サイバーセキュリティテスト完全ガイド

Kali Linuxによるペネトレーションテスト

Peter Kim [著] 株式会社クイープ [訳] 保要隆明、前田優人、美濃圭佑、八木橋優 [監訳]

セキュリティのプロならばこれを読め!

"敵の手の内を知る"テクニックを実践解説。

マイナビ

—あなたは大手の重工業メーカー Secure Universal Cyber Kittensに"ペンテスター"として雇用されている。仕事に必要なのはラップトップ、ネットワークケーブル .. そうそう忘れてはならないのが " 本書 "。この本はテストで生じる厄介な状況から救い出してくれるでしょう。
セキュリティテストのプロセスをアメリカンフットボールのゲーム進行になぞらえ12の異なる章より構成されています。もちろんアメリカンフットボール用語を知っている必要はありません。システムの安全性を守るためのありとあらゆる戦術がぎっしりと詰めこまれた本書は、セキュリティテストの " プレイブック " として活用できます。

CONTENTS

photo : StockLite / Dejan Popovic

サイバーセキュリティテスト完全ガイド

Kali Linuxによるペネトレーションテスト

Peter Kim [著]　株式会社クイープ [訳]　保要隆明、前田優人、美濃圭佑、八木橋優 [監訳]

THE HACKER PLAYBOOK 2

Practical Guide To Penetration Testing

マイナビ

・本書に記載された内容は情報の提供のみを目的としています。著者・翻訳者・出版社のいずれも本書の内容について何らかの保証をするものではなく、内容に関するいかなる運用結果についてもいっさいの責任を負いません。本書を用いての運用はすべて個人の責任と判断において行ってください。

・本書に登場するソフトウェアやサービスのバージョン、画面、機能、URL、製品情報は基本的に原著「The Hacker Playbook 2(ISBN: 9781512214567)」執筆時点のものです。執筆以降に変更されている箇所がありますのでご了承ください。また翻訳時の判断で情報を伏せている箇所がございます。

・原書の公式サイトは以下になります（英語）。本書で取り上げたデータなどは以下のサイトから入手可能です（サイトの管理・運営はすべて原著者で行っています）。
URL: http://TheHackerPlaybook.com
Github: https://www.github.com/cheetz
・本書の動作確認や正誤に関するサポート情報を以下のサイトで提供していきます。
https://book.mynavi.jp/supportsite/detail/9784839959555.html

監訳者まえがき

本書はPeter Kim 氏による『The Hacker Playbook 2』の日本語版です。

原題の「Playbook」というのは、アメリカンフットボールにおける戦術やフォーメーションが記された冊子のことです。敵陣に入ってからのチャンスではこんなプレイを、ディフェンスの押しが強いチームにはこんなプレイを、といったありとあらゆる戦術がぎっしりと詰まったプレイブックにたとえられる本書には、システムの安全性を守るハッカーに向けた、すばらしい知見が詰まっています。

情報システムのセキュリティを考えるとき、敵を知らなければシステムを守ることはできない、そんな言葉をよく耳にします。攻撃者がどのような手法でシステムを脅かすのかを知らなければ、攻撃に対する防御策を講じることもできないという意味です。実際に、昨今ではそういった攻撃者視点での安全性評価の重要性が広く認知され、自分達のシステムに対してセキュリティテストを実施する企業や組織も多くなっています。本書では、そういったセキュリティテストと同様に、攻撃者がどのようなツールを使ってシステムへの侵入を試みるのか、どのような切り口でシステムの脆弱性を探すのかといった攻撃者視点でのシステムの見方を紹介しています。

本書には、セキュリティ施策の最初の一歩である、現状把握に役立つさまざまなツールのハウツーやTips が散りばめられています。それらはセキュリティテストの初学者の助けになるのはもちろん、習熟したセキュリティテスターにも新たな知見を与えてくれるに違いありません。そういった情報をすぐに活用できるとは限りませんが、そういった情報はセキュリティテスターにとって力そのものです。いつか来るそのときに備え、自らの技術力や知識レベルを磨き上げる、そういった日々の修練にも役立つ書籍であると言えます。

また、セキュリティテストに直接携わるわけではない開発者の方にも本書は有用です。本書に記載されたさまざまな攻撃手法によって、自分達のシステムの情報がどこまで暴かれてしまうのかを知ることで、システム構築時に何を意識すればより安全なシステムを構築できるようになるのかを把握できます。また、自分達のシステムに対するセキュリティ施策の効果を実際に評価する際にも、本書の内容が役立つことがあるかもしれません。

多くのツールやTips を網羅し、セキュリティテストの実施にあたっても大いに役立つ書籍はそう多くはありません。ぜひ一度だけでなく二度三度と目を通し、困難に直面したときに助けを求める「プレイブック」として机上に備えておいていただければと思います。

監訳者一同

Kristen、愛犬Dexter、私の家族へ
私が何の話をしているのかまるで見当がつかなくても
私を支えてくれることに感謝している

まえがき

本書は『The Hacker Playbook』の第2版[†1]であり、第1版[†2]の延長線上にあります。本書で取り上げている脆弱性と攻撃は以下のとおりです。第1版で取り上げた攻撃や手法の中には、現在でも重要性を失っていないものがあります。そこで本書では、第1版を読み返さずに済むよう、そうした攻撃や手法も取り上げています。新しい攻撃の中には、この1年半の間に更新された攻撃が含まれています。

- Heartbleed
- ShellShock
- Kerberos の問題（ゴールデンチケットとスケルトンキー）
- PostgreSQL PTH
- 新しいスピアフィッシング
- より効果的で安価なドロップボックス
- より高速でスマートなパスワードクラッキング
- 新しい Wi-Fi 攻撃
- PowerShell スクリプト
- 特権昇格攻撃
- 大規模なネットワークハッキング
- ネットワーク内でのスマートな移動
- Burp モジュール
- プリンターエクスプロイト
- Backdoor Factory
- ZAP Proxy
- 固定キー機能
- NoSQL インジェクション
- 有償のツール（Cobalt Strike、Canvas、Core Impact）
- ラボセクション

本書では、この数年間に変化した攻撃について説明することに加えて、第1版の読者から寄せられたコメントやアドバイスをすべて反映させたいと考えました。そこで、攻撃をテストするラボ環境のセット

†1　『The Hacker Playbook 2: Practical Guide To Penetration Testing』(ISBN：9781512214567)
†2　『The Hacker Playbook: Practical Guide To Penetration Testing』(ISBN：9781494932633)

アップ方法を詳しく取り上げることに加えて、侵入テストに関する最新のヒントとトリックも取り上げています。さらに、多くの学校が筆者の本をカリキュラムに取り入れているため、内容が追いやすいものになるよう心がけました。脆弱性やエクスプロイトをテストするのに役立つラボセクションはできるだけ追加するようにしています。

