

攻撃を「隠す」、 攻撃から「隠れる」

2015/08/29
すみだセキュリティ勉強会
@ozuma5119



@ozuma5119

- セキュリティっぽいITエンジニア(pentester)
- Blog : ろば電子が詰まっている
 - <http://d.hatena.ne.jp/ozuma/>
- 科学写真家(と名乗っている)



Agenda.

- **第1部 攻撃者視点：攻撃を「隠す」**
 - 隠密ポートスキャン(nmap)
- **第2部 防御側視点：攻撃から「隠れる」**
 - 科学忍法・ssh分身の術



第一部

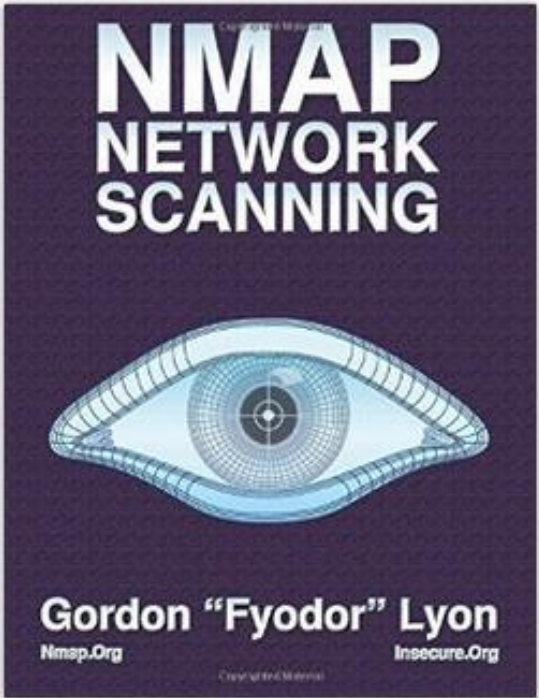
攻撃を「隠す」

隠密ポートスキャン(nmap)

ポートスキャナ - nmap

Amazon.co.jp: NMap Networ... x +

www.amazon.co.jp/NMap-Netwo 検索



NMap Network Scanning: Official NMap Project Guide to Network Discovery and Security Scanning (英語) ペーパーバック - 2012/10/23

Gordon Lyon (著)

★★★★★ 1件のカスタマーレビュー

すべてのフォーマットおよびエディションを表示する

ペーパーバック
¥ 6,351

¥ 8,282 より 4 中古品の出品
¥ 6,083 より 9 新品

NMap Network Scanning: Official NMap Project Guide to Network Discovery and Security Scanning

- Pen Test
- Basics
- More

Security Tools

- Password audit
- Sniffers
- Vuln scanners
- Web scanners
- Wireless
- Exploitation
- Packet crafters
- More

Site News

Advertising

About/Contact

Site Search

Sponsors:

Would you hand
over the keys to
your network?

Learn more



GFI LanGuard

Nmap Network Scanning

Nmap リファレンスガイド (Man Page)



Nmap リファレンスガイド (Man Page)

Table of Contents

[ツール説明](#)

[オプション概要](#)

[ターゲットの指定](#)

[ホストの発見](#)

[ポートスキャンの基本](#)

[ポートスキャンのテクニック](#)

[ポートの指定とスキャンの順序](#)

[サービスとバージョンの検出](#)

[OS 検出](#)

[タイミングとパフォーマンス](#)

[ファイアウォール/IDS の回避とスプーフィング](#)

[出力](#)

[その他のオプション](#)

[実行時の対話型操作](#)

[使用例](#)

[バグ](#)

[作者](#)

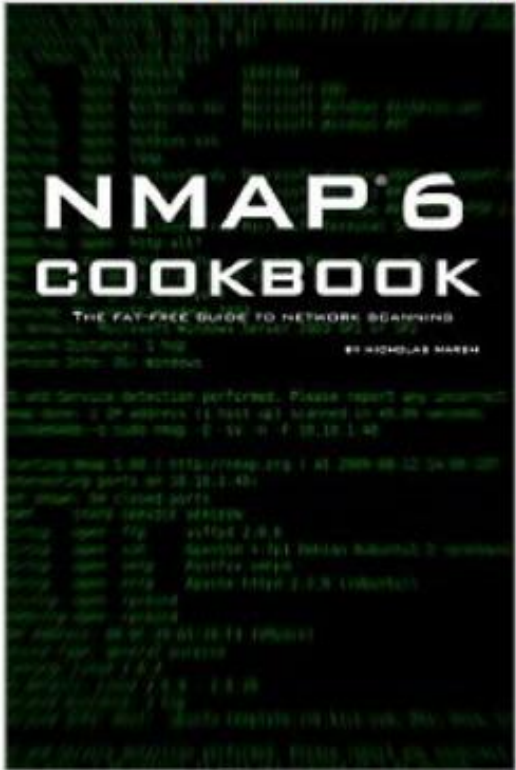
[法的な注意事項](#)

ファイル(F) 編集(E) 表示(V) 履歴(S) ブックマーク(B) ツール(T) ヘルプ(H)

Amazon.co.jp: Nmap 6 Cook... x +

www.amazon.co.jp/Nmap-Cookbook-F... 検索

なか見!検索↓




Nmap 6 Cookbook: The Fat-Free Guide to Network Security Scanning (English Edition) [Kindle版]


[Nicholas Marsh](#) (著)

★★★★☆ (1件のカスタマーレビュー)

Kindle 購入価格: ￥593

プライム会員: ￥0 (Kindle 端末上のストアから、無料でお読みいただけます) 

販売: [Amazon Services International, Inc.](#)

- **Amazon Whispernet** 経由の無料ワイヤレス配信を含む
- 紙の本の長さ: 227ページ (実ページ番号を含む) 
- 言語: 英語
- プライム会員の方は、Kindleオーナー ライブラリーを利用するとこの本を無料でお読みいただけます。Kindleオーナー ライブラリーは、KindleまたはFireタブレット 端末からのみ利用手続きができます。

Nmap 6 Cookbook: The Fat-Free Guide to Network Security Scanning (English Edition)

