Engineer

ペネトレーションテスト

🔓 許可を得た攻撃で、どの欠陥を悪用できるか確かめる試験

どのようなものか

ペネトレーションテストは、pentestとも略し、実際の攻撃をまねて、アプリケーション、システム、ネットワークのセキュリティー機能を回避する経路を探す検査です。NISTの情報セキュリティー試験・評価技術ガイドSP 800-115は、攻撃者と同じ道具や手法で、実際のシステムやデータに本物の攻撃を行うことも多いと説明します。セキュリティーとプライバシーの管理策を集めたSP 800-53 Rev. 5の短い定義は、通常、評価者が特定の制限の下で働くことも加えます。攻撃との違いはそこです。許可され、範囲を定め、開始前に書面で合意します。

ほかのセキュリティー試験と違うのは、目的です。脆弱性スキャナーは、見つけた状態を既知の欠陥の記述と比較し、何がありそうかを報告します。ペネトレーションテストの担当者は、その欠陥を実際に利用しようとします。SP 800-115は、スキャナーが脆弱性の存在の可能性だけを調べる一方、攻撃段階では悪用して存在を確認すると、明確に区別します。多くの試験は、一つか複数のシステム上の弱点を組み合わせ、単独より大きなアクセスを得る経路も探します。

OWASP Web Security Testing Guide（WSTG）は、ブラックボックステストや倫理的ハッキングとも呼ばれると記します。対象の内部設計を事前に知らず、外から攻撃者のように試しますが、一つ以上の有効な利用者アカウントを渡されることもよくあります。

どの試験にも、二つの選択があります。一つ目は開始位置です。外部試験は、範囲内のアドレス程度の情報だけで、ネットワークの外から始めます。内部試験は中から始め、通常は一般の従業員の権限で、権限昇格により先へ進もうとします。二つ目は、誰が知っているかです。SP 800-115は、公然と行うものをホワイトハット試験と呼び、IT担当者の認知と同意の下で実施します。秘密裏のもの、ブラックハット試験は、IT担当者に知らせず、ただし上級管理職の十分な認知と許可を得て行います。

SP 800-115は、作業を四段階に分け、認められる多くの分け方の一つだと脚注で補います。計画段階で規則を合意し、管理職の承認を文書に残し、目標を定め、試験自体は探索から始まります。探索では、対象の情報を集めてスキャンし、米国National Vulnerability Databaseなどの脆弱性データベースや、担当者自身の知識と照合します。ガイドが「あらゆるペネトレーションテストの核心」と呼ぶ攻撃段階では、候補の欠陥を一つずつ悪用しようとします。新しいアクセスが開けば、その位置から探索へ戻ります。報告は、三段階すべてと並行して行い、見つけた脆弱性、危険度、修正方法をまとめた報告書で終えます。同じ仕事でも、ほかの手法は違う分け方をします。WSTGが参考方法論に挙げるPenetration Testing Execution Standard（PTES）は、実施前の調整から報告まで、七段階を使います。

概念を判断に生かす

「ペネトレーションテストとは？」を実際の判断に生かしましょう。その概念を、開発または購入するシステムに結び付けて考えるお手伝いをします。 アカウント、パスワード、権限を整理し、業務に必要なアクセスだけを付与し、退職者の権限は当日に解除します。

サービスを見る お問い合わせ →

用語の背後にある前提を検証する

解説とリンク先の実績を参考に、プロジェクトについての質問を整理してください。ツールを選ぶ前に、前提を一緒に検討できます。 Linuxサーバーを守る1,000件のRBACルールを作成 — 1,000 セキュリティ上の穴を塞ぐアクセスルール

Linuxサーバーを守る1,000件のRBACルールを作成 お問い合わせ →

なぜ重要なのか

スキャナーの報告は、可能性の一覧です。その環境では悪用できないものもあり、まだ誰も記述していない欠陥や、無害に見える二つの弱点を合わせたときだけ現れるものは、見つけられません。ペネトレーションテストが答えるのは、攻撃者がここで実際に何をでき、どこまで進めるかです。SP 800-115は、実際の攻撃パターンへの耐性、必要な攻撃者の技能、有効な追加対策、防御側が気付いて対応するかも示せると加えます。

