サーバー攻撃の実際

油断は禁物！
素人でもここまでできてしまう

2002年11月9日（土）
堀上　明（ほりかみ　あきら）
技術士（情報工学）
ITコーディネータ

はじめに

本講演の目的

インターネット上に接続されているサーバーを攻撃するには、様々な方法がある。攻撃用に関するツール類も豊富にあり、コンピュータについてあまり詳しい知識がなくても、かなりのレベルまでの攻撃が可能となる。

本講演では、サーバーの攻撃に関する手順について概説し、セキュリティ対策の重要性を再認識する助けとしたい。

内容

Ⅰ．攻撃手順

1．ターゲッティング（その1）

ターゲッティングとは

ターゲットの情報を得るために、合法的に様々な情報を調べること。ハッキングの準備段階。

（1）ＷＥＢページから情報収集
（2）Ｐｉｎｇ
（3）Ｗｈｏｉｓ
（4）ネットワーク経路調査

1．ターゲッティング（その2）

（1）ＷＥＢページからの情報収集

・所在地、住所、電話番号
　企業の場合は、通常記載されている。
　個人の場合でも都道府県はわかる。
・関連企業、関連組織
　リンク、検索エンジンの関連ページ

1．ターゲッティング（その3）

1．ターゲッティング（その4）

（1）ＷＥＢページからの情報収集

・ニュース、近況
　合併、買収などのニュース、会計報告
　個人の場合は日記など
・問い合わせ窓口
　担当者の名前、メールアドレス
・ＷＥＢページ作成者の趣向、性格、言動
　検索エンジンで掲示板やチャット情報を取得

1. ターゲッティング（その5）

（1）ＷＥＢページからの情報収集

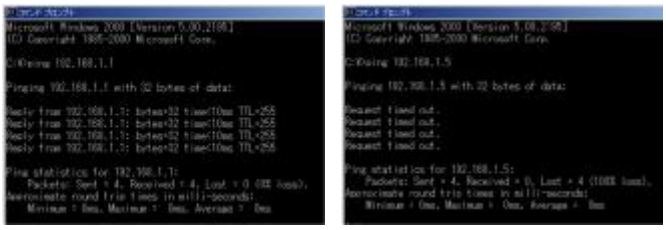
・ホームページを作成したソフト

```
<html>
<head>
<meta http-equiv="Content-Language" content="ja">
<meta http-equiv="Content-Type" content="text/html;
charset=shift_jis">
<meta name="GENERATOR" content="Microsoft FrontPage 4.0">
<meta name="ProgId" content="FrontPage.Editor.Document">
<title>あああああ</title>
</head>
```


1. ターゲッティング（その6）

（2）Ｐｉｎｇ

指定した相手へパケットを送信。返答の有無によって
ネットワーク上に存在しているかどうかを判定



1. ターゲッティング（その7）

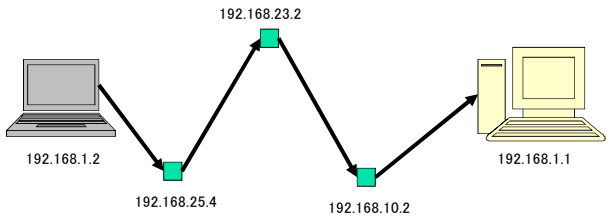
（3）ｗｈｏｉｓ

サーバー情報を確認するサービス

1. ターゲッティング（その8）

（4）ネットワーク経路調査

目的のサーバーまでのネットワーク経路を調べる。



1. ターゲッティング（その9）

（4）ネットワーク経路調査

Linuxの場合　tracerouteコマンド

Windowsの場合　tracertコマンドを使う

例）実行例

```
# traceroute -n 192.168.1.1

traceroute to 192.168.1.1(192.168.1.1), 以下略
1 192.168.25.4 0.536 ms 0.302 ms 0.299 ms
2 192.168.23.2 0.832 ms 0.810 ms 0.807 ms
3 192.168.10.2 32.403 ms 34.193 ms 33.235 ms
4 192.168.1.1 32.777 ms 32.951 ms 31.475 ms
```


