

backtrack における侵入テストの実用性

杉山 仁(山梨大学 総合情報処理センタ)

sugiyama[atmark]yamanashi.ac.jp

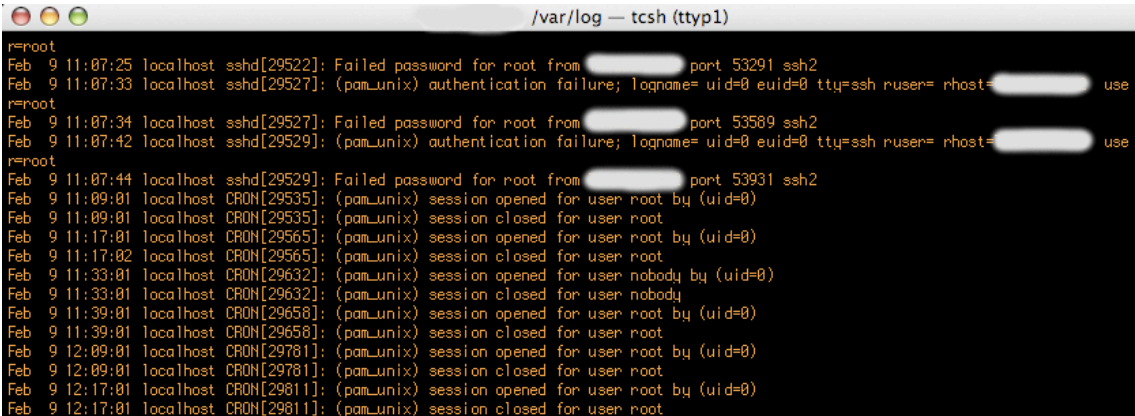
1. はじめに

インターネットが発達し、誰もが高速な環境で気軽に**Web**で情報を検索したり動画を観たりと一昔前では考えられないに時代になりました。

過去では、一部のユーザーのみがインターネットサービスを利用していましたが、現在では誰でも乗り入れるようになり、それに伴い悪意を持ったユーザーも増えているのが現状です。

性善説で運用されてきたネットワークも、現在では悲しいことですが性悪説で運用することが、必然になってきました。

現在、総合情報処理センタで運用しているサーバ群にも国内外から毎日のようにアタックが発生しています。



```

/var/log - tcsh (tty1)
r=root
Feb 9 11:07:25 localhost sshd[29522]: Failed password for root from [redacted] port 53291 ssh2
Feb 9 11:07:33 localhost sshd[29527]: (pam_unix) authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[redacted] use
r=root
Feb 9 11:07:34 localhost sshd[29527]: Failed password for root from [redacted] port 53509 ssh2
Feb 9 11:07:42 localhost sshd[29529]: (pam_unix) authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=[redacted] use
r=root
Feb 9 11:07:44 localhost sshd[29529]: Failed password for root from [redacted] port 53931 ssh2
Feb 9 11:09:01 localhost CRON[29535]: (pam_unix) session opened for user root by (uid=0)
Feb 9 11:09:01 localhost CRON[29535]: (pam_unix) session closed for user root
Feb 9 11:17:01 localhost CRON[29565]: (pam_unix) session opened for user root by (uid=0)
Feb 9 11:17:02 localhost CRON[29565]: (pam_unix) session closed for user root
Feb 9 11:33:01 localhost CRON[29632]: (pam_unix) session opened for user nobody by (uid=0)
Feb 9 11:33:01 localhost CRON[29632]: (pam_unix) session closed for user nobody
Feb 9 11:39:01 localhost CRON[29658]: (pam_unix) session opened for user root by (uid=0)
Feb 9 11:39:01 localhost CRON[29658]: (pam_unix) session closed for user root
Feb 9 12:09:01 localhost CRON[29781]: (pam_unix) session opened for user root by (uid=0)
Feb 9 12:09:01 localhost CRON[29781]: (pam_unix) session closed for user root
Feb 9 12:17:01 localhost CRON[29811]: (pam_unix) session opened for user root by (uid=0)
Feb 9 12:17:01 localhost CRON[29811]: (pam_unix) session closed for user root

```

学内で運用しているLinuxサーバのssh アタックの形跡

特に、組織で運営しているネットワークですので、踏み台にされて、そこから別のネットワークへの攻撃の拠点にされてしまいますと、組織としての信用が失われます。

今では、どこの組織も**firewall**を導入して必要なサービスをしているサーバや使用しているサービスポート以外は、外部との接続は遮断していると思いますが、今までの外部攻撃が**firewall**によって効かなくなった分、内部から

の攻撃にシフトしているとの調査結果もあります。(※1)

そこで、攻撃に対し耐えられるシステム構築をしているか、侵入テストの分野に設計・開発されたLinuxディストリビューションであるbacktrackを使用
して安全確認する方法を報告いたします。

