop3.mustermann.de registriert einen TCP/IP-Port-Listener auf Port 110)
(Der Client öffnet eine TCP/IP-Verbindung zum diesem POP3-Server auf Port 110)
+OK Microsoft Exchange POP3 server version 5.0.1457.10 ready
USER max@mustermann.de
+OK
PASS goldfisch
+OK User successfully logged on
STAT
+OK 1 9876
LIST
+OK mailbox has 1 messages (9876 bytes)
1 9876
.
RETR 1
+OK message follows
Date: Wed, 15 Aug 2007 14:44:12 +0100
From: eBay <info@ebay.de>
To: max@mustermann.de
Subject: Newsletter
Content-Type: text/plain; charset=us-ascii; format=flowed
Content-Transfer-Encoding: 7bit

Sehr geehrter Herr Mustermann,
...
DELE 1
+OK message marked for delete
QUIT
+OK Microsoft Exchange POP3 server version 5.0.1457.10 signing off
```

Listing 1.1: Beispielhafte Anwendung des POP3-Protokolls

Für den „normalen“ Internet-Anwender ist nicht transparent, welche Protokolle die Applikationen im Hintergrund einsetzen. Er mag zwar an dem Sicherheitsschloss in der Fußleiste seines Browsers erkennen, dass seine Daten gesichert übermittelt werden, aber ihm ist nicht klar, dass seine E-Mails im Klartext übertragen werden. Er kann auch nicht wissen, dass seine Anmeldedaten im Klartext übertragen werden.

Die Abbildung 1.3 zeigt den Mitschnitt einer POP3-Anmeldung auf einer „abgehörten“ Leitung:

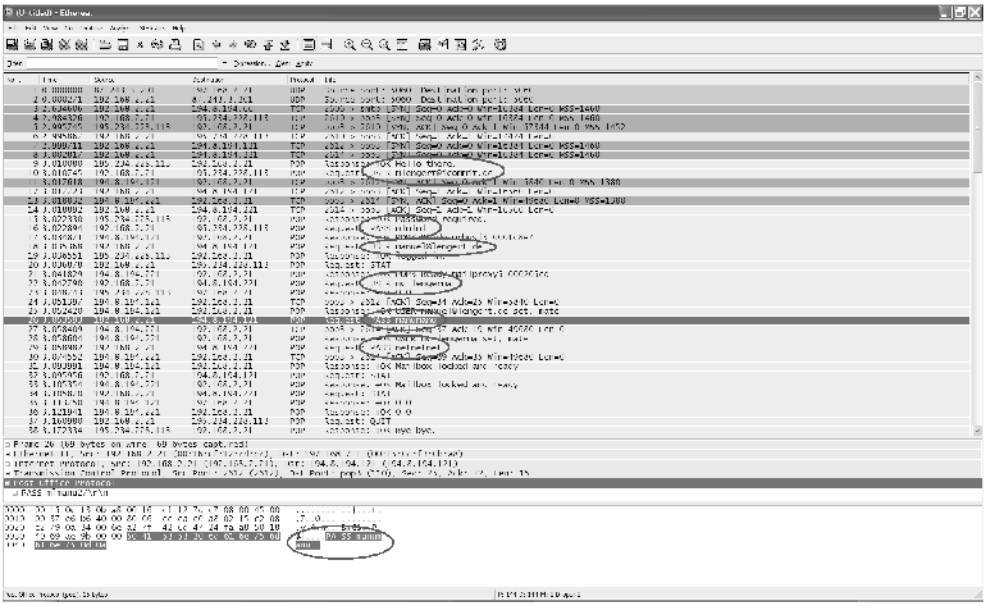


Abbildung 1.3: Mitschnitt einer POP3-Anmeldung auf einer ungesicherten Leitung

Für Hacker, die diese Missstände auszunutzen wissen, ist das Internet ein fruchtbares Feld. Mit Hilfe von Trojanern, Key-Loggern, Sniffern und Phishing-Mails lauschen sie Benutzerkonten und Passwörter völlig unbemerkt aus. Diese *digitalen Identitäten* setzen sie zu ihrem eigenen Vorteil ein, beispielsweise um auf fremde Rechnung im Internet einzukaufen.

Sicherheitsprotokolle wie bspw. HTTPS kennen keine Benutzernamen oder Passwörter; ihnen ist die Semantik der übertragenen Daten nicht bekannt. Sie verantworten lediglich den Aufbau einer verschlüsselten Verbindung. Erst wenn eine solche Verbindung zustande gekommen ist, besteht eine sichere Basis für die Eingabe einer digitalen Identität durch den Benutzer.

Fast alle Internet-Applikationen basieren auf der Eingabe eines Benutzernamens und eines Passworts, um den Benutzer zu authentifizieren. Web-Applikationen schalten eine Login-Seite vor ihren sicheren Bereich; FTP- und E-Mail-Clients erzwingen die Eingabe von Benutzer und Passwort in entsprechenden Dialogfeldern. Damit wird die gesamte Identifikation der Internet-Benutzer auf einen schwachen Authentifizierungsmechanismus reduziert!

In diesem Buch wird gezeigt, wie einfach es ist, an gültige Benutzerkonten zu gelangen und deren Passwörter zu brechen. Dass es zahlreiche Verfahren und Werkzeuge gibt, die den Diebstahl von Identitäten automatisieren. Wie einfach die bestehenden Sicherheitsmechanismen im Internet untergraben werden können: Unbedachte Benutzer verwenden kurze, einprägsame Passwörter; Hacker erstellen im Gegenzug Wörterbücher mit mehreren tausend Einträgen, um diese Benutzerpasswörter zu erraten.

Den wenigsten Benutzern ist klar, wie wichtig die Einhaltung einer strengen Passwort-Sicherheitsrichtlinie ist. Wer macht sich die Mühe, sein Passwort alle paar Wochen auf ein sicheres Passwort mit mindestens acht Zeichen zu ändern, das aus gemischten Buchstaben, Ziffern und Sonderzeichen besteht. Ein bekanntes, kryptisch wirkendes, aber einprägsames Passwort lautet zum Beispiel „2b | !2b,tihtq!“ (“to be or not to be, that is here the question!”).

Die grundsätzliche Sicherheit im Internet wird somit klar in die Verantwortung der Internet-Benutzer gelegt. Wer ein kurzes, leicht erratbares Passwort verwendet, wird schnell zum Opfer eines Missbrauchs. Wer ein langes, kompliziertes Passwort verwendet und dieses regelmäßig ändert, kann zwar davon ausgehen, dass seine Identität nicht gebrochen werden kann; ein ausreichender Schutz vor Netzwerk-Sniffern und Diebstahl besteht allerdings nicht.

Das Internet ist für die heutigen Bedürfnisse nicht mehr geeignet. Waren die Standard-Protokolle für den ursprünglichen Zweck des Internet, dem öffentlichen Austausch von Dokumenten, noch gut geeignet, so versagen sie in der heutigen Welt voller Internet-Shops, Auktionshäusern, Online-Banking-Applikationen, Music Stores und Chat-Rooms. Vor dem Hintergrund zweier gegenläufiger Entwicklungen, der Einführung neuer Geschäftsfelder in das Internet einerseits, und des konsequenten Festhaltens an alten Protokollen andererseits, ist das Internet eine einzige, eklatante Sicherheitslücke! Die Architektur des Internets lässt aus dieser Sicht einen verantwortungsvollen Umgang mit dem Thema Sicherheit vermissen.

1.5.4 Anonymität im Internet

Eines der größten Probleme des Internets ist die Anonymität seiner Benutzer. Zwar wird ein ausreichender Datenschutz gewährt, die Anonymität des Internets unterstützt in erster Linie jedoch die „bad guys“. Der Versuch beispielsweise, eine unerwünschte Spam-Mail bis zu ihrem Absender zurückzuverfolgen, scheitert bereits bei der Betrachtung der E-Mail-Header (Abbildung 1.4).

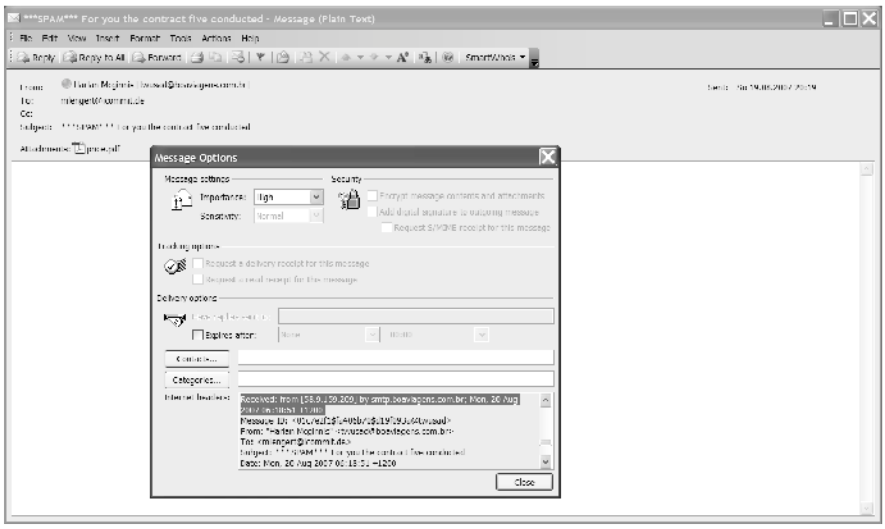


Abbildung 1.4: Eine Spam-Mail

Der Absender dieser E-Mail möchte offenbar eine Sicherheitslücke im Adobe Reader ausnutzen und verschickt eine PDF-Datei als Anhang einer ansonsten harmlos aussehenden E-Mail. Die PDF-Datei ist ein Trojaner, der in Wirklichkeit eine Schadsoftware enthält. Der Absender möchte diesen Trojaner auf einem fremden Rechner installieren.

Wird eine E-Mail ausgehend von ihrem Absender durch das Internet bis zu dem gewünschten Empfänger geroutet, so trägt jeder auf diesem Weg beteiligte Knoten seinen Servernamen und seine IP-Adresse in die E-Mail-Header ein. Auf diese Weise kann der Verlauf einer E-Mail im Internet nachvollzogen werden. Bei der Betrachtung der Header für die o.a. Spam-Mail fällt jedoch die folgende Ungereimtheit auf:

