

Hackerbremse: Fail2ban



Dr. Dirk Wetter, 12.12.2024

Motivation

- Klassiker
- Vorinstalliert, Default „suboptimal“
- Schattendasein, kann viel mehr
- Quick-wins, aber: Shoot in foot

about:me

- Open Source
 - OWASP: Stammtisch Hamburg, Konferenzen, Projekte
 - testssl.sh
 - Early days: 2006 Koautor Linux-Buch, vieles bei heise.de
- Brotwerb: Selbständig Infosec >14 Jahren
 - Technik: Pentests (Webapps, Netze, Systeme)
 - Beratung & Informationsecuritymanagement

Agenda

- Funktionsprinzip
- Konfiguration 101: wo finde ich was?
 - Beispiele zur Verdeutlichung
- Webserver-Verteidigung:
 - Scanner, Bots
 - Login, Formulare, Admin-Logins
 - GET-Requests! Und was ist mit POST??
 - Auswertung
 - Je nach Zeit: Demo

Funktionsprinzip

- Python-Service
 - Analysiert Logdateien → Posthum
 - Pattern Matching
 - Basierend darauf: Aktionen
 - Standard: iptables (nftables, firewall-cmd, pf, ip route)
 - Benachrichtigung: E-Mail, Slack, Matrix , irc/xmpp, \$whatever

Und meine Container?? 😞

- Plain Docker / docker-compose
 - Urs: `/var/lib/docker/containers/<id>/<datei>` JSON!
 - `podman --log-opt path=/var/log/container/file.json`
- Problem: JSON geht nicht wirklich: [fail2ban/#3526](#)
 - Docker: `/var/lib/docker/overlay2/<id>/diff/var/log/nginx/access.log`
 - Oder: volume mount in host

Und meine Container?? 😢

- K8s 🤷
- RAW tables?
- Networking API ([fail2ban/#3644](#))



Konfiguration 101

– /etc/fail2ban/

|__ fail2ban.conf

|__ fail2ban.local

Hauptverzeichnis

Haupt-Konfigurationsdatei (Distributor)

hier lokal, wenn nötig

Konfiguration 101 - Jails

- /etc/fail2ban/

| __ jail.conf
| __ jail.local

Jail-Konfigurationsdatei (Distributor)
hier lokal, meistens nötig

```
# YOU SHOULD NOT MODIFY THIS FILE.  
#  
# It will probably be overwritten or improved in a distribution update.  
#
```

/etc/fail2ban/jail.conf

```
# "bantime" is the number of seconds that a host is banned.  
bantime = 10m  
  
# A host is banned if it has generated "maxretry" during the last "findtime"  
# seconds.  
findtime = 10m  
  
# "maxretry" is the number of failures before a host get banned.  
maxretry = 5
```

/etc/fail2ban/jail.local (1)

```
:/etc/fail2ban 0# cat jail.local
```

```
[DEFAULT]
```

```
ignoreip = 127.0.0.1/8 81.169.████/32 81.169.████/32 198.245.████/32 2a01:238:4308:████/128
```

```
bantime.increment = true
```

```
bantime.rndtime = 360
```

```
bantime.factor = 1
```

```
bantime.formula = ban.Time * math.exp(float(ban.Count+1)*banFactor)/math.exp(1*banFactor)
```

```
:/etc/fail2ban 0#
```

Konfiguration 101

- /etc/fail2ban/

|__ action.d/

|__ filter.d/

|__ jail.d/

Was soll passieren?

Regex pattern für Logdatei

Hier deine Konfigurationen rein

Los gehts

- Klassiker SSH – vorkonfiguriert

```
/etc/fail2ban grep -A 10 '^[\sshd\]' jail.conf  
[sshd]
```

```
# To use more aggressive sshd modes set filter parameter "mode" in jail.local:  
# normal (default), ddos, extra or aggressive (combines all).  
# See "tests/files/logs/sshd" or "filter.d/sshd.conf" for usage example and details.  
#mode    = normal  
port     = ssh  
logpath = %(sshd_log)s  
backend  = %(sshd_backend)s
```

```
/etc/fail2ban cat jail.d/defaults-debian.conf  
[sshd]  
enabled = true  
/etc/fail2ban
```

