ハッキング

ハッキングにはさまざまな方法があり、このトピックは非常に興味深いものです。ホビーとしてのホワイトハットハッカーとして、この分野には学ぶべき知識がたくさんあると感じています。ここでは、私が探求したいくつかの方法を記録していきます。

デフォルトパスワード

一部のウェブサイト、政府機関のものも含めて、まだデフォルトのパスワードを使用しています。多くの企業やユーザーがデフォルトの認証情報を変更する一方で、変更しないところもあります。ユーザーはしばしば怠惰で、`12345678` のようなパスワードがまだよく見られます。これは特に古いシステムやニッチなシステムで顕著です。

nmap または Netcat

これらのツールは、サーバーのポートをスキャンするために使用されます。特に、80、22、443などの一般的に使用されるポートに注意を払ってください。AWS インスタンスの場合、デフォルトのユーザー名は `ec2-user` です。Azure インスタンスの場合、`azure-user` です。Google Cloud インスタンスの場合、デフォルトのユーザー名は通常 `ubuntu` または `google-cloud` です。その他のクラウドインスタンスでは、通常 `root` です。

ブラウザコンソールの使用

ブラウザのコンソールは、隠された情報を調査するのに役立ちます。時には、重要なデータが HTML や JavaScript コードに埋め込まれているものの、ページ上では見えないことがあります。

バックドア

人生において、バックドアは駐車場や裏口など、気付かれずに守られていない建物への不正な侵入を可能にします。同様に、システムにも通常のセキュリティプロトコルを迂回する隠れたバックドアが存在する場合があります。

ソーシャルエンジニアリング

人々のニックネーム、誕生日、そしてソーシャルメディアの投稿は、多くの個人情報を明らかにすることがあります。これらの詳細は、しばしば弱いパスワードの構築に使用されます。Wi-Fi ネットワークの場合、誰かの家の番号やその他の識別情報を知ることで、彼らの SSID やパスワードを推測するのに役立つことがあります。

SQL インジェクション

任意の入力フィールドに対して、`? 1=1` を使ってテストを行うことは、脆弱性や潜在的な SQL インジェクションポイントを特定するための一般的なテクニックです。

Actuator または Health API

API サーバーにおいて、Spring Boot のようなアプリケーションは、マシンやアプリケーションの健全性データを提供する`/actuator` エンドポイントを提供します。他のウェブフレームワークにも、機密性の高いサーバーの詳細を公開する同様の機能が存在します。

トラフィック監視

フロントエンドとバックエンドがどのように連携するかを理解するために、macOS では Charles Proxy のようなプロキシアプリケーションを使用して、リクエストログを記録・分析します。これにより、コンポーネント間のパスやデータ交換の詳細を把握することができます。

API の制限とエッジケース

API やサーバーの限界やエッジケースをテストすることは重要です。分散型サービス拒否（DDoS）攻撃は、リクエストの限界を超えさせようとする試みです。さらに、エッジケースとは、API が制限されたデータへのアクセスを許可してしまう可能性のあるシナリオです。これらをテストすることで、適切なアクセス制御が行われていることを確認できます。

管理パネル

時々、管理者や内部パネルが適切に保護されていないことがあります。`/admin` のようなパスにアクセスしたり、`admin.xx.com` のようなサブドメインを訪れたりして、これらのエリアが適切に保護されているかどうかを確認する価値があります。