第３回愛媛県インターネット・セキュリティセミナー

「ネットトラブル防衛&追跡・実践テクニック」

ー　　WEB110 からー

WEB110 代表　吉川誠司

1.ネットオークション詐欺の傾向と対策
2.出会い系サイトの深刻な被害事例
3.加害者の追跡テクニック
4.ブロードバンド時代のセキュリティー
5.コンピュータウィルス
6.通信傍受ソフトの脅威

1.オークション詐欺

●ポイント

相手の身元が判明している場合を除き、被害者が自力で解決するのは困難。
騙されてしまった後での救済方法は、容疑者が逮捕されない限り「ほぼない」。
大事なことは、被害に遭わないための万全の対策をとっておくこと。

●巧妙化する手口

オークションシステムの外で行われる取引
詐欺としての立件を免れる手口

●詐欺師の七つ道具

①偽造の身分証明書
②架空口座
③民間私書箱
④レンタルオフィス
⑤フリーメール
⑥無料プロバイダー
⑦プリペイド携帯電話

●騙されないためのチェックポイント

①現住所、固定電話番号の確認

mapion<http://www.mapion.co.jp/>

e-map<http://www.e-map.co.jp/>

インターネットタウンページ<http://itp.ne.jp/>

エンジェルラインの活用<http://www.ntt-east.co.jp/angel/>

②実メールアドレスの要求

③代金引換での取引

④エスクローサービスの利用

⑤評価システムの活用

●事後対策

①振込銀行へ組み戻し請求

②取引相手の通信ログの保全をオークション主催者に依頼する

③評価欄などで他の被害者がいないかを確認する

④被害者が複数いる事実と、相手からのメール、振込控え持って警察本部へ被害届提出

2.出会い系サイト

●トラブルのパターン

個人情報の悪用
脅迫
恐喝
美人局
窃盗
キャッチセールス
ぼったくり
ストーカーへの変貌

3.加害者の追跡テクニック

①メッセージヘッダーから発信地の割り出し
②Whois データベースの活用
②おとり捜査
③ロボット検索エンジンの活用
④過去の接触者への聞き取り捜査
⑤トラップメール、トラップサイト

4.ブロードバンド時代のセキュリティー

2001 年上半期（1 月− 6 月）の不正アクセス事件：959 件（2000 年の約 9 倍）
うち、ホームページを書き換え、データ消去などの被害：678 件
不正アクセスのターゲット：一般企業が 330 件と最多
不正アクセス被害の原因：公表されているセキュリティーホール

