A Construction Method of a Honeypot System to Safely Collect Unknown Malicious Codes

Kenji OHIRA†, JungSuk SONG†, Hiroki TAKAKURA‡, and Yasuo OKABE‡

† Graduate School of Informatics, Kyoto University, Yoshida-Hommachi, Sakyo ward, Kyoto, 606-8501 Japan
‡ Academic Center for Computing and Media Studies, Kyoto University, Yoshida-Hommachi, Sakyo ward, Kyoto, 606-8501 Japan

E-mail: †{ohira,oaktree}@net.ist.i.kyoto-u.ac.jp, ‡{takakura,okabe}@media.kyoto-u.ac.jp

Abstract It is considered that an attacker tests his attacking codes by sending them to randomly selected nodes in the Internet. Collecting and analyzing such beta-version attacking codes are considered to be effective especially against 0-day attacks because they can be used as an attack forecasting system to find and announce such pre-attacking attempts before the attack completes or be spread. However, we cannot predict which service in a system in operation is attacked. It is inappropriate to set a node which listens all TCP, UDP and any other ports because it can be revealed that the node is a honeypot by port scanning activity. It is requested that a honeypot dynamically opens and closes listening ports according to the trend of attacks. Attacking attempts are very varied. It is required to set a honeypot in filter-free or DMZ environment in order to collect various and especially new attacking codes. At the same time, it is required to do access monitoring and log collecting in attack-free environment. Even if a honeypot falls in an attacker’s control, monitoring and log collecting must be secured. In this paper, we propose a way to construct a safe and portable honeypot system which meets above by using virtual machines.

Key words Security, Honeypot, 0-day Attack, Attack Forecasting
1. まえがき

近年インターネット接続が安価になり、多くの人が参加できるようになったが、その分面インターネットにおけるセキュリティに詳しくない人の割合も増え、所有者に気付かれないままインターネット上での攻撃行為の踏み台サーバーにされているホストも数多く存在する。

セキュリティ報告書に基づくパッチ適用によって自身の管理するホストのセキュリティホールをふさごうと言う意識は徐々にではあるが高まりつつあると言われる。

しかしながらセキュリティ報告書に基づくパッチの公開時期と比べてそのセキュリティホールを突いた攻撃活動が活発化する時期が極めて近接している、あるいは攻撃活動が活発化の時期の方が早いケースも出てきている。これは0-day攻撃というカテゴリーに分類されるもので、公開されているパッチを適切に適用していたとしても攻撃されれば被害を免れ得ないものである。

そこで、攻撃プログラムも一般的なプログラム同様広く出回る前に数々の試験段階を経るものと考えられる。この試験段階での攻撃コードの発展を知ることができれば従来よりも早い段階でシステムの脆弱性を知ることができ、その対策を考えることができるようになると考えられる。本論文ではこのような未知の攻撃コードを取得し、それを解析することによりインターネット上での攻撃活動の予兆を警告する、「攻撃予知」システムの要件について検討し、さらにそれを実装するための手法について提案する。

以下2章で従来検知に関する既存研究について、3章で既存研究から未解決の問題とそれに対する提案手法について、4章で本提案の実装について、5章でその評価を述べ、6章にまとめて述べる。

2. 既存研究


図2 インライン型IDS

図1 ネットワーク型IDS

図3 定点観測装置

これらの定点観測システムは何を監視対象とするかという観点で分類できる。監視対象として
- システムコア
- プロセス
- 仮想ターミナル（キーティピング）
- ネットワーク（IPパケット）

が挙げられる。上に記したものを用いた詳細な記録が採取できる。

ここで、処理速度やスケーラビリティの観点から、詳細な記録が採取できることが必ずしも利点であるとは限らないことに注意する必要がある。監視対象を限定した（特定の攻撃に特化した）定点観測装置としてシステムレベルでの記録採取を行うシステムを導入し、広範に攻撃行為の予兆を検出する目的にはネットワーク（IPパケット）を観測するシステムを使用するのが適切であると考えられる。

