サーバのセキュリティ確保

総合情報基盤センター　助教　沖野 浩二

昨年は日本国内において、サーバ攻撃が多く新聞やニュースに取り上げられた。また、本学においても、サーバが学外から攻撃され、権利者権限が取得される事例も発生した。センターにおいても、インシデントの発生を予防するために、ネットワーク管理体制の強化を行っているが、実際に被害を防ぐには、各サーバの管理者の意識が重要になる。本稿は、サーバを運用する上で、管理者が知っておくべき必要な事項をまとめたものである。

１．はじめに

2011 年を代表するサイバー攻撃としては、SCE の PSN(PlayStation Network)の不正攻撃による情報漏えいや、三菱重工業や衆議院に対する機密取得を目的とした Virus 攻撃が挙げられる。これらの事件は、マスコミなどで大々的に取り上げられたことで覚えておられる方も多いと思う。

これらの攻撃は、大きな企業や政府を狙ったものであり、自分には関係ないと考えている方もおられると思うが、実際には、大学に対してもこれらの攻撃は発生している。

２．大学への攻撃

現在、富山大学は複数の FW によるセキュリティ防御を行っているが、一番外部にある FW では､1 分あたり 500 件から 15,000 件の通信を攻撃と判断して、通信遮断を行っている。この通信遮断は、Port Scan(どのようなサービスを提供しているかの調査)など単純な攻撃パターンがその大半を占めている。これらの攻撃パターンを解析したところ、本学の IP アドレスに対しては、世界中から攻撃の前兆とする調査が多数行われていることが判明している。加えて、これらの調査は定期的に行われていることも判明しており、外部公開しているサーバのセキュリティ情報を、部外者が蓄積している可能性が高いと考えている。

３．調査から攻撃へ

攻撃者側は、これらの事前調査を行うことによって、サイトの管理体制や利用可能なサーバのリストを作成していると思われる。本学においても 2011 年に発生したインシデントでは、下記のフローで、行われと考えている。

I.　事前調査

事前に大学の所有する空間に対して調査を行っておき、サーバ等の変化を観測しておく。また、実際に簡単な攻撃を行っておき、簡単に利用できるサーバのリストを作成しておく。これらの攻撃用は、インターネットで公開されているプログラムを利用し、行われていると思われる。

II.　攻撃,Bot 化

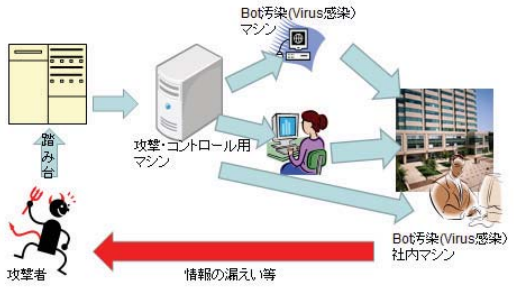
変化したサーバや簡単な攻撃が成功した

サーバに対しては、人間による攻撃が行われる。これらの攻撃により、より詳しい情報の収集や目的に応じたプログラムの導入が行われる。

III. 攻撃成功後

目的の攻撃が成功した場合には、次の目的のために、これらのサーバ資源が活用される。実際には、保存データの検索、内部データを利用した内部の他サーバへの攻撃、他サイトへの攻撃、フィッシングサイトの開設等が行われる。

実際に構築された攻撃者側のネットワーク構成は、下記のようなものである。



実際の攻撃では、攻撃者は複数の踏み台を経由し、攻撃を仕掛けてくる。また、大学内の攻撃が成功したサーバでは、踏み台としての利用や他の組織への攻撃・コントロール用サーバとして利用される事例も多い。

４．大学サーバへの攻撃目的

大学サーバへの攻撃目的は、大きく分けて次の 3 点だと考えられる。

- 攻撃の練習
- 大学情報環境の利用価値
- 大学所有のデータ取得

大学に設置されているサーバは、企業のように専任の部署が管理されているものではなく、研究者個人により運用されているものが多くある。これらの中にはセキュリティの意識なく Network に接続されたものがあり、昔からクラッカーの練習用として利用されてきた歴史がある。これが 1 番の攻撃の練習という目的である。

これに加えて近年の攻撃の特徴は、2 番目と 3 番目の目的が挙げられる。2 番目の大学情報環境の利用価値とは、大学ネットワークの特徴として、

- 広帯域なネットワークに接続されていること
- 多量の通信を発生させても違和感がないこと
- 大学のアドレスが、他の機関への攻撃時に利用できること
- 管理されていない場合も多く、発見される可能性が低いこと

などが挙げられる。大学のアドレスとは、Virus 付メールを発信する場合に、大学のアドレスを名乗ることで、相手を信用させるために利用するものである。

3 番目の大学所有のデータ取得とは、研究者が所有している研究情報や、大学向けに公開されている研究者向け DB のアクセス権を取得することを目的としているものだ。

これらは、三菱重工業や衆議院に対する攻撃と同様で、大学に対するサイバー攻撃であるといえる。機密情報を扱っている研究者に対して、これらの攻撃が成功した場合には、広域な範囲への影響が考えられる。

