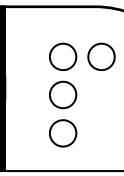
ラドウェアの振る舞い検知型 サーバクラッキング防御システム

***DefensePro* ホワイトペーパ**

Renaud Bidou
ラドウェア　シニアセキュリティ・スペシャリスト

October 2007

www.radware.com



目次

概要

インターネットアプリケーションの急速な発展により、新しい課題が生じています。世界では、手動プロセスを自動化するための革新的な技術が絶えず求められていますが、こうした手動プロセスから自動プロセスへの移行は時として、ハッカーやサイバー犯罪者が悪用可能な脆弱性をもたらすおそれがあります。こういった「悪者たち」の目的は、こうした自動プロセスを利用して、広範な攻撃を円滑に進めることにあります。長年ハッカーは、正当な通信形態にうまく統合した攻撃ツールを開発してきました。つまり、ネットワーク攻撃の検知、防御はますます難しくなってきているのです。最近の攻撃では、敵対的な行為を働くために、正当なインターネットアプリケーションが悪用されています。このような高度な攻撃者は、新しい、複雑なインターネット環境の無法地帯に「身を隠そう」とするのです。

実際のところ、コンピュータネットワークに侵入し、攻撃を仕掛ける手法は複数あります。しかし一般に、そのすべての手法が以下で説明されるような諜報活動、攻撃の計画、攻撃の実行という3つの運用段階で構成されています。

1. **諜報活動（情報収集）-**
   コンピュータネットワークへの典型的な侵入では、攻撃前の偵察スキャンが行われます。攻撃者はこのスキャン行為によって、標的とするネットワークの脆弱性に関する情報を収集します。どのようなアプリケーションの、どのバージョンが実装されているか、どのレベルのセキュリティパッチがインストールされているかといった情報は、ネットワークインフラとシステムの脆弱性を洗い出すのに役立ちます。さらに、スキャンの方法はここ数年でますます複雑化しています。現在の手法では、常時スキャンレートを変更し、スキャンの実行中におとり情報を送信することが可能です。そのため、このようなスキャンの検知は困難になっています。
2. **攻撃の計画** –
   サイバー攻撃者は諜報段階で得た情報をもとに、標的のネットワークに危害を及ぼす最も効果的な攻撃方法を決定することができます。本段階の目的は、最も効果的かつ効率的な方法で実行可能な攻撃を計画することです。すなわち、不要な操作を行うことなく、脆弱なネットワークリソース（ルータ、サーバ、アプリケーションなど）を直接狙います。不要な操作は疑念を招くおそれがあり、攻撃の成功率を下げることになります。
3. **攻撃の実行** –
   大半のネットワーク攻撃およびアプリケーション攻撃は、容易に入手可能な攻撃ツールによって実行することができます。こうしたツールはインターネットで簡単にダウンロードでき、初歩的なプログラミング技術を使用して、容易に修正して、事前攻撃を仕掛けることが可能です。

本書では、最初の攻撃段階である「情報収集活動」のため、過去数年に開発された手法について説明します。特にこの行為がもたらす脅威および検知における課題と、ラドウェアの侵入防御システムであるDefenseProを活用した、脅威の検知および軽減について詳しく述べます。

情報収集

スキャナとクラッカー

スキャナとクラッカーは、セキュリティテストの自動化に用いられる主要なツールです。通常、組織のセキュリティマネージャが担当するセキュリティ監査プロセスを迅速化するため、セキュリティ担当者の管理下で使用されます。社内にセキュリティ担当者がいない場合や、法的な理由がある場合は、サードパーティのセキュリティ監査会社によって、セキュリティテストの自動化を図ります。

スキャンツールおよびクラッキングツールは、pingスイープやポートスキャンなど、ネットワークベースの攻撃前の偵察行為を生成するために使用されます。あるいは、ユーザ名やパスワードのクラッキング、アプリケーションの脆弱性スキャンなど、アプリケーションに対する攻撃前の偵察行為の生成に使用されます。これらはすべて手動監査では何ヶ月もかかるため、自動化されるプロセスです。

