



# 最新ポートスキャナ対策

**Fourteenforty Research Institute, Inc.**

株式会社 フォティーンフォティ技術研究所

<http://www.fourteenforty.jp>

取締役 技術担当 金居良治



# お題目

- ポートスキャンとは？
- Tarpit を利用した対策
- OpenBSD pf を利用した対策
- Fourteenforty が独自に考案した対策

## ポートスキャンとは？

- ターゲットサーバ上で、どのようなサービスが実行されているかを検出する技術
- 脆弱性検出の基本的な手法で、脆弱性管理には必須のテクニック
- したがって、攻撃にも使用される技術
- nmap でスキャンした例

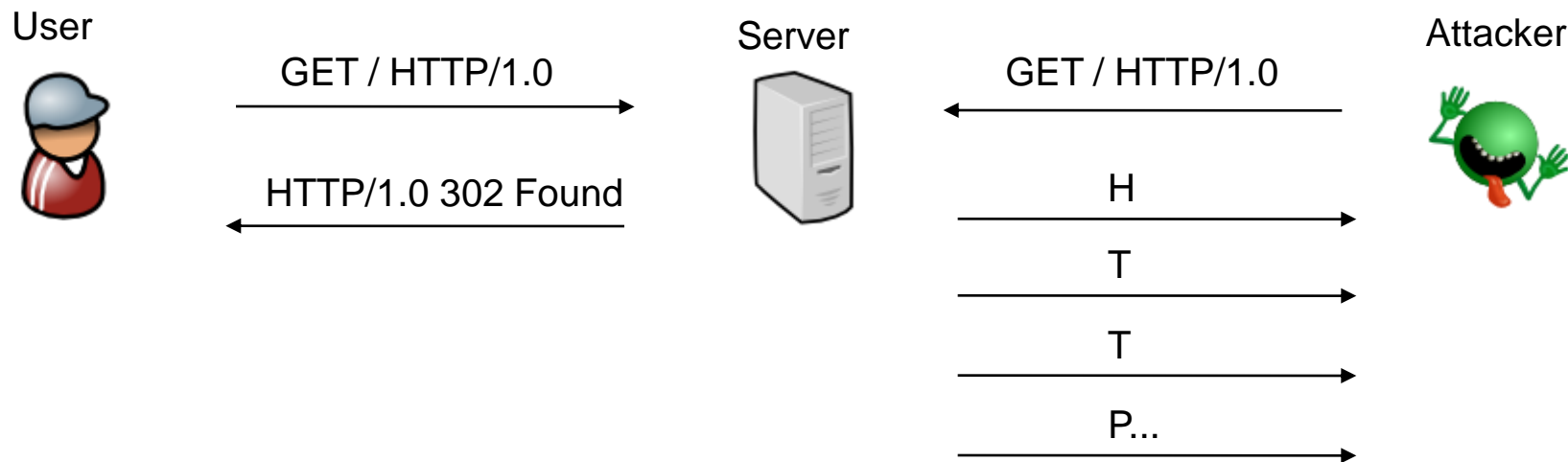
```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.3.0-dev ((Unix))
```

# Tarpit

- スキャンを遅らせ、スキャンにかかるコストを増加させる
- Spam 対策の spam tarpit は有名
- ネットワーク経由で広まるウイルスの伝搬速度を低下させることができる
- ipfilter (LinuxのFirewall), LaBrea

# Tarpit の実装 (アプリケーションレベル)

- アプリケーションレベルで遅延させる(プロトコル検出を遅延させる)
- sendmail 等々で同様の機能あり



## Tarpit の実装 (Layer 2, 3)

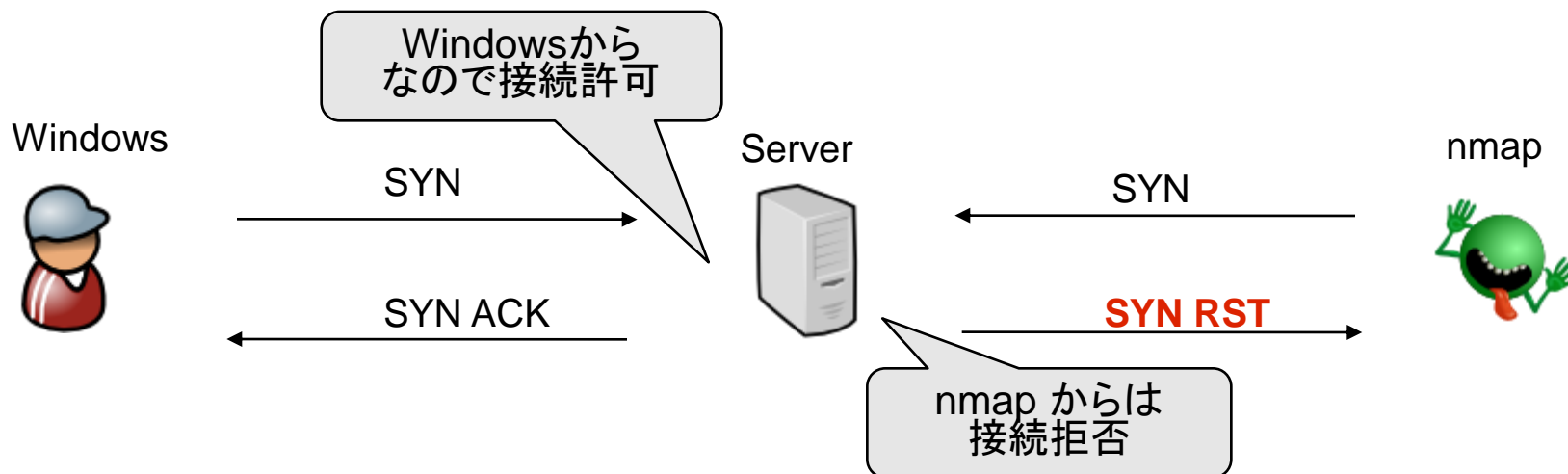
- TCP Window サイズを 0 にする  
→ プロトコル検出を遅延させる
  
