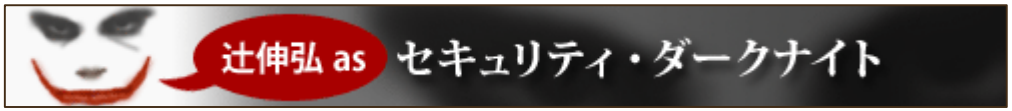
パスワードの破られ方入門

NTTデータ先端技術株式会社
辻 伸弘

自己紹介

自己紹介



おだいもく

0x01. 攻撃方法いろいろ
0x02. ツールあれこれ
0x03. 流行としては...
0x04. さいごに

0x01. 攻撃方法いろいろ

0x01. 攻撃方法いろいろ

主な攻撃手法

- ブルートフォース攻撃
- 辞書攻撃
- リバース攻撃
- リスト型攻撃

0x01. 攻撃方法いろいろ

ブルートフォース攻撃

brute force = 強引な

0000, 0001, 0002 ...

aaaa, bbbb, cccc ...

0x01. 攻撃方法いろいろ

辞書攻撃

よく使われる文字列を使用

123456, password, qwerty...

人名、サービス名、置き換えなど

0x01. 攻撃方法いろいろ

リバース攻撃

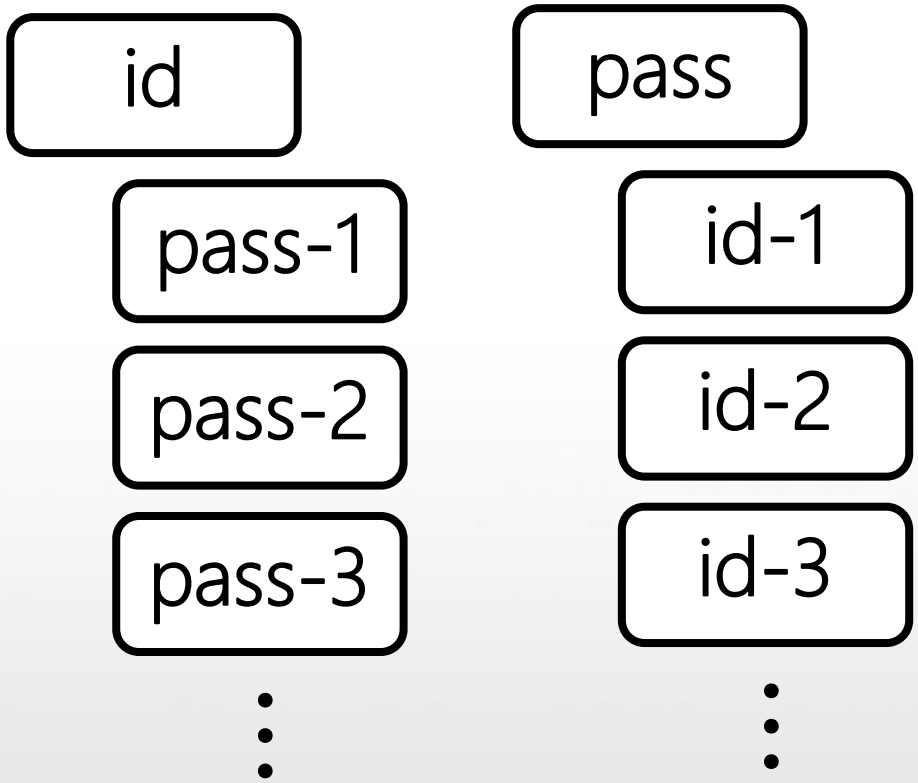