```
Received: from [58.9.159.209] by smtp.boaviagens.com.br; Mon, 20 Aug 2007 06:18:51 +1200
```

Der SMTP-Server **smtp.boaviagens.com.br** ist der Top-Level-Domain „**.br**“ in Brasilien zugeordnet. Wem ist aber die IP-Adresse **58.9.159.209** dieses SMTP-Servers zugeordnet? Eine Abfrage der öffentlichen Nameserver ergibt, dass die IP-Adresse **58.9.159.209** in den Zuständigkeitsbereich der *Asia Pacific Network Information Centre* (APNIC) fällt (Abbildung 1.5).

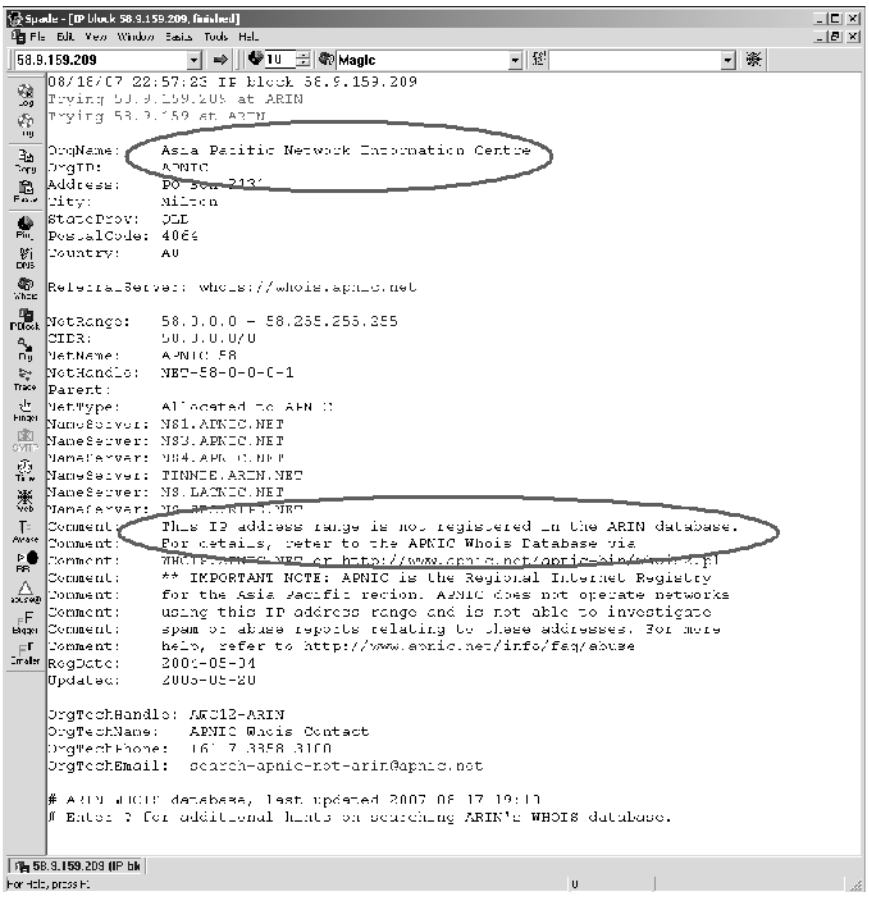


Abbildung 1.5: Abfrage der öffentlichen Nameserver

Die APNIC verwaltet IP-Adressen, DNS-Einträge und andere Netzwerkressourcen für die Region Asien und für den Pazifik.

IP-Adressen und Top-Level-Domains werden weltweit von der *Internet Assigned Numbers Authority* (IANA) verwaltet, einer Organisation, die die Struktur und Zuordnung von Internet-Adressen festlegt. Die IANA delegiert die eigentliche Registration von IP-Adressen an einige wenige regionale Internet-Registrare:

- *American Registry for Internet Numbers* (ARIN) für Nordamerika
- *Réseaux IP Européens Network Coordination Centre* (RIPE NCC) für Europa, den Nahen Osten und Zentralasien
- *Asia-Pacific Network Information Center* (APNIC) für Asien und für den Pazifik
- *Latin American and Caribbean Internet Addresses Registry* (LACNIC) für Lateinamerika und für die Karibik
- *African Network Information Center* (AfriNIC) für Afrika

Die Abfrage der IP-Adresse **58.9.159.209** bei der zuständigen APNIC ergibt, dass der gesamte Adressbereich **58.9.0.0 – 58.9.255.255**, in dem die IP-Adresse **58.9.159.209** liegt, einem ADSL-Provider in Bangkok zugeordnet ist (Abbildung 1.6).

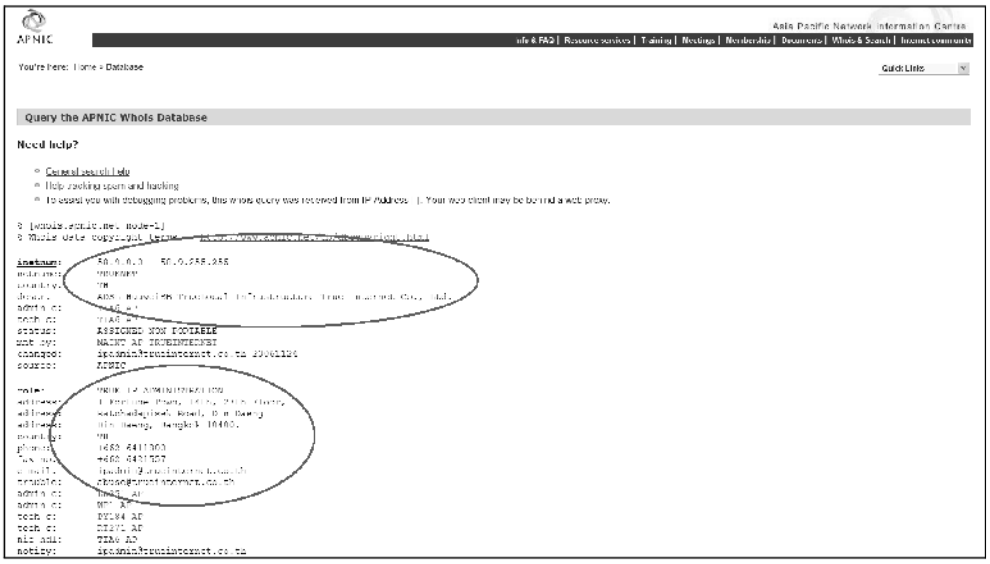


Abbildung 1.6: Abfrage einer IP-Adresse bei dem zuständigen Registrar

Mit Hilfe des Werkzeugs *Visual Route* kann die IP-Adresse nun bis zu dem Provider zurückverfolgt werden. Das Programm liefert die einzelnen Servernamen der Knotenpunkte auf der Strecke im Internet auf und führt für jeden dieser Knoten einen *Reverse-Lookup* durch, um den realen Servernamen zu ermitteln (Abbildung 1.7).

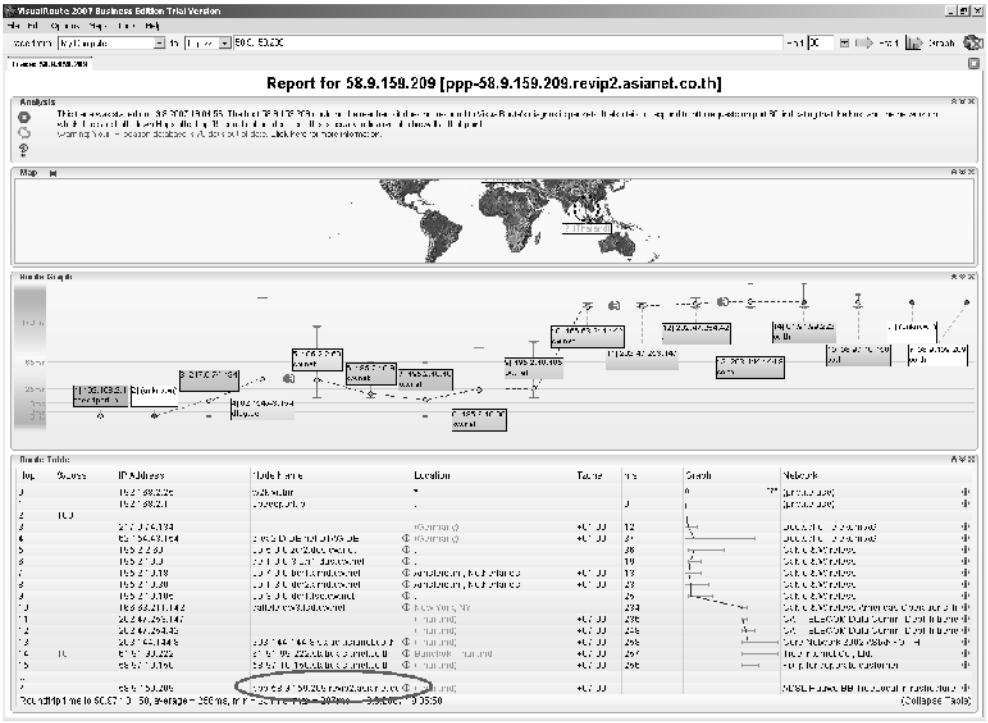


Abbildung 1.7: Auflösung der IP-Adresse und Zurückverfolgen der Route

Die IP-Adresse **58.9.159.209** ist dem Server **ppp-58.9.159.209.revip2.asianet.co.th** zugeordnet, einem Einwahlserver aus Thailand (Top-Level-Domain „**.th**“). In der gesendeten Spam-Mail wurde hingegen für die IP-Adresse **58.9.159.209** der Servername **smtp.boaviagens.com.br** angegeben; offensichtlich wurden die Mail-Header also bei dem Versand der E-Mail gefälscht.

Eine Abfrage der Ports des Servers **ppp-58.9.159.209.revip2.asianet.co.th** ergibt die offenen Ports 25 (SMTP) und 110 (POP3); es handelt sich also um einen reinen E-Mail-Server für den Versand und die Abfrage von E-Mails (Abbildung 1.8).

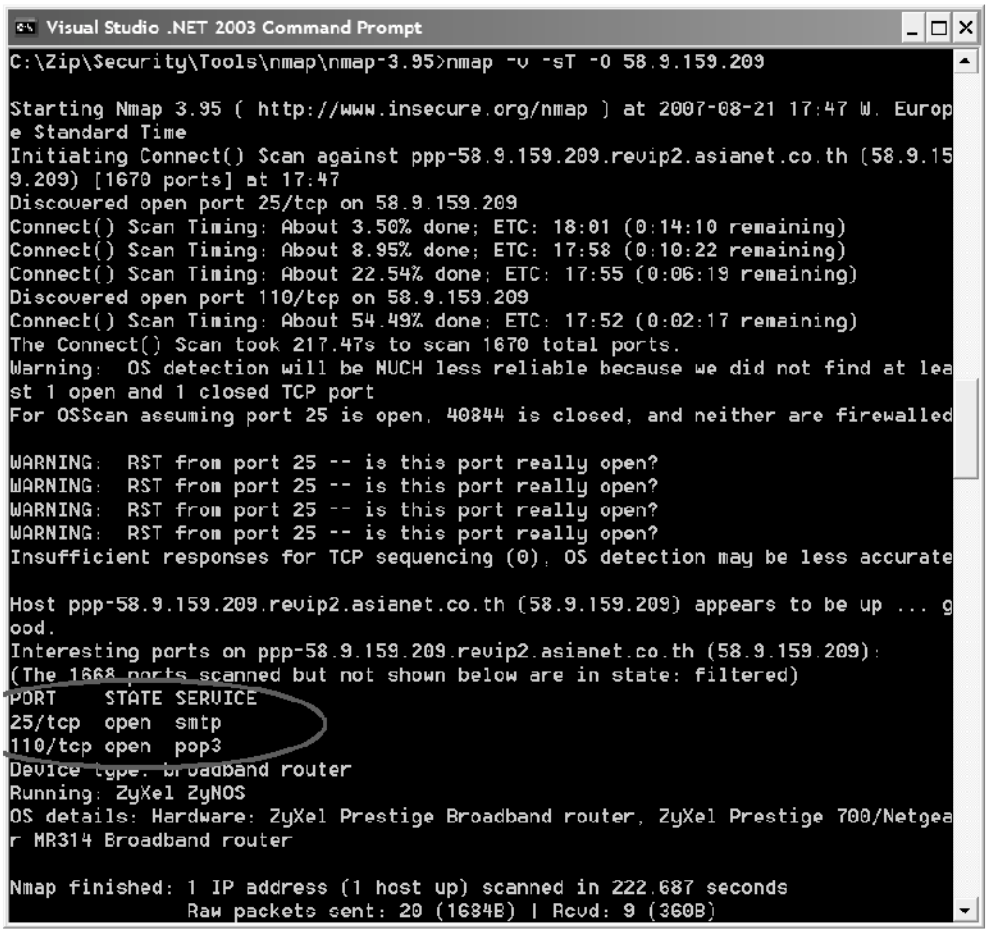


Abbildung 1.8: Verwendung des fraglichen Servers für SMTP und POP3

Weitere Informationen über die Dienstleistungen des Providers können über dessen Internet-Site ermittelt werden. Der Servername **ppp-58.9.159.209.revip2.asianet.co.th** legt nahe, dass dem Provider die Domäne **asianet.co.th** zugeordnet ist. Ein Blick auf die Homepage *http://www.asianet.co.th/* verdeutlicht, dass der asiatische Provider seinen Kunden einen Internetzugang gegen Vorkasse bietet, ohne dass der Kunde seine persönlichen Daten preisgeben muss (Abbildung 1.9). Anonymität gegen Vorkasse ...

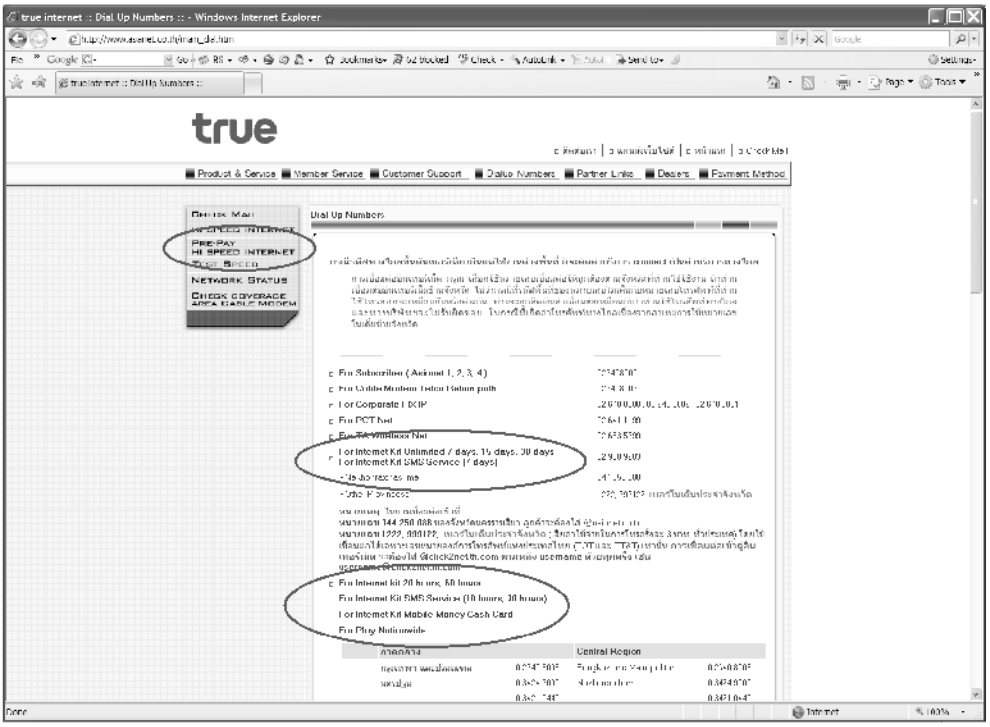


Abbildung 1.9:

Über den Absender der Spam-Mail ist nicht mehr herauszufinden. Wäre der Spammer bei dem Provider, über den er sich in das Internet eingewählt hat, namentlich jedoch bekannt, hätte ein Anfrage bei dem Provider vielleicht ein Ergebnis ergeben. Würde dieser die Information einer europäischen Behörde zur Verfügung stellen? Die derzeitige Rechtsprechung regelt solche Anforderungen bisher nicht ...

Aus diesem Grund wird es also auch in naher Zukunft nicht möglich sein, die Absender von Spam-Mails, die uns täglich zu Hunderten erreichen und unsere Computer zumüllen, zurückzuverfolgen und haftbar zu machen.

1.5.5 Das Leben im „Hier und Jetzt“

Von einem sicheren Internet ist die Gesellschaft noch weit entfernt. Unternehmen, die ihre Geschäftsmodelle im Internet betreiben, private Computernutzer, Telekommunikationsfirmen, Dienstleister, Software- und Hardware-Hersteller müssen sich daher der Sicherheitsschwächen des Internets bewusst sein und die erhöhten Kosten für mehr Sicherheit, mehr Qualität, mehr IT-Know-how und mehr Projektzeit in ihr Budget einkalkulieren.

Alle Internet-Benutzer müssen sich der folgenden Problematik bewusst sein:

Die aktuellen Standardprotokolle bieten keinen Schutz vor dem Ausspähen von Daten, vor dem Abfangen von Daten, vor der Veränderung und Zerstörung von Daten.

Die zugrunde liegenden Technologien unterstützen nicht die IT-Forensiker, also die Strafverfolger, sondern eher die Übeltäter: Indem die Anonymität des Hackers gewahrt bleibt, entgeht er den rechtlichen Konsequenzen seines Einbruchs.

Dieses Buch zeigt auf, mit welch einfachen Mitteln Angriffe im Internet möglich sind:

Wie werden Schadprogramme erstellt?

Wie werden Schadprogramme als Trojaner getarnt?

Wie werden Viren und Würmer erstellt und in Umlauf gebracht?

Wie werden Phishing-Sites erstellt?

Wie werden Rechner überwacht?

Wie werden Passwörter geknackt?

Allem voran wird umfassend die Frage untersucht:

Wie greift ein professioneller Hacker in ein Unternehmensnetzwerk ein?

Gegen die aufgezeigten Angriffe gibt es zahlreiche, wirksame Gegenmaßnahmen, die ein *Ethical Hacker* in einem Unternehmensnetzwerk einrichten kann. Den betroffenen Unternehmen obliegt die Aufgabe, ein angemessenes Budget in die Absicherung ihrer Applikationssoftware und Netzwerkinfrastruktur zu investieren, sowie die Hoffnung auf eine sicherheitsbewusste Weiterentwicklung der Internet-Protokolle. Das Kapitel 9 dieses Buchs führt den Leser in eine „Schöne neue Welt“ und beschreibt die grundsätzlichen Ansätze zur Absicherung von Netzwerken, Computersystemen und Kommunikationsleitungen.

2 Opfer, Täter, Vorgehensweisen

Hacking betrifft den privaten wie auch den geschäftlichen Bereich. Während der überwiegende Teil dieses Buchs den professionellen Angriff auf Unternehmensnetzwerke beschreibt, beleuchtet dieses Kapitel vorab den Angriff auf Privatanwender.

Wen greifen Hacker an? Welcher Schaden entsteht? Wie gehen die Angreifer vor?

Diese Fragen lassen sich durchgehend systematisch beantworten:

1. Wen greifen Hacker an?

   Jeder an das Internet angebundene Benutzer und jedes an das Internet angebundene Netzwerk und Computer-System ist das potentielle Ziel eines Angriffs!

2. Welcher Schaden entsteht bei einem Angriff?

   Der bei einem Angriff entstehende Schaden hängt davon ab, welches Ziel der Hacker verfolgt:

   - Abfangen von Daten:

     Der Hacker kann auf dem kompromittierten Rechner einen Network Sniffer installieren, um die im Netz ausgetauschten Nachrichten „abhören" zu können. Meist suchen Angreifer in dieser Netzwerkkommunikation nach Benutzerkonten und Passwörtern.

   - Lesen von Daten:

     Der Hacker kann die auf einem Rechner gespeicherten Daten ausspähen, beispielsweise um E-Mail-Adressen aus den lokal gespeicherten Adressbüchern auszulesen, um auf der lokalen Festplatte nach Bankdaten, Kreditkartensätzen oder Passwortdateien zu suchen oder zum Zweck der Wirtschaftsspionage.

   - Ändern von Daten:

     In den meisten Fällen müssen Hacker Veränderungen am Dateisystem und an der Prozessliste des kompromittierten Rechners vornehmen, damit ihre Schadsoftware unbemerkt installiert werden kann. Sie richten sich Backdoor-Applikationen ein, um zu jedem späteren Zeitpunkt einen uneingeschränkten Zugriff auf das System zu erhalten. Sie statten das System mit Spionage-Software aus, die Tastendrücke protokolliert und Screenshots erstellt. Sie installieren Dienste, um das System fernsteuern zu können. Sie tarnen die installierte Stealth-Software über Rootkits, so dass der Benutzer die gestarteten Prozesse nicht bemerken kann. Sie geben ihrer Schadsoftware unverfängliche Dateinamen wie zum Beispiel explorer.exe oder notepad.exe, um keine neuen Verzeichnisse oder Dateien auf dem System erzeugen zu müssen, und um so unauffällig wie möglich zu bleiben.

- Löschen von Daten:

  Ist das betroffene System das eigentliche Ziel eines geplanten Angriffs, kann ein immenser Schaden für den Besitzer entstehen. Wenn der Hacker beispielsweise Office-Dokumente unwiderruflich löscht, gehen für den Benutzer wichtige Daten verloren. Fertigt dieser nicht regelmäßig eine Sicherheitskopie seiner Daten an, besteht keine Möglichkeit mehr, auf die verloren gegangenen Dateien zurückzugreifen. Beschädigt der Hacker Systemdateien, kann der Rechner nicht mehr gestartet werden und muss neu installiert werden. Schlimmer wird die Situation, wenn der Hacker in ein Unternehmensnetzwerk eindringt und die in einer Datenbank gespeicherten Daten löscht (z.B. Kunden, Aufträge oder Zahlungsvorgänge).

- Erstellen von Daten:

  Gelingt es dem Hacker, einen Internet-Shop zu kompromittieren, kann er Bestell- und Zahlungsvorgänge auslösen. Dazu muss er nur die entsprechenden Datensätze in der Datenbank des Shop-Systems erzeugen. Gelingt es ihm, ein neues Benutzerkonto in dem Shop-System zu erstellen, kann er direkt über die Benutzeroberfläche des Shops eine Bestellung ausführen und diese über ein fremdes Konto verrechnen lassen.

3. Wie gehen die Angreifer vor?

   Hacker versenden Spam-Mails, um ihre Schadsoftware auf fremden Rechnern zu installieren. Diese wird geschickt als Trojaner im Anhang der E-Mail getarnt. Hacker erstellen Phishing-Sites, um digitale Identitäten zu stehlen. Sie erzeugen Viren, um fremde Systeme zu beschädigen und verteilen Würmer, um Denial-of-Service-Angriffe[1] auf bestimmte Dienste auszuführen. Sie erstellen Schadsoftware und installieren diese auf Fremdsystemen, einerseits um deren Ressourcen nutzen zu können, andererseits um diese fernsteuern zu können und bei der Ausführung von Angriffen ihrerseits anonym zu bleiben.

Hacker greifen alles an, was unmittelbar zu erreichen ist und was von anderen Rechnern aus erreicht werden kann. So gelangen sie über die Web-Server eines Unternehmens in das interne Unternehmensnetzwerk auf die Workstations der Anwender und auf die Entwickler-PCs der IT-Abteilung.

Das nachfolgende Kapitel beschreibt das „Wer-Wie-Was“ des Hackings:

- Wer wird angegriffen?
- Wie wird angegriffen?
- Was wird für den Angriff benutzt?

An einer erfolgreichen Übernahme eines Rechners sind immer zwei Parteien beteiligt: zum einen der Hacker, der aktiv angreift, und zum anderen der Benutzer, der diesen Angriff zulässt. Sei es aufgrund mangelnder Erfahrung oder schlichter Unbedarftheit: Dieses Kapitel zeigt, wie einfach Hacking sein kann und appelliert an den Leser, ein höheres Sicherheitsbewusstsein zu entwickeln.

1. Ein Denial-of-Service-Angriff (DoS) zielt darauf ab, einen oder mehrere Dienste eines Rechners arbeitsunfähig oder den Rechner insgesamt durch Überlastung oder Terminierung wichtiger Prozesse unerreichbar zu machen.

2.1 Opfer

Jede an das Internet angebundene Komponente ist das potentielle Ziel eines Hacker-Angriffs. Das betrifft:

- private Anwender
- Unternehmen
- Organisationen
- Institutionen
- Computersysteme
- Technologien

2.1.1 Private Anwender und Unternehmen

Ein Blick in die Nachrichten aus dem Jahre 2007 zeigt, wie die an das Internet angebundenen Benutzer attackiert werden.

Menschen

Bei Privatanwendern nutzen Hacker gern die Unerfahrenheit und Unbedarftheit der Computerbesitzer aus.

„Ein Drittel aller Cheats und Patches sind mit Malware verseucht"

Computerspieler sind ein beliebtes Ziel der Hacker-Community, da sie meist vollkommen unreflektiert neue Patches, Cheats[a] und Wallhacks[b] aus dem Internet herunterladen. Die Spiele-Community tauscht solche Zusatzprogramme über binäre Newsgroups und P2P-Netzwerke aus. Eine Auswertung von über 1.000 Dateien solcher Cheats und Patches in P2P-Netzwerken ergab, dass mehr als ein Drittel der analysierten Executables und ZIP/RAR-Archive Malware enthielt.

Erschwerend schalten die meisten Online-Spieler ihre AntiViren- und Firewall-Software aus, um einen reibungslosen Online-Spielablauf sicherzustellen. Damit stehen der Hacker-Community Tür und Tor auf den Gamer-PCs offen: Die ungesicherten Ports der Spiele-Computer werden gerne für den Einfall von Schadcode ausgenutzt!

Des Weiteren wird im Internet ein reger Handel mit Spieler-Accounts betrieben. Da die Login-Daten eines Online-Spielers meist auch dessen Kreditkartendaten enthalten, sind Spieler-Accounts für Hacker mindestens genauso attraktiv geworden wie einfache Kreditkartendateien.

a Ein Cheat ist ein Spielemodus, in dem der Spieler schwierige Abschnitte überspringen oder seine Spielerfigur mit besseren Eigenschaften ausstatten kann, um den weiteren Spieleverlauf zu vereinfachen.

b Wallhacks sind Cheats, die Wände und Hindernisse in Computerspielen halbtransparent erscheinen lassen, so dass der Spieler hindurchschauen kann.

„Urlauber in Internetcafés und WLANs betroffen“

Die meisten Betreiber von Internetcafés und WLANs verzichten auf die einfachsten Sicherheitsmaßnahmen. Fangen sich die Kunden beim Surfen eine Malware ein, sind die bereitgestellten Rechner schnell Malware-verseucht! Die heimlich installierte Spyware protokolliert Tastaturanschläge, erstellt Screenshots, schneidet den Datenverkehr mit und sendet das gesamte Protokoll an den Hacker. Besonders die von Hotels angebotenen Internet-Zugänge sind hochgradig gefährdet, da der Benutzer bei der Registrierung neben seinen Login-Daten auch entsprechende Zahlungsinformationen angeben muss.

„Handy-Spionage-Tools im Internet angeboten“

Im Internet werden Tools angeboten, die die vollständige Überwachung eines Handys ermöglichen. Dies umfasst

- die Protokollierung aller gesendeten und empfangenen SMS inklusive Datum, Uhrzeit, Absender und Inhalt
- die Aufzeichnung aller geführten Telefonate
- die Speicherung aller gesendeten und empfangenen E-Mails
- die Aufzeichnung der GPS-Position des Handy-Besitzers in regelmäßigen Abständen (z.B. minütlich)
- den Download oder den Versand des Protokolls in einem CSV-, RTF- oder XML-Format.

FlexiSpy[a] ist ein solches Handy-Spionage-Werkzeug. In Deutschland aus gutem Grund verboten, wird die Software in den USA unter dem Vorwand vertrieben, die eigenen Kinder besser schützen zu können oder den Lebensgefährten zu überwachen, wenn der Verdacht auf eine Affäre besteht! Abbildung 2.1 zeigt ein beispielhaftes Protokoll dieser Software:

a *http://www.flexispy.com/*

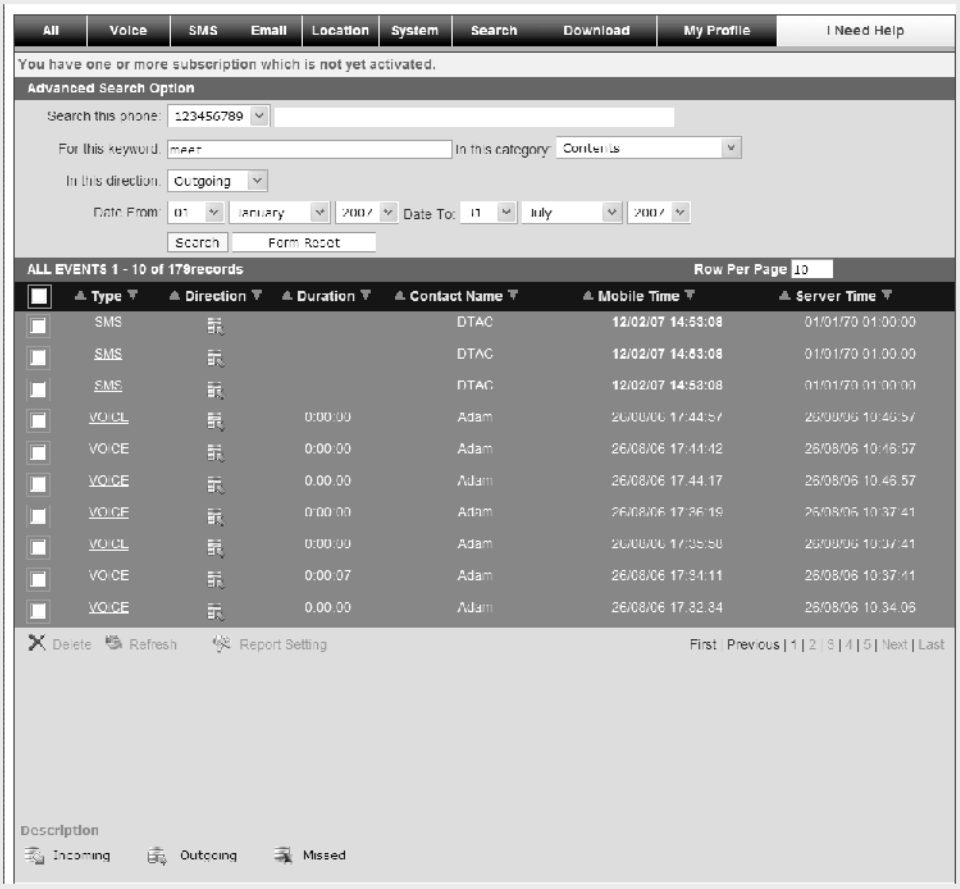


Abbildung 2.1: Handy-Überwachung mit der Spionage-Software „FlexiSpy"

Hacker missbrauchen eine solche Software, um Handys auszuspionieren. Sie überwachen die ein- und ausgehende SMS- und E-Mail-Kommunikation und suchen nach bestimmten Stichwörtern wie bspw. „Konto", „Kredit" und „Login".

„Trojaner infiziert Bewerber auf Monster.com"

Soziale Netzwerke geraten zunehmend in den Fokus der Hacker-Community. Hackergruppen platzieren Malware-infizierte Werbeelemente auf Job-Börsen und anderen Web-Seiten. Bei einem Klick durch den Benutzer löst ein gezielter Exploit auf diesen Seiten die Installation einer Schadsoftware aus. So haben Hacker in den USA beispielsweise ein Datenlager mit persönlichen Informationen von knapp 50.000 Bewerbern auf der Jobsuche-Plattform Monster.com angelegt. Die Datei enthielt Bank- und Kreditkarteninformationen, Sozialversicherungsnummern und Benutzernamen mit Passwörtern für Online-Accounts.

Unternehmen

Die meisten Unternehmen setzen Standard-Software und Standard-Hardware ein und verlassen sich auf die darin implementierten Sicherheitsmechnanismen. Dass dies in den wenigsten Fällen ausreichend vor Angriffen schützt, zeigen die folgenden Beispiele.

„Hacker zielen auf Führungskräfte und deren Angehörige ab"

Pro Tag werden mehrere hundert Millionen Spam-Mails versendet. Mittlerweile betreiben Hacker einen höheren Recherche-Aufwand, um ihre Opfer zum Öffnen der mit Schadware verseuchten Dateianhänge einer E-Mail zu verleiten. Gezielt werden die Mails an Unternehmensvorstände, Geschäftsführer und Finanzdirektoren geschickt; als Absender werden die E-Mail-Adressen ihrer Familienangehörigen oder Geschäftspartner eingesetzt. Beunruhigend ist, dass der E-Mail-Text persönliche Angaben enthält, bspw. die genaue Stellenbezeichnung der Zielperson. Die Spam-Mails reizen mit Investment-Informationen und Aktientrends und enthalten in dem Word- oder Excel-Anhang neben nichtssagenden Statistiken den eigentlich gefährlichen, ausführbaren Code.

Informationen über die Mitarbeiter eines Unternehmens können Hacker über eine Google-Suche in Diskussionsgruppen finden, auf den Internet-Seiten des Unternehmens oder in deren Intranets.

„Hacker nehmen Firmen-Intranets ins Visier"

Intranets dienen in den Unternehmen dazu, Prozesse zu beschleunigen und interne Informationen zwischen den Abteilungen auszutauschen. Die meisten Firmen rechnen nicht damit, dass Hacker in ihre Intranets eindringen können; entsprechend nachlässig sind diese Subnetze geschützt. Hacker attackieren jedoch gezielt solche Intranets, um Informationen über die internen Accounts der Mitarbeiter zu erhalten und sich mit deren Rechten in die internen Applikationen des Unternehmens einwählen zu können. Je nach Abteilung und Rang des Mitarbeiters können über dessen Rechte neue Geschäftsvorfälle erstellt und Zahlungstransaktionen abgewickelt werden.

„Spam-Großangriff steigert Aktienkurs um 20 Prozent"

Dass sich mit Stimmungsmache an der Börse viel Geld verdienen lässt, zeigte nicht nur Michael Douglas als Gordon Gecko in dem Film „Wall Street". Mittlerweile kaufen auch Hacker die Aktien mittelgroßer Unternehmen und versenden anschließend Spam-Mails mit Kaufempfehlungen. Im Juni 2007 bewarben über fünf Milliarden E-Mails die Aktie des Frankfurter Unternehmens „Talktech Telemedia", deren Aktienkurs schon nach wenigen Tagen um 20 Prozent anstieg. Die Spam-E-Mails enthielten PDF-Attachments, die den Anschein eines Investment-Newsletters erweckten.

Mit diesem „Pump-and-Dump"-Prinzip steigern die Versender durch massenhafte Verbreitung von Kaufempfehlungen das Interesse an den Unternehmensaktien, nur um diese dann schnellstmöglich wieder unter Profit zu verkaufen.

„Wirtschaftsspionage vernichtet Jobs in Deutschland“

Wenn ein Baumaterialhersteller beispielsweise einen Kleber erfindet, der das Anbringen von Dämmungen beschleunigt, gibt es Konkurrenten, die solche Erkenntnisse ausspionieren. Mitarbeiter kopieren vertrauliche Akten; Forscher verkaufen Kopien ihrer Projektergebnisse. Mittlerweile schätzen Experten, dass durch die zunehmende Wirtschaftsspionage jedes Jahr rund 50.000 Jobs vernichtet werden.

Abbildung 2.2 zeigt, wie ein Telekommunikationsunternehmen mit Hilfe des Tools *Web-Site Watcher* die Internet-Seiten der Konkurrenz beobachten kann:

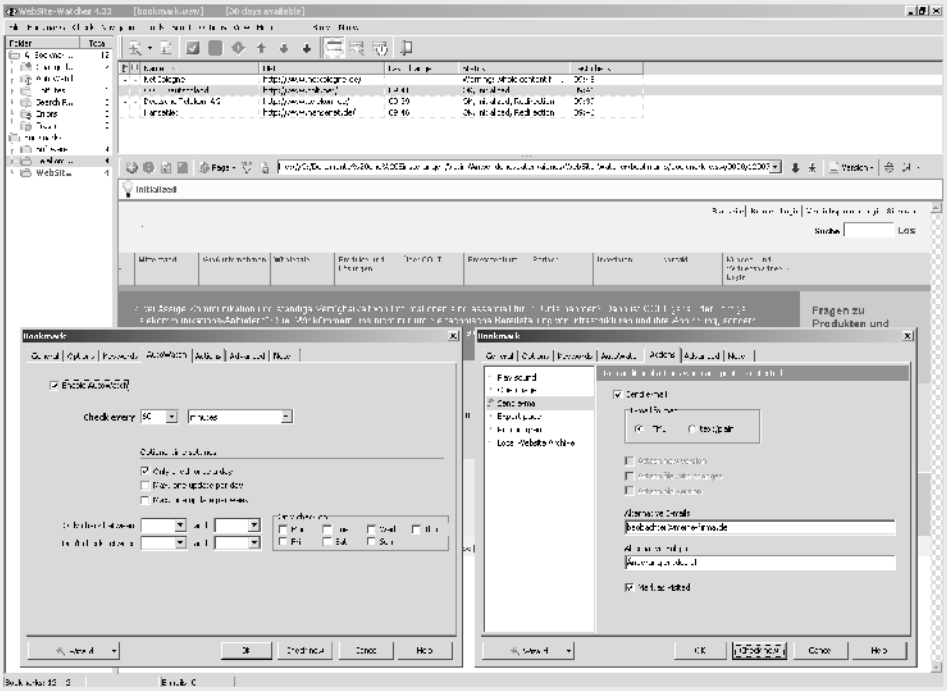


Abbildung 2.2: Beobachten konkurrenter Web-Sites mit dem *WebSite-Watcher*

Das Werkzeug lädt initial die zu beobachtende Web-Site auf den lokalen Rechner und beginnt dann im Hintergrund mit der Beobachtung von Veränderungen an dieser Web-Site. So wird beispielsweise automatisch eine E-Mail an den Beobachter versendet, wenn sich eine Seite geändert hat.

Angriffe

Die üblichen Angriffe reichen von Spam-Mails und Phishing-Sites über Viren, Würmer und Trojaner. Abschnitt 2.3 zeigt in aller Ausführlichkeit, wie solche Angriffe vorbereitet und ausgeführt werden.

2.1.2 Systeme und Technologien

Neben den Privatanwendern und Unternehmen sind insbesondere die Netzwerk- und Rechnersysteme sowie die darauf installierten Technologien das Ziel von Hacker-Angriffen. Abbildung 2.3 zeigt beispielhaft den Aufbau eines einfachen Unternehmensnetzwerks:

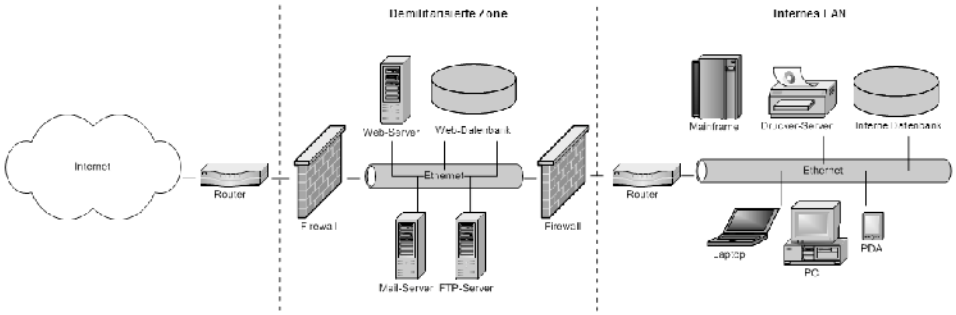


Abbildung 2.3: Schematischer Aufbau eines einfachen Unternehmensnetzwerks

Jede einzelne Komponente in einem solchen Netzwerk ist das potentielle Ziel eines Angriffs!

Ausgehend von den aus dem Internet erreichbaren Rechnern versucht der Hacker in das interne Firmennetz einzudringen. Er tastet die Router und Firewalls nach Lücken und Schwachstellen ab. Er greift den Web-Server und die Datenbank mittels Web-Server-Exploits und SQL-Injection an. Er wendet bekannte Exploits auf den FTP-Service und die Mail-Protokolle an. Gelangt der Hacker über die zweite Firewall hinaus, ist ihm sogar ein Zugriff auf die internen Netzwerkkomponenten möglich, welche in der Regel schwächer geschützt sind und seltener mit Sicherheitspatches aktualisiert werden.

Abbildung 2.3 vernachlässigt aufgrund der in der Praxis vorherrschenden Komplexität viele Teilaspekte firmeninterner Netzwerke:

- Einwahlmöglichkeiten mobiler Mitarbeiter über VPN
- Terminal-Server
- WLAN-Netze
- Hotspots

und vieles mehr. So werden in der Praxis beispielsweise kabellose Verbindungen wie Bluetooth, WiFi und WLAN von Außendienstmitarbeitern eingesetzt, die technisch schlecht gegen Abhörversuche abgeschirmt sind.

Die folgenden Beispiele aus den Nachrichten verdeutlichen, dass nicht nur die Einführung neuer Technologien ein hohes Sicherheitsrisiko für Firmen darstellt, sondern auch lang bewährte, ältere Technologien den Hackern zum Opfer fallen:

„AJAX macht Hacker glücklich“

Die Entwicklung dynamischer Anwendungen stellt zunächst ein hohes Sicherheitsrisiko dar, da neue Technologien zum Zeitpunkt ihrer Einführung in der Regel meist nicht ausreichend geschützt sind. Der Time-to-Market-Druck der Hersteller bewirkt, dass eine neue Technologie oder ein neues Produkt schnellstmöglich am Markt eingeführt wird; und erst später werden die erforderlichen Sicherheitsfeatures nachgeliefert. Den Firmenkunden dagegen fehlt oft die Erfahrung, eigene Sicherheitsmechanismen zu installieren, um solche Produkte und Technologien abzuschirmen.

„Asynchronous JavaScript and XML“, kurz AJAX, beflügelt die Entwicklung dynamischer Anwendungen. Browser-Anwendungen werden plötzlich genauso interaktiv wie herkömmliche GUI-Anwendungen.

Experten raten von dem AJAX-Einsatz ab, da Geschäftsanwendungen nur unzureichend geschützt sind: Durch den Einsatz von JavaScript wird die Browser-seitige Logik einer Applikation mehr oder weniger als lesbarer Text dargestellt! Dieser Programm-Code zeigt dem Hacker die Funktionsweise der Applikation. Meist ruft eine AJAX-Anwendung die Geschäftslogik in Form von Web-Services auf dem Server auf. Der JavaScript-Code auf dem Client zeigt dem Hacker, in welcher Reihenfolge diese Schnittstellen aufzurufen und zu nutzen sind. Die Web-Services sind öffentlich und anonym im Internet erreichbar, und somit steht den Hackern eine wesentliche Programmierschnittstelle der Anwendung offen.

„URI-Lücke trifft unzählige Windows-Programme“

Experten fanden eine Sicherheitslücke in dem URI-Protokoll[a], die es einem Angreifer ermöglicht, ungeprüfte Programme auf einemRechner zu starten. Die URI-Technologie wird von Windows zum Ausführen von Programmen aus dem Webbrowser heraus verwendet. So kann der Benutzer beispielsweise ein Executable in einer URL eingeben, und der Browser lädt das Executable herunter und startet es automatisch auf dem lokalen Rechner.

Da die meisten Windows-Programme gegen einen Start aus dem Internet Explorer oder aus einem anderen Browser nicht abgesichert sind, kann das Problem durch einen Microsoft-Patch alleine nicht gelöst werden, so dass eine zeitnahe Lösung des Problems nahezu ausgeschlossen ist.

a Uniform Resource Identifier

„Hacker konzentrieren sich auf Endnutzersysteme“

Nachdem private Anwender sensibler gegenüber Spam-Mails und Phishing-Sites geworden sind, geraten zunehmend Plugins und Nicht-Browser-Applikationen ins Visier der Hacker. Sie analysieren die Aufrufschnittstellen der Plugins von Browsern, Document-Readern und Toolbars und prüfen, wie die bestehenden Datenflüsse für das Einschleusen von Schadcode genutzt werden können. Da die Anwender die Plugins der Hersteller vertrauensvoll auf ihrem Rechner installiert haben, besteht eine hohe Wahrscheinlichkeit, dass der Schadcode unbemerkt auf den Rechner eines Opfers gelangen kann.

Das größte Sicherheitsproblem im Bereich der Schwachstellen sind die sog. „Zero-Day-Exploits“. Darunter versteht man Schwachstellen, die noch nicht gepatcht oder veröffentlicht wurden. Finden Hacker eine neue Sicherheitslücke in einer Software, dauert es eine ganze Zeit, bis diese Sicherheitslücke von dem zuständigen Hersteller durch einen Patch behoben wird. Dann dauert es einen weiteren Zeitraum, bis die Kunden und Anwender der Software den Sicherheitspatch auf ihren Systemen installiert haben. Experten schätzen, dass ein durchschnittlicher Zero-Day-Bug eine Lebenserwartung von durchschnittlich 348 Tagen hat, bevor er entdeckt oder gepatcht wird! Manche Schwachstellen werden bereits nach 100 Tagen bekannt gegeben, andere bleiben über drei Jahre unentdeckt. Einem Hacker bleibt also durchschnittlich ein ganzes Jahr, um neue Bugs für unlautere Zwecke auszunutzen.

2.2 Täter

Die Hacker-Community setzt sich aus den unterschiedlichsten Charakteren zusammen:

- *Script-Kiddies* nutzen vorgefertigte Skripte und Werkzeuge, um Viren, Würmer oder Trojaner in Umlauf zu bringen. Sie kennen die Arbeitsweise dieser Programme nicht und sind sich oft des Schadens nicht bewusst, den sie anrichten. Script-Kiddies sind häufig Jugendliche, die anderen durch ihren Vandalismus imponieren wollen.
- *Cracker* erstellen solche Skripte und Werkzeuge. Sie erbringen dabei einen beträchtlichen Programmieraufwand. So sind im Internet beispielsweise mehrere *Virus Construction Kits*, *Worm Generators* und *Trojan Creators* zu finden. *Cracker* verkaufen ihre Schadprogramme gegen Gebühr an Kriminelle, die diese Software einsetzen und verteilen.
- *Profis* verbringen ihre Zeit mit der Erkundung von Software und Hardware. Sie erlernen die Funktionsweise von Netzwerkprotokollen, analysieren die Struktur von Betriebssystemdiensten und senden experimentelle Signalfolgen an neue Hardware-Devices. Sobald ihnen eine Unregelmäßigkeit auffällt, erkunden sie das Problem und versuchen eine Systematik herauszufinden. Oft werden auf diese Weise neue Schwachstellen gefunden, und es entstehen entsprechende Exploits. Solche Hacker wollen sich in der Community meist einen Namen und gebührenden Respekt durch die Bekanntgabe neuer Sicherheitslücken verschaffen.

- *Insider* verfügen über interne Informationen. Dabei kann es sich um gekündigte Mitarbeiter handeln, die sich an ihrem ehemaligen Arbeitgeber für ihre unrechtmäßige Kündigung rächen wollen, oder um interne Mitarbeiter, die sich einen beträchtlichen Zusatzverdienst durch den Verkauf heißer Informationen verdienen wollen.

Der folgende Abschnitt zeigt, wie Hacker vorgehen, um ihre Schadsoftware auf den Rechnern privater Anwender zu installieren. Kapitel 3 vertieft anschließend die Vorgehensweise professioneller Hacker bei dem Versuch, in ein Unternehmensnetzwerk einzubrechen.

2.3 Vorgehensweisen

Dieser Abschnitt beschreibt, wie „Malware" entsteht und in Umlauf gebracht wird. Untersucht werden die folgenden Fragestellungen:

- Wie wird Malware erstellt?
- Wie entstehen Spam-Mails?
- Wie funktionieren Phishing-Sites?
- Wie werden Viren in Umlauf gebracht?
- Wie entstehen Würmer?
- Wie wird Spyware eingeschleust?

Unter *Malware* versteht man Schadprogramme, deren Funktionsweise von dem Besitzer eines Computers nicht erwünscht ist und aus diesem Grund von dem Hacker getarnt ausgeführt wird. Malware drückt sich in Viren, Würmern, Trojanern, Backdoor-Applikationen und Spyware aus, weshalb eine kurze Definition dieser Begriffe erfolgt:

- Ein *Virus* ist ein sich selbst verbreitendes Programm, das sich in andere Dateien einschleust. Ein Virus verbreitet sich, indem es Kopien von sich selbst erstellt und in andere ausführbare Programme oder Dokumente schreibt. Einmal in Umlauf gebracht, vermehren sich Viren durch das Ausführen der befallenen Programme und durch das Öffnen der befallenen Dokumente. So infizierte Dateien bezeichnet man als *Wirt*.
- *Würmer* verbreiten sich aktiv. Sie warten nicht darauf, aktiviert zu werden, sondern werden selbstständig tätig und infizieren andere Rechner, die über das Netzwerk erreichbar sind.
- Ein *Trojaner* ist eine Schadsoftware, die als nützliche Anwendung getarnt ist, aber ohne Wissen des Anwenders im Hintergrund eine gänzlich andere Funktion ausführt. Meist werden Trojaner mit Backdoor-Applikationen gekoppelt.
- Eine *Backdoor* ist ein Programm, das dem Hacker an den bestehenden Zugangssicherungen vorbei eine Hintertür für spätere Zugriffe offen hält. Sie ermöglicht dem Hacker, den kompromittierten Rechner zu kontrollieren und fernzusteuern.
- *Spyware* dient dazu, den Rechner eines Benutzers ohne dessen Wissen auszuschnüffeln. Beobachtet wird dessen Surfverhalten im Internet, und meist werden Tastaturanschläge protokolliert und Screenshots erstellt.

Hacker nutzen vielfältige Tools, um Malware zu erzeugen. Die verwendeten Werkzeuge werden in P2P-Foren, binären Newsgroups und über FTP-Server ausgetauscht. Sie verdeutlichen, mit welch geringem Aufwand Schädlinge erstellt und verteilt werden können.

2.3.1 Trojaner

Eines der bekanntesten Werkzeuge zur Erstellung eines Trojaners ist *Beast*. Abbildung 2.4 zeigt, wie ein Trojaner ohne jegliche Programmierung mit diesem Tool erstelllt werden kann:

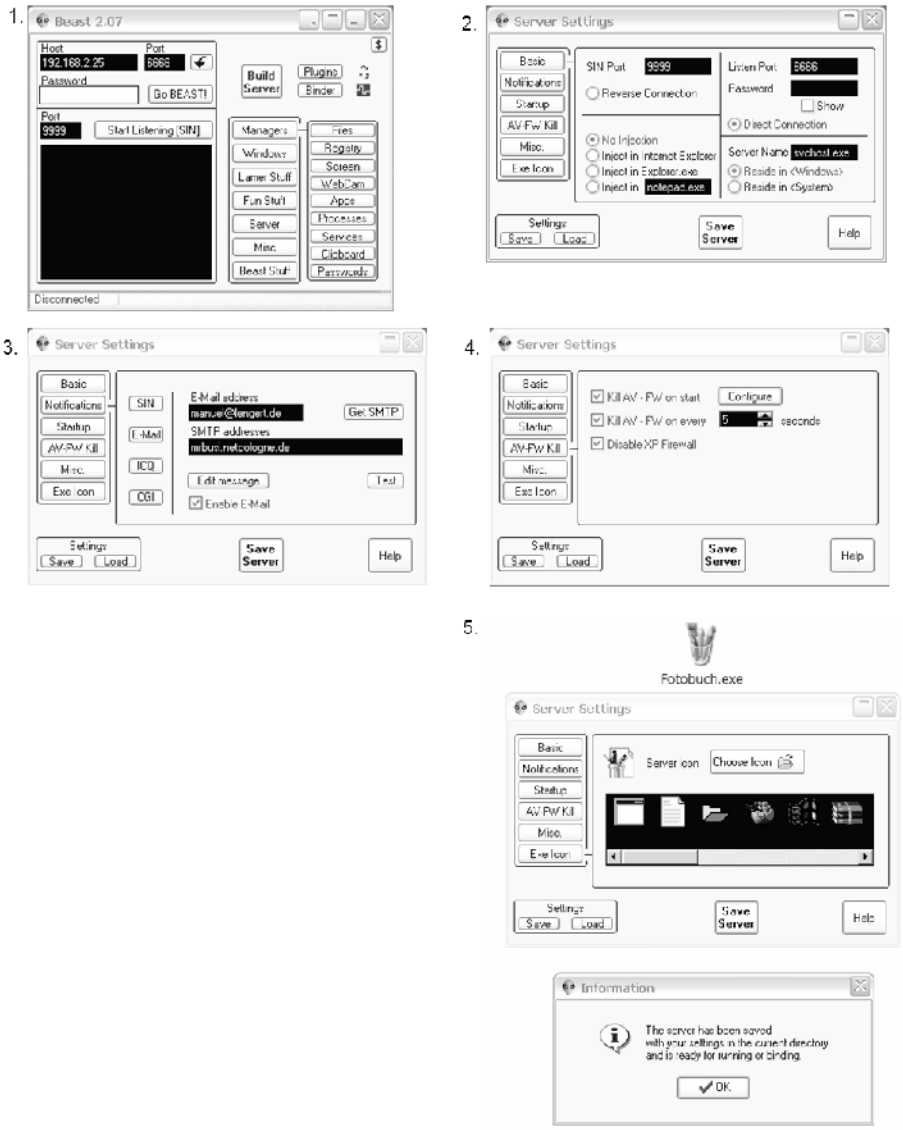


Abbildung 2.4: Erstellung eines Trojaners mit dem Hacker-Tool „Beast"

Das Werkzeug erstellt eine getarnte Backdoor-Applikation in den folgenden Schritten:

1. Über die Schaltfläche „Build Server“ wird ein Wizard aufgerufen, der die Erstellung und Konfiguration eines neuen Trojaners ermöglicht.
2. Die Backdoor registriert sich auf dem betroffenen Rechner als Port-Listener auf dem TCP/IP-Port 6666. Getarnt wird er unter dem Dateinamen „svchost.exe“, einem unter Windows gebräuchlichen Dateinamen, der von dem Betriebssystem selbst für die Ausführung von Web-Applikationen und COM+-Services eingesetzt wird. Alternativ besteht die Möglichkeit, den Trojaner in eine bestehende Datei zu „injizieren“. Dabei wird der Schadcode in eine bestehende Anwendung integriert und bei deren Aufruf automatisch aktiviert. Möglich ist jedes Executable auf dem Zielsystem, bspw. der Internet Explorer, der Datei-Explorer, eine Anwendung wie `notepad.exe` oder die Kommandozeile `cmd.exe` selbst.
3. Die Backdoor kann mit dem Hacker durch den Versand von E-Mails kommunizieren. So sind Benachrichtigungen des Trojaners über das SMTP-Protokoll an beliebige POP3-Accounts möglich. Hacker setzen eigene SMTP-Server auf oder richten sich POP3-Accounts bei Providern im Ausland ein, die für die technische Benutzung keine persönlichen Daten erheben.
