

DHCP によって管理されたセグメントに存在する 未使用 IP アドレスの監視手法

溝口 誠一郎[†], Erwan Le Malécot[†], 堀 良彰^{††}, 櫻井 幸一^{††}

[†] 九州大学大学院システム情報科学府 ^{††} 九州大学大学院システム情報科学研究院

インターネットを介した攻撃が増加しているなか、システム管理者はネットワークを不正攻撃から守るために様々な対策をたてているが、実際はネットワークでどのようなことが起きているかを判断するのは困難である。そこで、ネットワーク上の未使用 IP アドレスをハニーポットを用いて観測することによって、ネットワークの挙動を観測する。本研究では、ネットワークの挙動を調べる方法として、DHCP セグメントで監視を行う手法について考察している。これは、DHCP (Dynamic Honeypot Configuration Protocol) サービスを利用して、ハニーポットに動的に IP アドレスを割り当てる手法である。そして、この監視手法に関する更なる考察と、監視システムの設計が今後の課題である。

Monitoring Unused IP Addresses on Network Segments Managed by DHCP

Seiichiro Mizoguchi[†] Erwan Le Malécot[†] Yoshiaki Hori^{††} Kouichi Sakurai^{††}

[†] Graduate School of Information Science and Electrical Engineering, Kyushu University

^{††} Information Technology and Security Group,

Department of Computer Science and Communication Engineering, Kyushu University

New threats are constantly appearing on the Internet. System administrators have developed many tools to try to mitigate those threats, however, currently available countermeasures are still limited. Moreover, it is still difficult for system administrators to fully understand what happens in their networks in (near) real time. We focus on the monitoring of network traffic sent to unused IP addresses with honeypot devices to capture information about network activity. More precisely, we consider ways of handling such unused addresses on network segments managed via DHCP (Dynamic Host Configuration Protocol). In this paper, we propose to exploit that DHCP service to dynamically assign unused IP addresses to honeypot devices, and, discuss the design of such monitoring system.

1 研究背景

パーソナルコンピュータの普及とともに、インターネットは急速な広がりを見せ、世界中の人々がインターネットを利用する時代となった。しかし一方で、インターネット上には様々な脅威が存在するのも事実である。たとえば、ウィルスやワーム、スパイウェアなどの悪意のあるプログラム（マルウェア）がいたるところに存在し、対策を行っていないコンピュータはインターネットに接続して数分後には、何らかの攻撃を受ける¹⁾。最近では、ボットと呼ばれる不正プログラムに感染したホストがネットワークを構成し、DDoS 攻撃やスパムメールの送信などを行うようになっている²⁾

ネットワークは複雑化し、それによりインターネットからの攻撃も複雑化している。

そのようななか、ネットワークの挙動を観測することによって、それらの脅威を把握しようとするさまざまな試みがなされている¹⁾。それは、ネットワーク上にセンサーや観測用のコンピュータシステムを設置し、ネットワークに流れるデータを収集し分析するものである。そして、収集されたデータを分析することによって、ネットワークの挙動を知り、ネットワークに対してどのような攻撃が行われているかを知ることができる^{3) 4)}。これらの情報は、攻撃者の正体や動機、攻撃の方法を理解することにつながり、その後の対策を考える手助けとなる。

ネットワーク内の IP アドレスには、外部のネットワーク（たとえばインターネット）に対してサービスを提供している IP アドレスと、そうでない IP アドレスが存在する。たとえば、ウェブサーバやメールサーバは前者に属し、われわれが普段利用するコンピュータは後者に属している。そのうち、サービスを提供していない IP アドレスに対しては、外部のネットワーク上のホストが起点となる通信は通常は発生しない。つまり、もしそのような IP アドレスに対してアクセスが行われている場合は、そのアクセスは正当でない可能性が高い。そこで、サービスの提供されていない IP アドレスに対するアクセスを監視し分析することで、ネットワーク攻撃に関する情報を得ることができる。

