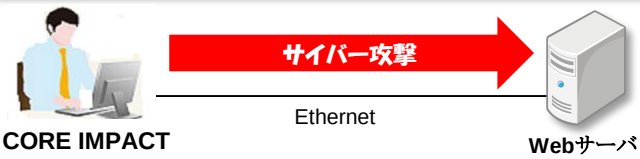
重要なIT資産を守るためには、攻撃者視点に立ったセキュリティ対策が重要です！
OS、Web、制御システムの脆弱性を狙うクラッカーの攻撃をリアルシミュレーション！

CORE IMPACT

CORE SECURITY社(米国)は、総合的なサイバー攻撃対策ソリューションを提供する企業です。
CORE IMPACTは、様々なIT資産（ネットワーク、Web、エンドポイント、モバイル、WiFi 等）のセキュリティ対策の有効性を可視化できるペネトレーションテスト（侵入テスト、以下ペンテスト）ツールです。クラッカーが実行する攻撃パターンをシミュレーションし、セキュリティ対策を施されたIT資産が本当に防御出来るのかを実証します。攻撃者の視点でセキュリティ対策を考え理解することで、次に何をすべきか、何が足りないのかを認識し、セキュリティ対策の為の無駄な投資を抑制する事が可能です。

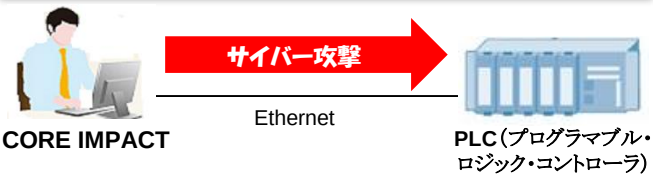
重要なIT資産のセキュリティ対策は万全ですか？サイバー攻撃シミュレーションによる実証試験は重要です！

使用例1）Webアプリケーション/サーバに対するペンテスト



・WebサーバーのOS（Windows/Linux等）に対してペンテスト。
・Webアプリに対し、OWASP Top10の脆弱性有無をテスト。
・ID/パスワードの堅牢性テスト。

使用例2）制御システム（SCADA）に対するペンテスト

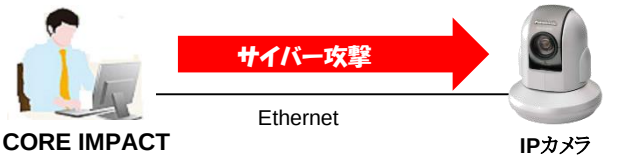


・PLCのマネジメントOS（Windows/Linux等）に対してペンテスト。
・SCADAプロトコルに対してペンテスト。

使用例3）IPS/IDS/WAF等セキュリティ機器の性能テスト

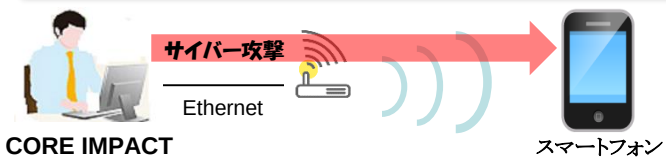
・回避テクニックを駆使し、IPS/IDS/WAFを突破できるかをテスト。
・OSやWebアプリ等の様々な攻撃を実施。IPS/IDS/WAFが防御・検知しているかをテスト。

使用例4）IPカメラに対するペンテスト



・IPカメラのOS（Windows/Linux等）に対してペンテスト。
・IPカメラサービス（プロトコル）に対してペンテスト。
・ID/パスワードの堅牢性テスト。

使用例 5）モバイル端末（スマートフォン等）に対するペンテスト



・OS（iPhone,Andoroid等）に対してペンテスト。
・フィッシング、Webフォーム偽装、アクセスポイント偽装など様々な攻撃をシミュレーション。

使用例6）WiFi機器に対するペンテスト

・WiFi機器のマネジメントOS（Windows/Linux）に対してペンテスト。
・パスワード（WEP, WPA-PSK and WPA2-PSK）の堅牢性テスト。
・様々な攻撃（Man In The Middle等）をシミュレーション。
・WiFi機器をクラッキングして、エンドポイント機器へピボッティング。