本論文ではネットワークモニタリングを対象とする。

ネットワークモニタリングはペイロードを監視対象とするかどうかによりさらに分類される。ペイロードを監視対象とした場合、より詳細な記録が取れる可能性がある。しかしながら、解釈すべき対象が多くなるため即時性が保たれず、保有すべきログの量が多くなることからスケーラビリティに課題がある。
か、ヘッダ情報に比べて圧倒的にプライバシーにかかわる情報が含まれていると解釈される可能性が高く、法的倫理的観点から厳格的に導入するには抵抗感があるのが実情である。

本論文でトラフィックモニタリングを行う対象のネットワークは観測装置専用のセグメントであり、ここで一般向けのサービスを行っていない。そのためこのネットワークに対して送信されるトラフィックを観測することによりプライバシーが侵害されるという指摘は当たらないものと考えられる。また、当該ネットワークはトラフィックモニタリングを行う者が当該通信の一方法事実であるため、通信の秘密を定められた諸法に抵触しないものと考えられる。その観点では、攻撃コードの著作権を論じられる可能性があるが、少なくとも日本国内においては公序良徳の観点から当該権利よりもトラフィックモニタリングの権利が優先されるものと考えられる。

本論文ではIPv6は保存を含むものとし、そのベイアードの解釈によって観測装置の挙動の変更をしないものとする。

パケットヘッダ（IPヘッダ、TCP/UDP/IOMPヘッダ）のみを解釈する観測装置を想定した場合。

（1）応答を全く返さないパッシブモニタ

（2）公開された脆弱性情報に基づいて自動的にポートを開放するシステム

（3）管理者の目視により不適切なポートを開けるシステム

（4）全ポートを開放しているシステム

が想定の状態として挙げられる。

これらの問題点として、それぞれ

（1）コネクションが成立しないので、TCPを利用した攻撃について、攻撃コードが含まれているパケットが送信されない

（2）脆弱性情報が公開されていないための攻撃に対する対応できない

（3）管理者の能力に大きく依存し、対応までの時間も長くなる

（4）観測装置であることがすぐに攻撃者に明らかになる場合（詳細は3.2.1に述べる）

という点が挙げられる。これらの課題を解決すべく、本論文では未公開の攻撃と思われる行為に対して、到達パケットのヘッダ情報の解析結果に基づいて動的に待受けポートを変更するシステムを3.3に提案する。

3. 操作手法

本提案では監視対象をネットワーク上で流れるパケットのみに限定する。これによる制御項目については3.1に述べた上で3.2に対応すべき課題を述べる。

3.1 管制事項

最初から暗号化された通信に使用された場合、提案方法には役に立たない。したがって多くの対策は非暗号化通信を使用したものである。SSL対応プロトコルとSSL非対応プロトコルが混在する（httpとhttpsのよう）ものについてはSSL非対応プロトコルが利用されることが多い。またSSHなどの暗号化通信を使用したアプリケーションについては機械

類が限られているためそれらについてはシステム単体を監視するような別の手法の観測装置を設置することにより対応する。

3.2 対応すべき課題

3.2.1 動的待受け

仮想全てのTCP/UDPポートで待受けるように設定した観測装置を設置した場合、ポートスキャンの応答から攻撃者に観測装置があることを察知されてしまう可能性が大きい。これに対し、本論文では、最近アクセスがあったボートについてのみ待受けプログラムを対応付けるシステムを提案する。提案するシステムの挙動は以下のとおりである。