第1版から変わっていないのは何でしょうか。第1版の目標の1つは、できるだけ「現実味」を持たせることでした。理論的な攻撃から距離を置くようにし、個人的に経験し、実際にうまくいくことがわかっているものに焦点を合わせるようにしました。もう1つの目標は、ペンテスターとしての基本的な知識が深まるようにすることでした。つまり、現在または未来の職場や顧客に対して読者の価値が高まるよう、手法を変えることを働きかけてみようと考えました。脆弱性スキャナーを実行し、レポートに書いてあるとおりのことを報告するだけでは、企業にとって何のメリットもありません。また、範囲が非常に限られた侵入テストは、安全であるかのような錯覚を与えます。第1版を読んでいる場合は安心してください。本書のボリュームは2倍近くになっており、たとえ読んだ記憶があることが書かれていたとしても、新しい情報が大量に見つかります。また、要望に応えて、ハッキングに役立つスクリプトやツールもいろいろ作成してみました。これはおそらく最も要望が多かったことの1つなので、これらのスクリプトをGitHub[†3]にアップロードし、簡単に確認できるようにしました。

第1版を読んでいない場合は、筆者のペンテスターとしての経験はどれくらいなのだろうと考えているかもしれませんね。筆者は、大手の金融機関、公共事業会社、Fortune 500のエンターテイメント企業、および政府機関で、8年前から侵入テストを行っています。そして数年前からは、オフェンシブネットワークセキュリティの指導とToorcon/Derbycon/BayThreatでの講演を行っています。また、多くのセキュリティ専門誌でよく取り上げられており、現在は南カリフォルニアで300名以上のメンバーを持つセキュリティコミュニティを主催しています。筆者が学んだことを共有し、それを独自のセキュリティライフスタイルに取り入れてもらえれば、と考えています。

技術面では、多くのツールや攻撃がこの数年間で様変わりしています。Pass-the-Hash攻撃とグループポリシー設定のパッチ攻撃では、攻撃の手順や手法が変化しています。

ここで注意しておきたい重要な点が1つあります。それは、筆者が有償のツールとオープンソースの両方を使用していることです。本書では、有償のツールごとに、それに相当するオープンソースのツールを紹介するようにしています。時折、オープンソースのツールしか使用しないと宣言するペンテスターに出会うこともあります。ペンテスターとしてはかなり強気の発言です。「現実」の攻撃を再現することになっていたとしたらどうでしょうか。オープンソースしか使用しないという制約なんて、「悪意を持つ何者か」にとっては知ったことではありません。侵入テストを成功に導くものであれば、どのようなツールでも使用する必要があります。

本書の対象読者は誰でしょうか。本書では、多少なりともMicrosoft Active Directoryの経験があり、Linuxを十分に理解しており、ネットワーキングの基礎知識があり、コーディングの経験があることを前

†3 https://github.com/cheetz

提としています。コーディングに関しては、Bash、Python、Perl、Ruby、C などの経験があれば十分です。また、脆弱性スキャナーや Metasploit などのエクスプロイトツールを使用した経験があることも前提としています。そうした知識はないものの、セキュリティに興味がある、という場合は、基礎から始めるようにしてください。基本的な知識を身につけてからでなければ、セキュリティの世界に飛び込むことはできません。

本書の対象となるのは、オフェンシブセキュリティの世界に進みたいと考えている人や、すでにその世界で活躍している人だけではありません。本書では、インシデントレスポンスサービスにとって価値のある情報や知見を提供しています。そうしたサービスでは、攻撃者がどのように考え、どのような手口を用いるのかを知る必要があります。

最後に、リサーチャーとペンテスターの違いについて少し説明しておきます。リサーチャーとペンテスターはどちらもリサーチと侵入テストの分野に精通している必要があります。このため、多くの場合は同列に扱われます。ですが本書では、これら2つの領域を少し切り離した上で、侵入テストに焦点を合わせています。本書での定義をもう少し明確にしておきましょう。リサーチャーとは、1つのこと、または限られた範囲のことに焦点を合わせ、アプリケーション、プロトコル、OS のリバーシングにより多くの時間を割く人のことです。リサーチャーの目標は、特定の脆弱性に対する未知のエクスプロイトを発見することです。これに対し、ペンテスターは、システムやアプリケーションをハッキングするにあたって既知のエクスプロイトを使用します —— 注意しておきますが、これは一般論です。オーバーラップする部分は常に存在します。ペンテスターは（Web のパラメータといった）脆弱性をファジングし、ゼロデイエクスプロイトを見つけ出します。ですが、リサーチャーとは異なり、すべての問題を洗い出すために時間を割くわけではありません。

最後の注意点

本書は、いわゆる「スーパーハッカー」になるための本ではありません。本書では、練習と調査をじっくり行い、ゲームを楽しんでもらいます。本書を読むことで、既成概念を打ち破り、より創造性豊かになり、システムの欠陥をよく理解できるようになることを願っています。

侵入テストは書面による許可を受けたシステムでのみ行うことを覚えておいてください。Google で「hacker jailed」を検索すれば、10代の若者がおもしろ半分にしたことで懲役刑に処せられた例がいくらでも見つかります。ハッキングが許可されているフリープラットフォームを利用すれば、さらに自分を鍛えるのに役立つでしょう。

はじめに

あなたはSecure Universal Cyber Kittens, Inc、略してSUCKという大手の重工業メーカーにペンテスターとして雇われています。SUCKでは、最も高い入札者に渡される未来の兵器を開発しており、「殺しのライセンス」—— は冗談として、「ハッキングの許可証」をあなたに発行しています。これにより、あらゆる手口を用いてSUCKのネットワークに侵入し、企業秘密を盗み出すことが完全に許可されています。

そこで、ラップトップ、ペネトレーションドロップボックス、Rubber Ducky、Proxmark、ケーブルをバッグに詰め込み... おっと、肝心の本書を詰め込むのを忘れるところでした。危機的状況から脱するときに頼りになるのが本書ですよね。あなたは最後のミッションのことをぼんやりと思い出します。

HIDカードをコピーし、ネットワークにドロップボックスを仕掛けた後、あなたはオフィスをあとにし、警備員に気づかれないようにこっそり抜け出します。ドロップボックスがあなたのSSHサーバーに接続してきて、SUCKのネットワークにアクセスできるようになります。ネットワーク上では極力物音を立てないようにして、IDSのシグネチャに引っかからないようにしたいところです。さて、何を探せばよいでしょうか。本書の第2章をめくっていたあなたは、プリンターのことを思い出します。MFP（Multi-Function Printer）を調べたところ、デフォルトのパスワードが設定されたままのプリンターが見つかります。そこで、このプリンターでLDAPの設定を変更し、netcatリスナーをセットアップし、Active Directoryの認証情報を手に入れます。それらのアカウントが持っているアクセス許可まではわからないため、SMBexecのカスタムペイロードを使ってWindowsマシンにpsexecを実行してみます。そして、それらの認証情報を使って通常のユーザーとしてシステムにアクセスできるようになります。第5章のPowerToolsを使ったトリックをいくつか試した後、ローカル管理者の権限が手に入ったので、Mimikatzを使ってメモリからパスワードを取り出します。やれやれ、これでは簡単すぎます。いくつかのアカウントのパスワードを取り出した後、ドメイン管理者の居場所を突き止めます。そして、ドメイン管理者のコンピュータに接続し、ここでもパスワードを取り出します。ドメイン管理者の認証情報があれば、psexec_ntdsgrabを使ってドメインコントローラをダンプするのは造作もないことです。あとは、足跡を消せば完了です。

本書を持ってきてよかったでしょう？

標準

第1章に進む前に、侵入テストに使用される基本情報と標準について理解しておく必要があります。これは偵察、脆弱性の検索とエクスプロイト、レポートの作成の土台となります。侵入テストを実行する正しい方法というものは存在しませんが、少なくとも基礎を押さえておく必要があります。

