SecPoint Portable Penetrator – 仮想版

導入ガイド

本マニュアルを慎重に読み導入を進めてください。本ソフトウェアの導入にはコツがあり、ステップを誤ると正常に動作致しませんのでご注意ください。

目次

導入前に

1.ユニット ID が必要です

日本での販売代理店であるブルースター株式会社よりライセンスを購入した際に発行される、10 桁の unit ID を入手してください。Unit ID は大文字小文字の区別がされますので、発行された通りにご利用ください。例：ExAmPle123

2.Vmware 仮想コンテナをご用意ください。

DVD-ROM もしくはブルースターより指定された url より複数個に分割された vmware コンテナを入手ください。

3.複数の rar ファイルを結合解凍してください

複数のファイルに rar ファイルに分割されています。Winrar が導入されていないパソコンの場合には、まずこちらをダウンロード・導入をしてください。３つの rar ファイルのうち Part1 となっているファイルをエキスプローラにてクリック（選択）し、マウスの右クリックにて「Extract here(ここに解凍する)」を選択してください。１つに結合された GB 単位の巨大な vmware コンテナが生成されます。
このファイルを C ドライブへわかりやすいディレクトリに保存します。

4.インテル Virtualization Technology に対応しているパソコンを用意します。

パソコンがこれに対応しているかは vmware player を導入する際に未対応の場合、警告メッセージが表示されます。Core i3/i5/i7 のパソコンは対応しています。またパソコンの BIOS 設定にて Intel Virtualization Technology が[Disabled]になっていましたら[Enabled]へ変更ください。

5.ハードディスクの空き容量

ハードディスク容量として 100GB 程度を利用しますので、充分な空き領域が導入先のハードディスクにあるか確認の上で導入をお願いいたします。初期シグネチャ更新時に大きく容量を消費します。

