実践 Metasploit

ペネトレーションテストによる脆弱性評価

David Kennedy, Jim O'Gorman
Devon Kearns, Mati Aharoni 著

青木 一史、秋山 満昭、岩村 誠
川古谷 裕平、川島 祐樹、辻 伸弘 監訳
宮本 久仁男

岡 真由美 訳

O'REILLY®
オライリー・ジャパン

METASPLOIT

The Penetration Tester's Guide

by David Kennedy,
Jim O'Gorman, Devon Kearns,
and Mati Aharoni

no starch
press

San Francisco

Title of English-language original: Metasploit: The Penetration Tester's Guide, ISBN978-1-59327-288-3, published by No Starch Press.

推薦の言葉

本書の内容である脆弱性テスト手法は、既存または新規の情報システムの脆弱性をチェックするために世界で広く使われている手法であって、本書では、その必要性、テスト実施方法、利用上の注意などが詳しく解説されている。さらに、本書内では、世の中で開発・使用されるシステムやソフトウェアをより信頼できるものとしていくために必要な手段が随所に紹介されている。

従来、このような本は日本国内ではほとんど発行されておらず、まさに望まれていた一冊である。

このような脆弱性テスト手法は、情報システムの脆弱性をチェックして、より強固でセキュアなシステムを実現する具体的な手段として、情報システムの設計・構築・運用に携わる技術者に大変有用なものである。また、現実にこのようなテストを実施する技術者のみならず、今後の時代を担う学生や技術者にとっても、情報システムの守るべきポイントを具体的に把握するという意味で重要である。

一方、このような技術は攻撃者側も使えるが、この書物を発刊することは、彼らよりはるかに多い一般技術者や学生に対する教育となり、攻撃に対抗する非常に大きな基盤となり得る。今後、世界からのさまざまな脅威に対応するにはこの種の知識は不可欠であり、知らないでは済まされない。本書の有効活用を期待したい。

2012年4月
情報セキュリティ大学院大学 学長
田中 英彦

監訳者まえがき

はじまりはいつも何気ない一言から、というのをこれほど思い知ったことはない……ある日、オライリー・ジャパンの宮川さんから問いかけがあったのが本書の原書『Metasploit: The Penetration Tester's Guide』だった。

宮川さん：「この本、どうでしょう？」
私：「すっごくいいじゃないですか！　オレもこういう本、欲しかったんですよ！」

今から思えば、この一言が暗黙の契約だったとしか思えない。

Metasploitといえば、知ってる人からしたら「脆弱性テストの定番ツール」というくらいにメジャーなものだ。しかし、その高機能さと（ある意味）危なさっぷりからか、まともに使い方を紹介している雑誌は僅少であり、書籍にいたっては絶無といっても過言ではない状態が続いていた。どの程度危ないかというと、Metasploitのアーカイブが、ウイルススキャナにより検知される程度なのだが。そんな状態を知る私が「こんな本が欲しかった」と言ったとして、それはもはや「しかたがない」としか表現できないと思う……

とはいえ、言ってしまった者としてはその責を全うすべく、「この人たちなら大丈夫」と確信する方々に、監訳者になっていただくべく声をかけた。その結果、今回の監訳者メンバーが集まったわけである。監訳作業そのものも紆余曲折あったが、なんとか本書を手に取っていただいてる読者の方に届けることができるようになった。

腕利きの技術者が監訳・検証し、正しく動作することを確認した本書の内容は、ペネトレーションテスターを目指す人にも、熟練の技術者にも、きっと役立つものであると確信している。

本書の使い方と注意

聡明な読者諸氏はすでにお気づきだと思うが、冒頭で書いたとおり、Metasploitはそれ自体がウイルススキャナに検知されるツールである。正しく使えばよいという話はあるが、Metasploitを用いる

ことで、ちょっと凝った攻撃も容易に実行できてしまうという側面も有している。本書を読む方には、いろんな思惑があると思う。しかし、本書は決して悪用されることを期待して書かれたものではないし、原著者も監訳者も、そのようなことは決して期待していない。

また本書には、原書の内容に加え、「シェルコードを読み解く」というタイトルで日本語版オリジナルの巻末付録を収録した。アセンブリ言語の知識習得をするためのきっかけとして、本書を読み解くのもいいだろう。