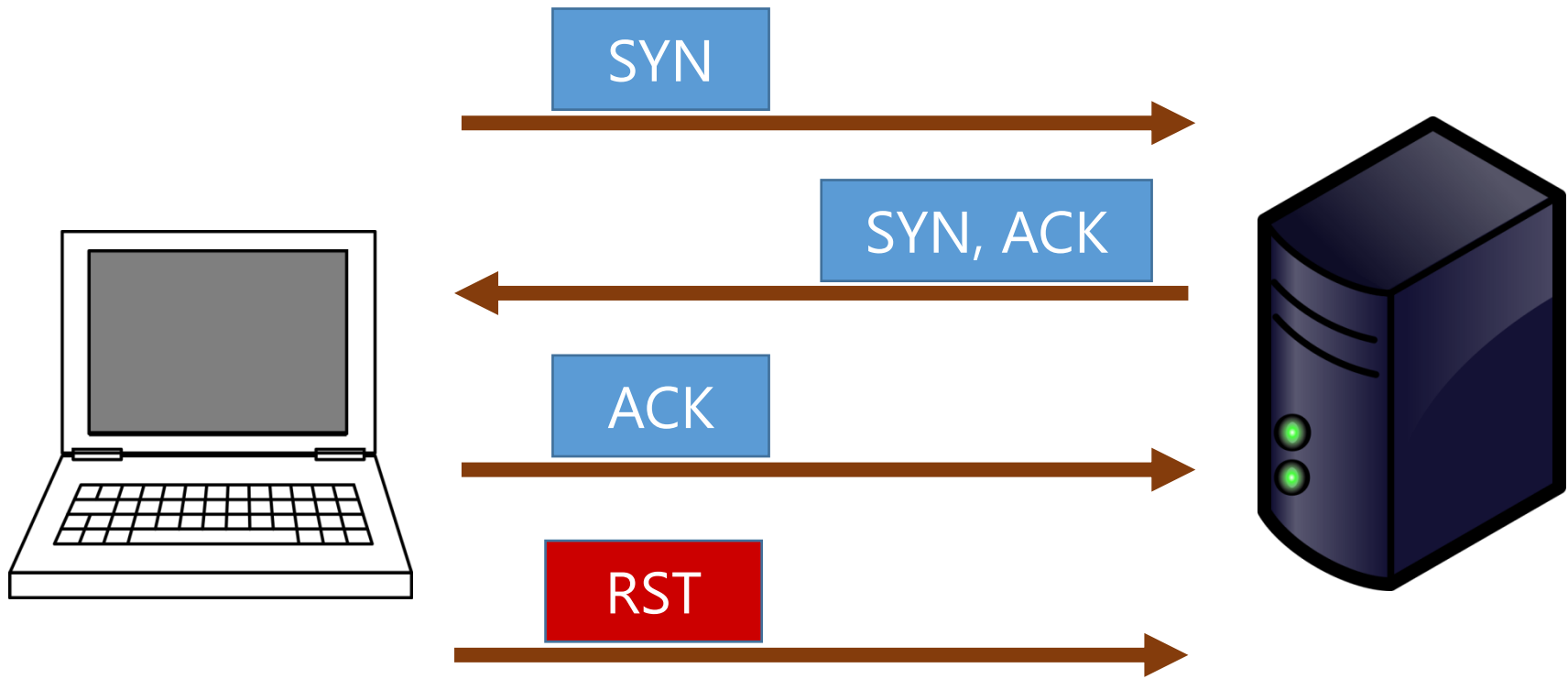
stealth scan



TCP connect() scan

```
# nmap -sT <ipaddr>
```

もしくはWebブラウザなどで直接見てみる

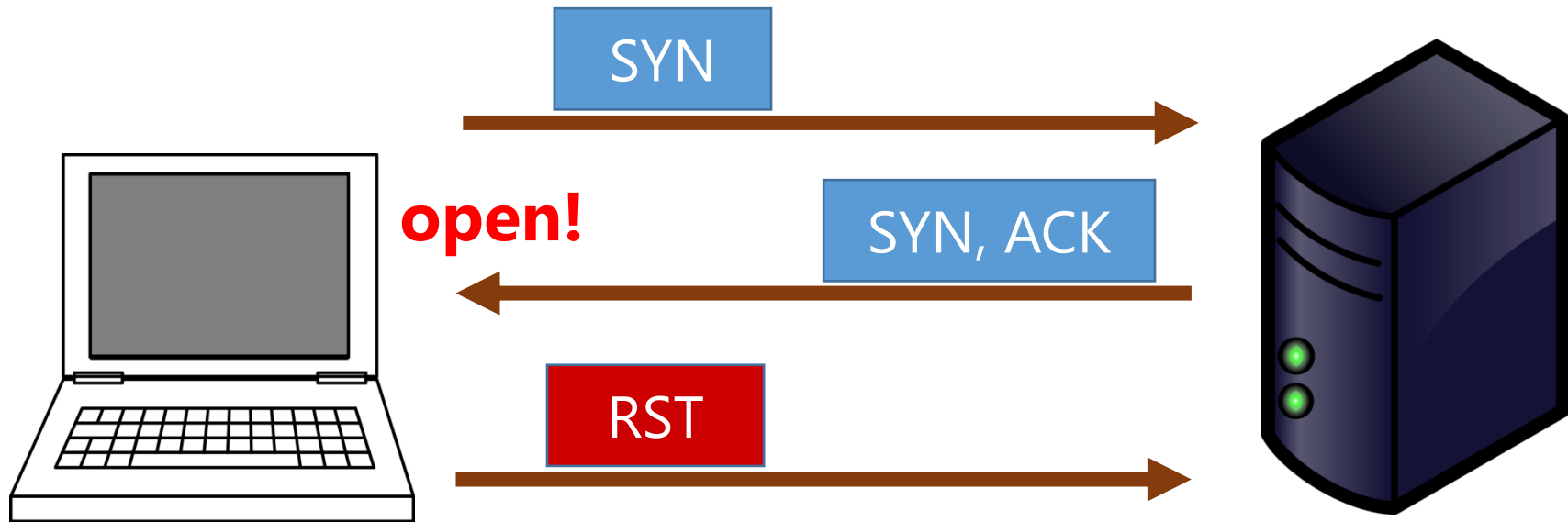


SYN scan (stealth scan)

```
# nmap -sS <ipaddr>
```

OR

```
# nmap <ipaddr>
```



don't establish 3-way handshake



```
ip.addr == 192.168.2.66 && tcp.port == 80
```

No.	Time	Source	Destination	Protocol	Info
5	...	192.168.2.66	192.168.2.1	TCP	37294→80 [SYN] Seq=0 Win=1024 Len=0
7	...	192.168.2.1	192.168.2.66	TCP	80→37294 [SYN, ACK] Seq=0 Ack=1 Len=0
8	...	192.168.2.66	192.168.2.1	TCP	37294→80 [RST] Seq=1 Win=0 Len=0

SYNスキャンは、 何を「隠して」いるのか

- 通常の手順(3WAYハンドシェイク)を介さないで、
 - **ログに残るのを隠す**
 - 「プロトコル通りに動いている」ことを前提とした検知から攻撃を隠す
- 行為自体を隠しているわけではない

Too slow to detect.



“Too Slow” means...

- ポートスキャンをゆっくり行くと、攻撃行為自体を隠すことができる
- nmapではdelayやtimeoutを細かく設定できるが、タイミングテンプレート(-T)を使うと楽

nmapの-Tオプション (タイミングテンプレート)