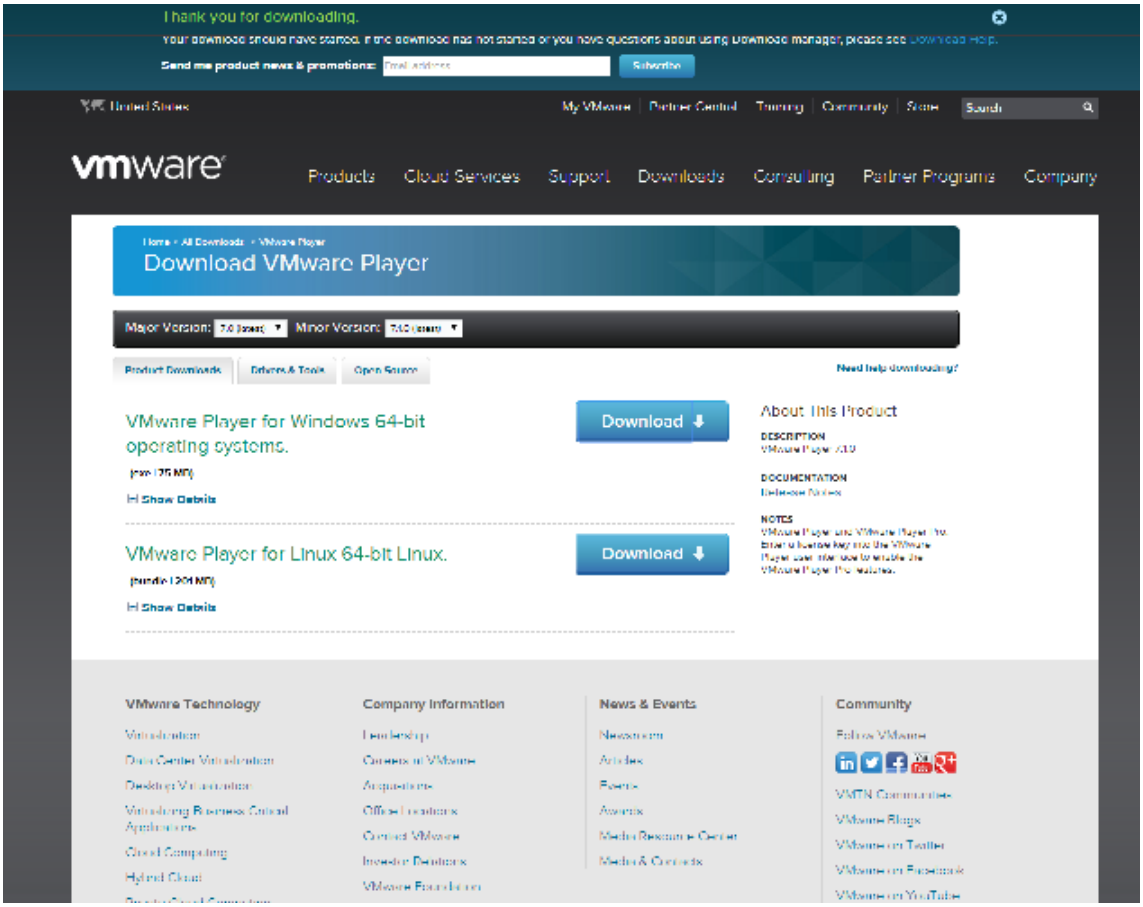
6.無線 LAN モジュールについて

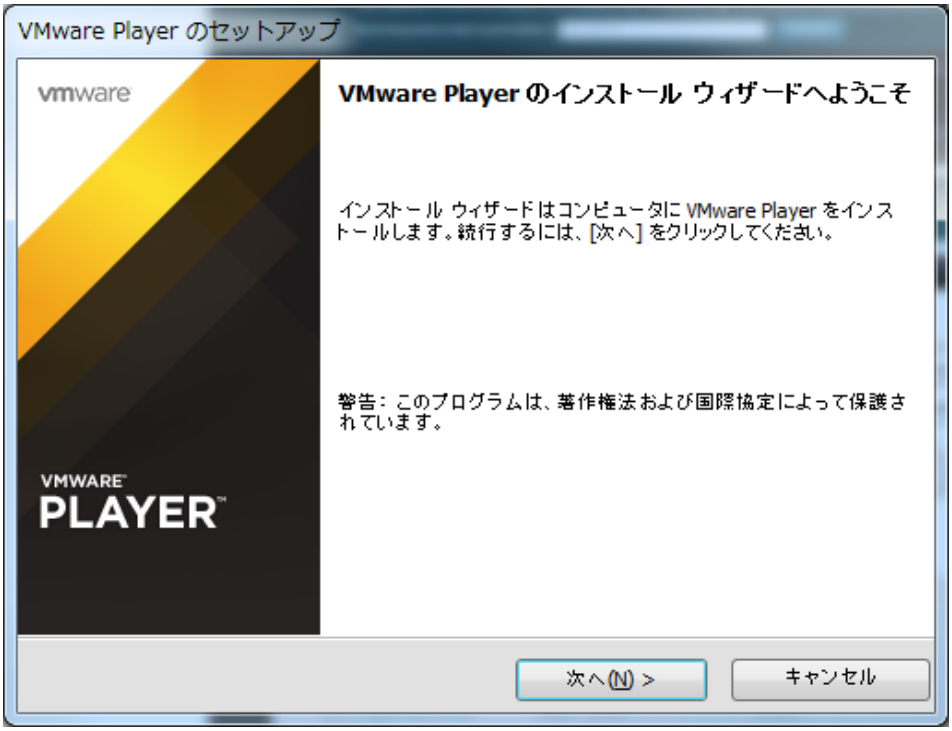
Portable Penetrator には、仮想環境上に無線 LAN モジュールが組み込まれています。標準で組み込まれているものは、Realtek RTL8187L,Ralink(MediaTek) RT3572,RT2770 と Atheros AR9271 の無線チップセットを搭載した無線 LAN モジュールです。
利用する Windows や MacBook へドライバの導入は必要ありません。
vmware 上で Portable Penetrator が起動した後に、USB ポートへ無線 LAN モジュールを装着し、Portable Penetrator に認識させます。

