Xpert.press

Bastian Ballmann

Network Hacks

Springer Vieweg

Xpert.press

Die Reihe **Xpert.press** vermittelt Professionals in den Bereichen Softwareentwicklung, Internettechnologie und IT-Management aktuell und kompetent relevantes Fachwissen über Technologien und Produkte zur Entwicklung und Anwendung moderner Informationstechnologien.

Bastian Ballmann

Network Hacks – Intensivkurs

Angriff und Verteidigung mit Python

Springer Vieweg

Bastian Ballmann

ISSN 1439-5428
ISBN 978-3-642-24304-2 978-3-642-24305-9 (eBook)
DOI 10.1007/978-3-642-24305-9

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier

Springer Vieweg ist eine Marke von Springer DE. Springer DE ist Teil der Fachverlagsgruppe Springer Science+Business Media
www.springer-vieweg.de

Für Datenreisende, Wissenshungrige und neugierige, netzwerkbegeisterte Lebewesen, die Spaß daran haben, den Dingen auf den Grund zu gehen.

Geleitwort

Erklärt dieses Buch nicht nur wie man in Systeme einbricht? Ist das nicht illegal?

Der Autor möchte beide Fragen verneinen. Wissen per se ist nicht illegal, sondern höchstens die Handlungen, die man mit diesem Wissen begeht.

Sie als Admin, Programmierer, IT-Beauftrager oder interessierter User können sich nicht wirkungsvoll vor einem Angreifer schützen, wenn Sie dessen Methoden nicht kennen! Sie können die Wirksamkeit Ihrer Firewalls, Intrusion-Detection-Systeme und sonstiger Sicherheitssoftware nicht überprüfen und beurteilen, wenn Sie nicht in der Lage sind Ihr Netz aus der Sicht eines Angreifer zu sehen. Sie können nicht die Gefahren gegen die Aufwände möglicher Schutzvorkehrungen abwägen, wenn Sie die Auswirkungen eines Angriffs nicht oder nur unzureichend kennen. Deswegen ist es wichtig zu verstehen wie Angriffe auf Computernetzwerke funktionieren.

Eine Auswahl an Angriffsmöglichkeiten wird Ihnen im Buch anhand von kurzen, praktischen Code-Beispielen erklärt, die Ihnen wirkungsvolle Demonstrationsmöglichkeiten an die Hand geben, mit denen Sie IT-Entscheider davon überzeugen können, dass es sinnvoll wäre etwas mehr Budget für Sicherheit zu investieren. Sie sollten am Ende des Buches in Lage sein diese Beispiele nicht nur zu verstehen, sondern auch an Ihre eigenen Bedürfnisse anzupassen.

Natürlich lehrt dieses Buch ebenfalls den bösen Buben, wie er eigene Angriffstools schreiben kann. IT-Security ist ein zweischneidiges Schwert und ein ständiger Wettkampf, der von der absichernden Seite niemals gewonnen werden kann, wenn sie sich selbst ihres Wissens beraubt!

Einleitung

Für wen ist dieses Buch?

Dieses Buch richtet sich an interessierte Python-Programmierer, die ihr Grundwissen mit einer gehörigen Portion Netzwerk-Code erweitern möchten, und an versierte Administratoren, die aktiv die Sicherheit ihrer Systeme und Netze überprüfen wollen. Der Inhalt dürfte ebenfalls White-, Gray- und BlackHat-Hacker interessieren, die wie ich Python als ihre bevorzugte Programmiersprache für kleine und große Hacks und Exploits entdeckt haben. Interessierte Computerbenutzer, die selber einmal lernen möchten ihr Netzwerk mit den Augen eines Angreifers zu sehen, werden genauso auf ihre Kosten kommen.

Es werden weder Kenntnisse in Python noch in Netzwerktechnologie vorausgesetzt. Das Wissen, das für dieses Buch benötigt wird, wird in den Kap. 2 und 3 vermittelt. Leser, die schon über ausreichende Python- und Netzwerk-Kenntnisse verfügen und eine bevorzugte Python-IDE ihr Eigen nennen, können sofort zu Kap. 5 springen und sich umgehend in die Hacking-Techniken stürzen.

Sie sollten das erlernte Wissen selbstverständlich nur auf ihre eigenen Systeme und Netzwerke bzw. nur mit ausdrücklicher Erlaubnis der Betreiber anwenden, da Sie ansonsten wahrscheinlich eine strafbare Handlung begehen!