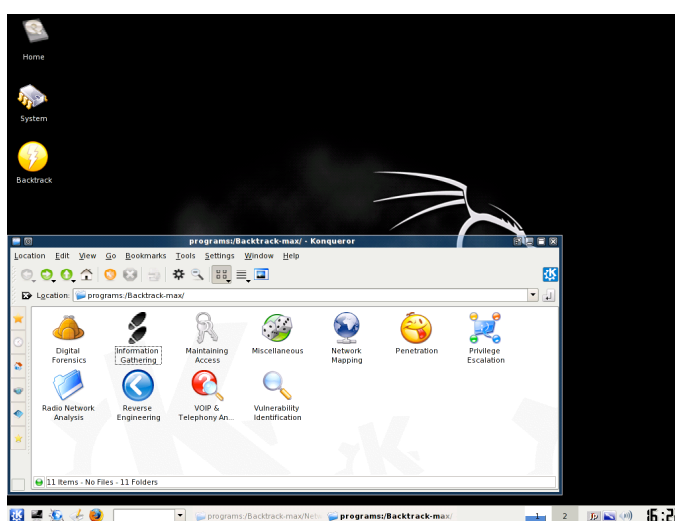
Debian,OpenSUSE,FreeBSD等のPC-UNIXが稼働するPCで各種ツールをインストールすれば済むと考えるかも知れませんが、backtrackのCDまたはUSBを持ってさえいれば、どこでもテスト可能であることと、各種ツールのインストール作業が必要ないのは大変魅力的です。

2. backtrackとは

侵入テストの分野に設計・開発されたLinuxディストリビューションであり、侵入や攻撃のツール群が予めインストールされています。

公式サイト(※2)より、ライブCD版とUSBドライブ版、VMware版の3種類がダウンロード可能です。

USB版・Vmware版の使用が、使い勝手が良いと思います。それはOSの設定変更が反映されるからです。ライブCDでの使用は、変更した設定等を保存する領域がありません。ただ、USB版はUSBへのインストールする為のものですが、インストールが多少苦勞するかも知れません。使用するにあたりもっとも簡単なのは、ライブCD版又はVMware版の使用です。今回は、VMware版を使用しています。



起動したbacktrack3 既にツール類がインストールされている。

デスクトップ環境はKDE

3. 調査の流れ

backtrackに各種ツールがあっても、調査するにあたり適当にツールを使用しても効率的ではありません。

ここは、クラッカーの立場として考えて見る必要があります。

3.1 情報の収集

ターゲットとなるホストや、該当するネットワークを決めます。

webでの検索、**nslookup,whois**コマンド等で調査を行います。

特に**Netcraft**(※3)のサイトは、非常に便利です。

3.2 スキャンニング

調査対象のホストに対し、そのホストがどのような**OS**でどのようなサービスを行っているのかを調査します。**OS**や提供しているサービスがわかれば攻撃手段が絞れてくるからです。

サービスは、開いているポートを発見したら、**telnet**コマンド等でサービスバナー情報を取得すれば、さらに詳細がつかめます。防御側としてはバナーを表示しない、もしくは偽りの情報を表示するように設定を変更するとよいでしょう。

3.3 侵入

調査対象のホストの**OS**・サービスのバージョンをスキャンニングで調査した後、そのホストの脆弱性をつく**Exploit**を仕掛けます。リモートログイン可能な状態(**FTP,Telnet,ssh**等のサービスが稼働)の場合は、ソフトの初期設定で使用しているユーザー名・パスワードや、ホスト名や組織の名称、組織の**web**から得た情報(メールアドレス等)から予測したユーザー名とパスワード、そしてパスワード辞書を使用した総当たり攻撃も有効です。

侵入に成功した場合、そのユーザーから管理者権限のあるユーザー(**root,administrator**など)へスイッチする場合も**Exploit**を使用します。

管理者権限さえ取得出来れば、そのホストは自分のものになったようなものです。バックドアを仕掛けたり、そのホストを踏み台にして他のホストへの接続をしたり(組織内の接続は甘い場合も多い)、自分のファイル置き場でも自由に使用出来ます。

3.4 証拠隠滅

侵入したホストで作業をすれば、その作業内容がそのままlogとして保存されます。logから侵入されたことが判明すれば、そのホストは二度と使えません。そこで侵入した形跡を消去します。該当のlogを消去するツールもネット上で公開されています。

防御側としては、例えば改竄されたlogでも侵入と判断出来る場合もあります。ある時間帯だけlogが不自然である、log自体のファイルサイズが0(/dev/nullへのシンボリックリンク)など、証拠を削除されても何かしら違和感があります。注意深くlogを確認することが大切です。