vmware player を導入

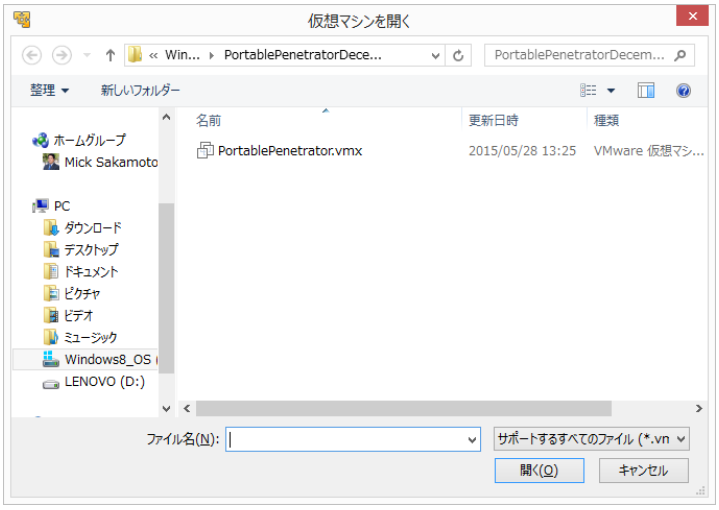
1.vmware player 上で動作しますのでインストールします。

vmware player を Google 検索などで検索し、最新のものを vmware 社のサイトよりダウンロードします。ダウンロード後にインストールします。特別なステップはありません。



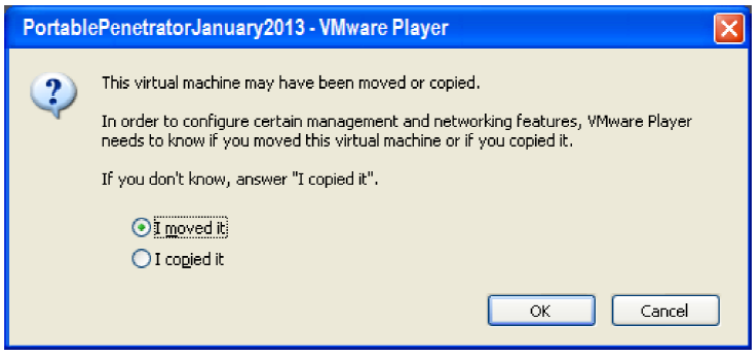


「仮想マシンを開く」を選択し、先程ダウンロードして 1 つにした仮想化コンテナを指定します。



仮想ファイルの vmx イメージを指定します。

仮想マシンが設定されます。RAM は標準の 1GB で大丈夫です。



コンテナは USB ドライブや DVD からローカルドライブに複写したかと聞いてくることがありますのでC ドライブにあることを確認し、「複写しました」を選択してください。