こうしたツールの大半は善意で開発されたものですが、悪意のある個人がこの「正当な」ツールを利用して、標的とするシステムの脆弱性を手早く効率的に見つけ出し、それをもとにネットワーク攻撃を仕掛けるおそれがあります。さらに、ワームは通常、自動スキャンや感染プロセスを経て増殖しますが、スキャナやクラッカーで使用される技術を模倣(または単純にコピー)して、自動的に感染できる潜在的に脆弱なホストを特定します。

したがって、非常に大規模なハッキングを阻止し、ワームをブロックして、標的とされたクラッキングを大幅に減速させ得る方法として、このようなツールをブロックできることが必須となっています。

スキャンツールとクラッキングツール

セキュリティテストを自動化するためのツールは数多くあります。簡潔に説明するため、ここではネットワーク層ツールとアプリケーション層ツールに分類します。

本書では、アプリケーション層ツール[1]のカテゴリに分類されるスキャナおよびクラッカーの検知と防御という、より困難なタスクに着目します。
アプリケーション層ツールに該当する主な脅威は、次の2つのカテゴリに分類可能です:

クラッキング攻撃 –

総当り攻撃や辞書攻撃などのクラッキング攻撃では、既知のリストからユーザ名やパスワードを推測して、アプリケーションへの侵入を試みます。この種の攻撃に伴うリスクは非常に明白です。いったん有効なユーザ名やパスワードが取得されると、攻撃者はサービスや情報に自由にアクセス可能となり、さらにはサーバの管理許可権さえも手に入れることができます。
さらに、アプリケーションにビルトインされた防御システムを起動してユーザを閉め出したり、認証中にシステムリソースを消費したりすることで、DoS(サービス拒否)攻撃を仕掛けられるリスクもあります。

---

[1] 前述のように、長年ハッカーは正当な通信形態にうまく統合した攻撃ツールを開発してきました。アプリケーション層のスキャンツールやクラッキングツールは、その一種です。

総当り攻撃ツールは通常、Mass Generatorと呼ばれる手法を採用しています。これは、同様の動作を大量かつ高速で仕掛けることを目的として、開発されたものです。総当り攻撃の場合、異なる種類のログインも同様の動作に含まれます。
また、典型的な総当り攻撃ツールは、汎用ブルートフォーサーと呼ばれます。これらのツールは、HTTP認証やFTP認証といった通常の認証から、CVS認証やpcAnywhereといった非常に個性的なものまで、20種類以上の認証形式をテストする手法など、複数のアプリケーションを狙うことができる機能を備えています。このようなタイプのツールは、Basic HTTP認証など標準で定義される認証手法をテストします。

アプリケーションの脆弱性スキャン

スキャナで何千回もテストを実行し、悪用可能な潜在的な脆弱性のリストを提供します。一般に、こうしたスキャナはサーバに対してエクスプロイトではなく、脆弱性の存在を示すだけの正当なリクエストを送信します。そしてそれ自体は、シグネチャベースの防御システムを起動するものではありません。

このようなスキャナは、次の3つの系統に分類可能です：

- **一般的なスキャナ**：何千回ものテストを実行し、悪用可能な潜在的な脆弱性のリストを提供します。
- **専用スキャナ:** このツールも複数の脆弱性をテストします。但し、特定の種類のOSやアプリケーションに影響を及ぼすものしかテストしません。
- **エクスプロイトツール**: 標的とするシステムに対して、実際に一連の攻撃を仕掛けるツールです。前述のように、この手法は容易に検知されるため、一般的ではありません。