だからこそ、スキャナーの出力を読まない人にも、発見事項が重みを持ちます。アカウントのない外部者が顧客テーブルを読んだという報告は、確率ではなく証拠です。SP 800-115は、最小のアクセスから、さらに大きなアクセスを得る反復過程と説明します。良い報告書は、その連鎖を一歩ずつ示し、最も少ない費用で直せる箇所で、経路を断てるようにします。

現実に即しているからこそ、費用がかかり、危険も伴います。NISTは、多くの労力と高度な専門知識が必要で、試験中にシステムが壊れたり、使えなくなったりする可能性があると警告します。経験豊かな担当者で危険は減らせても、完全にはなくせません。システムを攻撃して侵害するなど、通常は組織自身の方針が禁

じる行為も多くあります。そのためにあるのが実施規則、rules of engagement（ROE）です。開始前に合意する文書で、定めた活動だけを試験チームに許可し、それ以上は認めません。

これも、複数ある技法の一つであり、単独の判定ではありません。WSTGは、多くのチームがウェブアプリの主な安全確認に使うと指摘し、主な検査にも、唯一の検査にもすべきでないと論じます。ウェブアプリはほぼ常に個別開発なので、外からの試験は、標準製品の既知の欠陥探しより研究に近く、設計とコードが固まった開発後半に来ます。それでも、完成したアプリはあるがソースを読めない場合、試験しないままにするより、明らかに良いとガイドは補います。

頻度は費用によって決まります。SP 800-115は、高い費用と影響の可能性から、組織のネットワークやシステムは年一回で足りる場合があり、その間に軽いスキャンを定期的に行う案を示します。直接要求する標準もあります。WSTGは、決済カード業界のデータセキュリティー標準PCI DSSが、外部と内部の両方について、独自のペネトレーションテスト要件を定めると記します。

実際の活用例

大半の内容は、最初のリクエストを送る前に決まります。SP 800-115の付録Bは、実施規則のひな形です。目的と範囲、人員と日程、連絡方法と中止条件、対象と除外対象、許可する行為と禁止行為、試験データの扱い、結果の報告、署名欄を含みます。ウェブショップの外部試験用に縮めると、次のようになります。この記事用に作った例で、名前やアドレスは、文書用に予約された範囲から取っています。

```
実施規則：shop.example.comの外部試験

目的            外部者が悪用できる欠陥と、それぞれで進める範囲を調べる。
対象            203.0.113.10から203.0.113.20まで。WHOISで所有権を確認済み
除外対象        203.0.113.15（決済提供元で、こちらに試験権限はない）。
                ショップが呼ぶすべての第三者サービス
アカウント      顧客用二つ、サポート用一つ
日程            十一月3日から14日、19:00から06:00 CET。営業の繁忙時間を避ける
試験元IP        198.51.100.7と198.51.100.8だけ
許可            確認した欠陥を悪用して影響を示す。
                試験アカウントのデータを読む。試験用と明示した
                ファイルを一つアップロードし、最後に削除する
禁止            サービス妨害、顧客データの変更や削除、
                ソーシャルエンジニアリング、物理的な侵入
中止            本番ショップの停止、実顧客データの露出、または
                本物の侵入者の兆候があれば中止し、
                セキュリティー責任者へ電話する
```

再開	セキュリティー責任者の書面による許可がある場合だけ
試験データ	機微な情報。試験チームのノートパソコンに保存し、最終報告書から30日後に削除する
報告	毎日の進捗報告、十営業日以内の最終報告書
署名	試験チームの責任者、最高情報セキュリティー責任者

各行が、SP 800-115の問いに答えます。ガイドは、開始前に、対象のすべてのパブリックアドレスが組織に属することを確かめるよう求め、WHOIS登録情報を挙げます。本番サイトの試験は、営業の繁忙時間ではなく夕方以降を勧めます。管理者が、本物の攻撃と試験通信を見分けられるよう、試験者が使うアドレスも求めます。触れてはいけないシステムを除外リストと呼び、中止基準と再開手順を定めるよう説明します。本物の侵入者を見つけた場合も問います。中止すべきか、いつ、誰の権限で再開できるのか。少なくとも、試験責任者と上級管理職が、範囲と限界を理解したと署名します。

このような規則の下で、攻撃段階は、WSTGが示すSQLインジェクションの流れに従います。ショップの検索ページをスキャンして、疑わしい欠陥を見つけます。最初の証拠は、欄に一重引用符を入れたときのデータベースエラーです。次に、クエリーの文法を変える入力を送り、本来返してはいけないデータが返って初めて、欠陥を確認します。もしサポートアカウントのセッションが含まれていたら、サポートとしてログインして、そこから再び調べることになります。その場合、報告書は、フィルタリングされていない一つの入力欄、漏れた一つのセッション、一つのサポートアカウントによる全注文の閲覧という、経路全体を示します。