その他、使い方を間違えると容易に自爆し得るという側面を持っているのもMetasploitの特徴であろう。このあたりにも留意してほしい。個人の環境だからかまわないという方もいるかもしれないが、壊れることを想定していない環境が壊れて復旧を強いられるというのは、本当に嫌なものである。

本書の内容が、読者の環境をセキュアなものにし、運用中のシステムや使用しているアプリケーションをよりセキュアなものにするのに役立つことを祈念している。

2012年4月19日
監訳者を代表して
宮本 久仁男

謝辞

青木より

今回このような企画に携わることができてとても光栄に思う。本書を検証するうえで相談に乗ってもらった監訳メンバーに感謝する。検証作業が一発でうまくいかなかったところもあったが、監訳メンバーのアドバイスのおかげでスムーズに進めることができた。また、拙著『アナライジング・マルウェア』に続いて編集を担当してもらった宮川さんに感謝。いつもギリギリまでバタバタしてしまいスミマセン。より良い形で本書を出版できたのは宮川さんにいろいろ調整していただいたおかげである。そして、本書の監訳を後押ししてくれたNTT研究所の方々に感謝。最後に、これまで私を支えてきてくれた両親、出産で大変な時期だったにもかかわらず私の仕事に理解を示してくれた妻の直穂子、笑顔で私を癒やしてくれる佳穂に感謝を伝えたい。いつもありがとう。

秋山より

いつも慣れ親しんでいるツールにこのような奥深さがあることに気づけたのは、本書の監訳に携わることができたおかげである。日本のセキュリティ業界の第一線をひた走る各監訳メンバーと仕事ができたことを誇りに思うと同時に、各メンバーをまとめ上げた宮本氏の実行力と宮川氏の腕力はまさに「仕事のお手本」であったと改めて感じた。特に私の担当パートではNTTデータ先端技術株式会社の辻氏・川島氏による技術的バックアップがなければここまでの完成度には至らなかっただろう。また、NTT SC研メンバーの幅広い活動をいつも承認し強力に支援してくれている針生剛男氏と八木毅氏、そして公私ともに温かく見守ってくれる方々に感謝の気持ちを伝えたい。

岩村より

いつも親身になって相談に乗ってくれる「僕らの兄貴」宮本さんに誘ってもらえたことを大変誇りに思う。辻さんと川島さんのプロ意識の高さや仕事に対する想いを垣間見ることで、とても大事なことを思い出しつつ、監訳の仕事に取り組むことができた。拙著『アナライジング・マルウェア』でもお世話になった宮川さんの敏腕っぷりに今回もいろいろと助けられた。多くの理解とサポートをいただいた職場の方々、息子の出来事を我がことのように喜んでくれる家族、いつもマイペースな夫を温かく見守ってくれる佳奈、そんなみんなのおかげでまた一冊の本ができあがった。ありがとう。

川古谷より

今回このような本の出版に携わる機会を作ってくれた宮本氏、オライリー・ジャパン編集部の宮川氏に感謝する。さまざまな締め切りに追われ、私ひとりだけ原稿の提出が遅れるなか、忙しい仕事の合間を縫って手伝ってくれた監訳メンバーにも改めて感謝の気持ちを送りたい。すばらしいメンバーで一緒に仕事ができたことを誇りに思う。本書の監訳を行う際、さまざまな面で協力してくれたNTT研究所の方々にもこの場を借りて感謝の気持ちを伝えたい。最後に、子育てに大変なところ、本書執筆を温かく見守ってくれた由恵さん、家に帰ると笑顔で迎えてくれる湊人くん、いつもありがとう。

川島より

本プロジェクトに携わることができて、とても嬉しく思う。まずは声をかけてくれた辻さんに感謝。近くにいながら仕事でかかわることは少ないけれど、これだけ話をして、共感し、ときには議論をぶつけ合いながら、一緒に笑い、尊敬し合える存在は後にも先にも辻さん以外に現れないのではといつも思う。今回の監訳も一緒にできて本当に楽しかった。そして、宮本さんはじめNTT SC研のみんなと刺激的な時間を共有できてとても嬉しかった。監訳チームを温かく、ときには厳しく支えてれた編集の宮川さんに感謝。最後に、毎日パソコンの画面に向かっている私に文句ひとつ言わず、笑顔で支えてくれる妻の芽久美、いつも本当にありがとう。

