2015年度 Deep Space One / Nerdbox Freaks Working Group 活動報告

太田悟史 (sota@nict.go.jp)　菊地聡 (skikuchi@nict.go.jp)
小林朋幸 (t-kobayashi@nict.go.jp)　安田真悟 (s-yasuda@nict.go.jp)

2015 年 12 月 25 日

目 次

1 はじめに

ここでは，実ノードを用いた大規模なインターネットシミュレーション環境の構築の研究開発を行っている Deep Space One WG および, Nerdbox Freks WG の活動報告を行う．Deep Space One WG は実環境向けのハードウェアおよびソフトウェアを利用した, 大規模な実験用環境の構築・運用に関する研究に取り組んでいる．Nerdbox Freaks WG ではその大規模環境を利用する実験について, 革新技術に追従した実験を始めとした, より高度な実験についての情報の共有と議論を交わしている．

Deep Space One WG では主に StarBED を対象にした研究活動を行っている．StarBED および StarBED での実験補助ツールである SpringOS に関しては文献 [2] を参照していただきたい．

以降 Deep Space One WG 及び Nerdbox Freaks WG の本年度の主な活動について報告する．ネットワーク実験環境は, 多数の小型ノードによる編成からタウンネットワークまで, 多種多様でスケーラブルな実験が行われている．ネットワーク実験環境が複雑化大規模化するに従い, シナリオを持つ実験の制御も容易ではなくなっている．2 節では, 実験リソースと比例して増大する各種ログによるシナリオ操作に代わり, 全体を俯瞰する「シナリオログ」に基づく制御について検討している．

実験ノードの数の増加に比例して実験環境の準備時間が増えるのは効率が悪い．3 節では, 準備段階で行うハードディスクイメージの配布について, 現状のユニキャストによる配送機構をマルチキャストとした場合の影響を, 実装を踏まえて評価している．

セキュリティ対する関心が高まる中, ネットワークテストベッドでのセキュリティ系の実験・演習環境の構築が盛んに行われている．4 節では, サンドボックス型のセキュリティ検証モデルに必要とされる特徴に配慮した, 高詳細度模倣環境構築支援システムである「Alfons」について述べられている．5 節では, 前述の Alfons を用いて被攻撃環境を構築している．秋の WIDE 合宿では, その環境を元に Catch The Flag 演習環境としてデモを行った．Alfons により,5 名分の演習環境の準備から,17 名分の演習環境の提供を容易に実施できた．

2 シナリオ実行フレームワーク

Deep Space One/Nerdbox Freaks では，ネットワークテストベッドにおける利用者の実験をサポートするために新しいシナリオ実行フレームワークを検討している．

実験手順をシナリオとして記述し処理を自動化することで，作業を効率化すると共にその作業の再現性を

確保することができるため，ネットワーク実験者の多くは一般的なスクリプト言語で何らかの実験シナリオを記述している．しかし，特に初めての利用者にとって，不慣れな環境における実験シナリオを何の支援も無く作成することは難しく，実験開始までに想定以上の労力を費やさざるを得ない．

SpringOS には既にシナリオ機能が実装されているものの，独自言語による記述が必要であるために一般的なスクリプト言語と比べて習得コストが高くなる傾向があり，また，ログや内部挙動が分かりづらく利用者単独によるシナリオのデバッグ作業が難しい（開発者による支援が必要）などユーザビリティに課題を抱えている．

このような課題がある中で，開発者や施設職員の支援なく利用者だけで利用できるシナリオ機能を目指し，ユーザビリティを向上させるためにログ機能の検討から始めた．

シナリオログの検討とプロトタイプ

一般に，ネットワーク実験では複数のノードを利用するため，各ノード上にログが分散した状態となる．時系列順に記述されたこれらのログを単純に集約しても，時間情報に加えてノード情報が加わるため，可読性が極めて低い垂れ流しログとなってしまう．そこで，実験全体を俯瞰するログ「シナリオログ」として，時系列ログとは別の方法で記述することを考えた．

ネットワーク実験では「あるノード（群）からの通知が届いたら次の処理へ移行」のように，何らかの処理や状態をトリガーとする状態駆動型のシナリオ記述が求められる．そこで，個々のノード上で進む処理については従来通りの時系列ログを出力しつつ，シナリオログには実験全体の状態遷移過程を記録することでネットワーク実験に適したログ形式を検討した．

