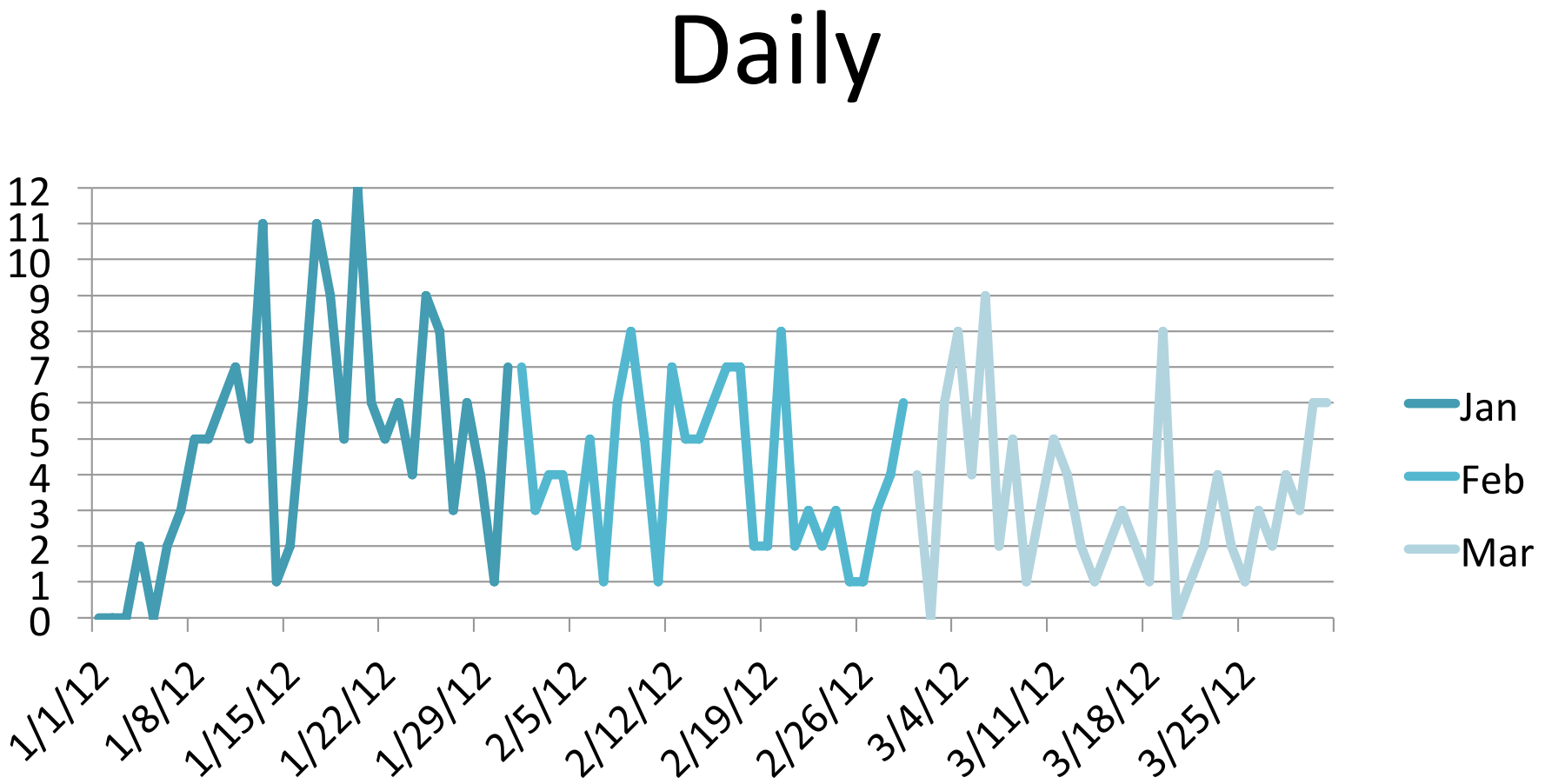
DDoS: practical survival guide

Alexander Lyamin
<la@highloadlab.com>

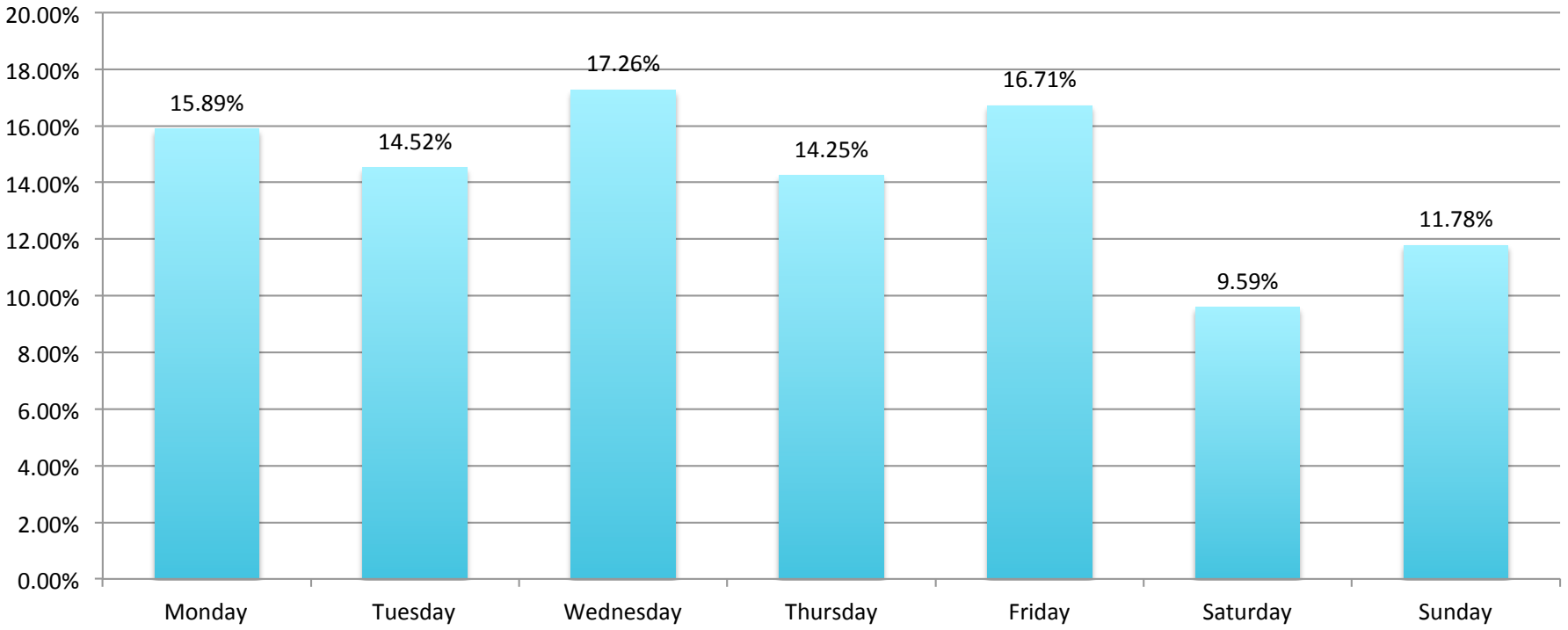
Poor mans version.