関連研究では、使われていない IP アドレスを探索するためにネットワークスキャンを行っているが、ネットワークの構成が変化するたびにスキャンを行う必要がある。そのため、厳密な意味で動的なハニーポットへの IP アドレス割り当てを行うことができない。

本研究では、使用されていない IP アドレスを監視し情報を得る方法として、DHCP (Dynamic Host Configuration Protocol) セグメント上の IP アドレスを監視する手法について考察する。この手法を利用することでネットワーク構成が変化しても、迅速にハニーポットへ動的に IP アドレスを割り当てることができる。また、DHCP セグメントはネットワークの中でも変化が大きいと考えられるので、そのセグメントを監視することは有効であると考えられる。以下の構成は、第 2 章でネットワークの監視手法について説明し第 3 章で関連研究とそれに従った実験について説明する。そして第 4 章で DHCP セグメントにおける未使用 IP アドレスの監視手法について記述し、第 5 章で結論と今後の課題を述べる。

2 ネットワークの監視方法

ここでは、ネットワークの挙動を監視する方法として、ネットワーク型不正侵入検知システムによる監視方法と、ハニーポットによる監視方法について説明する。

2.1 不正侵入検知システムによる監視

ネットワーク型不正侵入検知システム (Network-based Intrusion Detection System, NIDS) は、ネットワークに対する侵入や攻撃を監視するシステムである⁵⁾。NIDS は、ネットワークに配置され

ているルーターやサーバに導入され、ネットワークを流れるパケットをキャプチャーすることで、ネットワークの監視を行う。また NIDS は、その検知手法でシグネチャ型と異常検知型に分類される。シグネチャ型 IDS は、観測されたデータが既知の攻撃パターンと一致していれば、攻撃をされたと判断し、また異常検知型 IDS は、通常とは違う挙動が観測されたとき、あるいは認められていない動きが観測されたときに攻撃されたと判断する。

しかし IDS には、誤検知 (False Positive) と攻撃の見逃し (False Negative) の問題がある。シグネチャ型 IDS は、既知の攻撃パターンを利用しているため、未知の攻撃を検知することはできない。そのため、攻撃手法の複雑化やウィルスの亜種の増加によって、攻撃の見逃しが発生する。また異常検知型 IDS は、正常な挙動も攻撃と判断する、誤検知の問題を抱えている。

2.2 ハニーポットを利用した監視方法

ハニーポットとは、ネットワークセキュリティのためのおとりシステムである⁷⁾。ハニーポットの定義はさまざまな人が独自の定義を持っており、その表現は多様である。しかしそれらに共通していえることは、それらが何かしらの攻撃を受けるために設置されるということである。つまり、ハニーポットはプローブされ攻撃され、侵害されることに価値を有するセキュリティ資源である。そしておもに攻撃についての情報を収集するために利用される。

ハニーポットには、それを利用するユーザが存在せず、したがっていかなる生産性も持たない³⁾。そのため、ハニーポット内のファイルシステムが変更されることはなく、もし変更が加えられた場合、システムは侵害されたと考えられる。またハニーポットは、ネットワークに対するいかなる能動的な通信も行わないため、外部からのハニーポットに対するアクセスは不正なものにとらえることができる⁷⁾。

ハニーポットと IDS の違いは、ハニーポットが攻撃者との対話を許すということである。一般的なセキュリティのソリューションは、不正アクセスを遮断したり、ウィルスの侵入を防ぐといった、攻撃者との対話を行わないものである。それに対して、ハニーポットは、普通のコンピュータシステムと変わらないため、攻撃者から送られてきたパケットに応答することもできる。そのため、ハニー

ポットから得られる情報は、IDS よりもより詳細な情報となる。たとえば、攻撃者がシステムに侵入する様子や侵入したあとの行動まで、ハニーポットでは観測することができる⁷⁾。さらに、ハニーポットは監視用の IP アドレスを割り当てて監視を行うネットワークデバイスである。NIDS はネットワーク上に流れるパケットをキャプチャーするだけであるため、IP アドレスを必要としない。