●何が危険なのか
情報盗み見、データ破壊、第三者への不正侵入や DDOS(分散型サービス妨害)攻撃等の踏み台にされる
●接続形態の違いによる危険度差

1.ダイヤルアップ接続と常時接続の危険度差

2.ADSL と CATV の危険度差

3.接続方法による危険度差

●クラッカーの侵入方法

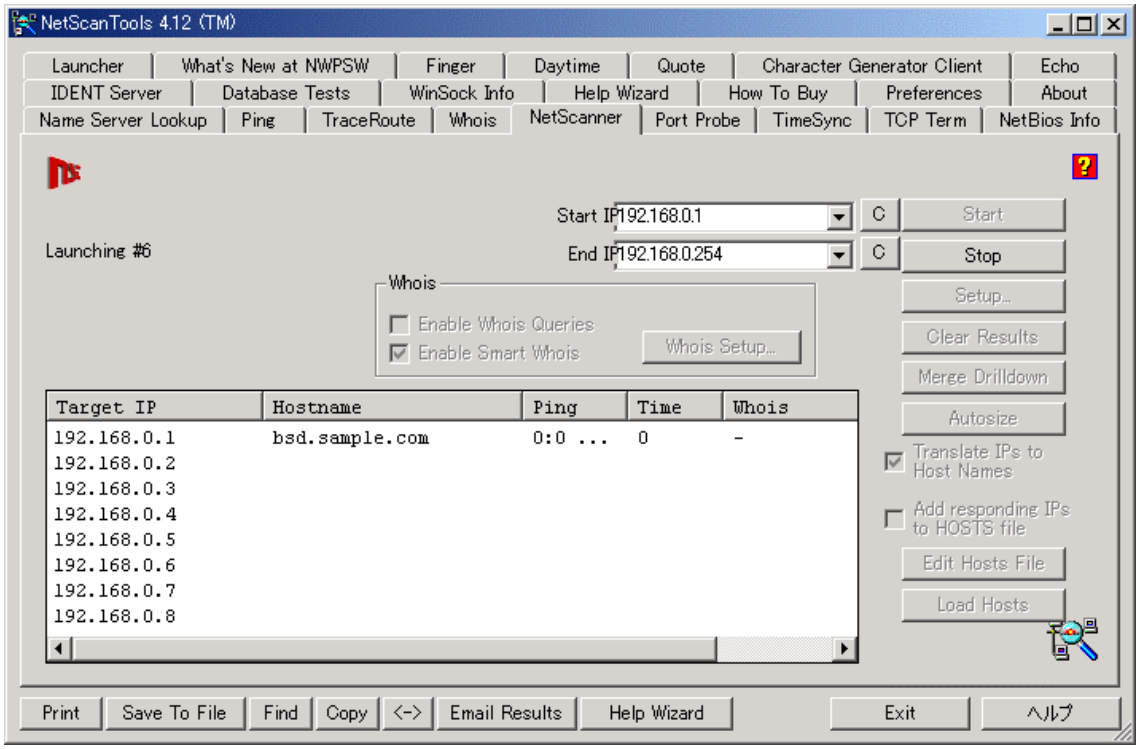
1.ターゲットの選定方法

クラッカーが最初に行うことは、いかに簡単に侵入できるコンピューターを探し出すか、ということ….。

2.IP スキャン

まずはスキャニングツールを用い、例えば「202.232.0.1ー202.233.10.224」などのある範囲を無作為もしくは作為的に指定し、そこにあるインターネットに接続されたコンピュータを探しだす。

NetScan Tools の NetScanner

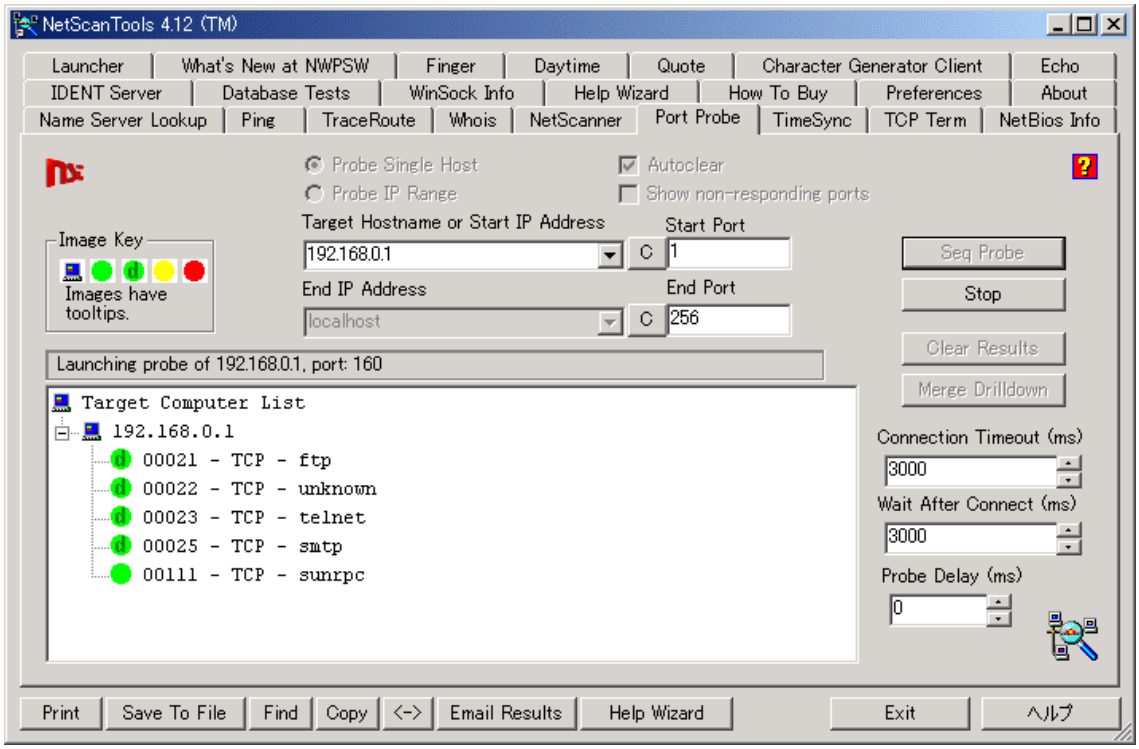


3.ポートスキャン

留守宅を確認した後（つまりアクティブなグローバル IP アドレスを特定した後）は、そのコンピュータのどこが甘いのか（どんなサービスが開いているか）を改めてスキャンしていく。こうした行為は「ポートスキャン」と呼ばれている…。