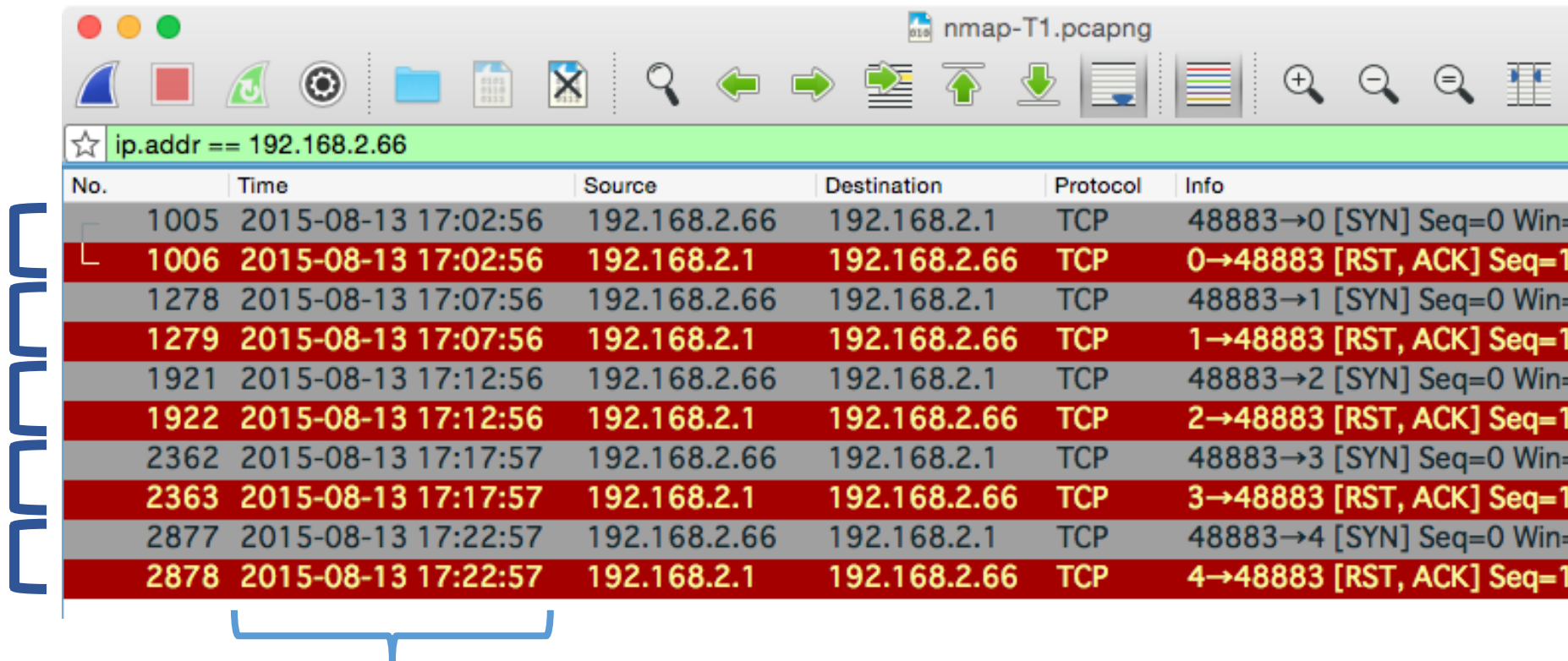
ゆっくり



早い

オプション	テンプレート名
-T0	paranoid (偏執スキャン)
-T1	sneaky (こそこそスキャン)
-T2	polite (丁寧スキャン)
-T3	normal (標準スキャン)
-T4	aggressive (イケイケスキャン)
-T5	insane (キ○ガイ スキャン)

nmap -T0 がどれだけ遅いか？



No.	Time	Source	Destination	Protocol	Info
1005	2015-08-13 17:02:56	192.168.2.66	192.168.2.1	TCP	48883→0 [SYN] Seq=0 Win=
1006	2015-08-13 17:02:56	192.168.2.1	192.168.2.66	TCP	0→48883 [RST, ACK] Seq=1
1278	2015-08-13 17:07:56	192.168.2.66	192.168.2.1	TCP	48883→1 [SYN] Seq=0 Win=
1279	2015-08-13 17:07:56	192.168.2.1	192.168.2.66	TCP	1→48883 [RST, ACK] Seq=1
1921	2015-08-13 17:12:56	192.168.2.66	192.168.2.1	TCP	48883→2 [SYN] Seq=0 Win=
1922	2015-08-13 17:12:56	192.168.2.1	192.168.2.66	TCP	2→48883 [RST, ACK] Seq=1
2362	2015-08-13 17:17:57	192.168.2.66	192.168.2.1	TCP	48883→3 [SYN] Seq=0 Win=
2363	2015-08-13 17:17:57	192.168.2.1	192.168.2.66	TCP	3→48883 [RST, ACK] Seq=1
2877	2015-08-13 17:22:57	192.168.2.66	192.168.2.1	TCP	48883→4 [SYN] Seq=0 Win=
2878	2015-08-13 17:22:57	192.168.2.1	192.168.2.66	TCP	4→48883 [RST, ACK] Seq=1

1つのTCPポートをスキャンするのに5分

Threshold (閾値)

- 侵入検知システムでは、Threshold以上の事象を「検知」としてアラート
 - これはインターネットに限った話ではない。敏感すぎる防犯センサなど...
- そしてThreshold以下の事象は、
「存在しない」

[illegible]

Minimize the number
of ports to scan.



よくある上位10ポートのみスキャン

```
# nmap -n --top-ports 10 192.168.2.66
```

```
.....(省略).....
```

```
Host is up (0.00029s
```

--top-ports <number>

PORT	STATE	SERVICE
------	-------	---------

21/tcp	open	ftp
--------	------	-----

22/tcp	open	ssh
--------	------	-----

23/tcp	closed	telnet
--------	--------	--------

25/tcp	closed	smtp
--------	--------	------

80/tcp	open	http
--------	------	------

110/tcp	closed	pop3
---------	--------	------

139/tcp	closed	netbios-ssn
---------	--------	-------------

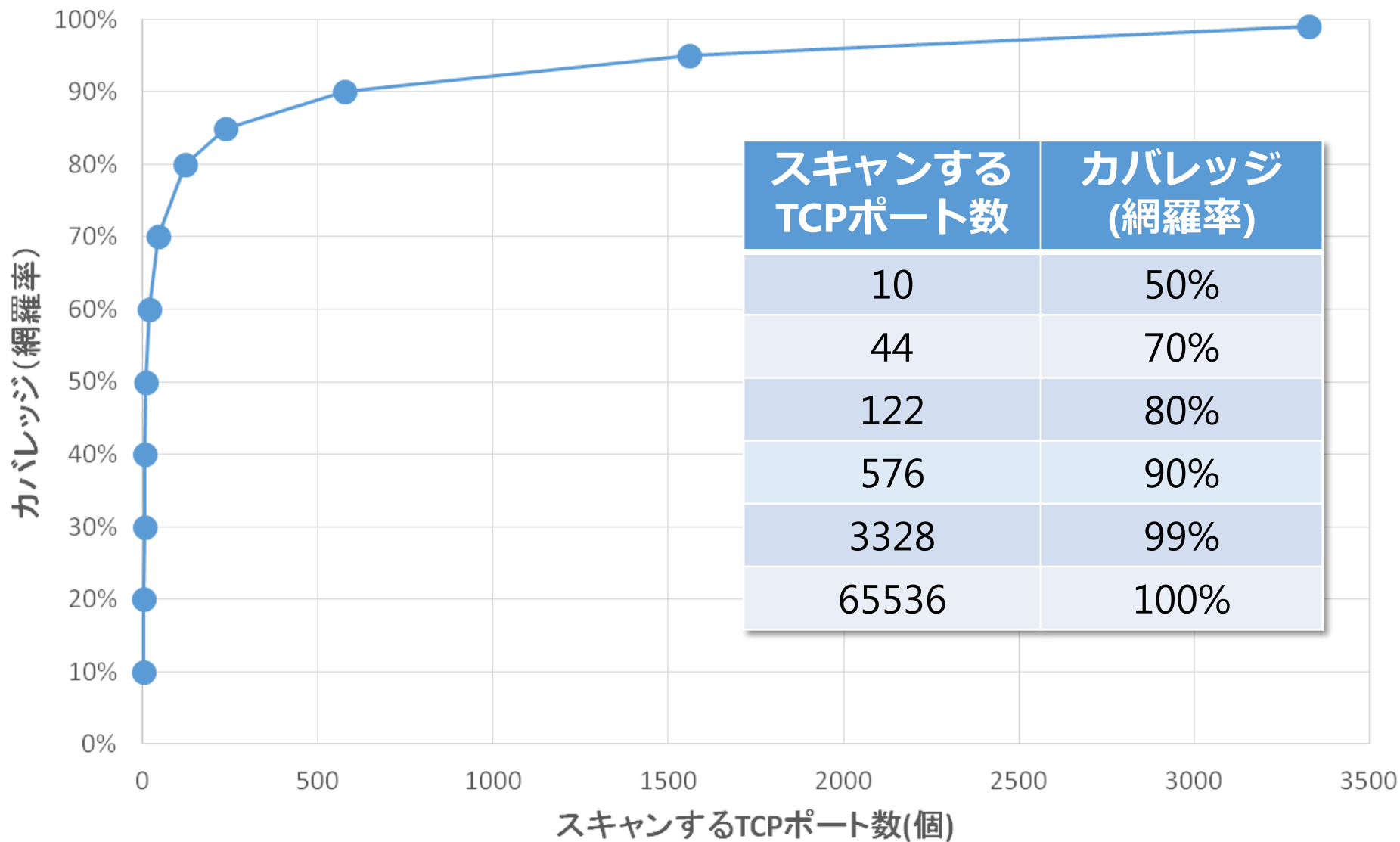
443/tcp	open	https
---------	------	-------