辻より

このようなプロジェクトにかかわらせていただいて本当に嬉しく思う。記事や講演資料を作っているときも同じような感覚がある。時間に追われつつ、辛くも楽しくもあるといった不思議な瞬間の連続である。そして、それが終わる頃にはいつも何人かの顔が浮かんでくる。今回も同じだった。10年と少し前に東京に出てくるきっかけをくれた渡辺勝弘さん、裕美さん。記事を書くきっかけを作ってくれた柿澤誠さん、宮田健さん、高橋睦美さん。いつも、遊びに付き合ってくれて、援護射撃をしてくれる検査チームのみんな。いつも、ボクの相方をしてくれて刺激となってくれる川島祐樹さん。いつも、けしかけてくれた長倉明日香さん。そして、一番手がかかる時期にボクを育ててくれた母、彼氏とのデートなのにボクを遊びに連れて行ってくれた母、やっと一緒に住めたのにすぐに出て行くボクを許してくれた母、そんな3人の母。みんな、ありがとう。

宮本より

本書を監訳するにあたり、多くの方々から支援を賜った。本書を監訳するきっかけを作ってくれて、そのあともマネジメントに不慣れな私の手助けをしてくれた編集の宮川さんに感謝。本書の監訳にかかわることを快諾して支援してくれた、日本電信電話株式会社 セキュアプラットフォーム研究所、NTTデータ先端技術株式会社 セキュリティ事業部、株式会社NTTデータ 技術開発本部セキュリティ技術センターおよびNTTDATA-CERTの方々に感謝。できの悪い弟子からの申し出を快諾いただいた、情報セキュリティ大学院大学の田中英彦学長に感謝。そして、日々の「あたりまえ」に感謝。気のおけない友人や同僚、そして家族と過ごす日常が、私自身の支えになっている。ありがとう。

序文

情報技術は複雑な分野であり、陳腐化した過去の技術と、新たに増え続ける多種多様なシステム、ソフトウェア、プロトコルが散乱している。今日の企業ネットワークの保護には、単なるパッチ管理やファイアウォール、ユーザー教育以上のものが関連してくる。何が機能して何が機能しないのか、頻繁かつ実務的な検証が求められるのだ。要するにこれがペネトレーションテストなのである。

ペネトレーションテストは他に類を見ない、やりがいのある仕事だ。犯罪者のように思考し、自分に有利になるようにゲリラ戦術を用い、非常に複雑な防御網の中から最も弱い部分を見つけることに対し、報酬が支払われる。発見する内容は驚きに満ちているとともに、憂慮すべきことでもある。ペネトレーションテストは、不謹慎なポルノサイトから、大規模な詐欺や犯罪活動までを暴露してきた。

ペネトレーションテストとは、組織のセキュリティに対する認識を無視し、そのシステムの弱点を証明することである。うまくいったペネトレーションテストで得られたデータは、アーキテクチャレビューや脆弱性評価では特定できなかった問題をあぶり出せることが多い。共有パスワードや相互接続ネットワーク、暗号化されていない重要データの山などは、テストで見つかる典型的なものだ。ずさんなシステム管理とやっつけ仕事の実装が作り出す問題が、組織に大きな脅威を突きつける一方、管理者が実施すべき大量のタスクのもとで、解決方法は放置されたままとなっている。ペネトレーションテストは、他へ追いやられた優先事項を明らかにし、本物の侵入から身を守るために組織がすべきことを明確にする。

ペネトレーションテスターは、企業の最も重要なリソースを取り扱う。間違った行動を取れば、現実世界に悲惨な結果をもたらし得る領域にアクセスするのだ。たった1つのパケットを間違った場所に送り込むだけで工場は休止し、1時間当たりの損失は数百万ドルにもなる。適切な担当者への報告を怠れば、地元警察とバツの悪い、みっともない会話を交わす羽目になるだろう。経験豊富なセキュリティ専門家でもテストを躊躇するのが、医療システムである。OpenVMSメインフレーム上で患者の血液型が混同されたり、Windows XPが動作するレントゲン機器でメモリが破損したりする事故の責任を取りたい人間などいない。重要なシステムほど暴露されやすいというのに、セキュリティパッチを当てるためにデータベースサーバーを落とし、障害を引き起こすリスクを背負いたいシステム管理者など存在しない。

