仮想ネットワークを利用した攻撃監視システム

- 安全に攻撃者・マルウェアの攻撃行為を観察する -

1　背景

一般に Honeypot とは攻撃者に対する “おとりシステム” である．Honeypot は攻撃者に侵入させやすい状態をつくり彼らの行動を監視することで，攻撃に関する対策を用意するのに使われている．Honeypot が得る攻撃に関する情報は多岐に渡る．例えば，彼らが侵入を行う目的，コンピュータへの攻撃に使うツール，そして，root 権限を得るために狙うプログラムの脆弱性などである．

一般に Honeypot はジレンマを持つ．そのジレンマとは，Honeypot 内部では侵入者に自由を与え行動を監視したい一方で，Honeypot を踏み台にした外部ホストへの攻撃を防ぎたいというジレンマである．侵入者にネットワークアクセスを許せば外部のホストが危険に晒され，一方でネットワークを遮断すればその中でできる行動にかなり制限がかかってしまい彼等の普段の行動を観察ができない．

2　目的

本提案では仮想ネットワークを持つことで外部に危害を与えずに侵入者の行動やマルウェアの挙動を観察できるシステムを構築し，そこで得られる情報を利用者にわかりやすく提示するのが目的である．

作成したシステムは上記のジレンマを解消して，侵入者にある程度の自由を与えつつその際に別のコンピュータに影響が出ないようにする．このシステムは後述する仮想ホストを作成し，侵入者が Honeypot 内部から外部へ向けて攻撃を行った場合に攻撃の宛先をその仮想ホストへリダイレクトさせる．このようにして攻撃を本システムが用意する仮想ホストから成るネットワーク (仮想ネットワーク) 内で安全に監視できる．

3　開発の内容

複数の仮想的なホストを内部に持つ攻撃監視システム (Honeypot) を実装した．図 1 のように，仮想的なホストを作り出し攻撃をそこへリダイレクトさせることでシステム外部のホストへ危害を与えることなく Honeypot 内での攻撃者の行動を観察することができるのが特長である．

このプロジェクトは大きく分けて「仮想ホスト」,「攻撃のリダイレクション」,「UI 部 (Viewer)」の 3 つに分けられる．

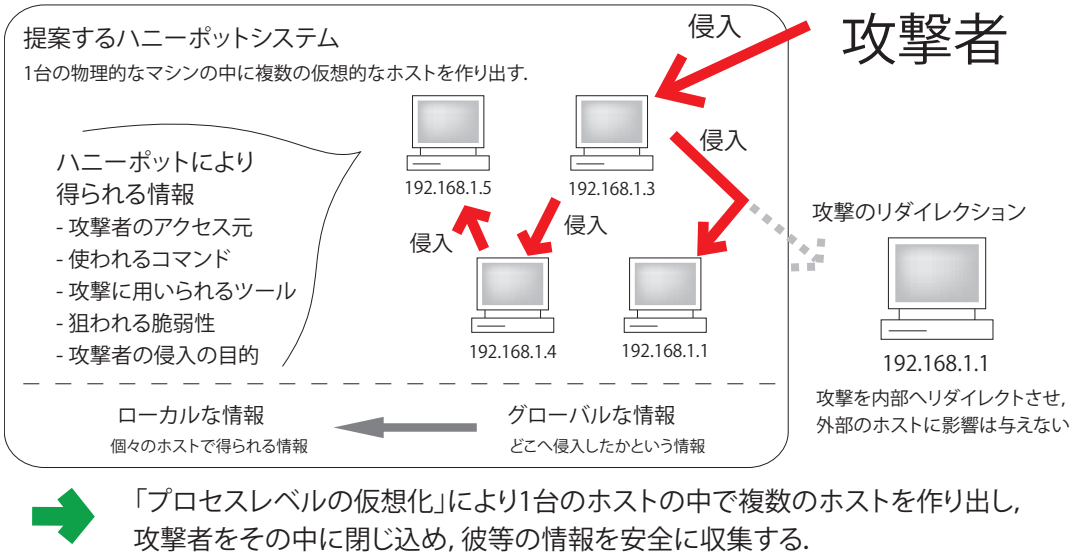

図 1　本プロジェクトの Honeypot システムの概観

3.1　仮想ホスト

仮想ホストは攻撃者やマルウェアのプロセスがあたかも複数のコンピュータで動いているかのようにふるまわせる機能である.