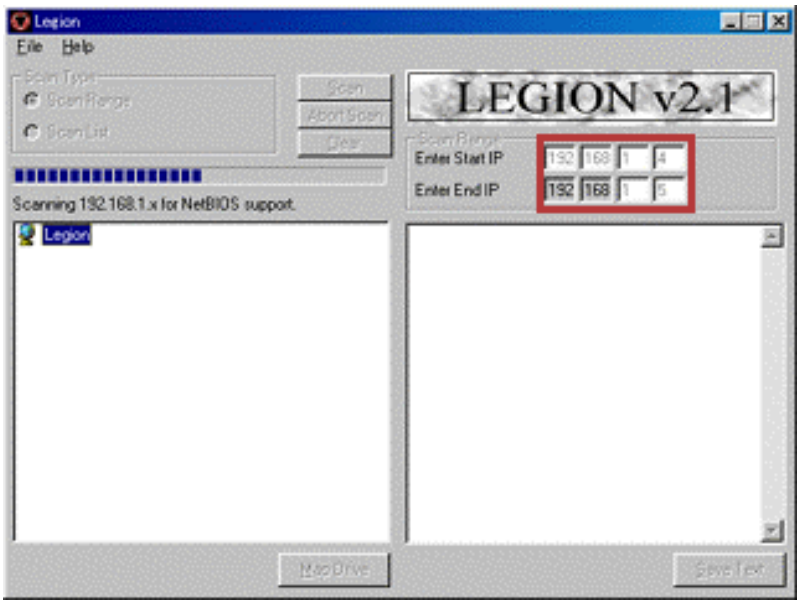
ポートスキャンを行うためのツールもネット上で容易に手に入る…。

NetScan Tools の PortProbe

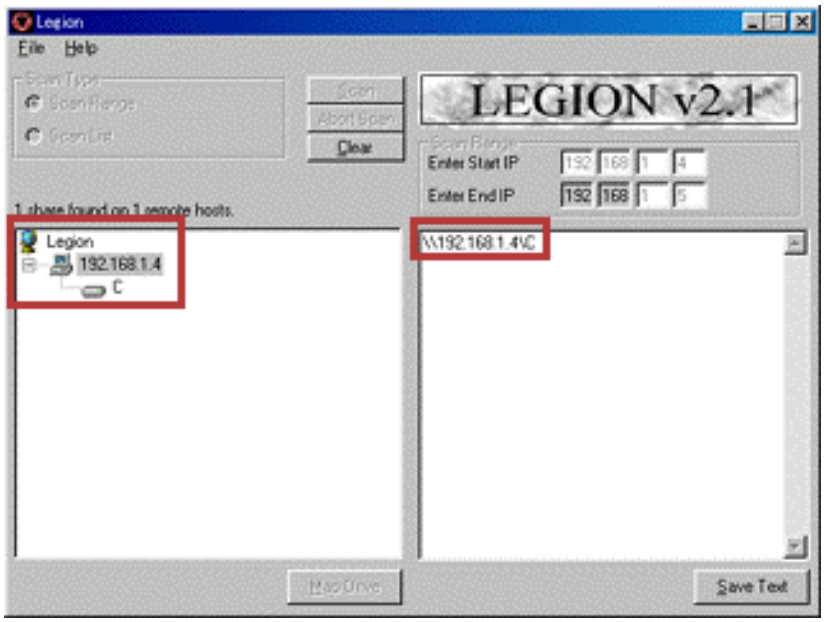


4.ファイル共有からの侵入

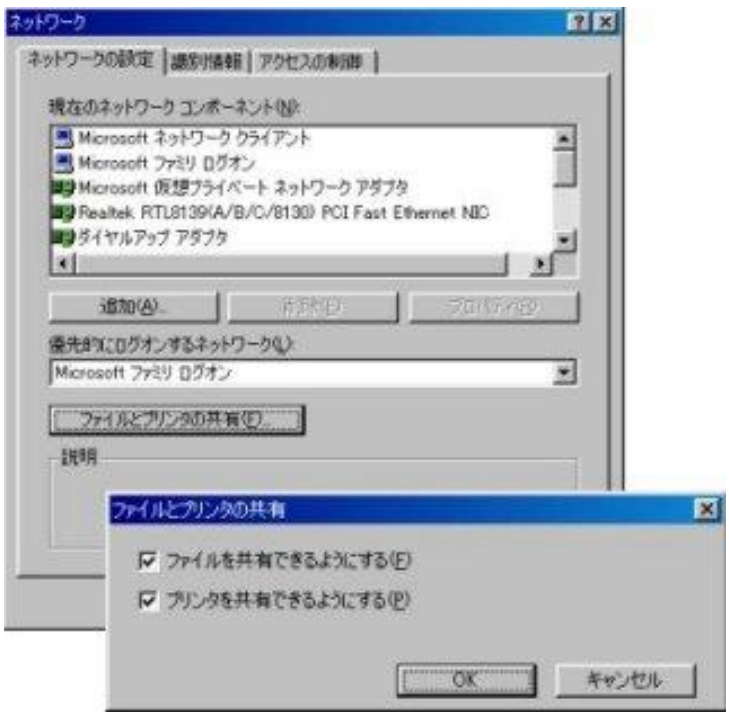
Windows95/98/Me を使用している場合、ファイル共有の設定行っていると、ここから侵入されてしまう可能性がある。ファイル共有からの侵入は、相手のグローバル IP アドレスがわかっていればアタックすることができるためポートスキャンは行なわず、「Legion v2.1」などの専用ツールを使用する…。



あとは「Scan」ボタンをクリックするだけで自動的にスキャニングを開始し、ファイル共有可能なコンピュータの IP アドレスと共有フォルダ、ドライブを表示してくれる。



ファイル共有を使用するのであれば、万が一侵入されても被害の少ないフォルダを作成し、ルーターやファイアウォールを使用し、ファイル共有サービスつまり NetBIOS のポート（137、138、139）を塞ぐことでインターネット経由の侵入を阻止することができる。もちろんファイル共有を使用する必要がなければサービス自体を停止するか、もしくはアンインストールしてしまうのがベスト。



5.トロイの木馬を使用した侵入

トロイの木馬を利用した侵入は「BackOrifice」「NetBus」に代表されるリモート操作ツールが有名。Macintosh であっても同様に「TakeDown」などのリモート操作ツールがある…。

