JNSA ワーキンググループ紹介

ハニーポットWG

ハニーポットWGリーダー
園田　道夫

■ はじめに

200年度に活動していた不正アクセス調査ワーキンググループが、追いかけるテーマが当初のものから離れてきたので、テーマを明確化する目的もあり活動を一度リセットし、ハニーポットワーキンググループとして2003年度に新装開店しました。2003年の9月には専用回線を準備、また専用マシンも購入しハニーポットをインストール、着々と準備を進めています。10月からは週に2回、メンバーが各々業務終了後に集まってはハニーポットをいじっています。

■ 活動の内容

文字通りハニーポットを中心にセキュリティ技術を調査学習しているワーキンググループです。しかし、それだけではなくハニーポットってそもそも売れるのか？みたいなことも議論しています。

ハニーポットに関わる技術というのは、これまでのセキュリティ技術のある意味集大成とも言えます。防衛技術、検知技術、そして攻撃技術について知見が無いと、構築し運用管理することは難しいものです。

このワーキンググループでは運用管理から、さらにその先にある情報公開についても検討をしています。

また、実際にハニーポットを構築もしています。構築している際に検討した論点や結果としてどういう実装になったかなどは、インターネットウィーク2003にて一端を紹介いたしましたが、正式なレポートは成果物として年度末にリリースする予定にしています。

現在構築中のハニーポットについて少し紹介しておきましょう。ハニーポットはご存知のとおり、囮とか罠とかいうニュアンスのサーバー、もしくはネットワークです。ネットワークのことはハニーネットと呼んだりもします。現在ワーキンググループにて構築中のものは小規模なハニーネットとでも言うべきもので、囮として使用されるサーバーは現在のところ3台（仮想的な意味で）あります。この3台はあるドメインを持ち、ごく一般的なサイトを構成しています。

サーバーソフトウエアはわざと旧型の穴があるものを用意しています。もちろん客寄せのためですが、回線が開通して機器を接続した途端に大量のワームのプローブアクセスに混じってお客さんらしきアクセスもあったりしましたので、もしかするとドメインもサーバーのコンテンツも全く必要無いのかも知れません。

他にサイト内にはIDSとパケットロガーも構築しています。何らかの怪しいアクセスが行われた場合、そのログを多角的に取得しておきたいという意味合いと、もう1つのテーマであるデータ解析の材料として実装しました。プロモーションがうまくいって、お客さんが多数いらっしゃるようだったら、今後検出精度等の比較も可能になると思います。

現在構築中のハニーポットはバージョン1ということになりますが、以降の計画としては、

- 現在の緩めのポリシーをキツイ方向に締めたらどういう反応があるか？
- 囮のタイプを変更してみるとどうなるか？

などを検討していくことになりますが、もしかすると多数のハニーポットを集中的に管理するような仕組みの導入と運用を実施していくかも知れません。この手の仕組みは単一のサイトのみでデータを取得・解析したところで限界は見えていますし、今後は相関解析という方法論の中に組み込んでいくことも考えていくべきだと思うからです。ある面dshield.org（incidents.org）の試みに近いようなことを、多くのサイト間で連携しないと、この技術がセキュリティ確保に役に立つのか、ひいては「売れる技術」たりえるのか、というところまで議論が行かないでしょう。実は「売れる技術」と「売れる製品」というのは違うと思いますが。

いずれにしてもこのハニーポットという、（今のところ）売れそうも無いが十分に魅力的な素材を追いかけて、技術や知識のみならずさまざまな方面での知見を深めていければ、と考えています。

みなさんもぜひ一度、活動に参加してみてください。