SecPoint の起動

vmware player でコンテナを起動します。

Penetrator を初期化します。

Google Chrome を起動し次の url を入力してアクセスします。

https://127.0.0.1/login.php?query=init

セキュリティ警告が表示されますが、「Proceed（継続）」を選択します。

ユニット ID を入力してログインします

日本での販売代理店であるブルースター株式会社よりライセンスを購入した際に発行される、10 桁の unit ID を入力しライセンス認証を行います。

ソフトウェアへライセンス認証がなされ利用が可能となります。

利用のためのログイン

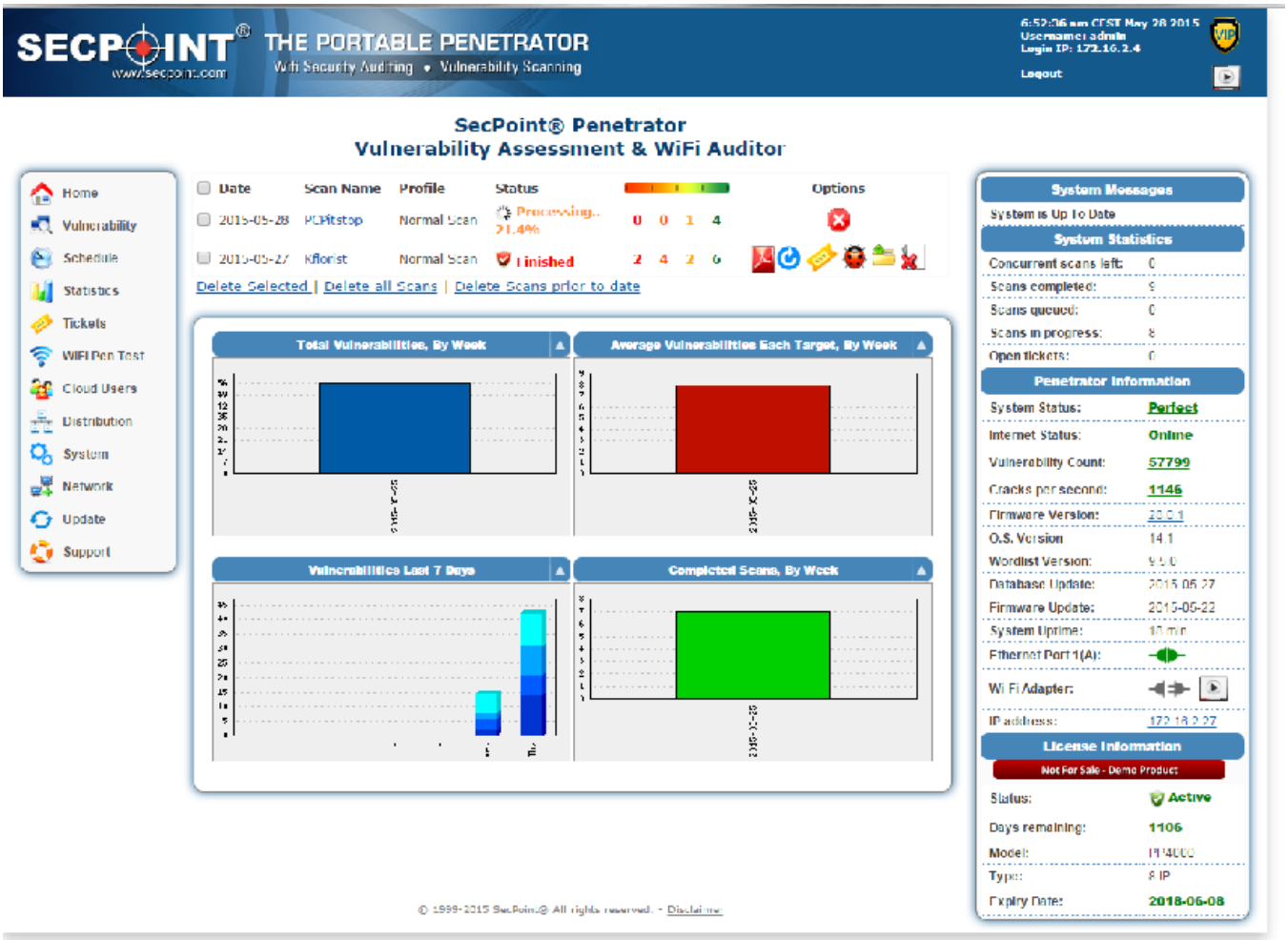
ログイン方法

以下の url を入力します。

https://127.0.0.1/login.php

日本での販売代理店であるブルースター株式会社よりライセンスを購入した際に発行される、10 桁の unit ID をパスワードとして入力します。Username は、admin です。

ログイン後の画面例



画面右のシステムステータスとインターネット接続状況が「Online(オンライン)」になっているか確認ください。これは SecPoint 管理画面と呼びます。

ネット接続がオフラインになっている場合

オフラインとなっている場合には、以下のポイントをチェックください

1) vmware player におけるネットワーク設定が「ブリッジモード」となっており、必要なネットワークアダプタが選択されているか

2)SecPoint 管理画面の左側「Network（ネットーク）」が DHCP など必要な設定になっているか

3)無線 LAN WiFi アダプタを接続するなどしてイーサネットポートが接続状態とならないか確認してみてください

4)パソコンを再起動し、vmware 上の SecPoint 上の chrome ブラウザからインターネット接続が可能か

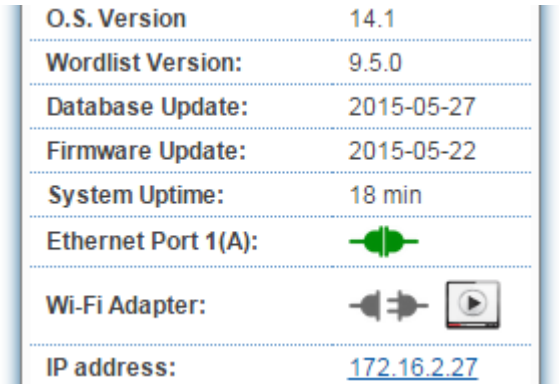
ファームウェア、データベース、ワードリストのアップデート

ファームウェア、データベース、ワードリストの最新版がある場合には、SecPoint 管理画面の右枠に警告として表示されます。警告をクリックすることでアップデート画面に飛びます。インターネット接続ができていることを確認して実行ください。