使用可能な攻撃経路の利用と、それによって生じるダメージに起因するリスクとのバランスを取ることこそ、ペネトレーションテスター全員が磨くべき技術である。このプロセスは、ツールとテクニックの技術的知識のみならず、その組織がどのようにシステムを運用しているのか、最も容易な通り道がどこに存在するのかに関する造詣の深さにかかっている。

本書では、多岐にわたる経歴を持つ4人のセキュリティ専門家の目を通して、ペネトレーションテストを見ていくことになる。著者には、企業のセキュリティのトップから、地下活動のようなエクスプロイト開発の開拓時代や脆弱性リサーチまでを経験した人間が含まれている。ペネトレーションテストやセキュリティ評価についての解説書は数多く出版されているし、ツールに特化した本も多い。しかし本書は両者のバランスを取り、基本的なツールとテクニックをカバーしながらも、成功するペネトレーションテストプロセスの全体的な構造の中でそれらをどう役立てるかを説明している。熟練したペネトレーションテスターは、最近体系化された、Penetration Test Execution Standard（PTES）に基づく方法論の解説からメリットが得られる。この分野に慣れていない読者は、どう着手するかだけでなく、なぜこれらのステップが重要なのか、全体図から見た場合どういう意味を持つのかといった豊富な情報を目にするだろう。

本書はMetasploit Frameworkに焦点を当てている。このオープンソースプラットフォームは、常に更新されるエクスプロイトの一貫した、信頼性の高いライブラリを提供し、新たなツールを構築するとともに、ペネトレーションテストをすべての角度から自動化する、完全な開発環境をもたらす。Frameworkの商用版であるMetasploit Expressと Metasploit Proもまた、本書で紹介されている。これらの製品は、大規模なペネトレーションテストをどのように実行し、自動化するかにおいて、異なる視点を提供する。

Metasploit Frameworkは、恥ずかしながら発展途上のプロジェクトである。開発者のコアなグループや、コミュニティの数多くの協力者からの送信によって、コードベースは日に数十回も更新されている。Frameworkについての本を執筆するなど、とても自虐的な試みである。ある章が校正される頃には、内容はすでに時代遅れかもしれない。しかし、読者の手元に本書が届いた時点でまだ内容が適切であるよう、著者らは本書の執筆に相当な苦労を重ねてきた。

本書にかかわったMetasploitチームは、コードの変更が正確に反映され、最終的な結果がMetasploit Frameworkのゼロデイをカバーできるよう、可能な限り努力している。今日入手可能なMetasploit Framework解説書として、本書は最良のものであると確信しており、しばらくはそうであり続けるだろう。本書が仕事に役立ち、読者諸氏の今後の取り組みにおいてよき参考資料となることを願ってやまない。

The Metasploit Project創設者
HD Moore

まえがき

Metasploit Frameworkは、情報セキュリティ専門家によって最も広く使われているツールの1つとなって久しいが、ソースコードそのものやブログなどのコメントを除けば、それについて書いたものは長い間ほとんど存在しなかった。しかしOffensive SecurityがオンラインコースのMetasploit Unleashedを開発したことにより、この状況は劇的に変わった。コース開設後まもなくNo Starch Pressが、Metasploit Unleashedでの仕事を拡大すべく、本書発行の可能性について連絡してきたのだ。

本書はMetasploit Frameworkの長所／短所と、Metasploit Frameworkをフル活用するための方法を教えるように構成されている。本書がカバーする範囲は精選されており（すべてのプラグインやエクスプロイトをカバーしているわけではないところに注意）、現在および将来のMetasploitを理解し、使いこなすために必要な基礎を網羅している。

本書の執筆を開始したとき、Metasploit Frameworkの開発者であるHD Mooreのコメントが頭に浮かんだ。Metasploit Unleashedコースの開発についてHDと話したとき、我々のひとりが彼に「コースがうまくいくといいのですが」と言った。するとこの何気ないコメントに対しHDは「それなら確実にうまくいくようにしよう」と返答したのだ。それが本書で達成しようとしていることだ。