445/tcp	closed	microsoft-ds
---------	--------	--------------

3389/tcp	closed	ms-wbt-server
----------	--------	---------------

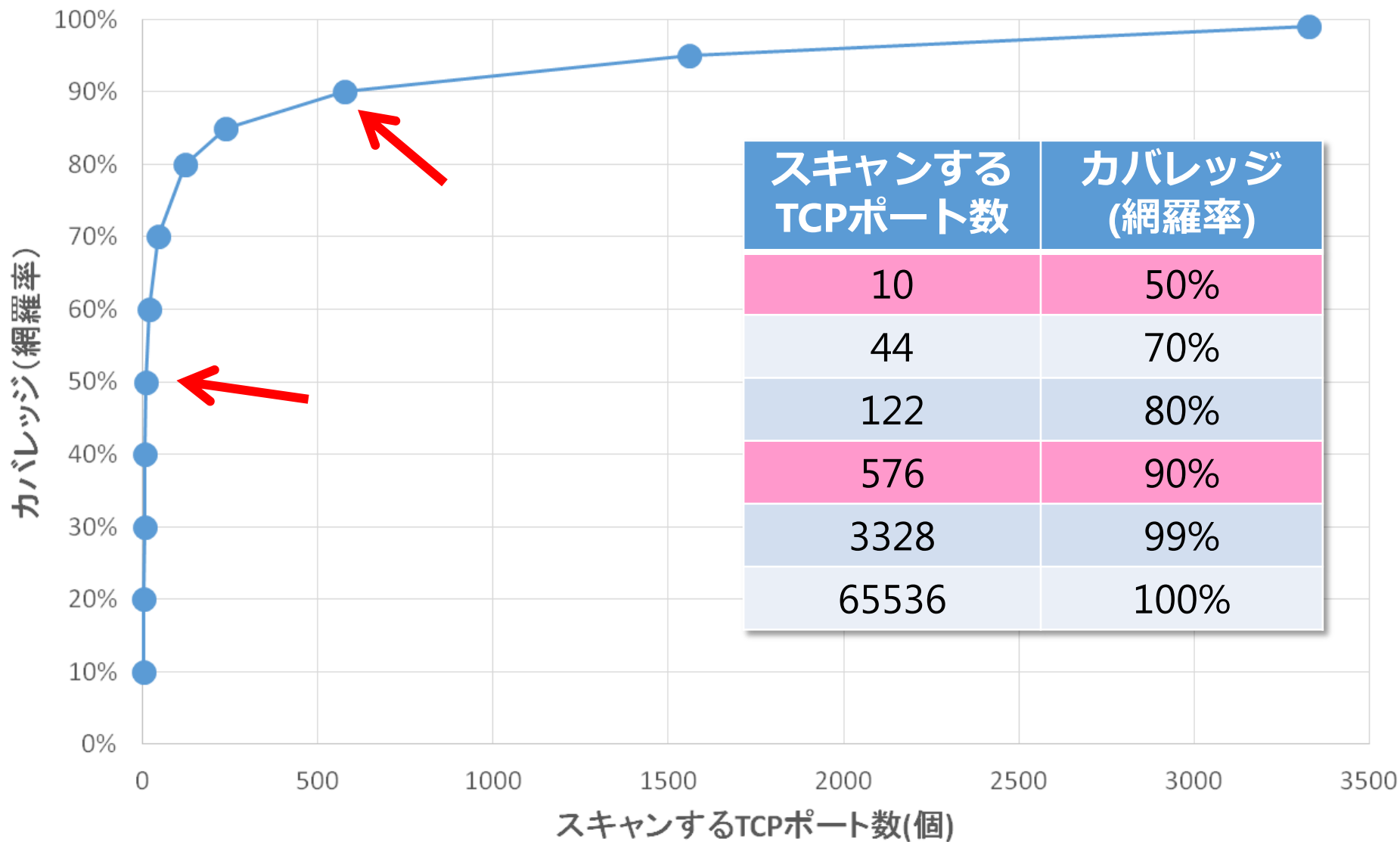
```
MAC Address: 00:0C:29:59:63:7E (VMware)
```

--top-portsオプションでスキャンするTCPポート数と、カバレッジ(網羅率)



「NMAP NETWORK SCANNING」, Gordon "Fyodor" Lyon (2008) より引用

--top-portsオプションでスキャンするTCPポート数と、カバレッジ(網羅率)



「NMAP NETWORK SCANNING」, Gordon "Fyodor" Lyon (2008) より引用

さらなる隠密スキャン

- キーワードだけ紹介
 - TCP Idle Scan (-sI)
 - FTPバウンススキャン (-b) [古典]
 - デコイ(囧) (-D)
 - MACアドレス偽装 (--spoof-mac)



第二部

ポートスキャンから
隠れる

科学忍法・ssh分身の術

Religious War: SSH 22/tcp

To change, or not to change
... that is the question.



sshd shouldn't use 22/tcp?

• 変えるべき派

- 攻撃されにくい。攻撃対象として選定されにくい（正当派）
- 攻撃ログが劇的に減るからやった方が
良い（ピンポンダッシュ嫌だよ派）
- 多くのドキュメントで変えることが推
奨されているから、変えたほうがいい
(流され派)

sshd shouldn't use 22/tcp?

• 変えても意味ないよ派

- ポートスキャンすれば一発でsshのポートは分かるんだからムダだよ
- ポートを変えるだけでセキュリティ対策しているつもりになっちゃうからダメだよ(?)

sshd shouldn't use 22/tcp?

- 変えても意味ないよ派

- ポートスキャンすれば一発でsshのポートは分かるんだからムダだよ
- ポートを変えるだけでセキュリティ対策しているつもりになっちゃうからダメだよ(?)

プリンタポートで
つかまえて



```
# nmap -n -sV -p1-65535 192.168.2.66
....(snip)....
PORT      STATE SERVICE      VERSION
9097/tcp  open  ssh          OpenSSH 5.3 (protoco
```

↓見えてないぞ!!!!!!

```
# nmap -n -sV -p1-65535 192.168.2.66
....(snip)....
PORT      STATE SERVICE      VERSION
9100/tcp  open  jetdirect?   Excluded from versio
```

Nmap Reference Guide

--allports (Don't exclude any ports from version detection)

By default, Nmap **version detection skips TCP port 9100** because some printers simply print anything sent to that port,(snip)....