主な用途

- ネットワーク/Webアプリケーションに対するペネトレーションテスト
- サイバー演習/訓練
- IPS/IDS/WAF等セキュリティ機器の性能テスト
- 標的型攻撃演習
- PCI-DSS/コンプライアンス順守状況の確認

主な導入メリット

- ペネトレーションテストの工数削減/品質定量化を実現
- クラッカーの攻撃を想定した防御体制を提案可能
- 顧客に最適なセキュリティ機器を選定/提案が可能
- 弊社による日本語サポートが受けられます
- PCI-DSSやコンプライアンス認定における工数の削減

日本コーネット・テクノロジー株式会社
東京都台東区東上野1-12-2　〒110-0015
(TEL) 03-5817-3655 (代) (FAX) 03-5817-3677
www.nihon-cornet.co.jp

Rev C

CORE IMPACT® PROFESSIONAL

CORE IMPACT

CORE SECURITY® Thinking Ahead

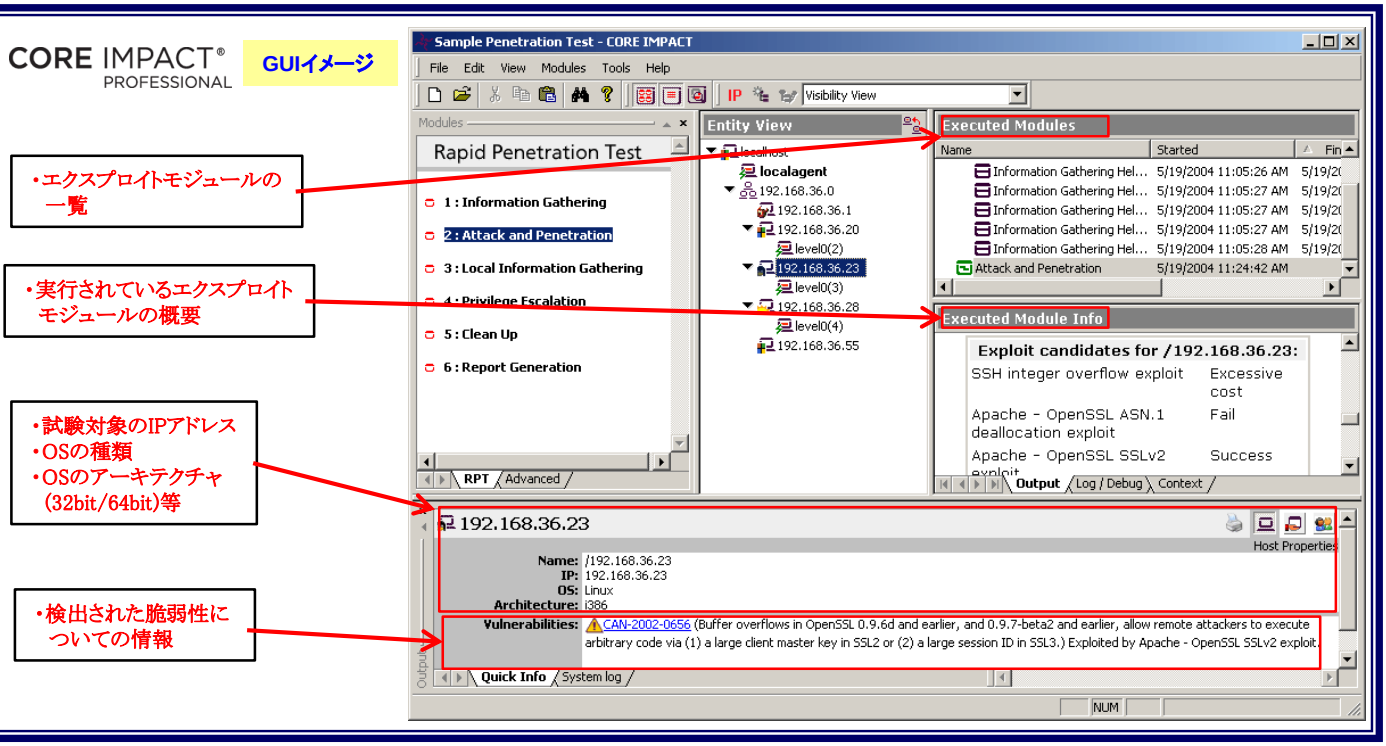
主な特長

● **業界最多のエクスプロイトモジュールによって、他に類を見ない多彩なペネトレーションテストを実現**

クラッカーは、【なりすまし】【情報奪取】【システムダウン】を目的として、攻撃可能なターゲットに対し、日夜ペンテストを行っています。CORE IMPACTは業界最多の3,000種類以上のエクスプロイトコードを有しています。クラッカーの攻撃を模倣しその対策を事前に実施する事で、サイバー攻撃を最小限に防ぐ事が可能になります。

● **専用GUIにより高い操作性を実現**

CORE IMPACT® PROFESSIONAL GUIイメージ



● **制御システムに対しペネトレーションテストを実施可能**

クラッカーの侵入の対象は一般的なITインフラに留まらず、社会インフラ等を構成する制御システムも対象となっています。制御システムの脆弱性を正しく把握することで、社会インフラや工場設備等に適切な防御体制の構築に役立ちます。

● **アクセスポイント偽装機能により、不正アクセスポイントを利用しているユーザを把握**

