6X-02

T-Pot を用いたサイバー攻撃の分析

須藤　啓介　　向井　宏明
金沢工業大学　工学部　情報工学科

1. 序論

近年，インターネットの普及とともにサイバー攻撃の被害数が年々増加し，インターネットに接続できる端末が標的とされ問題となっている．適切なセキュリティ対策を行うためには，サイバー攻撃の動向を把握する必要がある．本稿では，サイバー攻撃を分析するための検証方法として，インターネット上にマルチハニーポットである T-Pot を設置し，攻撃データの収集を 2 か月間行った．その結果、攻撃に使用されるユーザー名，パスワードの組み合わせなどのデータを収集することが出来たので報告する．

2. ハニーポットとは

ハニーポットとは，日本語で直訳すると蜜壺という意味をもつ単語であり，クラッカーから不正なアクセスを受けることを前提として作られたシステムのことである．ハニーポットの管理者は，システムにポートをわざと開放しておくなどの脆弱性を残したまま運用することでサイバー攻撃を促し不正侵入させ，最新の攻撃手法や傾向などを調査することが出来る．

ハニーポットには高対話型，低対話型と呼ばれる種類がある．高対話型は，脆弱性を残した本物の OS やアプリケーションをハニーポットとして運用するものである．高対話型は本物のシステムをハニーポットとして運用しているため，クラッカーが攻撃した内容を多く収集することができるというメリットもあるが，侵入された時のリスクが高いというデメリットもある．低対話型は OS やアプリケーションの動作をエミュレートして運用するものである．エミュレートした範囲でしか動作しないため，高対話型よりも得られる情報量は少ないが，安全に運用ができるというメリットがある[1]．

3. ハニーポットを用いた検証環境の構築

3. 1. 概要

サイバー攻撃を分析するための検証方法として，インターネット上にハニーポットを設置し，攻撃データの収集を行う．運用するハニーポットのネットワーク構成図を図 1 に示す．ハニーポットを運用するため，IP アドレスは金沢工業大学が所有するグローバル IP アドレスを設定して運用している．ハニーポットに攻撃を誘うため，ポートを 1 番から 64000 番まで開放して脆弱性を残している．

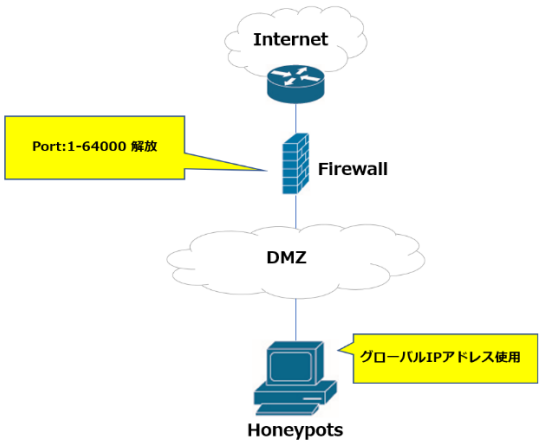

図 1　ネットワーク構成図

3. 2. T-Pot とは

今回使用したハニーポットは T-Pot(20.06.1)である．T-Pot は同一のホストに Docker を用いて複数のコンテナを作成し，その上で様々なハニーポットを運用するマルチハニーポットである．T-Pot は，インストールの種類として Standard，Sensor，Industrial，Collector，NextGen，Medical が存在するが，本研究でインストールするのは Standard である．Standard インストールを構成するハニーポットとツールを表 1 に示す[2]．

表 1　T-Pot を構成するハニーポットとツール

Honeypots	ADBHoney, Ciscoasa, Citrixhoneypot, Conpot, Cowrie, Dicompot, Dionaea, Elasticpot, Heralding, Honeysap, Honeytrap, Mailoney, Medpot, Rdpy, Snare & Tanner
Tools	Cockpit, Cyberchef, ELK, fatt, Elasticsearch Head, ewsposter, nginx / heimdall, spiderfoot, p0f, suricata