我々は、日々 Metasploitを利用してセキュリティコントロールを回避し、保護を迂回し、システムを組織的に攻撃している熟練したペネトレーションテスターのグループである。読者が有能なペネトレーションテスターになる手助けをするために本書を執筆した。HDの品質への意欲と集中は、Metasploit Framework内に明白に存在しており、本書もその持ち味に合わせようと努力した。この基準に我々がどこまで合わせることができたかの判断は、読者に任せたい。

はじめに

それほど遠くない将来、攻撃者が多国籍企業のデジタル資産を攻撃しようと決め、数百万ドルのインフラの背後にある何億ドルもの知的財産にターゲットを絞ったと想像してみよう。攻撃者はもちろん、Metasploitの最新バージョンの起動から始めるだろう。

ターゲットの周辺を調べたら、弱点を見つけ、秩序だった一連の攻撃を開始する。しかしネットワークへのほぼすべての角度からの侵害を終えても、お楽しみは始まったばかりだ。攻撃者はシステム内を探り、会社を動かしている、中核となる重要なビジネスコンポーネントを見つけ出す。キーを1回叩くだけで、会社の数百万ドルを自由にし、すべての機密データを漏洩させることができるのだ。

これで仕事は成功した。おめでとう。ビジネスに大きな影響を与えたところで、今度は報告書を作成する番だ。おかしな話だが、今日のペネトレーションテスターは、上で説明したような仮想敵の役割を自ら務め、高度なセキュリティを必要とする企業のリクエストで、合法な攻撃を実行しているのである。ペネトレーションテストの世界とセキュリティの将来へようこそ。

ペネトレーションテストを行う理由

企業は重要なインフラを守り、防御の抜け穴を見つけ、深刻なデータ侵害を防ぐために、セキュリティプログラムに数百万ドルを投じている。ペネトレーションテストはこれらのプログラムにおけるシステムの弱点と欠陥を識別する、最も有効な方法の1つだ。セキュリティコントロールの回避と、セキュリティメカニズムの迂回を試みることで、ペネトレーションテスターは、ハッカーが組織のセキュリティを侵害し、組織全体に損害を与えるであろう手法を識別することができる。

本書を読み進めるとき、1つのシステム、あるいは複数のシステムをターゲットとする必要はないことを覚えておいてほしい。攻撃者が組織にどのように深刻な被害を与える可能性があるか、またその影響はどの程度のものかを安全かつ統制の取れた方法で示すことは無論だが、収益を上げ、評判を守り、顧客を守ることが、最終的な目標なのである。

Metasploitを使う理由

Metasploitは単なるツールではない。平凡な、繰り返しの、複雑なタスクを自動化するのに必要なインフラを提供する、完全なフレームワークである。そのおかげで独自の、またはある面に特化したペネトレーションテストに専念し、情報セキュリティプログラム内のフローを識別することが可能になるのである。

本書を読み進め、方法論が確立されると、自分のペネトレーションテストでMetasploitを活用する方法がわかってくる。Metasploitを使うと、より高度な攻撃を作成、実行するのに、エクスプロイト、ペイロード、エンコーダなどを増やす攻撃ベクターを簡単に構築することができる。本書の各所で、Metasploit Frameworkを基盤とするいくつかのサードパーティ製ツール（筆者が作成したものも含む）について説明する。本書の目的は、Metasploit Frameworkに慣れてもらい、いくつかの高度な攻撃のサンプルを見て、これらのテクニックを責任を持って利用してもらうことである。筆者が執筆を楽しんだのと同様、本書を楽しんで読んでもらえることを願っている。ではお楽しみを始めよう。

Metasploitの簡単な歴史

Metasploitはもともと、当時セキュリティ会社に勤めていたHD Mooreが思いつき、開発したものだ。公開されているエクスプロイトコードの検証とサニタイズに大半の時間を費やしていることに気づいたHDは、エクスプロイトの作成と開発のための、柔軟かつメンテナンス可能なフレームワークの作成を始めた。2003年10月にリリースしたPerlベースの初のMetasploitは、計11のエクスプロイトをサポートしていた。