4. ツールの使用

4.1 攻撃の第一歩

まずは、攻撃対象のサーバがどのようなサービスを提供しているか調べます。サービスを調査するには、ポートスキャンを行います。

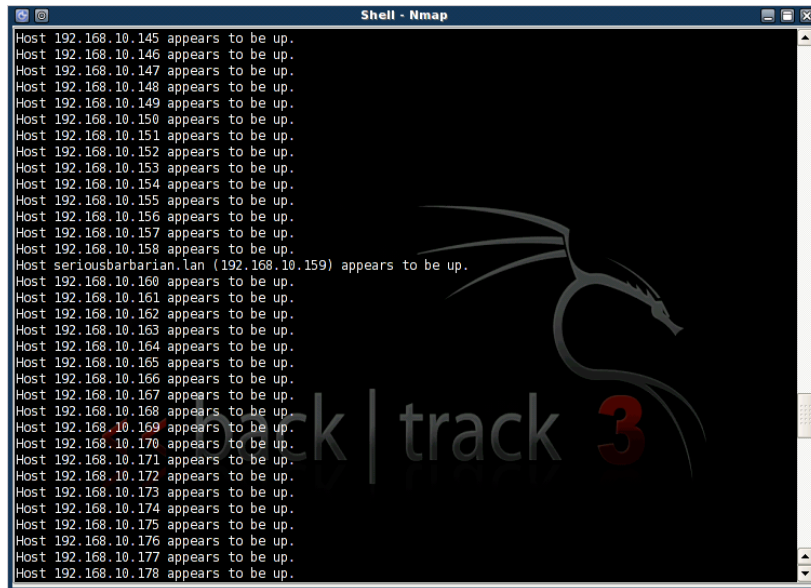
Nmap(※4)は、Windowsでも稼働する最もポピュラーなツールです。あらゆるOS用のbinaryやソースコードが公開されているので、特にbacktrackだから楽に使えるというものではありません。

Nmapは、KDEメニューから”Backtrack→Network Mapping→All→Nmap”にあります。

ネットワーク上にサービスポートの開いているホストを探す場合は、以下のコマンドオプションでスキャンします。

```
nmap -v -sP 192.168.10.0/24
```

IPアドレスの第三オクテットまでが192.168.10.*のネットワーク上に存在するホストをスキャンしています。



```
Host 192.168.10.145 appears to be up.
Host 192.168.10.146 appears to be up.
Host 192.168.10.147 appears to be up.
Host 192.168.10.148 appears to be up.
Host 192.168.10.149 appears to be up.
Host 192.168.10.150 appears to be up.
Host 192.168.10.151 appears to be up.
Host 192.168.10.152 appears to be up.
Host 192.168.10.153 appears to be up.
Host 192.168.10.154 appears to be up.
Host 192.168.10.155 appears to be up.
Host 192.168.10.156 appears to be up.
Host 192.168.10.157 appears to be up.
Host 192.168.10.158 appears to be up.
Host seriousbarbarian.lan (192.168.10.159) appears to be up.
Host 192.168.10.160 appears to be up.
Host 192.168.10.161 appears to be up.
Host 192.168.10.162 appears to be up.
Host 192.168.10.163 appears to be up.
Host 192.168.10.164 appears to be up.
Host 192.168.10.165 appears to be up.
Host 192.168.10.166 appears to be up.
Host 192.168.10.167 appears to be up.
Host 192.168.10.168 appears to be up.
Host 192.168.10.169 appears to be up.
Host 192.168.10.170 appears to be up.
Host 192.168.10.171 appears to be up.
Host 192.168.10.172 appears to be up.
Host 192.168.10.173 appears to be up.
Host 192.168.10.174 appears to be up.
Host 192.168.10.175 appears to be up.
Host 192.168.10.176 appears to be up.
Host 192.168.10.177 appears to be up.
Host 192.168.10.178 appears to be up.
```

実行した結果、192.168.10.159にホストがありました。
発見したホストに対して、再度以下のコマンドオプションで実行してみます。

```
nmap -v -A -O 192.168.10.159
```

下記は、nmap実行結果を一部抜粋したものです。

```
PORT STATE SERVICE VERSION
21/tcp open  tcpwrapped
22/tcp open  ssh      OpenSSH 5.1 (protocol 1.99)
|_ SSH Protocol Version 1: Server supports SSHv1
514/tcp  filtered shell
3689/tcp open  rendezvous Apple iTunes 8.0.2
Device type: storage-misc|remote management|switch|broadband router|VoIP gateway|general purpose
Running (JUST GUESSING) : BlueArc embedded (90%), IBM embedded (87%), HP embedded (87%), Allied Telesyn embedded (86%), Netopia embedded (85%), Vegastream embedded (85%), SCO OpenServer 5.X (85%)
Aggressive OS guesses: BlueArc Titan 2100 NAS device (90%), IBM BladeCenter management module (firmware BRET85L), IBM System Storage TS3100/TS3200 Express Model tape library, or HP StorageWorks MSL2024 tape library (87%), Allied Telesyn AT-9448Ts/XP switch (86%), Netopia 3346N or 3397GPB ADSL router (85%), Vegastream Vega 400 VoIP Gateway (85%), SCO OpenServer 5.0.7 (85%), SCO OpenServer 5.0.7 (x86) (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: -73 hops
TCP Sequence Prediction: Difficulty=256 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Mac OS X

TRACEROUTE (using port 21/tcp)
HOP RTT ADDRESS
1 1.26 192.168.75.2
2 3.01 seriousbarbarian.lan (192.168.10.159)
```