このようなコンセプトを一般的なスクリプト言語でどのように実現できるか，まずは Perl でプロトタイプを作成した．このプロトタイプでは，シナリオ（Perl スクリプト）としてユーザが各状態を定義し，シナリオ実行中にその状態の遷移過程を追跡することで，終了時に追跡結果をシナリオログとして出力する．複雑な状態遷移でも可読性を保てるように，シナリオログはテキストではなく図で出力している (図 1，図 2)．

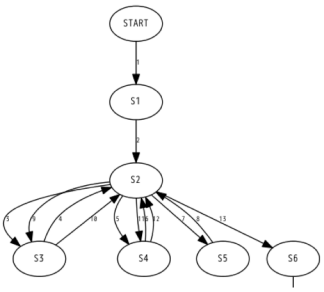

図 1: シナリオログ（正常終了）

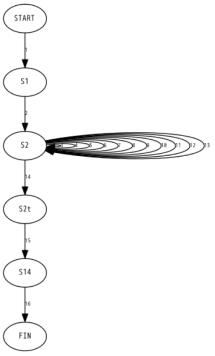

図 2: シナリオログ（タイムアウト）

これにより，異常終了時（図 2）には原因箇所が特定し易くなると共に，正常終了時（図 1）にも状態遷移の詳細な過程が一目で分かるなど，シナリオ全体を俯瞰するログとしてデバッグ作業にも耐えうる高い可読性が実現できることが分かった．

現状ではまだ，ログのプロトタイプに過ぎずシナリオ機能として実用的なものではない．今後の WG 活動の中で，新しいシナリオ実行フレームワークについて更に検討を進める．

3 ディスクデータのマルチキャスト配送

大規模実実験環境においては，環境構築時にハードディスクのイメージを配布する必要がある．雛形となる OS および実験用ソフトウェアを組み込んだイメージを作成した後，そのイメージを大規模に配布しなければならない．StarBED においては従来，TCP 上のユニキャストによる配布を行ってきた．今回はこの配布作業を UDP マルチキャストで行う方法を提案し，実装を行い，評価を行った．詳細については [1] を参照されたい．

4 高詳細度模倣環境の構築 $Alfons$

DS1 では，テストベッドのサイバー攻撃検証に対する応用について議論を行っている．マルウェアの挙動解析や，サイバー攻撃の演習を行うためには，それぞ

れの目的に合わせた模擬環境を構築する必要がある．マルウェアの解析ではサンドボックス検知を回避するために仮想ノードと物理ノードを適宜使い分けた混在環境が必要となってくる．既存の各種ネットワーク実験環境構築を支援するツールでは，仮想ノード，物理ノードどちらか一報を用いた実験環境を構築するツールが多く，両方のノードを透過的に扱う事が難しい．また，目的に合わせた多様なノードを準備する場合，反復的な検証や演習を行う際に多量のストレージを必要とし，実験の保存が困難になると共にノードの作り込みが煩雑になる．しかし，模擬環境は，解析や演習のポリシに基づきネットワークトポロジやネットワークノードが異なるが，利用する OS の種類や基本的なネットワークサービスの種類は重複が多く，それらの設定のみ異なる場合が多い．そこで，我々は主な重複物となるノードのディスクイメージと，それらを特徴付ける設定ファイルや検体などのファイルを個別に管理し，必要に応じて組み合わせる事でビルディングブロック式に環境構築を行うシステム「Alfons」を提案し，設計と実装を行った．詳細は wide-paper-deepspace1-simabuki-icm2015.txt および wide-paper-deepspace1-simabuki-ic2015.txt を参考にされたい．

5 サイバーレンジ環境による行動の解析

サイバー攻撃への対策に予防と早期発見がある．早期発見として Deep Packet Inspection(DPI) 等によるネットワーク監視が有効であるものの, 通常のサービスを利用された場合には識別が難しい．そこで攻撃者の挙動に着目し, 端末操作の挙動中に攻撃者特有の特徴を検知する方法を検討している．特徴を得るためにはある程度の攻撃者の挙動情報が必要である．今回, 攻撃者の挙動情報の収集を目的として,2015 年秋の WIDE 研究会にて Capture The Flag(CTF) 体験演習環境を元に, 参加者を攻撃者と見立てた挙動情報の収集を行った．

Capture The Flag(CTF)