- 存在しない IP アドレスへの arp/icmp/SYN scan に答える  
→ 存在しない IP へのポートスキャンやプロトコル検出はことごとくタイムアウトする

## OpenBSD pf

- OpenBSD なた達が作っているファイアウォール
- {Free,Net,Open}BSD で使える
- Windows にも移植されている (機能限定版)
- p0f という機能を使ってスキャナー対策が可能

# OpenBSD pf - p0f について

- Passive Os Fingerprinting (受動的OS検出)
- SYN パケットの IP オプションやTTL等の特徴的パターンから接続元のOSを特定する
- Fingerprint ファイルが必要



## Fourteenforty 独自の SYN スキャン対策

- SYN ACK や SYN RST のパケットを強制的に IP フラグメントに分割する
- IP フラグメントは、巨大なデータの分割送信を行う仕組み
- nmap 等のすべての SYN スキャナはフラグメントの再構成に対応していない
- 通常の TCP/IP スタックには影響を与えずに、ポートスキャンだけ出来なくなる
- しかも、Fingerprint ファイルが不要！

## 強制フラグメント方式の実装

- OpenBSD pf のルールの一部として実装
- ファイアウォールのルールと一緒にして、非常に柔軟な設定が可能

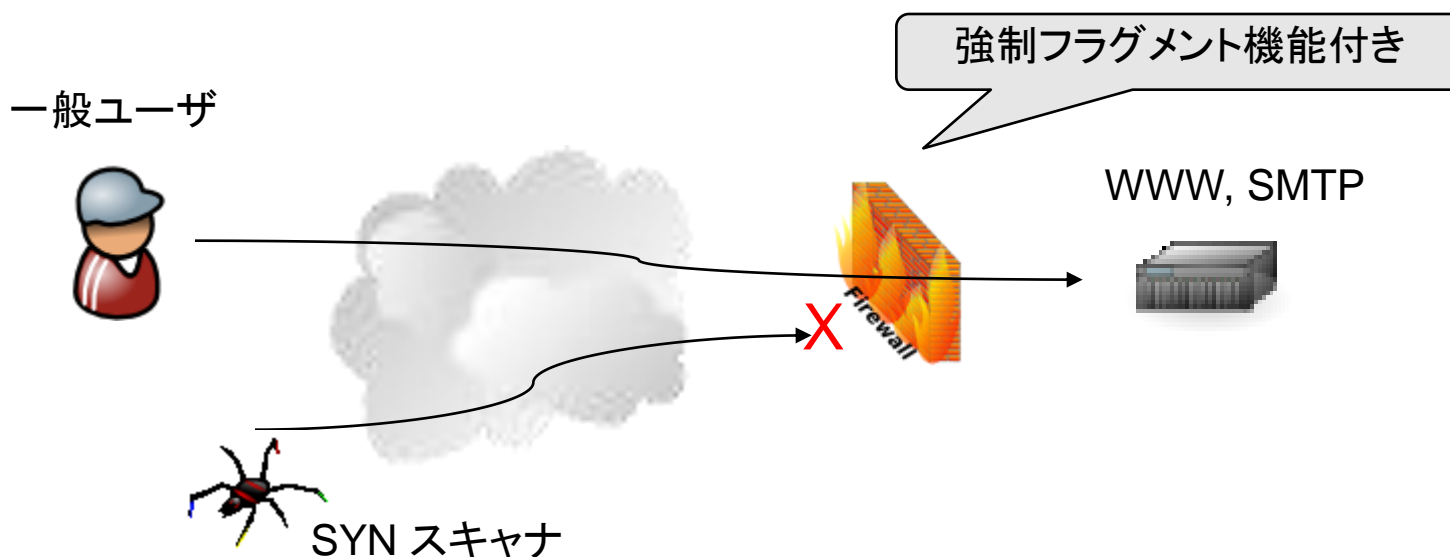
```
pass out inet proto tcp from any port 80 to any flags SA/SA forcefrag  
pass out inet proto tcp from any port 80 to any flags RA/RA forcefrag
```

→ port 80 への接続について強制フラグメントを有効にする

- nmap で SYN スキャンが出来なくなる事を確認

# 強制フラグメント方式の構成例

- ファイアウォールとして利用する場合



## 結論

- ポートスキャナ対策をご紹介
- 今まで無理だと思われていた SYN スキャン対策を Fourteenforty で考案
- これにより、攻撃にかかるコストを増加させる事が可能となる

ありがとうございました



**Fourteenforty Research Institute, Inc.**

株式会社 フォティーンフォティ技術研究所

<http://www.fourteenforty.jp>

取締役 技術担当 金居良治

[kanai@fourteenforty.jp](mailto:kanai@fourteenforty.jp)