Der Umfang dieses Buches erlaubt es nicht, die behandelten Themengebiete in voller Tiefe zu ergründen. Es will Basiswissen auf den wichtigsten netzwerkspezifischen Gebieten aufbauen. Falls Sie sich anschließend mit einem oder mehreren Bereichen eingehender befassen wollen, sollten Sie sich für diese Bereiche extra Fachliteratur anschaffen.

Wie ist dieses Buch aufgebaut?

Die verschiedenen Hacks sind nach Netzwerkprotokollen gruppiert und innerhalb der Kapitel nach Schwierigkeitsgrad geordnet. Abgesehen von den beiden Grund-

lagenkapiteln über Netzwerke (Kap. 2) und Python (Kap. 3) können die Kapitel in beliebiger Reihenfolge gelesen werden.

Die Codebeispiele sind ungekürzt abgedruckt, damit sie komplett abgetippt werden können. Sollte es Ihnen zu umständlich sein die Code-Beispiele abzutippen, finden Sie sie auch als Download auf der Seite http://datenterrorist.de/pythonnetwork-hacks/all.zip.

Am Ende eines jeden Kapitels werden Tools vorgestellt, die in Python programmiert sind und das jeweilige Protokoll angreifen, das in dem Kapitel behandelt wurde. Mit dem fundierten Vorwissen sollte es Ihnen dann nicht allzu schwer fallen, die Source Codes dieser Programme zu lesen und zu verstehen.

Die wichtigsten Sicherheitsprinzipien

Die wichtigsten Prinzipien beim Aufbau eines sicheren Netzes sind nach Auffassung des Autors:

1. Sicherheitslösungen sollten simpel sein. Firewall-Regeln, die niemand mehr verstehen kann, sind eine Garantie für Sicherheitslücken. Software, die kompliziert ist, hat mehr Bugs als simpler Code.
2. Weniger ist mehr. Mehr Code, mehr Systeme, mehr Server bieten mehr Angriffsfläche.
3. Sicherheitslösungen sollten Open Source sein. Andere Mitmenschen können nicht so effektiv nach Sicherheitslücken suchen, wenn der Source Code nicht verfügbar ist. Falls der Hersteller eine Sicherheitslücke gar nicht oder erst in ein paar Monaten beheben will, haben Sie kaum eine bis gar keine Möglichkeit, die Lücke selbst zu beheben. Proprietäre Software beinhaltet außerdem des öfteren Hintertüren (manchmal Law-Interception-Interface genannt). Firmen wie Cisco (RFC 3924), Skype (US-Patent-Nr 20110153809) und Microsoft (z.B. _NSAKEY siehe http://www.heise.de/tp/artikel/5/5263/1.html) belegen dies.
4. Eine Firewall ist nur ein Teil eines Sicherheitkonzepts, keine Box, die man hinstellt und dann ist man sicher.
5. Bleiben Sie auf dem neuesten Stand! Was heute als sicher gilt, kann in ein paar Stunden schon als Einfallstor missbraucht werden. Halten Sie deshalb alle Software und alle Systeme auf dem neuesten Stand, auch Drucker, Switches und Smartphones!
6. Die am schwächsten abgesicherte Komponente bestimmt die Qualität der Gesamtsicherheit, und das ist manchmal kein Computer, Telefon oder Drucker, sondern ein Mensch (Stichwort Social Engineering).
7. Es gibt keine 100%ige Sicherheit. Selbst ein ausgeschalteter Computer kann durch einen raffinierten Social Engineer noch missbraucht werden. Sie können es einem Angreifer nur so schwer machen, dass es seine Fähigkeiten übersteigt oder es sich für ihn nicht lohnt, doch dafür müssen Sie die Techniken und die Motivation eines Angreifers kennen.

Inhaltsverzeichnis

Kapitel 1
Installation

Zusammenfassung In diesem Kapitel erfahren Sie, für welche Betriebssysteme die Source Codes entwickelt wurden und auf welchen sie lauffähig sind, welche Python-Version Sie benötigen und wie man Python-Module bequem suchen, installieren und updaten kann. Des Weiteren werden eine Reihe von Entwicklungsumgebungen vorgestellt, um Ihnen eine Übersicht samt Entscheidungshilfen für eine moderne Entwicklungsumgebung zu geben, die Ihnen einen Teil der Arbeit abnimmt, und Sie bei der Fehlersuche unterstützt. Sie können natürlich die Quellcodes auch mit einem einfachen Texteditor eingeben.