”有益なデータを探す” という行動は, 宝物探しゲームの参加者とサイバー攻撃者の行動の一部と類似していると考え, 宝探しの要素を意識した内容とした．

内容

CTF 参加者には次の内容が伝えられ, 乗っ取り済み端末へ VNC 接続されている端末を操作し, 最終目的を達成する．

1. 最終目的は, 某社内のデータベースに登録されているデータを取得する事
2. すでに某社ネットワークの 1 端末を乗っ取り済み
3. 乗っ取り済みの端末には VNC 接続済み
4. 途中チェックポイント用のテキストファイルを取得する事

CTF 参加者は, 乗っ取り端末の正規利用者になりすまし, 乗っ取り端末上にある設定やメール等の情報をきっかけに社内ネットワークの状況を探索する．

今回は, サーバの運用方法や各個人のセキュリティ対策の弱点をあらかじめ設定しておく事で, 各サーバやデータベースへのアクセスが可能としてあるため, ネットワークやサーバの運用に知識があれば達成できる内容となっている．VNC 接続を行っている端末は Internet 接続が可能なため, 不明な点については各 CTF 参加者に検索してもらうこととした．

CTF 結果

今回の CTF 参加者は 17 名, うち 7 名がリタイヤし,10 名がゴールした．参加者は学生からネットワーク運用のエキスパートまで様々で, ゴール時間も 34 分から 1 時間 22 分とばらつきの幅が多かった．これは, スキル差も当然あるものの, ゴールまでの道筋とは別に用意された, 袋小路となっているファイルサーバの影響も考えられる．

環境構築

今回の演習環境を図 3 に示す．WIDE 研究会会場には VNC 用クライアントとして surface を持込み, 探索対象となる演習環境は StarBED で構築されている．体験用社内ネットワークは参加者 1 人につき 1 つ提供される．利用できるリソースの制限から一度に 5 セットの体験環境を用意しておき, 体験が終わる度に新たな環境を用いている．

1 つの演習環境には OS が Windows7 の踏み台クライアントと CentOS,Ubuntu 等の UNIX 系サーバが存在する. 社内ネットワークという前提からクライアント用セグメント, サーバ用セグメント, DMZ 用セグメントの 3 つのサブネットとそれらをまとめる Firewall という, 小規模で典型的な構成とした.

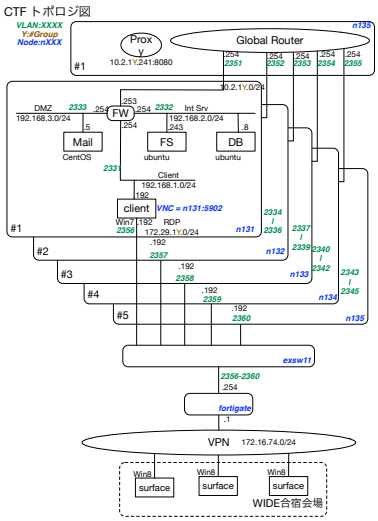

図 3: CTF トポロジ

環境の構築には前章の Alfons を利用している. 今回の体験環境の提供の流れは,Alfons を元に以下のようになっている.

1. ひな形環境の基礎部分 (ひな形基礎環境) の構築:Alfons
2. ひな形基礎環境を用いての詳細部分セットアップ:対応
3. ひな形環境としての保存:Alfons
4. ひな形環境に基づく 5 グループ分の構築:Alfons

典型的な OS とサービスをもつサーバのイメージは Alfons で予め用意されているため, OS のインストールは不要である. また,Alfons でネットワークトポロジと IPaddress の設定も容易に行えるため, ひな形となるネットワーク環境の準備作業にかかる時間が短くて済む. 今回は, ひな形ネットワーク環境上で, メールの送受信データやデータベースへのデータの挿入, 弱点の作り込みを行った.

17 名の参加者に対して, 前述の仕込みを終えたひな形環境を元に Alfons によって個別に演習環境を提供した. 実験環境を 1 度構築した後は, その実験環境を使い続けるのが主な利用方法であったが, Alfons により, 実験環境の構築段階を含めた試行が容易に行える.

観測

観測方法

今回はログインス時に入力キーをロギングするスクリプト (strace を利用) を起動し, サーバー上で入力したキーストロークを全て記録することとした. その結果, 参加者毎のサーバー別のコマンド内容を取得した.