この結果により、該当のIPはsshdが稼働しているMac OSXのホストだと判断します。

このように、簡単に稼働しているホストや、そのホストが提供しているサービスが簡単にわかります。

4.2 Metasploit Framework

攻撃対象のホストのOSがわかれば、そのOSにあわせた攻撃が出来ます。

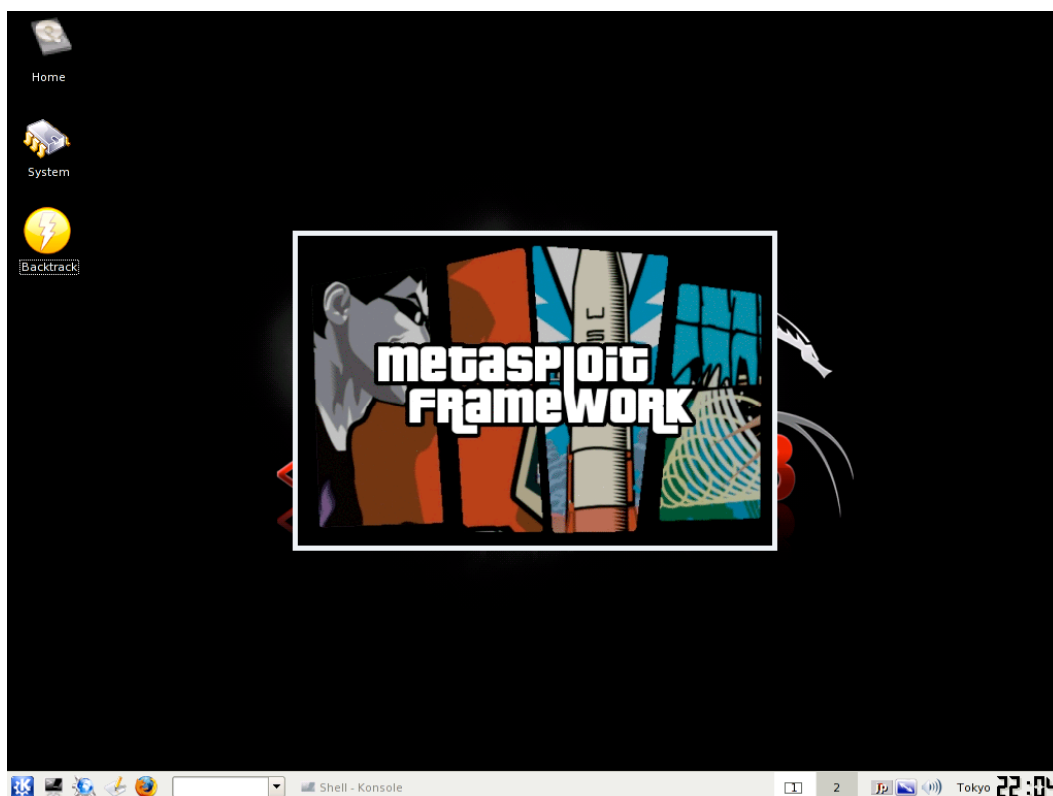
Packet Storm(※5)等のサイトからツールをダウンロードしインストールするのは大変面倒な作業です。

backtrackには、Metasploit Framework(※6)という強力なExploitツールがあります。

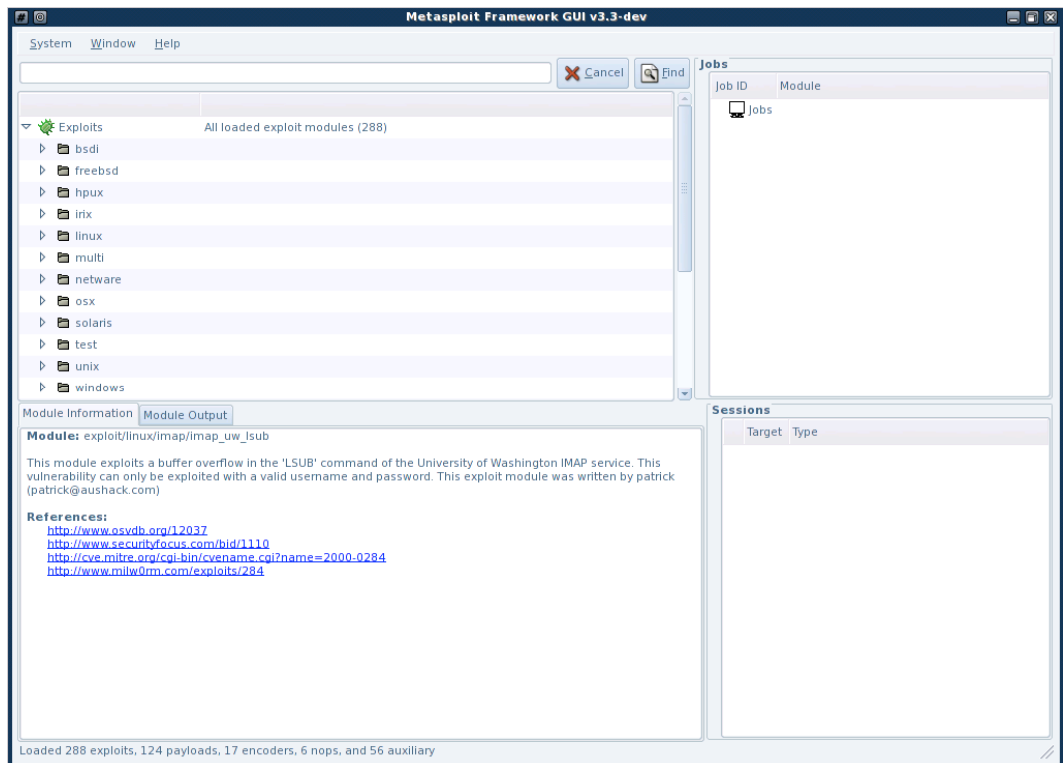
KDEメニューから”Backtrack→Penetration→Framework Version3”に関連のツール群があります。