2. スキャン（その1）

スキャンとは

ネットワーク上の任意のものを走査して情報を得る。

ポートスキャンが代表的。

（1）Ｐｉｎｇスィープ

（2）ポートスキャン

（3）バナー取得

2. スキャン（その2）

（1）Ｐｉｎｇスィープ

任意に与えられた範囲のＩＰアドレスに対して

どのようなＰＣが稼働しているかを調査。

例）123.45.678.912-920の間で実行

```
123.45.678.912  www.abc.com
123.45.678.913  www.xxx.net
123.45.678.914  www.peakxxx.net
123.45.678.917  www.dorodoro.com
123.45.678.918  www.obake.org
```


2. スキャン（その3）

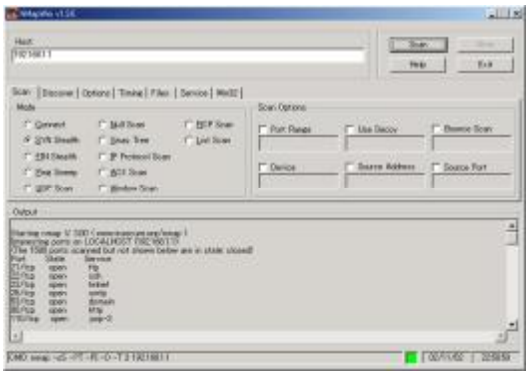
（2）ポートスキャン

サーバーが提供しているポートの開閉を調べる。
調査対象サーバーのＯＳや機種の推測も可能。
不正侵入を果たすための不可欠な行為。ただし、
結果はあくまで推測。

サービスとポート番号の例

ポート番号	プロトコル	内容
20	TCP/UDP	FTP
23	TCP/UDP	telnet
25	TCP/UDP	smtp
80	TCP/UDP	http
110	TCP/UDP	pop3

2. スキャン(その4)



2. スキャン(その5)

(３) バナー取得

telnetやftpで接続した時に表示される情報の取得。
デフォルトでは、サービスの提供するソフトウェアとバージョン情報が取得できる。

例)実行例

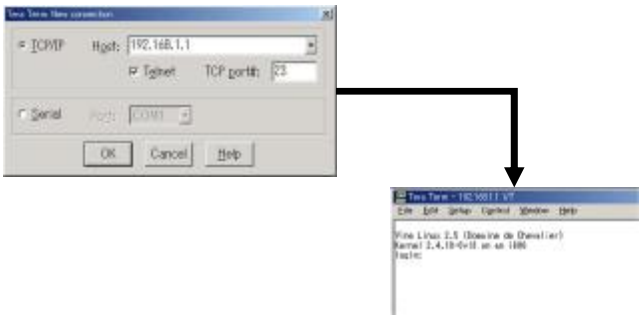
```
$telnet  192.168.1.1

Trying  192.168.1.1...
Connected  to  192.168.1.1

Vine  Linux2.0
Karnel  2.2.14-1v16  on  an  i686
```

バナー

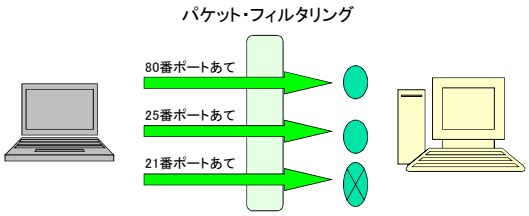
2. スキャン(その6)



3. パケット･フィルタリング調査(1)

パケット・フィルタリング調査とは

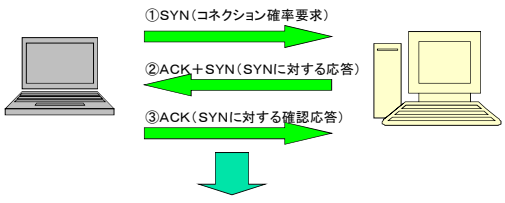
ポートスキャンではわからなかったサービスの存在や、フィルタリング・ルールを推測するための調査。



3. パケット･フィルタリング調査(2)

手順

ＴＣＰ／ＩＰにおけるコネクションの確立の手順。



コネクションの確立

3. パケット･フィルタリング調査(3)

送信するパケットに対する反応を調査する。

hping2 –n –c 5 –p ＜ポート番号＞ -s ＜IPアドレス＞

送信パケットと送信元ポート番号を組み合わせて反応を調査する。

フィルタリングされていてもセッションを確立することができる場合がある。

送信したパケット	SYN	FIN	ACK
開いているTCPポート(21)から返信されるパケット	SYN+ACK	返信なし	RST+ACK
閉じているTCPポート(113)から返信されるパケット	RST+ACK	RST+ACK	RST+ACK
フィルタリングされているTCPポート(22)から返信されるパケット	返信なし	RST+ACK	RST+ACK