1.1 Das richtige Betriebssystem

Alle Quellcodes dieses Buches wurden unter und für GNU/Linux Kernelversion 2.6.x / 3.0.x geschrieben und sind auch nur unter diesen Betriebssystemen getestet worden; sie sollten allerdings ebenfalls unter Linux 2.4 und Versionen größer 3.0 lauffähig sein. Vom Kapitel über Bluetooth abgesehen sollten die Code-Beispiele auch unter BSD-Derivaten und unter Mac OS X einwandfrei funktionieren. Der Autor freut sich über Erfolgsmeldungen per Mail. Von Netzwerk-Hacking unter Windows hält der Autor allerdings nicht sehr viel und kann deswegen keinerlei Aussage über die Lauffähigkeit der Scripte unter diesem Betriebssystem machen.

Falls Sie kein Linux- oder BSD-System installiert haben, reicht es aus ein Image in einer VirtualBox- (www.virtualbox.org) oder Vmware-Virtualisierungslösung (www.vmware.com) zu installieren. Entsprechende vorinstallierte Images finden Sie für VirtualBox unter virtualboxes.org und für Vmware unter www.vmware.com/appliances.

B. Ballmann, *Network Hacks – Intensivkurs*, Xpert.press,
DOI 10.1007/978-3-642-24305-9_1,

1.2 Die richtige Python-Version

Es gibt zwar schon seit ein paar Jahren Python 3 und wenn man sich auf dem Buchmarkt umschaut, findet man auch fast nur noch Bücher für die 3er Version, dieses Buch setzt allerdings für alle Beispiele ausschließlich Python in Version 2.7 voraus, weil die verwendeten Module auf dieser Python-Version aufbauen. Python 2.6 oder 2.5 sollte ebenfalls ausreichend sein.

Um zu überprüfen, welche Version von Python auf Ihrem System installiert ist, führen Sie den nachfolgenden Befehl aus:

```
python --version
Python 2.7.2
```

Sollte in der Ausgabe nicht wenigstens eine 2.5 stehen, empfiehlt der Autor, Ihre Python-Installation zu aktualisieren. Falls eine 3er Version installiert sein sollte, ist dies nicht weiter tragisch, denn Python 2 und 3 können friedlich nebeneinander existieren. Sie müssen lediglich darauf achten, bei allen Skripten in der ersten Zeile /usr/bin/python2 statt /usr/bin/python anzugeben!

1.3 Entwicklungsumgebung

Der Autor bevorzugt GNU/Emacs (www.gnu.org/software/emacs) als Entwicklungsumgebung, weil er die Editier- und Erweiterungsmöglichkeiten für unschlagbar hält. Emacs bietet alle gängigen Features wie Syntax Highlighting, Code Completion, Code Templates, Debugger Support, PyLint Integration und hat dank dem Gespann Rope, Pymacs und Ropemacs mit eine der besten Refactoring-Unterstützungen für Python. Um sofort in den Genuss all dieser Features zu kommen, empfiehlt der Autor die Installation der Erweiterung Emacs-for-Python, zu finden unter gabrielelanaro.github.com/emacs-for-python. Dank einer Menge an Plugins kann Emacs noch erweitert werden, z. B. zum E-Mail- und News-Client, IRC-Chat-Client oder Music-Player, und weitere Features bieten wie Sprachunterstützung, eingebaute Shells und Datei-Explorer bis hin zu Spielen wie Tetris. Manche Mitmenschen meinen, Emacs sei eher ein Betriebssystem als eine IDE.

Als alternativer Consolen-Editor sei hier natürlich ebenso Vi bzw. Vim (www.vim.org) erwähnt, um keine Glaubenskriege auszulösen oder zu unterstützen. Vi bietet ebenfalls alle gängigen Features einer modernen IDE. Wie gut die Python-Unterstützung ist, kann der Autor mangels Erfahrung allerdings nicht beurteilen.

Wer lieber mit einer grafischen Entwicklungsumgebung arbeiten möchte, dem sei als erstes die Entwicklung Eclipse (www.eclipse.org) und PyDev (pydev.org) nahegelegt. Eclipse bietet neben den üblichen Features Code Outline, einen verbesserten Debugger Support und eine schier unglaubliche Anzahl an weiteren Plugins wie z. B. UMLet für UML-Diagramme und Mylyn für die Integration eines Bugtracking-Systems.

Als alternative GUI-IDE möchte der Autor noch Eric4 (eric-ide.python-projects.org) und Spyder (code.google.com/p/spyderlib) aufführen, die ebenfalls die Standardeigenschaften plus Debugger, PyLint Support und Refactoring bieten.

