Einführung

Bei ihrer Einführung stand die Technik, die es Geräten erlaubte, sich zu einem Netzwerk zu verbinden, nur großen Unternehmen und Regierungen zur Verfügung. Heutzutage tragen die meisten Menschen ein voll vernetztes Gerät mit sich herum und mit dem Aufkommen des Internets der Dinge (Internet of Things, IoT) können Sie Ihren Kühlschrank und die heimische Alarmanlage an diese vernetzte Welt anbinden. Die Sicherheit dieser vernetzten Geräte wird daher immer wichtiger. Möglicherweise kümmert es Sie nicht sonderlich, wenn jemand weiß, welchen Joghurt Sie kaufen, doch wenn Ihr Smartphone über das gleiche Netzwerk wie Ihr Kühlschrank kompromittiert wird, könnten all Ihre persönlichen und finanziellen Daten in die Hände böser Hacker gelangen.

Dieses Buch heißt *Netzwerkprotokolle hacken*, weil Sie sich in die Gedankenwelt eines Angreifers hineinversetzen müssen, um Sicherheitslücken bei einem vernetzten Gerät aufzuspüren. Netzwerkprotokolle kommunizieren mit anderen Geräten über ein (öffentliches) Netzwerk. Sie durchlaufen häufig nicht die Prüfungen wie die anderen Komponenten des Gerätes und sind daher ein nahe liegendes Angriffsziel.

Warum sollten Sie dieses Buch lesen?

Viele Bücher behandeln das Erfassen (Capturing) von Netzwerkverkehr für Diagnosezwecke und eine grundlegende Netzwerkanalyse, kümmern sich aber nicht um die Sicherheitsaspekte der abgefangenen Protokolle. Im Gegensatz dazu konzentriert sich dieses Buch darauf, Protokolle auf ihre Sicherheitslücken hin zu analysieren.

Dieses Buch richtet sich an alle, die Netzwerkprotokolle analysieren und angreifen wollen, aber nicht wissen, wo sie anfangen sollen. Die Kapitel vermitteln Ihnen Techniken zum Erfassen von Netzwerkverkehr, zur Analyse der Protokolle und zur Aufdeckung und dem Exploit von Sicherheitslücken. Das Buch bietet Hintergrundinformationen zur Vernetzung und zur Sicherheit von Netzwerken, aber auch praktische Beispiel für zu analysierende Protokolle.

Ob Sie nun Netzwerkprotokolle angreifen wollen, um Sicherheitslücken an den Hersteller einer Anwendung zu melden, oder ob Sie nur wissen wollen, wie Ihr neuestes IoT-Gerät kommuniziert, Sie werden verschiedene interessante Themen entdecken.

Was finden Sie in diesem Buch?

Dieses Buch umfasst eine Mischung aus theoretischen und praktischen Kapiteln. Für die praktischen Kapitel habe ich eine Netzwerkbibliothek namens Canape Core entwickelt und zur Verfügung gestellt, mit der Sie eigene Tools zur Protokollanalyse und für Exploits schreiben können. Ich stelle auch eine beispielhafte Netzwerkanwendung namens *SuperFunkyChat* bereit, die ein benutzerdefiniertes Chat-Protokoll implementiert. Während Sie der Diskussion in den Kapiteln folgen, können Sie die Beispielanwendung nutzen, um die Protokollanalyse zu erlernen und die Beispielprotokolle anzugreifen. Hier eine kurze Beschreibung der jeweiligen Kapitel:

- **Kapitel 1: Netzwerk-Grundlagen**
  Dieses Kapitel erläutert die Grundlagen der Vernetzung von Computern, wobei es sich auf TCP/IP konzentriert, das die Basis anwendungsspezifischer Netzwerkprotokolle bildet. Die nachfolgenden Kapitel gehen davon aus, dass Sie die Grundlagen der Vernetzung beherrschen. Dieses Kapitel stellt auch den Ansatz vor, den ich zur Modellierung von Anwendungsprotokollen verwende. Dieses Modell teilt das Anwendungsprotokoll in flexible Schichten auf und abstrahiert komplexe technische Details. Auf diese Weise können wir uns auf bestimmte Teile des zu analysierenden Protokolls konzentrieren.
- **Kapitel 2: Capturing von Anwendungsverkehr**
  Dieses Kapitel führt in die Konzepte des passiven und aktiven Capturings von Netzwerkverkehr ein. Es ist das erste Kapitel, das die Canape-Core-Bibliotheken für praktische Aufgaben nutzt.
- **Kapitel 3: Strukturen von Netzwerk-Protokollen**
  Dieses Kapitel erläutert interne Strukturen, die bei Netzwerkprotokollen üblich sind, etwa die Repräsentation von Zahlen oder lesbarem Text. Bei der Analyse von Netzwerkverkehr können Sie dieses Wissen nutzen, um gängige Strukturen schnell zu identifizieren, und so die Analyse beschleunigen.
- **Kapitel 4: Fortgeschrittenes Capturing von Anwendungsverkehr**
  Dieses Kapitel untersucht eine Reihe fortgeschrittener Capturing-Techniken, die die Beispiele aus Kapitel 2 ergänzen. Zu diesen Techniken gehören etwa die »Network Address Translation« zur Umleitung von Verkehr und das Spoofing von ARP.