4. サービス調査(その1)

サービス調査とは

開いているポートに対して接続し、サービスの特定や動作状況を調べるもの。

（１）アプリ種類特定
（２）メール・ユーザー割りだし
（３）ＤＮＳ情報取得

4. サービス調査(その2)

(１) アプリ種類特定

前述の２（３）バナー取得で情報を得る。

```
C:ftp  192.168.50.1

Connected  to  192.168.50.1

220  target1  Microsoft  FTP  Service  (Version  4.0).
User  (192.168.50.1©none)):
```

4. サービス調査（その3）

（２）メールユーザー割り出し

ユーザー推測
リスト作成
user.txt

```
james
taro
admin
root
```

```
# smtp-cracker -h 192.168.1.1 -i user.txt -o result.txt -v

Connected to 192.168.1.1
using [VRFY] command
status: 100%
found 2 users in 1013857113 seconds
```

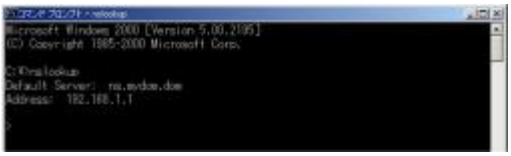
結果
result.txt

```
mail file for192.168.1.1
taro
root
```


4. サービス調査（その4）

（３）ＤＮＳ情報取得

ＤＮＳに問い合わせて情報を取得。



5. パスワード調査（その1）

パスワード調査とは

サービスのそれぞれの認証において、容易に推測できるパスワードが設定されていないか調査すること。

（１）ブルートフォースアタック

専用辞書等を用いて、パスワードを総当たりで当てはめ、パスワード文字列を自動的に見つけ出す攻撃。

5. パスワード調査（その2）

（１）ブルートフォースアタック

6. 脆弱性情報収集（その1）

脆弱性情報収集とは

サービス調査で取得した情報に関する脆弱性情報を調べること。

（１）情報収集

（２）情報検証

6. 脆弱性情報収集（その2）

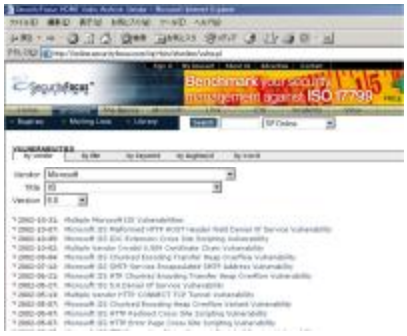
（１）情報収集

ａ．ターゲットサーバーの脆弱性調査（ツール）

6. 脆弱性情報収集（その3）

（１）情報収集

ｂ．脆弱性情報



6. 脆弱性情報収集（その4）

（２）情報検証

収集した脆弱性調査結果を元に、攻撃を試みる。

・Ｗｅｂページ書き換え

・ログの消去、書き換え

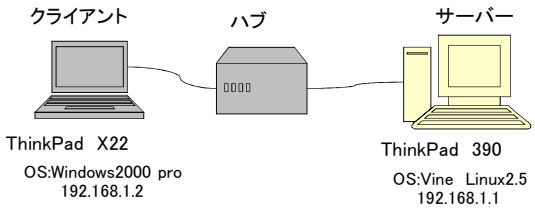
・ファイル消去、改ざん

などなど

II. デモ

１．デモ環境
２．Ｐｉｎｇ
３．ポートスキャン
４．脆弱性情報収集（バナー取得）
５．パスワード調査

II. デモ環境



III. まとめ

あたりまえのことですが．．．

サーバー攻撃に関してはツールが充実しており、セキュリティの甘いサーバーは、簡単に攻撃される。

また、直接のサーバー攻撃以外に、ウィルス対策なども必要である。

従って、サーバーを運用する場合は攻撃の種類を知っておくとともに、常に最新の情報を収集し、セキュリティ対策を怠ってはならない。

IV. 参考資料

１．「日経ネットワークセキュリティ 2002 Vol.1」
日経ＢＰ社 パソコンベストムック 2002年３月
２．「ハッカーの教科書」
データハウス社 IPSIRON著 2001年11月