vulsで踏み抜いた話

許　先明

Who am I ?

- @_seirios_ (Twitter)、SeonMeyong HEO(FaceBook)
- 太古の昔、ゲーマー
- いにしえのころ、X68000でTeXユーザー
- 大昔、ISPのネットワークエンジニア　　Interlink
- 昔々、コンサルタント　　IRI
- 昔、NetBSDを中心としたServer屋　　IRI
- ちょっと昔、運用屋さん　　ICO/IRI-Communications
- ついこの間まで、セキュリティ屋さん　　LAC
- 今、雲＋なんでもやさん　　BroadBand Tower

今日はあくまで個人の立場です
会社の見解とかそういうのとは関係ありません

本日のお題（２題）

- vuls on FreeBSDで踏み抜いた話（**まじ**）
- vuls on CentOSで踏み抜いた話（**誇張**）

前提

- **我が家**には、XenServer/NAS4Freeを利用した環境があります。
- VMが **30** 近く動いてます
- その中には、FreeBSD 10.0/11.0 CentOS 6/7があります
  - 自慢じゃないけどIPS/WAFも動いてます(on FreeBSD)

vuls on FreeBSD

- vulsはFreeBSDで動きます。
- root権限なんていらないもんね。
- pkgかんたんだもんね（棒）

vuls on FreeBSD

- vuls “-v” 動いてますか？
  - この間まで動いてなかった
- vulsrepo 便利だよね
  - でも、FreeBSDでちゃんと動いてますか？
  - この間まで、git pullしただけでは動かなかった

なんでversion出ないの？

- vulsは開発環境含めて、Linuxを前提にしている...
  - コマンドや設定ファイルの置き場所が違う！
  - Linuxの make はGNU make/ BSDのmakeはmake
- version文字列は、Makefile中に記載されているscriptで埋め込んでいる
  - BSD makeではこの部分が動かない→GNU拡張!
  - でも、Binary作るだけなら作れちゃうんだよorz...
- どうしたか
  - @kotakanbe にお願いして、MakefileをGNUmakefileにしてもらった
  - BSDな人は、pkg install gmakeして、gmake installしましょうね。

なんでvulsrepoが動かないの？

- FreeBSDのperlは、システムには入ってない
  - pkgで投入するしかない
  - 投入先は /usr/local/bin/perl
  - でも、vulsrepoは #! /bin/perl .... orz
- @usi360さんにお願いして、#! /bin/env perlしてもらった
  - envコマンドが、FreeBSDとLinuxで違う！
  - 入れたかったオプション(**-S -P**)は LinuxのEnvにはなかった。FreeBSD拡張
  - /etc/rc.confで設定してもPATHに/usr/local/binがない...
- どうしたか
  - /etc/rc.localからfcgiwrapを起動する (古臭い...)
    - いや、俺、Apache嫌いなんだよ。NGINXなんだよ。

不真面目なTips

- NGINXでvulsrepo動かすなら
  - いいからfcgiwrap使え！
- どこでも動かせる実装はこれだ！（ないわー）

```
1:  #! /bin/sh
2:  eval '(exit $?0)' && \
3:  eval 'PERL_BADLANG=x; PATH="$PATH:/usr/local/bin:."; export PERL_BADLANG; \
4:  exec perl -x -S -- "$0" ${1+"$@"};#' if 0; \
5:  eval 'setenv PERL_BADLANG x; setenv PATH "$PATH:/usr/local/bin:."; \
6:  exec perl -x -S -- "$0" $argv:q;#'.q
7:  #!perl -w
8:  +push@INC,'.';$0=~/(.*)/s;do(index($1,"/")<0?"./$1":$1); die$@if$@__END__+if 0
9:  ;#Don't touch/remove lines 1--8:
```

結論 -その１-

- だから、GNU拡張は(ry
- だから、BSD拡張は(ry
- だから、Linuxは(ry
- だから、POSIX...（まじ？）

vuls on CentOS

- というわけで、FreeBSDでのvuls環境は整ったんだよ。
  - 定常的に監視できるんだよ。
  - CentOSだろうがFreeBSDだろうが、CVE情報が取れるんだよ 💕