(low rate http attacks)

Q1 2012

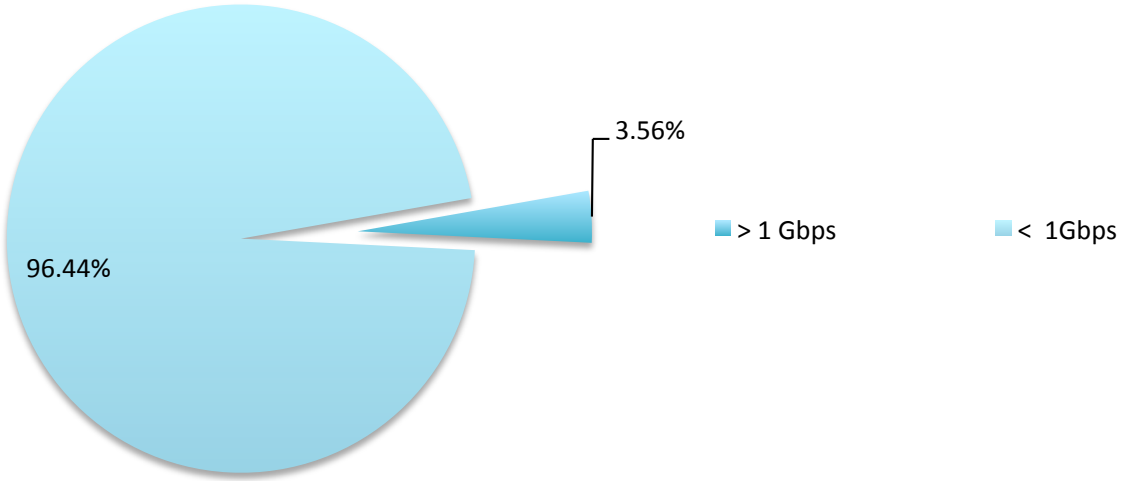
- Incidents: 365
- Daily max: 12
- Avg. botnet size: 2637
- Max botnet size: 37834