Wer nicht viele Ressourcen zum Programmieren zur Verfügung hat, aber eine GUI bevorzugt, dem empfiehlt der Autor Gedit mit den Plugins Class Browser, Externe Werkzeuge, PyLint, Python Code Completion, Python Doc String Wizard, Python Outline, Quelltext Kommentar und Rope Plugin. Die Installation ist etwas aufwändiger und im Funktionsumfang ein wenig eingeschränkter als bei den vorgenannten Umgebungen, allerdings verbraucht Gedit auch nur etwas ein Zehntel der Ressourcen von Eclipse.

Die Qual der Wahl sei dem Leser überlassen. Wer nicht wählen und mit möglichst geringem Aufwand einsteigen will, der installiert Eclipse und PyDev als Bundle von Aptana (aptana.com/products/studio3).

1.4 Python-Module

Python-Module findet man im Python-Packet-Index, der über pypi.python.org erreichbar ist. Neue Module können in drei Varianten installiert werden:

1. Download des Source-Archives, Entpacken und anschließendes Ausführen der magischen Zeile

   ```
   python setup.py install
   ```

2. Verwenden von easy_install mittels

   ```
   easy_install <modulname>
   ```

3. Mit Hilfe von pip (hierfür muss ggf. das Paket `python-pip` nachinstalliert werden)

   ```
   pip install <modulname>
   ```

Der Autor bevorzugt die Verwendung von `pip`, denn mit `pip` können Sie nicht nur bequem neue Module installieren und alte deinstallieren, sondern auch vorhandene updaten, in Listen exportieren, um sie andernorts alle zu reinstallieren, Module suchen und mehr.

Welche Python-Module für welche Tools und Scripte gebraucht werden, steht entweder am Anfang eines Kapitels oder vor dem jeweiligen Codeabschnitt, damit Sie nur die Module installieren müssen, die Sie auch wirklich verwenden wollen.

Kapitel 2
Netzwerk 4 Newbies

Zusammenfassung Computernetzwerke sind die Adern des Informationszeitalters, Protokolle die Sprache des Netzes.
Dieses Kapitel vermittelt Grundkenntnisse in Sachen Networking von der Hardware und dem Aufbau über die Funktionsweise aller gängigen Protokolle eines Ethernet-IP-TCP-Netzwerks bis hin zu Topologien und Man-in-the-middle-Attacken. Für alle, die ihr Wissen in Sachen Netzwerke erneuern oder neu aufbauen wollen.

2.1 Komponenten

Um überhaupt ein Computernetzwerk aufbauen zu können, braucht man eine Reihe von Hardware-Komponenten. Je nach Netzart umfassen diese neben Computern und Netzwerkkarten noch Kabel, Modems, altmodische Akkustikkoppler in Bananenkisten, Richtfunkantennen oder Satellitenschüsseln, sowie Router (Abschn. 2.14), Gateways (Abschn. 2.13), Firewalls (Abschn. 2.18), Bridges (Abschn. 2.15), Hubs und Switches.

Ein **Hub** ist einfach nur ein Kasten, in den viele Netzwerkkabel gesteckt werden und der alle eingehenden Signale an alle angeschlossenen Kabel weiterschickt. Diese Eigenschaft führt nicht nur zu einer Explosion des Netzwerktraffics, sondern auch dazu, dass Hubs heutzutage nicht mehr verbaut werden. Stattdessen setzt man **Switches** ein, um Netzwerkverbindungen zu bündeln. Der Unterschied zum Hub besteht darin, dass ein Switch sich die MAC-Adresse der Netzwerkkarte am Ende des Kabels merkt und Traffic gezielt nur an den Port verschickt, an dem der Zielrechner angeschlossen ist. Was MAC-Adressen sind und wie die Adressierung genau funktioniert, wird im Abschn. 2.4 erklärt.