パスワードを固定

ユーザID変更という逆パターン

弱いパスワードのユーザを探す

0x01. 攻撃方法いろいろ

ノーマルとリバース



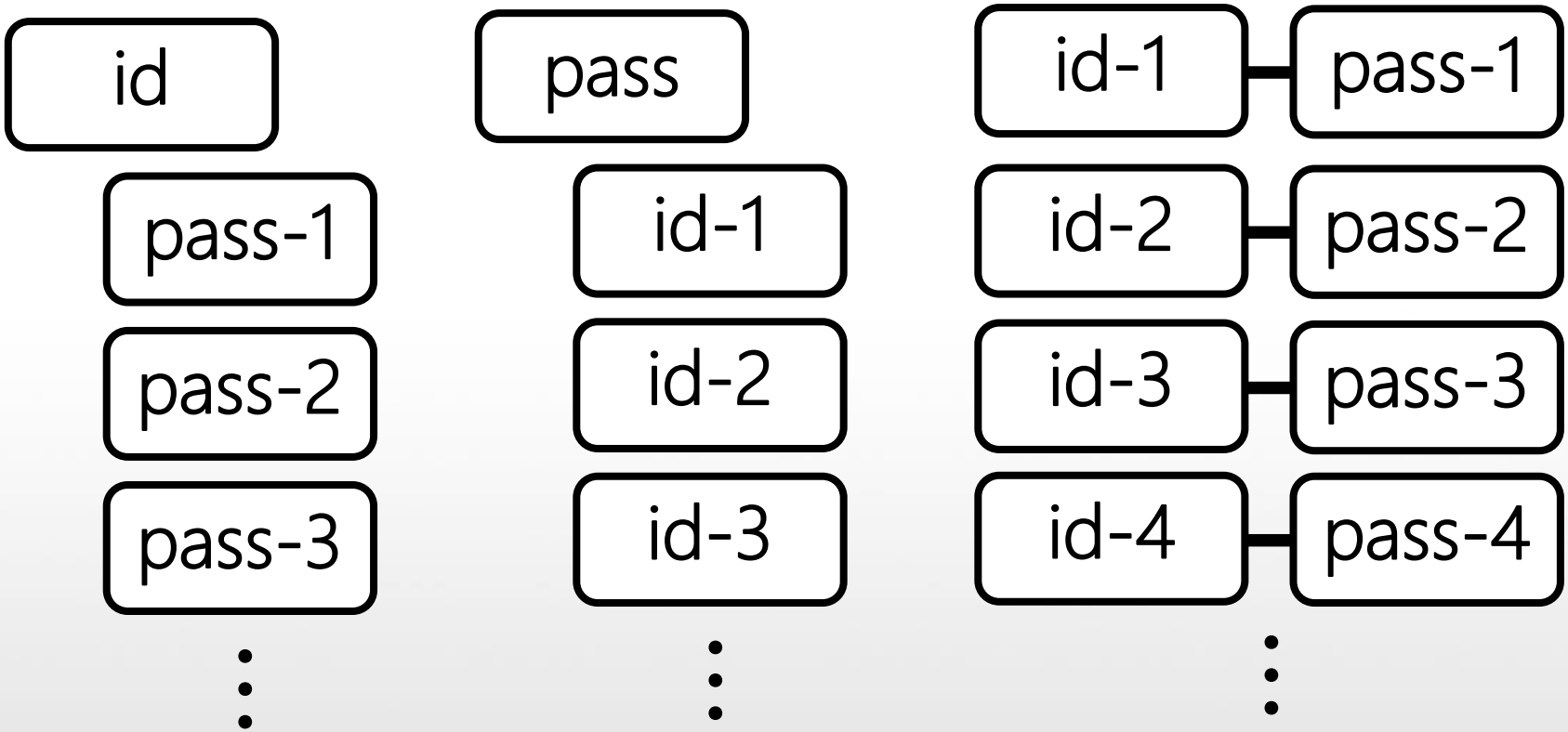
0x01. 攻撃方法いろいろ

リスト型攻撃

ユーザIDとパスワードが対のリスト

0x01. 攻撃方法いろいろ

ノーマルとリバースとリスト型



0x01. 攻撃方法いろいろ

リストはどうやって用意？

どこかから盗む or 買う

0x01. 攻撃方法いろいろ

リストはどうやって用意？

楽天ポイント盗み、電子マネーに＝不正アクセス容疑で中国人逮捕－岐阜県警

インターネット仮装商店街「楽天市場」に他人のIDとパスワードを使って不正アクセスし、商品を購入時のポイントを盗んで電子マネーに交換したなどとして、岐阜県警生活環境課などは8日、不正アクセス禁止法違反容疑などで、同県各務原市那加前洞新町の大学2年、孫路路容疑者（24）ら中国人2人を逮捕した。いずれも容疑を認めているという。