Penetration Testing Execution Standard（PTES）

侵入テストの現在の標準はPTES[†4]です。PTESは侵入テストを構成する基本的な要素を定義しており、あちこちで参照されています。PTES のテクニカルガイドラインは詳細情報の宝庫であるため、ぜひひととおり読んでみてください。PTES では、以下の7つのメインセクションからなるモデルが採用されています。

1. Pre-engagement Interactions（侵入テスト前の準備）
2. Intelligence Gathering（インテリジェンスの収集）
3. Threat Modeling（脅威モデルの定義）
4. Vulnerability Analysis（脆弱性の分析）
5. Exploitation（エクスプロイト）
6. Post Exploitation（ポストエクスプロイト）
7. Reporting（レポートの作成）

本書では、創造力を働かせ、自分にとってうまくいくものを見つけ出すことを奨励しています。PTESフレームワークは侵入テストを行うためのすばらしいモデルですが、個人的には、標準のモデルを調整した上で侵入テストを行うようにしています。個人的な経験から、筆者が使用する標準は以下のようなものになります。

1. Intelligence Gathering（インテリジェンスの収集）
2. Initial Foothold（最初の足場組み）
3. Local/Network Enumeration（ローカル／ネットワークの列挙）
4. Local Privilege Escalation（ローカルアカウントの特権の昇格）
5. Persistence（持続性の確立）
6. Lateral Movement（ネットワーク内の移動）
7. Domain Privilege Escalation（ドメインアカウントの特権の昇格）
8. Dumping Hashes（ハッシュのダンプ）
9. Data Identification/Exfiltration（データの特定と抽出）
10. Reporting（レポートの作成）

これらは侵入テストの際に筆者が何を行い、何に焦点を合わせるのかを示しています。ソーシャルエンジニアリングを通じて最初の足場を組んだ後は、特権付きのアカウントを搾取する必要があります。

†4 http://www.pentest-standard.org/

そのためには、システムとネットワークを列挙し、不適切な設定やローカルの脆弱性を探す必要があります。また、シェルにアクセスできなくなった場合に備えて、持続性を確保しておく必要もあります。システムにアクセスした後、またはローカル管理者の権限を手に入れた後は、ドメイン管理者のアカウントを手に入れることが可能かどうかを確認する必要があります。そのためには、他のコンピュータをハッキングすることで、最終的にドメイン管理者のアカウントを手に入れる必要があります。ドメインコントローラにおいて最も効果的なテストは、ドメインのハッシュをダンプすることです。このテストはそこで終わりではありません。顧客が実際に価値を見出すのは、個人を特定できる情報（PII）や知的財産（IP）など、顧客から要求された機密データにアクセスした後です。さらに、報酬の対象となるのがレポートであることは誰もが承知しています。よい標準テンプレートと価値の高いデータを提供することで、ライバルに差をつけてください。

もちろん、これはテストの過程で何が起きるかをかなり大ざっぱにまとめたものにすぎません。本書では、このプロセスをたどるのに役立つガイドラインを作成してみました。本書は、アメリカンフットボールのプレイブック（戦術書）に見立てた11の章で構成されています。ですが、心配はいりません。本書を読み進めるにあたって、アメフトの用語を知っている必要はありません。各章の内容は以下のとおりです。

- **第1章　試合の前に — セットアップ**
  ここでは、ラボ環境、攻撃用のマシン、本書で使用するツールのセットアップ方法について説明します。
- **第2章　スナップ前に — ネットワークのスキャン**
  「スナップ」はアメリカンフットボールにおいてプレイの最初に行う動作です。テストを行うには、環境をスキャンし、何に立ち向かうのかを理解する必要があります。ここでは、ディスカバリとスマートなスキャンについて詳しく説明します。
- **第3章　ドライブ — スキャン結果のエクスプロイト**
  第2章で特定された脆弱性をもとに、システムのエクスプロイトを開始します。ここで少し手を汚し、コンピュータのエクスプロイトに取りかかります。
- **第4章　スロー — 手動によるWebアプリケーションのテスト**
  時には創造力を働かせ、「オープンターゲット」を探す必要があるかもしれません。ここでは、Webアプリケーションの脆弱性を手動で調べて、検出されたものをエクスプロイトする方法について説明します。
- **第5章　ラテラルパス — ネットワーク内の移動**
  システムをハッキングした後は、ネットワーク内を移動する方法について説明します。
- **第6章　スクリーンパス — ソーシャルエンジニアリング**
  一般に、スクリーンパスは敵をだますためのプレイです。ここでは、ソーシャルエンジニアリン

グの手法について説明します。

- **第７章　オンサイドキック ― 物理的なアクセスが必要な攻撃**
  オンサイドキックは、わざと短いキックをして攻撃権を得るプレイです。ここでは、物理的なアクセスを必要とする攻撃について説明します。
- **第８章　クォーターバックスニーク ― アンチウイルススキャナーの回避**
  「あと数ヤード」というときには、クォーターバックスニークが最適です。侵入テストでは、アンチウイルスに捕まることがあります。ここでは、アンチウイルスを回避することで、そうした小さなハードルをクリアする方法について説明します。
- **第９章　スペシャルチーム ― クラッキング、エクスプロイト、トリック**
  ここでは、パスワードのクラッキング、エクスプロイト、NetHunter、その他のトリックを紹介します。
- **第１０章　ツーミニッツドリル ― ゼロからヒーローへ**
  試合は残り２分であり、あなたはドメイン管理者のアカウントにアクセスできない状況から何とか挽回しなければなりません。
- **第１１章　ゲーム終了後の分析 ― レポート**
  ここでは、侵入テストで検索されたものをレポートにまとめます。

更新情報

知ってのとおり、セキュリティは急速なペースで変化しており、絶えず何かがうまくいかなくなります。そうした変化や読者からのリクエストには随時対応したいと考えています。

本書の更新情報：`http://thehackerplaybook.com/subscribe`
Twitter：`@HackerPlaybook`
本書の Web サイト：`http://TheHackerPlaybook.com`
Github：`https://www.github.com/cheetz`
電子メール：`book@thehackerplaybook.com`

目次

THE SETUP

第1章 セットアップ

SUCK（Secure Universal Cyber Kittens, Inc.）への攻撃を開始する前に、攻撃の威力をテストするためのテストラボを構築し、攻撃用のマシンを作成し、エクスプロイトの仕組みを理解する必要があります。本格的な攻撃を実行するにあたって、練習とテストは非常に重要です。試したことのないエクスプロイトでテストを行い、重要なシステムをうっかりダウンさせたことがばれてしまい、会社から放り出されるようなヘマはしたくないはずです。

1.1 ラボの構築

アプリケーション、オペレーティングシステム（OS）、ネットワークアプリケーションがすべて揃った完全なラボを構築するのは難しいかもしれませんが、基本的なコンポーネントは揃えておく必要があります。これには、基本的なLinuxサーバーとWindowシステムが含まれます。

Windows OSは有償であるため、購入する必要があるかもしれません。学生の場合はたいていソフトウェアを無償で入手できるため、Microsoft DreamSpark[†1]で利用資格を満たしているかどうか調べてみるとよいでしょう。Windows Server 2012やその他のソフトウェアが利用可能となっています。