ハニーポットの種類は、対話レベルや実装の仕方によって様々である。実装のしかたでは、物理ハニーポットと仮想ハニーポットに分けられる。物理ハニーポットは、ひとつのコンピュータをハニーポットにしたものであり、仮想ハニーポットは物理的には存在しない、プロセスとして実現されるものである。そのため、仮想ハニーポットは物理ハニーポットよりも導入するコストが小さくなる。

ネットワークの監視は、対話のレベルによってその能力が異なる。ネットワークを監視するデバイスのことをセンサーとよび、NIDS やハニーポットはすべてセンサーとなる⁸⁾。

● 対話を行わないセンサー

これは、ネットワークに対していかなる対話も行わないネットワークデバイスをさす。対話を行わないとは、ネットワークからのパケットに対して何も応答しない。このようなセンサーは設計が単純で導入のコストが小さいため、ネットワーク上に大量に設置することができるが、得られる情報は限定される。

● 低対話型ハニーポット

低対話型ハニーポットは攻撃者との対話を制限したハニーポットである。これは一般的に、特定のオペレーティングシステムやサービスのエミュレータであり、攻撃者の行動はエミュレーションのレベルに制限される。これらのサービスはプロセスとして実行されるため、低対話型ハニーポットは仮想ハニーポットに分類される。また、システムが侵害された時のリスクが小さい。

● 高対話型ハニーポット

実際のオペレーティングシステムとアプリケーションを備えており、生産性がない点を除けば通常のコンピュータと同じである。そのため、低対話型ハニーポットに比べ、より詳細

な情報を得ることができるが、侵害された時のリスクは大きくなる。

3 関連研究

ハニーポットを利用したネットワークの監視、侵入検知方法を提案した研究として、Hassan らが提案したハイブリッド型ハニーポットフレームワーク (Hybrid Honeytrap Framework)⁶⁾ について説明する。この不正侵入検知システムは、異なる対話型のハニーポットをネットワークに導入し、不正侵入を検知するシステムである。

Hassan らが提案したシステムでは、未使用の IP アドレスを仮想ハニーポットの一つである Honeyd を用いて監視し、Honeyd へのトラフィックを高対話型ハニーポットへリダイレクトすることによって監視を行う。Honeyd は一つのサーバ上でプロセスとして起動され、一台のマシンで何千ものコンピュータを、ネットワークレベルでエミュレートすることができる。Honeyd にはトラフィックをリダイレクトする機能があり、Honeyd へのトラフィックを決められたホストへリダイレクトすることが可能である。この機能を利用し、複数の Honeyd が決められた役割を持つ高対話型ハニーポット（たとえばウェブサーバのふりをしているハニーポット）へトラフィックをリダイレクトすることで、攻撃者はあたかも、本物のサーバと対話しているような錯覚をうける。

Fig.1 は、ハイブリッド型ハニーポットフレームワークを示している。ゲートウェイの内側のネットワークは、一般のコンピュータが存在するプロダクション用ネットワークと、高対話型ハニーポット用のネットワークに分割されている。プロダクションネットワークには、通常のコンピュータと Honeyd のサーバが設置されている。まず Honeyd のサーバは、プロダクションネットワークに対してネットワークスキャンを行う。ネットワークスキャンには、nmap や p0f などのネットワークスキャンツールによって行われ、その結果をもとに、Honeyd に監視させる IP アドレスと Honeyd の構成を決定する。Honeyd によって IP アドレスの監視が始まると、そこへ向けられたトラフィックは高対話型ハニーポットにリダイレクトされる。

Hassan らの提案では、ハニーポットの設置をするためにネットワークスキャンを行う必要があり、その結果ネットワーク帯域を消費してしまう。使われていない IP アドレスを常に把握してはいないた