4. Beim Start der Applikation ist der Trojaner in der Lage, AntiViren- und Firewall-Software zu deaktivieren, damit die Backdoor ungestört auf dem System des Benutzers registriert werden kann.
5. Abschließend wird die Backdoor-Applikation über ein harmlos wirkendes Icon getarnt. Es entsteht ein als Trojaner getarntes, ausführbares Programm, das nun auf verschiedenen Wegen verteilt werden kann:
   - als Attachment einer E-Mail
   - als unbemerkter Download beim Aufruf einer infizierten Seite im Web-Browser
   - durch das Ausnutzen einer Sicherheitslücke in einer beliebigen Applikation, die dem Hacker den Upload und die Ausführung des Trojaners auf dem betroffenen Rechner erlaubt.

Die Backdoor wird dabei mit den vollen Rechten des unwissenden Benutzers installiert. Da die meisten Privatanwender gleichzeitig Administrator ihres Systems sind, gelangt die Backdoor bei ihrer Ausführung automatisch an alle Ressourcen des Systems.

Abbildung 2.5 zeigt einen Trojaner in Aktion und demonstriert, welches Kontrollmaß ein Hacker über einen kompromittierten Fremdrechner hat:

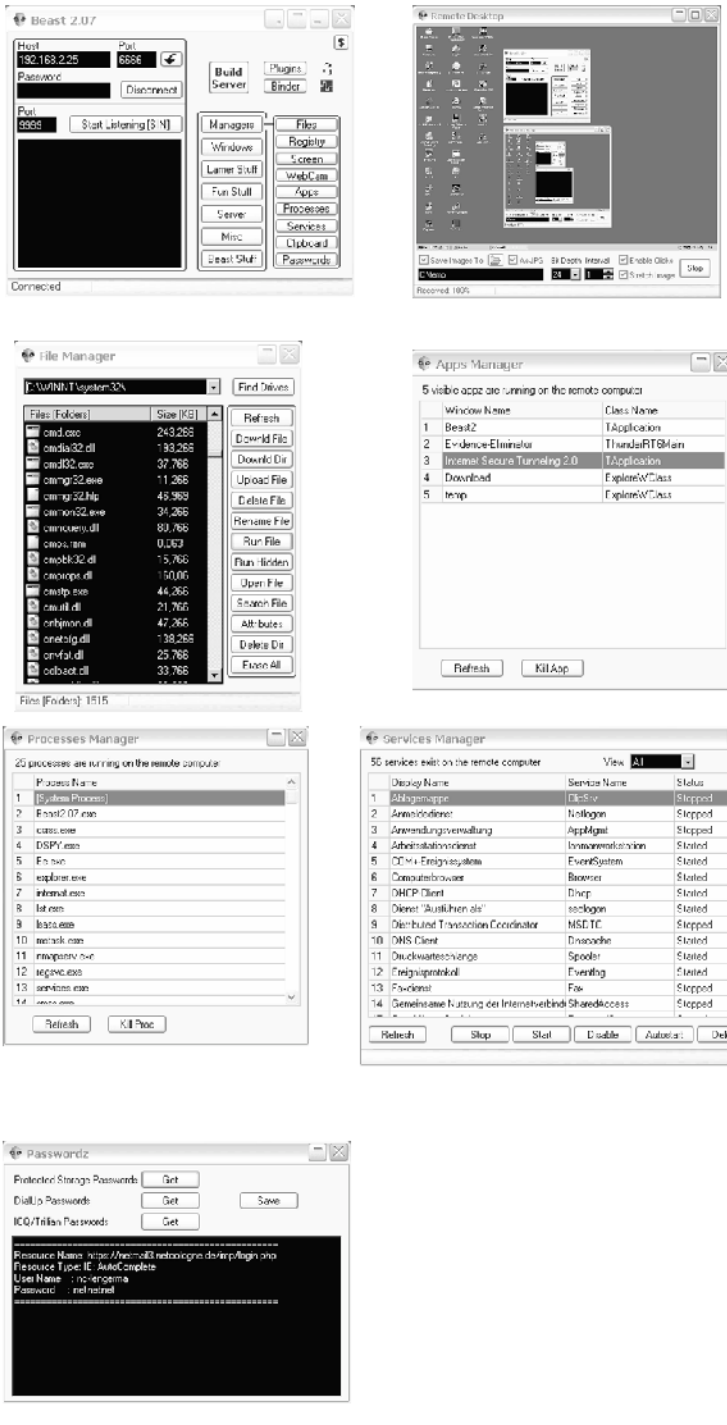


Abbildung 2.5: Trojaner in Aktion

Über die IP-Adresse 192.168.2.25 und den Port 6666 verbindet sich der Hacker mit seinem Opfer und kann dessen Rechner nach Belieben fernsteuern. Er hat Zugriff auf das Dateisystem des Rechners, auf die Registry, auf den Bildschirm, auf die laufenden Applikationen, Prozesse und Betriebssystemdienste. Nebenbei kann er den Cache des Internet-Explorers auslesen, um über die AutoComplete-Eigenschaft an die Passwörter des Anwenders zu gelangen.

Auf dem Port 6666 lauscht die Backdoor-Applikation auf dem Rechner des Opfers den Befehlen des Hackers. Die Screenshots in Abbildung 2.5 zeigen den Funktionsumfang des Trojaners auf:

- Der Hacker hat volle Kontrolle über den Bildschirm seines Opfers. Es ist ihm möglich, unbemerkt Screenshots zu erstellen, und über einen „Remote Desktop" kann er in die Anwendungen des Anwenders eingreifen, indem er Mausklicks absetzt und Eingaben über seine eigene Tastatur tätigt.
- Der Hacker hat vollen Zugriff auf das Dateisystem des Anwenders sowie auf alle von dort aus erreichbaren Netzwerkressourcen. Er kann weitere Dateien auf den Rechner seines Opfers hochladen und beliebige Applikationen ausführen. Letzteres ist ihm in einem sog. „versteckten" Modus möglich, so dass der Anwender von deren Ausführung nichts bemerkt (stealth mode).
- Der Hacker kann die laufenden Applikationen und Prozesse des Benutzers „abschießen"; er hat sogar die volle Kontrolle über die Betriebssystemdienste des Benutzers und kann diese starten, beenden, deaktivieren und beim Hochfahren des Systems automatisch starten.

Abbildung 2.6 zeigt das Bedienfeld, das dem Hacker für die Fernsteuerung seines Opfers zur Verfügung steht:

Abbildung 2.6: Bedienfeld der Backdoor

Folgende „Features“ bietet die Backdoor dem Hacker für die Kontrollausübung über sein Opfer:

Kategorie	Ressource	Befehl	Beschreibung
Managers	Files	Find Drives	Navigation durch das gesamte Dateisystem und alle erreichbaren Netzwerkressourcen
		Download File	Herunterladen einer Datei
		Download Directory	Herunterladen eines gesamten Verzeichnisses
		Upload File	Hochladen einer Datei
		Delete File	Löschen einer Datei
		Rename File	Umbenennen einer Datei
		Run File	Ausführen einer Datei
		Run File Hidden	Ausführen einer Datei in einem versteckten Modus, so dass der Benutzer die Ausführung nicht bemerkt
		Open File	Öffnen einer Datei
		Search File	Suche nach einer Datei
		Attributes	Anzeigen der Attribute einer Datei
		Delete Dir	Löschen eines gesamten Verzeichnisses
		Erase All	Löschen aller Dateien und Verzeichnisse!
	Registry	(Navigation)	Navigation durch die gesamte Registry
		Add Sub Key	Anlegen eines neuen Teilbaums
		Del Sub Key	Löschen eines Teilbaums
		Add Value	Anlegen eines neuen Schlüssels
		Del Value	Löschen eines Schlüssels
		Set Data	Ändern eines Schlüsselwertes
	Screen	Save Image	Erstellen eines Screenshots
	WebCam	Save Image	Erstellen von Fotos über die WebCam des Rechners!
	Apps	(Anzeige)	Anzeige aller laufenden Applikationen
		Kill Apps	Terminierung einer Applikation
	Processes	(Anzeige)	Anzeige aller laufenden Prozesse
		Kill Proc	Terminierung eines Prozesses
	Services	(Anzeige)	Anzeige aller Dienste
		Stop	Beenden eines Dienstes
		Start	Starten eines Dienstes
		Disable	Deaktivieren eines Dienstes

Tabelle 2.1: Befehlsumfang der Backdoor

Kategorie	Ressource	Befehl	Beschreibung
		Autostart	Automatischer Start eines Dienstes beim Hochfahren des Systems
		Delete	Löschen eines Dienstes
	Clipboard	(Anzeige)	Anzeige des Inhalts der Zwischenablage
		Set Text	Setzen der Zwischenablage auf einen bestimmten Text
		Lock	Löschen der Zwischenablage
	Passwords	Protected Storage Password	Auslesen des Internet-Explorer-Caches und Auswerten aller Eingaben, die über das Feature „AutoComplete" bisher getätigt wurden
		DialUp Passwords	Auslesen aller Dial-up-Passwörter
		ICQ/Trillian Passwords	Auslesen aller Messenger-Passwörter für ICQ und Trillian
Windows		Hide All	versteckt alle offenen Fenster
		Crash	bringt das System zum Absturz
		Power Off	schaltet das System ab
		Reboot	startet das System neu
		Shut Down	fährt das System runter
		Log Off	meldet den Benutzer ab
Lamer Stuff		Hide Icons	versteckt alle Icons auf dem Desktop
		Hide Tray	versteckt die Task-Leiste
		Hide Start	versteckt das Start-Menu
		Disable Tray	sperrt die Task-Leiste gegen Mausklicks
		Open CD	öffnet den Auswurf des CD/DVD-Laufwerks
		Lock Mouse	sperrt die Maus
		Hide Clock	versteckt die Systemuhr
		Swap But's	vertauscht die linke und rechte Maustaste
		Crazy Mouse	lässt den Mauszeiger auf zufällige Positionen springen
Fun Stuff		Hide Mouse	versteckt den Mauszeiger
		Lock CDs	sperrt den CD/DVD-Auswurf
		Go To URL	öffnet den Browser mit einem URL, den der Hacker festlegt
		Wallpaper	setzt das Hintergrundbild auf ein Image, das der Hacker auswählt
		Chat	eröffnet ein Chat-Fenster mit dem Opfer

Tabelle 2.1: Befehlsumfang der Backdoor (Forts.)

Kategorie	Ressource	Befehl	Beschreibung
		Restrictions	schränkt ein Opfer auf seinem eigenen System ein: System Disable Task Manager Disable Regedit Disable Command Prompt Disable Windows Keys Disable CD Burning Disable CD-ROM Autorun Disable Taskbar Right Click Disable Desktop Right Click Hide All Drives Remove Shut Down Button Remove Folder Options Menu Remove Run Button Remove Explorer File Menu Internet Explorer Disable Download Disable Close Button Disable Save As Disable Options Disable File/New Disable File/Open Disable Full Screen Remove Go Button Disable Favorites Disable Search Disable Printing Disable Right Click Disable Forward/Back Buttons Control Panel Hide Command Prompt in Start Menu Hide Display Hide Add/Remove Programs Hide Mouse Properties Hide Sounds And Audio Devices Hide User Accounts Hide Power Options Hide System Hide Date And Time Hide Regional And Lang. Options Hide Network Connections Hide Add Hardware Wizard Hide Phone And Modem Options

Tabelle 2.1: Befehlsumfang der Backdoor (Forts.)

Kategorie	Ressource	Befehl	Beschreibung
Server		Update	vollständige Neu-Konfiguration des Trojaners (siehe Abbildung 2.4), sofortige Abspeicherung und Ausführung auf dem Rechner des Opfers
		Close Server	Beendigung des Servers, so dass ein Absenden weiterer Befehle nicht mehr möglich ist
		Kill Server	Terminierung des Servers, so dass nicht mal mehr ein Connect durch den Hacker selbst möglich ist, ohne dass der Benutzer den Trojaner erneut gestartet hat
		Info	Abruf von Informationen über den Rechner des Opfers (bspw. Computername, Benutzerkonto-/gruppe) sowie über die konfigurierten Einstellungen des Trojaners selbst
Misc		Scanner	Aufruf eines Network Scanners, so dass der Hacker einen IP-Adressbereich von dem Rechner des Opfers aus auf aktive Devices abtasten kann (der Hacker selbst bleibt dabei anonym)
		Messages	Anzeige einer Message-Box auf dem Rechner des Opfers
		Run Appz	Ausführen eines beliebigen Kommandozeilenbefehls auf dem Rechner des Opfers und Umleitung der Ausgabe dieses Befehls auf den Rechner des Hackers
		KeyLogger	Download aller bisher aufgezeichneten Tastatureingaben
		Live Keys	Absenden von Tastatureingaben an die aktive Applikation auf dem Rechner des Opfers
		System Time	Modifikation des Systemdatums des Opfers

Tabelle 2.1: Befehlsumfang der Backdoor (Forts.)

Verfügt der Benutzer über eine Webcam, kann der Hacker sogar Fotos von dem Benutzer und dessen Umgebung anfertigen!

Die Tabelle 2.1 und die vorangehenden Abbildungen machen deutlich, welche Macht ein Hacker über den Rechner seines Opfers hat. Die folgenden Nachrichtenmeldungen aus 2007 unterstreichen den Stellenwert, den Trojaner im Vergleich zu Viren und Würmern in der Hacker-Community haben:

„Cyberattacken werden aggressiver: weniger Würmer, mehr Trojaner"

Würmer waren lange Zeit die größte Bedrohung im Internet, da sie sich selbständig vermehrten und für Denial-of-Service-Angriffe auf bestimmte Internet-Server angelegt wurden. Trojaner können sich dagegen nicht selbst vermehren, werden aber aufgrund der hohen Kontrolle, die sie dem Hacker ermöglichen, immer häufiger zum Ausspähen sensibler Nutzerdaten und zur Fernsteuerung fremder Systeme eingesetzt.

„Hacker kapern über 10.000 Web-Seiten"

Auf Basis des Hacker-Exploit-Kits *Mpack* haben Hacker ein Netz von mehr als 10.000 gehackten Web-Seiten geschaffen. Über die infizierten Web-Seiten werden die Surfer auf einen russischen Server weitergeleitet, dem eine Datenbank über Exploits für die Betriebssysteme und Browser der Benutzer zugrunde liegt. Während der Benutzer surft, sucht das Mpack-Kit einen geigneten Exploit aus der Datenbank heraus und installiert einen Keylogger sowie einen Trojaner auf dem Rechner des Opfers, mit deren Hilfe die Angreifer Benutzerkonten und Passwörter für Online-Banking-Seiten ausspähen können.

2.3.2 Spam

Spam-Mails sind unerwünschte, elektronisch übermittelte Nachrichten, die massenhaft zugestellt werden. Mittels Spam-Mails versenden Hacker als Trojaner getarnte Schadprogramme, oder sie nutzen die Sicherheitslücken in den angehängten PDF-, GIF- und ZIP-Dateien aus, um Kontrolle über die Rechner ihrer Opfer zu erlangen. Spam-Mails dienen Hackern auch dazu, unbedachte Benutzer auf ihre Phishing-Sites zu leiten, um dort deren Passwörter auszuspähen. Des Weiteren werden Spam-Mails für Werbezwecke des Absenders verschickt. Die Masse macht's: Bestellt nur ein Promille aller Spam-Empfänger das beworbene Produkt, lohnt sich das Geschäft für den Absender bereits. Bei einer Million versendeter Spam-Mails für ein Viagra-Produkt ergäben sich bereits 1.000 Besteller!

Spam-Mails können sehr einfach erstellt werden; noch einfacher ist die Tarnung der angehängten Datei. In dem folgenden Beispiel wird gezeigt, wie ein ausführbares Programm getarnt und verschickt wird. In Abbildung 2.7 wird dem Task-Manager, einer ausführbaren Systemdatei, der Dateiname `Urlaubsfoto.gif` verpasst.

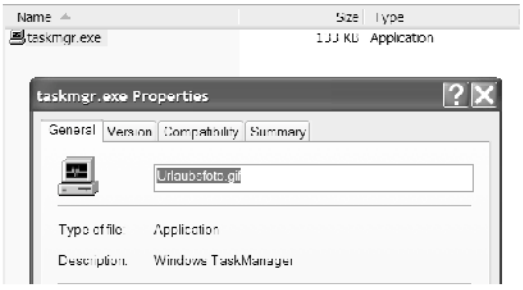


Abbildung 2.7: Tarnung eines E-Mail-Attachments

Anschließend wird die Dateiendung des Executables mit Hilfe des Hacking-Tools Create-Ext auf ein harmlos scheinendes GIF-Image umgebogen (Abbildung 2.8).

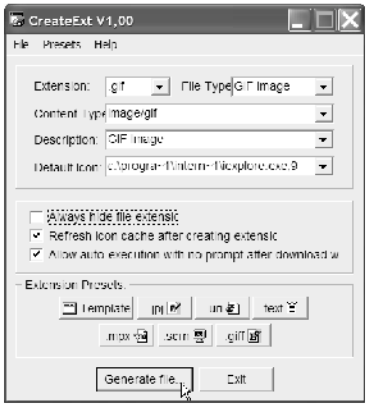


Abbildung 2.8: Verschleierung eines Executables als GIF-Image

Der Absender verfasst nun eine unverfänglich formulierte E-Mail und hängt seinen Trojaner als Attachment dieser E-Mail an. Die als GIF-Bild erscheinende Datei im Anhang ist in Wirklichkeit ausführbar, aber als solche nicht erkennbar, und wird in der Prozessliste des Betriebssystems als vollwertiger Prozess dargestellt (Abbildung 2.9).

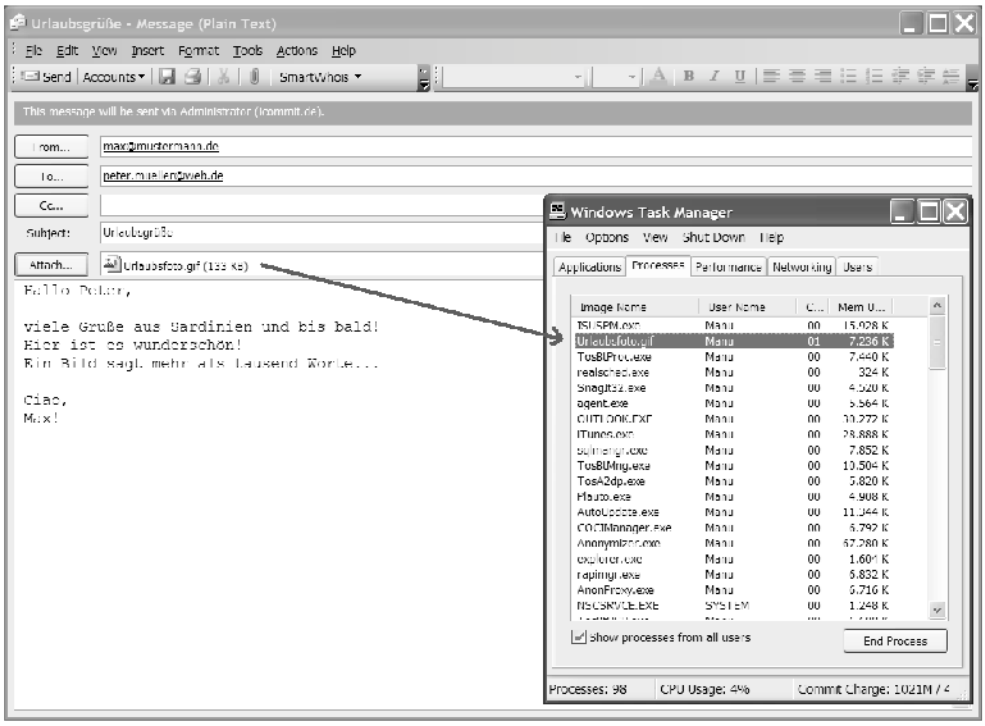


Abbildung 2.9: Versand einer Spam-Mail

Hinweis

Das oben aufgeführte Beispiel setzt voraus, dass die Dateierweiterung `.gif` nicht nur auf dem Rechner des Spammers, sondern auch auf dem betroffenen Zielsystem umgebogen ist. Dies wurde in dem Beispiel nicht demonstriert. Es ist aber über eine bekannte Sicherheitslücke in GIF-Dateien möglich, beim Öffnen eines GIF-Bildes Code auszuführen, der aus dem GIF-Bild ein Executable macht.

Um nicht zurückverfolgt werden zu können, versenden Spammer ihre Massen-E-Mails über anonyme Spam-Server, die die Hacker-Community zur Verfügung stellt. Wie aber gelangen Spammer an die ganzen E-Mail-Adressen, bei denen sie ihren Müll abladen? Nun, einerseits ist es möglich, den E-Mail-Versand über einen Virus oder einen Wurm abzuwickeln:

- Hierzu wird die Spam-Mail nur an einige wenige Empfänger geschickt.
- Öffnet einer dieser Empfänger das Attachment, reproduziert sich der darin enthaltene Virus und sendet die gleiche Mail an alle Kontakte weiter, die sich in dem Adressbuch des befallenen Opfers befinden.
- Wie eine Lawine vermehrt sich die Spam-Mail selbst und breitet sich wie ein Spinnennetz im Internet aus.

Andererseits stellt die Hacker-Community riesige E-Mail-Adress-Datenbanken gegen Gebühr zur Verfügung: je höher die Wahrscheinlichkeit, dass die darin aufgeführten E-Mail-Adressen tatsächlich existieren und von ihren Besitzern regelmäßig abgefragt werden, umso höher ist die Gebühr.

Um E-Mail-Adressen zu sammeln, installieren Hacker Trojaner auf den Rechnern unbedarfter Anwender. Diese Trojaner spähen die POP3-Account-Daten des Benutzers aus und melden sie dem Hacker.

Andere Hackergruppen wiederum sammeln die E-Mail-Adressen mit Hilfe automatisierter Tools. Abbildung 2.10 demonstriert, wie das Werkzeug *1st Email Address Spider* im Internet auf die Suche nach E-Mail-Adressen geht:

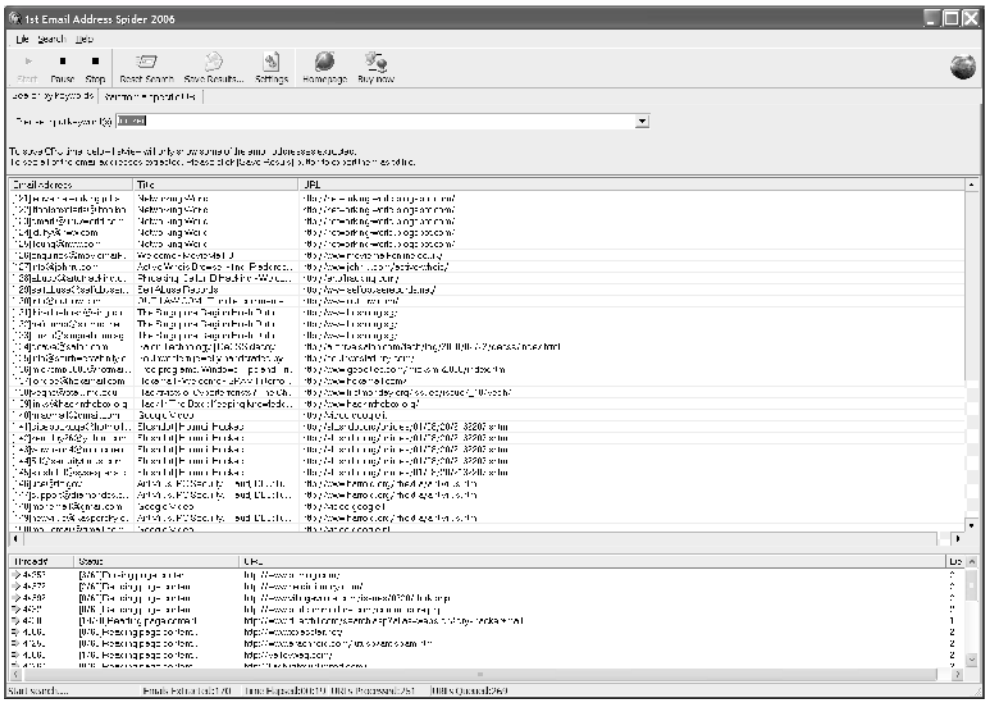


Abbildung 2.10: Auf der Suche nach E-Mail-Adressen ...

Der Hacker gibt ein oder mehrere Schlüsselwörter ein, die die Zielgruppe für die gesuchten E-Mail-Adressen eingrenzen. Der E-Mail-Spider führt für jedes dieser Schlüsselwörter eine Google-Suche durch. Jede der gefundenen Web-Seiten wird dann rekursiv nach E-Mail-Adressen durchsucht:

1. In dem HTML-Source-Code einer jeden Seite sucht der Spider nach Zeichenketten, die nach einer E-Mail-Adresse aussehen. Solche Zeichenketten können durch reguläre Ausdrücke beschrieben werden. Beispiel:

   ```
   \w+([-+.']\w+)*@\w+([-.]\w+)*\.\w+([-.]\w+)*
   ```

   Jede so gefundene E-Mail-Adresse wird gesammelt.

2. Anschließend wird der HTML-Source-Code dieser Seite nach absoluten und relativen Links durchsucht. Dies kann wiederum mit Hilfe regulärer Ausdrücke erfolgen. Beispiel:

   ```
   http(s)?://([\w-]+\.)+[\w-]+(/[\w- ./?%&=]*)?
   ```

   Jedem dieser Links wird gefolgt, um mit der referenzierten Seite wieder wie in Schritt 1 beschrieben zu verfahren.

Auf diese Weise durchläuft der E-Mail-Spider, ausgehend von einigen wenigen Startseiten, eine Vielzahl von Internet-Seiten und sammelt die dort veröffentlichten E-Mail-Adressen zwecks Ablage in einer Adress-Datenbank.

Hinweis

Die Sicherheitsbranche meldet im Jahr 2007:

„Attachment-Spam um das Zehnfache gestiegen"

Statistiken zur Auswertung des Werbemülls zeigen, dass die Spam-Szene die Ergebnisse verschiedener Dateianhänge austariert, um den Erfolg der entsprechenden Dateiendungen auszuwerten:

Spam-Mails mit Image-Attachment haben ca. sechs Prozent Anteil am Gesamt-Spam. Werbenachrichten mit PDF-, Excel-, Text- oder ZIP-Attachments sind zu 25 Prozent am Gesamt-Spam beteiligt.

Hersteller von AntiViren-Software wehren sich gegen Spam, indem sie die eingehenden E-Mails des Benutzers inspizieren.

- Dabei sucht die Software in dem Betreff und dem Inhalt der E-Mail nach bestimmten Schlüsselwörtern.
- Sie überprüfen das Absendedatum der E-Mail und die Verzögerung des Eintreffens.
- Sie befragen öffentliche Anti-Spam-Datenbanken, ob der Absender dort bekannt ist, und sie überprüfen, ob die E-Mail einen dort gelisteten URL enthält. Solche Anti-Spam-Datenbanken sind beispielsweise unter
  - *http://www.uceprotect.net/*
  - *http://www.spamhaus.org/*
  - *http://combined.njabl.org/*

  zu finden.

Die ersten beiden Kriterien sind für die Bewertung von Spam sicherlich sehr unscharf, da Schlüsselwörter wie „Viagra" beispielsweise durchaus absichtlich in einer E-Mail vorkommen dürfen. Auch sagen die Zeitstempel der E-Mail nicht viel aus, da sich die Übertragung im Internet je nach Auslastung der beteiligten Router und Mail-Server durchaus im Einzelfall verzögern kann. Mit ihrer Hilfe können höchstens Wahrscheinlichkeiten aufaddiert werden, die dem Anwender nahe legen, dass es sich um Spam handeln könnte. Nur die Abfrage gewissenhaft geführter Spam-Datenbanken kann einen verlässlichen Hinweis ergeben.

Anwender können vor Spam nicht zu 100 Prozent geschützt werden. Der einzige wirkliche Schutz besteht darin, keine Mails von unbekannten Absendern und erst recht keine Attachments zu öffnen. Diese organisatorischen Schutzmechanismen, die in der Verantwortung des Anwenders liegen, werden wiederum verwässert, wenn sich die Spam-Mail in Form eines Virus über die Adressbücher befreundeter Kontakte verbreitet ...

2.3.3 Phishing

Nichts ist leichter als Angeln. Einige einfache Werkzeuge reichen: ein Stock, eine Schnur und ein Haken. Der Köder ist schnell gefunden. Und je nachdem, in welchen Gewässern man fischt, können durchaus dicke Fische anbeißen ...

Gelingt es dem Hacker nicht, in ein gut geschütztes Online-Portal einzubrechen, so fragt er einfach deren Benutzer nach einer gültigen Kennung und meldet sich dann mit der gestohlenen Identität an.

Das Erstellen einer Phishing[2]-Site ist überraschend trivial: Dabei helfen bereits die gängigen Web-Browser! Die angewählte Seite muss lediglich aufgerufen und als Web-Seite (inklusive aller darin referenzierten Elemente) gespeichert werden. Abbildung 2.11 zeigt, wie die abgespeicherte Kopie der Anmeldeseite eines Online-Banking-Portals in einen lokalen Web-Server integriert werden kann.

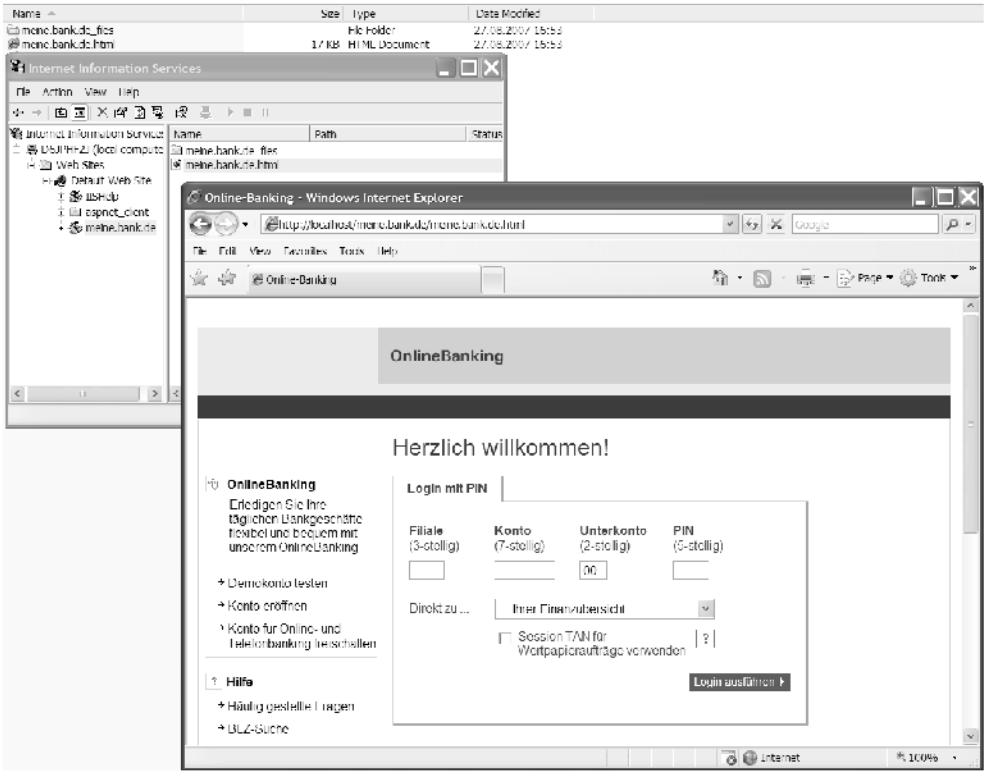


Abbildung 2.11: Kopieren der Anmeldeseite eines Online-Banking-Portals zwecks Phishing

2. „Phishing" ist ein Kunstwort und setzt sich aus den Begriffen „Password" und „Fishing" zusammen, beschreibt also das Abfangen von Passwörtern.

Ein Phisher würde nun einen fremden Web-Server im Internet kompromittieren und seine Phishing-Site dort hosten. Die kopierte Anmeldeseite für das Online-Banking-Portal würde er um ein Eingabefeld für die TAN des Benutzers erweitern; denn um eine Überweisung durchführen zu können, benötigt er das Konto, die PIN und eine TAN seines Opfers. Des Weiteren installiert er auf seinem Web-Server ein SSL-Zertifikat, so dass der Benutzer den Eindruck bekommt, er würde seine Anmeldung über eine sichere Verbindung abwickeln. Abbildung 2.12 zeigt die Vorgehensweise:

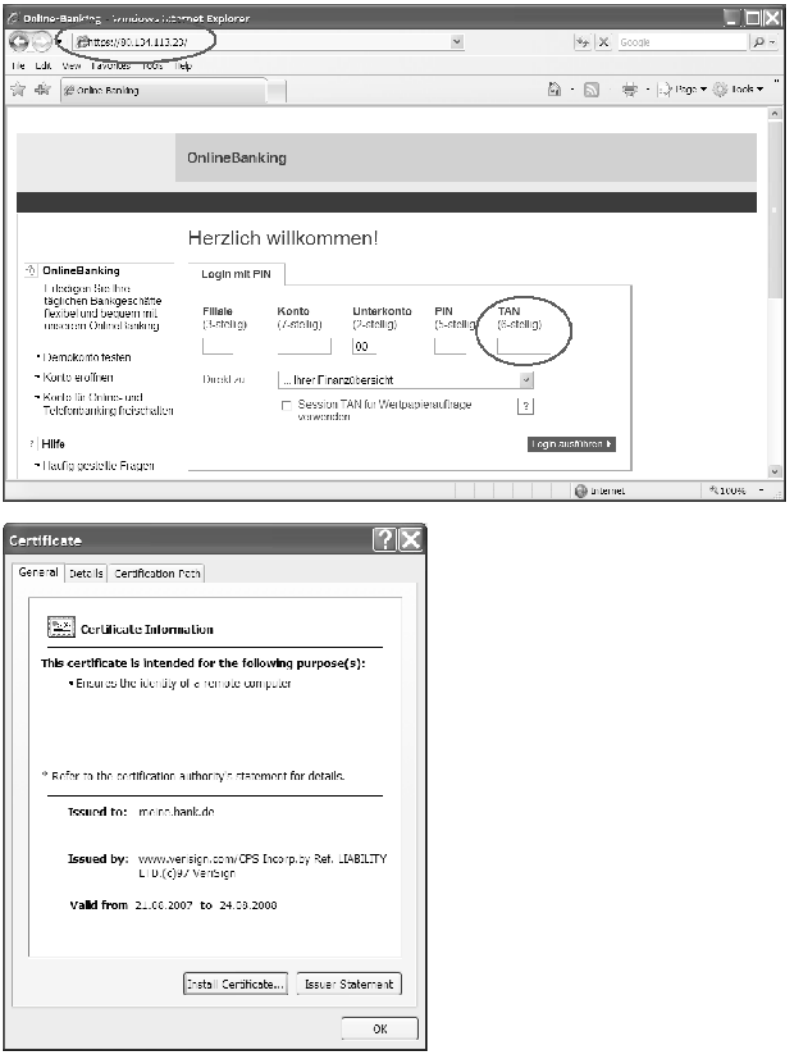


Abbildung 2.12: Modifzierte Anmeldung auf einer Phishing-Site mit PIN und TAN

Nun bleibt nur noch, der Anmeldeseite ein wenig Programmierung hinzuzufügen, so dass die eingegebenen Formulardaten in einer lokalen Datenbank gespeichert werden, bevor der Benutzer unwissentlich an das eigentliche Online-Banking-Portal weitergeleitet wird.

Im letzten Schritt formuliert der Phisher eine E-Mail, in der die Kunden der Bank über das vermeintlich geänderte Anmeldeverfahren informiert werden (Abbildung 2.13):

Abbildung 2.13: Versand einer Phishing-Mail

Die Phishing-Mail wird massenhaft an die dem Phisher bekannten E-Mail-Adressen verschickt oder über einen Virus oder Wurm verteilt. Die meisten Empfänger dieser E-Mail werden nicht Kunde der Online-Bank sein und die Mail verwerfen. Aber einen Teil der gewünschten Zielgruppe wird der Phisher mit einer solchen Mail erreichen ...

Die oben aufgeführte Phishing-Mail betrügt die unschuldigen Bank-Kunden gleich in mehrfacher Hinsicht:

- Unter dem Vorwand, die Sicherheit des Online-Bankings zu erhöhen, soll der Kunde ein Geheimnis preisgeben (eine seiner TANs).
- Die Mail enthält einen Link auf das vermeintlich echte Online-Banking-Portal, führt das Opfer aber unwissentlich auf die Phishing-Site. Den eigentlich über diesen Link adressierten Server kann der Benutzer nur herausfinden, indem er mit der Maus darüber fährt und die angezeigte IP-Adresse überprüft, oder indem er den HTML-Source-Code der E-Mail analysiert.

- Die Mail wird scheinbar von einer E-Mail-Adresse der echten Bank verschickt („From... *info@bank.de*“).
- Meldet sich der Kunde auf der Phishing-Site an, so speichert die von dem Phisher modifzierte Anmeldeseite die Anmeldedaten des Opfers ab und leitet die Anmeldung dann unbemerkt an das Original-Portal weiter.

Da Phishing so einfach und effektiv ist, wird der gesamte Vorgang von Hackern mittlerweile automatisiert:

„Phishing-Attacken häufen sich“

Nach Angaben des Branchenverbands Bitkom in Berlin stieg die Zahl der geschädigten Nutzer von Online-Banking in 2006 um 23 Prozent. Laut einer Bitkom-Hochrechnung haben Betrüger in 2006 insgesamt bundesweit in mehr als 3.250 Fällen rund 13 Mio. Euro von den Konten ihrer Opfer abgehoben. Man geht davon aus, dass sich die Zahl der Phishing-Opfer in 2007 nochmals um 25 Prozent erhöht. Dabei werden die Betrugsmethoden der Cyber-Kriminellen immer raffinierter: Nur noch 10 Prozent der Schäden entstehen durch E-Mails, die die Opfer auf gefälschten Bank-Seiten zur Eingabe ihrer Kontendaten verleiten. Stattdessen rüsten die Betrüger auf Trojaner um, die per E-Mail verschickt werden und die Daten auf dem Rechner des Opfers heimlich ausspähen.

„Phishing-Tool kreiert Betrüger-Sites in Sekunden“

Ein Hacking-Tool ermöglicht Identitätsdieben, eine Phishing-Site innerhalb von zwei Sekunden zu erstellen und auf einem gekaperten Server zu installieren. Das PHP-Skript installiert Bilder und JavaScript-Code automatisch in die richtigen Verzeichnisse.

Einer Gartner-Untersuchung zufolge haben sich Phishing-Attacken in den vergangenen zwei Jahren sogar verdoppelt. Demnach erlitten 2,3 Millionen Erwachsene finanziellen Schaden durch Online-Identitätsdiebstahl – der durchschnittliche Verlust liegt bei ca. 1.250 Dollar pro Opfer!

Der Diebstahl digitaler Identitäten erstreckt sich auf alle Internet-Portale, die einen Login erfordern: Amazon, eBay, Online-Banking und Rechnungsportale von Telekommunikationsunternehmen sind da nur wenige Beispiele.

2.3.4 Viren

Viren hängen sich an eine Datei, ihren sog. Wirt, und können erst aktiv werden, wenn der Wirt selbst die Kontrolle von der CPU erhält. Als Wirt werden meistens ausführbare Programme, Skripte oder Makros eingesetzt. Entsprechend spricht man von Link-Viren, Skript-Viren und Makro-Viren.

Viren können unterschiedlichste Schäden anstellen, aber im Prinzip bestehen die gleichen Möglichkeiten wie bei der Erstellung eines Trojaners (siehe Tabelle 2.1). Schäden, die Viren typischerweise anrichten, sind:

- Zerstörung von Dateien (betrifft: Programme und Daten)
- Zerstörung der Hardware (betrifft: Festplatten, Monitore, PCI-Karten, Prozessoren)
- Abstürze (betrifft: Betriebssystem, Dienste, Anwenderprogramme)
- Fehlverhalten (betrifft: Maus, Tastatur, CD/DVD-Laufwerk usw.)

Im Internet kursieren zahlreiche Virus Construction Kits, die in der Hacker-Community gegen Gebühr getauscht werden.

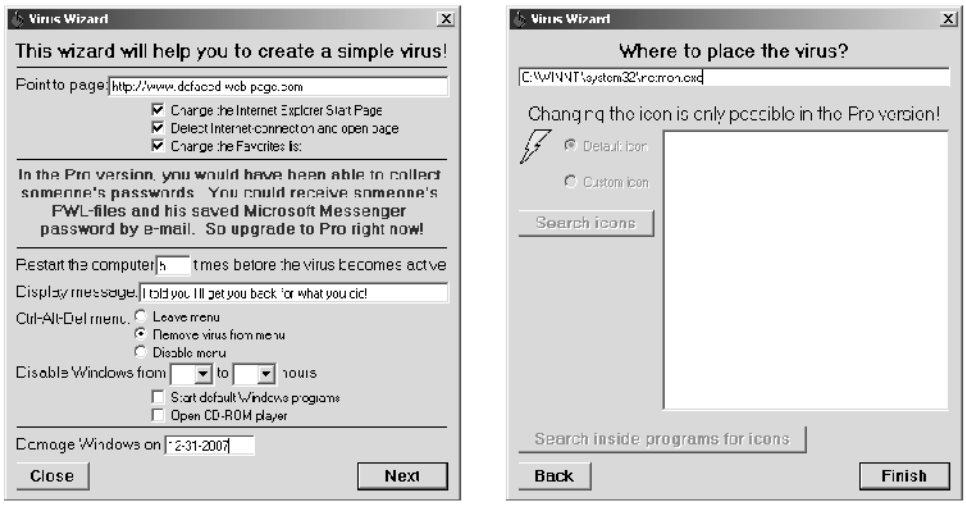


Abbildung 2.14: Erstellung eines Virus

Der *Virus Wizard* in Abbildung 2.14 zielt auf eine Denial-of-Service-Attacke (DoS) ab. Das Opfer ist die Domäne *www.defaced-web-page.com*. Der Virus stellt, einmal aktiviert, die folgenden Einstellungen auf dem infizierten Rechner ein:

- Die DoS-Attacke wird am 31.12.2007 ausgelöst.
- Ab diesem Zeitpunkt wird die Startseite des Internet-Explorers auf die Zieldomäne gesetzt, so dass der zuständige Server eine entsprechende Last erfährt.
- Der Virus selbst tarnt sich als Datei `netmon.exe` in dem Systemverzeichnis `c:\winnt\system32\`.
- Wenn nur ausreichend viele Rechner mit dem Virus infiziert sind, muss der Zielserver ab dem 31.12.2007 immer dann eine Anfrage beantworten, wenn nur einer der betroffenen Benutzer seinen Browser öffnet. Bei einigen Millionen Infektionen auf der Welt wird der Zielserver unter der Last der Anfragen unmittelbar ersticken und seinen Dienst verweigern.

Welche Verbreitung Computer-Viren im Internet haben, zeigt eine Veröffentlichung von Kaspersky Lab (Tabelle 2.2).

Virus	Kategorie	Beschreibung
Trojan-Spy.Win32.Banker.aqu	gierigster Schädling im Banken-bereich	gleichzeitige Ausbreitung in 87 verschiedenen Banken
Trojan-PSW.Win32.VB.kq	gierigster Schädling für elektro-nische Bezahlsysteme ...	simultaner Angriff auf vier Bezahl-systeme ...
Trojan-PSW.Win32.VB.kq	... und für Key Cards	... und vier Key-Card-Systeme
Backdoor.Win32.Hupigon.rc	am besten versteckter Schädling	Tarnung durch zehnfache Kompri-mierung mit verschiedenen ZIP-Programmen
Trojan.DOS.DiskEraser.b	kleinster Schädling	trotz einer Größe von neun Bytes kann der Schädling Festplatten-inhalte zerstören
Trojan.Win32.KillFiles.ki	größter Schädling	für das simple Löschen von Dateien streckt sich dieser Virus über 247 MB
Backdoor.Win32.Agobot.afy	feindseligster Schädling	löscht installierte AntiVirus-Programme
Email-Worm.Win32.NetSky.t	im E-Mail-Traffic am weitesten verbreiteter Schädling	ein älterer Wurm, der über 15 % des schädlichen E-Mail-Verkehrs auf sich vereint
Backdoor.Win32.Rbot	am weitesten verbreitete Familie unter den Trojanern	die Rbot-Familie brachte über 454 Modifikationen hervor
Warezov-Familie	am weitesten verbreitete Familie unter Viren und Würmern	die Warezov-Familie trat in 78 ver-schiedenen Modifikationen auf

Tabelle 2.2: Top-10-Viren-Liste (Kaspersky Lab, Stand: Juni 2007)

Um ein System zu befallen, vermehren sich Viren, indem sie sich an andere Programme hängen. Zu diesem Zweck prüft der Virus zunächst, ob die Zieldatei bereits infiziert ist. Ansonsten würde der Virus dieselbe Datei mehrfach infizieren und aufgrund der Dateigröße der befallenen Datei schnell auffallen. Dieses Erkennungsmuster bezeichnet man als Signatur des Virus. AntiViren-Programme suchen in den Dateien auf der Festplatte des Anwenders nach Virensignaturen. Wird die Signatur eines Virus gefunden, versucht die AntiViren-Software die befallene Datei von dem Virus zu befreien, indem sie den Virus von ihrem Wirt wieder abhängt. Hat der Virus jedoch Teile der ursprünglichen Datei zerstört, bleibt der AntiViren-Software nichts anderes übrig, als die mit dem Virus infizierte Datei in Quarantäne zu stellen und der Nutzung durch den Anwender zu entziehen.

Besonders schwierig zu finden sind Viren, die sich selbst tarnen:

- Metamorphe Viren ändern ihre Signatur. Bevor ein solcher Virus eine Datei befällt, erzeugt er temporär seinen eigenen Source-Code, modifiziert diesen und übersetzt sich wieder in ausführbaren Code zurück. Diese Übersetzung und Rückübersetzung ist möglich, da sich beide Formen, Maschinensprache und Assemblersprache,eindeutig in beide Richtungen umformen lassen[3]. Metamorphe Viren sind für Virenscanner schwer zu entdecken, da Virenscanner nach der vermeintlich eindeutigen Signatur eines Virus suchen.
- Verschlüsselte Viren codieren ihren ausführbaren Teil. Sie enthalten eine Entschlüsselungsroutine, die den eigentlichen Virus-Code zur Laufzeit wieder entschlüsselt. Hat ein AntiViren-Hersteller die Entschlüsselungsroutine eines solchen Virus erst einmal entdeckt, ist es allerdings ein Leichtes, auch den ausführbaren Teil des verschlüsselten Virus zu entschlüsseln, um dessen Signatur zu erhalten.
- Polymorphe Viren ändern ihre Gestalt, meist in verschlüsselter Form, so dass von Generation zu Generation verschiedene Varianten des Virus entstehen. Meist werden dabei mehrere unterschiedliche Verschlüsselungsverfahren eingesetzt.
- Stealth Viren tarnen sich, in dem sie ihren Code in ungenutzte Bereiche einer Datei kopieren oder sich in den Systemaufrufen des Betriebssystems festsetzen, damit sie zur Laufzeit Fake-Aussagen über die Größe und den Inhalt der befallenen Datei geben können.
- Retroviren gelten als besonders gefährlich, da sie AntiViren-Programme und Firewalls deaktivieren. Damit ermöglichen sie, dass auf dem befallenen System beliebige Backdoor-Applikationen installiert werden können.
- Das Problem der Computerviren besteht seit den 1980er Jahren. Mittlerweile wurden Viren weitestgehend von Würmern abgelöst, da Würmer keinen Wirt benötigen, um sich zu aktivieren.

2.3.5 Würmer

Würmer sind die wirklich gefährliche Plage des heutigen Internets. Einmal ausgesetzt, vermehren sie sich selbst und befallen aktiv alle in einem Netzwerk erreichbaren Rechner. Würmer sind nicht wie Viren auf ein externes Auslösen angewiesen; sie verbreiten sich daher schnell und effizient.

Würmer verbreiten sich über infizierte E-Mails oder über Netzwerke. In letzterem Fall kontaktieren sie selbst die von einem befallenen Rechner erreichbaren Netzwerkressourcen und versuchen alle Ziele zu befallen, derer sie habhaft werden können. Einige prominente Beispiele aus der Vergangenheit:

3. Mathematiker würden die Funktion Ü:A‡M, die einen in Assembler formulierten Quelltext in eine Maschinensprache übersetzt, als bijektiv bezeichnen, da eine Übersetzung in beide Richtungen eindeutig ist.

- Der Loveletter-Wurm, auch als „I love you“ bekannt, verbreitete sich im Mai 2000 explosionsartig per E-Mail mit der Betreffzeile „ILOVEYOU“. Die Mail enthielt im Anhang eine Datei mit dem Namen „LOVE-LETTER-FOR-YOU.TXT.vbs“, die viele Anwender für eine ungefährliche Textdatei hielten. Das tatsächliche VBScript-Makro versendete die Mail automatisch an alle Einträge im Adressbuch des betroffenen Anwenders und hat in wenigen Stunden viele Mailserver weltweit überlastet.
- Der Wurm Code Red befiel im Juli 2001 alle Computer, auf dem der Web-Server Internet Information Server von Microsoft installiert war. Der Wurm gab sich zu erkennen, indem er die Web-Seiten der befallenen Server mit dem Satz „Hacked By Chinese!“ verunstaltete.
- Der SQL-Slammer, auch unter der Bezeichnung Sapphire bekannt, befiel im Jahre 2003 alle Server, auf denen die Datenbank Microsoft SQL Server installiert war. Innerhalb von 30 Minuten befiel der Wurm über 75.000 Systeme (Abbildung 2.15). Obwohl die Sicherheitslücke, die der Wurm in der Datenbank ausnutzte, längst bekannt war und ein Patch des Herstellers vorlag, waren viele Datenbanken nicht aktualisiert, und der Wurm konnte in kürzester Zeit einen Großteil des Internet-Verkehrs lahm legen.

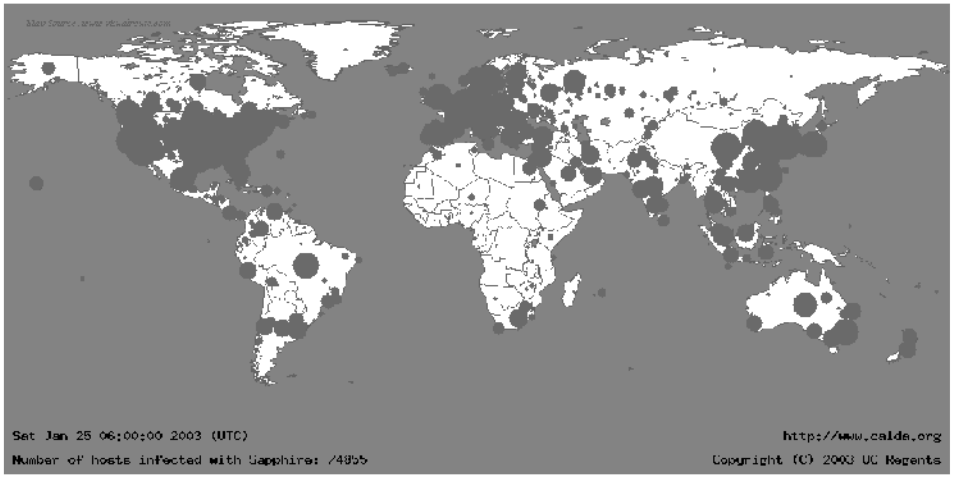


Abbildung 2.15: Ausbreitung des Wurms „SQL Slammer“ in 2003

Würmer lassen sich so einfach wie Viren erstellen. Abbildung 2.16 zeigt einen *Internet Worm Generator* in Aktion:

- Das Tool erstellt einen neuen Makrowurm, der sich in die Systemdatei notepad.exe unter *c:\winnt\system32* kompiliert und dort festsetzt.
- Der Wurm wird beim Hochfahren des befallenen Systems automatisch gestartet und verbreitet sich dann in Form von E-Mails über das Outlook-Adressbuch des Opfers.

