Über dieses Buch

Wer sollte dieses Buch lesen?

Das Buch richtet sich an angehende Netzwerkanalysten und bietet einen idealen Einstieg in das Thema, wenn Sie sich für die Analyse des Datenverkehrs interessieren, um zu verstehen, wie ein bestimmtes Programm arbeitet, wenn Sie die zu niedrige Geschwindigkeit des Netzwerks beheben möchten oder feststellen wollen, ob ein Computer mit Schadsoftware verseucht ist.

Wenn Sie die Aufzeichnung und Analyse des Datenverkehrs mittels Wireshark beherrschen, ermöglicht Ihnen das, wirklich zu begreifen, wie TCP/IP-Netzwerke funktionieren. Wireshark ist das weltweit verbreitetste Netzwerkanalysewerkzeug. Die Zeit, die Sie zum Vervollkommnen Ihrer Kenntnisse aufwenden, wird sich bei der Lektüre von technischen Dokumenten, Werbebroschüren, Sicherheitsanweisungen usw. mehr als bezahlt machen.

Das Buch ist ebenfalls dazu geeignet, die hier vermittelten Fähigkeiten bereits tätiger Netzwerkanalysten zu trainieren.

Im Wesentlichen wendet sich das Buch an alle, die genau wissen möchten, was in ihrem Netzwerk vor sich geht.

Welche Vorkenntnisse sind erforderlich?

Um sich näher mit diesem Buch (oder der Netzwerkanalyse im Allgemeinen) zu befassen, sollten Sie solide Kenntnisse der fundamentalen Konzepte von Netzwerken und den Grundlagen von TCP/IP mitbringen. Beispielsweise sollten Ihnen die Aufgaben eines Switches, eines Routers und einer Firewall bekannt sein. Die Konzepte von Ethernet- und einfachen drahtlosen Netzwerken sollten Ihnen ebenso vertraut sein wie die Adressierung in IP-Netzwerken.

An einigen Stellen im Buch müssen Sie auf die Kommandozeile zugreifen, etwa um den Pfad für das Verzeichnis einer Applikation anzugeben oder einfache Kommandozeilenprogramme wie `ipconfig`, `ifconfig`, `ping` oder `tracert`/`traceroute` auszuführen. Falls Ihnen diese Werkzeuge nicht geläufig sind: Im Internet finden Sie ein reichhaltiges Angebot an Quellen, denen Sie entnehmen können, wie diese Programme auf den verschiedenen Plattformen funktionieren.

Am Ende des Buchs (Anhang C) werden viele der im Buch erwähnten Begriffe und Technologien in einem Glossar erläutert. Wenn Ihnen beispielsweise der Begriff WinPcap bei dessen Besprechung im Buch nichts sagt, schlagen Sie ihn einfach im Glossar nach.

Welche Wireshark-Versionen werden behandelt?

Im Buch werden verschiedene Wireshark-Versionen (2.x.x) verwendet. Falls Sie noch immer Wireshark 1.x-Versionen nutzen, sollten Sie Ihre Version aktualisieren. Wireshark 2 bietet gegenüber älteren Versionen eine Vielzahl von Vorteilen, wie z.B. eine eigene Installation für Macintosh-Benutzer, die intelligente Scrollleiste, erheblich verbesserte Grafik, einen Indikator für zusammengehörige Pakete und vieles mehr.

Wo sind die im Buch verwendeten Mitschnittdateien erhältlich?

Sie sollten sich baldmöglichst unter `http://www.wiresharkbook.com` die im Buch verwendeten Mittschnittdateien und weitere, das Buch ergänzende Dateien herunterladen. Folgen Sie in der Kategorie BOOK SUPPLEMENTS dem Link WIRESHARK 101 ESSENTIAL SKILLS – 2ND EDITION und laden Sie sich den vollständigen Satz der die 2. Auflage des Buchs begleitenden Dokumente herunter.

Die begleitenden Dokumente sind im *.zip*-Format gespeichert. Erstellen Sie einen Ordner auf Ihrem lokalen System und entpacken Sie die Dateien.

Falls Sie zum Buch oder der Website Fragen haben, senden Sie diese (in englischer Sprache) an `info@wiresharkbook.com`.

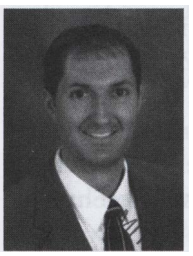
Wo gibt es weitere Informationen über Wireshark und die Untersuchung von Netzwerken?