まずは、”Framework3-MsfUpdate”を実行します。

実行後、Metasploit Frameworkは最新状態になります。そして”Framework3-MsfGUI”を実行します。



Metasploit Framework 起動画面(某ゲームを真似ています☺)



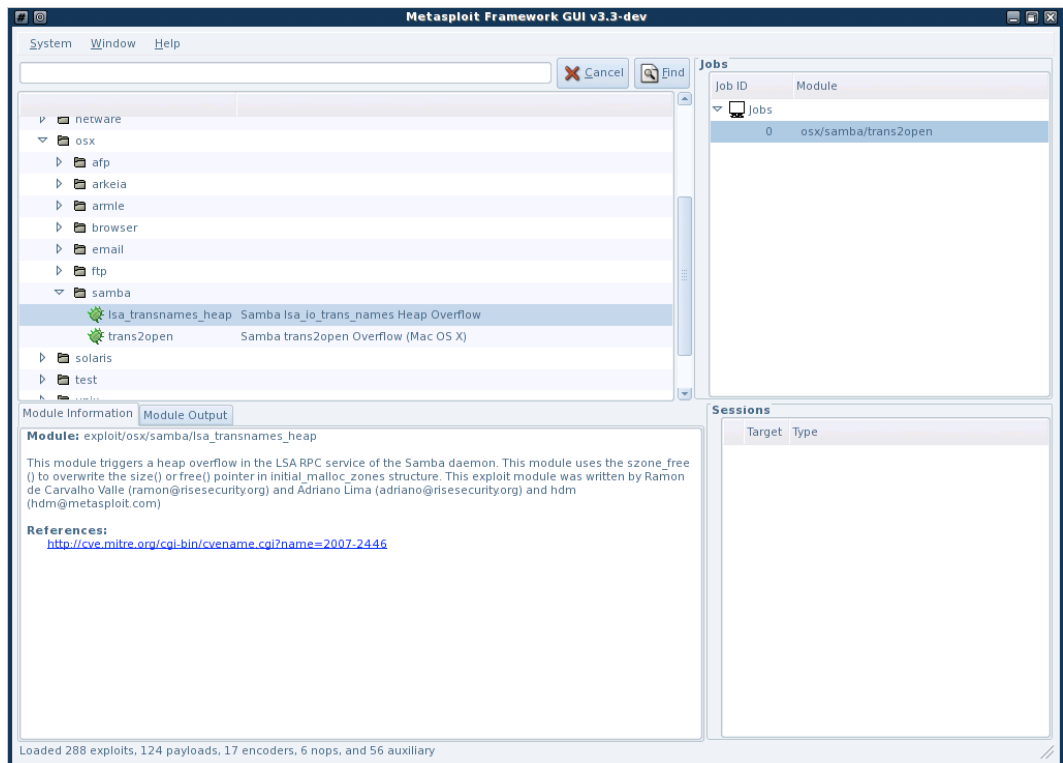
Metasploit Framework メイン画面

画面を見ると、**Exploits**(OSの脆弱性を利用するツール),**Auxiliary**(攻撃ツール),**OS**ごとに分類されています。項目をクリックすることにより、簡単に利用出来ます。

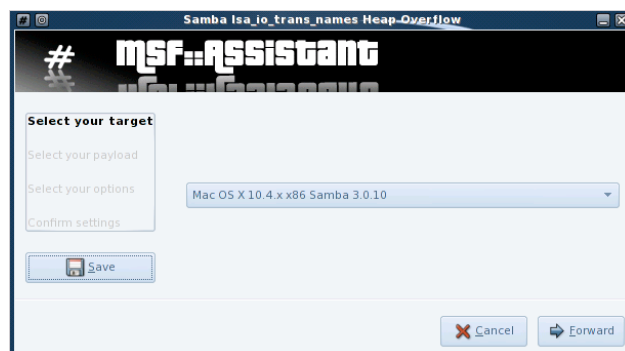
今回、時間の関係で検証用のサーバ(古い**OS**やパッチの当たってない**OS**)が用意出来なかったため脆弱性確認することは出来ませんでした、**OSX**の**samba**への攻撃例を示します。