同課によると、2人は「チャットサイトで知り合った中国人から、5月中旬に他人のIDなどを6万5000円で買った。電子マネーは買い物に使った」などと供述。自宅パソコンにはそれぞれ約80万件のIDなどがあり、うち約2万5000件は楽天市場にログイン可能だった。

楽天市場は5～7月にポイントを電子マネー「楽天エディ」に交換できるキャンペーンを実施していた。同課は、全国約250人の約300万円分が被害に遭ったとみている。（2013/12/08-16:45）

0x02. ツールあれこれ

0x02. ツールあれこれ

セキュリティ診断の現場でも使う

0x02. ツールあれこれ

どんなことができるのか？

```
medusa
[-h host | -H file]
[-u username | -U file]
[-p password | -P file]
[-C file]
-M module [OPT]
```

0x02. ツールあれこれ

どんなことができるのか？

オプション名	説明
-h	攻撃対象アドレスを直接指定
-H <file>	攻撃対象が記述されたファイルを指定
-u	ユーザ名を直接指定
-U <file>	ユーザ名が記述されたファイルを指定
-p	パスワードを直接指定
-P <file>	パスワードが記述されたファイルを指定
-C <file>	ユーザ名/パスワードが記述されたファイルを指定
-M	攻撃するサービスを指定

0x02. ツールあれこれ

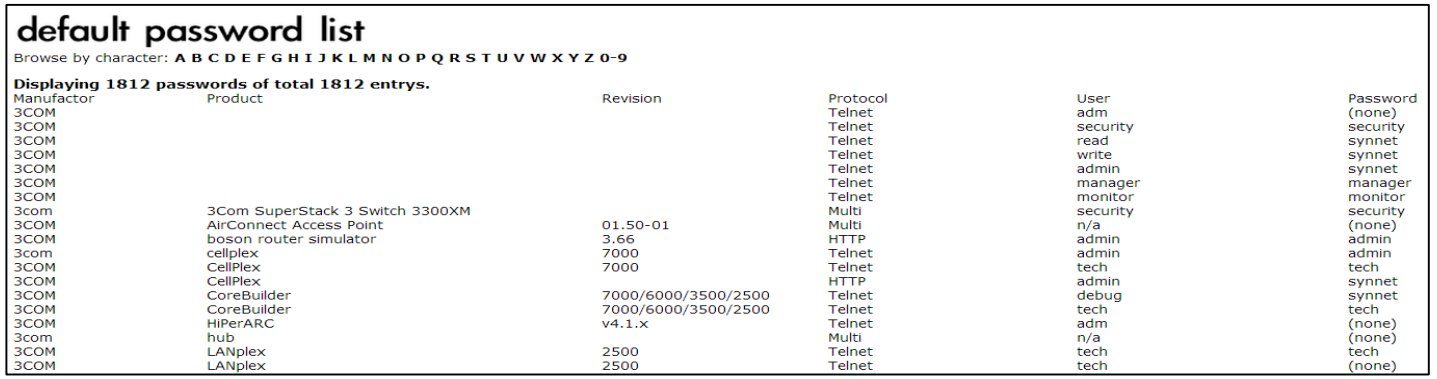
例えば

```
medusa ¥
 -h target-host
 -C ./list.txt
 -M web-form
 -m FORM:″login/login.php″
 -m DENY-SIGNAL:″ACCESS DENIED″
 -m FORM-DATA:″post?u=&p=&Login=Login″
```

```
:ockeghem:123456
:masanorik:123456789
:MasafumiNegishi:password
:ntsuji:adobe123
.
.
.
```

0x02. ツールあれこれ

その他にも…



default password list

Browse by character: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9

Displaying 1812 passwords of total 1812 entrys.