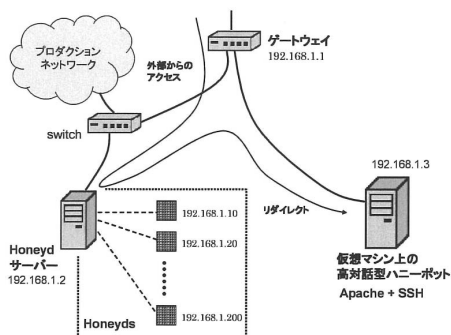


Fig. 1 未使用 IP アドレスの監視

め、ネットワークの変化に合わせて瞬時にハニーポットを配置することが難しい。さらに、監視している IP アドレスが、その他のプロダクションコンピュータに予約されている場合もある。ネットワークスキャンを行うだけでは、そういった事実が確認できない。

4 ネットワークの監視実験

Hassan らの提案したハイブリッド型ハニーポットをもとに、著者らの大学のネットワークを利用して未使用 IP アドレスの監視実験を行った。まず、Honeyd のサーバと高対話型ハニーポットとなるサーバを用意する。OS は両方とも Linux を使い、高対話型ハニーポットには OpenSSH¹¹⁾ とウェブサーバの Apache¹²⁾ をインストールしている。

次に、Honeyd のサーバを設置し、いくつかの使われていない IP アドレスを監視する。ハニーポットには通常、監視用に用意した IP アドレスを割り当てるが、Honeyd は DHCP (Dynamic Host Configuration Protocol) クライアントの機能を備えており、使用されていない IP アドレスを自動で割り当てることができる。Honeyd は SSH と HTTP に対するアクセスに応答し、それ以外のポートへのアクセスには応答しないように設定している。SSH と HTTP に対するアクセスは、Honeyd サーバをプロキシとして高対話型ハニーポットへとリダイレクトされる。そのため、攻撃者からは Honeyd が監視している IP アドレス上のマシンと対話しているように見えるが、実際は高対話型ハニーポットと対話することになる。実験は 2008 年 2 月中の 5

日間、25 個の未使用 IP アドレスを Honeyd を用いて監視し、高対話型ハニーポットから得られたログの分析を行った。また、高対話型ハニーポットの代わりに、マルウェア収集のために用いられる低対話型ハニーポットの Nepenthes¹³⁾ を用いた実験も行った。実験を行ったときのそれぞれのシステムの接続は、Fig.1 と同様になっている。

実験を行った結果、攻撃とみられるアクセスが複数観測された。これらは、特定のウェブページを辞書式に探す攻撃や、特定の ID でログイン試行を行うものであった。たとえば、特定のウェブページを探すアクセスは、1 秒間に約 1 回、6 分間で計 455 回のページ要求が行われていた。また SSH に対するアクセスでは、1 回の試行あたり 1 つの ID でログイン試行を行うものや、1 つの ID で複数回ログイン試行を行うものも見られた。試行に使われた ID を見ると、paul や scott のような英語圏で使われる名前や、tanaka や takahashi のような日本人の名前、root や admin のようなシステム管理者を狙ったものも見られた。さらに大学内の PC から攻撃が観測された。これは、高対話型ハニーポットの代わりに Nepenthes を利用したときに観測されたもので、その PC からアクセスを受けた結果、実行可能ファイルが 2 種類捕獲された。このファイルをフリーのアンチウイルスソフトである ClamAV⁹⁾ で検査したところ、マルウェアとは判断されなかったが、Nepenthes のエミュレートしている脆弱性を利用しているアクセスであったため、不正アクセスだと判断した。

5 DHCP サービスを利用した 未使用 IP アドレスの監視

実験では、大学のネットワーク内の DHCP セグメントにハニーポットを設置することで、IP アドレスの監視を行った。ここでは、DHCP セグメントを利用してネットワークの監視を行うことについて更なる考察を行う。まずはじめに、DHCP サービスとそのセグメントの特徴を説明し、DHCP セグメントを監視する意義について考察する。最後に DHCP セグメント上の使われていない IP アドレスを監視する方法について説明する。

5.1 DHCP サービス

DHCP (Dynamic Host Configuration Protocol) とは、コンピュータがネットワークに接続される際に、ネットワーク通信に必要な情報を提供するためのプロトコルである。必要な情報は、ゲー

