低対話型SSH 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 村井純研究室
総合政策学部 3年 菅藤 佑太
NECO Lab. 村井純研究室 インターネットと社会

背景

バレやすい

低対話型Honeypot

- OSやアプリケーションをエミュレート(今回はShell)
- 乗っ取られたり踏み台になる危険が少ない

危険

高対話型Honeypot

- 本物のOSで実現
- 乗っ取られたり踏み台になる危険がある

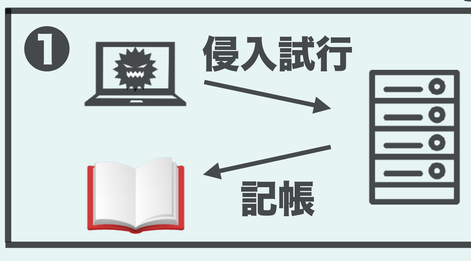
Honeypot
サイバー攻撃者による攻撃手法を調べる為に、わざと侵入し易いように設定された囮システム

BusyBox
標準UNIXコマンドで重要なプログラムを単一のファイルに詰め込んだもの

問題

低対話型Honeypotはコマンド入力時の挙動が実物のShellとは異なるため、侵入先がHoneypotであると攻撃者に知られてしまう

- コマンドを入力した際、実物のShellとは違う挙動をするとHoneypotだと分かってしまう
- デフォルトで実装されているコマンドやオプションが少なく、一般によく使われるものでも実装されていない
- 様々な種類のHoneypotごとに攻撃者がHoneypotであると見破る術が存在する



Honeypotを想定した攻撃者の攻撃フロー

❶ 攻撃対象に侵入試行をし、可能なら台帳に記入する
❷ 侵入先がHoneypotであるか否かの見極めをする
❸ ❶,❷をクリアしたら実際に攻撃を行う

目的

侵入/攻撃者に広く使われるコマンドの実装を行い挙動を本物に近似させることで、攻撃者にHoneypotであることを知られないようにする

手法

攻撃者の使うコマンドを低対話型Honeypotに実装する

- 攻撃者が使う様なコマンドが実装されていないものが多く、Honeypotであると知られない為に実装する

実装

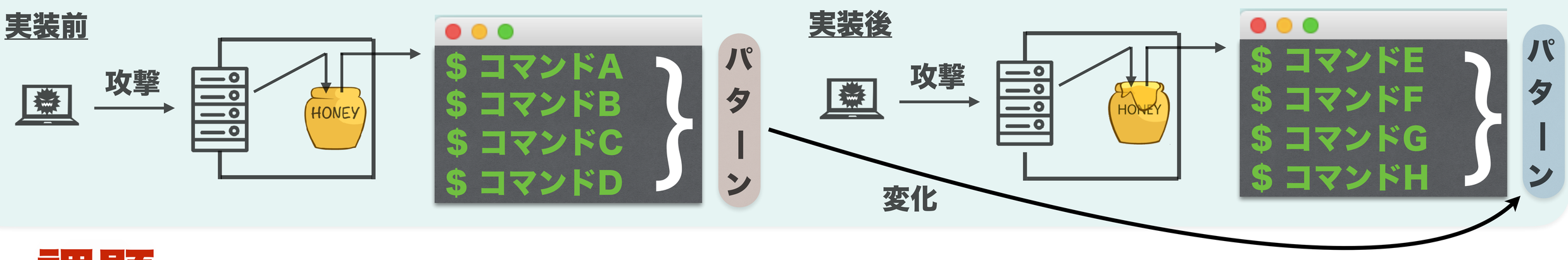
攻撃者の用いるコマンドでBusyBoxに含まれないものを低対話型に実装する

- BusyBox内のコマンド以外のものは侵入者特有である可能性がある

評価方法

Honeypotへの実装前と後でデータ収集を行い、シーケンシャルな攻撃ログの比較を行う

- 侵入され接続を切断するまでの間、入力されたコマンドのパターンデータをシーケンシャルに読み込んで比べる
- 以前の研究ではデータ収集において、Honeypotに未実装のコマンドを実装し* 侵入者の挙動の変化を観測した
(*実装したコマンド…ifconfig, netstat, free, service, echo, uname, which ping)



課題

- 実装コマンドの限界(出来ることとそうでないことの区別)
- 評価におけるシーケンシャルな攻撃ログの比較をどのように行うか(アルゴリズムの選定)