SecPoint 管理画面の左側に「Update(更新)」がありますので、「Automatic update」を選択し、自動的に更新されるように設定しておくことをお勧めいたします。

LAN 接続された別のパソコンからの利用

LAN 接続された別のパソコンから利用操作が可能となります。アプライアンス製品の場合には、この方法を利用するのが通常利用となります。IP アドレスは、SecPoint 管理画面の右側にある「IP address」がアクセス先アドレスとなります。



画面例の場合には、https://172.16.2.27/login.php/　となります。

利用に際しては、まず利用 IP アドレス認証が先に必要となります。

利用可能 IP アドレス認証作業

前述の LAN セグメントへ接続された別のパソコンからの利用には、IP アドレス認証作業が必要となります。サンプルの例では以下のアドレスにて接続します。PDF レポートを直線ダウンロードできるため便利です。

https://172.16.2.27/adminip/

日本での販売代理店であるブルースター株式会社よりライセンスを購入した際に発行される、10 桁の unit ID を認証キーとして入力します。

脆弱性検査の仕方

WEB サービスの検査

Penetrator を WAN や DMZ に直接接続するか、社内のファイアウオールによる影響を受けない設定を確認の上で、LAN セグメントよりインターネットへ接続可能なことを確認します。

「OWASP Top 10」「Best Scan」「Quick Web Scan」などの選択肢の中から、検査に最適なプロファイルを選択します。WEB サーバであれば、OWASP Top 10 を選択すると良いでしょう。DB サーバなどであれば、Quick Scan をお勧めします。WordPress などを利用している機器の場合は、「CMS Web Scan」を選択すると効率的にスキャンが可能です。スキャン対象が不明な場合には、エクスプロイト攻撃のシミュレーションも実施する Aggressive Scan を実施してください。

「PCIDSS for WebScan」は、クレジットカード決済を伴う WEB サービスに対して監査を行うプロファイルです。前述を四半期毎に実施することに加え、EC サイトで本プロファイルを毎月実施することをお勧めします。

検査対象がロードバランサー(LB)を利用している場合には、LB に対してではなく、各サーバのグローバル IP アドレスを利用している場合にはそれを把握し、それぞれの WEB サーバに対して検査を行ってください。ローカルＩＰである場合には、LB に対して実施します。IPS がある場合は、スキャナによるクロールが判別されてしまうことがあるため、IPS 機能を一時的に停止するかバイパスしてください。

社内 LAN での検査

社内でパソコンが利用されている業務時間帯もしくは週末などに全パソコンを起動しパソコンをログイン状態にして検査を行います。電源が投入されていないパソコンは調査されません。
社内 LAN にて利用されているセグメントを 192.168.1.0/24　などで指定します。対象レンジを設定しても未使用の IP に関しては 5 分程でスキップされます。また社内で利用されている IP アドレスのリストを CSV 形式でアップロードすることも可能です。
効率よくスキャンするため、指定するプロファイルは PCI DSS をお勧めします。一般的な社内利用においての機器および脆弱性情報が入っています。社内に Linux 機がある場合は、該当 IP アドレスのみに対して HIPAA を指定し、社内向け Web サービスが導入されたサーバがある場合は、OWASP Top 10 や CMS Web Scan を指定してください。

同時利用可能 IP 数がライセンスによって決まっておりますが、4IP ライセンスであれば 4 台ずつ調査がされます。推奨スキャンは以下の 3 つです。
「Best Scan」（主要脆弱性検査）
「HIPAA」（保険関係情報の取扱事業者）
「Aggressive Scan」（全脆弱性検査。エクスプロイト攻撃を含む約 6 万件）

「Best Scan」は、主要な脆弱性検査をすべての利用環境を想定し、時間をかけてスキャンを行います。

「HIPAA」は、PCI DSS に加えて医療機器の脆弱性および医療器に持ち入れられる汎用 Linux サーバなどがカバーされています。

「Aggressive Scan」は、PCI DSS の監査対象外のエクスプロイト攻撃(Flash や古い Java のセキュリティホールによる脆弱性をついた攻撃)による侵入手法であるエクスプロイト攻撃もエミュレーションします。PCI DSS や HIPAA よりも強く監査を行いますが、Best Scan よりも時間を要します。