トウェイやDNS (Domain Name Server) のIPアドレス、サブネットマスク、そしてクライアントが利用できるIPアドレスなどにあたる。DHCPサービスを提供するサーバは、使用されていないIPアドレスを管理しており、クライアントからの要求に応じて、IPアドレスを1つクライアントに割り当てる。また、クライアントがネットワークから切断されるときは、IPアドレスが解放されることをサーバに知らせる¹⁴⁾。

5.2 DHCP セグメントの特徴

DHCP セグメントは、一時的にネットワークを利用するコンピュータが利用する。それは、DHCP サービスによりIPアドレスを手動で設定する手間を省けるからである。そのため、組織外部の人間がコンピュータを接続する可能性が高い。企業ではポリシーが決められており、認証されていないコンピュータを容易に接続できないようになっていることが普通である。しかし、ポリシーが決められていない、あるいは正しく実行できていないネットワーク環境も多く、そのようなネットワークでは不審なコンピュータが接続される可能性もある。また、DHCP セグメントはネットワーク全体に比べ、トポロジーの変化が大きいと考えられる。

5.3 DHCP セグメントを監視する意義

Hassan らが提案したフレームワークでは、使われていないIPアドレスの探索のためにネットワークスキャンが必要であるが⁶⁾、スキャンによって得られた未使用IPアドレスが、必ずしも使われていないとは限らない。つまり監視しようとするIPアドレスが、ほかのプロダクションコンピュータ用に割り当てられている可能性があり、IPアドレスの衝突が起こる。DHCPサーバは使用されていないIPアドレスを管理しており、IPアドレスの重複が発生しないようにアドレスを割り当てているため、ハニーポットを追加することによるアドレスの衝突問題が回避される。

最後に、ハニーポットをネットワークに設置する場合は、ハニーポット用のセグメントを用意し、プロダクションと隔離することが一般的である。これは、ハニーポットが攻撃され侵入された場合、攻撃者がハニーポットを踏み台にしてセグメント内のコンピュータを攻撃する可能性があるからである⁶⁾。しかし、監視用のブロックを確保しハニーポットを設置した際、攻撃者によってそのブロックが発見されてしまうと、ハニーポットが攻撃さ

れたり、監視用ブロックを回避されたりする可能性がある¹⁰⁾。そのため、ハニーポットとプロダクションが混在できる環境が必要となると考えられる。

5.4 監視方法

はじめに、すべてのIPアドレスを監視する場合を考える。DHCPサーバは、それが管理しているセグメントの使われていないIPアドレスを保持している。ハニーポットのサーバは、まずそのアドレスをDHCPサーバに問い合わせる。問い合わせによってハニーポットのサーバは監視するIPアドレスを決定し、そのアドレス上でハニーポットによる監視を始める。監視を行っている際に、プロダクションからIPアドレスの割り当て要求が発生した場合、DHCPサーバはリストを参照するが、すべてのIPアドレスがハニーポットで使われている場合は、ハニーポットのサーバに問い合わせを行い、ハニーポットをひとつ停止させる。そして、開放されたIPアドレスをプロダクションに割り当てる。その後、プロダクションが使用していたIPアドレスが解放されると、DHCPサーバはそのIPアドレスを回収し、ハニーポットサーバに通知する。通知を受けたハニーポットサーバは、再びそのIPアドレスの監視を始める。

Fig.2はシステムが実装された場合の例を表している。ハニーポットのサーバは、デフォルトですべてのIPアドレスを監視している。そこにプロダクションが接続された場合、サーバはハニーポットをひとつ停止し、開放されたIPアドレスをプロダクションに割り当てる。プロダクションがネットワークから切断されると、ハニーポットのサーバがIPアドレスを回収し、再びハニーポットに割り当てる。