この脆弱性は**OSX 10.4.X**の脆弱性です。今回の攻撃対象は**OSX 10.4.X**ですが、既にパッチ対応済みの為、失敗に終わります。

http://support.apple.com/kb/HT1457?viewlocale=ja_JP



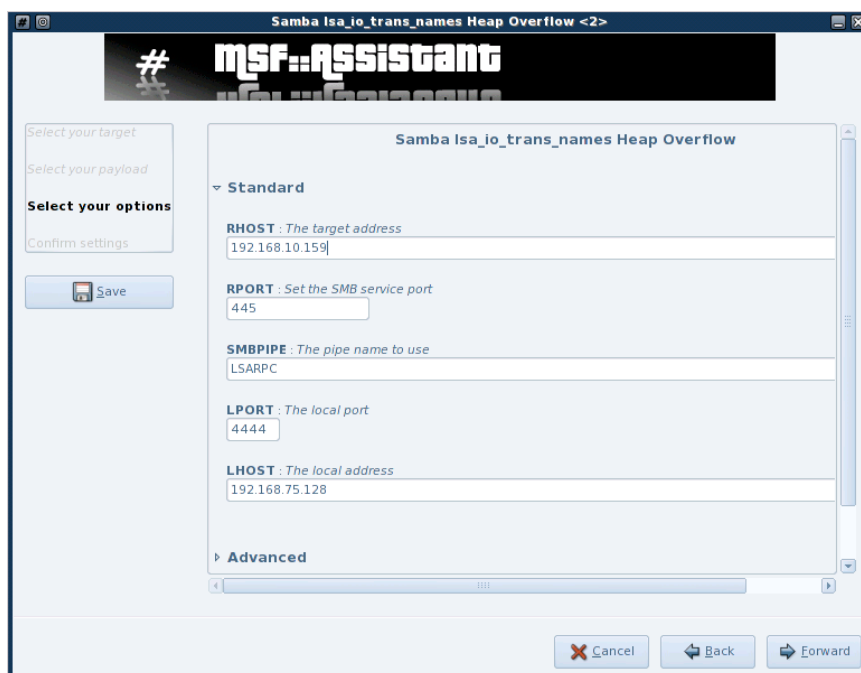
画面の“Expolits→osx→samba→Isa_transnames_heap”をダブルクリックで選択します。



攻撃対象のOSとサービスのバージョンが表示されます。
”Forward”ボタンを押下します。



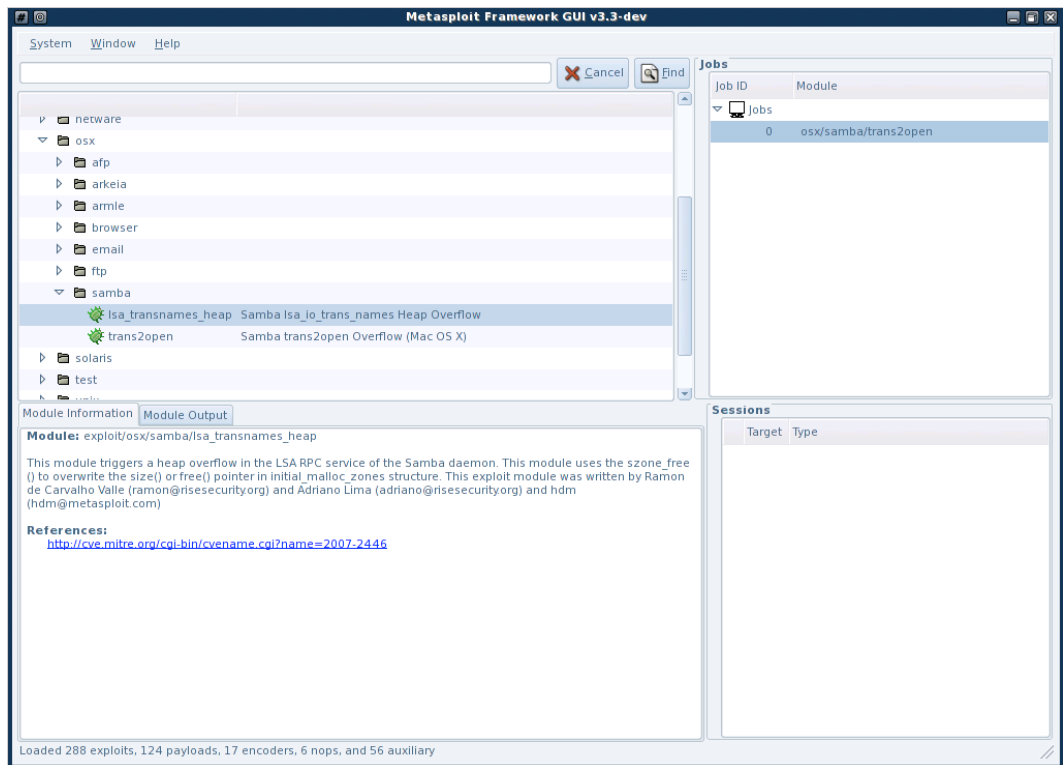
攻撃対象のホストのshellが使用出来るオプションを選択し、“Forward”ボタンを押下します。