B. Ballmann, *Network Hacks – Intensivkurs*, Xpert.press,
DOI 10.1007/978-3-642-24305-9_2,

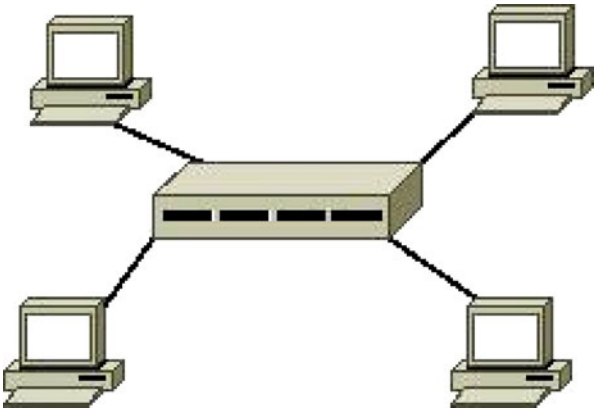

Abb. 2.1 Stern-Netzwerk

2.2 Topologien

Computernetzwerke kann man auf unterschiedliche Arten verkabeln. Die heutzutage üblichste Variante sind **Stern-Netzwerke** (siehe Abb. 2.1), bei denen alle angeschlossenen Computer über ein zentrales Verbindungsgerät miteinander verbunden sind. Der Nachteil dieser Verkabelungsart ist, dass ein Single-Point-of-Failure besteht und, dass das gesamte Netz zusammenbricht, sobald die zentrale Komponente ausfällt. Dieser Nachteil kann allerdings durch redundant (mehrfach) ausgelegte Komponenten umgangen werden.

Eine weitere Möglichkeit ist, alle Computer in einer Reihe miteinander zu verbinden, das sogenannte **Bus-Netzwerk** (siehe Abb. 2.2). Nachteil dieser Topologie ist, dass jeder angeschlossene Computer über zwei Netzwerkkarten verfügen muss und die Daten ggf. über viele Rechner verschickt werden. Sollte einer von ihnen ausfallen, können die dahinter liegenden Computer nicht mehr erreicht werden, und wenn ein Computer in der Kette unter hoher Last leidet, wird er zwangsweise zum Flaschenhals der Netzwerk-Kommunikation.

Der Autor hat in seiner beruflichen Laufbahn bisher nur wenige Bus-Netzwerke zu Gesicht bekommen und alle bestanden aus zwei Computern, die über diese Direktverbindung zeitkritische oder Traffic-intensive Dienste gefahren haben, wie das Replizieren von großen Datenbanken, Clustering von Applikation-Servern oder Syncen von Backupdaten auf einen weiteren Server. In allen Fällen diente das Bus-Netzwerk dazu, das Stern-Netz zu entlasten.

Als letzte Variante sei der Vollständigkeit halber noch das **Ring-Netzwerk** (Abb. 2.3) erwähnt, bei dem, wie der Name schon sagt, alle Computer im Kreis angeschlossen werden. Das Ring-Netz hat dieselben Nachteile wie ein Bus-Netzwerk mit dem Unterschied, dass das Netz nicht teilweise zusammenbricht, sobald ein

Abb. 2.2 Bus-Netzwerk

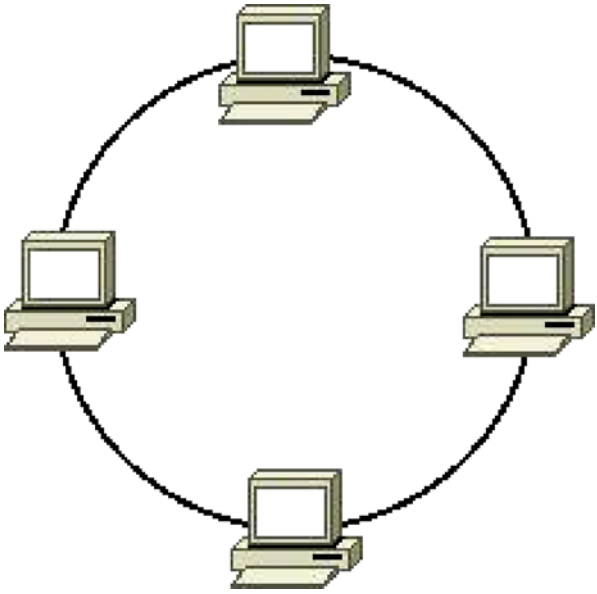

Abb. 2.3 Ring-Netzwerk

Computer ausfällt. In diesem Fall kann der Traffic in einem Ring-Netz einfach in die entgegengesetzte Richtung umgeleitet werden. Der Autor hat selber noch kein Ringnetz implementiert gesehen, hat sich aber sagen lassen, dass diese Topologie für Backbones (Netzwerkrückgrat) bei ISPs und großen Firmen verwendet wird.

Des Weiteren hört oder liest man öfters von **LAN** (Local Area Network), **WAN** (Wide Area Network) und manchmal auch von **MAN** (Middle Area Network). Ein LAN ist ein lokales Netzwerk, das meist auf ein Gebäude, ein Stockwerk oder ein Zimmer begrenzt ist. In modernen Netzen sind die Computer eines LANs mittels eines oder mehrerer Switches miteinander verbunden. Verbindet man mehrere LANs über Router oder VPNs (siehe Abschn. 2.17), so erhält man ein MAN. Umspannt das Netzwerk, wie beim Internet, gar mehrere Länder oder die ganze Welt, spricht man von einem WAN.