これらのアプリケーションスキャナは、サーバに対して何千ものアプリケーション要求を生成し、さまざまな動作の応答を解析します。アプリケーション応答の解析によって、標的とするアプリケーションの正確な情報（種類、バージョンなど）を特定することが可能です。そして通常、明らかになったアプリケーション情報にしたがって、ツールが脆弱性データベースを調査し、アプリケーションの種類およびバージョンに一致する、特定の一連のアプリケーション要求を選択して、偵察したアプリケーションにその情報を送ります。このような仕組みによって、ツールはアプリケーションにどの脆弱性が存在するか、自動で特定することができます。

次の図は、典型的なHTTPの脆弱性スキャンを示したものです：

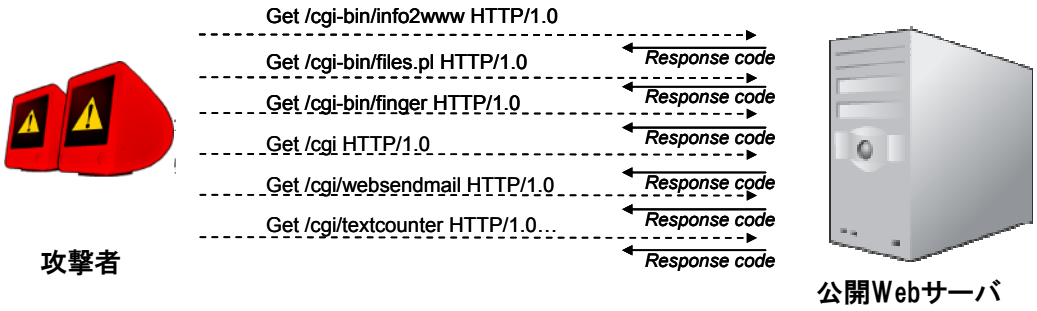


図1a - HTTPの脆弱性スキャン（第1段階）

ハッカーはスキャンの第1段階を終えると、次の成果が得られます：

- サーバアプリケーションの種類やバージョンに関する情報が明らかになる。
- スキャン実行中にサーバリソース（CPUおよびメモリ）が不正利用され、その結果、サービスの混乱が生じる。
- アプリケーションの既知の潜在的な脆弱性が検出される。
- 次の図1bに示されるように、スキャンの第2段階で高い成功率をもって、脆弱性に対して直接エクスプロイトを実行することができる。

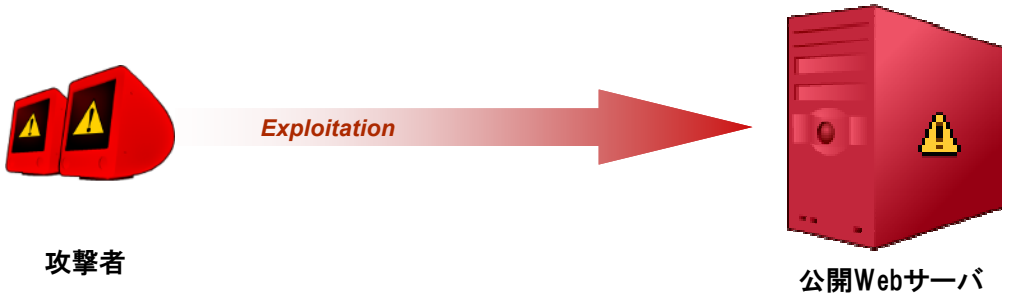


図1b - エクスプロイトの実行（第2段階）

定義によると、前述のアプリケーションに対する攻撃前の偵察行為は、正当なトラフィックに覆い隠されています。そのため通常、プロトコルルールに違反していません。または、アプリケーションの既知の脆弱性に対するエクスプロイトを示した、事前定義の攻撃シグネチャに一致しません。したがって、シグネチャベースの検知機能のみを搭載したNIPS（ネットワーク侵入防御システム）では、このような脅威に対して効果がありません。