プロセスが発行するシステムコールをそのプロセスが属している仮想ホストを元に変えることによってカーネル内部の動作を変化させる. プロセスがどの仮想ホストで動作しているかを識別させるためにその情報をプロセスを表すカーネル内部の構造体 (task_struct 構造体) に付け加え, その情報に基づいてプロセスとカーネルの通信であるシステムコールのふるまいを変更している.

3.2　攻撃のリダイレクション

攻撃のリダイレクトは, 具体的には, プロセスがネットワーク接続のためのシステムコール (sys_connect) を発行した際に動くフックをカーネル内部に挿入することにより, このシステムコールの動作を書き換えることができる.

本プロジェクトの Honeypot ではこのシステムコールの宛先である IP アドレスを自身のホストにし, ポート番号を特定のデーモンが待ち受けている番号に書き換えることにより, 1 つの OS 内の複数のプロセスがネットワークを通じて通信をしているかのように見せている.

3.3　UI 部 (Viewer)

Honeypot 内部のことを表示する Viewer では仮想ホストを表すノードの表示とグラフの表示を実装した.

Viewwer は Honeypot が動いている時にリアルタイムでどのホストで何が行われているか (どのような端末入力があるか) を表示することができる. リアルタイムで Honeypot を監視している場合をリアルタイムモー

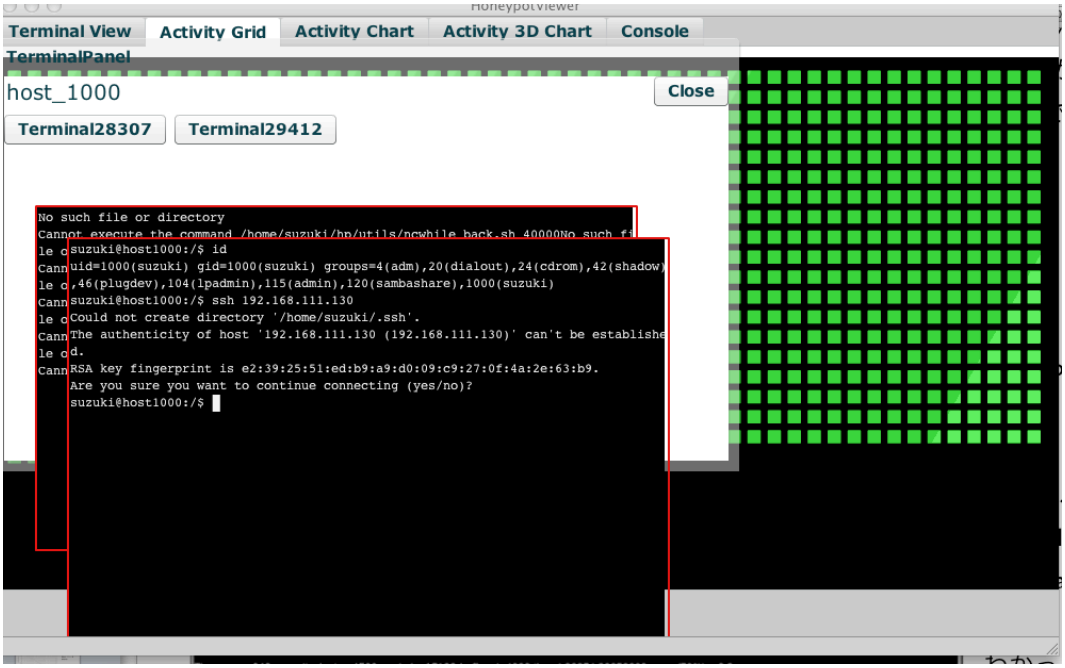

図 2　グリッド表示の上での端末表示

ド，記録された情報をもとに Honeypot 内部で行われたことを再生するリプレイモードがある．

3.3.1　グリッド表示と環状表示

仮想ホストを表すノードの表示には環状表示とグリッド表示の２つの方法をとった．環状表示のあとグリッド表示を行ったが，この場合は数が多くなってもノードの情報を問題なく見ることができた (図 2).