攻撃対象のIPアドレスを入力し、“Forward”ボタンを押下します。



設定を確認し、“Apply” ボタンを押下すると攻撃が始まります。



右上のjobが実行中の攻撃

攻撃に成功すると、右下のSessionに攻撃したホストが表示されshellが実行可能になります。

今回は、失敗したため、右上のjobの表示が無くなるだけでした。

4.3 Hydra

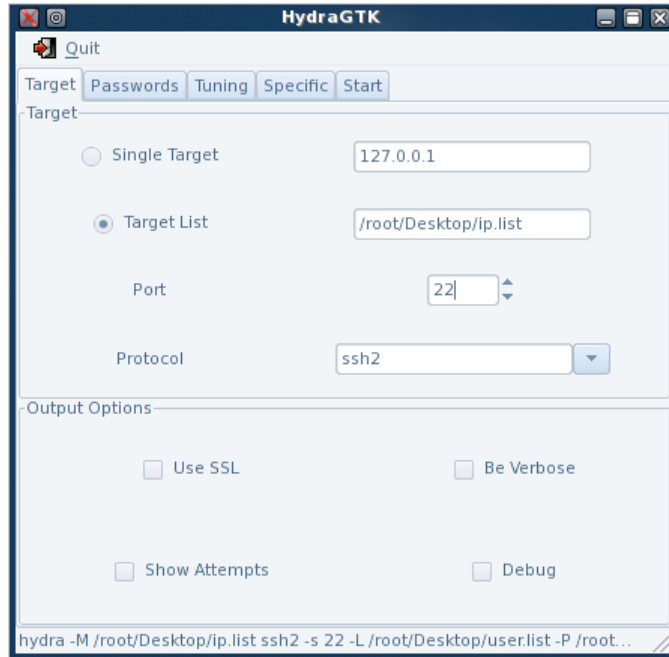
Nmapで調査した結果OSXのホストにsshdが動いていました。そこでsshで、そのホストに接続してみたいと思います。

総合情報処理センタで運用しているサーバ群にも国内外から毎日のようにssh攻撃が発生しています。IDとパスワードの辞書ファイルを使用し、コンピュータに疎いユーザーのIDとパスワードを総当たりで探す手段です。

もちろん、そのツールもインストールされています。

KDEメニューから”Backtrack→Privilege Escalation→PasswordAttacks→PasswordOnlineAttacks”に関連のツール群があります。

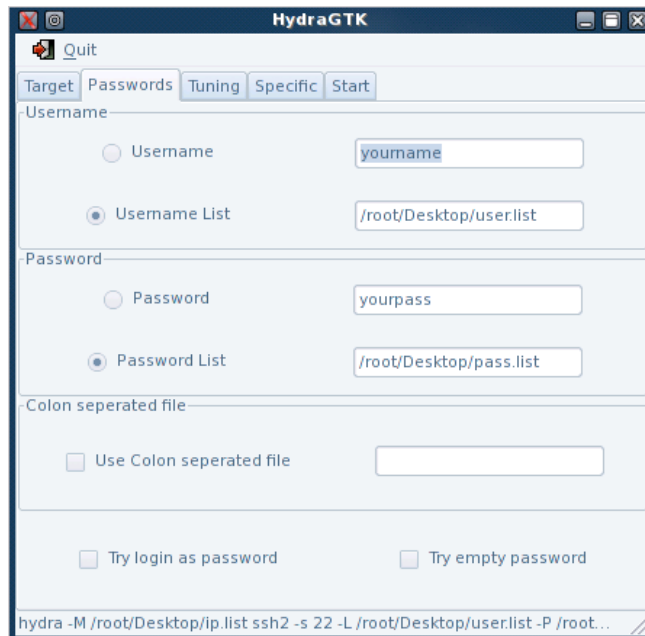
メジャーなHydraのGUI版であるXHydra(※7)を試してみます。



XHydraのターゲット設定画面

総当たりアタックする攻撃対象のIP(またはホスト名),サービスポート,プロトコルを設定します。

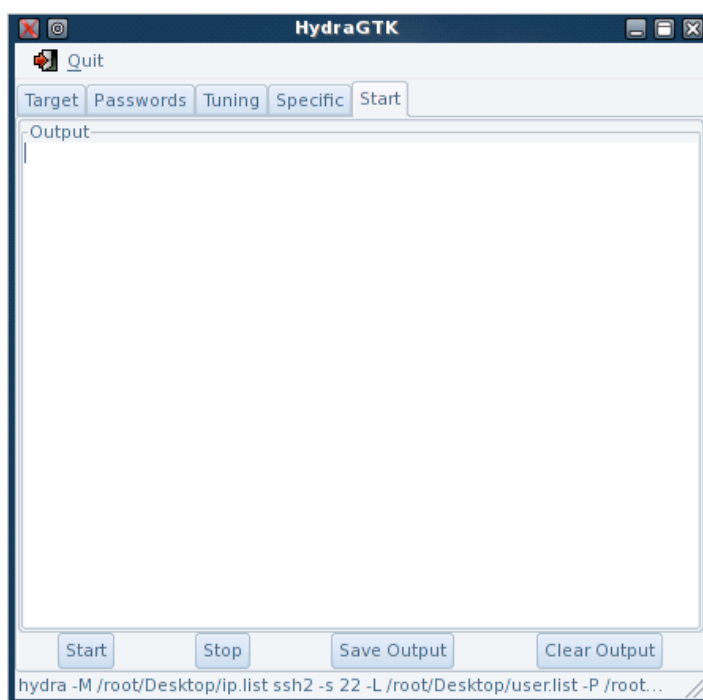
テキストファイルを作成し、リストを作っておけば複数のホストに対して自動的にアタックを行います。