●ユーザーレベルの対策

1.ルータによるパケットフィルタリング

①ルータ選びのポイント

・スループットとセキュリティー性能のバランス

・デフォルトでのパケット・フィルタリングの強度

ステートフル・パケット・インスペクション（SPI 機能）

ダイナミック・パケット・フィルタリング

侵入検知・通知システム（IDS）

閉じるべきポート表（http://web110.com/defence/ port.html）

トロイの木馬が使用するポート表（http://web110.com/defence/toroj.html）

2.ソフトウェアファイアーウォール

○Norton Internet Security

http://www.symantec.com/region/jp/products/nis/index.html

○ウィルスバスター2002

http://www.trendmicro.co.jp/product/vb2002/index.asp

○ZoneAlarm

http://www.zonelabs.com/

○BlackICE Defender

http://www.toyo.co.jp/security/ids/product/bi_dfndr.html

○Tiny Personal Firewall

http://www.tinysoftware.com/pwall.php

○ZoneAlarm　Pro 体験版

http://www.zonelabs.com/zap_download_trial_10.htm

○ZoneAlarm 日本語化パッチ

http://etcd.virtualave.net/zaj.html

●診断サービスを利用する

「Symantec Security Check」

（ファイアーウォール、Proxy、NAT/IP マスカレードは診断不可）

http://www.symantec.co.jp/region/jp/securitycheck/index.html

その他の自分のマシンをスキャンできるサイト。

○Shields Up！<https://grc.com/x/ne.dll?bh0bkyd2>

[ShieldsUP!] アイコンをクリックすると、コンピュータがスキャンされます。

日本語の説明ページは<http://www.upsizing.co.jp/news/report0426.htm>

5.コンピュータウィルス

●ウィルスの傾向

ウィルスの感染経路の 90%はメールから……

●ウィルスの見抜き方と感染時の対処法

１：こんなメールがウィルスメール

差出人、件名、本文が空白で、添付ファイル付きのメールはウィルスの可能性大。

