卒業論文 2018 年度 (平成 30 年)

低対話型 Honeypot のコマンド拡張による
高対話型 Honeypot への近似

慶應義塾大学 総合政策学部
菅藤 佑太

卒業論文要旨 - 2018 年度 (平成 30 年度)

低対話型 Honeypot のコマンド拡張による 高対話型 Honeypot への近似

PC の普及や IoT デバイスのシステム高度化により, 高度な処理系を組むことが可能になった. これによりデバイス上に Linux 系などの OS が搭載された機器が広く人々に使われるようになった. また,Linux 系 OS にリモートログインする手法として SSH がある． これを用いて不正に侵入する攻撃が行われている. 侵入された際に侵入者がどのような挙動をしているのかを知る手段として,Honeypot がある. 敢えて SSH で侵入しやすいような環境を作ることで, 侵入者にログイン試行に成功したと検知させ, その際に実行したコマンドのログを収集するものである. また現在では Shell の挙動をエミュレートした Honeypot が広く使用されており, この Honeypot は実行できるコマンドが少ない実装になっている. そのため Honeypot への侵入者に侵入先が Honeypot であると検知されてしまう. そこで事前実験では Honeypot のコマンドを拡張し, 拡張をしていない Honeypot とコマンドの拡張をした Honeypot で侵入ログを収集した. 収集したログを確率的な算出方法を使用することで比較した結果, より多くの侵入者のコマンド実行ログのパターンを取得できることを示した. 本研究ではコマンドを拡張した Honeypot の侵入ログがどれほど実際の OS に不正な SSH の侵入をされた際の侵入ログに近似したのかをを示すために, 拡張をしていない Honeypot とコマンドの拡張をした Honeypot と, さらに実際の OS を使用した Honeypot で侵入ログを収集した. この 3 つの侵入ログを自然言語処理の意味解析を用い, コマンドの一つ一つの意味をベクトル表現することで, 拡張した Honeypot で収集した侵入ログが, 拡張をしていない Honeypot で収集した侵入ログよりも, 実際の OS を使用した Honeypot で侵入ログに意味的に近くなることを評価した.

キーワード:
1. SSH, 2. Honeypot, 3. 機械学習, 4. 自然言語処理

慶應義塾大学 総合政策学部
菅藤 佑太

Abstract of Bachelor's Thesis - Academic Year 2018

Approximation of high-interaction honeypots by Command Extension of low-interaction honeypot

I was able to make high processing system, and a moving apparatus is wide, and the OS's such as the Linux system came to be in this way used for people on a device, and, meanwhile, one's apparatus is stepped over by an unjust invasion of SSH, and I am attacked to the network apparatus of the third party from an apparatus of oneself by the spread of PCs and the system advancement of the IoT device, and a problem made in the environment that a virus and a back door are installed, and is carried out a virus an apparatus of oneself illegally occurs. Let an intruder detect it by making the environment that there is ,Honeypot as a window what kind of ways an intruder behaves when was invaded, and is easy to invade it daringly in SSH when succeeded in a login trial, and Honeypot which collect the log of the command that carried out on this occasion, and emulated behavior of Shell now again is wide, and is used, and there are few commands that this Honeypot can carry out; as a result of being implemented, and therefore being detected by an intruder to Honeypot when invasion ahead was Honeypot, and expanding the command of Honeypot by the there prior experiment, and having compared the log that collected invasion log in Honeypot which expanded Honeypot and the command that did not expand, and collected by using a probabilistic calculation method, with Honeypot which expanded Honeypot and the command that did not expand, collected invasion log more in Honeypot using the real OS, and invasion log of Honeypot which showed that could acquire a pattern of the command practice log of more intruders, and expanded the command in this study used semantic analysis of the natural language processing for the real OS in the invasion log of these three how to show approximation したのかをを to invasion log when was invaded of unjust SSH, and evaluated a semantically thing nearby in invasion log than the invasion log that collected in Honeypot which the invasion log that collected in Honeypot which expanded because a vector expressed one one meaning of the command did not expand in Honeypot using the real OS.

Keywords :
1. SSH, 2. Honeypot, 3. Machine Learning, 4. Natural Language Processing

Keio University, Faculty of Policy Management Studies
Yuta Sugafuji

目 次

図 目 次

表 目 次