Würmer sind ausführbare Programme (Binärcode) oder interpretierter Source (Makrocode). Als solches sind Würmer darauf angewiesen, vom Benutzer ausgeführt zu werden (z.B. durch Starten der Applikation `notepad.exe`) oder durch Ausnutzen einer Sicherheitslücke automatisch aktiviert zu werden (z.B. im `Internet Explorer`). Mittlerweile gibt es Würmer, die sich über Bluetooth, P2P-Netzwerke und Instant-Messaging-Anwendungen verbreiten.

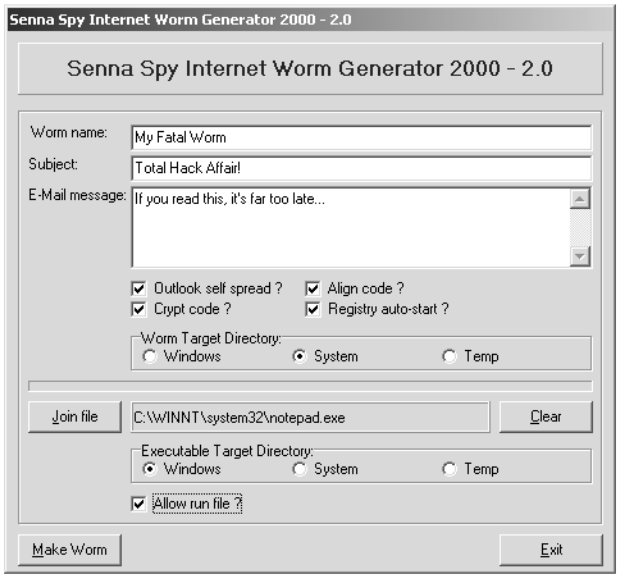


Abbildung 2.16: Erstellung eines Wurms

2.3.6 Spyware

Als Spyware bezeichnet man Software, die den Benutzer eines Computers ausspioniert, sog. Schnüffelprogramme. Da die meisten Benutzer volle Administrationsrechte auf ihrem Rechner haben, kann jede Applikation, die der Benutzer startet, frei auf alle Ressourcen des Rechners zugreifen. Gelingt es einem Hacker, den Benutzer zur Ausführung eines getarnten Executables zu verleiten, kann ohne Wissen des Anwenders eine vollwertige Spyware auf dem betroffenen Rechner des Opfers installiert werden. Dies ermöglicht dem Hacker, sämtliche Aktivitäten auf dem betroffenen Rechner zu überwachen: Tastatureingaben protokollieren, Screenshots erstellen und vieles mehr. Abbildung 2.17 zeigt die Konfiguration einer Spyware und verdeutlicht das Maß der Kontrolle des Hackers über die Benutzeraktivitäten seines Opfers:

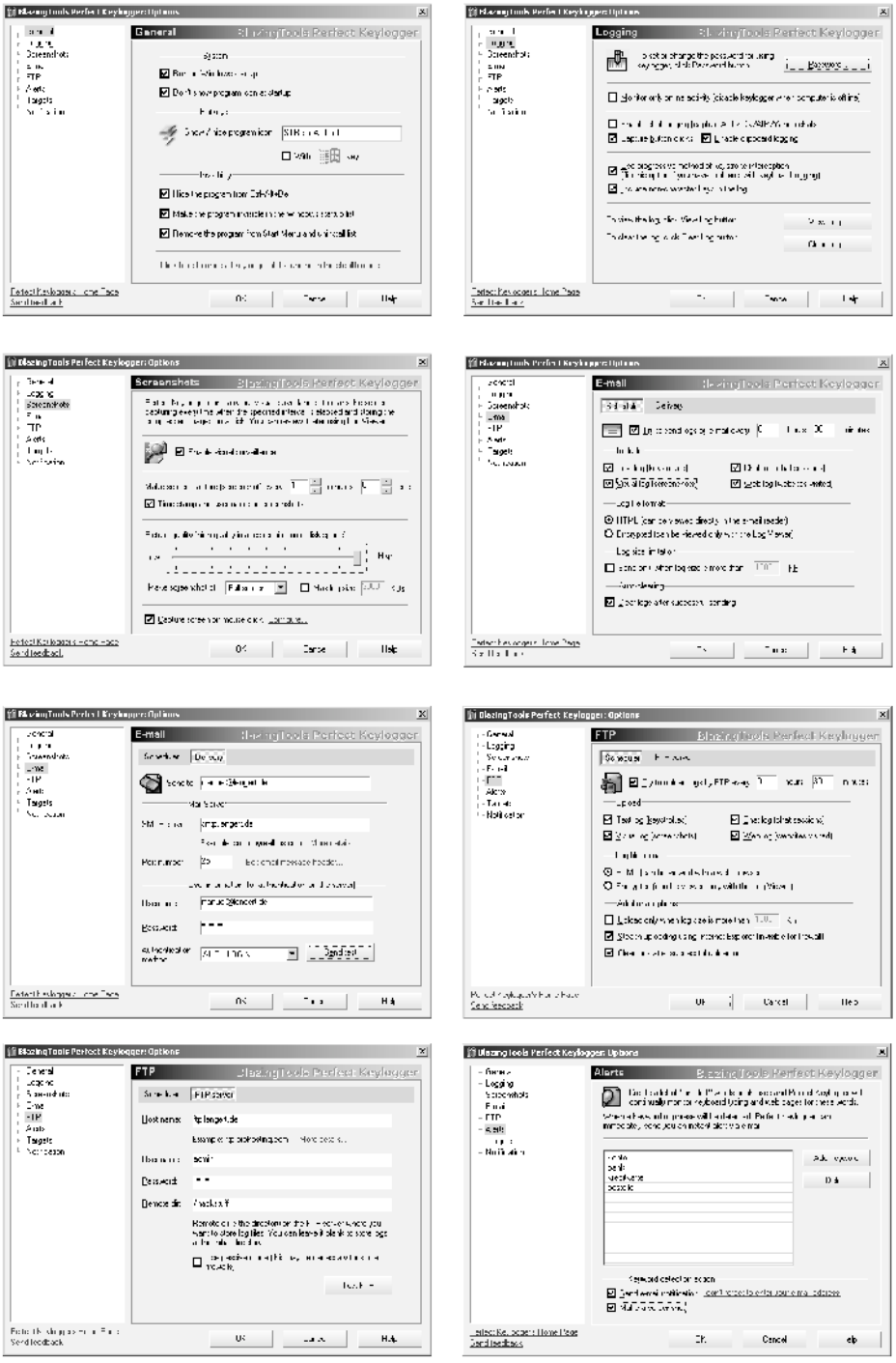


Abbildung 2.17: Spyware im Stealth Mode

Die Spyware kann von einem Hacker wie folgt konfiguriert werden:

- General

  Mit dem Hochfahren des Systems wird automatisch auch die Spyware gestartet, und zwar derart versteckt, dass die Spyware quasi unsichtbar bleibt: Sie ist weder im Task-Manager sichtbar noch im Start-Menü noch in der Liste der deinstallierbaren Programme und auch nicht in der Liste der beim Systemstart automatisch gestarteten Prozesse.

- Logging

  Protokolliert werden alle Tastaturanschläge und Mausklicks sowie Änderungen am Inhalt der Zwischenablage.

- Screenshots

  Minütlich wird ein Screenshot von der Bildschirmansicht des Benutzers erstellt und heimlich als Bilddatei abgespeichert. Auf den Screenshots wird ein Zeitstempel eingetragen. Zusätzlich wird bei jedem Mausklick ein weiterer Screenshot erstellt.

- E-Mail

  Die Spyware übermittelt die gesammelten Protokolle im Abstand von 30 Minuten automatisch per E-Mail an den Hacker. Dies umfasst das Tastaturprotokoll, die erstellten Screenshots, besuchte Web-Sites und aufgezeichnete Chat-Sessions.

- FTP

  Gleichfalls alle 30 Minuten lädt die Spyware die erstellten Protokolle auf einen FTP-Server hoch.

- Alerts

  Letztlich werden der Spyware einige Alerts eingestellt, so dass bei der Eingabe eines der Schlüsselwörter „konto“, „bank“, „kreditkarte“ oder „bestelle“ durch den Benutzer eine sofortige E-Mail-Notifikation inklusive Screenshot an den Hacker gesendet wird.

Abbildung 2.18 zeigt die Spyware-Protokolle, die dem Hacker automatisch zugestellt werden[4].

Links werden alle Tastaturanschläge („Keystrokes“) angezeigt inklusive aller Sondertasten. Rechts werden die aufgezeichneten Screenshots dargestellt.

Gibt der Benutzer eines der überwachten Schlüsselwörter ein, wird der Hacker umgehend per E-Mail darüber informiert. Abbildung 2.19 zeigt eine E-Mail, die das Opfer absendet und die mit Hilfe eines Hacker-Alerts unwissentlich von der Spyware überwacht wird:

4. Die in eckigen Klammern aufgeführten Tasten bezeichnen Sondertasten (z.B. [STRG], [ALT], [TABULATOR] und [EINGABE]).

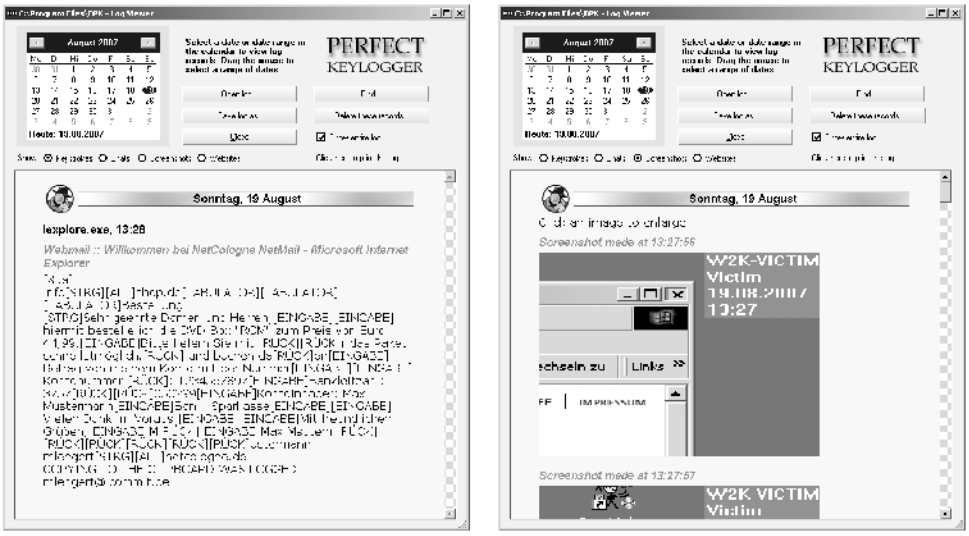


Abbildung 2.18: Spyware-Protokoll

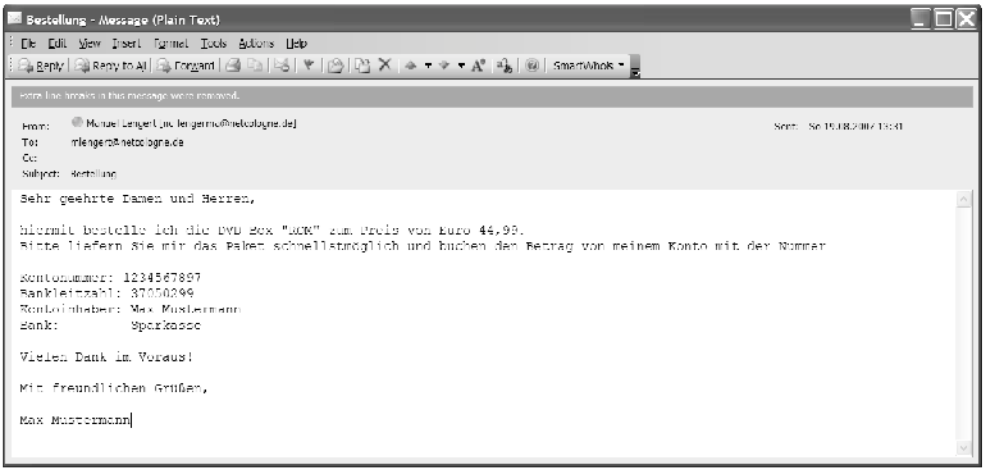


Abbildung 2.19: Spyware-Alert bei Eingabe von Bankdaten

Abbildung 2.20 demonstriert die von der Spyware aufgezeichneten Protokolle, die der Hacker bei einem Alert erhält:

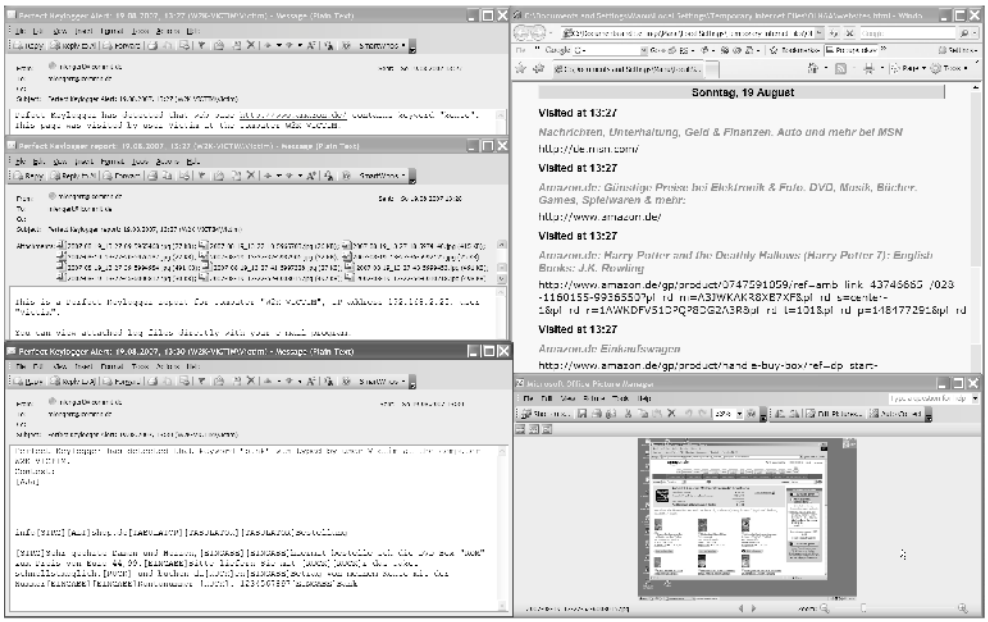


Abbildung 2.20: Spyware-Protokolle bei der Auslösung eines Alerts

Im Beispiel bestellt der Anwender per E-Mail eine DVD und gibt dabei seine Bankverbindung ein. Bei der Eingabe eines der Schlüsselwörter „konto“, „bank“, „kreditkarte“ oder „bestelle“ sendet die Spyware dem Hacker einige E-Mails mit den bisher aufgezeichneten Protokollen zu: besuchte Web-Sites, Screenshots und die von dem Opfer verfasste E-Mail, die dessen Bankverbindung enthält.

In den USA wird Spyware mittlerweile in vielen großen Unternehmen zur Kontrolle ihrer Mitarbeiter eingesetzt. Die Mitarbeiter werden einmalig über die Aufzeichnung ihrer Aktivitäten informiert und müssen der Installation der Spyware zustimmen. Anschließend können Systemadministratoren bei Bedarf auf die Aktivitätenprotokolle der Mitarbeiter zugreifen.

Nachdem in diesem Kapitel der Wirkungsgrad von Hackern im privaten Umfeld demonstriert wurde, widmet sich das nächste Kapitel dem professionellen Einbruch von Hackern in Unternehmensnetzwerke.

2.4 Goldene Regeln für jeden Internet-User

Die meisten Viren, Würmer und Trojaner zielen auf Privatanwender ab und können durch ihre massive Ausbreitung einen immensen Schaden anrichten: Datenverlust, Diebstahl sensibler Informationen, bis hin zum Blockieren des Netzwerkverkehrs und anvisierter Zielserver. Leider ermöglicht erst die Unbekümmertheit der meisten Computernutzer die Ausbreitung solcher Schädlinge. Ohne Anspruch auf Vollständigkeit folgen einige simple, aber wirksame Empfehlungen, mit denen sich Privatanwender vor der Verbreitung von Malware und dem Befall ihrer Rechner schützen können.

Regel 1: Nehmen Sie nichts von Fremden an!

Dies ist eine der ersten Regeln, die Kinder von ihren Eltern lernen. Warum aber öffnen so viele Computernutzer E-Mails von Personen, die sie nicht kennen? Spam-Mails sind darauf ausgelegt, Neugier zu erregen, Interesse zu wecken. Dabei geht es in erster Linie nicht darum, einfach nur Werbemüll zu versenden, sondern den Computernutzer dazu zu bringen, ein Attachment zu öffnen oder einem Link zu folgen, um Schadsoftware auf einem fremden Rechner auszuführen. Die Folgen eines solchen unbedachten Tuns wurden in diesem Kapitel ausführlich beschrieben. Einem Großteil der drohenden Gefahr können Sie ausweichen, wenn Sie ausschließlich die Post von Bekannten öffnen und jede andere E-Mail ungelesen löschen. Wenn Sie dem Link in einer E-Mail folgen möchten, sollten Sie niemals auf den Link klicken[5], sondern den URL von Hand in einem Browserfenster eingeben. Seriöse Shops und Banken führen niemals URLs in dem Nachrichtentext einer E-Mail auf, weil Spam-Mails den Benutzer über gefälschte URLs auf Phishing-Sites führen.

Regel 2: Seien Sie sich darüber bewusst: Nichts muss so sein, wie es scheint!

Alle Informationen, aus denen eine E-Mail zusammengesetzt ist, können gefälscht sein:

- Der Absender kann den Anzeigenamen seiner E-Mail-Adresse fälschen (z.B. *Online Banking* statt *Johnny Hacker*).
- Die E-Mail-Adresse des Absenders kann gefälscht werden (z.B. *info@meine-bank.de* statt *hacker@internet-provider.de*).
- Der Name und die IP-Adresse des Mail-Servers, über den die E-Mail verschickt wurde, kann gefälscht werden (z.B. *smtp.web.de* statt *80.101.150.25*).
- In der E-Mail enthaltene Links müssen nicht auf den angezeigten URL verweisen (beispielsweise wird *onlinebanking@meine-bank.de* angezeigt, der Link verweist jedoch auf den Phishing-Server *80.101.150.80*).
- Attachments sind nicht zwingend harmlose Grafiken, Filme oder Dokumente, sondern können durchaus beliebige Anwendungen ausführen, insbesondere Malware.

Computernutzer müssen davon ausgehen, dass eine E-Mail nicht unbedingt von dem angezeigten Absender selbst verschickt wurde. Geschickt organisierte Spam-Mails verteilen sich über die Outlook-Adressbücher miteinander kommunizierender Computernutzer, so dass sich Spam von Freund zu Freund, von Kollege zu Kollege, von Geschäftspartner zu Geschäftspartner verbreitet. Ähnlich der Vernetzung auf sozialen Plattformen, wo Kontakte untereinander gepflegt und ausgetauscht werden, verteilt sich der Spam unter Menschen, die einander vertrauen. Mit dem Unterschied, dass nicht der Mensch selbst die Spam-Mail verschickt, sondern ein Trojaner auf dessen Rechner unbemerkt das E-Mail-Konto des betroffenen Benutzers ausnutzt!

Hinterfragen Sie daher kritisch, ob die E-Mail Ihres Freundes den richtigen Ton trifft. Wenn Sie persönlich auf Aktien, Medikamente, Urlaubsfotos oder Nachrichten aus der Wirtschaft angesprochen werden, sollten Sie stutzig werden.

Wenn Sie Bilder, Videos, Office- oder PDF-Dokumente aus einer E-Mail öffnen, müssen Sie sicher sein, dass die E-Mail tatsächlich von dem angegebenen Absender stammt. Selbst wenn das der Fall ist, heißt das noch lange nicht, dass der Absender den Ursprung dieser weitergeleiteten Mail selbst überprüft hat. Er könnte unwissentlich einen Schädling an Sie durchgereicht haben. Vielleicht nutzt er nichtmals eine AntiViren-Software?

5. Es sei denn, Sie sind absolut sicher, dass der Link zu dem gewünschten Ziel führt.

Regel 3: Seien Sie grundsätzlich misstrauisch!

Viele Quellen im Internet sind nicht vertrauenswürdig: P2P-Netzwerke und binäre Newsgroups verteilen u.a. Malware. Download-Software enthält nicht nur das, was an der Oberfläche angeboten wird: Bildschirmschoner, Gamer-Cheats und Trailer können Malware enthalten, die sich unbemerkt installiert!

Regel 4: Geben Sie keine vertraulichen Daten preis!

Viele Unternehmen fordern den Anwender für den freien Download ihrer Software auf, sich im Gegenzug zu registrieren. Dabei sind persönliche Daten einzugeben. Leider reichen nicht wenige Unternehmen Ihre Daten zum Verkauf weiter. Es ist sogar davon auszugehen, dass es einem Hacker gelingt, unbemerkt in das Unternehmensnetzwerk einzubrechen und die Daten der registrierten Benutzer auszuspähen. Aus diesem Grund sollten Privatanwender grundsätzlich keine persönlichen Daten preisgeben: keinen Namen, keine Adresse, keine Telefonnummer und erst recht keine E-Mail-Adresse! Wenn die Eingabe einer E-Mail-Adresse zwingend erforderlich ist, um sich erfolgreich registrieren zu können, dann richten Sie zu diesem Zweck einen speziellen Alias für Ihr E-Mail-Konto ein. Geben Sie nie die wahre Bezeichnung Ihres E-Mail-Kontos preis, beispielsweise *vorname.nachname@provider.de*. Verwenden Sie stattdessen Aliase wie zum Beispiel *tageszeitung@provider.de*, *shop@provider.de* und *auktionshaus@provider.de*. Erhalten Sie unerwünschten Werbemüll, können Sie den Alias jederzeit löschen und werden fortan nicht mehr belästigt. Richten Sie über fünfzig Aliase ein: Jeder Alias wird nur genau einmal kommuniziert. Sollten Sie einmal eine unerwünschte E-Mail von einem Unternehmen bekommen, dem Sie den Alias nicht genannt haben, wissen Sie sofort, welches schwarze Schaf Ihre Daten weiterverkauft hat[6]! Und sollten sich in diesem Fall an das Unternehmen selbst oder an eine öffentliche Beschwerdestelle wenden ...

Seien Sie vorsichtig, welche persönlichen Daten Sie preisgeben. Gehen Sie davon aus, dass soziale Plattformen wie *Xing*[7], *Monster*[8] und *Stayfriends*[9] von Dritten abgetastet werden, um persönliche Informationen zu sammeln. Um zu überprüfen, welche Spuren Sie bereits im Internet hinterlassen haben: Suchen Sie über Google mal nach Ihrem Namen, Ihrer E-Mail-Adresse oder sonstigen persönlichen Daten!

Misstrauen Sie sämtlichen E-Mails, in denen Sie aufgefordert werden, Geheimnisse preiszugeben. Ihre Bank wird Sie niemals auffordern, außerhalb des OnlineBankings Ihre PIN oder eine Ihrer TANs einzugeben.

Regel 5: Speichern Sie niemals vertrauliche Daten auf Ihrem Rechner!

Passwörter, Bankverbindungen und Kreditkartennummern gehören nicht auf Ihren Rechner, denn dort können sie leicht ausspioniert werden. Solche Daten sollten Sie auch keiner Sicherheitssoftware anvertrauen, die „speziell gesicherte Dateien" für den Schutz persönlicher Daten anbietet: Hacker konzentrieren sich besonders darauf, solche Software anzugreifen, um an die verwalteten Geheimnisse zu gelangen. Passwörter und Zahlungsdaten dürfen niemals dort abgelegt werden, wo man sie benötigt!

---

6. Erhalten Sie an den Alias *tageszeitung@provider.de* eine E-Mail von einem Online-Shop, können Sie sicher sein, dass die Tageszeitung Ihre E-Mail-Adresse an den Online-Shop weiter verkauft hat.
7. *www.xing.com*
8. *www.monster.de*
9. *www.stayfriends.de*

Regel 6: Halten Sie sich fern von Internet-Cafés und WLAN-HotSpots!

Computer in Internet-Cafés sind besonders der Gefahr ausgesetzt, mit Malware verseucht zu werden. Der Besuch vieler Web-Sites durch unbekümmerte User birgt ein hohes Risiko, sich einen Virus, Wurm oder sonstigen Trojaner einzufangen.

Wählen Sie sich auch nicht in WLAN-HotSpots ein! Alle Rechner, die mit einem bestimmten WLAN-HotSpot kommunizieren, sind unweigerlich miteinander vernetzt. Wissen Sie, wer solche Netze abtastet, um sich auf einen ungeschützten Rechner aufzuwählen?

Regel 7: Schotten Sie Ihren Rechner ab!

Seltsamerweise lassen viele Computernutzer ihren Rechner dauernd an und schalten lediglich den Bildschirm aus. Unwissend, dass der DSL-Router eine permanente Internet-Verbindung aufrecht hält, ist der Rechner somit ständigen Angriffsversuchen ausgesetzt. Schalten Sie Ihren Rechner stattdessen auf *Stand-By*.

Wenn Sie auf Ihrem Rechner wichtige Arbeiten ausführen, so dass Sie ein Ausfall teuer zu stehen kommt, sollten Sie darüber nachdenken, einen preiswerten Zweitrechner fürs Surfen und Mailen einzusetzen. Schotten Sie den Rechner, dessen Daten geschützt werden müssen, vom Netz ab. Arbeiten Sie bestenfalls mit einem Notebook und deaktivieren Sie die WLAN-Karte und die Bluetooth-Verbindung. Fängt sich der andere Rechner, den Sie für die Internet-Kommunikation einsetzen, eine Schadsoftware ein, trifft Sie das nicht so hart. Wenn Sie sich nur einen Rechner leisten können, dann aktivieren Sie die Internet-Verbindung nur dann, wenn Sie sie tatsächlich benötigen. Eine Firewall kann Sie nur bedingt schützen. Aber ein physikalischer Schutz wie ein getrenntes Netzwerkkabel oder eine deaktivierte WLAN-Verbindung bieten einen bestechenden Schutz!

Regel 8: Entziehen Sie sich selbst Ihre Admin-Rechte!

Der wirksamste Schutz besteht darin, die eigenen Rechte zu beschneiden. Die meisten Computernutzer verfügen über administrative Rechte. Damit läuft jede Software-Installation erfolgreich durch. Allerdings wird dabei gerne übersehen, dass jede Applikation, die der Anwender aufruft, mit dessen Rechten gestartet wird. Insbesondere E-Mail-Attachments werden, einmal aufgerufen, mit den Rechten des angemeldeten Benutzers gestartet. Ein Paradies für Keylogger, Screenshot-Captures, Remote-Desktops, Viren, Würmer und Hintertüren, wenn der Benutzer selbst Administrator des Systems ist! Denn die meisten Malware-Programme benötigen uneingeschränkte Rechte für ihre Installation, um beispielsweise Treiber für die Protokollierung der Tastaturanschläge einzurichten.

Aber wie häufig installieren Sie Programme? Fünf bis zehnmal im Monat? Und in der restlichen Zeit arbeiten Sie als ganz gewöhnlicher Benutzer mit Outlook, Word, Adobe Reader und anderen Applikationen?

Lassen Sie die Malware erfolglos ins Leere laufen, indem Sie sich zwei Benutzerkonten auf Ihrem Rechner einrichten: ein Administratorkonto und ein einfaches Benutzerkonto mit stark eingeschränkten Rechten. Das Administratorkonto verwenden Sie für Software-Installationen und in Situationen, in denen Sie bevorzugte Rechte benötigen. Arbeiten Sie ansonsten immer mit dem reduzierten Benutzerkonto. Damit beeinflussen Sie Ihre Arbeit nicht, denn die meisten Applikationen benötigen für ihre Ausführung keine administrativen Rechte. Sie schränken jedoch merklich den Wirkungsgrad von Schadsoftware ein, denn Treiberinstallationen sind mit gewöhnlichen Benutzerrechten nicht möglich.

3 Professioneller Einbruch

Hacker haben ein wohldefiniertes Ziel: Sie brechen in Netzwerke ein, um Informationen über ein Unternehmen, dessen Angestellte, Produkte oder Projekte zu beschaffen. Hacker verschaffen sich Zugriff auf die Kundendaten eines Unternehmens, insbesondere auf Bankverbindungen und Kreditkartensätze. Sie erlangen Kontrolle über die Unternehmensrechner, um diese für eigene Zwecke einsetzen und fernsteuern zu können. Oder sie stören die Dienste, die ein Unternehmen bereitstellt, oder setzen diese sogar ganz außer Kraft. Manche Hacker modifizieren Web-Sites, um politische oder religiöse Botschaften zu verbreiten (*defacing*).

Ein professioneller Hacker geht methodisch vor. Er verfolgt einen Plan und bereitet diesen sorgfältig vor, indem er zunächst möglichst viele Informationen über sein Zielnetzwerk sammelt, eine Angriffsstrategie entwickelt und erst dann gezielt zuschlägt.

Wie gehen professionelle Hacker vor? Was müssen Sicherheitsverantwortliche bedenken? Wie läuft ein typischer Einbruch ab?

Dieses Kapitel zeigt den typischen Ablauf eines professionellen Einbruchs. Es verdeutlicht, dass Hacker keinem Zufallsmuster folgen, sondern methodisch die schwächste Komponente in dem Netzwerk ihres Opfers suchen, bevor sie diese gezielt angreifen.

3.1 Vorgehensmodell

Ein professioneller Einbruch verläuft in fünf Phasen (Abbildung 3.1):

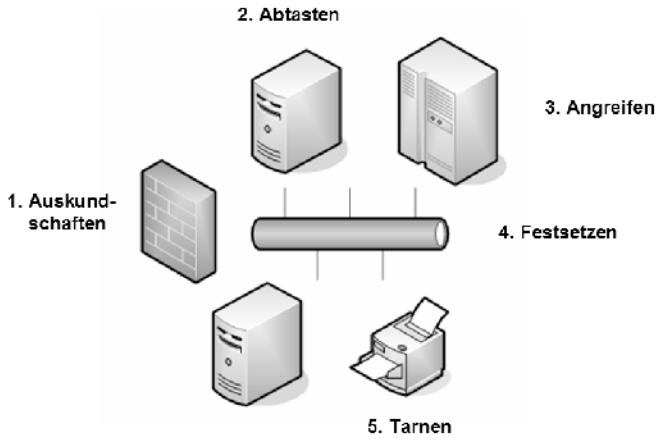


Abbildung 3.1: Vorgehensmodell eines professionellen Einbruchs

1. Phase: Auskundschaften
   Bevor eine Verbindung mit dem Zielnetzwerk hergestellt wird, beschafft der Hacker möglichst viele Informationen über das Opfer, beispielsweise der dem Unternehmen offiziell zugeteilte IP-Adressbereich. Diese Phase wird im Hacker-Jargon auch als *Reconnaissance* bezeichnet.
2. Phase: Abtasten
   Mit Hilfe automatisierter Scanner überprüft der Hacker, hinter welchen IP-Adressen sich aktive Komponenten im Zielnetzwerk befinden, um welche Devices es sich dabei handelt, welche Betriebssysteme darauf installiert sind und welche Dienste dort bereitgestellt werden.
3. Phase: Angreifen
   Anschließend verschafft sich der Hacker an geeigneter Stelle einen Zugang in das Netzwerk, beispielsweise durch die Anwendung bekannter Exploits[1]. Hat er die Kontrolle über einen Rechner erlangt, ist ihm die uneingeschränkte Fernsteuerung dieses Rechners möglich.
4. Phase: Festsetzen
   Um zu einem späteren Zeitpunkt wieder ungestört auf das System zugreifen zu können, installiert der Hacker eine Backdoor-Applikation. Diese Hintertür ermöglicht ihm zu jedem späteren Zeitpunkt, an den bestehenden Zugangssicherungen vorbei in das System zu gelangen.
5. Phase: Tarnen
   Damit der Einbruch nicht auffällt, tarnt der Hacker die von ihm installierte Software und verwischt anschließend seine Spuren, indem er die von dem Zielsystem automatisch erzeugten Protokolleinträge löscht.

3.2 Phase 1: Auskundschaften

Das Herstellen einer Verbindung wird von einer *Firewall* oder einem *Intrusion Detection System* protokolliert. Da dabei die Gefahr besteht, dass der Angreifer entdeckt wird, erfolgt die vorangehende Recherche ohne elektronischen Kontakt zum Zielnetzwerk. Ein gut vorbereiteter Hacker verbringt ca. 90 Prozent seines Aufwands mit der Erstellung eines Sicherheitsprofils (*Footprinting*). Nur ca. 10 Prozent seines Aufwands wendet er für die eigentliche Ausführung des Angriffs auf.

Bei der Erstellung eines Sicherheitsprofils helfen die folgenden Werkzeuge:

- Per *DNS-Report* oder *whois-Abfrage* können die öffentlichen Nameserver im Internet über die Domänen des Unternehmens befragt werden.
- Mit Hilfe eines *Web-Crawlers* kann die gesamte Web-Site eines Unternehmens gespiegelt werden. Anschließend wird auf der lokalen Kopie recherchiert (insbesondere in den Kommentaren und Meta-Tags der HTML-Seiten).
- Per *Google-Hacking*: Geschickt formulierte Suchabfragen liefern vielfältige Informationen über Betriebssysteme, Datenbanken, Web-Server, E-Mail-Adressen und vielem mehr.

1. Ein *Exploit* ist eine Software, die spezifische Schwächen einer anderen Software ausnutzt, um Befehle auf dem betroffenen Rechner an dieser Software vorbei auszuführen oder privilegierte Rechte für die Ausführung weiterer Befehle zu erlangen.

Abbildung 3.2 zeigt am Beispiel von *DNSstuff.com*[2], welche Informationen im Internet über das Netzwerk eines Unternehmens öffentlich verfügbar sind:

- der Name des für die Domäne zuständigen Providers (hier: `Provider AG`[3])
- der dem Unternehmen zugeteilte IP-Adressbereich (hier: `195.234.8.15` bis `195.234.47.11`)
- die Lokation der IP-Adresse (hier: `Frankfurt, Hessen, DE [Germany]`)
- der zuständige Registrar (hier: `whois.ripe.net`)
- den Link des zuständigen whois-Servers (hier: `195.234.47.11`)
- *DNSstuff.org* bietet den Zugriff auf weit mehr Informationen als hier abgebildet. Ein vollständiger Überblick kann dem Kapitel 4 entnommen werden.

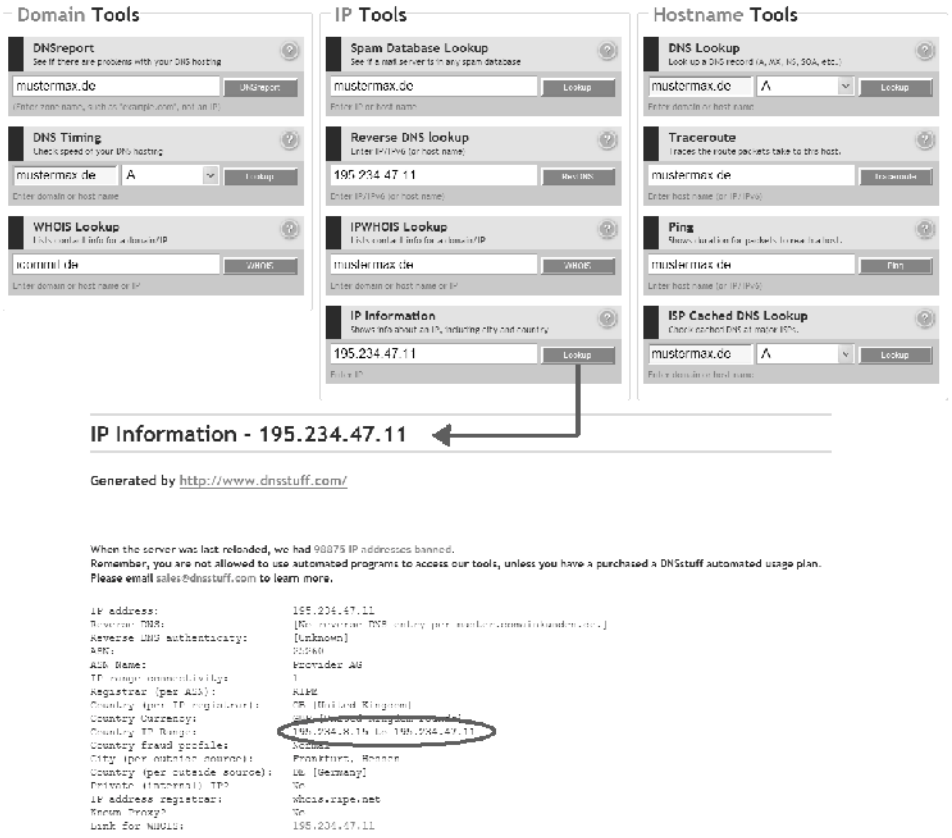


Abbildung 3.2: Footprinting über *DNSstuff.com*

2. *http://www.dnsstuff.com/*
3. Namen geändert.

Ein Hacker erhebt im Rahmen des Footprintings wesentlich mehr Informationen, u.a.

- über die Domänen des Unternehmens
- über die dem Unternehmen zugeteilten IP-Blöcke
- über die installierten Netzwerkdienste und –applikationen
- über die zugrunde liegende Systemarchitektur
- über alle verfügbaren Kontakte

DNSstuff.com ist nur eines von vielen Reconnaissance-Werkzeugen, aber bei weitem nicht die einzige Möglichkeit, ein Unternehmen auszukundschaften. Stellenanzeigen im Internet können beispielsweise Aufschluss geben über die eingesetzten Betriebssysteme, Firewalls und Netzwerk-Devices; so lassen sich erste Ansätze über die Netzwerktopologie und über die Systemarchitektur erkennen.

Intelligente Suchabfragen über Google bringen erstaunliche Erkenntnisse zu Tage. Der folgende Kasten zeigt, wie mittels *Google Hacking* wertvolle Informationen über Betriebssysteme, Server-Versionen und Datenbanken gesammelt werden können, ohne dass sich der Hacker ein einziges Mal mit dem Zielnetzwerk verbinden muss.

Hinweis

Ist der Domänenname eines Unternehmens bekannt (z.B. `meine-firma.de`), können geschickt formulierte Google-Abfragen Aufschluss über die eingesetzten Systeme eines Unternehmens ergeben.

Die folgende Tabelle zeigt einige Beispiele:

Google-Abfrage	Ergebnis

`site:meine-firma.de -site:www.meine-firma.de`	findet alle Subdomains eines Unternehmens, zum Beispiel
	`news.meine-firma.de`
	`intranet.meine-firma.de`
	`debian.meine-firma.de`
	`secure.meine-firma.de`
	`personal.meine-firma.de`

`intitle:index.of "server at" site:meine-firma.de`	liefert nicht nur die auf einem Web-Server gespeicherten Dateien, sondern meist auch die Version des Web-Servers und des Betriebssystems, zum Beispiel `Apache/2.0.54 (Debian GNU/Linux) Server at debian.meine-firma.de Port 80`

`@meine-firma.de`	findet die im Internet veröffentlichten E-Mail-Adressen des Unternehmens, zum Beispiel
	`m.mueller@meine-firma.de`
	`k.schmitz@meine-firma.de`
	`s.meier@meine-firma.de`

`"#include <stdio.h>" site:meine-firma.de`	sucht nach Quellcode auf den Seiten des Unternehmens

Tabelle 3.2: Google Hacking

`intitle:error site:meine-firma.de`	**sucht nach Fehlermeldungen auf den Web-Seiten des Unternehmens; diese können Aufschluss über die eingesetzten Programmiersprachen und Datenbanken geben**

`"Warning: Access denied for user:" site:meine-firma.de`	**sucht nach Datenbankfehlermeldungen auf den Internet-Seiten des Unternehmens, und findet zum Beispiel**
	`Warning: Can't connect to MySQL server on '213.198.47.11' (113) in /home/www/web20/html/neu/db.php3 on line 2`
	
	`Warning: Access denied for user: 'wwwrun@localhost' (Using password: NO) in /home/www/web20/html/neu/db.php3 on line 3`

Tabelle 3.2: Google Hacking (Forts.)

Die Liste der Google-Suchabfragen lässt sich beliebig erweitern. Hacker suchen via Google nach

- Login-Seiten
- Benutzernamen und Passwörtern
- Backups und temporären Dateien
- Fehlermeldungen von Web-Servern, Datenbanken und Programmiersprachen
- nach Konfigurationsdateien
- nach Office-Dokumenten (deren Eigenschaften nützliche Informationen wie bspw. interne Accountnamen enthalten können)

und vielem mehr. Üblicherweise werden solche Recherchen nicht manuell, sondern mit Hilfe automatisierter Tools durchgeführt.

Führt *Google Hacking* nicht weiter, kann der Hacker die gesamte Web-Site des Unternehmens herunterladen und lokal auswerten. Bei diesem Vorgang unterstützt ein *Web-Crawler*, also ein Programm, das Web-Seiten analysiert und den darin enthaltenen Links und Referenzen folgt. Web-Crawler, auch unter der Bezeichnung *Spider* oder *Robot* bekannt, werden vornehmlich von Suchmaschinen eingesetzt. Abbildung 3.3 zeigt den *WebWhacker* bei dem Kopiervorgang der Web-Site *johnny.ihackstuff.com* auf die lokale Festplatte.

Aus Sicht der zu schützenden Unternehmen kommt es noch schlimmer: Das Internet hostet nicht nur alle derzeit bekannten Web-Sites, sondern archiviert beinahe alle Änderungen der Domäneninhalte im Internet!

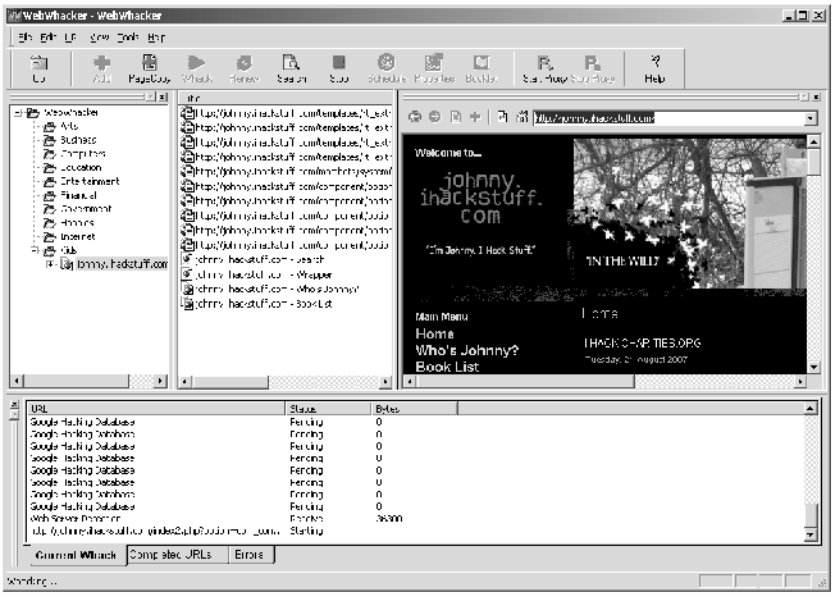


Abbildung 3.3: Spiegeln einer Web-Site mit dem *WebWhacker*

Das Internet-Archiv *www.archive.org* registriert Änderungen an den im Internet registrierten Web-Sites. Ganz automatisch und ohne eigenes Zutun! Bei Eingabe eines URLs in dem Eingabeformular von *archive.org* (Abbildung 3.4) erhält der Interessent eine tabellarische Übersicht aller Tage, an denen eine neue Version der Web-Site für diese Domäne hochgeladen wurde; beginnend mit der jüngsten Änderung, über viele Jahre hinweg zurück bis hin zum ersten Launch der Web-Site. Jede dieser historisierten Änderungen ist verlinkt mit einem Archiv der damaligen Version. Bei einem Klick auf ein Versionsdatum wird das zugehörige Archiv auf einen internen Server bei *archive.org* entpackt, und die ursprünglichen Inhalte stehen dem Benutzer online zur Verfügung!

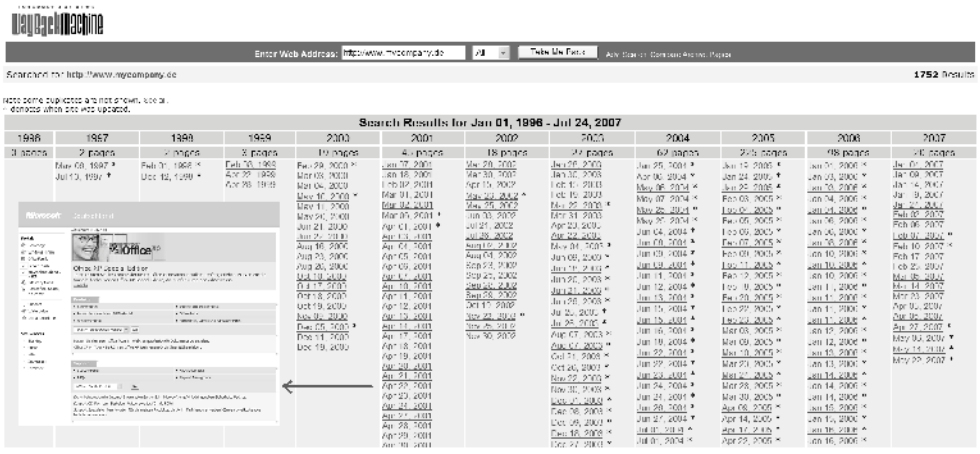


Abbildung 3.4: Archivierte Web-Sites unter *archive.org*

Dieses Beispiel macht deutlich, dass grundsätzlich jede Information sicherheitsgefährdend ist, die jemals im Internet veröffentlicht wurde! Insbesondere versehentlich hochgeladene Dateien befinden sich auch Jahre danach noch im anonymen Zugriff Dritter:

- Sicherheitskopien von Konfigurationsdateien (*.config.bak*, *.reg.bak*, *.ini.bak*, *global.asa.bak*)
- Protokolle von FTP-Uploads (*ws_ftp.log*)
- Reports von Vulnerability Scannern

und vieles mehr.

archive.org ist als zentrales Archiv öffentlich zugänglich! Fast alles, was bisher online gestellt wurde, ist heute noch in den dort vorgehaltenen Archiven verfügbar, und meistens haben die darin enthaltenen Informationen auch heute noch Gültigkeit. Dies gilt besonders für

- Datenbank-Connection-Strings
- interne IP-Adressen und Hostnamen
- und im schlimmsten Fall sogar für bekannte Schwachstellen und Exploits.

3.3 Phase 2: Abtasten

Hat sich der Hacker einen Überblick über die Netzwerkinfrastruktur des Unternehmens verschafft, sucht er einen offenen Zugang. Die folgenden Techniken zeigen mögliche Eingangstüren auf:

- Network Scanning
- Port Scanning
- Vulnerability Scanning

Jede dieser drei Techniken verfeinert stufenweise die Suche des Hackers nach einer offenen Lücke in den bestehenden Zugangssicherungen des Unternehmensnetzwerks.

3.3.1 Network Scanning

Mittels *Network Scanning*, dem Abtasten des Netzwerks, werden die aktiven, von außen erreichbaren Geräte des Unternehmensnetzwerks identifiziert. Die Freeware *Angry IP Scanner* ist ein solches *Network Scanning Tool*. Abbildung 3.5 zeigt die möglichen Ergebnisse eines Network Scans.

Nach der Eingabe eines IP-Adressbereichs nummeriert das Tool alle IP-Adressen in diesem Bereich durch und pingt die dahinter befindlichen Devices an. Auf diese Weise findet der Hacker heraus, hinter welchen IP-Adressen sich aktive Geräte befinden. Für jede aktive IP führt das Werkzeug einen *Reverse Lookup* durch, um ausgehend von der IP-Adresse den zugehörigen Servernamen zu ermitteln. Letzterer lässt häufig auf den Einsatz des Servers schließen. Beispielsweise deutet `web.mycompany.de` auf einen Web-Server hin, `ftp.mycompany.de` auf einen FTP-Server und `smtp.mycompany.de` und `pop3.mycompany.de` auf reine E-Mail-Server. Der Servername `intranet.mycompany.de` legt ein ungeschütztes Intranet nahe, während `pc-004711.mycompany.de`, `pc-000815.mycompany.de` und `mmueller.mycompany.de` auf temporär offene Testsysteme schließen lassen.

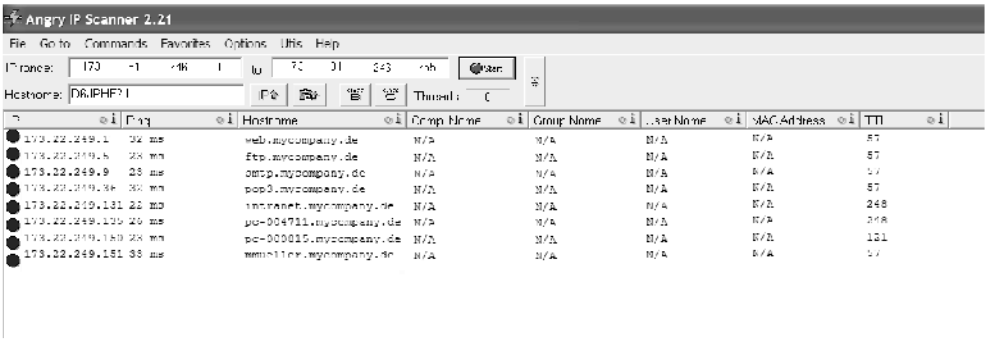


Abbildung 3.5: Network Scanning mit dem *Angry IP Scanner*

3.3.2 Port Scanning

Nachdem der Hacker die IP-Adressen seines Ziels abgetastet hat, fertigt er eine Skizze der zugrunde liegenden Netzwerktopologie an. Oft lassen bereits die Servernamen einen Rückschluss auf den Einsatz der Rechner zu (beispielsweise *web.mycompany.de*, *smtp.mycompany.de*, *intranet.mycompany.de*). Meist müssen jedoch zusätzlich die auf den ausfindig gemachten Servern laufenden Dienste identifiziert werden. Dies geschieht mittels *Port Scanning*.

Betriebssystemdienste und Applikationen verwenden Ports, um eingehende Netzwerknachrichten zu empfangen und zu verarbeiten. Ein *Port* ist kein physikalischer Anschluss, sondern ein numerischer Identifikator, der mit einem Betriebssystemdienst oder einer an diesem Port registrierten Applikation verknüpft ist. Diese bezeichnet man als *Port Listener*.

Der folgende Kasten nennt einige bekannte Ports:

Dienste	Port	Protokoll	Beschreibung
ftp-data	20	tcp	File Transfer Protocol (Daten)
ftp	21	tcp	File Transfer Protocol (Steuerung)
telnet	23	tcp	Telephone Networking Service
smtp	25	tcp	Simple Mail Transfer Protocol
nicname	43	tcp	Whois
domain	53	tcp	Domain Name Server
sql*net	66	tcp	Oracle SQL*NET
http	80	tcp	HyperText Transfer Protocol
kerberos	88	tcp	Kerberos (Authentication Protocol)
pop3	110	tcp	Post Office Protocol – Version 3
sqlserv	118	tcp	SQL Services
cisco-sys	132	tcp	CISCO System Maintenance
netbios-ns	137	tcp	NetBIOS Name Service
netbios-ssn	139	tcp	NetBIOS Session Service
https	443	tcp	http protocol over TLS/SSL
mysql	3306	tcp	MySQL

Tabelle 3.3: Wohldefinierte Ports

Eine vollständige Liste wohldefinierter Ports kann der Seite *http://www.iana.org/assignments/port-numbers* der IANA[a] entnommen werden.

a IANA = Internet Assigned Numbers Authority, *http://www.iana.org/*.

Ports sind die Türen und Fenster, über die ein Angreifer in ein Computer-System eindringen kann. Ist bekannt, welche Ports auf einem Rechner offen sind, können bereits weitreichende Rückschlüsse auf die verfügbaren Dienste geschlossen werden und damit auf den Einsatz des Rechners.

Einer der bekanntesten Port Scanner ist *NMAP*, ein Kommandozeilenwerkzeug, das mit UNIX- und LINUX-Distributionen ausgeliefert wird, aber auch in Verbindung mit WinPcap[4] und CYGWIN[5] unter Windows zur Verfügung steht. *NMAP* sucht in den vorgegebenen IP-Adressbereichen nach aktiven Komponenten, tastet die Ports eines Rechners ab, identifiziert das dort laufende Betriebssystem und umgeht über diverse Timing-Einstellungen die Protokollierung in den vorgeschalteten Firewalls. Abbildung 3.6 zeigt auf der linken Seite die möglichen Eingabeparameter des Tools, auf der rechten Seite einen beispielhaften Port Scan.

4. *http://www.winpcap.org/*
5. *http://www.cygwin.com/*

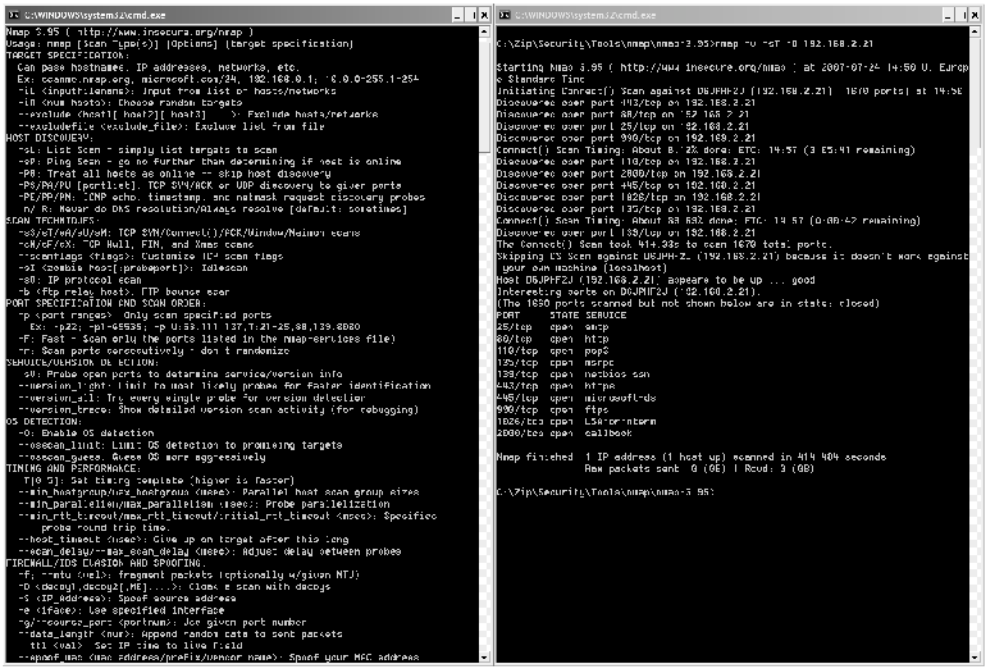


Abbildung 3.6: Port Scanning mit *NMAP*

Der Kommandozeilenaufruf