Spoonmの支援を得たHDは、最初のものを完全に書き換えた新版Metasploit 2.0を2004年4月にリリースした。同バージョンは19のエクスプロイトと27以上のペイロードに対応。このリリース後まもなく、Matt Miller（Skape）がMetasploit開発チームに加わった。プロジェクトの認知度が高まるにつれ、Metasploit Frameworkは情報セキュリティコミュニティから強い支持を得るようになり、急速にペネトレーションテストとエクスプロイトの必須ツールとなっていった。

Rubyプログラミング言語で完全に書き直した後、Metasploitチームは2007年にMetasploit 3.0をリリースした。PerlからRubyへとFrameworkを移行するのに、15万行を超える新たなコードの記述と、18か月間もの歳月が必要だった。3.0のリリースにより、Metasploitはセキュリティコミュニティでより広く受け入れられ、ユーザーへの貢献度も大きく向上した。

2009年秋、脆弱性スキャニング市場を主導するRapid7がMetasploitを買収。これによりHDは、Metasploit Frameworkの開発に特化したチームを持つことができるようになった。買収以降は、人々の想像を上回る迅速さで更新が行われている。Rapid7はMetasploit Frameworkを基盤とした2種類の商用版、Metasploit ExpressとMetasploit Proをリリースした。Metasploit ExpressはGUIを備え、報告書作成などの便利な機能を追加、機能性が向上したMetasploit Frameworkの簡易版。Metasploit ProはMetasploit Expressの拡張版で、コラボレーションとグループペネトレーションテストを特徴とし、1クリックでのVPNトンネル設定などが可能となっている。

本書について

本書はMetasploit Frameworkの基礎から、エクスプロイトの高度なテクニックに至るすべてを教えられるように構成されている。初心者には役に立つチュートリアルを、熟練者にはクイックリファレンスを提供するのが本書の目的である。しかし常に手を引いて導くわけにはいかない。ペネトレーションテストの分野では、プログラミングに関する知識は間違いなく強みであり、本書の多くの例でもRubyまたはPython言語を使っている。高度なエクスプロイトや攻撃のカスタマイズに役立てられるよう、RubyやPythonなどのプログラミング言語を学習することを推奨はするものの、プログラミング言語の知識は必須ではない。

Metasploitにもっと慣れてくると、Metasploit Frameworkが新機能やエクスプロイト、攻撃などで頻繁に更新されているのに気づくだろう。本書は、Metasploitは絶えず変化しており、この迅速な開

発についていくことができる印刷物は存在しないという認識に基づいて書かれている。そのため本書は、基本を重視している。Metasploitがどう機能するかをいったん理解すれば、Frameworkの更新にすぐに追いつけるからだ。

本書の内容

これから始める場合、あるいは次のレベルへとスキルを向上させたい場合、本書はどう役立つのだろうか。各章はその前の章をもとに書かれているので、ペネトレーションテスターが一から基礎を積み上げるように、スキルを積み上げていくのに役立てることができる。