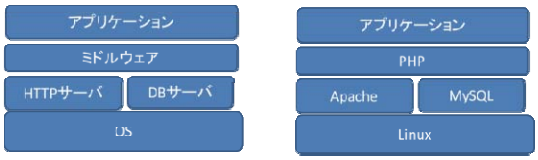
研究者が特に注意すべき機密情報の例としては、

個人情報　医療情報　研究情報

が挙げられる。これらの保護は、法的にも求められるものであり、加えて特許等の知的財産の申請にも影響がある。これらの情報を扱っている方は、特に厳重なサーバ管理をお願いします。

５．サーバの攻撃ポイント

実際に攻撃者側はどのように攻撃するかについて説明するが、その前に、実際にサーバがどのような構成で動いているかを考える。一般に Web 等のサーバは、OS に HTTP サーバが基本であり、その上に目的に応じて PHP や Perl,Java Servlet 等のアプリケーションや DB サーバを組み合わせて構築される。有名な例としては、LAMP（Linux+Apache+MySQL+PHP,Perl 等）と呼ばれるものが代表的なものである。



これらのサーバに対して行われる代表的な攻撃手法として代表的なものは、下記のように構成要素ごとに挙げられる。

実際には、この他にも多数の攻撃手法があり、攻撃ツールも日々進化しているのが実際である。また、簡単なツールならば internet 上から容易に入手することが可能であり、これらのツールの利用方法を説明している日本語の雑誌も販売されている。

実際の攻撃を防ぐ場合には、これらのすべての要素をコントロールする必要がある。特にサーバ側でページを作成するものに関しては、攻撃可能な要素が広範囲に広がるため、リスクの把握には、多大なコストが発生する。実際に PSN の事件の原因は、DB サーバへの SQL injection によるものであり、この攻撃が成功したのは、既知の脆弱性への対応が行われなかったためだと言われている。PSN のようにそれを商売としている企業でさえ、リスクを把握し、適切に対応することが難しいと言える実例であると言える。

６．管理者の対応

このようなリスクに対応すべく、管理者が行うことは、導入のフェーズに合わせて下記のような項目がある。

I. 導入前

サーバを公開する目的の明確化や運用することによるリスクの把握である。重要な機密を扱うサーバをインターネットに公開して得る利益と、それに係る運用コストや、漏えいした時のリスクを鑑みて判断する必要がある。

II.　構築中

サーバを構築する場合には、技術的な要素や運用後の体制を含めて、じっくりと調べるまた考えることが必要である。運用開始をしたのちに構成を変更するには多大なコストが発生する場合があるため、この時点で適切なサーバの構成や体制を検討することがとても重要である。また、技術力が

ない場合には、SI 業者に相談することも良いと思われる。

具体的な Web アプリケーションにおけるセキュリティに関しては、
http://www.ipa.go.jp/security/awareness/vendor/programmingv2/web.html
が参考になる。

III. 運用開始後

この中で、一番重要なポイントになる。7 章にまとめたものを掲載する。

IV. インシデント対応

学内でよくある事例として、公開を意識していないのに、実際には設定ミス（正確には制限等の適切な設定を行わず）で公開されていたという場合がある。このようなことが起こらないように公開サーバには必要なデータ以外を保存しないようにすることが望まれる。また、不正アクセス等の発生した場合の手順も考えておく必要がある。

７．運用中の確認項目

実際に運用しているサーバに対して行うことが必要な項目を挙げる。

情報収集

セキュリティ情報を収集することが重要である。無関心や学生任せなどのサーバが狙われていることが多い。セキュリティの情報は、(独)情報処理推進機構の
http://www.ipa.go.jp/security/index.html
にまとまっているので、ぜひ参考にしてください。

リスク要因の低減

・安易なパスワードの利用
・卒業生など利用していないアカウントの削除
・実験に使用したプログラムなど、現在では不必要なサービス等の停止
・外部からの接続等に対してアクセス制限
・サーバに格納してあるデータの確認。機密情報等はサーバには保存せず、外付け HDD 等で格納し、利用時のみ接続する

LOG の確認

サーバには、access log 等が残されているので、定期的にこれらの log を確認して、不正アクセス等が発生していないかを確認してください。

セキュリティの対策

・セキュリティ UPDATE
OS やミドルウェアも含めてセキュリティ Patch を適応する。また、これらの提供が終了した OS やアプリケーションは利用しない。
・アクセス制限の設定
ssh を限られた範囲(IP アドレスやドメイン名などによる制限)からのアクセスにする。
・認証方式
公開鍵認証など Password 以外の高度な認証を利用する

８．さいごに

実際にサーバを運用するには、セキュリティを意識する必要がある。本稿に記載している項目は、実際の運用時に最低限必要な項目を列挙したものである。皆様方には、これらを参考にして少しでも安全なネットワーク運用に協力いただければ幸いである。