必要な観測内容については, 今後の課題とする.

観測結果

参加者全員が実行したコマンドとその数を図 4 にまとめた. サーバは UNIX 系のものだけであったので, コマンド内容は UNIX コマンドだけとなっている. ディレクトリの探索とファイルを閲覧するためのコマンドが多数を占めているのがわかる. mysql コマンドが多いのは, データベースが mysql だけであった事と, ゴールがデータベースの中味であると伝えられていた結果, 操作が集中したためと予想される.

history は正規の運用者が実施しているコマンドを探るためで, これが多いのは探索行動の特徴と捉えられる. また,whoami コマンドや user コマンドなどは通常の運用コマンドで多用される事がない.

課題

今回の試行環境の構築や参加者のアンケートから, 次の課題が挙げられる.

1. 収集ログの分析
   コマンドオプションによる分類や,OS 別の得手不得手, 利用コマンドによる世代推定や, 通常の運用者との比較等.
2. 演習環境のリアリティの向上
   踏み台となるクライアントの生活感がまだ不足している. 一度も起動されていないアプリケーションや,「最近使ったファイル」がない, 等.

3. 観測方法
   必要となる観測項目の検討を行う．また, 攻撃者の観測を見据えた場合の, 発見が困難な観測手法.

4. 構築方法
   高詳細部分の自動生成や, 脆弱部分の自動投入, 演習中の動的対応等.

まとめ

今回は Capture The Flag の演習体験を通じてサイバー攻撃者の探索行動に似た挙動を得るため,Alfons を用いて演習環境を構築した．Alfons の利用により, 初期状態の演習環境を参加者単位に構築・提供することが出来た．行動の観測については入力キーのロギングで取得し, 実施コマンドの全体的な内容について確認した. 今後はログ内容を精査するとともに, 演習環境と観測機能を充実させていきたい.

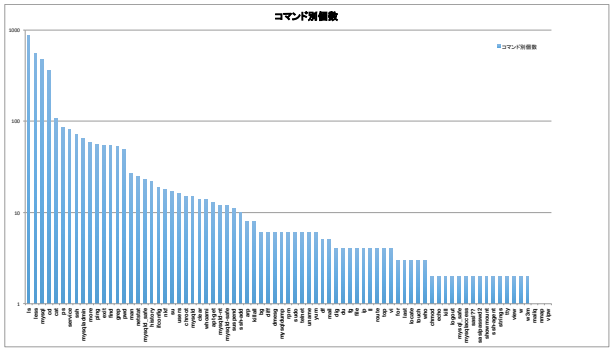

図 4: 実行コマンド

6　おわりに

Deep Space One WG および Nerdbox Freaks WG の活動は, ネットワークテストベッドの運用と利用の双方の側面で研究を行い, 情報交換や議論を交わすことにより, 相互に発展を狙うものである.

ネットワークテストベッドは複数のエミュレータ／シミュレータの連携環境など, 今後も複雑化する実験環境へ対応しなければならない．セキュリティ関連の検証では、スケーラブルでありながら高詳細な模擬環境が必要であり, それに対応したシステムは今後ますます発展する予定である．ますます大規模化する実験環境に対して, 構築支援に加えて実験遂行の支援が必要である．人の手による全体管理が困難になりつつある今, 全体を俯瞰できる実験遂行支援の提供が急がれる.

本年度も秋の WIDE 合宿にて, 合宿ネットワークを用いた実験に参加している．利用を快諾していただいた皆様に, この場で感謝したい.

来年度も Deep Space One WG と Nerdbox Freaks WG との協調により，柔軟な高度な実験環境を目指し，研究開発を継続する.

参考文献

[1] 小林朋幸, 菊地聡, 知念賢一, 宮地利幸, 三輪信介, “**テストベッドにおけるマルチキャストによるディスクイメージの配布**” 情報処理学会 マルチメディア，分散，協調とモバイル *(DICOMO)* 論文集, pp. 1136–1144, 2015 年, 7 月.

[2] 宮地利幸, 中田潤也, 知念賢一, ラズバン・ベウラン, 三輪信介, 岡田崇, 三角真, 宇多仁, 芳炭将, 丹康雄, 中川晋一, 篠田陽一, “*StarBED:* **大規模ネットワーク実証環境**”, 情報処理, 第 49 巻, 第 1 号, pp. 57-70, 2008 年, 1 月.