Manufactor	Product	Revision	Protocol	User	Password
3COM			Telnet	adm	(none)
3COM			Telnet	security	security
3COM			Telnet	read	synnet
3COM			Telnet	write	synnet
3COM			Telnet	admin	synnet
3COM			Telnet	manager	manager
3COM			Telnet	monitor	monitor
3com	3Com SuperStack 3 Switch 3300XM		Multi	security	security
3COM	AirConnect Access Point	01.50-01	Multi	n/a	(none)
3COM	boson router simulator	3.66	HTTP	admin	admin
3com	cellplex	7000	Telnet	admin	admin
3COM	CellPlex	7000	Telnet	tech	tech
3COM	CellPlex		HTTP	admin	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)
3com	hub		Multi	n/a	(none)
3COM	LANplex	2500	Telnet	tech	tech
3COM	LANplex	2500	Telnet	tech	(none)

CIRT.net suspicion breeds confidence

Home

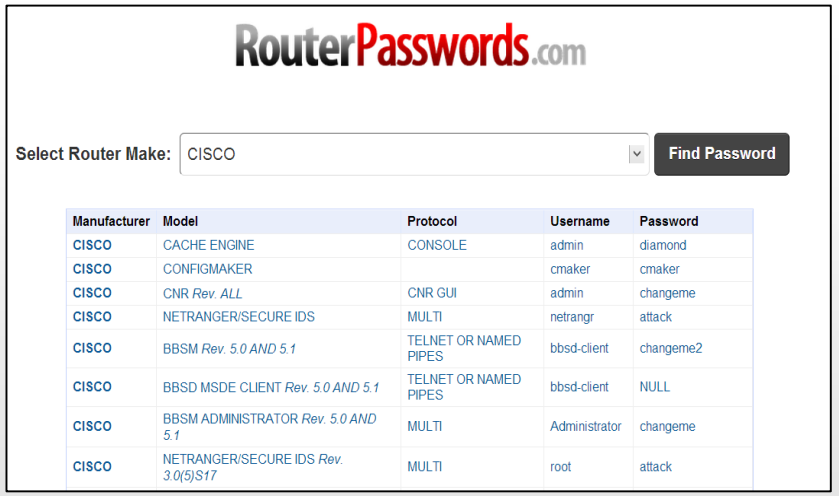
Default Passwords

@PASSDB RSS FIREFOX SEARCH

Search

481 vendors, 1974 passwords

2Wire, Inc.	360 Systems	3COM
3M	Accelerated Networks	ACCTON
Acer	Actiontec	Adaptec
ADC Kentrox	AdComplete.com	AddPac Technology
Adobe	ADT	Adtech
Adtran	Advanced Integration	AIRAYA Corp
Airlink	AirLink Plus	Aironet
Airway	Aladdin	Alcatel



