サーバハードニング（強化）の重要性

株式会社エス・アイ・ディ・シー
代表取締役　里吉　昌博

「情報セキュリティ」は、数年前はコンピュータおたくが、日の当たらない場所で取り交わす会話に出てくる程度でした。それが徐々に局面が広がり、今ではネットワーク世界でビジネスを行う上で必要不可欠なものと言われるまでになってきました。

企業は通常、ファイアウォールやウィルス対策ソフト、またセキュリティポリシーなどのソリューションを組み合わせて、自社のセキュリティ問題に対応しています。しかし、ポリシーや技術的に強固なファイアウォールを適切に実装することが、優れたセキュリティインフラ（基盤）を形成するベースとなるものですが、その一方で、BlasterやSoBigなどのワームによって引き起こされた最近のセキュリティインシデント（事故）により、ファイアウォールやポリシーだけでは、その手の攻撃から企業ネットワークを守れないことが浮き彫りになりました。

かつては、情報セキュリティを説明するのに「城」の例えが多く用いられておりました。中世の城のように外壁を強固にすれば、企業は安全だと教えられたものです。

しかし何度となく、それは間違いであることが明らかにされてきました。

本当に安全な環境にするためには、城内の各所にまた城を築き、それぞれが自分自身とお互いを攻撃から守るような仕組みになっていなければならないのです。

このように、セキュリティがいくつもの「層」のように配置され、その各層が中心部分を守る役目を担う構造を説明するために、最近では、「城」ではなく、「玉ねぎ」が最も適切な例えとして用いられるようになりました。まだ日本では馴染みが深くありませんが、セキュリティ先進国である北米においては、レイヤー化されたセキュリティアプローチを説明するのに、よく用いられております。

こうして、ホストベースのセキュリティとサーバ・ハードニングが脚光を浴びることになりました。サーバ・ハードニングとは、ビジネス要件を満たしながらも、サーバのセキュリティをより堅牢にする設定を行うことです。ほとんどのOSは、利用条件に対応した適切なアクセス制御などの設定が行われることが想定されており、デフォルト設定のままでは安全性に問題がある場合が多くあります。

本稿では初期設定のWindows 2000 Serverを例として、一般に広く見受けられる脆弱性と、サーバをハードニング（強化）してそれらの脆弱性に対処する方法について述べます。しかし本稿では、発生する可能性のある脆弱性のすべて網羅するわけではなく、代表的な例を取り上げて、それらを解消する方法を示すことに重点を置くことにします。

■ 攻撃のシナリオ

システム：Windows 2000 Server、Active Directory（AD）を使用
攻 撃 者：組織内のLAN上に存在する

これは最も一般的なシナリオで、悪意のある第三者が最も攻撃を行いやすいシナリオでもあります。攻撃者は、Windows 2000 ServerのCDに収められている一般的なリソースキットツールやサポートツールなどを悪用して、システムに関する非常に有用な情報を取得することが可能になります。

例えば、すべてのWindows 2000のCDに付属するサポートツールの「LDP」を使えば、ADオブジェクトを、LDAPを用いて一覧表示することができます。リソースキットに含まれている「Gettype」を使うと、攻撃者はリモートのWindows Serverのバージョンと種類を正確に特定できます。また同じく「ENUMPROP」を使うと、リモートのAD Serverをコマンドラインから一覧表示することが可能です。

攻撃の前にシステム情報を見ることができるという

のは、悪意のある第三者がターゲットを絞った攻撃を実行するための十分な情報を収集するのに最良の方法であり、そのおかげで攻撃が成功する確率も高くなり、不審なログファイルやアラートの発生を抑えることができます。

上に挙げた3つのツールを使用すれば、攻撃者は次のような情報を手にすることができます。

・ システム名
・ ドメイン名
・ ユーザリスト
・ 最終ログイン時間などのアカウント情報
・ オープン共有
・ 使用されている認証機能の種類　など。

さらに攻撃者は、単純なポートスキャンを行うことでも、貴重な情報を入手できます。この場合攻撃者は「Nmap」のようなツールを用いて、システム上で稼動しているサービスをすべて明らかにすることができます。

Windows 2000 Serverの初期設定では、次のようなサービスがデフォルトで提供されています。

```
# nmap 3.48 scan initiated Fri Jun 25 04:21:10 2004 as: nmap -sV 192.168.1.116
Interesting ports on 192.168.1.116:
(The 1633 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Microsoft ftpd 5.0
25/tcp   open  smtp         Microsoft ESMTP 5.0.2195.6713
53/tcp    open  domain     Microsoft DNS
80/tcp   open  http         Microsoft IIS webserver 5.0
88/tcp   open  kerberos-sec Microsoft Windows kerberos-sec
119/tcp  open  nntp?
135/tcp  open  msrpc        Microsoft Windows msrpc
139/tcp  open  netbios-ssn
389/tcp  open  ldap         Microsoft LDAP server
443/tcp  open  https?
445/tcp  open  microsoft-ds Microsoft Windows 2000 microsoft-ds
464/tcp  open  kpasswd5?
1026/tcp open  msrpc        Microsoft Windows msrpc
1029/tcp open  ncacn_http   ncacn_http 1.0
1083/tcp open  mstask       Microsoft mstask (task server - c:winntsystem32Mstask.exe)
3372/tcp open  msdtc?
3389/tcp open  ms-term-serv?
```

■ 攻撃ベクトル

Windows 2000 Serverのようなシステムを首尾よく攻撃する方法は数多くありますが、ここではその一部を取り上げることにします。

• Kerberos攻撃 – システムでKerberos認証サービスが動作している場合、攻撃者はKerberos用ポート（TCP 88番）をトラフィックで溢れさせて、Kerberosサーバを使用不能にすることができます。これによりクライアントは、傍受やクラッキングが容易なSMB認証を使わざるを得なくなります。