こうした攻撃前の偵察行為を効果的に防御できるのは、アプリケーショントラフィックのパターンの変化を評価できる動作ベースのシステムのみです。

ラドウェアのDefensePro

ラドウェアのサーバクラッキング防御システムでは、既知および未知のアプリケーションスキャンと総当り攻撃を検知して防御できる、動作型サーバベースの技術を採用しています。

この振る舞い検知型の防御技術は、ラドウェアのDefenseProのフルスペクトル防御技術の一種です。同技術には、ネットワークに対するDoS(サービス拒否)/DDoS(分散型サービス拒否)攻撃を緩和する、振る舞い検知型ネットワークベースの防御技術、ネットワークに対する攻撃前の偵察行為およびゼロデイワームの増殖を軽減する、振る舞い検知型ユーザベースの防御技術、およびアプリケーションの既知の脆弱性を狙ったエクスプロイトに対する、シグネチャベースのステートフルな防御技術があります。

図2は、DefensePro内部に実装された、独自の防御セキュリティ層のアーキテクチャを示したものです。サーバクラッキング防御は、図の第2層にあたる動作型サーバベース技術の1つです。

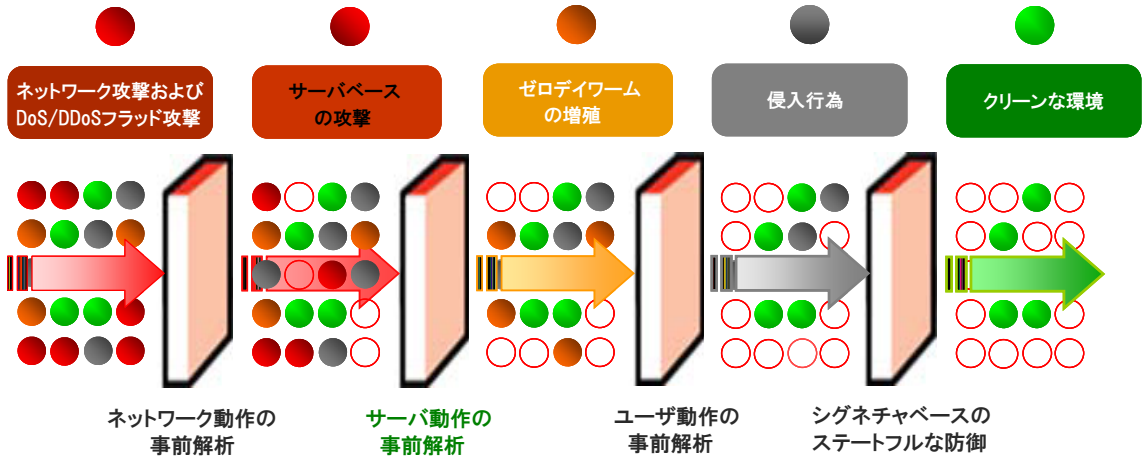


図2 - DefenseProのマルチレイヤ防御システム

サーバクラッキングの防御

動作型のサーバクラッキング防御によって、次の既知および未知(ゼロデイ型)の脅威が検知、防御されます。

- Web認証における総当り攻撃および辞書攻撃
- HTTPの脆弱性スキャン
- SMTP(メール)に対する総当り攻撃および辞書攻撃
- FTPに対する総当り攻撃および辞書攻撃
- POP3(メール)に対する総当り攻撃および辞書攻撃
- MySQLに対する総当り攻撃および辞書攻撃

- MSSQLへの総当り攻撃および辞書攻撃
- SIPに対する総当り攻撃および辞書攻撃
- SIPスキャン

SIPスキャンと総当り攻撃について

SIPスキャン -

SIPスキャンにおける攻撃者の目的は、アプリケーションの脆弱性を狙った通常のスキャンの場合とは若干異なります。SIPの脆弱な実装を見つけることができる一方で、SIP加入者のリストを入手し、SPIT（Spam over IP Telephony）とも呼ばれるSIPスパムメッセージを送信できることが、SIPスキャンの真の利得なのです。攻撃者は推測した加入者名に対して、スクリプトを使ってSPITメッセージを送信し、応答した加入者を記録します。SPITは加入者にとって厄介な上、大量に送信すると、サービスの混乱を引き起こすことができます。