ユーザーIDとパスワードの設定画面

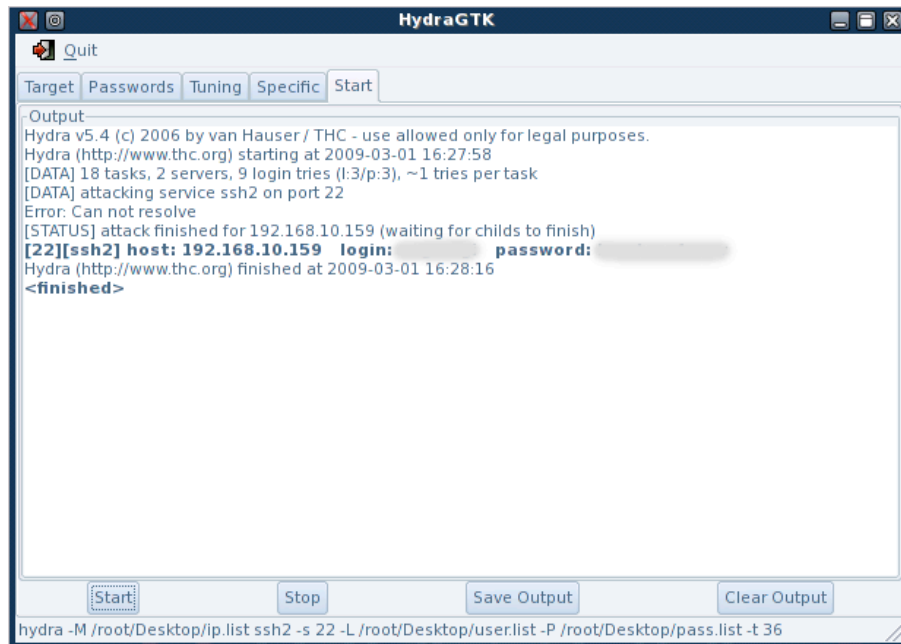
ホストに登録されているであろうユーザーIDとパスワードを設定します。テキストファイルを作成し、ユーザーIDとパスワードのリストを作っておけば複数のホストに対して自動的にアタックを行います。

インターネット上には、よく使われるユーザーIDやパスワードのリストが公開されています。(辞書ファイル) それらを利用することもおすすめします。



スタート画面

設定が終われば、後は**"Start"**ボタンを押下すれば実行します。



実行結果

sshアタックに成功すると、太文字で接続が成功したIP(ホスト名)とIDとパスワードが表示されます。

後は、判明したIDとパスワードで手動で接続して下さい。

5. まとめ

今回紹介したツール以外にも様々なツールがインストールされています。

(例えばCISCO出荷時のデフォルトのパスワードがある機器を検索するツールや、無線LANのWEPキー解析ツールなど)

全て紹介すると一冊の本になるでしょう。どこかの出版社で出版して頂くとありがたいですが。

今回はbacktrackの紹介というよりは、インストール済みのツールの紹介ですが、これらのツールがインストール不要で使用出来るのは、大変魅力的です。新規にサーバを立ち上げた時や、許可なくサービスをしているサーバを探し、そのサーバが正しく運用されているかの調査など大変実用的なディストリビューションです。

(もちろん、使用するにあたり調査対象のホスト管理者やネットワーク管理者に許可を取らなくてはなりません。)

専用のPCを持たなくてもライブCDやUSBで、どのPCでも調査用のPCになることもかなり実用的だと思います。

是非、このbacktrackを使用して組織内の安全を保つのに役立ければと思います。

謝辞

山梨大学総合情報処理センターの佐藤様には、このような報告書を書く機会を頂き、ここに深く感謝いたします。

参考web

※1 金融機関のシステム攻撃は外部よりも内部から (ITmediaエンタープライズ2005年6月23日)

<http://www.itmedia.co.jp/enterprise/articles/0506/23/news007.html>

※2 backtrack公式web <http://www.remote-exploit.org/backtrack.html>

現在(2009/02/28)Version4のβ版が、ubuntuベースとなって公開されている。

※3 netcraft <http://news.netcraft.com/>

※4 Insecure.Org – Nmap Free Security Scanner, Tools & Hacking resources

<http://insecure.org/>

※5 [packet storm] <http://packetstormsecurity.org/>

※6 The Metasploit Project <http://www.metasploit.com/>

※7 Hydra公式web <http://freeworld.thc.org/>

参考書籍

O'REILLY Andrew Lockhart著 ネットワークセキュリティHacks 第2版

ISBN978-4-87311-327-2