1. ドメインの構築

MicrosoftのActive Directory環境を使って練習するのもよいですが、最も効果的な学習法の1つは、環境を自分で構築してみることです。Active Directory環境のノウハウを習得すれば、あとできっと役立つはずです。本書では、Active Directoryのドメインコントローラのセットアップ方法をステップ形式でまとめてあるため、本書を読みながら実際に環境を構築してみてください。ドメインコントローラやク

†1 https://www.dreamspark.com/

ライアントを一度も構築したことがない場合は、まずそれらを構築してみることを強くお勧めします。攻撃の対象となるものを本当に理解するには、その仕組みを知っておく必要があります。

以下の例では、Windows Server 2012 R2 と Windows 10/8/7 を使って Windows ドメイン環境を構築します。本書では、最近の OS に焦点を合わせたいと考えています。ただし、古いエクスプロイトをテストしたいと考えている場合は、Windows XP SP2 のインストールを検討してもよいでしょう。なお、本書の Web サイトに Active Directory のインストールガイド[†2]があるのでチェックしてみてください。

2. 追加のサーバーの構築

ここでは、筆者が推奨する脆弱な仮想マシンを紹介します。本書のラボの多くで、これら 2 つのフレームワークをテストに使用します。自分で練習する場合は、本書の巻末で示す他のテストサーバーを検討してください。

Metasploitable 2

一般的な脆弱性が意図的に仕込まれた、脆弱な Ubuntu Linux 仮想マシンです。Metasploit などのセキュリティツールのテストや、一般的な攻撃の例示に最適です。仮想マシン（VM）をダウンロードして仮想プラットフォームでブートすればよいだけなので、セットアップは比較的簡単です。

```
http://sourceforge.net/projects/metasploitable/files/Metasploitable2
```

OWASPBWA

Metasploitable 2 がサービスに照準を合わせているのに対し、OWASPBWA（OWASP Broken Web Applications Project）は脆弱な Web アプリケーションに照準を合わせています。脆弱な Web アプリケーションを 1 つの仮想マシン（VM）にまとめたものとしては、OWASPBWA は最大級のコレクションの 1 つです。本書の Web サンプルの多くは、この VM を使用します。セットアップは Metasploitable 2 と同様に、VM をダウンロードしてブートするだけです。

```
http://sourceforge.net/projects/owaspbwa/files/
```

3. 練習

他の職業と同様に、侵入テスト（ペネトレーションテスト）でも経験がものを言います。テストはどれもまったく異なるため、環境の変化に適応できることが求められます。ろくに練習もせず、いろいろなツールを試してみることも、エクスプロイトでさまざまなペイロードを使ってみることもないようでは、行き詰まってしまった場合に状況を打開することはできないでしょう。

---

†2　http://www.thehackerplaybook.com/Windows_Domain.htm

1.2　侵入テストマシンの構築

本書の第1版[†3]では、すべてを自動化するスクリプトを作成するのではなく、読者にツールを構築させてインストールさせたのはなぜか、という質問がいくつか寄せられました。そうした手順を踏ませた主な理由の1つは、それらが非常に重要なツールであり、自分のレパートリーを増やすのに役立つからです。たとえばKali Linuxはものすごい数のツールで構成されていますが、必要なツールがインストールされていることを知らなかったり、攻撃を実際に試していなかったりすれば、いざというときに宝の持ち腐れになってしまいます。

1.　侵入テストマシンのセットアップ

第1版を読んでマシンをすでにセットアップしている場合は、本節にざっと目を通すだけでかまいません。知ってのとおり、筆者はいつもノートPCを2台持ち歩くようにしています。1台目はWindowsマシンで、もう1台はMac OS XかLinuxマシンです。ノートPCを2台持ち歩いているのは、Mac OS Xマシンがネットワークに接続できないという非常に特殊な状況で侵入テストを行ったことがあるためです。そのときは、その原因を突き止めることに時間をかけるのではなく、すべての攻撃とスキャンをWindowsマシンから開始し、Mac OS Xの問題は時間が空いたときに修正しました。ノートPCが2台あったことで何度助けられたことか。

ベースシステム[†4]でWindowsを実行するのか、Mac OS Xを実行するのか、それとも何らかのLinuxディストリビューションを実行するのかは重要ではありません。ただし、約束事がいくつかあります。1つは、仮想マシン（VM）プラットフォームをインストールする必要があることです。VirtualBox[†5]やVMware Workstation Player[†6]を使用してもよいですし、他のVMを使用してもよいでしょう。どちらもWindowsでは無償ですが、Mac OS XではVirtualBoxのみ無償となっています。有償のVMプラットフォームには、暗号化、スナップショット、はるかに便利なVM管理など、多くの機能が搭載されています。このため、ぜひとも入手したいところです。

ツールのほとんどはVMにインストールすることになるため、ベースシステムに余計なものが含まれていない状態にすることが最も重要となります。ベースシステムでは、個人のサイトも閲覧しないでください。そうすれば、ベースシステムが常にクリーンな状態に保たれます。クライアントサイトにマルウェアを持ち込んだり ―― 筆者は何度も目撃しています ―― 未知の脆弱なサービスを待ち受けたりすることはなくなります。マシンをセットアップした後は、設定済みのクリーンな状態のVMでスナップショットを作成します。そうすれば、新たなテストを行うときに、ベースラインイメージに戻して、ツールにパッ

†3　『The Hacker Playbook: Practical Guide To Penetration Testing』(Createspace Independent Pub) ISBN：978-1494932633

†4　［訳注］テストを行う前の仮想マシンイメージ。

†5　https://www.virtualbox.org

†6　https://my.vmware.com/web/vmware/downloads

チやアップデートをあて、必要なツールを追加するだけで済みます。真面目な話、この方法で苦境から救われます。過去の検査で、すでにインストールされているはずのツールのセットアップに時間を取られすぎたことが何度あったか知れません。

2. ハードウェア

◈ 侵入テスト用のノートPC

侵入テスト用のノート PC の基本的な要件は、第 1 版からそれほど変化していません。基本的な要件は以下のとおりです。

- 少なくとも 8GB の RAM を搭載したノート PC
- 500GB のストレージ（SSD を強く推奨）
- Intel Core i7 クアッドコアプロセッサ

◈ パスワードクラッキング用のデスクトップ

これは完全にオプションですが、筆者がハッシュに不正アクセスしたテストの多くで、より高性能なパスワードクラッキング装置が必要となりました。Celeron プロセッサと 8 基の GPU を搭載した夢のようなマシンを購入するという手もありますが、筆者は驚くべきパスワードクラッキング能力を備えた大容量の多目的マシンを構築しています。後ほど、パスワードクラッキング用に組み立てたマシンの仕様とツール、そしてその方法をとった理由を示します。

パスワードクラッキング／多目的ハッキングマシン

- ケース：CORSAIR Vengeance C70
- ビデオカード：SAPPHIRE 100360SR Radeon R9 295x2 8GB GDDR5
- ストレージ：SAMSUNG 840 EVO MZ-7TE500BW 2.5" 500GB SATA III TLC Internal SSD
- 電源：SILVERSTONE ST1500 1500W ATX
- RAM：CORSAIR Vengeance Pro 16GB (2 x 8GB) 240-Pin DDR3 SDRAM DDR3 1600
- CPU：Intel Core i7-4790K 4.0GHz
- マザーボード：ASUS MAXIMUS VII FORMULA
- CPU クーラー：Cooler Master Hyper 212 EV

