4Z-7

SSH における攻撃ツールの識別
Detect attack tool of SSH brute force

福島大学共生システム理工研究科
篠田研究室　マルダン ムイデン

1.はじめに

1.1 研究背景

近年ネットワークは発展し,あらゆる人がネットワークを利用するようになっているいる.インターネットを通じてゲーム,電子メールの送信,オンラインショッピング,SNS の利用,行政手続きなど様々なことが行えるようになった.その一方でネットワークを利用する不正行為も問題となってきた.不正行為はシステムの脆弱性を突くものや一般ユーザのホストを乗っ取り他のホストへの攻撃の踏み台にするものなど無数の種類が存在する.これらの行為への対処は一般的に各ホストやネットワークの管理者に委ねられており,各管理者はネットワークの安全性を高めるため,ファイアーウォールや IDS(侵入検知システム)などを設置する対策を行っている。

1.2 研究目的

一般的な IDS では、パッケット分析やパターン照合により不正アクセスを検出することができるが、さらに分析し、相手の情報を取ることはできない。本研究では、様々な攻撃の中で 、SSH 攻撃を対象にして、攻撃者が用いたツールを検出する。検出結果により、攻撃団体を発見する可能性を高める方式を提案。

2.研究方法

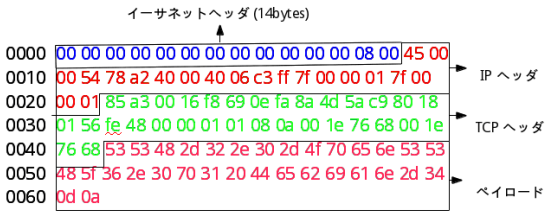
パケットキャプチャーにより、既に知られているブルートフォースツールが通信する時に発生する特徴的なデータを確定し、フィンガープリント用のパラメータとして預ける（タイミング、攻撃回数、ユーザー名、用いた SSH ライブラリ、バージョン交換段階でのパケット長など）。また、未知の攻撃ツールに対しては、ハニーポットのログファイルにより、新たな攻撃ツールを収集し、分析を行う。サンプルとしては、ネット上で流行っている SSH 攻撃ツールを表 1 に示している。

ツール番号	ツール名
1	bruteSSH
2	Metasploit
3	Hydra
4	Medusa
5	nCrack
6	patator

表 1　既知の SSH 攻撃ツール

2.1 既知の攻撃ツールの識別

SSH 通信は、暗号化された通信であるが、コネ久ションが立ち上がる前に、SSH サーバと SSH クライアントの間でバージョン交換を行う。この段階でのパケットの長さとペイロードは攻撃ツールによって違うので、フィンガープリントとして使える。表 2



と図 2 に示している。

図 2 wireshark によるパケット分析

ツール名	Length	info
bruteSSH	92	SSH-2.0-paramiko_1.7.7.1
Metasploit	87	SSH-2.0-OpenSSH_5.0
Hydra	87	SSH-2.0-libssh-0.5.2
Medusa	86	SSH2.0-MEDUSA_1.0
nCrack	86	SSH-2.0-OpenSSH_5.2
patator	92	SSH-2.0-paramiko_1.7.7.1

表 2　パケットの長さとペイロード

そして、攻撃者が試したユーザー名や攻撃回数から攻撃辞書を推測することができる。よって、攻撃

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.

辞書内臓のツールを確かめることが可能となる。
表3に示している。

回数	ユーザー名	国家
350	root	オランダ
4	root	インド
3	oracle	オランダ
2	msr	オランダ
1	zt	オランダ
1	user0	オランダ
1	ss2701	オランダ
1	sir	オランダ
1	roo	オランダ

表3 ユーザー名と攻撃回数

また、攻撃の頻度は図3に示しているようにツールの設置や種類によっても違うので、フィンガープリントとして使うことは考えられる。

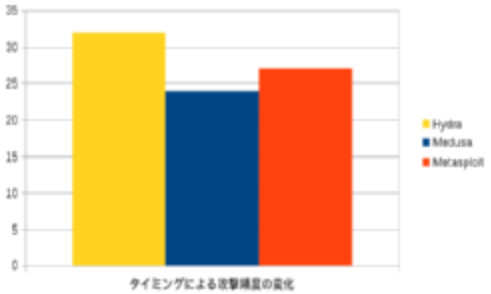


図3 ネットワーク状況により攻撃頻度変化

最後に、フィンガープリントとして使えるパラメータを表4に示している。

パラメータ番号	パラメータ
1	SSH Client library
2	パケットの長さ
3	攻撃の時間差
4	攻撃回数
5	試したユーザー名

表4

2.2 未知の攻撃ツールの識別

未知の攻撃ツールの識別は、SSH向けハニーポットの一種であるKippoを用いて、新たな攻撃ツールを収集し、さらに分析を行うことで、識別できる攻撃ツールの種類を増加。

3.終わりに

3.1 研究結果

ある一ヶ月のキャプチャーにより取られたデータに対し、識別を行った結果を図4に示す。

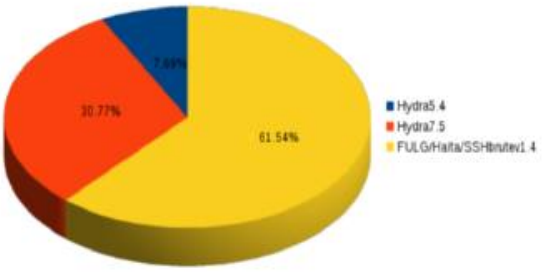


図4

3.2 今後の展望

今後は、識別できる攻撃ツールの種類を増加することとパスワードのランダム化を実現し、 攻撃の関連性を確認できる機能を作ることを期待している、

参考文献

[1] Analyzing Malicious SSH Login Attempts 、http://www.symantec.com/connect/articles/analyzing-malicious-ssh-login-attempts
[2] Snort,http://www.snort.org.
[3] Bro, http://www.bro-ids.org/
[4] The Secure Shell,http://docstore.mik.ua/orelly/
[5] Beyond the SSH Attacks GOVCERT.NL
[6] nmap,http://nmap.org/book/osdetect.html
[7] kippo http://code.google.com/p/kippo/
[8] BruteSSH2 - 21st Century War Dialer
、SANS Vancouver B.C
[9] RFC4250,RFC4251,RFC4252,RFC4253,RFC4254,RFC4255,RFC4256,RFC4335,RFC4344,RFC4345,RFC4419,

Copyright ©2014 Information Processing Society of Japan.
All Rights Reserved.