<https://nmap.org/book/man-version-detection.html>

```
# nmap -n -sV -p1-65535 --allports 192.168.2.60
PORT      STATE SERVICE VERSION
9100/tcp  open  ssh      OpenSSH 5.3 (protocol 2)
```

見えた!!!!!!

デバイス (4) ———— プリンターと FAX (4) ———— 未指定 (1) ————
EV2336W EPSON LP-S230DW-000000 USB HS SERIAL CONVERTER

MAGNATE
PFU-65 USB Keyboard
USB Optical Mouse

EPSON LP-S230DW-000000のプロパティ

全 | 標準 TCP/IP ポート モニターの構成 | X

ポートの設定

ポート名(P): NtwkPort00

プリンター名または IP アドレス(A): 192.168.2. [REDACTED]

プロトコル

☒ Raw(R) ☐ LPR(L)

Raw 設定

ポート番号(N): 9100

LPR 設定

キュー名(Q): lp

☐ LPR バイト カウントを有効にする(B)

- sshd(は9100-9107/tcpへ隠すと見
つかりにくい (気がするよ)

科学忍法・ssh分身の術



```
# nmap -sV -p0-65535 192.168.2.66
```



Version Detection Scan

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2200/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)

nmap -sV -p0-65535 192.168.2.66

2203/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2204/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2205/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2206/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2207/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2208/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2209/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2210/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2211/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2212/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2213/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2214/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2215/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2200/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)

nmap -sV -p0-65535 192.168.2.66

2203/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2204/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2205/tcp			
2206/tcp			
2207/tcp			
2208/tcp			
2209/tcp			
2210/tcp			
2211/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2212/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2213/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2214/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2215/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)

2233/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2234/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2235/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)

```
# nmap -sV -p0-65535 192.168.2.66
```

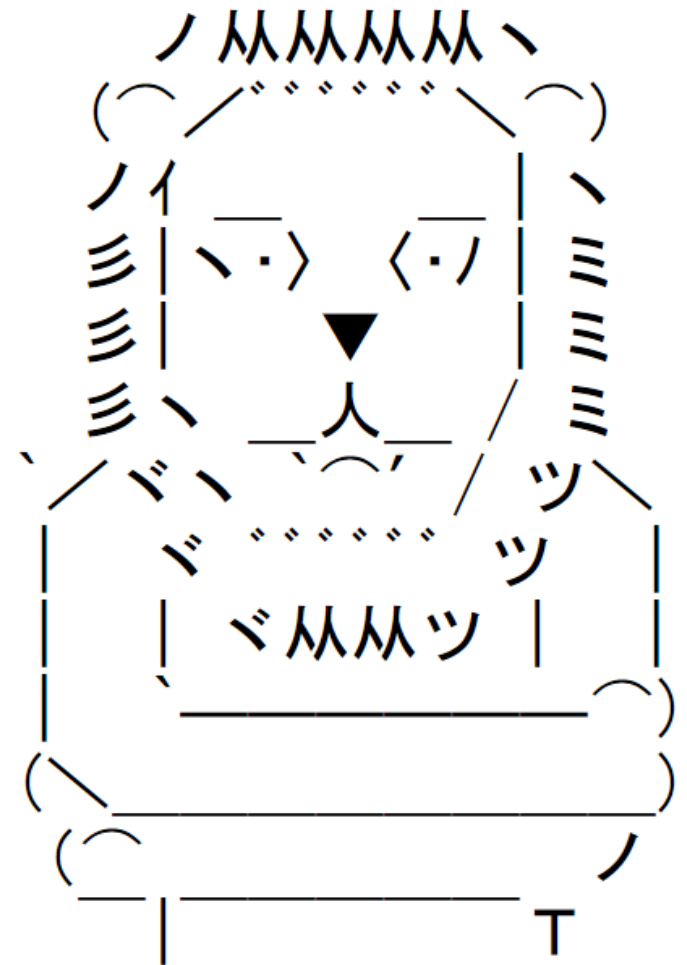
2238/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2239/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2240/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2241/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2242/tcp	open		
2243/tcp	open		
2244/tcp	open		

本物は 2245/tcp

2245/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2246/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2247/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2248/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2249/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2250/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)

「ポートスキャンすれば一発でsshのポートは分かるんだからムダだよ」

お前それサバンナでも
同じ事言えんの？



Decoy (囃)

- "Decoys are **fake** military equipment that are intended to **deceive** the enemy."
 - Wikipedia [Decoy] より引用



フレア：
赤外線誘導ミサイルへのデコイ

3 Missions of Decoy

- saturation – 飽和
- seduction – 誘惑
- detection – 露見

David L. Adamy "Electronic Warfare Against a New Generation of Threats"
<http://www.amazon.com/dp/1608078698>

PORT	STATE	SERVICE	VERSION
22/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2200/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2201/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2202/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2203/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2204/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2205/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2206/tcp	open	ssh	
2207/tcp	open	ssh	
2208/tcp	open	ssh	
2209/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2210/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2211/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2212/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2213/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2214/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2215/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)

偽のssh開放ポート：
ポートスキャナへのデコイ

3 Missions of Decoy

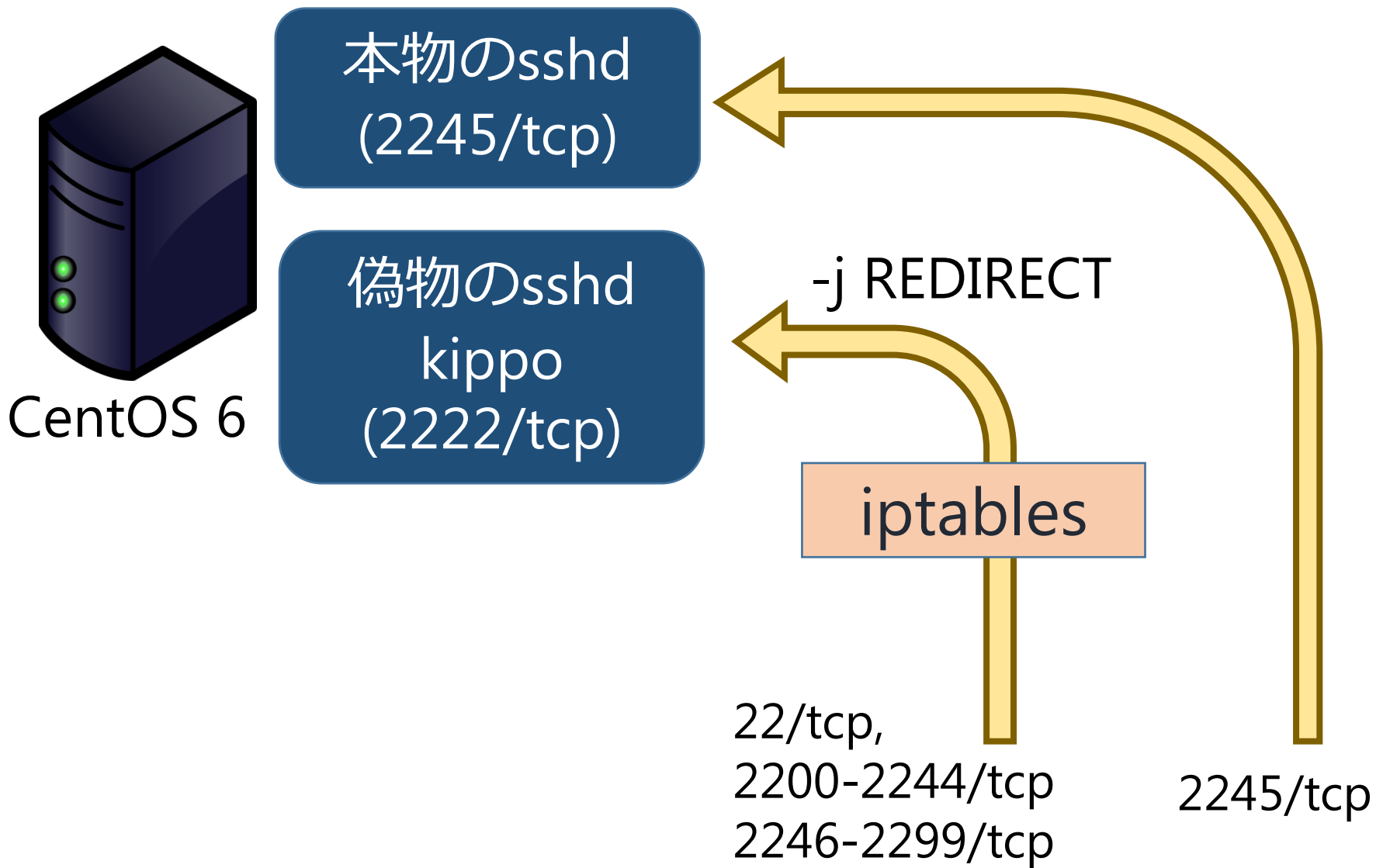
- **saturation – 飽和**
- seduction – 誘惑
- detection – 露見

