4W-6

仮想環境を用いたハニーポットファームの実現

天野 將宏† 蓑原 隆‡
拓殖大学大学院工学研究科† 拓殖大学工学部‡

1 はじめに

インターネットの普及に伴い，ネットワークに接続するコンピュータは様々な種類の不正アクセスの脅威にさらされるようになっている．このように日々深刻化する不正アクセスに対抗するためには侵入時にどうのような通信が行われたか，マルウェアがどのような動作するかなど不正アクセスの調査が重要である．

不正アクセス調査においてはしばしば不正なものと正常なものをいかに区別するか問題になる．これに対して，攻撃を受けることを前提としたハニーポットと呼ばれるおとりを設置し，ハニーポットへのアクセスを監視するという手法が提案されている．ハニーポットは正規の通信の対象外であることから不正アクセスおよび誤りのみによってアクセスされると考えられ，不正アクセスの区別が容易になる．

ハニーポットでは実際に計算機に攻撃させることで不正アクセスの調査を行うことから，不正アクセスの経路となることを防ぐよう安全に運用することが難しい．また，監視範囲が設置したアドレスを対象とした通信に限定される問題がある．

解決案として，監視対象の通信を十分に管理されたハニーポットが設置してある専用ネットワークに集約し監視を行うハニーポットファーム[1]が提案されている．ハニーポットファームに集約した場合においても監視対象アドレスごとにハニーポットが必要であることに変わりはなく，物理的に計算機を設置することは現実的ではない．広範囲のアドレスに対してハニーポットを設置する場合への不正アクセスの通信待ちがおき効率的な監視ではない．

そこで本研究では，ハニーポットファームにおいて少ない計算機で多数のアドレスを効率的に監視するために仮想環境を利用してハニーポットを実現する．

A Scalable Honeyfarm by using the Virtual Environment.
†Masahiro AMANO, Graduate School of Engineering,Takushoku University
‡Takashi MINOHARA, Department of Computer Science,Takushoku University

2 仮想環境によるハニーポットファーム

仮想環境は一台の物理的な計算機で仮想的に独立したサーバ環境を実現する方法で，ホストとなるOSのカーネル，メモリ管理，ファイルシステムを仮想サーバで共有することで，仮想環境ごとに通信，各プロセス，メモリ，ファイルシステムを独立しているように扱うことができる．

仮想環境を利用することで，一台の計算機に多数のハニーポットを実現することが可能であるが，ハニーポットは原理的に不正アクセスを待つ受動的なシステムであることから広範囲アドレスに対してハニーポットを設置した場合，実際にはアクセスを受けないものが発生する可能性がある．そこで実際にアクセスが発生したタイミングで，効率的に不正アクセスの監視を行うハニーポットファームシステムを開発する．

スケーラブルなハニーポットを実現するために，外部から監視対象アドレスへの通信が発生し，ハニーポットの応答が要求された時点で仮想環境にアドレスを割り当てることで，不要なアドレス割り当てを削減する．仮想環境の作成処理を自動化することでハニーポット管理者の管理コストを削減する．

3 IPアドレスの自動割り当て

ハニーポットファームシステムの運用は仮想環境を事前に複数台起動しておき，監視対象のIPアドレスへの通信がシステム届いたときに，アドレスの割り当てていない仮想環境に攻撃パケット内の送信先IPアドレスを割り当てている．

IPアドレス割当ての処理の流れを図1に示す．ハニーポットファームのネットワークに攻撃者からの新たなアクセスが到着すると，ネットワークのゲートウェイは該当する計算機を探すためのARPリクエストを送信する．ハニーポット管理プロセスは，ARPリクエストを受信し，ARPの送信先IPをすでに割当てているかどうか確認する．未割当てであれば空いている仮想環境にアドレスを割当て，仮想環境の起動を確認するためのARPリクエストを再構成して送信する．起動が終了した仮想環境はARPリクエストを受信するとゲートウェイに対してARPリプライを返すので，ゲー