3.3.2　端末入力の表示

環状表示やグリッド表示機能の中のノードをクリックすると Honeypot 内部で行われている端末入力を表示することができる (図 2).

3.3.3　再生機能

UI 部はリアルタイムで Honeypot 内で行われている攻撃を見る機能 (リアルタイムモード) に加えて，リプレイモードとして，ある期間に記録しておいたデータを元にその間に何が行われていたかを再生することができる．

3.3.4　グラフ表示機能

仮想ホストを表すノードを縦軸，時間を横軸，アクティビティの大きさを高さとして 3 次元のグラフを描画した．このグラフは Honeypot 管理者が「いつ・どこの」仮想ホストに注目すればいいかを手助けする (図 3).

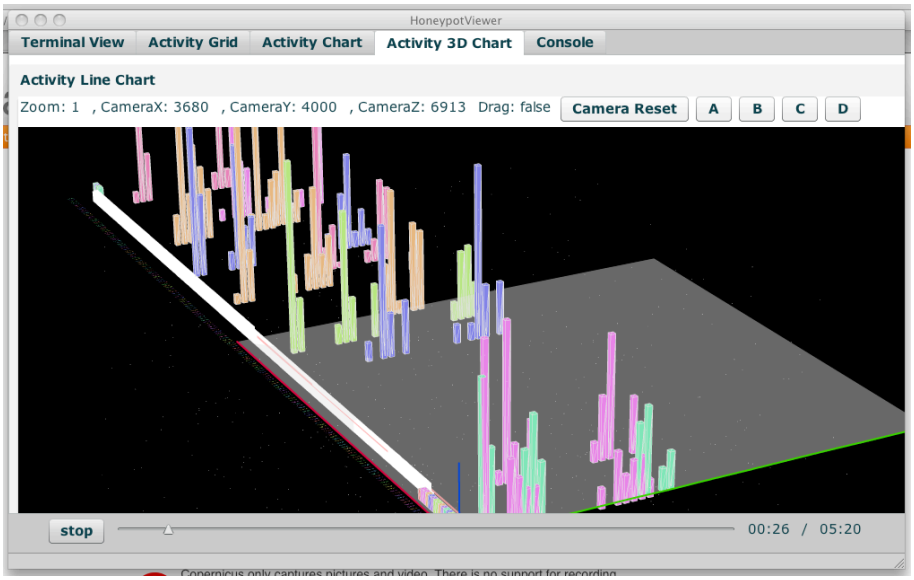

図 3　3 次元空間での仮想ホストのアクティビティ表示

4　従来の技術との相違

既存の Honeypot システム (例えば Sebek) では攻撃者の観察と同時に外部のホストを安全に保つのは難しい．また，Honeypot 内から外部へ向かう接続をリダイレクトする研究はいくつかある[*1]が，そのシステム自体のセキュリティの問題や何台もホストを用意したときの使いやすさ，そして利用者へ侵入者の情報を提供する方法が十分とは言えず，今回の提案ではこれらを解消するシステムを構築した．

本プロジェクトでではこれまでにない数千という規模で仮想的なホストを作り出すことができ，更にそれらの仮想ホスト間での Activity を可視化するようなシステムを作成した．

5　期待される効果

インターネット上の攻撃者の手法を，外部のホストに危害を与えずに知ることができる．

6　活用の見通し

Honeypot に外部からの監視機能を追加したのち，実環境での実験を通じて活用してく．

7　クリエータ名 (所属)

鈴木 友博 (東京大学大学院情報理工学系研究科)

[*1] Potemkin [Vrable et al., 2005], Internet attacks monitoring with dynamic connection redirection mechanisms[E.Alata, 2008] など