1章 ペネトレーションテストの基本

1章ではペネトレーションテストにまつわる方法論を確立する。

2章 Metasploitの基本

2章はMetasploit Framework内のさまざまなツールへの導入部である。

3章 インテリジェンスギャザリング

3章ではペネトレーションテストの予備調査段階でのMetasploit活用法を示す。

4章 脆弱性スキャン

4章では脆弱性の識別と脆弱性スキャン技術の活用について解説する。

5章 エクスプロイトを楽しもう

5章ではエクスプロイトを実際に体験する。

6章 Meterpreter

6章ではポストエクスプロイトの十徳ナイフであるMeterpreterについて解説する。

7章 検出の回避

7章ではアンチウイルス回避テクニックの基礎概念に集中する。

8章 クライアントサイド攻撃を用いたエクスプロイト

8章ではクライアントサイドのエクスプロイトとブラウザのバグをカバーする。

9章 Metasploit Auxiliaryモジュール

9章ではauxiliaryモジュールについて解説する。

10章 Social-Engineer Toolkit

10章ではソーシャルエンジニアリング攻撃でのSocial-Engineer Toolkitの使い方について解説する。

11章 Fast-Track

11章では自動ペネトレーションテストフレームワークFast-Trackについて解説する。

12章 Karmetasploit

12章では無線LAN攻撃用のKarmetasploitの使い方について解説する。

13章 独自モジュールの構築

13章では独自のエクスプロイトモジュールの構築方法について解説する。

14章 独自エクスプロイトの作成

14章ではファジングとバッファオーバーフローからエクスプロイトモジュールを作成する方法について解説する。

15章 Metasploit Frameworkへのエクスプロイトの移植

15章では既存のエクスプロイトをMetasploitベースのモジュールへ移植する方法を詳しく見ていく。

16章 Meterpreterスクリプティング

16章では独自のMeterpreterスクリプトの作成方法について解説する。

17章 ペネトレーションテストのシミュレーション

17章ではペネトレーションテストのシミュレーションを通じて、すべてをまとめて見ていく。

付録A ターゲットマシンの設定

付録Aでは本書の例を試すためのテスト環境を設定する方法について解説する。

付録B 早見表

付録BはMetasploitのさまざまなインターフェイスとユーティリティでよく使われるコマンドと構文のリファレンスである。

付録C シェルコードを読み解く

付録Cは監訳者による日本語版オリジナルの記事である。本書で利用されたシェルコードを1つピックアップし、シェルコードの内部構造について詳しく解説する。

倫理上の注意

本書を執筆した目的は、読者がペネトレーションテスターとしてのスキルを向上させる手助けをすることだ。ペネトレーションテスターとしてセキュリティ規則を無視することになるが、それはあくまで仕事の一部である。規則を無視する場合でも、以下のことを心に留めておこう。

- 悪意を持たない

- 愚かにならない
- 書面で許可を得ることなくターゲットを攻撃しない
- 自分の行動が招く結果を考慮する
- 違法行為を行えば、逮捕、刑務所行きである

本書の著訳者および発行者は、本書で説明されているペネトレーションテスト技術の不正な利用を容認せず、また一切推奨しない。本書の目的は、読者を賢くすることであり、トラブルに巻き込むことではない。もしトラブルに巻き込まれても、我々は助けられないからだ。

本書の表記

本書は、以下の表記を使用する。

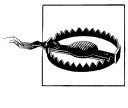
太字（Bold）
: 新しい用語、強調やキーワードフレーズは太字で表記する。

等幅（`Constant Width`）
: プログラムのコード、コマンド、配列、要素、文、オプション、スイッチ、変数、属性、キー、関数、型、クラス、名前空間、メソッド、モジュール、プロパティ、パラメータ、値、オブジェクト、イベント、イベントハンドラ、XMLタグ、HTMLタグ、マクロ、ファイルの内容、コマンドからの出力は、等幅で表記する。

等幅太字（`Constant Width Bold`）
: ユーザーが入力するコマンドやテキストは、等幅太字で表記する。重要な部分を強調するために使う場合もある。

等幅イタリック（*`Constant Width Italic`*）
: ユーザーが入力する値で置き換えられる部分は、等幅斜体で表記する。

このアイコンは、ヒントや提案や一般的注意事項を表す。



このアイコンは、警告や要注意事項を表す。

意見と質問

本書（日本語翻訳版）の内容については、最大限の努力をもって検証および確認しているが、誤りや不正確な点、誤解や混乱を招くような表現、単純な誤植に気づかれることもあるだろう。本書を読んで気づいたことは、今後の版で改善できるように知らせてほしい。将来の改訂に関する提案なども歓迎する。

株式会社オライリー・ジャパン
〒160-0002 東京都新宿区坂町26番地27 インテリジェントプラザビル1F
電話　03-3356-5227
FAX　03-3356-5261
電子メール　japan@oreilly.co.jp

本書に関する技術的な質問や意見については、次のあて先に電子メール（英文）を送ってほしい。

info@nostarch.com

本書に関連するファイルは本書のWebページからダウンロードできる。

http://www.oreilly.co.jp/books/9784873115382/
http://oreilly.com/catalog/9781593272883/（原書）
http://nostarch.com/metasploit.htm（原書）

