The Cabin in the Internet

～操作者の観測～

"The Cabin in the Woods"(2012)
Directed by Drew Goddard

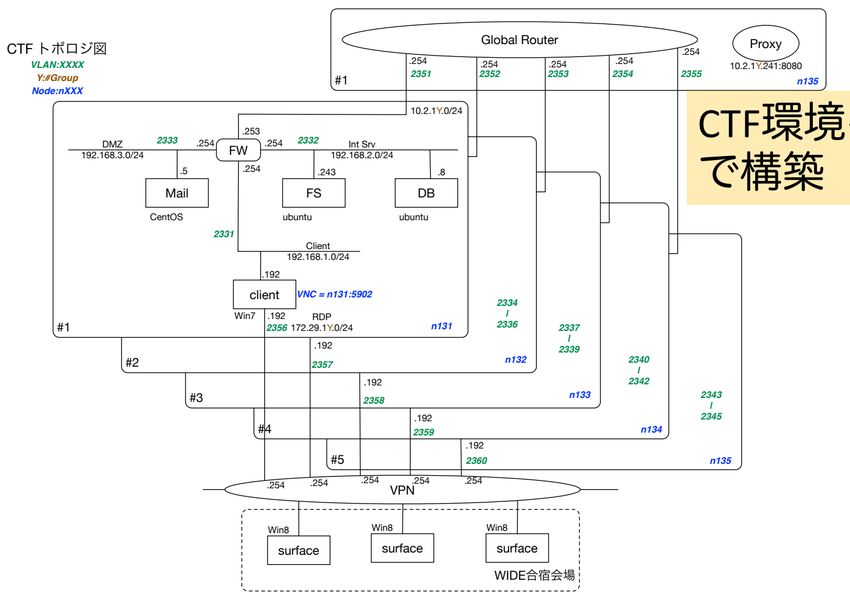
太田 悟史、安田 真悟　国立研究開発法人 情報通信研究機構
サイバー攻撃対策総合研究センター サイバー攻撃検証研究室

目的

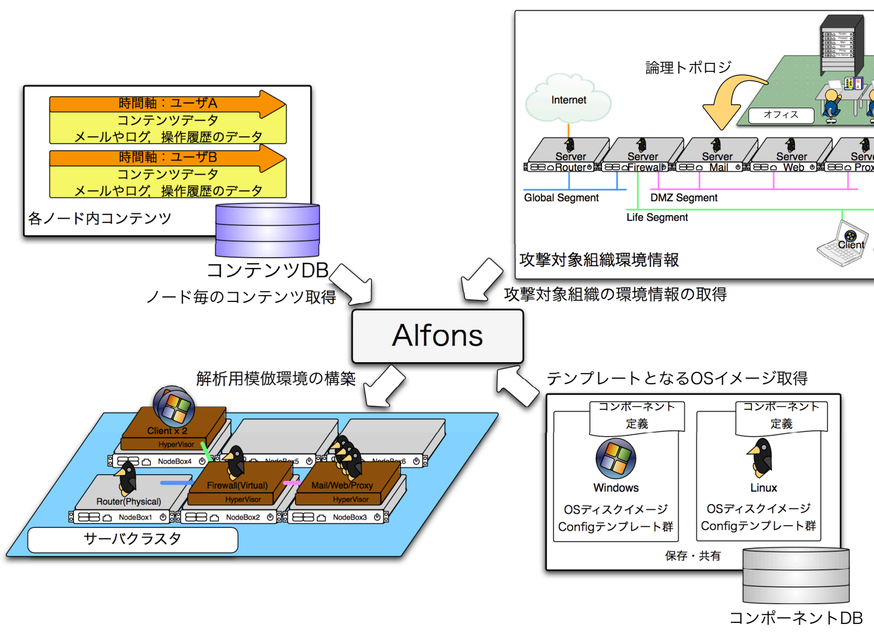
サイバー攻撃により、侵入されてしまった端末や奪取されてしまったユーザーアカウントなどを用いた“攻撃活動”を検知できれば、被害範囲を抑えられる。
攻撃活動を検知するためには、多くの攻撃活動を通じて、その特徴を得る必要がある。
本研究では、活動対象となる被害環境の構築と、挙動の観測について検討する。

CTFによる観測

「目的となる情報を探索する」という意味では、サーバー内のデータ取得を目的としたCTF（Capture the Flag）での参加者の挙動は疑似的な攻撃者として扱える。



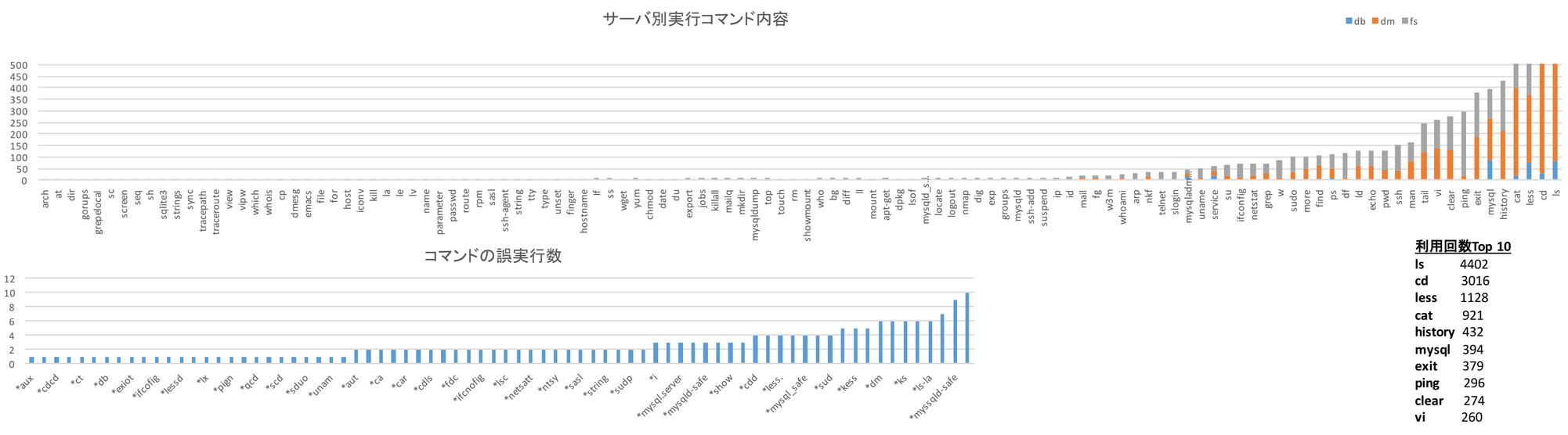
CTF環境をStarBEDで構築



環境の構築

被害環境をCTF参加者毎に構築していた。
雛形環境を元に、“Alfons”を用いて、ネットワークを含めた構築を実施。Alfonsは設定ファイルを別途配布できるため、複数の被害環境を容易に構築できる。

結果(全参加者の実行コマンド)



利用回数Top 10

ls	4402
cd	3016
less	1128
cat	921
history	432
mysql	394
exit	379
ping	296
clear	274
vi	260

Future work

- 他挙動データ(通常運用時のコマンド内容、リアルな攻撃内容）との比較
- 観測機能の検討： キーロガー(現状)の他に、hypervisor での取得やパケットのDPI
- 被害環境の多様化
- 観測途中での、動的な被害環境の変更

国立研究開発法人 情報通信研究機構
サイバー攻撃対策総合研究センター
StarBED