• SMBによるパスワードの解読 – 初期設定のシステムでは、anonymous（匿名）ネットワーク接続が可

能で、これをブルートフォース（総当り）攻撃に使用することができるようになっています。システム情報列挙などによって集めた情報をもとに、攻撃者は特定のアカウントに照準を合わせることができ、さらにはパスワードポリシーを把握して、その要件を満たしていないアカウントに的を絞ることも可能です。

- RPC/DCOMの脆弱性－検索エンジンでインターネットを検索すると、リモートプロシージャコール（RPC）やDCOMの悪用に関するコンセプト証明用のツールが多数見つかります。RPCやDCOMは初期設定システム上で有効になっており、攻撃者はこれらを悪用して、管理者権利でコマンドを実行することが可能です。
- IIS－MicrosoftのIIS Web ServerとFTP Serverにはどちらも、RPC/DCOMの脆弱性によく似た、リモートからのシステムの不正使用につながる既知の脆弱性が存在します。これによって攻撃者は、リモートから管理者機能を使うことが可能になります。

上に挙げた攻撃に成功すると、悪意のある第三者はシステム上のあらゆるデータの閲覧、コピー、消去、改変が容易にできるようになり、場合によっては、そのシステムを踏み台にして他のシステムへの攻撃を実行することができます。このようなケースでは、攻撃者が追跡の手を逃れる可能性が通常より高くなります。

■ 防御のシナリオ

お気付きの通り、こうした攻撃のほとんどは、実質的な防御策としてファイアウォールだけしか設置していない企業が大半を占めている状況では、悪意のある第三者が企業LANの外部にいても有効に行うことが可能です。

またこれらのサービスがインターネット上で利用可能になっていれば、攻撃の対象とされる危険性があります。

事実、RPC/DCOMの脆弱性やIIS脆弱性は、Blaster、Code Red、Nimdaのような大量メール送信型ワームによる攻撃で悪用されてきました。

これらの攻撃に対処するポイントは、単にこれらのシステムを無効にしたり、ファイアウォールで阻止したりすることではありません。実際に、設計に工夫を凝らして安全性を高めたアーキテクチャすべてが、可用性が高く有効に業務が行えるものになっているわけではありません。

こうした攻撃のほとんどは、サーバ・ハードニングやホストベースのセキュリティ措置によって防ぐことができるのです。

最も単純なレベルのサーバ・ハードニングは、最低限のアクセスポリシーに従ったものです。サービス、機能、アクセスポイントなどで必要のないものは提供を停止するか、最低限、利用を制限する必要があります。

例えば、一覧表示のタスクの実行をほぼ不可能にするには、管理者はシステムへのanonymous接続ができないように設定するだけでいいのです。これにより、適正な信用証明を持たない者は、システム情報の一覧表示ができなくなります。

これを行うには、次のレジストリキーにレジストリ値（RestrictAnonymous）以下を追加することです：

システムキー：
　[HKEY_LOCAL_MACHINESYSTEMCurrentControlSetControlLSA]
レジストリ値：
　RestrictAnonymous
データの種類：
　REG_DWORD (DWORD値)

値のデータ：
（0 = 許可, 1 = 許可しない, 2 = 匿名アクセス許可が必要）

使用しないサービスを無効にすることで、攻撃者がそれらのサービスの脆弱性を悪用するのを防ぐことができます。必要とされるサービスに関しては、攻撃に対するシステムの抵抗力を増すための詳細な設定が数多く用意されております。

また、ファイル、ディレクトリ、レジストリなどのパーミッションを変更するのも、自動化された攻撃を防ぐのに非常に有効な方法です。例えば、ワームやトロイの木馬の多くは、レジストリキーの「Run Once」（一度だけ実行）セクションに書き込みを行おうとします。これらのキーを書き込み不可にするだけで、この攻撃ベクトルを悪用する悪質コードが機能するのを阻止することが可能です。

パーミッションやコマンドプロンプト（cmd.exe）の位置を変更すれば、Code RedやCode Redに似た手動の（Unicode脆弱性の悪用）攻撃などを無効にできます。

また、組み込みTFTPクライアントを用いて、脆弱なシステムにファイルを転送したり、システムからファイルを転送する攻撃もよく行なわれます。この攻撃の発生を防止するには、「tftp.exe」のパーミッションを制限するか、場合によってはtftp.exeそのものを削除すれば解決します。

■サーバ・ハードニングに伴う問題点

サーバ・ハードニングに伴う実質的な問題点として、適用可能な設定が文字通り数百通りも存在することが挙げられます。これらの設定の中には、アプリケーションやその機能を実行できるかどうかに影響を及ぼすものもあれば、及ぼさないものもあります。

中には、ネットワーク全体に深刻な影響を及ぼす可能性があるものもあります。システムにいかなる変更を加える場合も、実装する前に、実際の本番システムではないシステムで、それぞれの設定を徹底的にテストしておくことをお勧めします。

OS内部の仕組みを完全に理解していない経験の浅いシステム管理者なら普通は、こうした問題の発生を危惧して、システムの強化には手を出さないことが多いのも事実です。

サーバ・ハードニングのリサーチ、テスト、実装には、熟練した外部の支援がなければコストがかさむ恐れもあります。しかし長い目で見て、システムのセキュリティ、信頼性、パフォーマンスの向上につながれば、実行する価値のある投資と言えるでしょう。

こうした問題に対応し、OSのセキュリティ設定を自動的にハードニング（強化）するツールを弊社でも開発しました。http://www.security-sensei.com/をご参照いただければ幸いです。