反論：防御になっていない？

- 遅延装置は、鍵をかけたドアと同じ
 - 破られない錠前は無いが、侵入を遅らせることはできる
- 十分な遅延効果があれば、攻撃を検知してブロックするまでの時間も十分に取ることができる

ガッチャマンの つくりかた





偽物のsshd - kippo

- **kippo** : sshハニーポット
 - sshサーバとして振る舞い、様々なデータ取得が可能
 - 今回は単なるダミーsshdとして利用
 - blog: sshハニーポットをkippoで作ってみる
 - <http://d.hatena.ne.jp/ozuma/20130829/1377703104>

本物のsshd(2245/tcp)以外は、偽物のsshd(kippo; 2222/tcp)へ

```
# iptables -A PREROUTING -t nat -i eth0 -p tcp --  
dport 2200:2244 -j REDIRECT --to-ports 2222  
# iptables -A PREROUTING -t nat -i eth0 -p tcp --  
dport 2246:2299 -j REDIRECT --to-ports 2222
```

- ループは発生しないため、2222/tcpの特別扱いは不要。
※2222/tcpを2222/tcpへ-j REDIRECTしてもだいじょうぶ

kippo.cfgでバナー設定

```
ssh_version_string = SSH-2.0-OpenSSH_5.3
```

PORT	STATE	SERVICE	VERSION
2242/tcp	open	ssh	OpenSSH 5.1p1 Debian 5 (proto
2243/tcp	open	ssh	OpenSSH 5.1p1 Debian 5 (proto
2244/tcp	open	ssh	OpenSSH 5.1p1 Debian 5 (proto
2245/tcp	open	ssh	OpenSSH 5.3 (protocol 2.0)
2246/tcp	open	ssh	OpenSSH 5.1p1 Debian 5 (proto
2246/tcp	open	ssh	OpenSSH 5.1p1 Debian 5 (proto

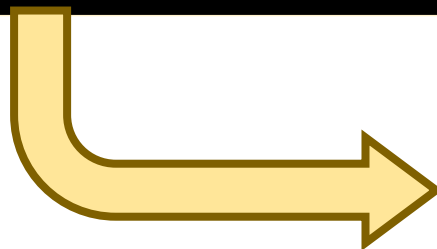
揃えないとすぐバレるぞ!!

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|_ 1024 bc:92:50:82:82:bc:d0:ab:b8:a2:6f:34:bb:f7:fd:bd (DSA)
|_ 2048 ea:63:6a:de:44:98:c3:c9:35:88:d7:e9:81:cc:f7:47 (RSA)
2200/tcp  open  ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|_ 1024 bc:92:50:82:82:bc:d0:ab:b8:a2:6f:34:bb:f7:fd:bd (DSA)
|_ 2048 ea:63:6a:de:44:98:c3:c9:35:88:d7:e9:81:cc:f7:47 (RSA)
2201/tcp  open  ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|_ 1024 bc:92:50:82:82:bc:d0:ab:b8:a2:6f:34:bb:f7:fd:bd (DSA)
|_ 2048 ea:63:6a:de:44:98:c3:c9:35:88:d7:e9:81:cc:f7:47 (RSA)
2202/tcp  open  ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|_ 1024 bc:92:50:82:82:bc:d0:ab:b8:a2:6f:34:bb:f7:fd:bd (DSA)
|_ 2048 ea:63:6a:de:44:98:c3:c9:35:88:d7:e9:81:cc:f7:47 (RSA)
2203/tcp  open  ssh      OpenSSH 5.3 (protocol 2.0)
| ssh-hostkey:
|_ 1024 bc:92:50:82:82:bc:d0:ab:b8:a2:6f:34:bb:f7:fd:bd (DSA)
|_ 2048 ea:63:6a:de:44:98:c3:c9:35:88:d7:e9:81:cc:f7:47 (RSA)
```

nmap -A でkey fingerprintが...

本物のkeyを、kippoのkeyとしてコピー?

```
/etc/ssh/ssh_host_dsa_key  
/etc/ssh/ssh_host_dsa_key.pub  
/etc/ssh/ssh_host_rsa_key  
/etc/ssh/ssh_host_rsa_key.pub
```