Heatmap | Count | CVSS Severity | CVSS Score

CveID / CweID / ServerName / Platform / Container / Summary / CVSS (AV) / CVSS (AC) / CVSS (Au) / CVSS (C) / CVSS (I) / CVSS (A)

ScanTime / Family / Release / Packages

				CVSS Severity	healthy	Low			Medium			Totals
ScanTime	Family	Release	Packages	CVSS Score	healthy	1	1.5	3.5	4	4.9	5	
2017-03-21T14:00:22+09:00	centos	7.3.1611	healthy		2							2
	FreeBSD	11.0-RELEASE-p2	healthy		3							3
			mariadb101-client								2	2
		11.0-RELEASE-p8	healthy		16							16
			mariadb101-client								6	6
			mariadb101-server			3	6	21	21	3		54
2017-03-22T14:00:19+09:00	centos	7.3.1611	healthy		2							2
	FreeBSD	11.0-RELEASE-p2	healthy		3							3
			mariadb101-client								2	2
		11.0-RELEASE-p8	healthy		16							16
			mariadb101-client								6	6
			mariadb101-server			3	6	21	21	3		54
2017-03-24T14:00:21+09:00	centos	7.3.1611	healthy		2							2
	FreeBSD	11.0-RELEASE-p2	healthy		5							5
		11.0-RELEASE-p8	healthy		22							22
Totals					71	6	12	42	42	6	16	195

vuls on CentOS

- あれれ？、CentOSのscanでエラーが出てるぞ？
- 単に繋げてないっぽい
- でも、手元のOS-Xからはvulsでscanできる...
- なぜじゃ？

vuls on CentOS

- slack の出番だ

seirios Feb 14 ☆

ちょっと誰か知っている人がいたら助けてください。

1. Target

vuls target machine: CentOS release 5.11

sshd version: OpenSSH_4.3p2, OpenSSL 0.9.8e-fips-rhel5 01 Jul 2008

2. Scanner

FreeBSD 11.0-RELEASE-p7

ssh version: OpenSSH_7.2p2, OpenSSL 1.0.2j-freebsd 26 Sep 2016

上記環境で、

I) scanner から ssh monitor@target すると、問題なく、パスワードもなしでloginできる

II) しかし、vulsからアクセスすると、エラーが出る。

config.toml

```
[servers.target]
host    = "xxx.xxx.xxx.xxx"
user        = "monitor"
```

Error Messages

```
time="Feb 14 16:26:24" level=info msg="Detecting OS of servers... "
time="Feb 14 16:26:24" level=debug msg="Failed to Dial to vul01, err:
ssh: handshake failed: ssh: unable to authenticate, attempted methods
[none publickey], no supported methods remain, Retrying in
552.330144ms..."
```

さて、これ、何がおかしいんだろう？

ちなみに、別のtarget(for ex. CentOS7とかFreeBSD)は正常に動作する。

seirios Feb 14

えっと、ものすごい怪しい挙動なので、もう少し詳細に。

a2 Feb 14

ユーザはmonitorで、sshは問題ないけど、vuls経由だとNGなのですよね

seirios Feb 14

1. ScannerのConsoleから作業した場合

1.1 ssh monitor@target して loginできる。

1.2 vuls scan して失敗

2. Mac から ssh でscannerにloginして、そこから作業した場合

2.1 ssh monitor@target して login できる。

2.2 vuls scan して成功

seirios Feb 14

@a2 ですです。

seirios Feb 14

あ、もしかして...ちょっと確認してきます。もしかしたら...

