欺瞞を用いた能動的サイバー攻撃防御手法の提案と実装

A proposal and implementation of deception-based active cyber defense method

山田　大・システム分科会・情報セキュリティ大学院大学

Abstract: It has been difficult to prevent all of the increasingly targeted attacks known as advanced persistent threat called APT, so that we must assume that the attacker has been already inside our information system. The aim of this study is to establish a basis for deceptive approaches to APT to fail cyber attacks when targeted and to avoid being targeted. In this thesis, we model them, propose and implement deceptive methods in the reconnaissance stage including after intrusion into the organization network, evaluate its performance and show its effectiveness.

1. 背景と目的

標的型攻撃ヤバい！

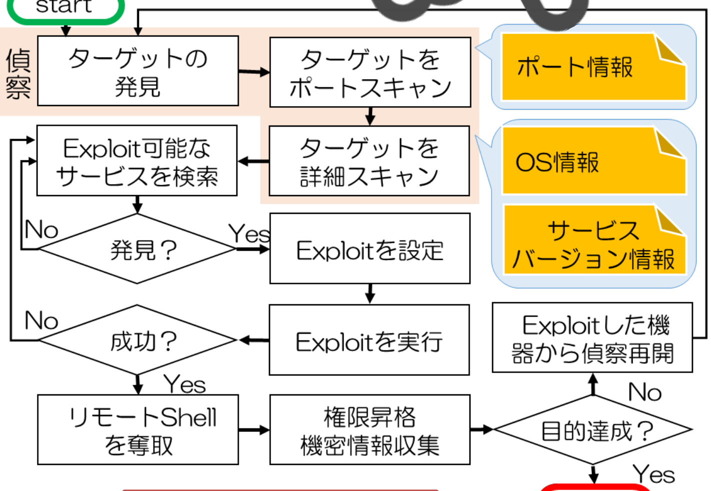
でも防げん。。。せやっ！

嫌がらせしたろ(`･ω･´)

2. 提案

ニセの偵察情報をつかませたれ！

- ポート情報
- OS情報
- サービス情報



start

偵察

ターゲットの発見

ターゲットをポートスキャン

ポート情報

Exploit可能なサービスを検索

ターゲットを詳細スキャン

OS情報

No 発見？ Yes

Exploitを設定

サービスバージョン情報

No 成功？

Exploitを実行

Exploitした機器から偵察再開

Yes

リモートShellを奪取

権限昇格 機密情報収集

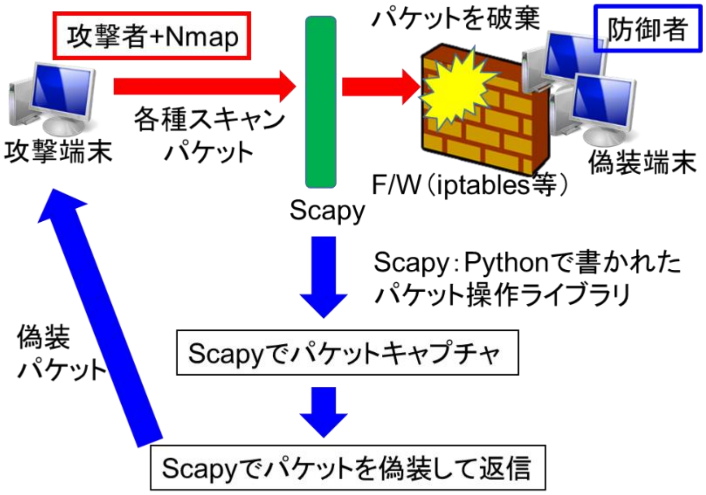
No 目的達成？ Yes

end

標的型攻撃フロー

一番有名な偵察ツールはNmapやから、とりあえずお前からな！

3. 実装概要



攻撃者+Nmap

攻撃端末

各種スキャンパケット

Scapy

パケットを破棄

防御者

F/W（iptables等）

偽装端末

偽装パケット

Scapy：Pythonで書かれたパケット操作ライブラリ

Scapyでパケットキャプチャ

Scapyでパケットを偽装して返信

4. 結果

5. 評価

早い！　遅延小さいよ！

安い！　Pythonはタダ！

（成果物がタダとは言っていない）

旨い！　簡単に嫌がらせできる！

三拍子！