```
${kippodir}/data
```

もはや本末転倒だぞ!!

確かに区別が付かなくなった

```
# nmap -n -A -p0-65535 192.168.2.66
```

```
.....(省略).....
```

```
PORT      STATE SERVICE VERSION
```

```
.....(省略).....
```

```
2222/tcp open  ssh      OpenSSH 5.3 (protocol 2.0)
```

```
| ssh-hostkey:
```

```
|   1024 bc:92:50:82:82:bc:d0:ab:b8:a2:6f:34:bb:f7:fd
```

```
|_  2048 ea:63:6a:de:44:98:c3:c9:35:88:d7:e9:81:cc:f7
```

```
2245/tcp open  ssh      OpenSSH 5.3 (protocol 2.0)
```

```
| ssh-hostkey:
```

```
|   1024 bc:92:50:82:82:bc:d0:ab:b8:a2:6f:34:bb:f7:fd
```

```
|_  2048 ea:63:6a:de:44:98:c3:c9:35:88:d7:e9:81:cc:f7
```

TCP Intercept: Cisco ASA 5500





ASDM を使用した Cisco ASA 5500 シリーズ コンフィギュレーション ガイド ASA 5505、ASA 5510、ASA 5520、ASA 5540、ASA 5550、ASA 5580、ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、および ASA 5585-X 用ソフトウェア バージョン 8.4 および 8.6

接続の設定

- ASDM を使用した Cisco ASA 5500 シリーズ コンフィギュレーション ガイド ASA 5505、ASA 5510、ASA 5520、ASA 5540、ASA 5550、ASA 5580、ASA 5512-X、ASA 5515-X、ASA 5525-X、ASA 5545-X、ASA 5555-X、および ASA 5585-X 用ソフトウェア バージョン 8.4 および 8.6
- このマニュアルについて
- ASA の開始
 - Cisco ASA 5500 シリーズの概要
 - スタートアップ ガイド
 - ASDM ユーザ インター

発行日;2012/09/25 | [英語版ドキュメント](#)(2012/06/20 版) | [ダウンロード](#); [この章](#) , [ドキュメント全体](#) (PDF - 22ME

目次

接続の設定

[接続の設定に関する情報](#)

[TCP 代行受信および初期接続の制限](#)

[クライアントレス SSL 互換での管理パケットの TCP 代行受信](#)

[デッド接続検出 \(DCD\)](#)

[TCP シーケンスのランダム化](#)

[TCP の正規化](#)

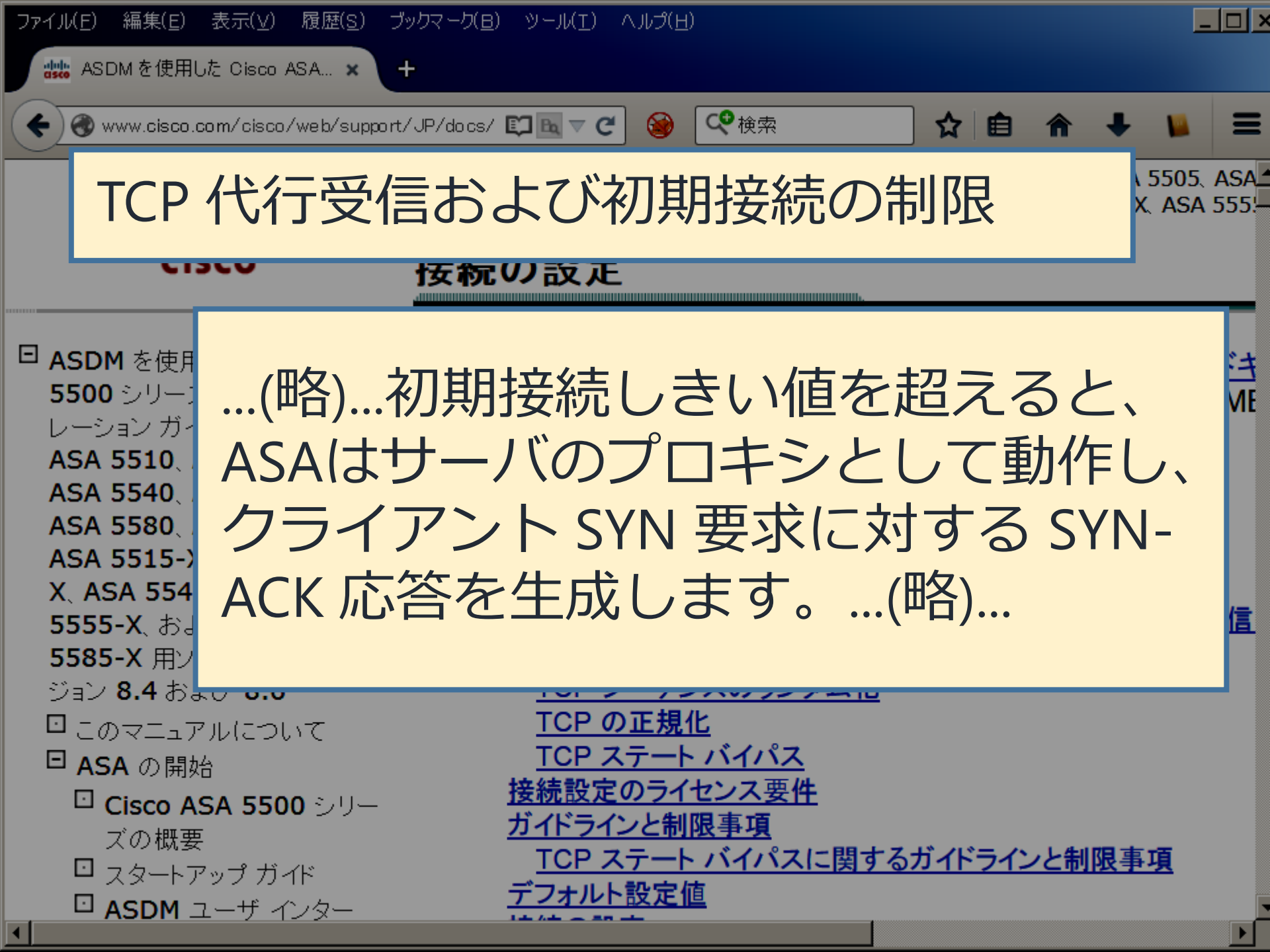
[TCP ステート バイパス](#)

[接続設定のライセンス要件](#)