（1）初期状態では全ての観測装置において待受ける

（2）TCP/UDPポートへのアクセスがあった場合、宛先

ポート番号などの情報をアクセス記録サーバに通知

（3）アクセス記録サーバはデータベースにアクセス日時お

よび宛先ポート番号などの情報をデータベースに記録

（4）アクセス記録サーバは当該ポートへのアクセスがあっ

たことを他の観測装置に通知

（5）アクセス情報を受け取った観測装置は当該ポートで待

受けるプログラムを起動

（6）アクセス記録サーバは予め設定した期間中全くアクセ

スのなかったポートについて待受けプログラムを終了するよう

観測装置に通知

ただし、あるポートで待受けるプログラムがどういう応答を

行うべきかは事前にわからない。これは攻撃攻撃対象を既知の攻

撃に限った場合で同様であり、同一のポートに対する攻撃

が単一種類である保証はない。このようなポートで待受ける

プログラムにどのような応答をさせるのがよいか、一般化は難

しいが、本提案では、TCPについてはSYNが送られてきた場

合にはSYN+ACKで応答し、3-way handshake終了後にどのように

ベイアードに対しても特別の意味はない文字列を返す設定

にした。この装置に対して攻撃者が送信するバケットを

収集している。UDPポートについてはTCPのような3-way

handshake手順はため、どのようなバケットに対しても特別

の意味はない文字列を返す設定にした。この装置に対し

て攻撃者が送信するバケットを収集している。

3.2.2 制御用チャンネルの保護

本論文で提案するシステムは観測装置とアクセス記録装置を

観測装置から構成されている。観測装置については権力フィルタのか

けられていない環境におくことが求められるが、アクセス記録

観測装置を含めた制御の一部については外部からの攻撃に晒さ

れないようする必要がある。この要求に対応するべく、観測

装置以外のホストについてはパケットフィルタリングを適切に

設定し、外部から直接アクセスできるアドレスを付与しない

などの対策が求められる。

また、観測装置が攻撃者の制御下に入る可能性も皆無ではない

ため、観測装置からアクセス記録装置にアクセスできない

ようにするとも求められる。この場合、観測装置のネット

ワークインタフェースをモニタリングするだけの行為も攻撃者

の攻撃行為に含まる。そのため、管理用の装置に直接つな

がっているネットワークに観測装置が直接つながっていないよ
うに配置することも求められる。

上述の要求を実現するため、図4に示すような配置で観測装置を設置することを提案する。

図4 サンドイッチ配置の観測装置

図4において、アクセス記録用装置と観測装置の間に中継用のノードを用意し、このノードを経由してアクセス記録用装置から観測装置にポータ開放命令を送信する。ここで中継用ノードにフィルタリングを設定し、逆向きのアクセスはできないようにする。また中継用のノードでNATをすることにより、ポート開放命令のパケットを観測装置上で取得してもアクセス記録用装置のIPアドレスが容易にはわからなくなるようにしている。

さらに観測装置が攻撃者の制御下に入りた場合、その観測装置からの報文は偽装や失効をされる可能性があるため、観測装置からインターネットに向かう経路上にブロッキング装置を設置し、観測装置に到達するパケットに関する情報はこのブロッキング装置上で取得し、アクセス記録装置に報告するようにしている。

4. 実装

4.1 VMware

アクセス記録装置以外の装置（観測装置、ブロッキング装置、中継用ノード）は全て単一ホスト上でVMware仮想ホストとして構築した。

これにより、極力汎用的な形式を維持したままサンドイッチ構造全体を単一の機器上に収められるため、広範に本機器を設置する際に機器装置を容易にできると考えられる。

ここで、ブロッキング装置は一般的に利用されているスイッチング機能のミラーリング機能を利用するなどすれば同様の効果を得ることができる。しかし観測装置を広範に配置することを考え入れた場合、観測装置に流入するトラフィックの内容を全て管理用ネットワークを通じてアクセス記録サーバへ転送することは、特に既知の攻撃がトラフィックの大部分を占める場合、非効率的である。そのため本実装ではこの部分も仮想ホストの形で実装することとした。また、この形式を採用することにより、ブロッキング装置を、観測装置が外部に対して攻撃活動を開始した際の、通信遮断装置として利用することも可能となる。

なお、VMwareでは単一物理ホスト上の仮想ネットワークは10個までに制限されているため、単一物理ホスト上の観測装置最大設置可能数は3システムである。

4.2 ネットワーク

観測装置設置ネットワークとして京都大学が保有するクラスBネットワーク（130.54/16、133.3/16）からそれぞれ/28のサブネット割当を受け、ここに本提案システムを接続した。