この手法の問題点は、DHCPサーバとハニーポットのサーバがどのように情報のやり取りを行うかということである。特に、プロダクションがIPアドレスを解放したときに、そのことをどのようにして検知するかが問題となる。DHCPのプロトコルでは、IPアドレスの解放の際に、そのことをDHCPサーバに通知することになっている(DHCP RELEASEと呼ばれる)が、通知を行う前にネットワークから切断されることもあるため、工夫が必要となる。また、DHCPサーバがハニーポットを停止させる間はプロダクションコンピュータはIPアドレスを割り当てられないため、予備のIPアドレスを用意し

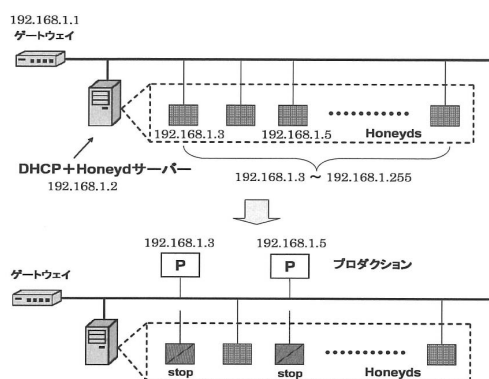


Fig. 2 すべての IP アドレスを監視する様子

ておき、バックグラウンドでハニーポットの停止作業を行えばよい。さらに、すべての IP アドレスにハニーポットを配置すると、接続されているコンピュータの密度が高くなり不自然に見える。その場合は、デフォルトで起動するハニーポットの数を変更することで対応する。具体的には、ネットワーク全体の構成を調べ、その構成に見合った数のハニーポットを配置するのがよい⁶⁾。

6 結論と課題

本研究では、ネットワーク上の未使用 IP アドレスを監視する手法として、ハニーポットを利用した IP アドレスの監視システムについて考察を行った。さらに、その監視手法のひとつとして、DHCP セグメントを監視する手法を提案した。DHCP セグメントは、一時的にネットワークを利用するコンピュータが接続される環境であり、ネットワーク全体と比較して挙動が異なると考えられる。今後の課題として、DHCP セグメントを監視する手法について更なる考察を進め、システムの設計と構築を行っていく。

参考文献

- 1) E. Alata, "Lessons learned from the deployment of a high-interaction honeypot," Proceedings of the Sixth European Dependable Computing Conference, October 2006.
- 2) 須藤年章, "仮想インターネットを用いたボットネット挙動解析システムの評価," Computer Security Symposium, October 2006.
- 3) Niels Provos, "Virtual Honeypots," May 2007.
- 4) Evan Cooke, "The Dark Oracle: Perspective-Aware Unused and Unreachable Address Discovery," 3rd Symposium on Networked System Design & Implementation, May 2006.
- 5) David Elson, "Intrusion detection, Theory and Practice" March 27 2003. <http://www.securityfocus.com/infocus/1203/>
- 6) Hassan Artail, "A hybrid honeypot framework for improving intrusion detection systems in protecting organizational networks," Computers & Security, *ELSEVIER*, vol. 25, pp. 274-288, February 2006.
- 7) Lance Spitzner, 訳：小池英樹他, "ハニーポット-ネットワーク・セキュリティのおとりシステム-", 慶応義塾大学出版会, 2004.
- 8) Georgios Portokalidis, "SweetBait: Zero-Hour Worm Detection and Containment Using Honeypots," Computer Networks, *ELSEVIER*, vol. 51, pp. 1256-1274, April 2007.
- 9) Clam Anti Virus, April 2008. <http://www.clamav.net/>
- 10) Sushant Sinha, "Shedding light on the dark-address," The 14th Annual Network & Distributed System Security Symposium February 28th - March 2nd, 2007.
- 11) OpenSSH, April 2008. <http://www.openssh.org/>
- 12) The Apache Software Foundation, April 2008. <http://www.apache.org/>
- 13) Nepenthes - finest collection - , April 2008. <http://nepenthes.mwcollect.org/>
- 14) RFC 2131 - Dynamic Host Configuration Protocol, IETF, March 1997.