SIP総当り攻撃 -

Register総当り攻撃とは、ユーザアカウントのアクセス権を獲得し、サービスにアクセスしようとする試みです。これにより、攻撃者は無料でサービスを利用することが可能になります。その結果、収益の損失、評判の低下に加え、課金内容の検証作業が発生します。
ラドウェアのDefenseProによるVoIP防御の詳細については、以下のホワイトペーパー「ラドウェアによるマルチレイヤのVoIPセキュリティ」を参照してください。
http://www.radware.com/content/document.asp?_v=about&document=7490

振る舞い検知型サーバクラッキング防御技術

ラドウェアの振る舞い検知ベースのサーバクラッキング防御メカニズムでは、サーバアプリケーションに対するスキャンや総当り攻撃を試みるユーザを検知するため、高度な統計エンジンと振る舞い検知型のファジーロジック意思決定エンジンを採用しています。このエンジンは、防御されたサーバで生成された複数のアプリケーション応答メッセージを分類し、そこからユーザ識別子を抽出します。

そして、統計エンジンが複数の応答メッセージの頻度、品質、分布パラメータなど統計的特性をユーザごとに計算します。

ファジーロジック意思決定エンジンは、各特性パラメータに対してアノマリのウエイトを割り当て、専門ルールによってそのウエイトを相互に関連付け、ユーザごとにアノマリの度合いを決定します。

システム管理者が直面する防御システムの課題の1つに、意思決定が可能になるまで（例：特定の閾値を超えるまで）システムがユーザの動作を監視する、タイムアウト間隔の定義があります。このタイムアウトの設定を誤ると、即座に誤検出あるいは検出漏れのある決定につながるおそれがあります。監視期間が長すぎると誤検出の可能性が高まり、逆に短すぎるとシステムがスキャンや総当り攻撃を検知できないリスクが高まります。

このような問題を解決するため、ラドウェアのサーバクラッキング意思決定エンジンでは、ユーザのアノマリの度合いに応じてユーザ監視間隔を自動調整します。この動的な監視間隔によって、意思決定を行うために、システムがユーザを疑わしいと見なし、アクティビティを解析し続ける期間が決定されます。このような適応プロセスによって、システムの意思決定の精度が向上し、システム管理者による設定およびメンテナンス作業が大幅に削減されます。

いったん攻撃者とみなされたユーザはブロックされるため、攻撃対象のサーバに対するこのソースからの接続は、それ以上受け入れられません。攻撃があった場合は、DefenseProが動的ブロックリストにそのソースIPアドレスを挿入します。あるいは、過去に同様の攻撃ライフサイクルで既にブロックされているソースIPアドレスの場合、ブロック期間を延長します。

サーバクラッキング防御のクローズドフィードバックメカニズム

動的なユーザ監視間隔に加え、DefenseProのクローズドフィードバックモジュールがさらに、誤検出による意思決定を最小限に抑えます。DefenseProが採用するクローズドフィードバック手法は、動的なブロック期間が特徴です。
システムは攻撃行為を発見すると、まず攻撃者に対して非常に短時間のブロック期間を適用します。この間に、システムはブロックしたユーザの軌跡を記録し、継続的に異常な行為を働いているか確認します。一時的な行為であることが確認されると、システムは直ちにブロック期間をゼロにし、ユーザを解放します。継続的な異常行為である場合は、ブロック期間が自動的に延長されます。図3は、サーバクラッキング防御の意思決定プロセスを示したものです。