本当に重要なのは GPU だけであることを考えると、パスワードクラッキングが目的にしては確かに過剰ですが、筆者のレパートリーにぜひとも加えたいシステムでした。

3. オープンソースを使用するか、ソフトウェアを購入するか

本章では、オープンソースのソフトウェアと有償のソフトウェアを比較することが読者のためになると考えています。ソフトウェア製品を購入する余裕があるとは限りませんが、販売されているソフトウェアと、攻撃者が使用しているかもしれないソフトウェアを知っておくことは非常に重要です。防御する側にとっても、また攻撃を仕掛ける側にとっても、ツールの良し悪しが結果を左右することは間違いありません。本書では、筆者が非常に便利であると感じているさまざまなソフトウェア製品を紹介します。これらのツールは、さまざまな攻撃が仕掛けられた状況において役立つ可能性があります。ここでは、ソフトウェア製品ごとにそれに相当するオープンソースのソフトウェアを示したいと考えていますが、常にオープンソースのソフトウェアがあるとは限りません。

◈ 本書で使用するソフトウェア製品

- Burp Suite Pro
- Canvas
- Cobalt Strike
- Core Impact
- Nessus
- Nexpose

◈ Kali Linux

Kali Linux[†7]は、しばしば攻撃的な侵入テストの標準と見なされているDebianベースのLinuxディストリビューションです。Kali Linuxには、さまざまなセキュリティツールが含まれており、1つのフレームワークとしてあらかじめ構成されています。Kali Linuxはオフェンシブセキュリティプラットフォームの出発点として最適です。本書では主に、このLinuxディストリビューションに手を加えていきます。ぜひVMをダウンロードしてテストに使用してください。

◈ Back Box

Kali Linuxは標準と見なされていますが、1つのツール、OS、プロセスに依存するのは決して得策ではありません —— これは本書全体の不断のテーマです。特定のツールのサポートが打ち切られるかもしれないという問題もありますが、視野が狭くなり、古い手法から抜け出せなくなることのほうが問題です。Back Box[†8]は、セキュリティプラットフォームの構築とサポートに積極的に取り組んでいるコミュニティの1つです。Back Boxの主な違いの1つは、Ubuntuをベースにしていることです。もう1つは（こちら

†7 https://www.kali.org/
†8 http://www.backbox.org/

のほうが重要ですが)、Kali Linuxのように全員がrootとして作業を行うのではなく、デフォルトのユーザー権限を管理できることです。Ubuntu のほうが使いやすいというユーザーもいますし、ツールによってはUbuntu 用に開発されていて、Ubuntu のほうが Kali Linux よりも動作が安定しているというケースもありました。Back Box もあなたが利用できるツールの 1 つにすぎません。どのようなツールが利用できるのかを知っておいて損はありません。

4. マシンのセットアップ

どのセキュリティディストリビューションにも含まれていないツールや、手持ちのツールセットで変更しなければならないツールがいろいろあります。筆者はそれらをディレクトリにまとめて、すぐに使えるようにしています。インストールが必要なツールは以下のとおりです。

偵察／スキャンツール

- Discover
- EyeWitness
- HTTPScreenShot
- WMAP
- SpiderFoot
- Masscan
- Gitrob
- CMSmap
- Recon-ng
- SPARTA
- WPScan
- パスワードリスト

エクスプロイト

- Burp Suite Pro
- ZAP Proxy
- NoSQLMap
- SQLMap
- SQLNinja

- BeEF Exploitation Framework
- Responder
- プリンターエクスプロイト
- Veil
- WifiPhisher
- Wifite
- SET

エクスプロイト後

- 本書のカスタムスクリプト
- SMBexec
- Veil
- WCE
- Mimikatz
- PowerSploit
- Nishang
- The Backdoor Factory
- DSHashes
- Net-Creds

5. Kali Linux のセットアップ

攻撃用のホストをセットアップする方法はさまざまですが、本書で掲載する例はすべて再現してもらいたいと考えています。先へ進む前に、以下の設定を使ってホストをセットアップしてください。これらのツールは定期的に変更されるため、以下の設定は少し調整する必要があるかもしれません。本書のWeb サイトで最新情報[†9]を忘れずにチェックしてください。すべての設定とソフトウェアに関する部分はGitHub[†10]からダウンロードできます。コマンドを1つ1つ入力する代わりに、ファイルからコピーできるようになります。

本書はKali Linux プラットフォームをベースとしているため、Kali Linux ディストリビューションをダウ

†9 http://www.thehackerplaybook.com
†10 http://www.github.com/cheetz/thp2

ンロード[†11]するとよいでしょう。VMware イメージ[†12]と VMware Workstation Player もダウンロードすることを強くお勧めします。これは gz 圧縮された tar アーカイブファイルなので、解凍してから vmx ファイルを読み込んでください。

◈ Kali VM が起動したら

1. ユーザー名 `root` とデフォルトのパスワード `toor` でログインします。
2. ターミナルを開きます。
3. パスワードを変更します。

```
passwd
```

4. イメージを更新します。

```
apt-get update
apt-get dist-upgrade
```

5. Metasploit データベースをセットアップします。

```
service postgresql start
```

6. ブート時に PostgreSQL データベースを起動するようにします。

```
update-rc.d postgresql enable
```

7. 下記のコマンドを実行します。これにより、`database.yml` ファイルが作成されます[†13]。

```
msfdb init
```

8. gedit をインストールします[†14]。

```
apt-get install gedit
```

---

†11 http://www.kali.org/downloads/

†12 https://www.offensive-security.com/kali-linux-vmware-arm-image-download/

†13 [訳注] 最新の Kali Linux では、`msfdb init` を実行すると `database.yml` を作成できる。

†14 [訳注] gedit はデフォルトでインストールされていることもある。

9. 多くのネットワーク管理者はDHCPなどのログでKaliという名前のシステムを検索します。あなたがテストを行っている企業の命名規則に従って、ホスト名をKaliから変更し、保存します。

```
gedit /etc/hostname
gedit /etc/hosts
reboot
```

10. Metasploitのログ機能を有効にします（オプション）。
    - ◇ これが「オプション」であるのは、ログがかなり大きくなるためですが、コマンドとその結果はすべてMetasploitのコマンドラインインターフェイスから記録できます。一括攻撃／クエリや、クライアントがそうしたログを要求した場合に、これが非常に役立ちます。新しいイメージの場合は、ログを構成する前に、`.msf5`フォルダ[†15]を作成してください。このフォルダを作成するには、`msfconsole`と入力してMsfconsoleを起動した後、終了します。
    - ◇ コマンドプロンプトに以下のコマンドを入力します。

```
echo "spool /root/msf_console.log" > /root/.msf4/msfconsole.rc
```

    - ◇ ログは`/root/msf_console.log`に格納されます。

◈ ツールのインストール

The Backdoor Factory

PE、ELF、Mach-Oのバイナリにシェルコードでパッチをあてるツール。

```
git clone https://github.com/secretsquirrel/the-backdoor-factory \
/opt/the-backdoorfactory
cd /opt/the-backdoor-factory
./install.sh
```

HTTPScreenShot

多くのWebサイトのスクリーンショットとHTMLを集めるためのツール。

```
pip install selenium
git clone https://github.com/breenmachine/httpscreenshot.git /opt/httpscreenshot
cd /opt/httpscreenshot
chmod +x install-dependencies.sh && ./install-dependencies.sh
```