```
nmap -v -sT -O 192.168.2.21
```

bedeutet:

- -v steht für „verbosity mode“, also ausführliche Ausgaben auf der Konsole,
- -sT steht für einen *TCP Connect() Scan* (so dass jeder überprüfte Port ordnungsgemäß geöffnet und anschließend wieder geschlossen wird),
- -O steht für „OS Detection“, also den Versuch, das Betriebssystem herauszufinden,
- 192.168.2.21 ist die IP-Adresse des abzutastenden Rechners.

Das Tool ermittelt im Beispiel der Abbildung 3.6 die offenen Ports 25, 80, 100, 135, 139, 443, 445, 990, 1026 und 2000.

Häufig wenden sich Angriffe gegen den Port 139, den sog. *NetBIOS-Service*, da dieser Dienst auf vielen Windows-Systemen bestimmte Abfragen über die verfügbaren Netzwerkressourcen unterstützt, ohne dass sich der Client am System authentifizieren muss.

3.3.3 Vulnerability Scanning

Mit den vorliegenden Informationen über aktive Geräte und offene Ports ist der Angreifer gewappnet, eine Angriffsstrategie zu entwerfen:

- Welche Exploits sind für die vorliegenden Betriebssysteme und Dienste bekannt?
- Welche Komponente scheint am schwächsten abgesichert zu sein?
- Welcher Angriff verspricht den schnellsten Erfolg?

Das Internet stellt umfangreiche Datenbanken über bekannte Schwachstellen und Exploits zur Verfügung:

- Die US-CERT veröffentlicht unter *http://www.us-cert.gov/* die sog. „US-CERT Vulnerability Notes".
- Parallel wird unter *http://cve.mitre.org/* die Datenbank „Common Vulnerabilities and Exposures" geführt.

Beide Plattformen bieten sehr ausführliche Informationen über bestehende Sicherheitslücken.Weitere Datenbanken finden sich unter:

- *www.securitytracker.com*
- *www.microsoft.com/security*

Professionelle Hacker bedienen sich natürlich ihrer eigenen Informationskanäle und warten nicht darauf, dass die in ihrer Community längst bekannten Exploits veröffentlicht werden. Denn wird eine Schwachstelle erst den Herstellern bekannt, ist die Behebung nur eine Frage der Zeit ...

3.4 Phase 3: Angreifen

Wenn es nicht gelingt, über eine Seitentür in das Zielsystem einzudringen, ist ein Login erforderlich. Der Hacker muss zunächst herausfinden, welche Benutzerkonten in dem Zielsystem definiert sind und anschließend das zugehörige Passwort cracken.

In den meisten Betriebssystemen sind bestimmte Benutzerkonten vordefiniert (z.B. „Administrator" oder „Gast"). Sind diese Konten mit schwachen Passwörtern verknüpft, ist es ein Leichtes, das Passwort zu brechen und sich als „legitimierter" Benutzer in das System einzuwählen. Meist wird direkt der Administrator-Account angegriffen, da dieser mit allen erforderlichen Rechten im System ausgestattet ist.

Oft aber können die Benutzerkonten in der Domäne eines Unternehmens viel einfacher ermittelt werden: Sind dem Hacker ein oder mehrere Mitarbeiter des Unternehmens namentlich bekannt (Stichwort: *Google Hacking*), kann er die in den meisten Unternehmen etablierten Namenskonventionen nutzen und sich durch die einzelnen Logins probieren. Einem Mitarbeiter namens „Max Mustermann" könnte bspw. eines der folgenden Benutzerkonten zugeordnet sein:

- `Mustermann`
- `MMustermann`

- `M.Mustermann`
- `Max.Mustermann`
- `Max-Mustermann`
- `mm`
- `muma`
- `musmax`

Ist die Namenskonvention einmal ersichtlich, können die meisten Benutzerkonten eines Unternehmens aus einem einfachen Namensverzeichnis der Mitarbeiter abgeleitet werden (z.B. aus einem internen Telefonbuch).

Eine der wichtigsten Erkenntnisse in diesem Zusammenhang ist, dass Hacker sich beim Cracken von Passwörtern nicht auf ein einziges Benutzerkonto festfahren. Natürlich versuchen sie zunächst, des Administrator-Passworts habhaft zu werden. Mißlingt dies aber, probieren sie bestimmte, schwache Passwörter auf allen Benutzerkonten des Unternehmens aus, um „irgendwo reinzukommen“. Ausgangspunkt des Crackings ist also häufig das Passwort und nicht der Account! Beispielsweise sind „abc123“ und „123456“ schwache Passwörter, die von vielen Benutzern verwendet werden. Hacker stellen eine Liste aller Benutzerkonten des Unternehmens zusammen und probieren schwache Passwörter mit jedem einzelnen Account aus. Im Allgemeinen besteht eine hohe Wahrscheinlichkeit, dass nur ein einziger Benutzer seinem Konto ein solches schwaches Passwort zugeordnet hat.

Für das Cracken von Passwörtern stehen dem Hacker verschiedene Tools zur Verfügung. Die Bekanntesten sind *John the Ripper* und *L0phtCrack*, das später als *LC4* und *LC5* von *@stake* weiter entwickelt und nun, aus gutem Grund, von *Symantec* aufgekauft und vom Markt genommen wurde. *LC5* ermittelt die auf einem Rechner eingerichteten Benutzerkonten und versucht die zugehörigen Passwörter zu brechen (Abbildung 3.7). Ganz automatisch ...

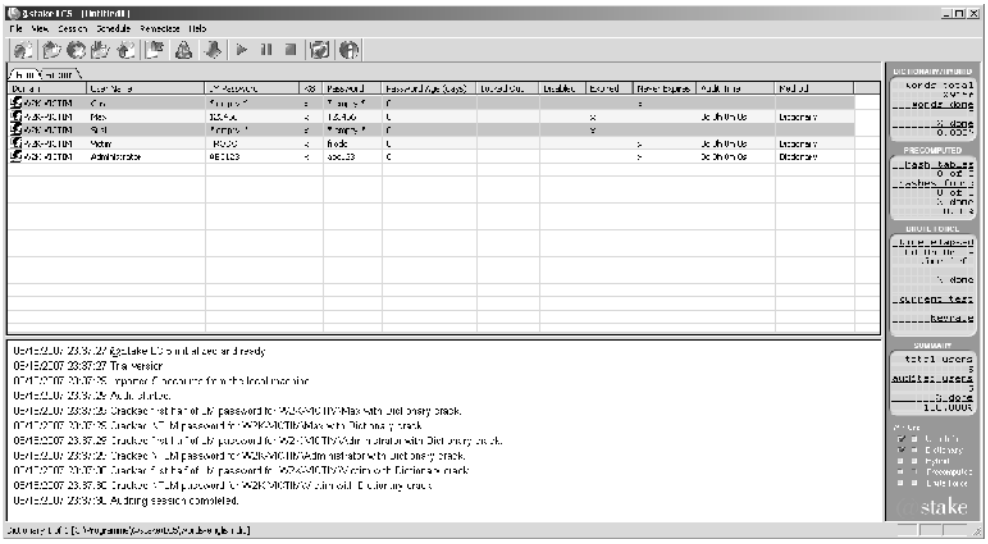


Abbildung 3.7: Password-Cracking mit *LC5*

In diesem Beispiel findet *LC5* zwei Benutzerkonten mit leerem Passwort (`Gast` und `Susi`) und sowie drei weitere Accounts mit Administrationsrechten (`Max`, `Victim` und `Administrator`). Die Passwörter dieser Accounts wurden automatisch innerhalb von zwei Sekunden gecrackt.

LC5 erwartet als Eingabe eine IP-Adresse oder eine SAM-Datei. *SAM* steht für „Security Access Manager" und bezeichnet eine Windows-Systemdatei, in der Informationen über die auf einem Windows-System eingerichteten Benutzerkonten gespeichert sind. Diese SAM-Datei enthält zudem die Hashwerte der Passwörter für diese Benutzerkonten. *LC5* extrahiert nun aus dieser verschlüsselten Datei zunächst alle darin aufgeführten Benutzerkonten und beginnt anschließend, die zugehörigen Passwörter zu brechen.

Password Cracker wenden im Allgemeinen mehrere unterschiedliche Strategien an:

- Mit Hilfe sog. *Dictionaries* wird eine Liste vordefinierter Passwörter systematisch „ausprobiert". Ein Dictionary enthält häufig verwendete Passwörter wie bspw. „123456" oder „abc123" und kann je nach Umfang mehrere tausend Einträge umfassen.
- Ist das Passwort nicht im Dictionary enthalten, wird eine „hybride Attacke" angewendet. Darunter versteht man die Kombination der in dem Dictionary enthaltenen Wörter mit Präfixen oder Postfixen, die aus Ziffern und Sonderzeichen bestehen. Aus „goldfisch" wird somit beispielsweise „goldfisch123" oder „$goldfisch$".
- Eine verzweifelt anmutende Strategie ist die sog. „Brute Force Attack". Bei diesem Ansatz werden alle (!) syntaktisch möglichen Passwörter vorgeneriert, begonnen mit Passwörtern der Länge 1, bis zu Passwörtern der Länge 20 oder mehr! Dies entspricht bei 26 Buchstaben in Groß- oder Kleinschreibung, 10 Ziffern und 32 Sonderzeichen einer extrem hohen Anzahl an Möglichkeiten. Im Internet[6] befindet sich ein sog. „Brute Force Attack Estimator", der die Anzahl der Passwörter berechnet, die bei einer Brute Force Attacke ausprobiert werden müssen: Bei einem Passwort der Länge 6 mit 3 Buchstaben und 3 Ziffern ergeben sich bereits über 17 Millionen mögliche Kombinationen! Wie lange mag ein Rechner benötigen, um das Passwort eines Accounts auf diese Weise im Klartext zu ermitteln?
- In manchen Fällen ist der Hashwert eines Passworts bekannt, bspw. weil ein Network Sniffer den Benutzernamen und den Passwort-Hash im Rahmen eines Anmeldeverfahrens protokollieren konnte. In solchen Fällen kann der Hacker auf vorberechnete Hashwerte zurückgreifen: Im Internet werden seit langem Datenbanken getauscht, die das Passwort eines Benutzers nach der Eingabe des Hashwertes über eine simple Abfrage im Klartext zurückliefern! Hacking-Tools wie LC5 versuchen die Hashwerte kurzer Passwörter selbständig aufzulösen.

6. *http://www.mandylionlabs.com/PRCCalc/BruteForceCalc.htm*

3.5 Phase 4: Festsetzen

Hat der Hacker erst einmal einen Zugang auf das Zielsystem erlangt, installiert er eine *Hintertür* (eine sog. *Backdoor-Application*). Darunter versteht man eine Software, die dem Hacker ermöglicht, zu einem späteren Zeitpunkt unter Umgehung aller Zugangssicherungen erneut auf den kompromittierten Rechner zugreifen zu können. Bekannte Backdoors sind *Sub Seven* und *Back Orifice*: Beide installieren einen Port Listener, über den der befallene Rechner vom Computer des Hackers aus ferngesteuert werden kann.

Eine einmal installierte Hintertür kann nur schwer auf einem infizierten Rechner entdeckt werden. Oft ändert die Schadsoftware ihren Port und ihre Signatur, so dass sie von den gängigen AntiViren-Programmen und Internet-Security-Suites nicht entdeckt werden kann.

Eine mögliche Gegenmaßnahme wird in Form des Kommandozeilenwerkzeugs *netstat* unter Windows ausgeliefert. Das Kommando