4. 検証結果

T-Pot を 2020 年 10 月 1 日から同年 12 月 1 日の 2 か月間運用した．運用して得られたデータの一部を順に紹介する．

(1)T-Pot を構成する 15 種類のハニーポットが，実験期間に受けた攻撃件数を表 2 に示す．

(2)各ハニーポットが攻撃を受けた国名と件数の結果を表 3 に示す．

(3)各ハニーポットがアクセス試行に使用されたユーザー名とその試行回数の上位 10 件の結果を表 4 に示す．

(4)各ハニーポットがアクセス試行に使用されたパスワードとその試行回数の上位 10 件の結果を表 5 に示す．

(5)Wireshark を用いて T-Pot に対する SSH 通信をキャプチャした結果をフローグラフにしたものを図 2 に示す．

Cyber attacks analysis with T-Pot
Sudou Keisuke and Hiroaki Mukai
Department of Information and Computer Science, College of Engineering, Kanazawa Institute of Technology

表 2　各ハニーポットの攻撃件数

	ハニーポット名	攻撃件数
1	Dionaea	9,089,727
2	Cowrie	4,726,573
3	Heralding	787,098
4	Honeytrap	477,199
5	Rdpy	207,887
6	Mailoney	57,690
7	Tanner	9,895
8	Adbhoney	7,847
9	Ciscoasa	3,347
10	CitrixHoneypot	2,178
11	ElasticPot	1,610
12	ConPot	1,285
13	Dicompot	89
14	Honeysap	25
15	Medpot	3

表 3　攻撃元の国名と攻撃件数

	国名	攻撃件数
1	China	1,515,521
2	Vietnam	1,328,761
3	India	1,084,507
4	Ireland	953,986
5	United States	864,061
6	Russia	805,032
7	Pakistan	685,503
8	Indonesia	668,426
9	Venezuela	495,550
10	Brazil	464,611

表 4　アクセス試行に使用されたユーザー名と試行回数

	ユーザー名	試行回数
1	root	328,603
2	guest	93,473
3	sa	78,702
4	nproc	11,931
5	admin	9,970
6	test	9,390
7	ubuntu	4,911
8	postgres	4,571
9	oracle	4,280
10	user	4,262

表 5　アクセス試行に使用されたパスワードと試行回数

	パスワード	試行回数
1	guest	92,345
2	root	70,783
3	123456	23,360
4	nproc	11,931
5	password	10,835
6		9,364
7	123	9,106
8	12345678	6,809
9	1234	4,757
10	test	4,569

図 2　SSH 通信をパケットキャプチャした結果

5. サイバー攻撃の分析

T-Pot を 2 か月間運用した結果，サイバー攻撃の傾向を可視化することが出来た．サイバー攻撃には流行があり，局所的に攻撃が増加している箇所があることや，攻撃元国家によって，攻撃件数が急増している箇所が確認された．

攻撃に使用されているユーザー名を確認すると，root，sa，admin などの管理者権限を持つユーザー名や，guest，test，ubuntu などのテスト環境，簡易的にシステムを構築する際の初期設定に使用されるユーザー名が多く確認された．

攻撃に使用されているパスワードを確認すると，guest，root などのユーザー名と同様のパスワードや，123456，password などの覚えやすいパスワード，1qaz2wsx などのキーボードの左上段から順にタイプするなどの一見堅牢に見えるパスワードが確認された．

6. 結論

サイバー攻撃を分析するための検証方法として，インターネット上にマルチハニーポットである T-Pot を設置し，攻撃データの収集を 2 か月間行った．その結果，サイバー攻撃の傾向，攻撃元国家，攻撃に使用されるユーザー名，パスワードなどのデータを収集することが出来た．

収集したデータを分析すると，ユーザー名に管理者権限を持つものを使用することや，テスト環境などの簡易的にシステムを構築する際の初期設定に使用されるユーザー名が多く確認された．またパスワードには，ユーザー名と同様なパスワードを設定することや，覚えやすいパスワードが設定されていた．

したがってユーザー名，パスワードに対する攻撃を対策することがサイバー攻撃の被害を減少させることにつながると考えられる．そこで，ハニーポットを用いて収集したユーザー名，パスワードのデータを参照して，サイバー攻撃に使用されるユーザー名，パスワードは設定できないようにするシステムの開発が今後必要と考えられる．

参考文献

[1] 馬場一輝，梅原英一，”ハニーポットによる学内ネットワークへの不正アクセスの観測”，東京都市大学，2017-04.
[2] T-Pot, https://github.com/telekom-security/tpotce，引用日：2020 年 12 月 11 日