デフォルトでは、HTTPScreenShotがうまくいくのは、64ビットのKaliで実行している場合に限られます。32ビットPAEを実行している場合は、次の方法でi686 phatomjsをインストールしてください。

†15 ［訳注］翻訳時の最新版。

```
wget https://bitbucket.org/ariya/phantomjs/downloads/phantomjs-1.9.8-linuxi68
6.tar.bz2
bzip2 -d phantomjs-1.9.8-linux-i686.tar.bz2
tar xvf phantomjs-1.9.8-linux-i686.tar
cp phantomjs-1.9.8-linux-i686/bin/phantomjs /usr/bin/
```

SMBexec

Samba を使って psexec スタイルの攻撃をすばやく仕掛けるツール。

1. 以下のコマンドを実行します。

```
git clone https://github.com/pentestgeek/smbexec.git /opt/smbexec
cd /opt/smbexec && ./install.sh
```

2. [1 - Debian/Ubuntu and derivatives] を選択します。
3. すべてデフォルト値を選択します。
4. `./install.sh` を実行します。
5. [4] を選択して smbexec バイナリをコンパイルします †16。
6. コンパイルが完了したら、[5] を選択して終了します。

Masscan

最も高速なインターネットポートスキャナー。インターネット全体を 6 分足らずでスキャンできます。

```
apt-get install git gcc make libpcap-dev
git clone https://github.com/robertdavidgraham/masscan.git /opt/masscan
cd /opt/masscan
make
make install
```

Gitrob

GitHub リポジトリの偵察ツール。

```
git clone https://github.com/michenriksen/gitrob.git /opt/gitrob
gem install bundler
service postgresql start
su postgres
createuser -s gitrob --pwprompt
createdb -O gitrob gitrob
exit
```

† 16 [訳注] mingw の gcc がインストールされていない場合は以下のコマンドでインストールする必要がある。

```
apt-get install mingw32
apt-get install mingw-w64
```

```
cd /opt/gitrob/bin
gem install gitrob
```

CMSmap

セキュリティホールの検出プロセスを自動化するPythonベースのCMS（Content Management System）スキャナー。オープンソースとして提供されています。

```
git clone https://github.com/Dionach/CMSmap /opt/CMSmap
```

WPScan

WordPressの脆弱性スキャナー／ブルートフォースツール[†17]。

```
git clone https://github.com/wpscanteam/wpscan.git /opt/wpscan
cd /opt/wpscan && ./wpscan.rb --update
```

EyeWitness

Webサイトのスクリーンショットを作成し、サーバーのヘッダー情報を提供し、可能であればデフォルトの認証情報を特定するツール。

```
git clone https://github.com/ChrisTruncer/EyeWitness.git /opt/EyeWitness
```

Praedasploit

一般的に検出されるプリンターエクスプロイトで構成されたフレームワーク。

```
git clone https://github.com/MooseDojo/praedasploit /opt/praedasploit
```

SQLMap

SQLインジェクションツール。

```
git clone https://github.com/sqlmapproject/sqlmap /opt/sqlmap
```

Recon-ng

Pythonベースの本格的なWeb偵察フレームワーク。

```
git clone https://bitbucket.org/LaNMaSteR53/recon-ng.git /opt/recon-ng
```

Discoverスクリプト

さまざまな侵入テストのタスクの自動化に使用されるカスタムbashスクリプト。

```
git clone https://github.com/leebaird/discover /opt/discover
cd /opt/discover && ./update.sh
```

†17 [訳注] Kali LinuxにはWPScanがデフォルトで含まれている。

BeEF (Browser Exploitation Framework)

クロスサイトスクリプティング攻撃フレームワーク。

```
cd /opt/
wget https://raw.github.com/beefproject/beef/a6a7536e/install-beef
chmod +x install-beef
./install-beef
```

Responder

LLMNR（Link-Local Multicast Name Resolution）、NBT-NS（NetBIOS over TCP/IP Name Service）、mDNS (multicast Domain Name System) をターゲットとするポイズナー。NTLM (Windows NT LAN Manager) のバージョン 1 および 2、LMv2、NTLMSSP（NTLM Security Support Provider）、HTTP Basic 認証をサポートしており、不正な HTTP/SMB/MSSQL/FTP/LDAP 認証サーバーが組み込まれています。Responder は NTLM チャレンジ／レスポンスハッシュの取得に使用されます。

```
git clone https://github.com/SpiderLabs/Responder.git /opt/Responder
```

本書のカスタムスクリプト

本書のために筆者が作成したカスタムスクリプト。

```
git clone https://github.com/cheetz/Easy-P.git /opt/Easy-P
git clone https://github.com/cheetz/Password_Plus_One /opt/Password_Plus_One
git clone https://github.com/cheetz/PowerShell_Popup /opt/PowerShell_Popup
git clone https://github.com/cheetz/icmpshock /opt/icmpshock
git clone https://github.com/cheetz/brutescrape /opt/brutescrape
git clone https://www.github.com/cheetz/reddit_xss /opt/reddit_xss
```

フォークバージョン

本書で使用する PowerSploit と Powertools のフォークバージョン。元のソースをコピーして、リポジトリを別途作成してください。

```
git clone https://github.com/cheetz/PowerSploit /opt/HP_PowerSploit
git clone https://github.com/cheetz/PowerTools /opt/HP_PowerTools
git clone https://github.com/cheetz/nishang /opt/nishang
```

DSHashes

NTDSXtract に適した形式でユーザーハッシュを抽出するツール。

1. `https://storage.googleapis.com/google-code-archive-source/v2/code.google.com/ptscripts/source-archive.zip` をダウンロードします。
2. `dshashes.py` を `/opt/NTDSXtract/dshashes.py` へ移動します。

SPARTA

ネットワークインフラストラクチャの侵入テストを容易にするPythonベースのGUIアプリケーション。侵入テストのスキャンフェーズとスキャン結果を列挙するフェーズを手助けします。

```
git clone https://github.com/secforce/sparta.git /opt/sparta
apt-get install python-elixir
apt-get install ldap-utils rwho rsh-client x11-apps finger
```

NoSQLMap

MongoDBデータベースサーバーとWebアプリケーションを対象とする自動侵入ツールセット。

```
git clone https://github.com/tcstool/NoSQLMap.git /opt/NoSQLMap
```

SpiderFoot

オープンソースのフットプリンティングツール。

```
mkdir /opt/spiderfoot/ && cd /opt/spiderfoot
wget http://sourceforge.net/projects/spiderfoot/files/spiderfoot-2.3.0-src.ta
r.gz/download
tar xzvf download
pip install lxml
pip install netaddr
pip install M2Crypto
pip install cherrypy
pip install mako
```

WCE (Windows Credential Editor)

メモリからパスワードを抜き出すために使用されるツール。以下のサイトからダウンロードし、

`http://www.ampliasecurity.com/research/windows-credentials-editor/`

たとえば以下の方法で`/opt`に保存してください。

```
wget www.ampliasecurity.com/research/wce_v1_4beta_universal.zip
mkdir /opt/wce && unzip wce_v1* -d /opt/wce && rm wce_v1*.zip
```

Mimikatz

メモリ、ゴールデンチケット、スケルトンキーなどから平文のパスワードを抽出するためのツール[†18]。

```
cd /opt/ && wget http://blog.gentilkiwi.com/downloads/mimikatz_trunk.zip
unzip -d ./mimikatz mimikatz_trunk.zip
```