Daily
12
11
10
9
8
7
6
5
4
3
2
1
0
1/1/12
1/8/12
1/15/12
1/22/12
1/29/12
2/5/12
2/12/12
2/19/12
2/26/12
3/4/12
3/11/12
3/18/12
3/25/12
Jan
Feb
Mar

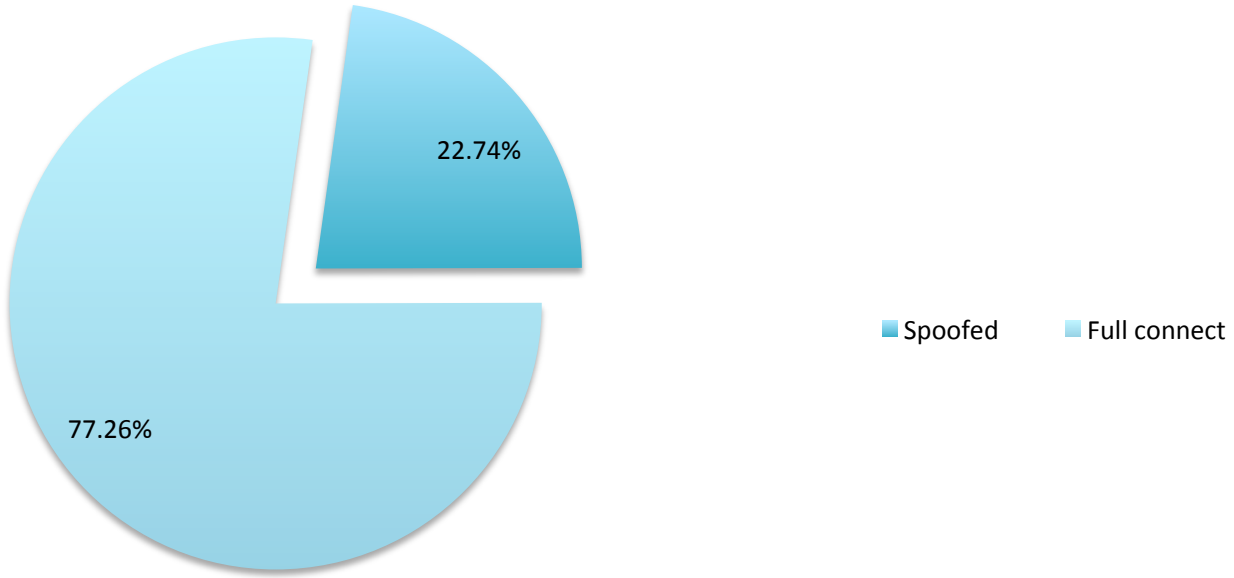
Weekday distribution



High speed attacks



Spoofed source attacks



Scary stuff

- DNS: NIC, Masterhost, FastVPS.
- DataCenters: CROK, WAhome.
- “Invisible” russsian elections botnets.
- Minerbot.

New reality

- 1k botnet - 100-160 USD.
- Readily available botnet toolkits.
- Fall of prices - 20 USD/day.