```
netstat -a
```

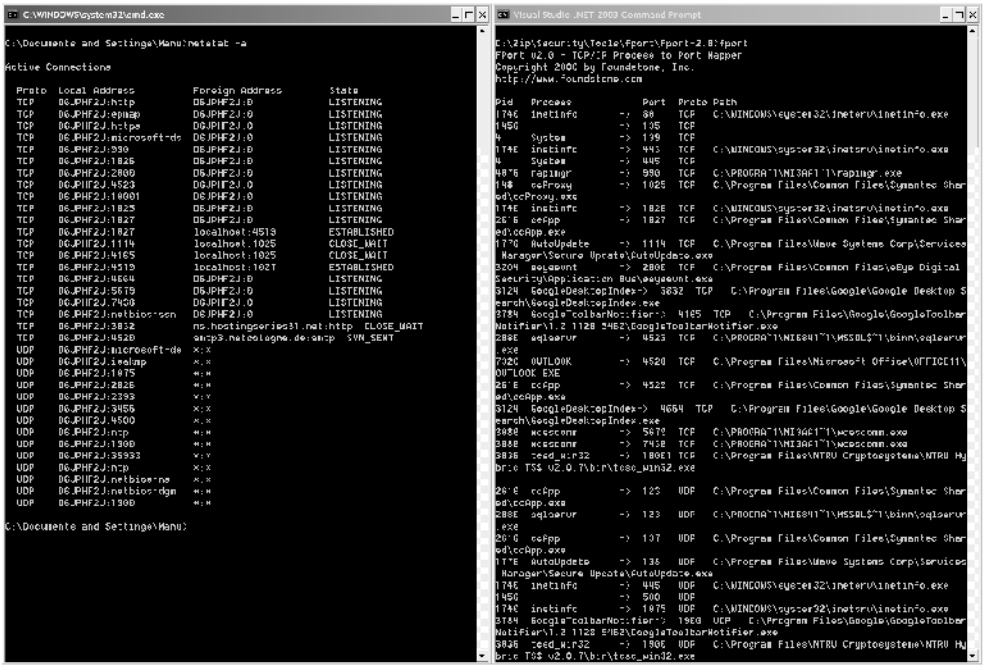


Abbildung 3.8: Port-Listener unter *netstat* und *fport*

zeigt alle offenen Ports eines Rechners an; leider fehlt dieser Auflistung jedoch die Zuordnung der Prozesse, die sich hinter diesen Ports registriert haben. Dieses Defizit wird durch das Tool *fport*[7] ausgebessert. *fport* zeigt im Vergleich zu *netstat*, wie die offenen Ports den

7. *http://www.scanwith.com/download/Fport.htm*

Prozessen und Executables im Dateisystem zugeordnet sind (Abbildung 3.8). Während `netstat` nur die offenen Ports und Protokolle aufführt, ordnet `fport` diesen Ports ihre Port-Listener im Dateisystem zu. Für den Administrator ist so besser ersichtlich, welche Prozesse aus welchen Verzeichnissen gestartet wurden. Besteht ein Verdacht auf eingeschleuste Schadsoftware, kann `fport` dem Administrator nützliche Hinweise auf Trojaner und Stealth-Software geben.

Erst mit dieser Information (und auch viel weiterem Fachwissen!) kann sich der Benutzer einen Überblick darüber verschaffen, ob auf seinem Rechner ausschließlich die gewünschten Dienste laufen oder nicht doch heimlich Schadsoftware eingeschleust wurde.

3.6 Phase 5: Tarnen

Um nicht entdeckt zu werden, verwischt ein Hacker die Spuren seines Eindringens. Abhängig von der Art des Angriffs löscht der Hacker nicht nur die von ihm verursachten Einträge im Event-Log des Systems, sondern insbesondere die Protokolleinträge in den Log-Dateien der Netzwerkmonitore und Firewalls des angegriffenen Rechners. Mit Hilfe sogenannter *Stealth Tools*[8] und *Rootkits*[9] versteckt der Angreifer die eingeschleusten Dateien, Verzeichnisse, Prozesse und Services, so dass diese über die gewöhnlichen Zugriffswerkzeuge des Betriebssystems gar nicht erst mehr angezeigt werden:

- Dateien und Verzeichnisse werden dabei derart versteckt, dass sie dem Benutzer weder über den *Explorer* noch über die Kommandozeilenwerkzeuge `dir` (Windows) und `ll` (UNIX) offenbart werden.
- Prozesse und Services werden versteckt, indem beispielsweise die Original-Dateien des Task-Managers `taskmgr.exe` (Windows) oder des Kommandozeilenwerkzeugs `ps` (UNIX) durch modifizierte Executables ausgetauscht werden! Diese modifizierten Werkzeuge erwecken den Anschein ihres Originals, fälschen jedoch die erzeugte Ausgabe, so dass der Administrator bestimmte Informationen erst gar nicht erhält! Beispielsweise unterdrücken diese modifizierte Werkzeuge die Anzeige der installierten Backdoor-Prozesse, so dass der Administrator die von dem Angreifer ausgeführten Prozesse gar nicht erst bemerken kann[10]!

Abbildung 3.9 zeigt einen Auszug der Executables (`*.exe`) in dem Windows-Systemverzeichnis `C:\WINDOWS\system32\` einer Standard-Windows-XP-Professional-Installation mit Service Pack 2.

Diese EXE-Dateien haben offensichtlich allesamt exakt die gleichen Attribute ihrer Originale in der Standard-Windows-Installation. Und doch wurden die meisten dieser Dateien von einem Angreifer ausgetauscht! Weitere EXE-Dateien sind in dem System-

8. *Stealth Tools* dienen der Tarnung von Dateien und Prozessen. Mit ihrer Hilfe können Dateigrößen verfälscht, Dateien versteckt, Prozesse getarnt und vor dem Administrator eines Systems verborgen werden.
9. Ein *Rootkit* ist eine Sammlung von Werkzeugen, die der Angreifer auf einem gekaperten System installiert, um seine Aktivitäten zu verdecken und um Dateien und Prozesse vor den Benutzern und Administratoren dieses Systems zu verstecken. Rootkits sind spezielle Stealth Tools.
10. Erst durch die Installation spezieller *Anti-Rootkits* kann der Administrator die verdeckten Tätigkeiten des Angreifers aufdecken. Hinweise auf verfügbare Produkte können Kapitel 8 entnommen werden.

verzeichnis abgelegt und werden nicht angezeigt. Zudem lassen sich die von dem Angreifer eingeschleusten Dateien weder durch ihre Originale ersetzen noch löschen!

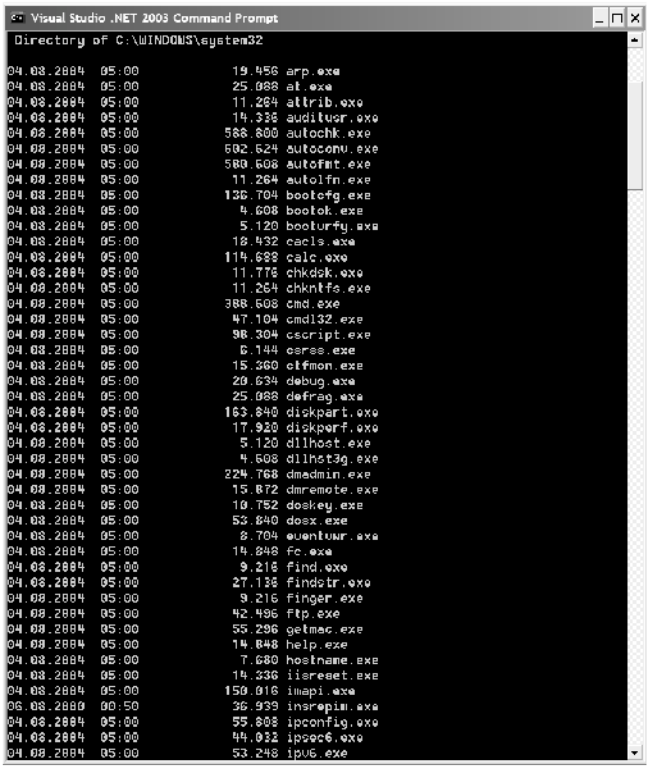


Abbildung 3.9: Getarnte Executables in einem Dateisystem

Gefälscht werden bei einer solchen Anzeige nicht nur die Dateigrößen und die Zeitstempel, sondern insbesondere die Liste der dargestellten Einträge: Manche Dateien werden erst gar nicht angezeigt, andere Dateien werden mit falschen Attributen angezeigt und wiederum andere Dateien werden „hinzugedichtet". Ein einziger *Fake* also, mit dem der Systemadministrator hereingelegt werden soll ...

Glücklicherweise gibt es Werkzeuge, mit denen Administratoren solche Tarnungen auffliegen lassen können. Allerdings erfordert die Anwendung dieser Methoden und Verfahren ein Know-How, das weit über die Möglichkeiten des gewöhnlichen Privatanwenders hinaus geht und selbst für erfahrene Sicherheitsspezialisten die ein oder andere Herausforderung bietet!

3.7 Ausblick

In diesem Kapitel wurde ein Überblick über die typische Vorgehensweise eines professionellen Angreifers dargeboten. Die nachfolgenden Kapitel widmen sich im Detail den einzelnen Phasen des dargestellten Vorgehensmodells.

4 Auskundschaften

Der Begriff *Reconnaissance* bezeichnet das Auskundschaften des Angriffsziels und ist eine der beiden wichtigsten Phasen in der Vorbereitung des Hackers. Mit den gewonnenen Informationen kann sich der Hacker ein detailliertes Bild von der Netzwerktopologie und der Systemarchitektur seines Opfers machen. Die zweite wichtige Phase ist das Abtasten des Zielnetzwerks, das sog. *Scanning*, dem Kapitel 5 gewidmet ist.

4.1 Entdecken und entdeckt werden

In der Vorbereitungsphase sammelt der Angreifer möglichst viele Informationen über sein Opfer, bevor er den eigentlichen Angriff ausführt. Dies sind oftmals Erkenntnisse, die nichtmals den technischen Aufbau des Zielnetzwerks meinen, sondern auf das Opfer selbst bezogen sind: das Unternehmen und dessen Umfeld. So sammeln Hacker Kontaktinformationen über die Mitarbeiter und Geschäftspartner des Unternehmens, über die eingesetzten Technologien und über das Geschäftsmodell. Wichtige Informationsquellen stellen dabei Job-Plattformen, Stellenanzeigen, Nachrichten und Presseinformationen dar.

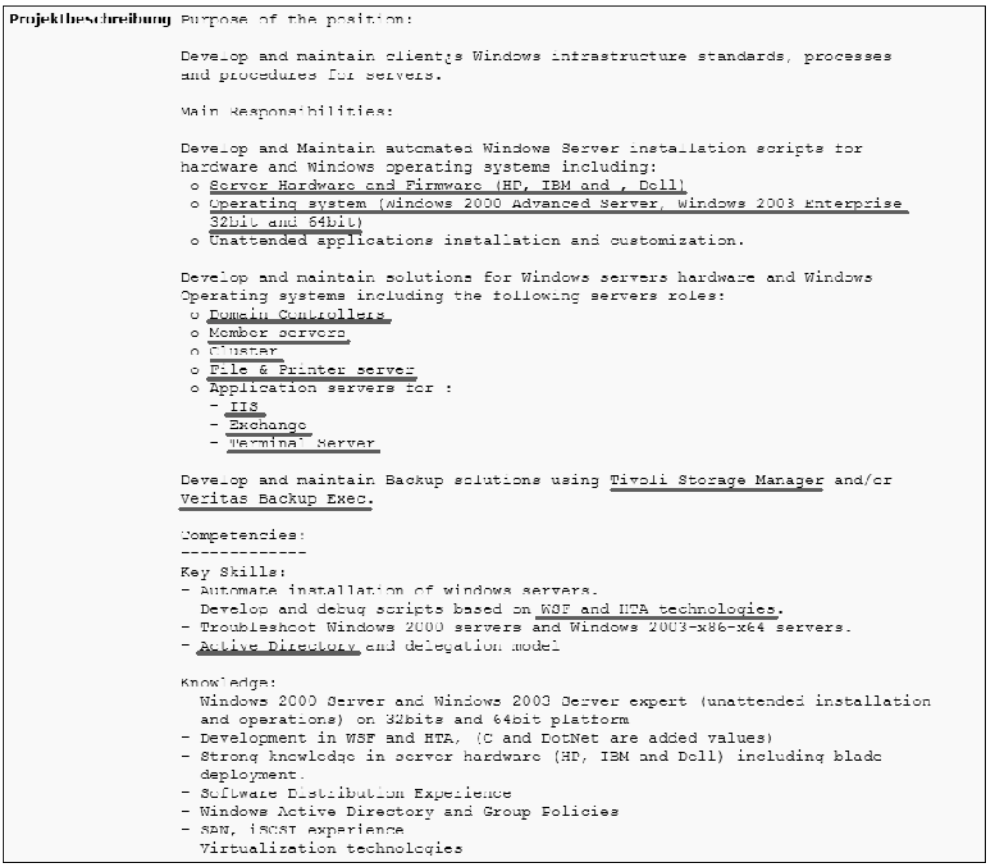
4.1.1 „Harmlose" Quellen

Abbildung 4.1 zeigt, welche Brisanz bereits die Stellenanzeigen eines Unternehmens bergen.

Der Stellenanzeige kann entnommen werden, dass Hardware der Hersteller *HP*, *IBM* und *Dell* eingesetzt wird, auf denen die Betriebssysteme *Windows 2000 Advanced Server* und *Windows 2003 Enterprise Server* installiert sind[1]. Zudem befinden sich in dem Unternehmensnetzwerk mindestens

- ein Domain-Controller
- ein Member-Server[2]
- ein Cluster
- ein File- und Printer-Server
- ein *Internet Information Server*
- ein *Exchange Server*
- ein *Terminal Server*
- ein *Tivoli Storage Manager* bzw. *Veritas Backup Exec*.

1. Siehe die unterstrichenen Zeilen in Abbildung 4.1.
2. Darunter fallen File Server, Application Server, Datenbank-Server, Web-Server, Certificate Server und Remote-Access-Server.



Projektbeschreibung Purpose of the position:

Develop and maintain clients Windows infrastructure standards, processes and procedures for servers.

Main Responsibilities:

Develop and Maintain automated Windows Server installation scripts for hardware and Windows operating systems including:
- o Server Hardware and Firmware (HP, IBM and , Dell)
- o Operating system (Windows 2000 Advanced Server, Windows 2003 Enterprise 32bit and 64bit)
- o Unattended applications installation and customization.

Develop and maintain solutions for Windows servers hardware and Windows Operating systems including the following servers roles:
- o Domain Controllers
- o Member servers
- o Cluster
- o File & Printer server
- o Application servers for :
  - IIS
  - Exchange
  - Terminal Server

Develop and maintain Backup solutions using Tivoli Storage Manager and/or Veritas Backup Exec.

Competencies:

Key Skills:
- Automate installation of windows servers.
  Develop and debug scripts based on WSF and HTA technologies.
- Troubleshoot Windows 2000 servers and Windows 2003-x86-x64 servers.
- Active Directory and delegation model

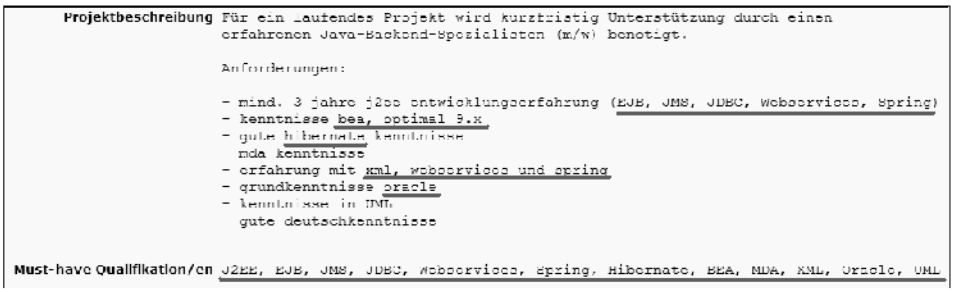
Knowledge:
  Windows 2000 Server and Windows 2003 Server expert (unattended installation and operations) on 32bits and 64bit platform
- Development in WSF and HTA, (C and DotNet are added values)
- Strong knowledge in server hardware (HP, IBM and Dell) including blade deployment.
- Software Distribution Experience
- Windows Active Directory and Group Policies
- SAN, iSCSI experience
  Virtualization technologies

Abbildung 4.1: Stellenanzeige „Netzwerk-Administrator"

Einer weiteren Stellenanzeige (Abbildung 4.2) kann entnommen werden, dass die interne Entwicklung mit Java und Oracle unter Einsatz der folgenden Komponenten betrieben wird:

- *BEA WebLogic Server 9.x*: einem EJB[3]-Applikationsserver
- *Hibernate*: einer Framework zur Abbildung von Java-Objekten in relationale Datenbankmodelle
- *Spring*: einer Open-Source-Framework zur ganzheitlichen Java-Entwicklung von Applikationen und Geschäftslogik

3. *Enterprise JavaBeans* (EJB) sind Java-Komponenten, die auf einem Applikationsserver laufen und die Geschäftslogik einer Anwendung abbilden. Dies umfasst Komponenten für die Objektpersistierung (*Entity Beans*), Prozessabwicklung (*Session Beans*), Kommunikation mit Legacy-Systemen (*Message Driven Beans*) und Web-Services.



Projektbeschreibung Für ein laufendes Projekt wird kurzfristig Unterstützung durch einen erfahrenen Java-Backend-Spezialisten (m/w) benötigt.

Anforderungen:

- mind. 3 jahre j2ee entwicklungserfahrung (EJB, JMS, JDBC, Webservices, Spring)
- kenntnisse bea, optimal 9.x
- gute b hernate kenntnisse
  mda kenntnisse
- erfahrung mit xml, webservices und spring
- grundkenntnisse oracle
- kenntnisse in UML
  gute deutschkenntnisse

Must-have Qualifikation/en J2EE, EJB, JMS, JDBC, Webservices, Spring, Hibernate, BEA, MDA, XML, Oracle, UML

Abbildung 4.2: Stellenanzeige „Systementwickler"

Allein diese wenigen Informationen aus einigen harmlos erscheinenden Stellenanzeigen geben einem Hacker bereits weitreichende Kenntnis über die eingesetzte Hardware und Software: Denn wer 1 und 1 zusammenrechnen kann, weiß um die Standard-Dienste dieser Komponenten und kennt die zugehörigen Ports (Tabelle 4.1):

Server	Port	Protokoll	Dienst
Windows 2000 Advanced Server	42	TCP	WINS[a]
	53	UDP	DNS-Auflösung
	67	UDP	DHCP-Server[b]
	88	TCP	Kerberos
	135	TCP	RPC[c] für MSMQ[d], Exchange, Zertifikatsdienste, Clusterdienste, MSDTC[e], Ereignisprotokoll, Faxdienst und vieles mehr
	137	UDP	NetBIOS-Namensauflösung[f]
	139	TCP	NetBIOS-Sitzungsdienst für Computerbrowser, Leistungsdatenprotokolle, Druckspooler, Anmeldedienst, Verteiltes Dateisystem und vieles mehr
	161	UDP	SNMP[g]
	445	TCP	SMB[h]
	464	TCP	Kerberos Password
	1801	TCP	MSMQ
Internet Information Server	20	TCP	FTP (Daten)
	21	TCP	FTP (Steuerung)
	23	TCP	Telnet
	80	TCP	HTTP
	389	TCP	LDAP[i]

Tabelle 4.1: Standard-Dienste und ihre Ports

Server	Port	Protokoll	Dienst
	443	TCP	HTTPS
	42424	TCP	ASP.NET Sitzungsstatus
Exchange Server	25	TCP	SMTP
	110	TCP	POP3
	119	TCP	NNTP
	135	TCP	Administration
	143	TCP	IMAP[j]
	389	TCP	LDAP
Terminal Server	3389	TCP	RDP-Client[k]
Oracle	66	TCP	SQL*NET
	1521	TCP	SQL*NET 2
	1525	TCP	SQL*NET 1
	1526	TCP	Listener Port
	1575	TCP	Oracle Names

a *Windows Internet Naming* (WINS) ist ein in dem Betriebssystem Microsoft Windows integrierter Netzwerkdienst zur dynamischen Auflösung von NetBIOS-Namen.

b *Dynamic Host Configuration Protocol* (DHCP) ist ein Netzwerkprotokoll, das die dynamische Zuordnung einer IP-Adresse für einen anfragenden Rechner ermöglicht.

c *Remote Procedure Call* (RPC) ermöglicht den Aufruf von Server-Diensten über die Grenzen des lokalen Rechners hinweg.

d *Microsoft Message Queueing* (MSMQ) ist ein Nachrichtenprotokoll, das Applikationen, die auf verschiedenen Rechnern ablaufen, gestattet, ausfallsicher miteinander zu kommunizieren.

e *Microsoft Distributed Transaction Coordinator* (MSDTC) ist ein in Windows integrierter Betriebssystemdienst, der für die Koordination von Transaktionen zwischen Datenbanken, Message-Queues, Dateisystemen und anderen Ressourcen zuständig ist.

f *NetBIOS* bedeutet *Network Basic Input/Output System* und bezeichnet eine Aufrufschnittstelle, die mehreren separaten Rechnern gestattet, über ein LAN miteinander zu kommunizieren.

g Das *Simple Network Management Protocol* (SNMP) ist ein Netzwerkprotokoll für die zentrale Überwachung und Steuerung von Routern, Switches, Servern, Druckern, Computern uvm.

h *Server Message Block* (SMB) ist ein Kommunikationsprotokoll für Datei-, Druck- und Serverdienste in Netzwerken und Bestandteil des LAN-Managers. In der Software *Samba* ermöglicht es beispielsweise Windows-Systemen den Zugriff auf UNIX-basierte Dateisysteme.

i *Lightweight Directory Access Protocol* (LDAP) ist eine einfache Abfragesprache für Verzeichnisdienste. LDAP wird beispielsweise für Zugriffe auf Maildienste und Active Directories eingesetzt und unterscheidet sich von Datenbankabfragesprachen wie SQL durch den Verzicht auf Transaktionen.

j *Internet Message Access Protocol* (IMAP) ermöglicht den Empfang von E-Mails und wurde weitestgehend durch POP3 ersetzt.

k *Remote Desktop Protocol* (RDP) ist ein Netzwerkprotokoll, das die Implementierung von Terminaldiensten zwischen zwei Rechnern ermöglicht.

Tabelle 4.1: Standard-Dienste und ihre Ports (Forts.)

Allein eine Stellenbeschreibung kann ausführlich über die Infrastruktur eines Unternehmens informieren. Wenn der Hacker an die IP-Adressen solcher Server gelangt, ist es ihm ein leichtes, eine bekannte Sicherheitslücke anzuwenden, um in das Unternehmensnetzwerk einzudringen. Dabei unterstützen ihn Vulnerability-Datenbanken wie beispielsweise

- *http://www.us-cert.gov/*
- *http://cve.mitre.org/*
- *http://www.ciac.org/*
- *http://www.securityfocus.com/*
- *http://secunia.com/*
- *http://www.securityspace.com/*
- *http://www.windowsecurity.com/*
- *http://www.tecchannel.de/*
- *http://support.microsoft.com/*
- *http://www.microsoft.com/technet/security/*
- *http://www.oracle.com/technology/deploy/security/alerts.htm*
- *http://www.dba-oracle.com/*

insbesondere aber die innerhalb der Hacker-Community ausgetauschten Informationen.

4.1.2 Informationsbeschaffung

Weitere wichtige Informationsquellen für das Auskundschaften eines Opfers sind Nachrichten und Presseinformationen, die das Unternehmen veröffentlicht.

Eine besondere Form der Informationsbeschaffung stellt das sog. *Dumpster Diving* dar, wörtlich übersetzt „der Sprung in den Müllcontainer". Die meisten Mitarbeiter eines Unternehmens gehen sehr nachlässig mit der Entsorgung sensibler Dokumente um: Fachkonzepte, Spezifikationen und Netzwerkdokumentationen werden nicht in einem Aktenvernichter zerschreddert, sondern landen sorglos im Müll. Hacker beschaffen sich solche Dokumente aus dem Altpapier und studieren die darin enthaltenen internen Informationen; die zwar nicht für sie bestimmt, aber sehr einfach zugänglich sind!

Abbildung 4.3: Dumpster Diving

Eine weitere wichtige Form der Informationsbeschaffung ist das sog. *Social Engineering*: Ein Hacker fälscht einen Mitarbeiterausweis und verschafft sich den Zugang zu einem

Unternehmensgebäude. Nichts ist einfacher, als eine schwere Kiste in Richtung Eingang zu tragen und sich von einem hilfsbereiten Mitarbeiter die Tür aufhalten zu lassen! Dort angekommen, kann sich der Social Engineer als Mitarbeiter der Help-Desk-Abteilung ausgeben und sich in einem Fachbereich den Zugriff auf einen Anwendungsrechner verschaffen. Unter dem Vorwand, eine erforderliche Sicherheitssoftware installieren zu müssen, richtet der Social Engineer eine Backdoor-Applikation auf dem PC ein und verschwindet wieder.

Beliebte Methoden der Social Engineers sind Telefonate, in denen sie die Mitarbeiter eines Unternehmens nach Passwörtern, internen Telefonnummern und anderen sensiblen Informationen fragen. Die meisten Mitarbeiter sind hilfsbereit und unbekümmert und geben die geforderten Informationen preis, wenn ihnen eine schlüssige Begründung vorgelegt wird. Ist ein Mitarbeiter jedoch misstrauisch, spielt der Social Engineer seine Autorität aus: Er setzt den Mitarbeiter unter Druck, in dem er sich als Abteilungsleiter ausgibt und mit Konsequenzen droht. Um diese Rolle glaubwürdig spielen zu können, benötigt der Social Engineer weitere Informationen über den Abteilungsleiter, die er sich durch vorangehende Telefonate mit anderen Mitarbeitern des Unternehmens beschafft.

4.1.3 Verdeckte Ermittlung

In der Hacker-Community gibt es einen Leitspruch, der lautet:

"Wenn du ein guter Hacker bist, kennt jeder deinen Namen. Bist du aber ein wirklich guter Hacker, weiß niemand, wer du bist."

Das A und O des Auskundschaftens ist, unentdeckt zu bleiben. Aus diesem Grund bedienen sich Hacker verschiedener Methoden, um anonym zu bleiben.

Den höchsten Stellenwert haben Informationsquellen, die keinen direkten Kontakt des Angreifers mit seinem Opfer erfordern. Ein solches Auskundschaften bezeichnet man als *passive Reconnaissance* (Abbildung 4.4):

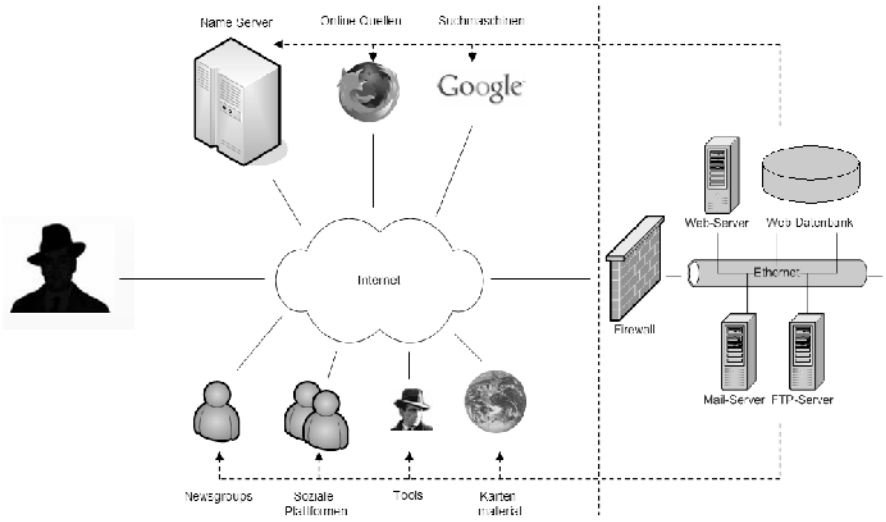


Abbildung 4.4: Passive Reconnaissance

Der Angreifer fragt öffentliche Quellen ab, die ihm die gewünschten Informationen zur Verfügung stellen: Nameserver, Web-Site-Archive, Suchmaschinen, Newsgroups, soziale Netzwerke wie zum Beispiel *www.xing.de*, Reconnaissance-Werkzeuge und Kartenmaterial. Er selbst tritt dem Opfer gegenüber nicht in Erscheinung.

Bei der *aktiven Reconnaissance* kontaktiert der Angreifer sein Opfer. Er verbindet sich mit dessen Netzwerk, sucht aktive Geräte und offene Ports. Da bei dieser Form der Erkundung eine hohe Überschneidung mit der nachfolgenden Phase des Abtastens besteht, unterscheiden manche Experten nicht zwischen aktiver Reconnaissance und Scanning.

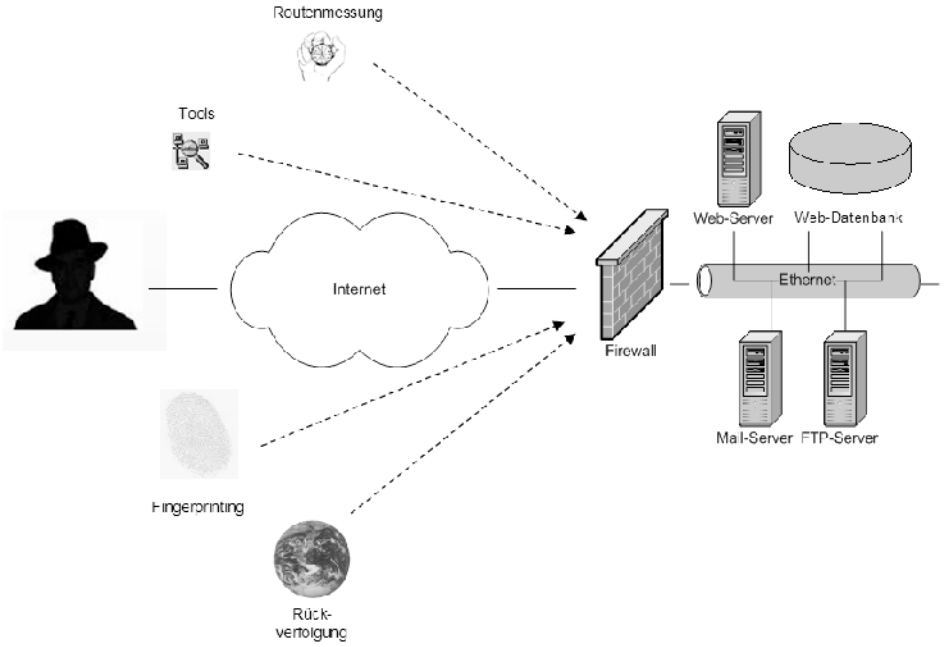


Abbildung 4.5: Aktive Reconnaissance

Aktive Reconnaissance wird angewendet, wenn das Risiko, entdeckt zu werden, gering ist, oder wenn schnelle Ergebnisse vorliegen müssen. Der Hacker nutzt automatisierte Tools, um Router, Switches, Firewalls und Server im Zielnetzwerk zu identifizieren und misst die Netzwerkpfade dorthin aus. Er versucht die installierten Betriebssysteme auf diesen Devices zu erkennen (*Fingerprinting*) und nutzt Visualisierungstools, um die Netzwerkrouten ausmessen und verfolgen zu können. Das aktive Erkunden gleicht dem „Rütteln an der Tür", um zu überprüfen, ob jemand etwas bemerkt und reagiert.

In der Erkundungsphase geht der Hacker typischerweise wie folgt vor:

1. Zuerst werden die Domänen des Unternehmens ermittelt. Diese Recherche umfasst nicht nur die offizielle Web-Site des Unternehmens (z.B. *www.firma.de*), sondern insbesondere auch Intranets, Test-Plattformen und interne Abteilungsserver.

2. Im nächsten Schritt wird der IP-Adressbereich des Unternehmens ermittelt. Mit dieser Information kennt der Hacker die IP-Adressen der direkt an das Internet angebundenen und öffentlich erreichbaren Server.
3. Durch ein „Anpingen" dieser IP-Adressen erfährt der Hacker, welche Geräte aktiv sind. Diese Geräte tastet er über einen Port-Scan ab. Zudem ermittelt er die Betriebssysteme der aktiven Komponenten und die darauf laufenden Dienste.

Reconnaissance umfasst typischerweise die ersten beiden Schritte, während der dritte Schritt der Phase des Abtastens zugeordnet wird (*Scanning*). Das Ergebnis aller drei Schritte wird als *Footprint* bezeichnet: ein Sicherheitsprofil des Unternehmens, das nicht nur Informationen über Domänen und Netzwerkblöcke enthält, sondern auch Aufschluss über Netzwerkdienste gibt, über die Systemarchitektur, über Anmeldeverfahren, Telefonnummern und Kontaktadressen. Ein vollständiger Durchschlag der Netztopologie ...

Die mittels Reconnaissance erkundeten Informationen sind nicht nur für Hacker interessant, sondern insbesondere für die sicherheitsverantwortlichen Administratoren der Unternehmen: Denn die vorgestellten Techniken geben ein detailliertes Bild, welche Informationen über das Unternehmen öffentlich abrufbar sind.

Proxy Server

Um bei der aktiven Erkundung des Zielnetzwerks selbst unentdeckt zu bleiben, verbergen Hacker ihre Aktivitäten hinter Proxy-Servern. Denn um erfahren zu können, ob eine IP-Adresse mit einem aktiven Gerät verknüpft ist, muss eine TCP- oder UDP-Verbindung mit dem Rechner hinter dieser IP-Adresse hergestellt werden. Eine solche Verbindung wird von einer *Firewall* bzw. von einem *Intrusion Detection System* protokolliert. Daher nutzen umsichtige Hacker einen *Proxy-Server* für die Herstellung von Verbindungen. Ein Proxy-Server hat die Funktion des bloßen Durchleitens. Der Hacker kann mit Hilfe eines Proxy-Servers den Zielrechner kontaktieren und dabei selbst verborgen bleiben, indem er sich mit dem Proxy verbindet und die Verbindungsanfrage von dem Proxy-Server an den Zielrechner stellen lässt. Abbildung 4.6 verdeutlicht die Vorgehensweise:

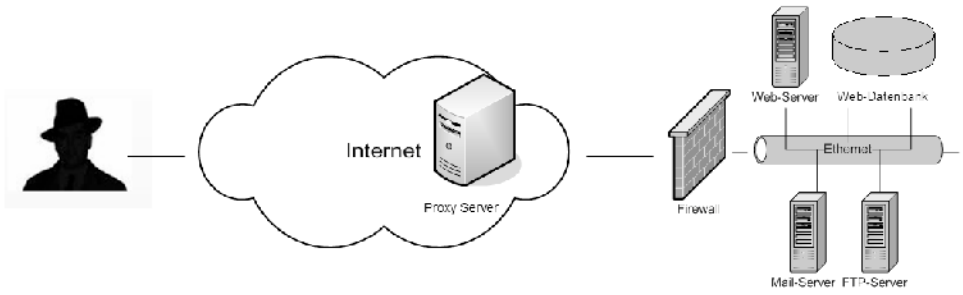


Abbildung 4.6: Proxy-Server

Aus Sicht des protokollierenden Zielnetzwerks tritt der Proxy als sichtbarer Client auf, nicht der Rechner des Hackers!

Im Internet finden sich zahlreiche, frei verfügbare Proxy-Server, die zu diesem Zweck verwendet werden können. Eine Google-Abfrage nach `"free proxy server"` liefert eine umfassende Übersicht! Es gibt allerdings auch kommerzielle Proxy-Server: Abbildung 4.7 zeigt die Funktionsweise des *Anonymizer*:

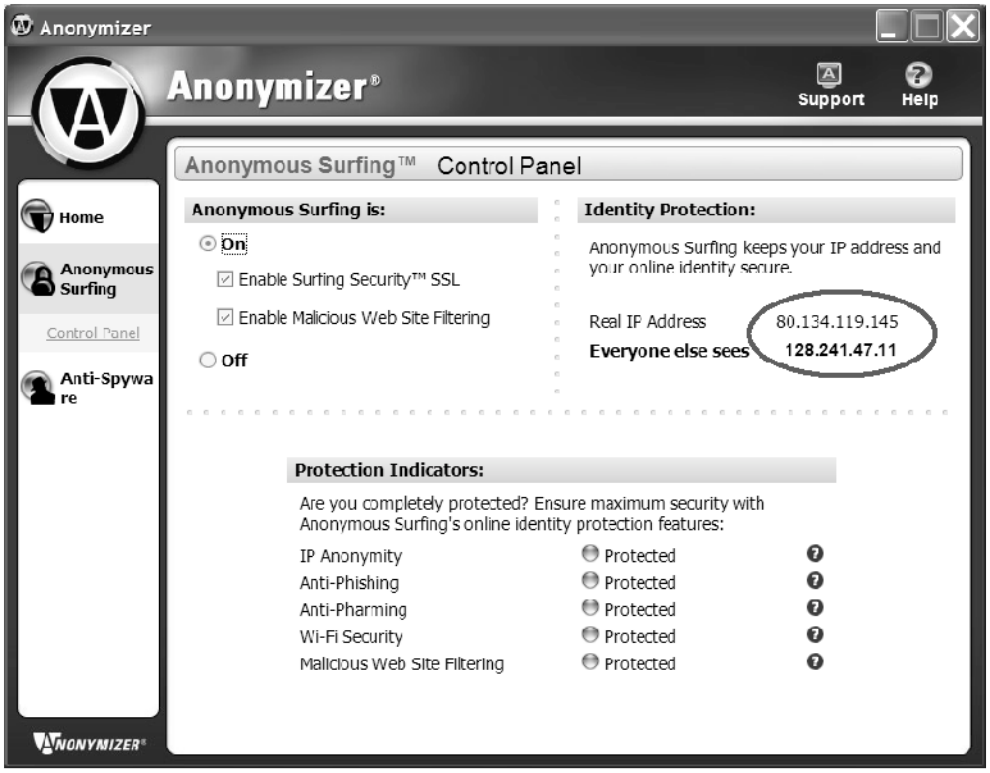


Abbildung 4.7: Anonymes Surfen mit dem *Anonymizer*

Ist der *Anonymizer* als Client-Software auf dem Rechner des Benutzers installiert, wird jede Internet-Datenkommunikation dieses Rechners automatisch auf die Server des Produktherstellers umgeleitet; diese treten mit dem eigentlich adressierten Server in Kontakt, so dass die eigentliche IP-Adresse des Benutzers verborgen bleibt! Auf diese Weise ist es nicht möglich, die Internet-Aktivitäten des Benutzers zurückzuverfolgen[4], und der Benutzer kann anonym surfen[5].

Echte Hacker verlassen sich weder auf kommerzielle Software noch auf „frei verfügbare Proxies“: Wer kann schon sicher sein, ob diese nicht als Falle aufgestellt wurden und den durchgeleiteten Netzwerkverkehr heimlich protokollieren?

4. Die Identität des Benutzers ist in diesem Fall ausschließlich der Firma *Anonymizer, Inc.* in den USA bekannt, dem Betreiber der *Anonymizer*-Server. *Anonymizer, Inc.* wirbt damit, die Aktivitäten ihrer Kunden selbst nicht zu protokollieren.
5. Der „Anonymizer“ ist ein kommerzielles Produkt und gegen Gebühr unter *http://www.anonymizer.com/* erhältlich.

Proxy Chains

Professionelle Hacker bauen sich eigene Proxy-Netzwerke auf, indem sie fremde Server im Internet kompromittieren und zweckentfremden. Ein Hacker installiert seine Schadsoftware auf einem solchen Rechner, unbemerkt von dessen Eigentümer oder Betreiber. Diese *Stealth-Software* wartet dann nach ihrer Installation nicht-interaktiv auf die Anfragen ihres „Masters“. Der kompromittierte Rechner wird so zum willenlosen, ferngesteuerten „Zombie“.

Mittlerweile sind Tausende von Servern im Internet unter fremder Kontrolle und somit empfänglich für Missbrauch. Abbildung 4.8 veranschaulicht, wie Hacker ein vollwertiges Netzwerk kompromittierter Rechner als Proxy-Server ausnutzen, unbemerkt von den betroffenen Betreibern.

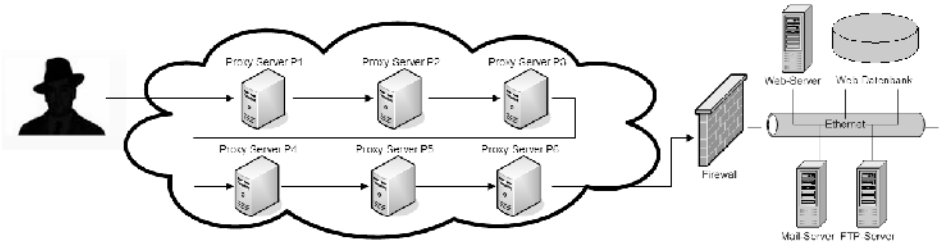


Abbildung 4.8: Verkettung von Proxy-Servern zu einer *Proxy Chain*

Die Verkettung mehrerer Rechner zu einer Kette von Proxy-Servern, einer sog. *Proxy Chain*, zeigt, dass es beinahe unmöglich ist, den Kommunikationsweg vom Opfer bis zum Angreifer zurückzuverfolgen: Ist der Hacker geschickt und umsichtig, bleibt seine Identität anonym!

4.2 Passives Auskundschaften

Beim passiven Auskundschaften des Zielnetzwerks versucht der Hacker herauszufinden, wer sein Opfer ist und wo er es findet. Dabei recherchiert er u.a. die folgenden Informationen:

- Domänen

  Die Hauptdomänen eines Unternehmens können über eine einfache Google-Suche nach der Firmenbezeichnung des Unternehmens ermittelt werden. Nicht veröffentlichte Domänen werden über die Google-Abfrage