観測装置、アクセス記録装置等の接続関係を図5に示す。

図5 実験ネットワーク構成図


4.3 データベース

アクセス記録装置のデータベースはMySQL4.0.26を用いて構築した。データベース上に設定したテーブルとその内容は表1及び表2の通りである。

<table>
<thead>
<tr>
<th>列名</th>
<th>意味</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>不正コード記録の通し番号</td>
</tr>
<tr>
<td>time</td>
<td>アクセス日時</td>
</tr>
<tr>
<td>src.addr</td>
<td>送信元IPアドレス</td>
</tr>
<tr>
<td>src.port</td>
<td>送信元ポート番号</td>
</tr>
<tr>
<td>dst.addr</td>
<td>順先IPアドレス</td>
</tr>
<tr>
<td>dst.port</td>
<td>順先ポート番号</td>
</tr>
<tr>
<td>protocol</td>
<td>トランスポート層プロトコル種類（TCP, UDP, ...)</td>
</tr>
<tr>
<td>size</td>
<td>パケット長</td>
</tr>
<tr>
<td>md5</td>
<td>ベイロードのMD5ハッシュ値</td>
</tr>
<tr>
<td>detection</td>
<td>バッファーオーバーフローの検出結果</td>
</tr>
<tr>
<td>payload</td>
<td>ベイロードをBASE64エンコードした文字列</td>
</tr>
</tbody>
</table>
表2 アクセス記録保存用テーブル

<table>
<thead>
<tr>
<th>列名</th>
<th>意味</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>アクセス記録の通し番号</td>
</tr>
<tr>
<td>time</td>
<td>アクセス時刻</td>
</tr>
<tr>
<td>src.addr</td>
<td>送信元IPアドレス</td>
</tr>
<tr>
<td>src.port</td>
<td>送信元ポート番号</td>
</tr>
<tr>
<td>dst.addr</td>
<td>宛先IPアドレス</td>
</tr>
<tr>
<td>dst.port</td>
<td>宛先ポート番号</td>
</tr>
<tr>
<td>open.time</td>
<td>ボート開放命令を出した日時 (0はポート開放命令を出した日時)</td>
</tr>
<tr>
<td>close.time</td>
<td>ボート閉塞命令を出した日時 (0はポート開放命令を出した日時)</td>
</tr>
</tbody>
</table>

4.4 プログラム

4.4.1 アクセス情報通知プログラム

ブリッジング装置上のiptablesによりアクセス情報を生成し、
syslogに出力させる。またブリッジング装置のsyslog出力元としてアクセス記録装置を指す。

4.4.2 アクセス情報データベース登録プログラム

このプログラムはアクセス記録装置上に設置する。ネットワーク経由でブリッジング装置から送信されるsyslogをFIFOキュー（名前つきパイプ）に入力し、このFIFOキューを1行ずつ読み込み、解析を行い、宛先ポート番号などの情報を含めたSQL文を生成し、データベースに登録する。あるポートへのアクセスの記録がデータベース上にある場合、アクセス時刻（表2参照）の項目を更新する。データベース上にない場合には新規項目として追加する。この時開放命令時刻及び閉塞命令時刻の項目はいずれも0（未発令）で設定する。

4.4.3 待受け開始指示プログラム

このプログラムはアクセス記録装置上に設置する。一定時間（本実装では5分）ごとにcronにより起動され、データベースを検索。1台の命令時刻が0（未発令）のものがあれば、そのポートで待ち受けるプログラムを起動するよう管理下の全ての観測装置に対して命令を送信し、開放命令時刻の項目をその時刻で更新する。

4.4.4 待受けプログラム

このプログラムは観測装置上に設置する。本実装ではmwcx-collected使用した。待ち受けのプログラムはどのような通信に対しても同一の文字列を返す設定をしている。

4.4.5 待受け終了指示プログラム

このプログラムはアクセス記録装置上に設置する。一定時間（本実装では5分）ごとにcronにより起動され、データベースを検索。あるポート上的1台の命令時刻が0（未発令）のものがあれば、そのポートで待ち受けるプログラムを終了するよう管理下の全ての観測装置に対して命令を送信し、閉塞命令時刻の項目をその時刻で更新する。