トウェイは起動した仮想環境に対して最初のアクセスを送信することができる．

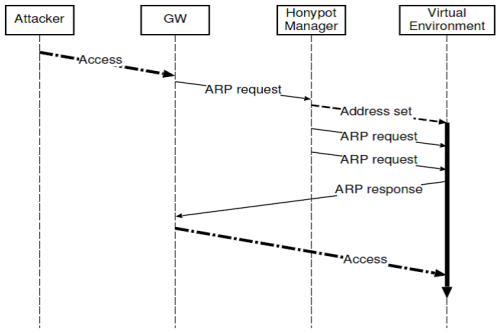

図 1: アクセス時のアドレス割り当ての流れ

4　試作システムの評価

提案方法のハニーポットファームシステムを用いた場合，どの程度コンピュータ資源が必要となるか，また仮想環境の起動にどの程度時間がかかるか評価を行った．なお，ハニーポットファームシステムを下記に示す条件の PC 上に作成した．

- CPU 1.5Ghz
- メモリ 512MB
- カーネル 2.6.16
- 仮想環境 OpenVZ 2.6.16-026test

4.1　スケーラビリティの評価

提案方法によって一台の物理マシンあたり何台の仮想環境を作成できるか評価するため，仮想環境一台あたりのディスク使用量とメモリ使用量を計測した．計測の結果は，仮想環境一台につき約 330MB のディスク容量，8MB のメモリ容量を消費していることが分かった．

試作システムの評価から，仮想環境を用いたハニーポットファームシステムは PC サーバ機ならば一台につき 100 台以上のハニーポットで監視可能と考えられる．

4.2　割り当て時間の計測

仮想環境に動的にアドレスを割り当てるために仮想環境に事前に割り当てる方法に比べ遅れが発生してしまう．そこで，監視対象のアドレスに対するアクセスがあった際の仮想環境への IP アドレスの割り当て時間を調べるために，IP アドレスの割り当て処理に要する時間を計測した．また，仮想環境の起動している数による IP アドレスの割り当て時間への影響を比較するために，仮想環境の起動数の異なる条件で IP アドレスの割り当て処理に要する時間を計測した．なお，割り当て時間は ARP リクエストパケットを取得してから仮想環境への割り当てにかかる時間となる．

計測は ARP リクエストパケットを取得してから割り当て処理が終わるまでの時間で，表 1 となる．計測結果から割り当て時間はおよそ 300ms という値であり，この値は通常の ARP 処理時間に比べ大きく攻撃者に通常と違うシステムであると気づかれる可能性がある．

表 1: 平均割り当て時間

仮想環境数	20	40	60
平均割り当て時間 (ms)	256	272	294
標準偏差	27	28	30

仮想環境の割り当て処理にはシェルスクリプトが含まれる OpenVZ のコマンドを流用している．計測結果は，仮想環境の数が増えるにつれ平均割り当て時間が増加しており，仮想環境のプロセス数が増えたことによりシェルスクリプトの実行時間に遅れがでていると考えるられ，シェルスクリプトの処理をプログラムに直接組み最適化することで，ハニーポットシステムの起動時間の短縮が可能と考える．

仮想マシンによるハニーポットファームを実現しようという Potemkin HoneypFarm では，起動時間が 326ms[3]とあり本システムでも同等の性能もしくそれ以上の性能を持つことが分かる．

5　まとめ

本稿では，監視対象に届く通信をハニーポット専用ネットワークに転送し，ハニーポットの集中管理を行うハニーポットファームのためのハニーポットシステムとして，仮想環境を利用しアクセス発生時にアドレス割り当て行うことで効率的な運用ができるハニーポットファームシステムを提案した．実際に試作システムを作成し評価した結果，1 台の PC サーバによって 100 台以上のハニーポットを実現できる見込みが得られた．今後，システムに差分による共有ファイルシステムなどの機能を実装し，さらに機能を最適化していくことで，実用的なハニーファームシステムを完成させていく．

参考文献

[1] The Honeynet Project: ”Know Your Enemy –Learning about Security Threats–”, Addison Wesley (2004).

[2] Lance Spitzner: ”Honeypot Farms”, http://www.securityfocus.com/printable/infocus/1720, Aug. 2003.

[3] Michael Vrable, Justin Ma: ”Scalability, fidelity, and containment in the potemkin virtual honeyfarm”, Symposium on Operating System Principale, pp.148 - 162 (2005).