  ```
  site:meine-firma.de -site:www.meine-firma.de
  ```

  gefunden. Beispielsweise werden dabei gefunden:

  ```
  webmail.meine-firma.de
  news.meine-firma.de
  ```

```
secure.meine-firma.de
test.meine-firma.de
```

- IP-Adressbereiche

  Die dem Unternehmen offiziell zugeteilten IP-Adressen können über eine Anfrage bei der *ARIN*, über ein *whois*-Abfrage oder mit Hilfe von Werkzeugen wie *nslookup* oder *DNSstuff.com* in kurzer Zeit ermittelt werden. Beispiele folgen in Abschnitt 4.2.1.

- Suchmaschinen

  Suchmaschinen sind schier unerschöpfliche Informationsquellen. Sucht man nach dem Firmennamen und folgt den gelisteten Treffern, erhält man eine umfassende Übersicht über die Produkte, Geschäftspartner und Mitarbeiter des Unternehmens. Darüber hinaus bietet *Google Hacking* umfangreiche Abfragemöglichkeiten. So lassen sich beispielsweise die bisher veröffentlichten E-Mail-Adressen der Domäne eines Unternehmens über die folgende Google-Suche ermitteln:

  ```
  @meine-firma.de
  ```

- Newsgroups

  Newsgroups dienen u.a dem Austausch von Problemen und Lösungen. Beispielsweise stellen Entwickler eine Anfrage in einer Newsgroup, wenn sie eine Fehlermeldung nicht verstehen oder ein bestimmtes Implementierungsproblem nicht lösen können; Administratoren posten Ausschnitte aus Konfigurations- und Protokolldateien in Newsgroups.

  Google durchsucht nicht nur die Web-Seiten eines Unternehmens nach Schlüsselwörtern, sondern insbesondere auch alle Inhalte von Newsgroups. So finden sich bei einer dedizierten Suche unter *groups.google.com* häufig wertvolle Hinweise über

  - Servernamen
  - interne IP-Adressen
  - eingesetzte Hard- und Software
  - E-Mail-Adressen
  - Namen von Entwicklern und Testern
  - Telefonnummern
  - Arbeitsprozesse
  - Benutzerkennungen und Passwörter
  - Einstellungen von Ports
  - interne URLs und Netzwerkressourcen

  und vieles mehr.

- Geschäftspartner und Mitarbeiter

  Job-Plattformen wie beispielsweise

  - *www.xing.com*
  - *www.linkedin.com*
  - *www.gulp.de*
  - *www.monster.de*

und soziale Plattformen wie

- *www.stayfriends.de*

bieten weitere Informationen über die Mitarbeiter und Geschäftspartner eines Unternehmens. Die dort abgestellten Profile beschreiben die Anforderungen an die Mitarbeiter und enthalten in den Skill-Sheets häufig Informationen über die eingesetzte Hard- und Software in einem Unternehmen. Insbesondere die geknüpften Kontaktlisten lassen darauf schließen, wer mit wem zu tun hat.

- Web-Seiten

  Oft enthält der HTML-Source-Code einer Web-Site wertvolle Kommentare; in vielen Fällen wurden dort schon Namen und E-Mail-Adressen der Web 2.0-Entwickler gefunden! Bei interaktiven Browseranwendungen können Hacker durch die Analyse des JavaScript-Codes herausfinden, wie die Aufrufschnittstelle eines Servers zu bedienen ist.

- Archivierte Web-Seiten

  Wie in Kapitel 3 bemerkt, werden alle Änderungen an Web-Seiten im Internet registriert und archiviert. Das Zentralarchiv *www.archive.org* hält alle alten Versionen einer Web-Site vor und stellt diese online zur Verfügung. Damit ist jede Information, die jemals auf einer Web-Site veröffentlicht wurde, sicherheitsgefährdend! Dies umfasst nicht nur die HTML-Seiten einer Web-Site, sondern sämtliche Dateien in der Verzeichnisstruktur des Web-Servers: Upload-Protokolle, Konfigurationsdateien, Backup-Dateien. Da in vielen Fällen die dort eingetragenen Informationen auch heute noch aktuell sind, stellen Web-Archive eine besondere Informationsquelle für Hacker dar. Hacker suchen dort nach

  - Datenbank-Connection-Strings
  - internen IP-Adressen und Servernamen
  - Benutzernamen

  und vielem mehr.

- Lokalisierung

  Benötigt der Hacker einen physischen Zugang zum Unternehmensgelände, beispielsweise weil er einen Angriff als Social Engineer plant, helfen ihm Satellitenfotos, die über

  - *maps.google.de*
  - Google Earth

  zur Verfügung stehen.

4.2.1 Wer bist du?

Ist dem Hacker nur die Domäne seines Opfers bekannt, muss er weitere Informationen über das Netzwerk hinter dieser Domain erheben. Ein geeigneter Start für eine entsprechende Recherche sind die für die IP-Adressverwaltung zuständigen Internet-Registrare

- *American Registry for Internet Numbers* (ARIN) für Nordamerika
- *Réseaux IP Européens Network Coordination Centre* (RIPE NCC) für Europa, den Nahen Osten und Zentralasien

- *Asia-Pacific Network Information Center* (APNIC) für Asien und für den Pazifik
- *Latin American and Caribbean Internet Addresses Registry* (LACNIC) für Lateinamerika und für die Karibik
- *African Network Information Center* (AfriNIC) für Afrika

Die folgenden Abschnitte beschreiben zunächst, wie „nackte whois-Anfragen" gestellt werden können und wie die Ergebnisse zu interpretieren sind. Auf dieser Basis werden anschließend komfortable Werkzeuge mit Benutzeroberfläche vorgestellt.

who.is

Die Internet-Seite *http://www.who.is/* bietet eine einheitliche Schnittstelle zur Abfrage von Domaininformationen. Unabhängig von der Kontinental-Zuständigkeit der einzelnen Internet-Registrare zeigt *who.is* alle bekannten Informationen über eine Domäne an. *who.is* selbst prüft nach der Eingabe eines Domainnamens, an welchen Registrar die Anfrage weiterzureichen ist, interpretiert dessen Ergebnis und gibt dieses als Antwort auf die Anfrage des Anwenders aus. Abbildung 4.9 zeigt die whois-Anfrage für einen Server, der in der URL einer Spam-E-Mail auftaucht:

Abbildung 4.9: whois-Anfrage über *who.is*

Listing 4.1 zeigt das Ergebnis der whois-Abfrage:

```
[01] Registry Whois      Domain Name: desibany.com
[02]
[03]                     Status: clientDeleteProhibited, clientRenewProhibited,
[04]                             clientTransferProhibited, clientUpdateProhibited
[05]
[06]                     Registrar: COMPUTER SERVICES LANGENBACH GMBH DBA JOKER.COM
[07]                     Whois Server: whois.joker.com
[08]                     Referral URL: http://www.joker.com
[09]
[10]                     Expiration Date: 2008-09-04
```

Listing 4.1: Ergebnis einer whois-Abfrage

```
[11]                    Creation Date: 2007-09-04
[12]                    Last Update Date: 2007-09-04
[13]
[14]                    Name Servers:
[15]                        ns1.metdns87.com
[16]                        ns2.metdns87.com
[17]                        ns3.metdns87.com
[18]                        ns4.metdns87.com
[19] ------------------------------------------------------------------------------
[20] Extended Info      IP Address: 211.110.100.135
[21]                    IP Location:  Korea, Republic of
[22]                    Website Status: inactive
[23]                    Cache Date: 2007-09-05 11:37:26 MST
[24] ------------------------------------------------------------------------------
[25] Available Domains  No route to host (113) Unable to retrieve Available
[26] Domains.
[27] ------------------------------------------------------------------------------
[28] Whois              domain:       desibany.com
[29]                    owner:        Speshilov Evgeny
[30]                    organization: Speshilov INC
[31]                    email:        admin@speshilovinc.com
[32]                    address:      Marksa 52, Office 12
[33]                    city:         Omsk
[34]                    state:        --
[35]                    postal-code:  644119
[36]                    country:      RU
[37]                    phone:        +738.12282296
[38]                    admin-c:      CCOM-1114955  admin@speshilovinc.com
[39]                    tech-c:       CCOM-1114955  admin@speshilovinc.com
[40]                    billing-c:    CCOM-1114955  admin@speshilovinc.com
[41]                    nserver:      ns1.metdns87.com 211.110.100.135
[42]                    nserver:      ns2.metdns87.com 210.51.162.250
[43]                    nserver:      ns3.metdns87.com 211.110.100.135
[44]                    nserver:      ns4.metdns87.com 210.51.162.250
[45]                    status:       lock
[46]                    created:      2007-09-04 10:01:47 UTC
[47]                    modified:     2007-09-04 16:15:56 UTC
[48]                    expires:      2008-09-04 10:01:47 UTC
[49]
[50]                    contact-hdl:  CCOM-1114955
[51]                    person:       Speshilov Evgeny
```

Listing 4.1: Ergebnis einer whois-Abfrage (Forts.)

```
[52]                    organization: Speshilov INC
[53]                    email:        admin@speshilovinc.com
[54]                    address:      Marksa 52, Office 12
[55]                    city:         Omsk
[56]                    state:        --
[57]                    postal-code:  644119
[58]                    country:      RU
[59]                    phone:        +738.12282296
[60]
[61]                    source:       joker.com live whois service
[62]                    query-time:   0.020031
[63]                    db-updated:   2007-09-05 11:36:36
[64]
[65]                    NOTE: By submitting a WHOIS query, you agree to abide by
[66]                          following terms of use: You agree that you may use
[67]                          this data only for lawful purposes and that under no
[68]                          circumstances will you use this data to:
[69]                          (1) allow, enable, or otherwise support the
[70]                              transmission of mass unsolicited, commercial
[71]                              advertising or solicitations via direct mail,
[72]                              e-mail, telephone, or facsimile; or
[73]                          (2) enable high volume, automated, electronic
[74]                              processes that apply to Joker.com (or its
[75]                              computer systems).
[76]                     The compilation, repackaging,
[77]                         dissemination or other use of this data is expressly
[78]                          prohibited without the prior written consent of
[79]                          Joker.com.
```

Listing 4.1: Ergebnis einer whois-Abfrage (Forts.)

Die whois-Abfrage liefert:

- Zeile 3-4: Status der Domäne[6]
- Zeile 6: zuständiger Registrar
- Zeile 7-8: zuständiger whois-Server
- Zeile 15-18: Nameserver der Domäne[7]

6. *client...Prohibited* bedeutet, dass jeder Versuch, die Domäne ohne Genehmigung des eingetragenen Providers bzw. Providers zu löschen oder an einen anderen Eigentümer zu übertragen, abgewiesen werden muss.
7. Es müssen immer mindestens zwei Nameserver bei dem Registrar angegeben werden. Fällt der Primary Nameserver aus, wird die Anfrage an einen Secondary Nameserver weitergereicht.

- Zeile 20-23: IP-Adresse und Lokalisierung der Domäne
- Zeile 29-37: Kontaktinformationen über den Eigentümer der Domäne (owner-c)
- Zeile 38: Kontaktinformationen über den zuständigen Administrator (admin-c)
- Zeile 39: Kontaktinformationen über den technischen Ansprechpartner (tech-c)
- Zeile 40: Kontaktinformationen über den zuständigen Abrechnungspartner (billing-c)
- Zeile 41-44: IP-Adressen der Nameserver

Sind dem Hacker die Nameserver der Domain bekannt, kann er diese nach weiteren Informationen über das Unternehmensnetzwerk befragen (*Nameserver Lookup*).

nslookup

Um einen Rechner in einem Netz adressieren zu können, muss dessen Hostname zunächst in eine IP-Adresse übersetzt werden. Innerhalb eines Unternehmensnetzwerks sind für diese *Namensauflösung* sog. *Name Server* (NS) zuständig. Im weltweiten Internet werden *Domain Name Server* (DNS) für die Auflösung von Domainnamen eingesetzt.

Nameserver Ein Hostname besteht aus mehreren Labels, die durch einen Punkt voneinander getrennt sind. Beispielsweise besteht der Hostname *www.meine-firma.de*, von rechts nach links aufgelöst, aus einer Top-Level-Domain *de*, aus einem Label *meine-firma* und einem weiteren Label *www*. Maximal kann ein Hostname aus 255 Zeichen bestehen und sich in beliebig viele Labels aufteilen. Da die Anzahl der möglichen Hostnamen unglaublich groß ist, eignet sich eine zentrale Namensauflösung durch eine einzige Instanz im Internet nicht. Ein solches Server-Cluster würde schnell unter der Last der gleichzeitig eingehenden Anfragen zusammenbrechen.

Aus diesem Grund ist das DNS-System im Internet als verteilte, hierarchische Datenbank organisiert und besteht aus tausenden, weltweit verstreuten Servern. Jeder dieser Server ist für eine bestimmte Teilmenge von Hostnamen zuständig. Trifft eine Anfrage ein, die der Server selbst nicht beantworten kann, delegiert er die Anfrage an den in der DNS-Hierarchie über ihm stehenden Nameserver weiter. Abbildung 4.10 beschreibt das Prinzip.

Jeder aufzulösende Hostname wird bei dem *Root Name Server* angefragt. Dieser Root-Server betrachtet das am weitesten rechts stehende Label und delegiert die Anfrage an den für die Top-Level-Domain zuständigen Nameserver weiter. Dieses Prinzip wird iteriert, bis der Hostname innerhalb der Nameserver-Hierarchie soweit zerlegt wurde, dass der zuständige Nameserver den Hostnamen in eine IP-Adresse auflösen kann.

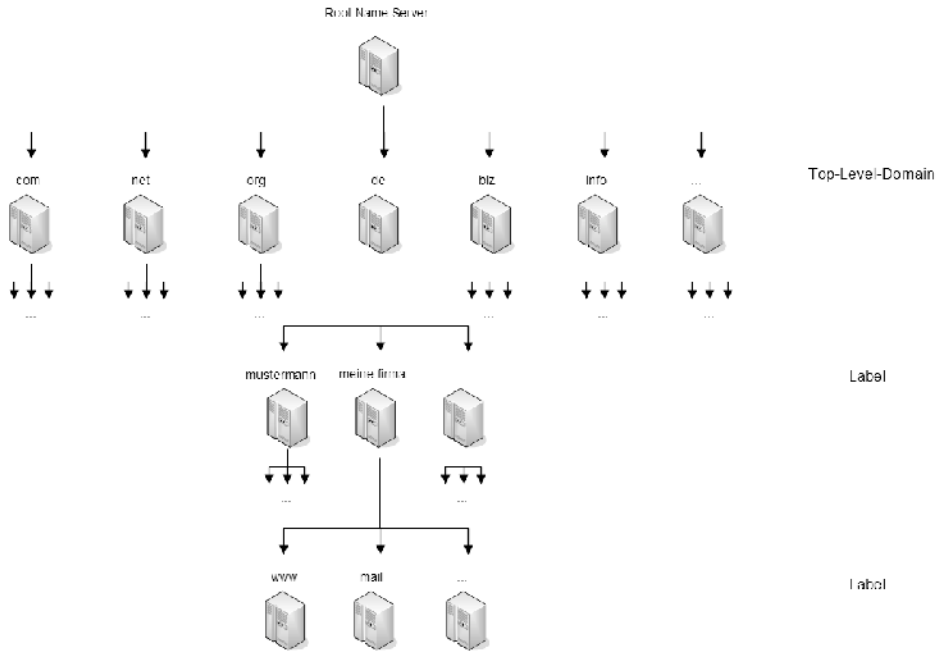


Abbildung 4.10: Domain Name Server als verteilte, hierarchisch organisierte Datenbank

Lookup Das Tool *nslookup* führt einen „Nameserver-Lookup" durch und wird mit UNIX und Windows in Form eines Kommandozeilenwerkzeugs ausgeliefert. Es befragt einen beliebigen Nameserver nach den dort hinterlegten Einträgen für eine bestimmte Domain und lässt diesen Nameserver die Anfrage innerhalb der DNS-Hierarchie delegieren, bis eine Auflösung vorgenommen werden konnte.

Die Anfrage

```
>nslookup
server ns1.metdns87.com
set type=any
desibany.com
```

liefert beispielsweise:

```
[01]        primary name server = ns1.metdns87.com
[02]        responsible mail addr = hostmaster.desibany.com
[03]        serial  = 2007041100
[04]        refresh = 10800 (3 hours)
[05]        retry   = 3600 (1 hour)
[06]        expire  = 3600000 (41 days 16 hours)
[07]        default TTL = 3600 (1 hour)
```

```
[08]desibany.com        nameserver = ns1.metdns87.com
[09]desibany.com        nameserver = ns2.metdns87.com
[10]desibany.com        nameserver = ns3.metdns87.com
[11]desibany.com        nameserver = ns4.metdns87.com
[12]desibany.com        preference = 10, mail exchanger = smtp1.desibany.com
[13]desibany.com        preference = 20, mail exchanger = smtp2.desibany.com
[14]desibany.com        internet address = 211.110.100.135
[15]ns1.metdns87.com    internet address = 211.110.100.135
[16]ns2.metdns87.com    internet address = 210.51.162.250
[17]ns3.metdns87.com    internet address = 211.110.100.135
[18]ns4.metdns87.com    internet address = 210.51.162.250
[19]smtp1.desibany.com  internet address = 211.110.100.154
[20]smtp2.desibany.com  internet address = 210.51.162.251
[21]www.desibany.com    canonical name = ns1.desibany.com
```

Jedem Nameserver liegt eine Datenbasis der von ihm verwalteten Hostnamen und IP-Adressen zugrunde. Diese Datenbasis wird als *Zonenfile* bezeichnet und auf dem Nameserver verwaltet. Das oben aufgeführte Ergebnis ist die Antwort des für die Domain `desibany.com` zuständigen Nameservers auf Basis der Angaben in dessen Zonenfile für diese Domain:

- Die Zeilen 1-7 liefern administrative Angaben, insbesondere über die Aktualität des Eintrags (*SOA-Record*).
- Die Zeilen 8-11 benennen die Nameserver, die den Domainnamen `desibany.com` auflösen können (*NS-Records*). Aus Gründen der Ausfallsicherheit müssen mindestens zwei Nameserver angeführt werden.
- Die Zeilen 12 und 13 geben die Mailserver für die angefragte Domain an[8] (*MX-Records*). Wiederum werden zwei Mailserver aufgeführt, denen in dem Attribut `preference` eine Priorität zugeordnet ist. Die eingehenden Mailanfragen beantwortet zunächst der Mailserver mit der kleinsten Zahl, also der höchsten Priorität. Bei einem Ausfall kann auf die nachfolgenden Mailserver mit geringerer Priorität ausgewichen werden.
- Die Zeilen 14-20 lösen die für die Domain `desibany.com` relevanten Hostnamen in IP-Adressen auf (*A-Records*). Dies umfasst neben der Domain selbst die Nameserver und Mailserver der vorangehenden Zeilen.
- In der Zeile 21 wird ein Alias festgelegt (*CNAME* = canonical name), so dass die Domain nicht nur über den URL *http://desibany.com/*, sondern auch über den im Web üblicheren URL *http://www.desibany.com/* aufgerufen werden kann.

Eine Zonendatei enthält die Einträge sämtlicher Hostnamen und Domains, die der Nameserver auflösen kann. Das Werkzeug *nslookup* fragt einen Nameserver über den Port 53 (UDP) an, und der Nameserver liefert eine aufbereitete, lesbare Ausgabe, die er aus den Einträgen seines Zonenfiles für die angefragte Domain generiert.

8. Falls der Domain Maildienste zugeordnet sind.

Resource Records Die einzelnen Einträge in einem Zonenfile bezeichnet man als *Resource Records* (RR). Tabelle 4.2 gibt eine Übersicht über die verschiedenen RR-Typen:

RR	Bezeichnung	Beschreibung
A	Adress-Record	ordnet einem Hostnamen eine IPv4-Adresse zu. In dem Beispiel `meine-firma.de. 3600 IN A 218.117.47.11` wird der Internet-Domain `meine-firma.de` (`IN`) über einen Address-Record (`A`) die IP-Adresse `218.117.47.11` zugeordnet. Diese Information verbleibt für `3600` Sekunden („Time to Live") in dem Cache des Nameservers, bevor der Nameserver den Eintrag aktualisiert.
CNAME	Alias	kanonischer Name („Alias") für einen Host. Beispiel: `www 3600 IN CNAME meine-firma.de.`
MX	Mail Exchange	legt den für diese Domain zuständigen Mailserver fest. Beispiel: `mail IN MX 10 smtp.meine-firma.de.`
NS	Nameserver	Hostname eines zuständigen Nameservers. Beispiel: `meine-firma.de.3600IN NS ns1.meine-firma.de.`
PTR	Domain Name Pointer	ermöglicht einen *Reverse Lookup*, d.h. die Ermittlung des Hostnamens ausgehend von einer IP-Adresse
SOA	Start of Authority	enthält wichtige Angaben zur Aktualität des Zonenfiles
TXT	frei definierbarer Text	ermöglicht die Kommentierung der Einträge und Weiterreichung der Information an den anfragenden Client. Beispiel: `intranet.meine-firma.de. 3600 IN TXT "nur für Mitarbeiter"`

Tabelle 4.2: Resource Records

Zonentransfers Nameserver sind für die Namensauflösung in Netzen zuständig. Da Anwender nicht direkt die IP-Adressen der adressierten Server angeben, sondern lesbare Hostnamen verwenden, hätte der Ausfall eines Nameservers weitreichende Konsequenzen in einer Netzwerkkommunikation. Aus diesem Grund werden DNS-Daten auf mehreren Nameservern redundant vorgehalten. Findet eine Änderung an diesen Daten statt, so müssen alle betroffenen Nameserver aktualisiert werden. Diese Synchronisation wird als *Zonentransfer* bezeichnet. Dabei wird die gewünschte Änderung zunächst in dem Zonenfile des *Primary Nameservers* eingetragen, dem sog. *Master*, und anschließend an die *Secondary Nameserver*, die sog. *Slaves*, durchgereicht.

Damit die Nameserver ein Zonenfile untereinander abgleichen können, wird eine Seriennummer und ein Zeitstempel geführt. Diese Angaben werden in dem *SOA-Record*, dem *Start of Authority*, zu Beginn des Zonenfiles verwaltet. In dem Beispiel