この試験は、ほかの検査と並べて行い、置き換えにはしません。創業者のNextMarinerでの仕事を記録した、継続的なセキュリティースキャンを紹介するページは、自動で行う静的解析、稼働中のインスタンスへの動的試験、依存関係検査に加え、脅威モデルとOWASP試験ガイドに基づく評価を含む、文書化したセキュリティー監査を説明します。組み合わせる理由も明記します。スキャナーは、誰かが既に記述した種類の問題を探し、プラットフォーム固有の問題を洗い出すのは、脅威モデルです。

問題が起きるところ

書面の許可なしに試験します。 チームリーダーの口頭の了承だけでは、社内方針が禁じる攻撃を許可できず、試験者も依頼者も守れません。先に実施規則を書き、通信を一つでも送る前に、試験責任者と上級管理職が署名します。

所有していないアドレスを試験します。 古い図から写した一覧には、現在は他者が所有するものが混じることがあり、共有基盤では、他の顧客が隣にいます。SP 800-115の求めどおり、範囲内のすべてのパブリックアドレスが組織のものだと確かめ、すべての第三者サービスを、名前付きで除外リストに加えます。

スキャンを、ペネトレーションテストと称して提供します。 スキャナーの報告に表紙を付け替えても、可能性の一覧であり、証拠ではありません。全発見事項について、何をして、どのアクセスを得て、その次は何ができたかという、悪用の証拠を求めます。

唯一のセキュリティー試験にします。 一回の試験が見るのは、一時点に外から見える、リスクの一部です。WSTGは、設計時に脅威モデリング、開発時にコードレビューとソース解析、その後の試験段階にペネトレーションテストを置きます。すべてを行い、前の検査で確かめられなかったことを、攻撃による試験で確認します。

中止の規則を決めずに始めます。 本番サービスを止めたり、本物の侵入の兆候を見つけたりしたとき、誰が中止し、誰が再開させるかを決めていなければ、切迫した場で即興の判断になります。中止条件、電話連絡網、再開手順を、実施規則に入れます。

結果を、普通のデータとして扱います。 報告書は、攻撃者が悪用できる箇所の地図です。SP 800-115は、試験結果を機微な情報として扱うべきだと説明します。開始前に、発見事項の収集、送付、保管、廃棄方法を合意し、報告書全体を受け取る人を制限します。

再試験せず、発見事項を完了にします。 修正が部分的だったり、欠陥と違う箇所へ入ったりする場合があります。WSTGは、前のレビューで見つかった脆弱性を悪用しようとする検査を、焦点を絞ったペネトレーションテストと呼びます。デプロイ済みのコードで、本当に特定の欠陥を直せたかを示します。完了とする前に、各修正へ元の攻撃を再実行します。

秘密裏の試験なら、すべて見つかると思い込みます。 SP 800-115によれば、秘密裏の試験が調べるのは、攻撃者が与え得る損害です。全制御を試したり、すべての脆弱性を見つけたりはせず、通常は基本的な弱点から入ります。網羅性が目的なら公然の試験を、防御側が気付くかを知りたいなら秘密裏の試験を選びます。

参考資料

- NIST SP 800-115：情報セキュリティー試験・評価技術ガイド — セキュリティー試験の計画と実行、ペネトレーションテストの四段階と実施規則のひな形です。
- OWASP Web Security Testing Guide v4.2：序論 — レビューやソース解析との位置付けと、唯一の手法にすべきでない理由です。
- OWASP WSTG v4.2：ペネトレーションテストの方法論 — PTES、PCI DSSの指針、PTF、NIST SP 800-115、OSSTMMの概要です。
- NIST SP 800-53 Rev. 5：情報システムと組織のセキュリティー・プライバシー管理策 — 管理策CA-8で、ペネトレーションテストと実施規則を扱う、NISTの管理策一覧です。

用語集

実際の制約に合わせて選ぶ

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

用語を実務に結び付ける

「ペネトレーションテストとは？」がお客様の組織にどう当てはまるかをご相談ください。現在のシステムの具体例が一つあれば、話を始められます。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く 連絡先カード

心を込めて丁寧に制作： D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/glossary/penetration-test/