New competition

Apache mod_evasive

THOMAS MCCALL AND HIS BICYCLE.
(*From a Photograph by Bruce and Howie, of Kilmarnock.*)

Apache mod_evasive

<IfModule mod_evasive20.c>
DOSHashTableSize 3097
DOSPageCount 8
DOSSiteCount 100
DOSPageInterval 2
DOSSiteInterval 2
DOSBlockingPeriod 600
DOSEmailNotify secure@adminmail.com
</IfModule>

Apache mod_evasive

Positive	Negative
It works!	Apache

Iptables --string

Iptables --string

iptables -A INPUT -p tcp -m tcp --dport 80 -m string --string "GET / HTTP" --algo kmp --to 1024 -m recent --set --name httpddos --rsource

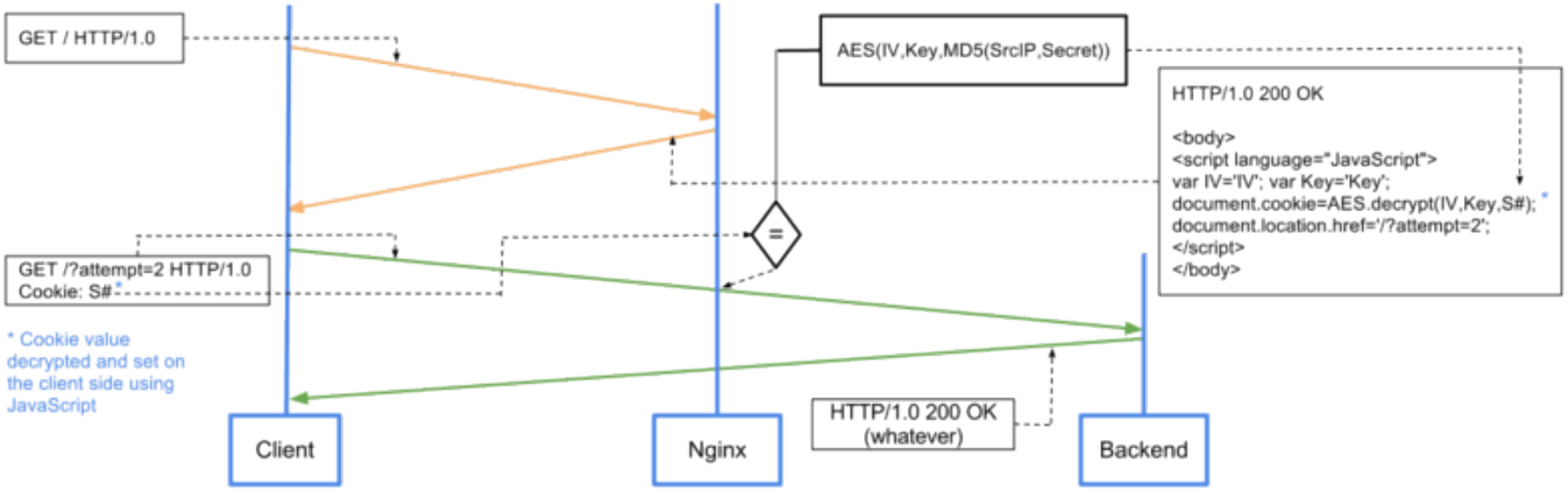
iptables -A INPUT -p tcp -m tcp --dport 80 -m string --string "GET / HTTP" --algo kmp --to 1024 -m recent --update --seconds 10 --hitcount 2 --name httpddos --rsource -j DROP