4.5 使用機材

本実装に使用した機材の性能は以下のとおりである。

- CPU: Intel Pentium 4.32GHz × 2
- Mem: 2GB
- NIF: 4口
- OS: Windows Server 2003
- 仮想ホスト
  - Mem: 各128MB (ブリッジング装置)
  - Mem: 各128MB (仮想向けノード)
  - Mem: 各256MB (観測装置)
- 仮想NIF: 各最大4口
- OS: Linux 2.6.15
- データベースサーバー
  - CPU: Intel Xeon 3.8GHz × 2
- Mem: 2GB
- NIF: 4口
- OS: Linux 2.4.21

4.6 コード解析プログラムとの連携

本実装では株式会社セキュアウェア[5]から提供されたシステムを利用して、ベイリードの検証を行っている。当該システムはベイリード中に仕込まれたバイナリ形式のプログラムを複数の仮想仕様からアセンプリ言語表現に変換して表示するものである。これにより、ある未知のコードがどのような正規行為をしようとしているのか、またある2つの不正コードがどのような役割関係にあるのか等の推定を容易に行うことに寄与している。

5.評価

本提案システムにより取得された攻撃コードの例を図6に示す。

図6中，dc[1-3]は図5のものに対応している。win-xpは観測装置と同一のセグメント上に設置された，Windows XPを搭載した物理ホストである。zombie[1-3]はインターネット上に実在する、我々の管理下にはないホストである。

ここで、ID 1913679とID 1913681を比較すると、ベイリーードのMD5ハッシュ値が等しいことから、同一の攻撃者が同一の内容で複数のノードに対して攻撃コードを送出していることがわかる。また同時に、単純に無意味な応答を返す観測装置に対してても実システムと同様の攻撃活動を展開していることがわかる。

次にID 1913570とID 1913679を比較すると、同一の攻撃者が同一観測装置の同一ポートに対して異なる攻撃コードを送出していることがある。このことから、あるポートで待受けするプログラムがどのような応答を返すべきであるかを予め知ることが難しいことがわかる。

逆にID 1921885とID 191219891のように、同一の攻撃者が同一観測装置の異なるポートに対して同一の攻撃コードを送出していることもわかる。

この攻撃パターンは従来のIDSでは検出されておらず、また数種の脆弱性公開サイトで対象情報は記載されていなかったことから、本提案システムにより未知の攻撃コードを収集することが可能であると考える。

また、仮想化の実システムと通常装置のそれぞれに到達した攻撃を比較した結果、本実験で使用したネットワークについて
<table>
<thead>
<tr>
<th>ID</th>
<th>日時</th>
<th>送信元</th>
<th>命先</th>
<th>プロトコル</th>
<th>サイズ</th>
<th>MD5</th>
<th>コード</th>
</tr>
</thead>
<tbody>
<tr>
<td>1913570</td>
<td>2006/04/14 14:51:36</td>
<td>zombie1 :3284</td>
<td>dc1 :445</td>
<td>tcp</td>
<td>4383</td>
<td>c84f3695e018133c-1</td>
<td>[1]e(1275,1298): **** e7e8ad65a98f8af5 call-&gt;pop structre ****</td>
</tr>
</tbody>
</table>

図6 取得された攻撃コード

は応答内容の差異から実システムであるか否かを検証した上で
本格的な攻撃活動に入るように攻撃は観測されなかった。

6. むすび

本論文では、インターネット上の攻撃活動について、その試
験コードを捕らえることにより、活動が本格化する前に予兆を
捕らえる「攻撃予知」システムの安全な構築方法を提案した。

この攻撃予知システムにより、シグネチャベース IDS やファ
イアウォールなどの従来方式では攻撃行為として認識されずに
防ぎきられなかった攻撃行為についても疑わしい通信として捉え
ることができ、IDS やファイアウォールと連携することでその
蔓延を抑えることが可能になる。

本システムに関する今後の検討課題として、
・ ポートを開放する仮想ノードのランダム化
・ 待受けプログラムの起動数に上限設定
・ 応答文字列の動的変更等を行った際の攻撃行為の傾向変化観察、また観測箇所設定場
所の広範化によるより多くの攻撃コードの収集及びその解析が
挙げられる。

文 献
[1] M. Bailey, et. al., "The Internet Motion Sensor: A Dis-
tributed Blackhole Monitoring System", 12th Annual Net-
work and Distributed System Security Symposium, 2005.

- 6 -