seirios Feb 14

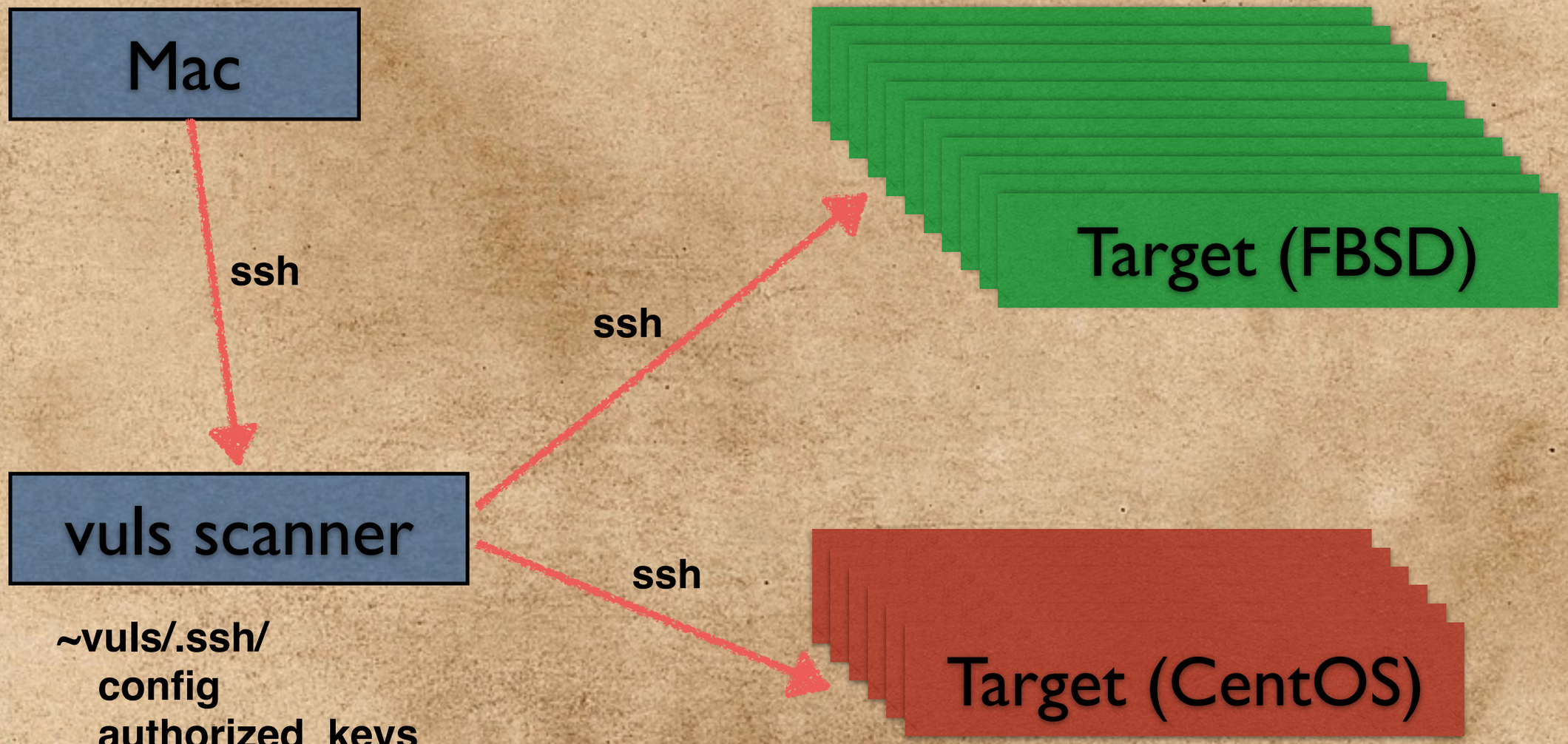
おおう、id_ed25519か、authorized_keysが壊れているのかも... (edited)

seirios Feb 14

違いますね。でも、1.1 が失敗しているので、sshdの設定の気がしてきた。

ええええ、全然わかんねー

通信経路はこう



結局何よ?

- Mac -> vuls scannerは「当然」sshで接続
- vuls scanner -> targetは「当然」sshで接続

- FreeBSDのopensshは OpenSSH 7.2
- CentOS6のopensshは OpenSSH 5.3

あ!

自分の環境

- よく考えたら、
  - vuls scannerには、ed25519の鍵しかない
  - Macは、RSA鍵とed25519鍵がある
  - Macは ssh-agentが動いている...
  - CentOSのOpenSSHは...

ed25519は

OpenSSH6.5

から利用できるようになった

結論 - その2 -

- sshのような基本ソフトウェアはさっさと更新しろ
- 脆弱な設定は使うな。できるだけ安全な新しいテクノロジを使え

とかやると、こんな罠にはまるんだよ

- だからCentOSは(ry
- これだからRHEは(ry