Laden Sie sich Lauras kostenlosen vierteiligen Einführungskurs in Wireshark im All-Access-Pass-Portal herunter oder schauen Sie ihn online an (`http://www.lcuportal2.com`).

Weitere Information zum All Access Pass und andere Schulungsmöglichkeiten finden Sie unter `http://www.chappellU.com`.

Vorwort von Gerald Combs

Was geht da eigentlich im Netzwerk vor?



Das ist eine dieser so einfachen Fragen, auf die es nur sehr komplexe Antworten gibt. Die Frage ist für viele Leute von großer Bedeutung, insbesondere, wenn der Lebensunterhalt von Netzwerkproblemen betroffen ist.

Als ich das erste Mal jemanden bei einer Netzwerkanalyse beobachtete, wurde dazu ein Oszilloskop verwendet. Das war in den 1980ern, und Werkzeuge zur Netzwerkanalyse waren Mangelware.

In den Räumlichkeiten unserer Universität stand uns einzig und allein ein Oszilloskop zur Verfügung. Dieses Gerät zeigte uns die etwa rechteckförmigen, auf und ab hüpfenden elektrischen Signale an, aus denen die Ethernet-Frames bestanden, die kreuz und quer durch unser Netzwerk flogen. Es war zwar nur ein sehr begrenzter und beschränkter Einblick ins Netzwerk, aber dennoch faszinierend.

Einige Jahre später, an einer anderen Universität, musste ich mich im Netzwerk der IT-Abteilung auf Fehlersuche begeben. Inzwischen besaßen wir bessere Werkzeuge wie etwa `tcpdump` und einen Sniffer, der uns statt elektrischer Signale Pakete anzeigte. Dessen ungeachtet war es zunächst etwas beängstigend, denn unser Netzwerk bestand aus einem bunt zusammengewürfelten Haufen unterschiedlicher Technologien: Ethernet, FDDI, Token Ring, IPX, DECnet, IP, AppleTalk usw.

Anfangs ergab vieles keinen Sinn, aber es war noch immer faszinierend. Die Inhalte der einzelnen, durch das Netzwerk gesendeten Nachrichten waren erkennbar, und gleichzeitig konnte man all die schlauen Verfahren bei der Arbeit beobachten, die sich die Leute ausgedacht haben, damit Computer miteinander kommunizieren können. Diese Faszination ist zu einer Leidenschaft geworden, die bis heute anhält.

Einige Zeit später musste ich bei einem Internetanbieter die Frage »Was geht da eigentlich im Netzwerk vor?« beantworten. Die feinen Werkzeuge, an deren Gebrauch ich mich gewöhnt hatte, standen dort nicht zur Verfügung und ich hatte das Gefühl, blind zu sein.

Ich begann damit, einen Protokoll-Analyzer zu schreiben, und veröffentlichte diesen als quelloffenes Programm. Dank der Beiträge eines erstaunlich begabten Teams von Entwicklern und Anwendern wurde er zum weltweit beliebtesten Programm dieser Art.

Ich bin der Ansicht, dass jedermann über ein grundlegendes Verständnis von Computernetzwerken verfügen sollte. Sie sind ein unerlässlicher Bestandteil der heutigen Gesellschaft, und daher ist es wichtig, ihre Funktionsweise zu kennen.

Ebenso wichtig ist die Erkenntnis, dass Wireshark Ihnen dieses Wissen nicht einfach so vermitteln kann – das vermag kein Werkzeug zu leisten. Erfreulicherweise ist Wireshark von einem lebhaften Umfeld umgeben: vom Entwicklerteam über die Gemeinschaft der Anwender, Firmen, die mit Wireshark im Zusammenhang stehende Produkte und Dienste anbieten (wie mein Arbeitgeber), bis hin zu Lehrenden wie Laura. In diesem bemerkenswerten Ökosystem sammeln sich Menschen, die nicht nur brennend daran interessiert sind, Netzwerkprotokolle zu analysieren, sondern ebenso sehr daran, einander zu helfen. Es ist eine Ehre, ein Teil davon zu sein.

Auf den ersten Blick ergeben Netzwerke nur wenig Sinn (so jedenfalls erging es mir), aber das ist schon in Ordnung. Laura hilft Ihnen dabei zu verstehen, wie diese funktionieren (und auch, warum sie oft eben nicht funktionieren). Sie vermittelt Ihnen die nötigen Kenntnisse, um Wireshark optimal auszureizen.

Und was geht in *Ihrem* Netzwerk vor?

Gerald Combs
Urheber von Wireshark® (vormals *Ethereal*)