[ガイドラインと制限事項](#)

[TCP ステート バイパスに関するガイドラインと制限事項](#)

[デフォルト設定値](#)



TCP 代行受信および初期接続の制限

...(略)...初期接続しきい値を超えると、ASAはサーバのプロキシとして動作し、クライアント SYN 要求に対する SYN-ACK 応答を生成します。...(略)...

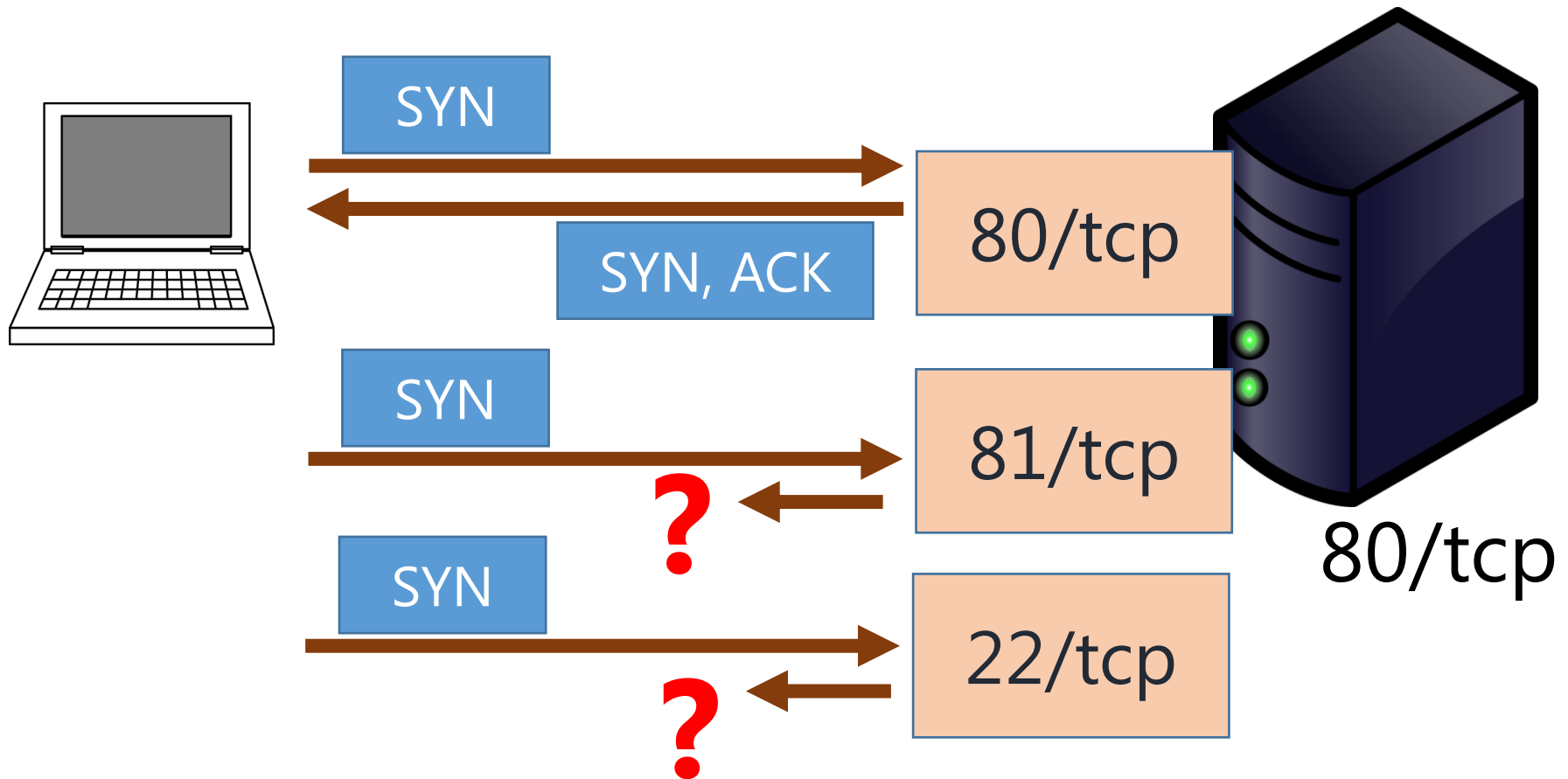
逆に全ポートfilteredに見せる

- iptablesのlimit, hashlimitモジュールを使うことで対策可能(説明省略)
- 参考) yasulib memo:
フルポートスキャンから開放ポートを隠す方法
 - <http://d.hatena.ne.jp/yasulib/20150302/1425282464>

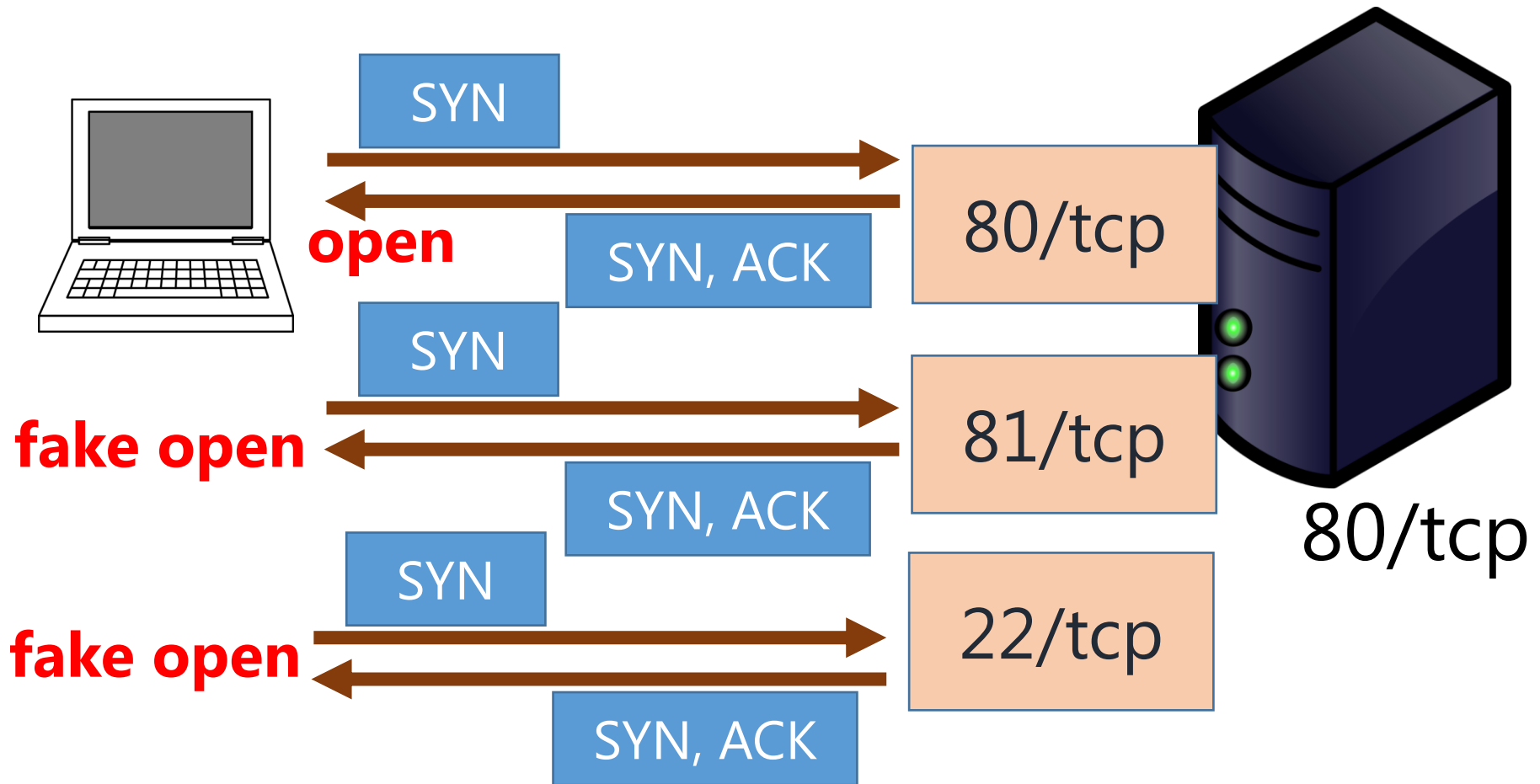
All ports open.



only http(80/tcp), but...



Every SYN packet is welcome.





Advertisement

三宅英明, 大角祐介「新しいLinuxの教科書」 SBクリエイティブ

<http://www.amazon.co.jp/dp/4797380942/>

amazon.co.jp
プライム

本 ▾



アドビ製品 サマーセール 8/28まで

カテゴリー ▾

Amazonポイント: 残高を確認

マイストア

ギフト券

タイムセール

Amazonで出品

こんにちは。サインイン
アカウントサービス ▾

今すぐ登録
プライム ▾

0 カート

本 詳細検索 ジャンル一覧 新刊・予約 Amazonランキング コミック・ラノベ 雑誌 文庫・新書 Amazon Student 本のお買い得情報 本買取

本 > コンピュータ・IT > OS

新しいLinuxの教科書 大型本 - 2015/6/6

大角 祐介 (著)

★★★★★ ▾ 1 件のカスタマーレビュー

すべての フォーマットおよびエディションを表示する

大型本

¥ 2,916

¥ 2,400 より 3 中古品の出品

¥ 2,916 より 1 新品

住所からお届け予定日を確認

562-0001 - 大阪府箕面市箕面 ▾

詳細

8/21 金曜日 にお届けするには、今から**18 時間 53 分**以内に
「お急ぎ便」または「当日お急ぎ便」を選択して注文を確定して
ください (有料オプション。Amazonプライム会員は無料)



この画像を表示

Would you like to see this page in English? [Click here.](#)

シェアする    

¥ 2,916

ポイント: 88pt (3%)

[詳細はこちら](#)

通常配送無料 [詳細](#)

在庫あり。在庫状況について
この商品は、Amazon.co.jp が販売
発送します。
ギフトラッピングを利用できます。

数量: 1 ▾

☐ お急ぎ便無料でカートに入れ
[Amazonプライム無料体験につ](#)
[て](#)

amazonstudent [Amazon Student](#)会員なら、この商品は +10% Amazon