†18 [訳注] 有名な攻撃ツールなので、ChromeやFirefoxでアクセスするとセキュリティ警告が表示される。

SET (Social-Engineer Toolkit)

ソーシャルエンジニアリングに使用されるツール。

```
git clone https://github.com/trustedsec/social-engineer-toolkit/ /opt/set/
cd /opt/set && ./setup.py install
```

PowerSploit

エクスプロイト後に使用される PowerShell スクリプト。

```
git clone https://github.com/mattifestation/PowerSploit.git /opt/PowerSploit
cd /opt/PowerSploit && wget https://raw.githubusercontent.com/obscuresec/random/ \
master/StartListener.py && wget https://raw.githubusercontent.com/darkoperator/ \
powershell_scripts/master/ps_encoder.py
```

Nishang

エクスプロイトの前後に使用される PowerShell スクリプト。

```
git clone https://github.com/samratashok/nishang /opt/nishang
```

Veil-Framework

検出を回避することに的を絞った攻撃側のツールキット。本書 (原書) の執筆時点では、アンチウイルスの検知を回避するペイロードを生成する Veil-Evasion、それらをターゲットに送信する Veil-Catapult、Windows ドメインで状況を把握する Veil-PowerView が含まれています。Veil は Python ベースの Meterpreter 実行ファイルの作成に使用されます。

```
git clone https://github.com/Veil-Framework/Veil /opt/Veil
cd /opt/Veil/ && ./Install.sh -c
```

Burp Suite Pro

Web 侵入テストツール。`http://portswigger.net/burp/proxy.html` からダウンロードできますが、Professional Edition の購入を強くお勧めします。349 ドルの価値は十分にあります。

OWASP ZAP (Zed Attack Proxy)

Web アプリケーションの脆弱性を発見するための使いやすい統合侵入テスト。`https://github.com/zaproxy/zaproxy/wiki/Downloads` からダウンロードできます。Kali Linux にはデフォルトで含まれています (owasp-zap)。

SecLists

Burp と一緒に使用することでパラメータをファジング[†19]するためのスクリプト。

---

†19 [訳注] ソフトウェアの脆弱性を発見するためのテスト手法の 1 つ。

```
git clone https://github.com/danielmiessler/SecLists.git /opt/SecLists
```

パスワードリスト

さまざまなパスワードリストについては、第9章を参照してください。

Net-Creds ネットワーク解析

ユーザー名とパスワードを捕捉したPCAPファイルを解析するツール。

```
git clone https://github.com/DanMcInerney/net-creds.git /opt/net-creds
```

Firefox アドオンのインストール

- Web Developer アドオン

  `https://addons.mozilla.org/en-US/firefox/addon/web-developer/`

- Tamper Data

  `https://addons.mozilla.org/en-US/firefox/addon/tamper-data/`

- Foxy Proxy

  `https://addons.mozilla.org/en-US/firefox/addon/foxyproxy-standard/`

- User Agent Switcher

  `https://addons.mozilla.org/en-US/firefox/addon/user-agent-switcher/`

Wifite

Wi-Fi ネットワークに対する攻撃ツール。

```
git clone https://github.com/derv82/wifite /opt/wifite
```

WifiPhisher

自動Wi-Fi フィッシングツール。

```
git clone https://github.com/sophron/wifiphisher.git /opt/wifiphisher
cd /opt/wifiphisher && python setup.py install
```

フィッシング（オプション）

- Phishing Frenzy

```
git clone https://github.com/pentestgeek/phishing-frenzy.git \
/var/www/phishing-frenzy
```

- 追加のカスタムリスト

```
git clone https://github.com/macubergeek/gitlist.git /opt/gitlist
```

本書の Web サイトで更新情報を確認してください。

http://thehackerplaybook.com/updates/

6. Windows VM

Windows 10/8/7 の仮想マシン（VM）もぜひ構成しておいてください。というのも、筆者が行ってきた数々のテストでは、アプリケーションが Internet Explorer や Cain & Abel などのツールを要求するからです —— これらは Windows でしか動作しません。PowerShell を使った攻撃はどれも、Windows ホストでコマンドを実行することを要求します。複数の OS を用意しておけば、多くの時間や手間が省けます。そう考えると、常に万が一に備えておくことが重要となります。

◈ Windows に追加するツール

- HxD（バイナリエディタ）
- Evade（アンチウイルス検知回避に使用）
- Hyperion（アンチウイルス検知回避に使用）
- Metasploit
- Nexpose/Nessus
- Nmap
- oclHashcat
- Cain & Abel
- Burp Suite Pro
- Nishang
- PowerSploit
- Firefox アドオン（15 ページを参照）
  - Web Developer アドオン
  - Tamper Data
  - Foxy Proxy
  - User Agent Switcher

7. Windows のセットアップ

Windows の共通テストプラットフォームをセットアップしておけば、Kali Linux ホストを補完するのに役立つはずです。検査に引っかかるわけにはいきませんから、ホスト名を変更し、NetBIOS が必要でなければ無効にし、これらのマシンをできるだけ頑健な状態にしておいてください。

Windows で特にセットアップしておくものはありませんが、通常、筆者は以下のツールをインストールすることにしています。

- HxD

  `http://mh-nexus.de/en/hxd/`

- Evade

  `https://www.securepla.net/antivirus-now-you-see-me-now-you-dont`

- Hyperion

  `http://www.nullsecurity.net/tools/binary.html`

  Windows コンパイラをダウンロードしてインストールします。解凍後の `Hyperion` フォルダで `make` を実行すると、バイナリが生成されるはずです。

  `http://sourceforge.net/projects/mingw/`

- Metasploit

  `http://www.metasploit.com/`

- Nessus または Nexpose

  `http://www.tenable.com/products/nessus-vulnerability-scanner`

  `https://www.rapid7.com/jp/products/nexpose/`

  どちらかをダウンロードしてインストールします。ソフトウェアを購入する場合は Nessus のほうが手頃な価格ですが、どちらでもうまくいきます。

- Nmap

  `http://nmap.org/download.html`

- oclHashcat

  `http://hashcat.net/oclhashcat/`

- Cain & Abel

  `http://www.oxid.it/cain.html`

- Burp Proxy Pro

  `http://portswigger.net/burp/download.html`

- Nishang

  `https://github.com/samratashok/nishang`

- PowerSploit
  `https://github.com/mattifestation/PowerSploit/`
- Firefox アドオン（15 ページを参照）
  - Web Developer アドオン
  - Tamper Data
  - Foxy Proxy
  - User Agent Switcher

8. PowerShell によるパワーアップ

PowerShell によって侵入テストはまさに様変わりしています。PowerShell を使ったことがない場合は、ぜひ空いた時間に基本的な PowerShell スクリプトを書いてみてください。PowerShell を使い始めるにあたって手助けが必要な場合は、以下のビデオを観てください。

- Intro to PowerShell Scripting for Security
  `http://www.irongeek.com/i.php?page=videos/hack3rcon5/h01-intro-to-powershell-scripting-for-security`