RouterPasswords.com

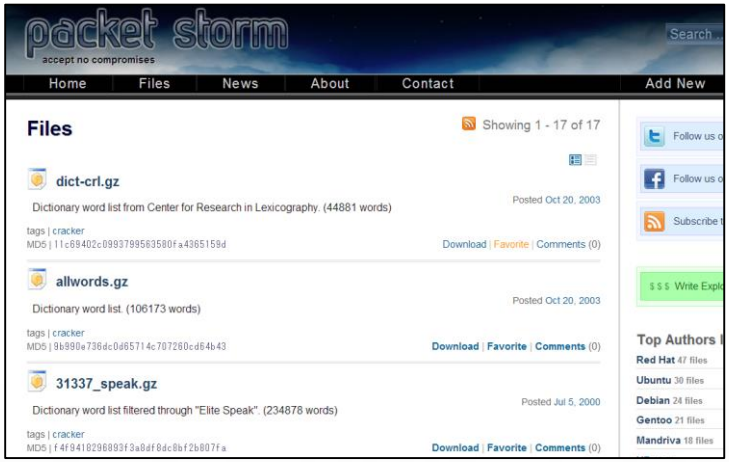
Select Router Make: CISCO Find Password

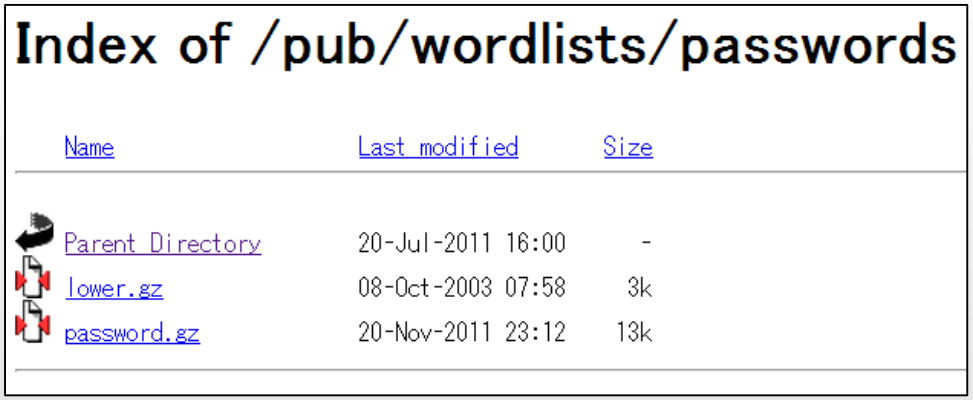
Manufacturer	Model	Protocol	Username	Password
CISCO	CACHE ENGINE	CONSOLE	admin	diamond
CISCO	CONFIGMAKER		cmaker	cmaker
CISCO	CNR *Rev. ALL*	CNR GUI	admin	changeme
CISCO	NETRANGER/SECURE IDS	MULTI	netrangr	attack
CISCO	BBSM *Rev. 5.0 AND 5.1*	TELNET OR NAMED PIPES	bbsd-client	changeme2
CISCO	BBSD MSDE CLIENT *Rev. 5.0 AND 5.1*	TELNET OR NAMED PIPES	bbsd-client	NULL
CISCO	BBSM ADMINISTRATOR *Rev. 5.0 AND 5.1*	MULTI	Administrator	changeme
CISCO	NETRANGER/SECURE IDS *Rev. 3.0(5)S17*	MULTI	root	attack

0x02. ツールあれこれ

ちなみに

1	123456
2	123456789
3	password
4	adobe123
5	12345678
6	qwerty
7	1234567
8	111111
9	photoshop
10	123123
11	1234567890
12	000000
13	abc123
14	1234
15	adobe1
16	macromedia
17	azerty
18	iloveyou





0x03. 流行としては…

0x03. 流行としては...

リスト型攻撃ではありますが

被害サイト	被害件数
Ameba	243,266 件
Goo ID	108,716 件
KONAMI ID	35,252 件
じゃらんnet	27,620 件
dinos	約 15,000件

0x03. 流行としては...

Adobeの漏えいでは

順位	パスワード	件数
1位	123456	191万1938 件
2位	123456789	44万6162 件
3位	password	34万5834 件
4位	adobe123	21万1659 件
5位	12345678	20万1580 件
6位	qwerty	13万832 件

0x03. 流行としては...

Adobeの漏えいでは

順位	パスワード	件数
1位	123456	191万1938 件
2位	123456789	44万6162 件
3位	password	34万5834 件
4位	adobe123	21万1659 件
5位	12345678	20万1580 件
6位	qwerty	13万832 件

0x03. 流行としては...

流行はあるものの

流行だけが危ないわけではない。

「木を見て、森を見ず」

になってはいけない。

0x03. 流行としては...

攻撃側はとっても有利。
その状況が継続している。

さいごに

さいごに

リスト型攻撃は

　使い回しをやめることで。

辞書攻撃は

　複雑なパスワード設定で。

さいごに

そのためには...

THANK YOU <3