監訳者のWebページには、正誤表や追加情報が掲載されている。以下のアドレスでアクセスできる。

https://sites.google.com/site/metasploitbook/

オライリーに関するその他の情報については、次のオライリーのWebサイトを参照してほしい。

http://www.oreilly.co.jp/
http://www.oreilly.com/

謝辞

この貴重なツールをコミュニティに提供するために懸命に働いてきた方々をはじめ、多くの方々に感謝したい。特にMetasploitチームのHD Moore、James Lee、David D. Rude II、Tod Beardsley、Jonathan Cran、Stephen Fewer、Joshua Drake、Mario Ceballos、Ramon Valle、Patrick Webster、Efrain Torres、Alexandre Maloteaux、Wei Chen、Steve Tornio、Nathan Keltner、Chris Gates、Carlos Perez、Matt Weeks、Raphael Mudgeに心から感謝する。Meterpreterスクリプティングの章の一部の記述を手伝ってくれたCarlos Perezにも心から感謝している。

本書のテクニカルレビュアーであるScott Whiteのすばらしさにもお礼を言いたい。

Offensive Securityには我々を団結させてくれたことに感謝する。Offensive Securityのモットーである「いっそうの努力」は、我々を元気づけたり、苦しめたりした（ryujinは悪魔だ）。

情報セキュリティのコミュニティにも感謝すべきメンバーは数多くいるが、名前を挙げるには多すぎて、誰かの名前を抜かしてしまう可能性が高い。だからセキュリティコミュニティの仲間たちに感謝するとともに、我々全員からハグを贈りたい。

No Starch Press全員の計り知れない努力には、特別な賛辞を送る。Bill、Alison、Travis、Tylerそして黒子として働いてくれたNo Starch Pressのその他全員と仕事をできたのは、心からの喜びだ。

最後に、我々の家族に心からありがとうと言いたい。我々全員が既婚者で、半数には子供がいる。キーボードをすり減らすほど時間を費やし、家族とは十分な時間を一緒に過ごせなかった。理解してくれて、ありがとう。このコードを更新したら埋め合わせするから…ちょっと待て、このメモリコラプションの原因を見つけたら、いや、この`svn update`を終えたら、いやいやこのファザー実行設定をしたら…

David Kennedy（Twitter: @dave_rel1k）より

本書を多くの人々に捧げたい。キーボードを夜遅くまで叩き続ける私に我慢してくれた、愛する妻のErin。私を若く、同時に年寄りにもしてくれる3人の子供たち。父のJimと母のJanna。そばにいてくれた継母のDeb。現在の私があるのは継母のおかげだ。本のために一生懸命働き、すばらしい友人でいてくれるJim、Dookie、Mutsにも感謝する。Offensive Securityのよき友たち。Chris "Logan" Hadnagy。兄のShawn Sullivan。そしてDiebold のみんな。そのセキュリティ業界への貢献が我々皆を元気づけている、よき友人HD Moore。友人全員、そして機会を与えてくれて、私を信頼してくれたScott Angelo。最後に、神の助けがなければ、なにひとつとして実現しなかっただろう。

Devon Kearns（@dookie2000ca）より

私ののめり込みをサポートするだけでなく勇気づけてくれた、美しく辛抱強い妻。君は私のインスピレーションであり、モチベーションだ。この道のりにおいて君がそばにいなければ、どこへもたどり着けなかっただろう。共著者のみんな、新参者を信頼し、仲間として歓迎してくれてありがとう。最後に、この愉快な一団をまとめてくれただけでなく、私にチャンスをくれたMatiに特に感謝したい。

Mati Aharoni（@backtracklinux）より

本書の共著者には特に感謝を贈りたい。その費やした時間と献身は本当に感動ものだ。Jim、Devon、Daveは、セキュリティ業界における本当にすばらしい友であり、仲間である。

Jim O'Gorman（@_Elwood_）より

Matteo、Chris "Logan"、そしてOffensive Securityの全員に感謝する。また、Robert、Matt、Chris、そしてStrikeForceの同僚にも心から感謝したい。そしてすばらしい妻、Melissa。君が手に持っている本が、私がいつも家事をさぼっていただけではない証拠だ。そしてJakeとJoe、仕事をしていると言ったのに、君たちとただゲームで遊んでいるだけだとお母さんに言うのはやめてほしい。君たち3人は、私の人生に相当な影響力を持っているのだから。最後に共著者のMati、Devon、Dave。本書に私の名前を載せてくれてありがとう。ただ家事をさぼっていただけなのに。

目次

コラム目次