ちょっと長いビデオですが、PowerShell を使い始めるのに必要な基礎が身につくはずです。

本書が PowerShell にこれほど注目するのはなぜでしょうか。PowerShell には、侵入テストに対して以下のメリットがあります。

- Windows 7 以降のマシンにデフォルトでインストールされている
- PowerShell スクリプトはメモリ内で実行できる
- アンチウイルスソフトを起動させることがほとんどない
- .NET Framework のクラスを利用
- （Active Directory へのクエリに）ユーザーの認証情報を利用する
- Active Directory の管理に使用できる
- PowerShell スクリプトをリモートで実行できる
- Windows への攻撃をスクリプト化するのがはるかに容易になる
- 現在、PowerShell には多くのツールが組み込まれており、PowerShell を理解すれば、侵入テストの腕が上がり、効率がよくなる

Windows のコマンドプロンプトに `powershell` と入力すれば、PowerShell のコマンドレットをいつでも実行できます。PowerShell を起動した後は、`help` と入力することで、ヘルパーメニューを表示でき

試し読みはお楽しみ
いただけましたか？

ここからはManatee
おすすめの商品を
ご紹介します。

Tech Book Zone Manatee

3.10
2017

おすすめ電子書籍

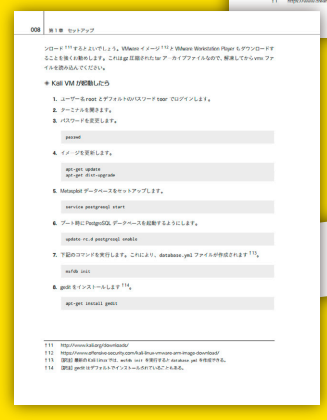
Tech Book Zone Manatee

1

セキュリティのプロなら必読!
敵の手の内を知るテクニック

情報システムのセキュリティを考えるとき、敵を知らないと防御できません。昨今は攻撃者視点での安全性評価の重要性が認知され、自分達のシステムに対してセキュリティテストを実施する組織が増えています。『サイバーセキュリティテスト完全ガイド』は、攻撃者がどのような手口でシステムへの侵入を試みるのか、脆弱性を探すのかという視点でシステムの見方を紹介。セキュリティテストに直接携わらない開発者にも有用な一冊です。

さまざまな攻撃によって自分達のシステムの情報がどこまで暴かれてしまうかを知ろう



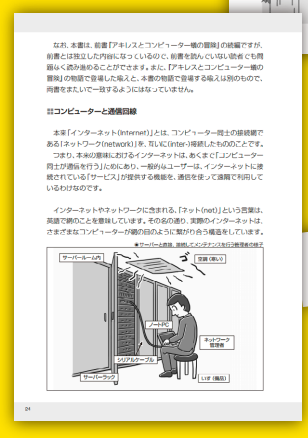
自らの技術力や知識レベルを磨き上げる日々の修練にも役立つ内容

2

インターネットに進入したハッカーを追跡!

本書では寓話的な物語＋解説の形で、インターネットの動作原理を技術的下地がなくてもわかるように説明しています。主人公のアキレスとネットワークに詳しい不思議な蜘蛛が、ハッカー（クラッカー）であるカピバラを追いかけるという物語を通じて、パケットによる通信、プロトコル、さまざまなサービス、クラウド、公開鍵といった技術の仕組みを解説。また、そこに潜む危険性など、セキュリティについても取り上げています。

アキレスと蜘蛛のストーリーが、ネットワーク技術の理解をサポート!



物語の出来事をネットワークの仕組みに当てはめて詳細に解説

「サーバ・クラウド技術」

セキュリティ

サイバーセキュリティテスト完全ガイド

マイナビ出版
Peter Kim（著者）、
株式会社クイープ（翻訳）、
保要隆明・前田優人・美濃圭佑・八木橋優（監訳）
400 ページ　価格：3,650 円（PDF）

セキュリティ

ネットワークをめぐるアキレスの冒険
インターネットの動作原理とセキュリティの基礎知識

シーアンドアール研究所
坂本俊之（著者）
価格：2,070 円（PDF・EPUB）

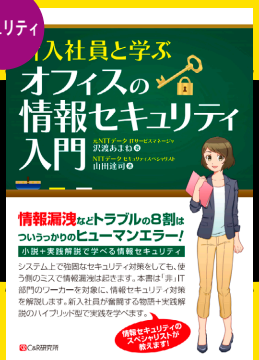
Tech Book Zone Manatee

「サーバ・クラウド技術」

3.10 2017

「ものがたり」と「解説」で情報セキュリティを知る

セキュリティ



3

新入社員と学ぶ オフィスの情報セキュリティ入門

注目を集めている情報セキュリティについて、非 IT 部門一般社員ができることを中心に、わかりやすく解説。本書は小説と解説のパートにわかれており、小説を楽しく読みながら、情報セキュリティについて学べます。

シーアンドアール研究所
沢渡あまね・山田達司(著者)
280 ページ　価格：1,750 円(PDF)

AWS を活用するノウハウを現場のエンジニアが解説！

クラウド

4

効果的な導入・運用のための Amazon Web Services 活用入門

開発現場での導入が進む「アマゾン ウェブ サービス(AWS)」。本書は、AWS の日本ユーザーグループである JAWS-UG のメンバーが多く集まって執筆しました。まさに現場の導入と運用のノウハウがつまった 1 冊です。

マイナビ出版
420 ページ　価格：3,229 円(PDF)

OpenStack で構築するプライベートクラウド

クラウド

5

OpenStack 徹底活用テクニックガイド

業界標準のクラウド OS である OpenStack で、プライベートクラウドを構築する際のポイントを丁寧に解説。企業や団体といった IT 利用者の視点で、OpenStack がどのようにシステム開発や運用に役立つのかがわかります。

シーアンドアール研究所
澤橋松王(著者)
264 ページ　価格：3,577 円(PDF・EPUB)

Windows コンテナー技術を基礎から理解できる

ネットワーク

6

Windows コンテナー技術入門

Windows コンテナーの基本的な概念とシステム構築についてハンズオン形式で解説。コマンドや手順の紹介だけでなく、技術の生まれた背景、チーム開発・運用の実際など、現場で役立つ情報も数多く盛り込みました。

インプレス
真壁徹(著者)
208 ページ　価格：2,700 円(PDF)

nginx を活用するための幅広いノウハウを凝縮

ネットワーク

7

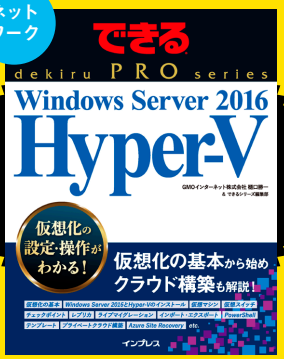
nginx 実践ガイド

nginx を使って Web アプリケーションを構築・運用する際、動作の検証方法や、Web システムの中で nginx と直接関係ない部分も解説しました。ネットワーク全般やネットワークプログラムの動作に関する知識が得られます。

インプレス
渡辺高志(著者)
280 ページ　価格：3,024 円(PDF)

本格的な仮想環境を Hyper-V で構築！

ネットワーク



8

できる PRO Windows Server 2016 Hyper-V

Windows Server 2016 Hyper-V は、クラウドの実現に不可欠です。本書では仮想化の基礎知識から、Hyper-V での仮想マシンや仮想スイッチの設定・操作、プライベートクラウドの構築、Azure との連携などを解説します。

インプレス
樋口勝一・できるシリーズ編集部(著者)
344 ページ　価格：3,456 円(PDF)