```
meine-firma.de.   1800  IN  SOA  ns1.meine-firma.de. hostmaster.meine-firma.de.
                                 (
                                    4711  ; Seriennummer
                                    300   ; Refresh
                                    100   ; Retry
                                    6000  ; Expire
                                 )
```

wird für die Domäne `meine-firma.de` der primäre Nameserver `ns1.meine-firma.de` festgelegt und die E-Mail-Adresse `hostmaster@meine-firma.de` des zuständigen DNS-Administrators hinterlegt[9]. Mit jeder Änderung des Zonenfiles wird die Seriennummer um 1 inkrementiert; z.Zt. hat das Zonenfile die Seriennummer `4711`. Im Abstand von `300` Sekunden fragen die Slaves nun ihren Master, ob sich etwas geändert hat („Refresh"); dies erfolgt durch Vergleich der Seriennummern in den Zonenfiles von Master und Slave. Antwortet der Master nicht, wird die Anfrage nach `100` Sekunden durch den Slave wiederholt („Retry"). Erst nach `6000` Sekunden, in denen der Master wiederholt nicht antwortet, gibt der Slave auf und weist sämtliche DNS-Anfragen für die betroffenen Domains zurück („Expire").

DNS-Angriffe Durch die Abfrage eines Nameservers erhält ein Hacker die IP-Adressen aller mit einer Domain in Zusammenhang stehenden Server: Nameserver, Mailserver und Aliase. Da Nameserver im Allgemeinen eine zentrale Bedeutung für die Netzwerkkommunikation haben, sind sie häufig dedizierten DNS-Angriffen ausgesetzt:

- **Zonentransfer**

  Zonentransfers werden über den TCP-Port 53 veranlasst. Gelingt es einem Angreifer, das Zonenfile eines Nameservers herunterzuladen, so gewinnt er nicht nur Informationen über eine Domain, die ihm bereits bekannt ist; er erhält zudem eine Auflistung aller Hostnamen und IP-Adressen in dem Netzwerk des Unternehmens! Dies betrifft insbesondere die dort intern eingesetzten Server.

- **Denial of Service**

  Über eine verteilte DoS-Attacke (DDoS) können Nameserver lahmgelegt werden. Durch die Last eingehender Anfragen sind sie nicht mehr in der Lage, legitimierte Anfragen zu beantworten. Somit ist eine Kommunikation in dem betroffenen Netz kaum mehr möglich.

- **DNS-Spoofing**

  Beim DNS-Spoofing wird dem anfragenden Client eine gefälschte IP-Adresse zurück geliefert, so dass dieser unwissentlich auf einen anderen Server geleitet wird. Gelingt es beispielsweise, den für die Domäne `meine.bank.de` zuständigen Nameserver zu *spoofen*, können Opfer auf eine Phishing-Site geführt werden, deren URL in der Adresszeile des Browsers exakt mit der URL der Bank übereinstimmt!

Nachdem mit *who.is* und *nslookup* sehr einfache Werkzeuge vorgestellt wurden, stellen die restlichen Abschnitte komfortablere Tools vor.

DNSstuff.com

Die Internet-Plattform *www.dnsstuff.com* stellt eine umfassende Werkzeug-Palette zur Abfrage von Nameservern zur Verfügung (Abbildung 4.11).

9. In der DNS-Notation wird das „@" in der E-Mail-Adresse durch einen Punkt ersetzt.

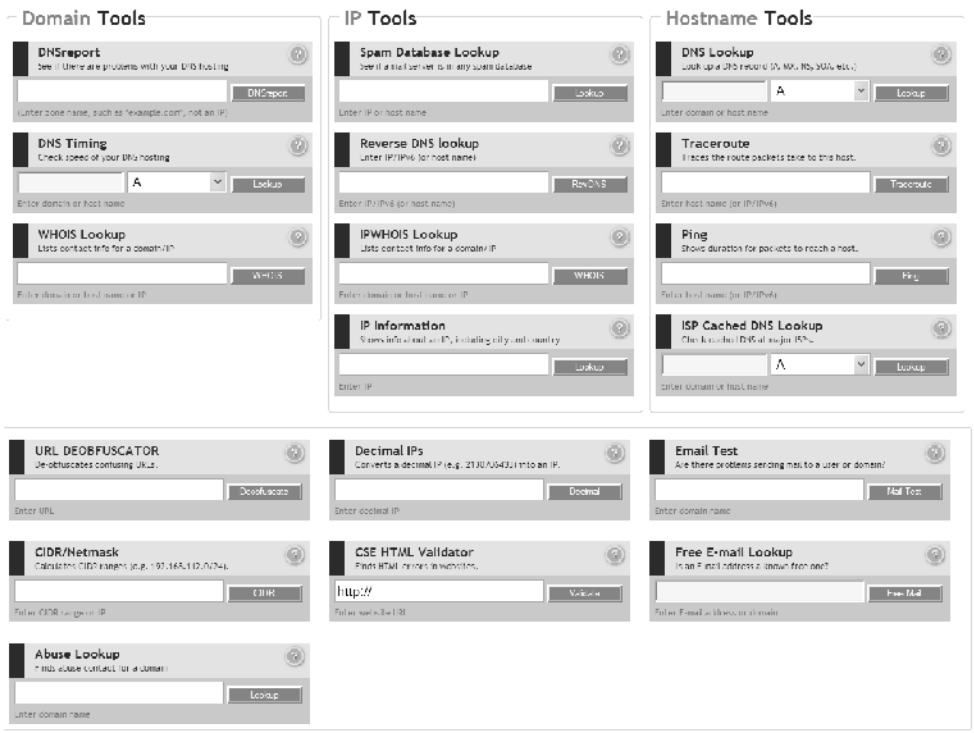


Abbildung 4.11: Nameserver-Abfragen über *DNSstuff.com*

Im oberen Bereich der Seite werden Abfragewerkzeuge bereitgestellt; der untere Bereich bietet kleine nützliche Tools. Die Tabelle 4.3 beschreibt den Einsatz der Werkzeuge:

Kategorie	Tool	Beschreibung
Domain Tools	DNSreport	analysiert über einen Nameserver-Lookup die Resource Records für eine Domäne und bewertet die Vollständigkeit und Richtigkeit dieser Einträge
	DNS Timing	misst die Zugriffszeit auf die Resource Records des Nameservers aus und traversiert, ausgehend vom Root-Nameserver, durch die DNS-Hierarchie, bis der zuständige Nameserver gefunden wurde. Übliche Zugriffszeiten liegen zwischen 30 und 150 ms. Beim Ausmessen kann zwischen den einzelnen RR-Typen unterschieden werden (A, AAAA/IPv6, CNAME, MX, PTR, SOA, SPF, SRV, TXT).
	WHOIS Lookup	Die Whois-Abfrage liefert die rohe Ausgabe des whois-Servers zurück, der für die angefragte Domain zuständig ist (vgl. *who.is* im Abschnitt 4.2.1).

Tabelle 4.3: Werkzeuge von *DNSstuff.com*

Kategorie	Tool	Beschreibung
IP Tools	Spam Database Lookup	fragt die eingegebene IP-Adresse bei mehreren Anti-Spam-Datenbanken ab und stellt die Antworten in einem gemeinsamen Report zusammen
	Reverse DNS Lookup	ermittelt den Hostnamen für die eingegebene IP-Adresse
	IPWHOIS Lookup	führt eine Whois-Abfrage durch (vgl. WHOIS Lookup)
	IP Information	lokalisiert den Standort des Servers für eine angefragte IP-Adresse auf einer Weltkarte
Hostname Tools	DNS Lookup	führt einen Nameserver-Lookup für eine Domäne durch und zeigt den Resource Record des zuständigen Nameservers an (A, AAAA/IPv6, ALL (ANY), CNAME, MX, NS, PTR, SOA, SPF, SRV, TXT)
	Traceroute	misst die Netzwerkroute zu der angegebenen IP-Adresse und führt alle Komponenten auf dieser Strecke auf
	Ping	prüft mittels eines ICMP-Requests („Ping"), ob der angefragte Server aktiv ist und misst die durchschnittliche Antwortzeit dieses Servers
	ISP Cached DNS Lookup	fragt die Resource Records einer Domain weltweit bei verschiedenen bekannten Internet-Providern ab (A, AAAA/IPv6, ALL (ANY), CNAME, MX, NS, PTR, SOA, SPF, SRV, TXT). Bei Abweichungen lässt sich nach einer DNS-Änderung auf diese Weise erkennen, welche Nameserver cachen und wann sie die Änderung bemerken.

Utilities	URL Deobfuscator	deobfuskiert URLs, die von Spammern verschickt wurden und den Anschein erwecken, auf einen „harmlosen" Server zu verzweigen.
		Beispiel: Der URL
		http://www.american-shop.com@2130704711:0815/%2a
		wird von dem *URL Deobfuscator* aufgelöst zu
		`Step 0 You entered:`
		`http://www.american-shop.com@2130704711:0815/*`
		`Step 1 Extract username/password`
		`http://2130704711:0815/*`
		`Step 2 Remove port (e.g. ":80")`
		`http://2130704711/*`
		`Step 3 Decode octets (e.g. "%25")`
		`http://2130704711/*`
		`Step 4 Convert decimal to IP`
		`http://126.255.249.71/*`
		`http://www.american-shop.com@2130704711:0815/* is:`
		`http://126.255.249.71:0815/* .`
		`With a username of www.american-shop.com`
		In Wirklichkeit führt dieser URL also nicht auf die Site *www.american-shop.com*, sondern auf die IP-Adresse `126.255.249.71`!

Tabelle 4.3: Werkzeuge von *DNSstuff.com (Forts.)*

Kategorie	Tool	Beschreibung

	CIDR/Netmask	löst einen in CIDR-Notation[a] formulierten IP-Adressbereich auf
		Beispiel: Der CIDR-Ausdruck `58.9.159.209/24` wird aufgelöst in
		`Location: Thailand (high) [City: Bangkok, Krung Thep Mahanakhon]`
		`CIDR range 58.9.159.209/24`
		`Netmask 255.255.255.0`
		`Wildcard Bits 0.0.0.255`
		`First IP in range 58.9.159.0 (network address)`
		`Last IP in range 58.9.159.255 (broadcast address)`
		`First useable IP in range 58.9.159.1`
		`Last useable IP in range 58.9.159.254`
		`Number of useable IPs in range 254`

	Abuse Lookup	sucht aus einer Whois-Abfrage die E-Mail-Adresse der Domain heraus, die bei Beschwerden wegen Mißbrauch zu kontaktieren ist
	Decimal IPs	konvertiert eine IP-Adresse in ihr dezimal-numerisches Äquivalent Beispiel: `IP 58.9.159.209 is decimal 973709265.` Browser rechnen die kontaktierte IP-Adresse intern auf diese Weise in eine Dezimalzahl um. In der Vergangenheit konnten Hacker eine Sicherheitslücke in den gängigen Browsern ausnutzen, die den URL einer als unsicher geltenden Internet-Zone in eine weniger abgesicherte Intranet-Zone bewerteten. Beispiel: *http://973709265/welcome.htm*
	CSE HTML Validator	überprüft eine HTML-Seite auf syntaktische Fehler
	Email Test	ermittelt mit Hilfe eines Nameserver-Lookups den für eine Domain zuständigen Mailserver und prüft, ob dieser zum aktuellen Zeitpunkt verfügbar ist
	Free E-Mail Lookup	prüft, ob eine E-Mail-Adresse frei verfügbar oder über eine Domäne bereits belegt ist

a *Classless Inter-Domain Routing* (CIDR) ist ein Umrechnungsverfahren für IPv4-Adressen, das zur Reduzierung von Routing-Tabellen eingeführt wurde. Eine IPv4-Adresse, bestehend aus vier Blöcken mit jeweils einem Byte, wird als 32bit-Zahl dargestellt. CIDR gestattet die Darstellung ganzer Subnetze mit Hilfe einer einfachen Postfix-Notation. Beispielsweise meint der Ausdruck `192.168.2.0/24` das Subnetz `255.255.255.0` und damit den gesamten Class-C-Bereich `192.168.2.0 - 192.168.2.255`. Der Postfix `/24` bedeutet dabei, dass die ersten drei Bytes (24 Bits) von links betrachtet unveränderlich sind.

Tabelle 4.3: Werkzeuge von *DNSstuff.com (Forts.)*

Mit Hilfe der Plattform *DNSstuff.com* kann sich ein Hacker auf komfortable Weise ein umfassendes Bild von seinem Zielnetzwerk machen. Ein besonders wichtiges Werkzeug ist dabei der *DNSreport*.

DNSreport *DNSreport* führt einen Nameserver-Lookup für eine Domäne durch und analysiert die gesamten Resource Records für diese Domäne (Abbildung 4.12). Nach Bewertung der Vollständigkeit und Richtigkeit der Resource-Records meldet das Werkzeug semantische Fehler in der Definition der Nameserver-Angaben und gibt nützliche Hinweise für einen abgesicherten Aufbau des Zonenfiles.

DNSreport for meine-firma.de

Generated by http://www.dnsreport.com/ at 09:05:34 GMT on 06 Sep 2007.

Email link to results

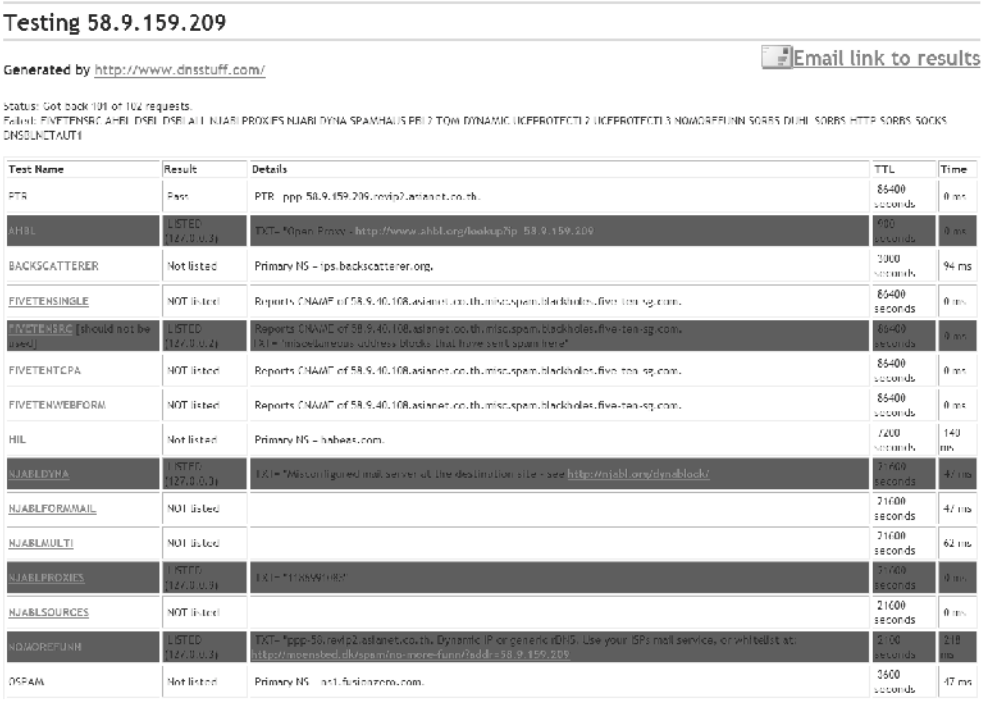
Category	Status	Test Name	Information
MX	INFO	MX Record	Your 2 MX records are: 10 smtp2.meine-firma.de. [TTL 86400] IP 195.214.218.112 [TTL 3600] [GB] IP=195.234.228.151 [TTL=3600] [GB] 10 smtp1.meine-firma.de. [TTL=86400] IP=195.234.228.112 [TTL=3600] [GB] IP=195.214.218.151 [TTL=3600] [GB]
	PASS	Low port test	OK. Our local DNS server that uses a low port number can get your MX record. Some DNS servers are behind firewalls that block low port numbers. This does not guarantee that your DNS server does not block low ports (this specific lookup must be cached), but is a good indication that it does not.
	PASS	Invalid characters	OK. All of your MX records appear to use valid hostnames, without any invalid characters.
	PASS	All MX IPs public	OK. All of your MX records appear to use public IPs. If there were any private IPs, they would not be reachable, causing slight mail delays, extra resource usage, and possibly bounced mail.
	PASS	MX records are not CNAMEs	OK. Looking up your MX record did not just return a CNAME. If an MX record query returns a CNAME, extra processing is required, and some mail servers may not be able to handle it.
	PASS	MX A lookups have no CNAMEs	OK. There appear to be no CNAMEs returned for A records lookups from your MX records (CNAMEs are prohibited in MX records, according to RFC974, RFC1034 3.6.2, RFC1912 2.4, and RFC2181 10.3).
	PASS	MX is host name, not IP	OK. All of your MX records are host names (as opposed to IP addresses, which are not allowed in MX records).
	PASS	Multiple MX records	OK. You have multiple MX records. This means that if one is down or unreachable, the other(s) will be able to accept mail for you.
	PASS	Differing MX A records	OK. I did not detect differing IPs for your MX records (this would happen if your DNS servers return different IPs than the DNS servers that are authoritative for the hostname in your MX records).
	FAIL	**Duplicate MX records**	WARNING: You have duplicate MX records. This means that mailservers may try delivering mail to the same IP more than once. Although technically valid, this is very confusing, and wastes resources. The duplicate MX records are: smtp2.meine-firma.de. and smtp1.meine-firma.de. both resolve to 195.234.228.151.
	FAIL	**Reverse DNS entries for MX records**	ERROR: The IP of one or more of your mail server(s) have no reverse DNS (PTR) entries/" (If you see "Timeout" below, it may mean that your DNS servers did not respond fast enough)"/. RFC1912 2.1 says you should have a reverse DNS for all your mail servers. It is strongly urged that you have them, as many mailservers will not accept mail from mailservers with no reverse DNS entry. You can double-check using the 'Reverse DNS Lookup' tool at the DNSstuff site if you recently changed your reverse DNS entry (it contacts your servers in real time; the reverse DNS lookups in the DNS report use our local caching DNS server). The problem MX records are: 151.228.234.195.in-addr.arpa [No reverse DNS entry (rcode: 3 ancount: 0) (check it)] 151.228.234.195.in-addr.arpa [No reverse DNS entry (rcode: 3 ancount: 0) (check it)]

Abbildung 4.12: DNSreport

Im Beispiel wurden zwei Fehler in den eingetragenen MX-Records gefunden, während die restlichen Prüfungen erfolgreich verliefen.

Spam Database Lookup Dieses Tool ermöglicht dem Hacker zu überprüfen, ob der Spam-Server, den er verwendet, bereits in einer öffentlichen Anti-Spam-Datenbank eingetragen ist (Abbildung 4.13). Gleiches gilt für die in seiner Spam-E-Mail aufgeführten URLs.

Im Beispiel haben mehrere Anti-Spam-Datenbanken den SMTP-Server `58.9.159.209` als Spam-Server gelistet, meist durch Kommentierung in dem Resource Record TXT ihrer Zonenfiles.



Testing 58.9.159.209

Generated by http://www.dnsstuff.com/

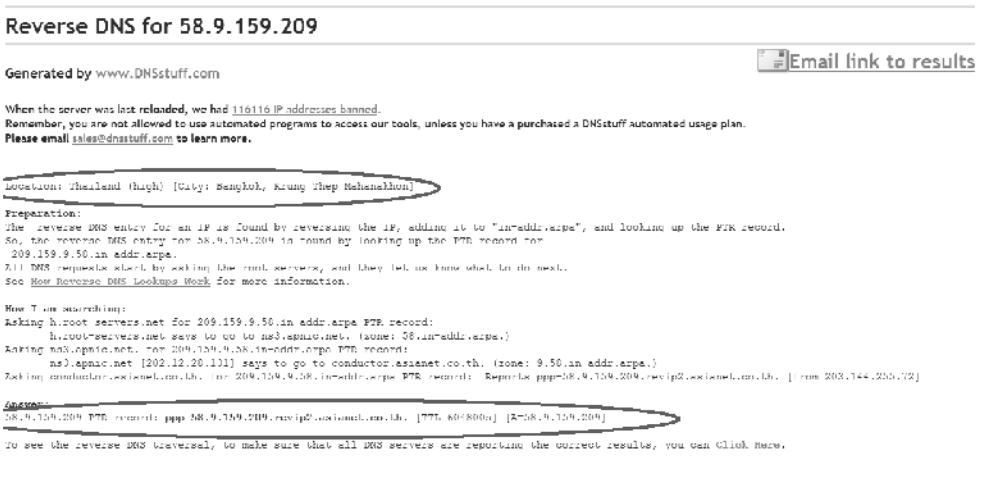
Email link to results

Status: Got back 101 of 102 requests.
Failed: FIVETENSRC AHBL DSBL DSBL ALL NJABL PROXIES NJABL DYNA SPAMHAUS PBL2 TQM DYNAMIC UCEPROTECTL2 UCEPROTECTL3 NOMOREFUNN SORBS DUHL SORBS HTTP SORBS SOCKS DNSBLNETAUT1

Test Name	Result	Details	TTL	Time
PTR	Pass	PTR - ppp-58.9.159.209.revip2.asianet.co.th.	86400 seconds	0 ms
AHBL	LISTED (127.0.0.3)	TXT= "Open Proxy - http://www.ahbl.org/lookup?ip=58.9.159.209	900 seconds	0 ms
BACKSCATTERER	Not listed	Primary NS - ips.backscatterer.org.	3000 seconds	94 ms
FIVETENSINGLE	NOT listed	Reports CNAME of 58.9.40.108.asianet.co.th.misc.spam.blackholes.five-ten-sg.com.	86400 seconds	0 ms
FIVETENSRC [should not be used]	LISTED (127.0.0.2)	Reports CNAME of 58.9.40.108.asianet.co.th.misc.spam.blackholes.five-ten-sg.com. TXT= "miscellaneous address blocks that have sent spam here"	86400 seconds	0 ms
FIVETENTCPA	NOT listed	Reports CNAME of 58.9.40.108.asianet.co.th.misc.spam.blackholes.five-ten-sg.com.	86400 seconds	0 ms
FIVETENWEBFORM	NOT listed	Reports CNAME of 58.9.40.108.asianet.co.th.misc.spam.blackholes.five-ten-sg.com.	86400 seconds	0 ms
HIL	Not listed	Primary NS - habeas.com.	7200 seconds	140 ms
NJABLDYNA	LISTED (127.0.0.3)	TXT= "Misconfigured mail server at the destination site - see http://njabl.org/dynablock/	21600 seconds	47 ms
NJABLFORMMAIL	NOT listed		21600 seconds	47 ms
NJABLMULTI	NOT listed		21600 seconds	62 ms
NJABLPROXIES	LISTED (127.0.0.5)	TXT= "118699108"	21600 seconds	0 ms
NJABLSOURCES	NOT listed		21600 seconds	0 ms
NOMOREFUNN	LISTED (127.0.0.3)	TXT= "ppp-58.revip2.asianet.co.th. Dynamic IP or generic rDNS. Use your ISPs mail service, or whitelist at: http://moensted.dk/spam/no-more-funn/?addr=58.9.159.209	2100 seconds	218 ms
OSPAM	Not listed	Primary NS - ns1.fusionzero.com.	3600 seconds	47 ms

Abbildung 4.13: Spam Database Lookup

Reverse DNS Lookup *Reverse DNS Lookup* ist ein nützliches Werkzeug zur Herleitung des Hostnamens für eine IP-Adresse sowie zur Lokalisierung der IP-Adresse (Abbildung 4.14).



Reverse DNS for 58.9.159.209

Generated by www.DNSstuff.com

Email link to results

When the server was last reloaded, we had 116116 IP addresses banned.
Remember, you are not allowed to use automated programs to access our tools, unless you have a purchased a DNSstuff automated usage plan.
Please email sales@dnsstuff.com to learn more.

Location: Thailand (high) [City: Bangkok, Krung Thep Mahanakhon]

Preparation:
The reverse DNS entry for an IP is found by reversing the IP, adding it to "in-addr.arpa", and looking up the PTR record.
So, the reverse DNS entry for 58.9.159.209 is found by looking up the PTR record for
209.159.9.58.in-addr.arpa.
All DNS requests start by asking the root servers, and they let us know what to do next.
See How Reverse DNS Lookups Work for more information.

How I am searching:
Asking h.root-servers.net for 209.159.9.58.in-addr.arpa PTR record:
h.root-servers.net says to go to ns3.apnic.net. (zone: 58.in-addr.arpa.)
Asking ns3.apnic.net. for 209.159.9.58.in-addr.arpa PTR record:
ns3.apnic.net [202.12.28.131] says to go to conductor.asianet.co.th. (zone: 9.58.in-addr.arpa.)
Asking conductor.asianet.co.th. for 209.159.9.58.in-addr.arpa PTR record: Reports ppp-58.9.159.209.revip2.asianet.co.th. [from 203.144.255.72]

Answer:
58.9.159.209 PTR record: ppp-58.9.159.209.revip2.asianet.co.th. [TTL 604800s] [A=58.9.159.209]

To see the reverse DNS traversal, to make sure that all DNS servers are reporting the correct results, you can Click Here.

Abbildung 4.14: Reverse DNS Lookup

IP Information *IP Information* lokalisiert eine IP-Adresse und zeigt den Ausschnitt einer Weltkarte mit dem Standort des Servers an (Abbildung 4.15).

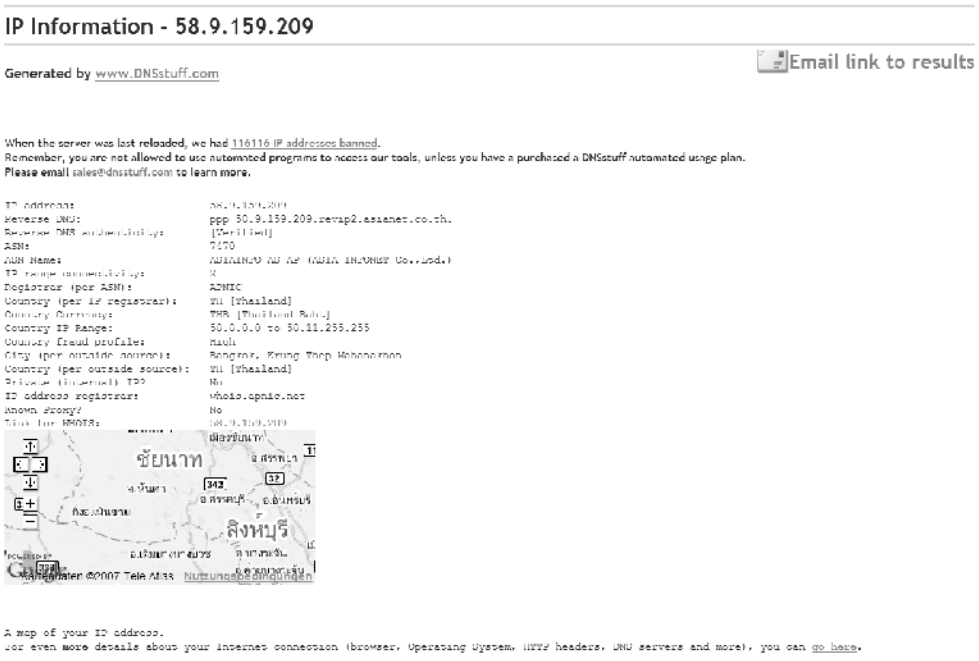


Abbildung 4.15: IP Information

Traceroute *Traceroute* misst die Netzwerkroute, ausgehend von *www.dnsstuff.com*, bis zu der angegebenen IP-Adresse aus und führt alle Komponenten auf dieser Strecke inklusive Hostnamen, IP-Adresse, Land und Betriebssystem auf (Abbildung 4.16).

Traceroute to desibany.com

Generated by www.DNSstuff.com at 09:47:13 GMT on 06 Sep 2007.

Email link to results

Hop	T1	T2	T3	Best	Graph	IP	Hostname	Dist	TTL	Ctry	Time
1	0	*	*	0.5 ms		74.53.59.130 AS0 IANA RSVD 0	82.3b.354a.static.theplanet.com.		255	US	Unix: 9:47:14.584
2	0	*	*	0.5 ms [+0ms]		12.96.160.42 AS21844 THEPLANET-AS	xl2.dsr02.dlstx2.theplanet.com.	0 miles [+0]	254	US	Unix: 9:47:14.622
3	2	*	*	0.7 ms [+0ms]		70.87.253.121 AS21844 THEPLANET-AS	79.fd.5746.static.theplanet.com.	0 miles [+0]	253	US	Unix: 9:47:14.634
4	0	*	*	0.7 ms [+0ms]		70.87.253.21 AS21844 THEPLANET-AS	ct3.1.ibr03.dlstx3.theplanet.com.	0 miles [+0]	61	US	[Router did not respond]
5	0	*	*	0.9 ms [+0ms]		157.238.225.5 AS2914 NTTA-2914	xe-4.4.r03.dlstx09.us.bb.gin.ntt.net.	0 miles [+0]	251	US	Unix: 9:47:14.710
6	1	*	*	1.0 ms [+0ms]		129.250.2.153 AS2914 NTTA-2914	be-2.r20.dlstx09.us.bb.gin.ntt.net.	0 miles [+0]	250	US	Unix: 9:47:14.728
7	6	*	*	6.0 ms [+5ms]		129.250.3.130 AS2914 NTTA-2914	bs-0.r20.hstntx01.us.bb.gin.ntt.net.	0 miles [+0]	249	US	Unix: 9:47:14.771
8	6	*	*	6.2 ms [+0ms]		129.250.3.25 AS2914 NTTA-2914	be-0.r21.hstntx01.us.bb.gin.ntt.net.	0 miles [+0]	248	US	Unix: 9:47:14.797
9	46	*	*	46 ms [+39ms]		129.250.3.121 AS2914 NTTA-2914	as-1.r21.isanca03.us.bb.gin.ntt.net.	0 miles [+0]	247	US	Unix: 9:47:14.898
10	61	*	*	61 ms [+15ms]		129.250.3.162 AS2914 NTTA-2914	pe-2.r01.isanca03.us.bb.gin.ntt.net.	0 miles [+0]	246	US	Unix: 9:47:14.980
11	65	*	*	65 ms [+3ms]		204.1.253.134 AS2914 NTTA-2914	ge-1.14.r01.isanca03.us.ce.gin.ntt.net.	0 miles [+0]	245	US	Unix: 9:47:14.982
12	184	*	*	184 ms [+118ms]		58.229.14.177 AS9318 HANARO-AS	unknown.hananet.net	0 miles [+0]	245	KR	Unix: 9:47:15.365
13	202	*	*	187 ms [+2ms]		210.180.96.2 AS9318 HANARO-AS	cats0962.usr.hananet.net.	-1 miles [+0] 0 miles [+0]	244	KR	[Router did not respond]
14	187	*	*	187 ms [+0ms]		211.117.1.74 AS9318 HANARO-AS	unknown.hananet.net	-1 miles [+0] 0 miles [+0]	243	KR	Unix: 9:47:15.321
15	202	*	*	190 ms [+3ms]		58.229.9.114 AS9318 HANARO-AS	unknown.hananet.net	-1 miles [+0] 0 miles [+0]	242	KR	Unix: 9:47:15.401
16	190	*	*	190 ms [+0ms]		58.229.85.214 AS9318 HANARO-AS	unknown.hananet.net	-1 miles [+0] 0 miles [+0]	241	KR	Unix: 9:47:15.455
17	265	*	*	265 ms [+75ms]		211.59.32.170 AS9318 HANARO-AS	unknown.hananet.net	-1 miles [+0] 0 miles [+0]	49	KR	Unix: 0:37:25.655
18	297	*	*	297 ms [+32ms]		211.110.100.135 AS9277 THRUNET-AS-KR	[Reached Destination]desibany.com [No PTR]		239	KR	Unix: 19:49:18.705

Abbildung 4.16: Traceroute

Smart Whois

Smart Whois ist ein Netzwerkinformationstool, das von der Firma *Tamosoft* unter *http://www.tamos.com/products/smartwhois/* vertrieben wird. *Smart Whois* stellt die Ergebnisse einer whois-Abfrage und eines Nameserver-Lookups in Kürze zusammen:

- IP-Adressen
- Hostnamen
- Domains

Das Werkzeug ermittelt aus über 20 Servern durch automatische Abfrage des zuständigen Registrars den Eigentümer und Betreiber einer Domäne sowie die zuständigen Ansprechpartner. Dabei ordnet es die angefragte IP-Adresse ihrem Netzadressbereich zu und führt diese Abfrage rekursiv über die beteiligten Provider bis zu dem Kontinentalzuständigen Internet-Registrar fort (Abbildung 4.17).

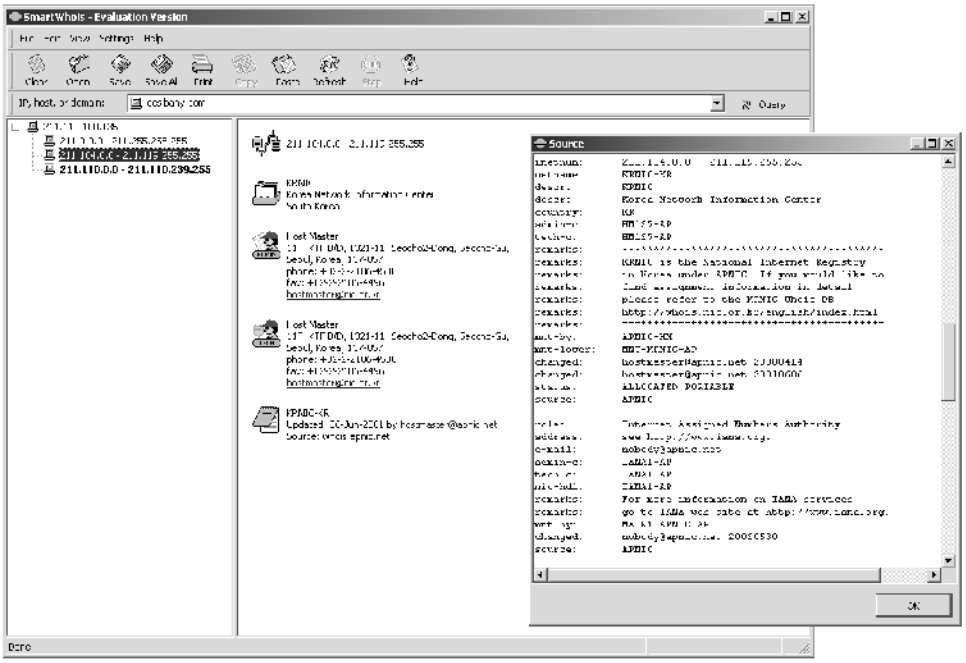


Abbildung 4.17: Smart Whois

Smart Whois kann in Microsoft Outlook und in den Internet Explorer integriert werden. Im Speziellen ermöglicht *Smart Whois* die automatisierte Abfrage von mehreren IP-Adressen oder Domain-Listen („Batch Processing")!

Netcraft

Netcraft ist ein Informationsdienstleister mit Sitz in England, der weltweite Messungen im Internet durchführt und die Ergebnisse auf der Seite *http://news.netcraft.com/* bereitstellt. Die Firma bietet eine kostenlose Anti-Phishing-Toolbar, die sich nahtlos in den Browser integriert und im Hintergrund verschiedene Überprüfungen über die aufgerufenen URLs durchführt. Anwender können Phishing-Sites, auf die sie geleitet wurden, über die Toolbar an Netcraft melden und automatisch in ihrem Browser sperren. Netcraft hat eine hohe Durchdringung im Internet, daher gelten die veröffentlichten Statistiken als sehr zuverlässig. Die Tabellen 4.4 und 4.5 zeigen beispielsweise aktuelle Netcraft-Statistiken über Phishing-Vorfälle[10]:

10. Stand: August 2007

Land	Anzahl der Sites	Phishing-Vorfälle	Anteil bekannter Phishing-Sites
Süd-Korea	1.495.720	24.520	8,1%
Türkei	388.997	8.514	2,8%
Rumänien	100.559	8.368	2,8%
Taiwan	159.198	6.915	2,3%
Israel	70.106	5.060	1,7%

Tabelle 4.4: Die fünf „phishigsten" Länder

Hoster	Anzahl der Phishing-Sites	Anteil der gehosteten Phishing-Sites
Deutsche Telekom AG	8.454	2.8%
CHINANET jiangsu province network	8.435	2.8%
Hanaro Telecom Inc.	7.276	2.4%
KRNIC	6.911	2.3%
Road Runner HoldCo LLC	6.740	2.2%

Tabelle 4.5: Die fünf „phishigsten" Internet-Service-Provider

Weitere abrufbare Statistiken sind:

- *Most Visited Web Sites*
  führt die weltweit am häufigsten abgerufenen Web-Sites auf, aufschlüsselbar nach den einzelnen Ländern.
- *What's that site running?*
  zeigt das für eine Internet-Site eingesetzte Betriebssystem und den eingesetzten Web-Server an.
- *Search Web by Domain*
  durchsucht alle weltweit registrierten Domänennamen nach Zeichenketten. Auf diese Weise können die nicht-veröffentlichten Domänen eines Unternehmens ermittelt werden, beispielsweise *intranet.meine-firma.de*.
- *Sites on the Move*
  zeigt ein Ranking der Provider an, die in der letzten Zeit den meisten Zuwachs an registrierten Domains hatten.
- *Web Server Survey*
  schlüsselt die Marktanteile der führenden Web-Server auf (Apache, Microsoft, Sun, lighttpd, Google, NCSA, andere).

Der Report *What's that site running?* ermöglicht Hackern ein zuverlässiges *Fingerprinting* ihrer Opfer (Abbildung 4.18), denn der Report hält die folgenden Informationen bereit:

- über das eingesetzte Betriebssystem auf dem Server, der die Web-Site der Domäne hostet
- über eingesetzte Web-Server und installierte Module (z.B. PHP, SSL etc.)

- über den Eigentümer der IP-Adresse und des Netzwerkblocks
- über eine vollständige Historie über die Änderungen an der Site-Konfiguration inklusive Zeitstempel und IP-Adressen
- über die Reboots des Servers

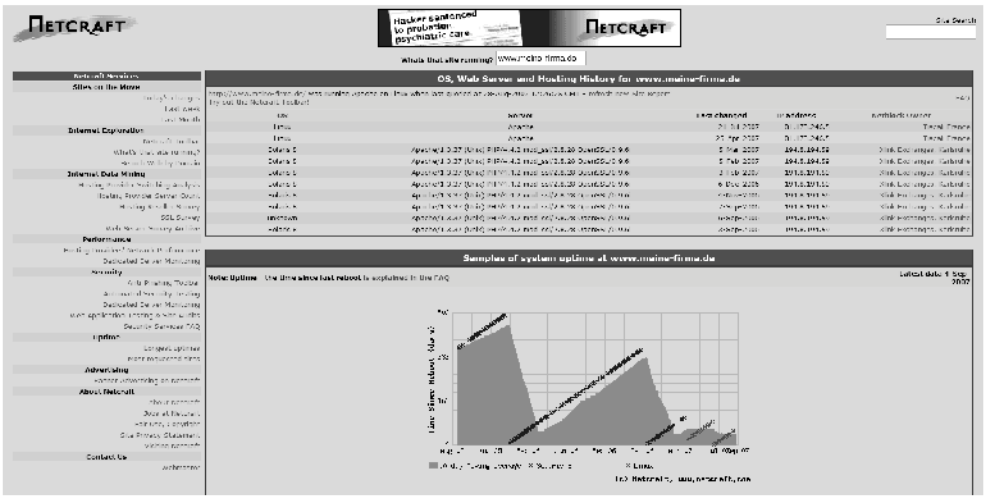


Abbildung 4.18: Fingerprinting mit *Netcraft*

Hacker müssen sich mit Hilfe dieses Tools nicht mit den Servern ihrer Opfer verbinden, um die verwendeten Betriebssysteme und Web-Server zu ermitteln!

archive.org

Die Plattform *www.archive.org* registriert alle inhaltlichen Änderungen an den im Internet gehosteten Web-Sites. Mit jeder Änderung, die *archive.org* feststellt, lagert die Plattform eine Kopie der bisherigen Web-Site in ihr zentrales Datenarchiv ein. Auf Anfrage wird dem Interessenten eine Übersicht aller alten Versionen mit Datumstempel angezeigt, mit der Möglichkeit, nachträglich auf die alten Web-Site-Versionen zugreifen zu können (Abbildung 4.19).

Klickt der Benutzer auf ein Versionsdatum, wird die eingelagerte Web-Site-Version auf einem Server bei *archive.org* entpackt, so dass ein vollständiger Online-Zugriff auf diese Altversion möglich ist. Die Änderungen, die *archive.org* nachhält, reichen über viele Jahre bis zum ersten Launch der Web-Site zurück.

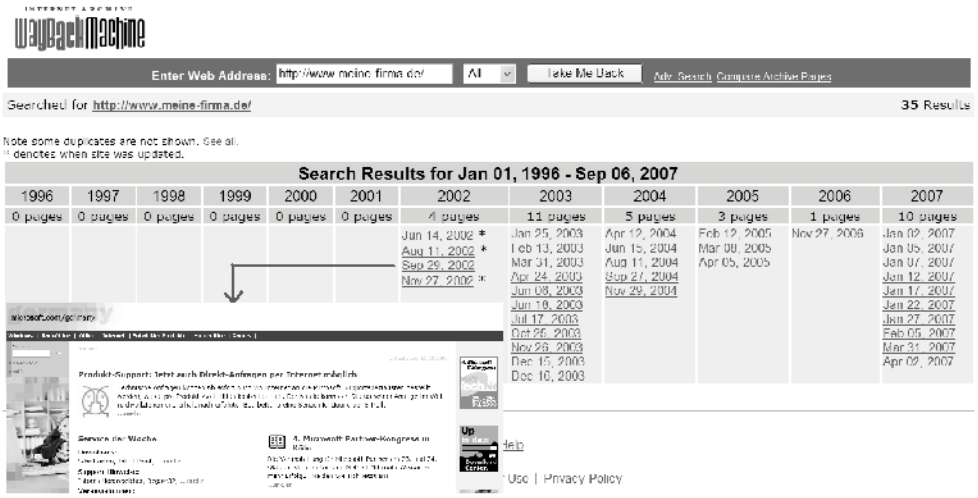


Abbildung 4.19: Zugriff auf alte Web-Sites mit *archive.org*

Einem Hacker ermöglicht diese Plattform die vollständige Spiegelung einer alten Web-Site, um dort nach interessanten Informationen zu suchen, beispielsweise

- nach Backup-Dateien (`.bak`), die Source-Code oder Konfigurationseinstellungen enthalten
- nach Protokollen (`.log`), die interne IP-Adressen, Hostnamen oder Verzeichnisstrukturen verraten

Meist haben die dort gefundenen Angaben auch heute noch Gültigkeit! Dies betrifft insbesondere Datenbank-Connection-Strings, Benutzernamen und Passwörter.

4.2.2 Wo bist du?

In manchen Fällen ist es für einen Hacker erforderlich, das Ziel zu lokalisieren. Benötigt er als Social Engineer beispielsweise einen Zugang zu dem Gelände eines Unternehmens, helfen ihm bei der Vorbereitung seines Angriffs Satellitenfotos und Land- bzw. Stadtkarten.

Satellitenfotos

Satellitenfotos steht über *maps.google.de* und *Google Earth* zur Verfügung (Abbildung 4.20). Weitere Fotos aus der Umgebung eines Unternehmens kann der Hacker zum Beispiel über eine dedizierte Google-Bilder-Suche finden (*images.google.de*).

Abbildung 4.20: Satellitenfotos aus *maps.google.de*

www.utrace.de

Um eine IP-Adresse lokalisieren zu können, muss der Standort des zugehörigen Servers ausgemacht werden. Dabei unterstützt das Tool *http://www.utrace.de/*: Nach Eingabe einer IP-Adresse werden wahlweise Satellitenfotos, schematische Karten und Hybridkarten von der Ziel-IP-Adresse angezeigt (Abbildung 4.21).

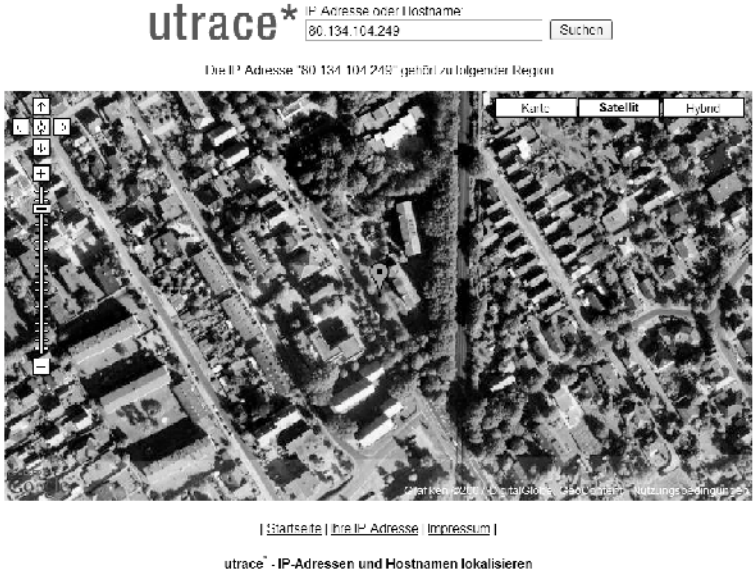


Abbildung 4.21: Lokalisierung einer IP-Adresse über *www.utrace.com*

4.3 Aktives Auskundschaften

Das aktive Auskundschaften eines Ziels erfordert, dass der Hacker sein Opfer kontaktiert. Um dabei anonym zu bleiben, kann der Hacker einen Proxy-Server vorschalten oder von dem kompromittierten Rechner eines anderen Opfers aus agieren.

4.3.1 Wer bist du?

Das aktive Auskundschaften umfasst insbesondere das Abtasten des Zielnetzwerks:

- Welche IP-Adressen sind erreichbar?
- Welche Geräte befinden sich in dem Netz?
- Wie sieht die Netztopologie des Opfers aus?

Da diese Fragestellungen das Thema des nächsten Kapitels sind, werden im Folgenden Werkzeuge vorgestellt, die den Hacker unterstützen, weitere Erkenntnisse über die Methoden des passiven Auskundschaftens hinaus zu erlangen.

Traceroute

Wird ein genaues Bild von der Netzwerkroute zwischen dem Angreifer und dem Opfer benötigt, muss ein Trace durchgeführt werden, und zwar ausgehend von dem Rechner des Angreifers. Entsprechende Kommandozeilenwerkzeuge werden in den Standard-Installationen von UNIX (*traceroute*) und Windows (*tracert*) mitgeliefert.

Ein Traceroute ermittelt die einzelnen Netzwerkkomponenten, die auf der Route eines Paketes von der Quelle zum Ziel liegen. Das Werkzeug misst die Wegzeiten zu den einzelnen Zwischenstationen und führt für jede Komponente einen *Reverse Lookup* durch. Aus dem so ermittelten Hostnamen kann meist schnell erkannt werden, ob es sich bei dem Device um einen Router, einen Switch, ein Gateway, eine Firewall oder Ähnliches handelt.

Abbildung 4.22 zeigt die Ausgabe eines Traceroute-Befehls.

Eine Google-Suche nach den in Abbildung 4.22 aufgeführten Devices ergibt eine ganze Reihe unterschiedlichster Tiscali-Router und Gateways.

Traceroute macht von einem besonderen Feature des IP-Protokolls Gebrauch: dem Parameter *Time To Live* (TTL). Die TTL wird im Header eines UDP- oder ICMP-Paketes verschickt. Jeder Router, der ein solches Paket verarbeitet, dekrementiert diese TTL. Hat die TTL eines Pakets den Wert 0 erreicht, sendet der Router die Nachricht „TTL exceeded“ an den Absender zurück. Router mit reversen DNS-Einträgen enthüllen dabei ihren Namen, ihre Netzwerkanbindung und ihre geographische Lokation.

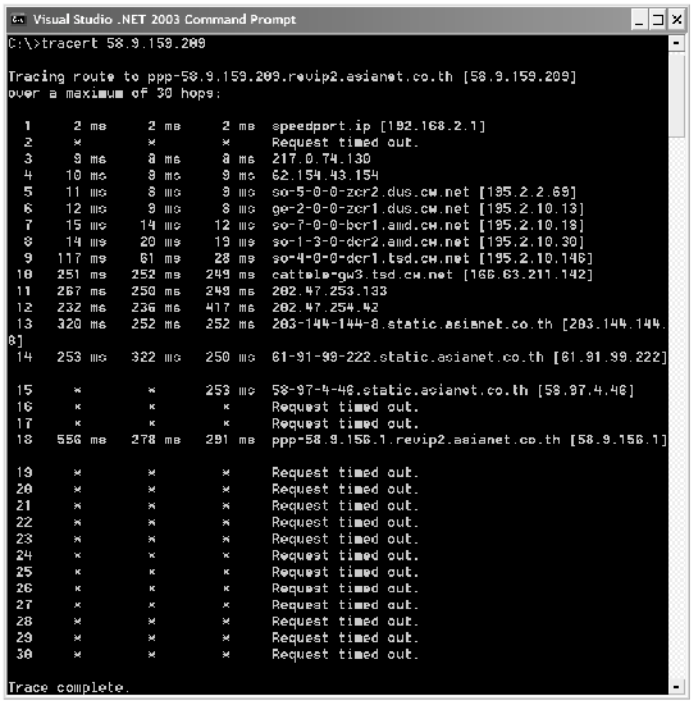


Abbildung 4.22: Traceroute

Traceroute ermittelt die einzelnen Stationen einer Netzwerk-Route, indem es fortlaufend Pakete mit jeweils steigender TTL an das Ziel schickt. Abbildung 4.23 verdeutlicht das Prinzip:

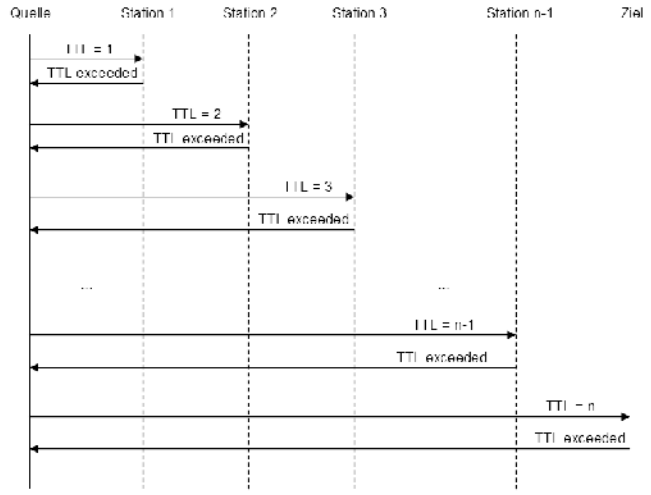


Abbildung 4.23: Ausmessung einer Netzwerkroute mit Hilfe von „Time to Live" (TTL)

Beginnend mit der TTL 1 antwortet die erste Komponente an den Absender zurück. Über die TTL 2 antwortet die zweite Komponente usw. Der Algorithmus endet, wenn das eigentliche Ziel antwortet. Die mit diesem Paket verwendete TTL markiert die Anzahl der Stationen auf der Netzwerkroute vom Absender zum Ziel.

Das Ergebnis ist eine Liste der beteiligten Netzwerkdevices über den Router und die Firewall des Zielnetzwerks hinaus bis hin zu dem adressierten Server. Wendet der Hacker dieses Verfahren für alle ihm bekannten Server in dem Zielnetzwerk an, also beispielsweise auf die IP-Adressen der

- Web-Server
- Mail-Server
- FTP-Server
- Datenbank-Server

kann er sich ein erstes Bild von der Netzwerktopologie seines Opfers machen.

Teleport Pro

Ein weiterer Ansatz ist, die gesamte Datei- und Verzeichnisstruktur der Web-Site einer Domain zu kopieren, um anschließend auf dieser lokalen Kopie zu recherchieren. Ein hilfreiches Werkzeug ist *Teleport Pro*[11], ein sog. „Offline Browsing Webspider" der Firma *TENMAX.com*. Teleport Pro ermöglicht

- den Download einer gesamten Web-Site
- das Anfertigen einer exakten Kopie der Web-Site, so dass alle Inhalte innerhalb der lokalen Kopie miteinander verlinkt sind und sich offline genauso verhalten wie beim Online-Surfen
- das Durchsuchen einer Web-Site nach Dateitypen (Executables, DLLs, Archive usw.)
- die Suche nach Schlüsselwörtern innerhalb einer Web-Site.

Abbildung 4.24 zeigt den *Teleport Pro* in Aktion:

11. Download unter *http://www.tenmax.com/teleport/pro/home.htm*.

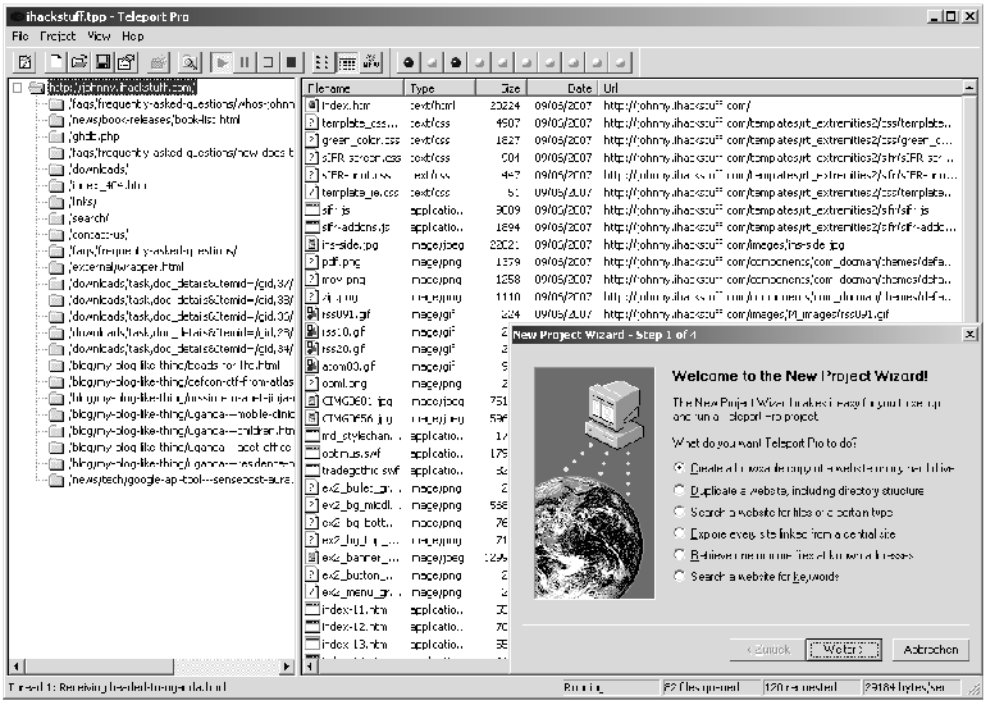


Abbildung 4.24: Spiegelung einer Web-Site mit dem *Teleport Pro*

Die Suche nach bestimmten Dateitypen kann insbesondere auf `.bak`- und `.config`-Dateien ausgeweitet werden, um interne Informationen über Konfigurationseinstellungen u.ä. zu finden.

4.3.2 Wo bist du?

Die einzelnen Stationen, die ein Nachrichtenpaket in einem Netzwerk von ihrem Absender bis zu ihrem Ziel durchläuft, können nicht nur mittels eines Traceroute ermittelt werden. Weiterführende Werkzeuge visualisieren die Netzwerkroute auf einer Weltkarte und zeigen ausführliche Informationen über die einzelnen Stationen eines Paketes an.

McAfee Visual Trace

Die Firma *McAfee.com Corp.* hat ein bekanntes Visualisierungswerkzeug namens *NeoTrace* in ihr Firewall-Produkt integriert und vertreibt dies nun unter der Bezeichnung *McAfee Visual Trace*. Die Vorversion *NeoTrace Pro* kann als Trial-Version in diversen Download-Archiven herunter geladen werden[12].

12. Das Download-Archiv: *http://www.das-download-archiv.de/download_file549.html*.
Vollversion.de: *http://www.vollversion.de/download/neotrace_express_910.html*.
Freenet: *http://download.freenet.de/archiv_n/neotrace_pro_3551.html*.

NeoTrace misst den Netzwerkpfad einer Nachricht von ihrer Quelle bis zum Ziel und stellt die Stationen dieser Route auf einer Weltkarte dar (Abbildungen 4.25).

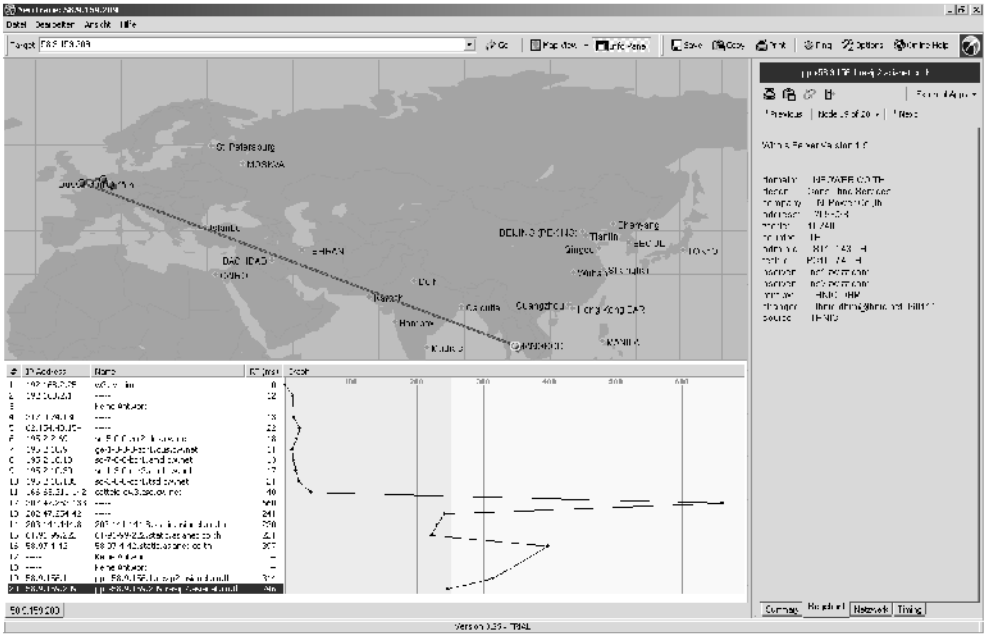


Abbildung 4.25: Visualisierung einer Netzwerkroute mit *NeoTrace*

Zu jeder Station werden die folgenden Informationen angezeigt (Abbildung 4.26):

- Netzwerk-Lokation
  - Servername (z.B. `cattele-gw3.tsd.cw.net`)
  - IP-Adresse (z.B. `166.63.211.142`)
  - Zeit in ms (z.B. `40 ms`)
  - geographische Koordinaten (z.B. `Southwark (51.500N, 0.117W)`)
  - Eigentümer des Netzwerks, dem diese IP-Adresse angehört
- Registrierungsdetails des Eigentümers
  - Firma
  - postalische Adresse
  - Admin-C
  - Tech-C
  - Nameserver
  - E-Mail-Adresse

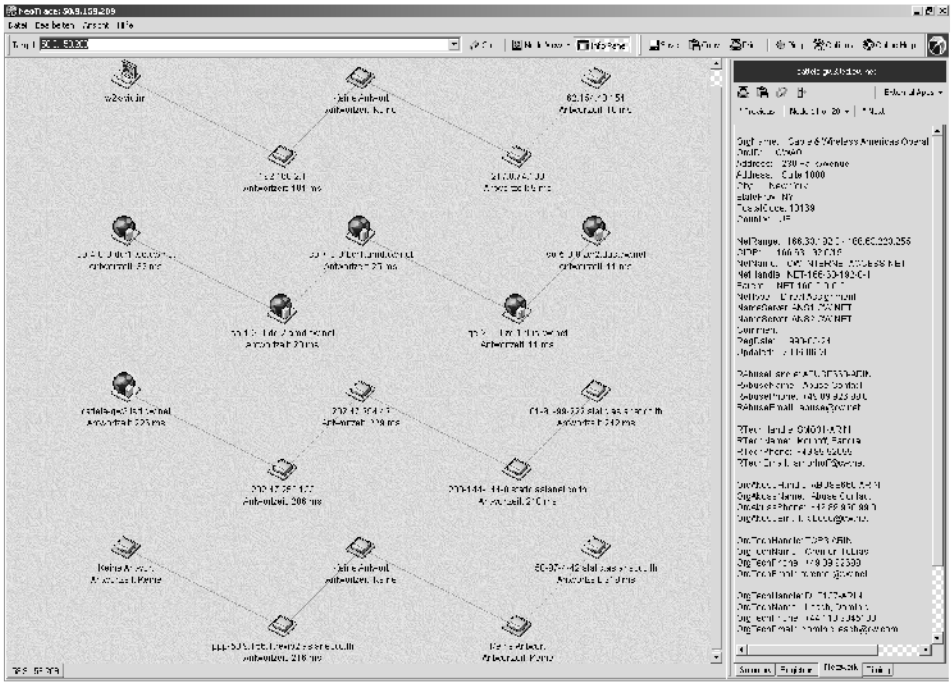


Abbildung 4.26: Stationen auf einer Netzwerkroute

NeoTrace verfolgt IP-Adressen zurück und ordnet Hosts geographisch zu.

Visual Route 2007

Das Werkzeug *Visual Route 2007* von *Visualware* zeigt die Netzwerkroute eines Nachrichtenpaketes auf einer Karte an (Abbildung 4.27) und stellt die üblichen Erkundungswerkzeuge bereit:

- traceroute
- ping
- Reverse DNS
- whois

VisualRoute steht unter *http://www.visualroute.com/* in einer 30-Tage-Testversion zum Download zur Verfügung.

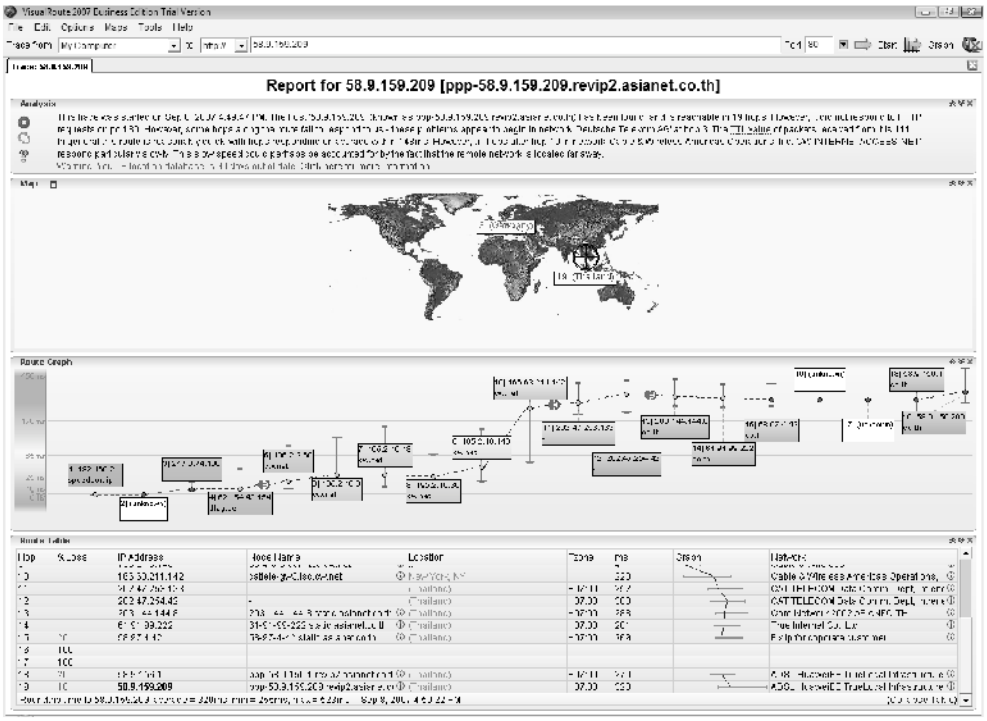


Abbildung 4.27: Visualisierung einer Netzwerkroute mit *VisualRoute 2007*

Re@d Notify

Ein interessantes Tool, um das soziale Netzwerk eines Opfers zu erkunden, ist das Produkt *Re@d Notify* der Firma *ReadNotify.com*. *Re@d Notify* protokolliert den Verlauf einer E-Mail, so dass der Absender Antworten auf die folgenden Fragen erhält:

- Wann wurde die E-Mail geöffnet?
- Wo sind die Empfänger? (Weltkarte und Stadt des Providers)
- Wie lauten die IP-Adressen der Empfänger?
- Welche URLs in der E-Mail wurden aufgerufen?
- Welcher Empfänger brauchte wie lange, um die E-Mail zu lesen?
- Wie oft wurde die E-Mail geöffnet?
- Wann und an wen wurde die E-Mail weitergeleitet?

Re@d Notify erfordert keine Client-Software. Um den Verlauf einer E-Mail beobachten zu können, sendet der Absender die E-Mail nicht an die E-Mail-Adresse des eigentlichen Ziels, sondern an einen Server der Firma *ReadNotify.com*. Beispiel: Anstatt die E-Mail an *max@mustermann.de* zu adressieren, wird die E-Mail an die Adresse *max@mustermann.de.readnotify.com* geschickt. *Re@d Notify* fügt der E-Mail einen eindeutigen Identifier bei und imple-

mentiert einen Mechanismus in dem Inhalt der E-Mail, der beim Öffnen, Weiterleiten und Löschen der E-Mail automatisch ausgelöst wird und eine Mitteilung an die Server von *Re@dNotify.com* schickt. Der Absender kann auf diesen Servern dann in regelmäßigen Abständen das Verlaufsprotokoll dieser E-Mail einsehen. Abbildung 4.28 zeigt ein Beispiel:

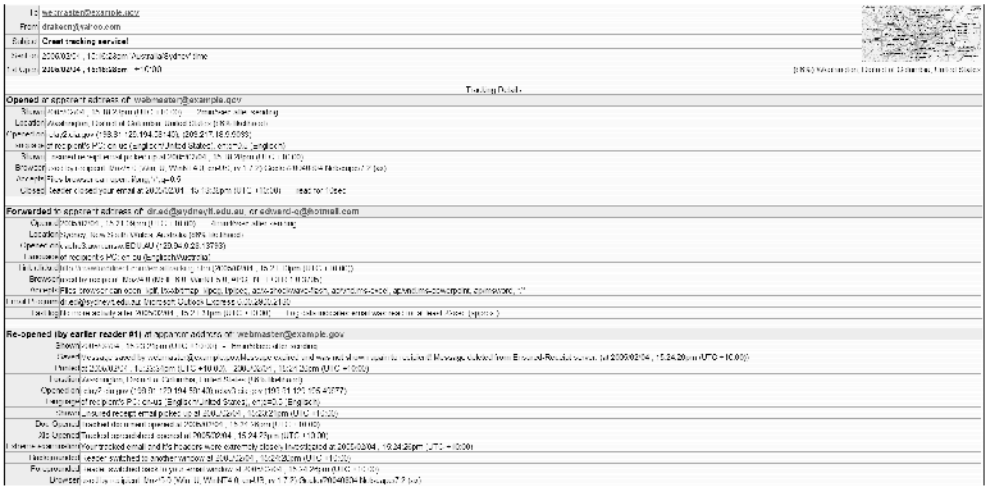


Abbildung 4.28: Verlaufsprotokoll einer E-Mail über *Re@d Notify*

Hacker können mit Hilfe eines solchen Verlaufprotokolls erkennen, wer seine E-Mails an wen weiterleitet, an wen die Empfänger weiterleiten usw. Auf diese Weise kann er sich ein Bild über das soziale Netzwerk seines Opfers verschaffen. Die erhaltenen Informationen setzt er ein, um sein Opfer gezielter ansprechen zu können. Beispielsweise gibt er sich als Freund oder Geschäftspartner seines Opfers aus und sendet diesem eine E-Mail mit einem Trojaner im Anhang zu. Das Opfer wird den Mailanhang wahrscheinlich öffnen, weil ihm der Absender bekannt ist, und er wird sich auf diese Weise unwissentlich eine Schadsoftware installieren.

In Kapitel 4 wurde eine Vielzahl von Reconnaissance-Werkzeugen vorgestellt, die Hackern die Informationsbeschaffung über ihre Opfer vereinfachen. Das nächste Kapitel beschäftigt sich mit der Abtastung des Zielnetzwerks, um mögliche Seitentüren zu finden und schwach abgesicherte Komponenten aufzuspüren.

4.4 Gegenmaßnahmen

Dieses Kapitel hat in aller Ausführlichkeit gezeigt, welche Informationen über Unternehmen, Mitarbeiter, Netzwerke und Systeme im Internet öffentlich für Dritte abrufbar sind. Gleichzeitig wurde verdeutlicht, dass Angreifer den Zugriff auf diese Informationen vollständig anonymisieren können, so dass man ihre Spuren nicht zurückverfolgen kann.

Leider ist gegen beides kein Kraut gewachsen: Einerseits verstehen die an dem Auf- und Ausbau des Internets beteiligten Unternehmen, Organisationen und Personen das *World Wide Web* als Informations- und Kommunikationsplattform und damit als freies Sammel-

becken für Informationen aller Art. Andererseits erlauben die derzeit eingesetzten Standard-Protokolle keinen ausreichenden Schutz, um Angreifer von einem erfolgreichen Einbruch bis zu ihren anfänglichen Recherchen zurückverfolgen zu können.

Aus diesem Grund besteht eine wirksame Schutzmaßnahme darin, sich Bewusstsein darüber zu verschaffen, welche Informationen im Internet veröffentlicht werden und wie ein Angreifer diese Informationen gezielt einsetzen kann.

Seien Sie sich darüber im Klaren, welche Informationen über Sie im Internet abrufbar sind und wie diese Informationen gegen Sie eingesetzt werden können!

Ihr Name und Ihre E-Mail-Adresse taucht in zahlreichen Ergebnissen von Suchmaschinen auf: in Newsgroups, in sozialen Netzwerken wie *www.stayfriends.de*, in Job-Plattformen wie *www.monster.de* und *www.xing.com*. Wenn Sie eine Homepage betreiben, wird Ihr Name und Ihre E-Mail-Adresse in öffentlichen Nameservern und in *whois*-Datenbanken verwaltet. In einigen Fällen sind Ihre persönlichen Daten über eine Suchmaschinen-Abfrage zwar nicht direkt abrufbar, können aber ohne weiteres über Umwege ermittelt werden[13]. Zudem kann jeder Internet-Nutzer Satellitenfotos über Ihr Haus, Ihre Wohnung und Ihre Nachbarschaft einsehen.

Wenn Sie sich darüber bewusst sind, welche Informationen im Internet über Sie veröffentlicht sind, sollten Sie den Umfang dieser persönlichen Angaben empfindlich einschränken! Müssen Sie Ihren vollständigen Lebenslauf auf *Xing* oder *LinkedIn* veröffentlichen? Müssen Sie dort unbedingt Ihre Telefonnummern und E-Mail-Adressen hinterlegen? Benötigen Sie unbedingt einen *PayPal*-Account? Müssen Sie anderen Menschen Ihre Hobbies auf Ihrer persönlichen Web-Site mitteilen? Warum geben Sie Ihr Geburtsdatum auf *StayFriends* an? Sind Fotos von Ihnen im Internet abrufbar? Was ist auf diesen Fotos aus Ihrer Umgebung alles zu sehen?

Bereinigen Sie die Daten, die andere Unternehmen und Plattformen über Sie speichern! Löschen Sie persönliche Anmeldekonten, die Sie nicht zwingend benötigen! Seien Sie sich darüber im Klaren, dass Angreifer in Shops und Zahlungssysteme einbrechen und an Ihre Daten gelangen können, obwohl Ihnen von dem verantwortlichen Unternehmen zugesichert wurde, dass Ihre Daten sicher gespeichert werden.

Stellen Sie einen Sicherheitsbeauftragten ein oder beauftragen Sie einen Ethical Hacker!

Jedes deutsche Unternehmen hat laut Bundesdatenschutzgesetz (BDSG) ab einer gewissen Größe einen Datenschutzbeauftragten einzustellen[14]. Die Aufgabe des Datenschützers ist die Überwachung der Datenverarbeitungsprogramme sowie die Sensibilisierung des datenverarbeitenden Personals mit dem Thema „Datenschutz".

Warum aber gibt es kein „Bundessicherheitsgesetz für Informationstechnologie"? Warum sind Unternehmen und Behörden nicht verpflichtet, einen Sicherheitsbeauftragten einzustellen?

13. Beispielsweise über den Namen Ihrer Domain oder über die IP-Adresse des hostenden Web-Servers.
14. Alle öffentliche Stellen (wie beispielsweise Behörden) sowie nicht-öffentliche Stellen (wie Firmen, Vereine und Kanzleien), bei denen mehr als 10 Personen einen Zugriff auf elektronisch gespeicherte, personenbezogene Daten haben, müssen per Gesetz einen Datenschutzbeauftragten bestellen. Werden personenbezogene Daten nicht-elektronisch verwaltet, gilt diese Auflage für Stellen mit mehr als 20 Personen mit Zugriff auf diese Daten.

Solange sich der Gesetzgeber mit der Zwangsinstallation von „Bundestrojanern“ verirrt, anstatt die Sicherheit von Unternehmensnetzwerken und IT-Systemen durch die Beauftragung von ausgewiesenen Sicherheitsspezialisten wirksam durchzusetzen, sind allein Sie für Ihre Sicherheit verantwortlich! Allein Sie sind dafür zuständig, die über Ihre Kunden gespeicherten Daten vor Einbrüchen zu schützen!

Die meisten Unternehmen verfügen nicht über das erforderliche Security-Know-How und sind daher auf Sicherheitsexperten angewiesen. Stellen Sie daher einen Sicherheitsbeauftragten ein! Dessen Aufgabe ist, die Absicherung Ihrer Netzwerke und IT-Systeme sicherzustellen. Insbesondere hat ein solcher Sicherheitsbeauftragter zu überprüfen, welche Informationen Ihr Unternehmen veröffentlicht, und wie sensibel diese Informationen in Bezug auf Ihre IT-Sicherheit ist. Einige Beispiele:

- Stellenanzeigen dürfen keine Details über die eingesetzte Hard- und Software umfassen, insbesondere keine Herstellerbezeichnungen oder Versionsnummern.
- E-Mail-Adressen, die veröffentlicht werden müssen, sollten keine personenbezogene Bezeichnung enthalten, sondern sich auf die jeweilige Aufgabe beziehen. Der technische Ansprechpartner einer Domain (Tech-C) sollte bei der Registrierung beispielsweise die E-Mail-Adresse *tech-c@meine-firma.de* anstatt *max.mustermann@meine-firma.de* verwenden.
- URLs, die in einer Web-Anwendung verwendet werden, sollten keine Hinweise auf die zugrunde liegende Verzeichnisstruktur auf dem Web-Server enthalten. Der URL *https://portal.meine-firma.de/login.aspx?redirect=/contractor/welcome.aspx* könnte vermuten lassen, dass das Verzeichnis `/contractor` alle Skripte einer bestimmten Rolle enthält („Kunde“). Vielleicht gibt es andere Rollen? Beispielsweise `/supplier`, `/reseller` oder `/employee`. Und im schlimmsten Fall kann ein Angreifer über solche „Hinweise“ in die Bereiche einer Web-Applikation vorstoßen, die eigentlich besonders geschützt sein sollten ...
- Fahrlässig entsorgter Papiermüll kann wertvolle Hinweise über aktuelle Produktentwicklungen, über Forschungsergebnisse und über die Mitarbeiter einer Organisation liefern (*Dumpster Diving*).

Insbesondere sollte ein Sicherheitsbeauftragter die Spuren untersuchen, die die Mitarbeiter des Unternehmens im Internet hinterlassen. Was diskutieren die eigenen Entwickler in öffentlichen Newsgroups, wenn sie ein technisches Problem nicht lösen können? Geben sie dabei sensible Informationen über die im Unternehmen eingesetzte Hard- und Software preis? Posten sie Auszüge aus internen Log-Files? Tauschen sie E-Mail-Adressen oder Telefonnummern aus?

Ist Ihr Unternehmen zu klein, um eine Stelle für einen Sicherheitsbeauftragten einzurichten, so beauftragen Sie in regelmäßigen Abständen einen externen Sicherheitsspezialisten mit der punktuellen Bearbeitung der o.a. Aufgaben. Das Budget für einen solchen Beratungsauftrag steht in keinem Verhältnis zu dem finanziellen oder Image-Schaden, der im Falle eines Einbruchs entsteht! Ein Ethical Hacker jedoch kann bereits im Vorfeld die Schwachstellen Ihrer Infrastruktur und Ihrer Systeme analysieren und präventiv geeignete Gegenmaßnahmen einrichten. Zudem ist ein solcher Sicherheitsspezialist geeignet, Ihre Mitarbeiter zu schulen und auf den sensiblen Umgang mit Daten und Information zu sensibilisieren.

Geben Sie nur preis, was unbedingt erforderlich ist, und verschleiern Sie sensible Informationen!

Sind Sie der Netzwerk- oder Systemadministrator eines Unternehmens, dann sorgen Sie dafür, dass nur solche Rechner an das öffentliche Internet angebunden werden, die zwingend für die Informationsbereitstellung oder externe Prozessautomatisierung erforderlich sind! Deinstallieren Sie auf diesen Systemen alle nicht zwingend benötigten Dienste! Hinterfragen Sie hartnäckig bei der internen Entwicklungsabteilung, welche Dienste wofür benötigt werden!

Veranlassen Sie die Löschung Ihrer alten Web-Sites auf *archive.org*! Sperren Sie Ihre Domänen gegen „What's that site running?"-Abfragen auf *NetCraft*! Überprüfen Sie die Satellitenfotos Ihres Firmengeländes und veranlassen Sie, dass die Anzeige Ihrer Bereiche „geschwärzt" wird! Führen Sie Reviews Ihrer Web-Sites durch und stellen Sie sicher, dass die HTML-Seiten keine Kommentare, E-Mail-Adressen, Namen oder sonstige interne Informationen enthalten.

Schränken Sie den Zugriff auf Ressourcen empfindlich ein!

Nicht jeder Mitarbeiter muss auf jede Netzwerkressource zugreifen können. Nicht jeder Mitarbeiter muss jedes Dokument aufrufen können. Führen Sie strikte Zugriffsrichtlinien ein! Mittlerweile ist jedes fünfte Unternehmen in Deutschland von dem Problem der Wirtschaftsspionage betroffen! Mitarbeiter geben unbedacht Dokumente an Dritte heraus oder verkaufen diese sogar vorsätzlich gegen Geld! Analysieren Sie, wer welche Informationen einsehen darf und wer diese Informationen ändern darf. Installieren Sie diese Zugriffsberechtigungen in Ihren IT-Systemen! Führen Sie einen Genehmigungsprozess ein, der die explizite Freigabe eines angeforderten Zugriffs für einen Mitarbeiter durch seinen Vorgesetzten erzwingt. Sorgen Sie dafür, dass die Benutzerkonten gekündigter Mitarbeiter umgehend gelöscht werden.

Sensibilisieren Sie Ihre Mitarbeiter!

Die Mitarbeiter eines Unternehmens sind beliebte Angriffsziele. Daher gelten für Mitarbeiter die gleichen Regeln wie für Privatanwender. Schlagen Sie nochmals die in Kapitel 2 beschriebenen Gegenmaßnahmen gegen Viren, Würmer und Trojaner nach!

Schulen Sie Ihre Mitarbeiter und sensibilisieren Sie sie auf die Vertraulichkeit von Informationen! Lassen Sie Ihre Mitarbeiter stets hinterfragen, wer eine Auskunft benötigt und wofür! Schützen Sie Ihre Mitarbeiter somit vor Social Engineers: erst hinterfragen, dann helfen.