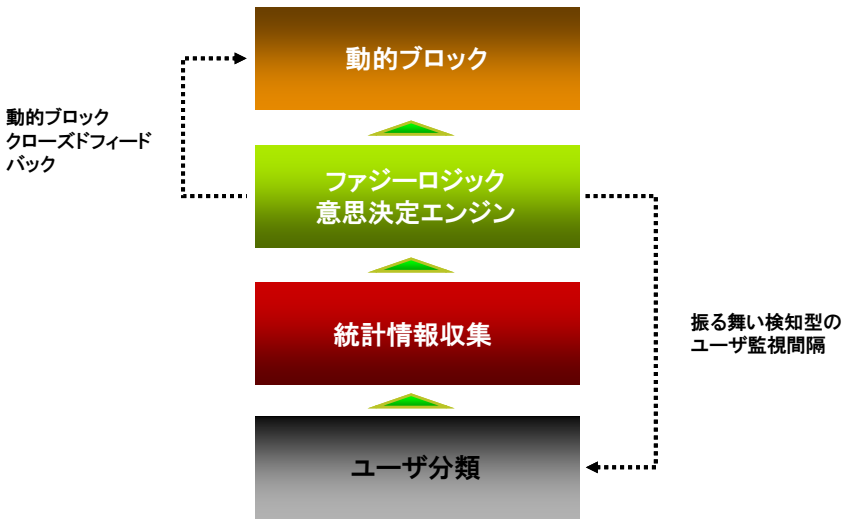


図3 - サーバクラッキング防御の意思決定プロセス

まとめ

ラドウェアのDefenseProは、シグネチャベースの防御、ゼロデイワームの増殖およびネットワークに対するDoS/DDoSフラッド攻撃に対応した適応動作型ネットワークベースの防御、および帯域管理など、複数の防御レイヤを統合したものです。攻撃の次の段階を調査する一連のサーバクラッキング防御機能が、振る舞い検知型サーバベースの防御技術によって、IPS(侵入防御システム)の機能を補完します。

現在の脅威およびセキュリティの課題を考慮すると、効果的な防御システムとは、次の主要機能を備えたものであると結論付けられます。

- **広範なセキュリティ**
  アプリケーションの保護には、ネットワーク層、トランスポート層、アプリケーション層を対象とした、マルチレイヤの防御技術が含まれる必要があります。事前の動作ベースのセキュリティ技術と、シグネチャベースのセキュリティ技術によって、既知および未知の攻撃を阻止する必要があります。
- **拡張性**
  セキュリティ製品は、トラフィックの遅延を最小限に抑えながら、高速環境で動作可能でなければなりません。この重要な機能は、先進的なセキュリティ技術を備えた高度なハードウェアアーキテクチャによって実現されるものです。
- **低TCO(総所有コスト)**
  TCOを低く抑えると、システムはより人的要因に依存しない(「手のかからない」なシステム)ことを余儀なくされます。人的要因に拠らなくなるため、これまでセキュリティ担当者が行っていた操作を、システムで自動実行する必要があります。
- **精度**
  製品が提供する検知および防御技術の精度は、特にリアルタイム環境において最重要事項です。セキュリティ製品は誤検出や誤防御(パケットの不要な廃棄)があると、たとえ低い割合であっても、役に立たないものになってしまいます。

ラドウェアの振る舞い検知型サーバクラッキング防御システムは、アプリケーションの脆弱性スキャンなどアプリケーションに対する攻撃前の偵察行為、総当り攻撃、およびアプリケーションサーバリソースの不正使用をすべて、リアルタイムで正確に防御する能力を備えています。
振る舞い検知型防御システムは統計アルゴリズムを採用しており、進行中の攻撃パターンの特徴を明らかにして、それを基に人の手を介さずに攻撃をフィルタリングします。このように、ラドウェアのDefenseProは、上記のすべての主要機能を満たすように設計されたNIPS(ネットワーク侵入防御システム)を取り入れたものであるといえます。