- **Kapitel 5: Analyse auf der Datenleitung**
  Dieses Kapitel stellt Methoden zur Analyse des aufgezeichneten Netzwerkverkehrs vor und nutzt dabei die in Kapitel 2 erläuterten passiven und aktiven Techniken. In diesem Kapitel lassen wir die *SuperFunkyChat*-Anwendung erstmals Beispielverkehr erzeugen.
- **Kapitel 6: Reverse Engineering einer Anwendung**
  In diesem Kapitel werden Techniken zum Reverse Engineering von Netzwerkprogrammen erläutert. Reverse Engineering erlaubt die Analyse eines Protokolls, ohne dass Sie dazu Beispielverkehr benötigen. Diese Methoden helfen auch dabei, die verwendete Verschlüsselungs- oder Verschleierungstechnik zu identifizieren, sodass sich der aufgezeichnete Verkehr besser analysieren lässt.
- **Kapitel 7: Sicherheit von Netzwerkprotokollen**
  Dieses Kapitel versorgt Sie mit Hintergrundinformationen zu Techniken und kryptografischen Algorithmen, die zur Absicherung von Netzwerkprotokollen verwendet werden. Der Schutz der über öffentliche Netzwerke laufenden Daten vor Enthüllung oder Veränderung ist für die Sicherheit des Netzwerkprotokolls von höchster Bedeutung.
- **Kapitel 8: Implementierung des Netzwerkprotokolls**
  Dieses Kapitel erläutert Techniken zur Implementierung des Anwendungsprotokolls in selbst entwickeltem Code. Auf diese Weise können Sie das Verhalten des Protokolls testen und Sicherheitslücken aufspüren.
- **Kapitel 9: Die Hauptursachen für Sicherheitslücken**
  Dieses Kapitel zeigt gängige Sicherheitslücken auf, denen Sie bei einem Netzwerkprotokoll begegnen werden. Wenn Sie die Hauptursachen für Sicherheitslücken kennen, können Sie diese während der Analyse einfacher identifizieren.
- **Kapitel 10: Sicherheitslücken aufspüren und ausnutzen**
  Dieses Kapitel beschreibt den Prozess der Aufspürens von Sicherheitslücken anhand der Hauptursachen aus Kapitel 9 und demonstriert eine Reihe von Möglichkeiten, wie Sie das ausnutzen können. Dazu entwickeln wir eigenen Shell-Code und umgehen möglicherweise getroffene Gegenmaßnahmen durch »Return-Oriented Programming«.
- **Anhang A: Toolkit für die Netzwerkprotokoll-Analyse**
  In diesem Anhang finden Sie die Beschreibung einiger der Tools, die ich zur Protokollanalyse häufig einsetze. Viele dieser Tools werden auch im Text angesprochen.

Wie Sie dieses Buch nutzen

Wenn Sie Ihr Grundlagenwissen in Sachen Vernetzung auffrischen wollen, lesen Sie zuerst Kapitel 1. Wenn Sie mit den Grundlagen vertraut sind, können Sie mit den Kapiteln 2 und 3 weitermachen sowie in Kapitel 5 praktische Erfahrungen mit dem Aufzeichnen von Netzwerkverkehr und dem Analyseprozess sammeln.

Mit dem Wissen um die Grundlagen des Erfassens und der Analyse können Sie mit den Kapiteln 7 bis 10 weitermachen. Darin finden Sie praxisorientierte Hinweise, wie man Sicherheitslücken dieser Protokolle aufspürt und ausnutzt. Die Kapitel 4 und 6 enthalten weiterführende Informationen zu zusätzlichen Capturing-Techniken und dem Reverse Engineering von Anwendungen. Wenn Sie wollen, können Sie diese lesen, nachdem Sie die anderen Kapitel durchgelesen haben.

Für die praktischen Beispiele müssen Sie .NET Core (*https://www.microsoft.com/net/core/*) installieren. Das ist die plattformübergreifende Version der .NET-Runtime von Microsoft, die unter Windows, Linux und macOS läuft. Sie können Versionen von Canape Core über *https://github.com/tyranid/CANAPE.Core/releases/* und *SuperFunkyChat* über *https://github.com/tyranid/ExampleChatApplication/releases/* herunterladen. Beide nutzen .NET Core als Runtime. Links zu diesen Websites finden Sie in den Ressourcen zu diesem Buch auf *https://www.dpunkt.de/netze_hacken*.

Um die Canape-Core-Beispielskripten auszuführen, müssen Sie *CANAPE.Cli* nutzen, das im Releasepaket enthalten ist, das Sie aus dem Github-Repository zu Canape Core heruntergeladen haben. Führen Sie das Skript mit der folgenden Kommandozeile aus und ersetzen Sie dabei `script.csx` durch den Namen des Skripts, das Sie ausführen wollen.

```
dotnet exec CANAPE.Cli.dll script.csx
```

Alle Beispiel-Listings aus den praktischen Kapiteln sowie die Paket-Captures (erfassten Pakete) stehen auf der Webseite zu diesem Buch unter *https://www.dpunkt.de/netze_hacken* zur Verfügung. Bevor Sie anfangen, sollten Sie sich diese Beispiele herunterladen, damit Sie den praktischen Kapiteln folgen können, ohne eine große Menge Quellcode von Hand eingeben zu müssen.

Kontakt

Ich bin immer an positivem wie negativem Feedback zu meiner Arbeit interessiert und dieses Buch bildet da keine Ausnahme. Sie erreichen mich per E-Mail unter *attacking.network.protocols@gmail.com*.

Sie können mir auch auf Twitter unter *@tiraniddo* folgen oder meinen Blog unter *https://tyranidslair.blogspot.com/* abonnieren, wo ich über meine neuesten Forschungen zur IT-Sicherheit schreibe.