Iptables --string

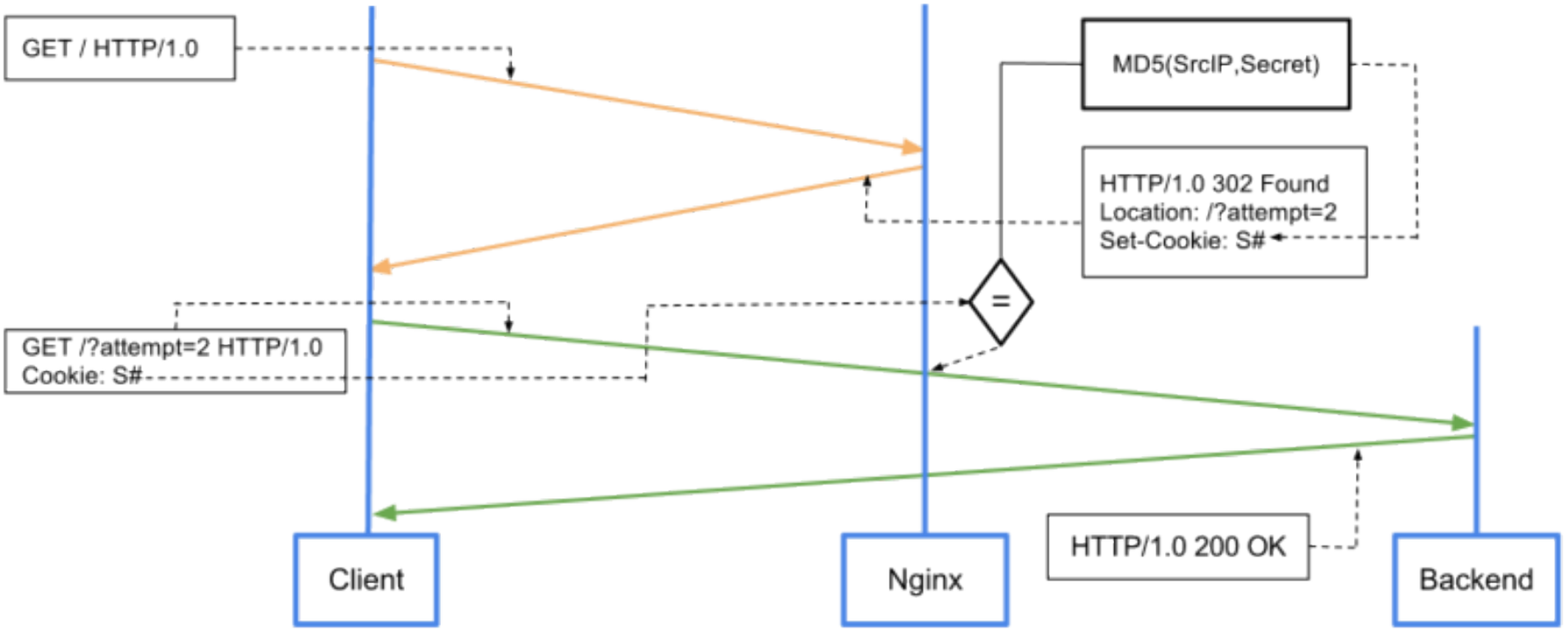
Positive	Negative
It works.	Not always works. (fragmentet packets)
Its fast.	Not always fast. (kmp matched packets)
	Orphaned sockets + retransmit.
	Requires conntrack(statefull is bad).

NGINX testcookie_module

JS


GET / HTTP/1.0
AES(IV,Key,MD5(SrcIP,Secret))
HTTP/1.0 200 OK
<body>
<script language="JavaScript">
var IV='IV'; var Key='Key';
document.cookie=AES.decrypt(IV,Key,S#); *
document.location.href='/?attempt=2';
</script>
</body>
=
GET /?attempt=2 HTTP/1.0
Cookie: S# *
* Cookie value decrypted and set on the client side using JavaScript
HTTP/1.0 200 OK
(whatever)
Client
Nginx
Backend

Cookie/Redirect



NGINX testcookie_module

```
    testcookie_name BPC;
    testcookie_secret keepmescret;
    testcookie_session $remote_addr;
    testcookie_arg attempt;
    testcookie_max_attempts 3;
    testcookie_fallback /cookies.html?backurl=http://$host$request_uri;
    testcookie_get_only on;
location / {
     testcookie on;
     proxy_set_header Host $host;
     proxy_set_header X-Real-IP $remote_addr;
     proxy_pass http://127.0.0.1:8080;
 }
```

More reading: http://habrahabr.ru/post/139931/

NGINX testcookie_module

Positive	Negative
It works. NGINX. Its fast. Predictable. Expandable (Flash, QT checks).	Doesn’t block traffic.* Alternates UX. Is not effective on FBS. * That’s what ipset is for.