MITM(マンインザミドル)攻撃等、アクセスポイントを偽装する攻撃をシミュレーション可能です。最新のワイヤレスペンテストドロップボックスであるWiFi Pineapple Mark Vをサポートし、最新のWiFiシステムにおけるペンテストが可能です。

● **ワイヤレス機器(AP等)、モバイル機器(スマートフォン等)、IPカメラ、制御機器(SCADA)など、様々な攻撃パターンを搭載**

IoT(インターネットオブシングス)の普及により、様々なモノがインターネットに接続され、セキュリティの確保が急務となっている中、業界最多の攻撃パターンを持つCore Impactを導入する事で、定量的なセキュリティ堅牢性テストが可能となります。

● **業界最高クラスの自動Webアプリケーションテストエンジンを搭載**

主要なWebアプリケーションの攻撃を網羅しているOWASP(オープンウェブアプリケーションセキュリティプロジェクト)Top10をサポートし、対象機器にWebアプリケーションのリスクが存在しているかを検証可能です。

● **サードパーティ製スキャナのスキャン結果の読み込みやMetasploitのエクスプロイトコードも使用可能**

CORE IMPACTは主要なサードパーティ製のスキャナのスキャン結果を読み込むことで効率的にペンテストを行うことが可能です。また、オープンソースで有名なMetasploit FrameworkをCORE IMPACTから実行する事も可能となっています。

● **種類豊富なレポート機能により、正しい脆弱性改善策を実施**

ペンテストの実行結果は勿論の事、結果に対する改善策プランの提示や、PCI、FISMA等コンプライアンスに準拠したレポートを出力可能です。

CORE IMPACTシステム要件

ハードウェア要件
- Core2Duo 2.8GHz以上のプロセッサ
- 4GB RAM
- 10GB以上のディスクスペース

オペレーティングシステム
- Windows Server 2008 R2,2012、Windows 7, 8

ブラウザ
- Microsoft IE 最新バージョンがインストールされていること

CORNET TECHNOLOGY 日本コーネット・テクノロジー株式会社
東京都台東区東上野1-12-2 〒110-0015
(TEL) 03-5817-3655 (代) (FAX) 03-5817-3677
www.nihon-cornet.co.jp

Rev C