IoT、SIP 電話機、ルータの検査

Web 画面を利用した設定 UI を持っている場合は、その機能を有効化した上で検査を行ってください。また設定画面にてオプションとなっている機能などをすべて有効化し、オプション機能に脆弱性が含まれていないか検査を行うことも重要です。すべてのオプションを有効化し、WEB の管理画面も有効化して検査にかけてください。ルータなど WAN 側と LAN 側がある場合は、両方からそれぞれ検査う必要があります。web 認証機能を用いて管理画面に入る場合には、脆弱性検査は行えませんので該当部分を外した検査用ファームウェアのビルドをお願いいたします。

「Aggressive Scan」（全脆弱性検査。エクスプロイト攻撃を含む約 6 万件）

「Best Scan」（主要脆弱性検査）

「Firewall Scan」（ファイアウオールの検査）:Ping 応答しない機器はこちらを選択ください

ファイアウオールスキャンは、シスコやジュニパー製品などでの既知の脆弱性を調査するものです。自社製品にスキャンを行ってもあまり意味はございませんので、Best Scan を選択ください。

Wifi 脆弱性診断の仕方

手法 1:WPS(Wifi Protected Setup)を用いた WEP/WPA/WPA2 のクラック

主要ルータは親機と子機に付属したボタンを押すだけで接続認証が可能となる WPS 機能を装備しています。この暗号キーは 1 千万件の組み合わせがありますが、2011 年 12 月に 11,000 件の組み合わせでパスワードが入手できる脆弱性があることが判明しました。

WPS のピンは WEP、WPA、WPA2 の暗号通信において解読が可能です。
ターゲットとなる SSID を選択し、受信電波が良好である場合、5 分～60 分後、%の数字が 0.2%や 1%と表示されたら、その機器には脆弱性がありクラックが開始されていることになります。
暗号キー長がどれだけ長いか、複雑であるかは関係ありません。

WPS が有効でない場合には、60 分経過しても WPS クラックは実行できないことになりますので、別のクラック手法を試します。

手法 2:WPA/WPA2 辞書攻撃

受信電波が-80 では難しく、-40 程度であれば良好です。おおよそ、-50 か-60 であればクラックは可能です。ターゲットとなる SSID を選択し、「Wifi Bomb」か「ターゲットとなる特定の通信利用者」を選択します。親機と子機の通信が弱まり、ハンドシェイクにて再接続する際にクラック処理が開始されます。再接続がされるまで時間を要します。おおよそ 20 秒から 2 時間ほどを要しますが、これは再接続頻度や信号の強さなどによって異なります。
次に利用する辞書を選択します。本ソリューションでは 11 億件の辞書を装備しています。
インテルデュアルコアの Core i5 の CPU であれば、1 秒間に 2000 個のキーでクラックを試みることができます。クアッドコアの Core i7 であれば 1 秒間に 4000 個のクラックが可能です。WPA/WPA2 は、最小 8 文字の暗号キーですので、約 1 億件の 8 文字以下の辞書はスキップされます。このため最大１０億件の辞書攻撃となります。効率的な攻撃を行うため、辞書ファイルを選択して効率的なクラックを試みてください。

手法 3:WEP クラックのみ

WEP 手法はとても簡単かつ高速にクラックが可能です。現在はゲーム機で利用されていますが、一般的には利用が好ましくない無線 LAN の利用手法とされています。この方式をオープンにしているだけで脆弱性を抱えていると顧客企業へ指摘する必要があります。

受信電波が-80 では難しく、-40 程度であれば良好です。おおよそ、-60 以上であればクラックは可能です。通信トラフィックをみてクラックを行いますので、２～３人接続している SSID であれば効率的に早くクラックが可能です。スニフィングにより親機と子機の間の通信を 1 分から数時間でクラックが完了します。通信量やシグナルの強さによって時間は変わります。

フラグメンテーション技術を使って親機と子機の間の通信をクラックすることも可能で、こちらのほうが早くパスワードを入手することも可能ですが、膨大な通信トラフィックが発生いたします。

Exploit Armitage について

700 以上のエクスプロイトを実行させることができ、侵入の可否を調査することができます。しかし、同時にターゲットとなるパソコンをクラッシュさせる危険性があるため、高度な脆弱性診断技術をもっていなければ利用しないようにしてください。

利用のためのマニュアルは、以下の URL にございます。（英語）
http://www.fastandeasyhacking.com/manual

起動した際のパスワードは以下になります。
appliance10STRONG

取り扱いには注意の上でご活用ください。