Neuron network PyBrain

Neuron network PyBrain

Request:

0.0.0.0 - - [20/Dec/2011:15:00:03 +0400] "GET /forum/rss.php?topic=347425 HTTP/1.0" 200 1685 "-" "Mozilla/5.0 (Windows; U; Windows NT 5.1; pl; rv:1.9) Gecko/2008052906 Firefox/3.0»

Dictionary:

['__UA___OS_U', '__UA_EMPTY', '__REQ___METHOD_POST', '__REQ___HTTP_VER_HTTP/1.0', '__REQ___URL___NETLOC_', '__REQ___URL___PATH_/forum/rss.php', '__REQ___URL___PATH_/forum/index.php', '__REQ___URL___SCHEME_', '__REQ___HTTP_VER_HTTP/1.1', '__UA___VER_Firefox/3.0', '__REFER___NETLOC_www.mozilla-europe.org', '__UA___OS_Windows', '__UA___BASE_Mozilla/5.0', '__CODE_503', '__UA___OS_pl', '__REFER___PATH_/', '__REFER___SCHEME_http', '__NO_REFER__', '__REQ___METHOD_GET', '__UA___OS_Windows NT 5.1', '__UA___OS_rv:1.9', '__REQ___URL___QS_topic', '__UA___VER_Gecko/2008052906’

Далее: http://habrahabr.ru/post/136237/

Neuron network PyBrain

Positive	Negative
It works. Nerd award!	May not work. No historical analysis.

tcpdump

tcpdump

tcpdump -v -n -w attack.log dst port 80 -c 250

tcpdump -nr attack.log |awk '{print $3}' |grep -oE '[0-9]{1,}\.[0-9]{1,}\.[0-9]{1,}\.[0-9]{1,}' |sort |uniq -c |sort -rn

tcpdump

Positive	Negative
It works.	why tcpdump? Ask kernel!

Results?

- Every solution works.
- Not always.
- Not for everyone.
- UPTIME > DOWNTIME.

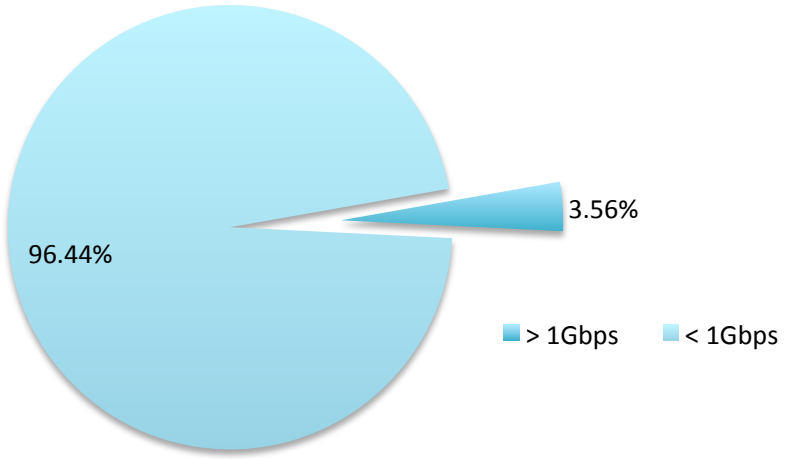
Definition of happiness

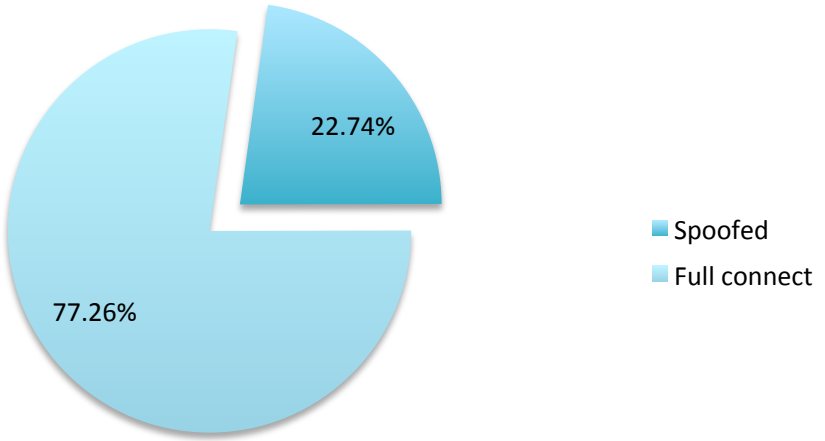
- Minimal FALSE POSITIVES.
- No vulnerabilities on lower levels.
- Up to challenge.

NGINX testcookie_module

One last thing…

(protect your TCP stack)





Have a fun ride!

Homework.

1. NGINX/ipset preinstalled.
2. No stateful firewalls.
3. Dedicated IP per critical published service.
4. Blackhole communities present and tested.