添付ファイルの拡張子が「exe」「pif」「doc」「xls」に関しては要注意。

2：ウィルスプログラムを実行してしまったら…

トレンドマイクロ・ウィルスバスターオンラインスキャン

http://www.trendmicro.co.jp/hcall/scan.htm

●普段のウィルス対策

１：知人からのメールでも添付ファイルは不用意に実行しない。

２：ウィルス定義ファイルは常に最新のものに更新しておく。

3：ブラウザーのアクティブスクリプトはオフにしておく。

4：HTML メールの受信を拒否できるメールクライアントに変更する。

5：OS のセキュリティーパッチを当てておく

6.通信傍受ソフトの脅威

●パケット盗聴

盗聴することによって得られる情報

1. ユーザ名とパスワード
2. メールの内容
3. クレジットカードの情報
4. 住所や電話番号等の個人情報

① 盗聴の手法

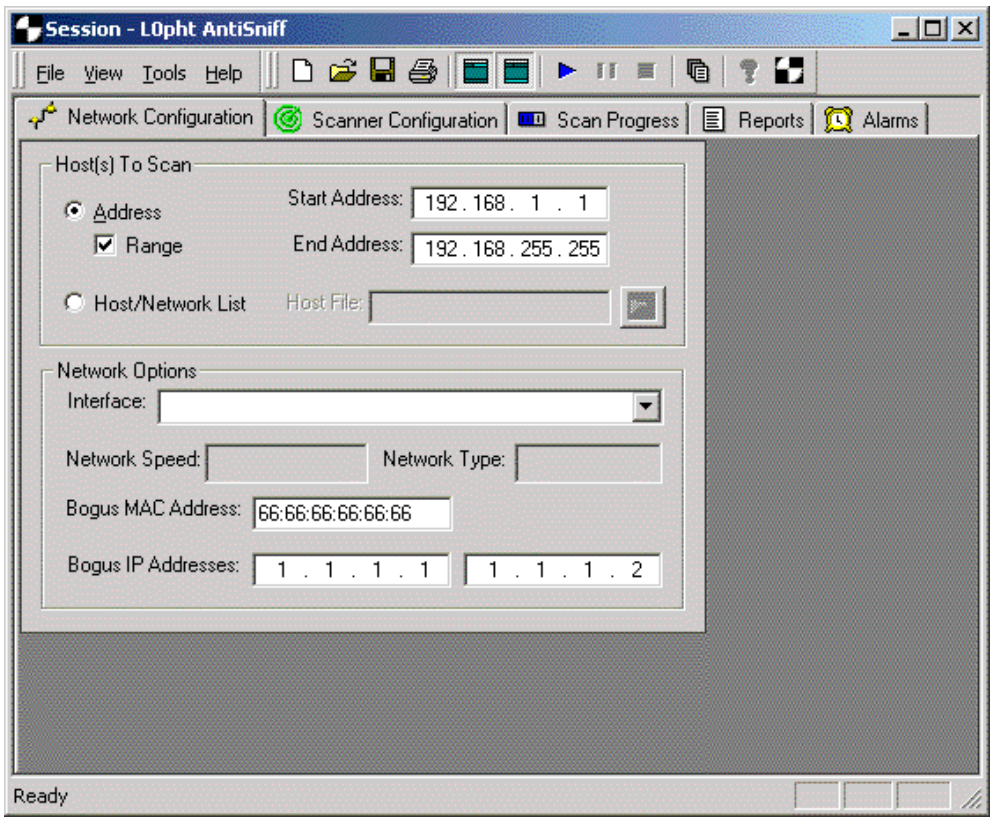
②盗聴を防ぐには

盗聴を防ぐには、インフラ/アプリケーション/監視の 3 つの側面から考えて行くことが必要である…。

③パケットモニタを発見するには

Windows 環境で動作するパケットモニタ発見ツール

AntiSniff（http://www.securitysoftwaretech.com/antisniff/）



●スパイウェア

①スパイウェアとは

スパイウェアと疑わしいソフトウェアは 900 種類程度確認されている。実際にどういったソフトウェアがスパイウェアなのか「SpyChecker」「Spyware List」といったスパイウェアのリストなどを利用して自分の使用しているソフトウェアなどと照らし合わせてみよう…。

②スパイウェア対策

スパイウェアの対策は、ソフトウェアに含まれるスパイプログラムの除去、もしくはサーバへの情報送信のフィルタリングということになるだろう…。

スパイプログラムの除去するソフトウェア

Lavasoft の「Ad-aware 5.62 Final」（フリーソフトウェア）

（http://www.lsfileserv.com/aaw.html）

スパイウェアによる情報送信をブロックするには、情報の送信先をローカルホストとすることで情報送信をブロックする「SpyBlocker」や、スパイウェアを検知しフィルタリングを行ってくれる「ZoneAlarm」などのソフトウェアファイアウォールを導入するとよいだろう。

SpyBlocker

http://personal.atl.bellsouth.net/mia/k/r/kryp/sb.htm