Los gehts

- SSH mit speziellen Ansprüchen

```
/etc/fail2ban cat jail.d/sshd.conf
[sshd]
enabled = true
port      = 31337
filter    = sshd
logpath   = %(sshd_log)s
backend   = %(sshd_backend)s
findtime = 7200
bantime = 3700
action = iptables-log[name=sshd, port="31337", protocol=tcp, blocktype=DROP]
/etc/fail2ban
```

```
/etc/fail2ban grep -v '^#' filter.d/sshd.conf | sed '/^$/d'  
[INCLUDES]  
before = common.conf  
[DEFAULT]  
_daemon = sshd  
_pref = (?:(?:error|fatal): (?:PAM: )?)?  
_suff = (?: (?:port \d+|on \S+|\[preauth\])\{0,3\}\s*  
_on_port_opt = (?: (?:port \d+|on \S+)\{0,2\}  
_authng_user = (?: (?:invalid|authenticating) user <F-USER>\S+.*?</F-USER>)?  
_alg_match = (?:(?:\w+ (?!found\b)\{0,2\}\w+)  
_pam_auth = pam_[a-z]+  
[Definition]  
prefregex = ^<F-MLFID>%(_prefix_line)s</F-MLFID>%(_pref)s<F-CONTENT>.+</F-CONTENT>$  
cmnfailre = ^[A]uthentication(?:failure|error|failed) for <F-USER>.*</F-USER> from <HOST>( via \S+)?%(_suff)s$  
    ^User not known to the underlying authentication module for <F-USER>.*</F-USER> from <HOST>%(_suff)s$  
    <cmnfailre-failed-pub-<publickey>>  
    ^Failed <cmnfailre> for (?:cond_inv>invalid user )?<F-USER>(?:cond_user>\S+)|(?:cond_inv)(?:(! from ).)*?|[^:]+)</F-USER> from <HOST>%(_on_port_opt)s(?: ssh\d*)?(?:cond_user): |(?:(! from ).)*$)  
    ^<F-USER>ROOT</F-USER> LOGIN REFUSED FROM <HOST>  
    ^[iI](?:illegal|invalid) user <F-USER>.*?</F-USER> from <HOST>%(_suff)s$  
    ^User <F-USER>\S+.*?</F-USER> from <HOST> not allowed because not listed in AllowUsers%(_suff)s$  
    ^User <F-USER>\S+.*?</F-USER> from <HOST> not allowed because listed in DenyUsers%(_suff)s$  
    ^User <F-USER>\S+.*?</F-USER> from <HOST> not allowed because not in any group%(_suff)s$  
    ^refused connect from \S+ \(<HOST>\)  
    ^Received <F-MLFFORGET>disconnect</F-MLFFORGET> from <HOST>%(_on_port_opt)s:\s*3: .*: Auth fail%(_suff)s$  
    ^User <F-USER>\S+.*?</F-USER> from <HOST> not allowed because a group is listed in DenyGroups%(_suff)s$  
    ^User <F-USER>\S+.*?</F-USER> from <HOST> not allowed because none of user's groups are listed in AllowGroups%(_suff)s$  
    ^<F-NOFAIL>%(_pam_auth)s(\ssshd:auth\):\s+authentication failure;</F-NOFAIL>(?:\s+(?:logname|e?uid|tty)=\S*)\{0,4\}\s+ruser=<F-ALT_USER>\S*</F-ALT_USER>\s+rhost=<HOST>(?:\s+user=<F-USER>\S*</F-USER>)?(?:\s+)?%(_suff)s$  
    ^maximum authentication attempts exceeded for <F-USER>.*</F-USER> from <HOST>%(_on_port_opt)s(?: ssh\d*)?(?:\s+)?%(_suff)s$  
    ^User <F-USER>\S+.*?</F-USER> not allowed because account is locked%(_suff)s$  
    ^<F-MLFFORGET>Disconnecting</F-MLFFORGET>(?: from )?: (?:invalid|authenticating)) user <F-USER>\S+</F-USER> <HOST>%(_on_port_opt)s:\s*Change of username or service not allowed:\s*.*\[preauth\]\s*$  
    ^Disconnecting: Too many authentication failures(?: for <F-USER>\S+.*?</F-USER>)?(?:\s+)?%(_suff)s$  
    ^<F-NOFAIL>Received <F-MLFFORGET>disconnect</F-MLFFORGET></F-NOFAIL> from <HOST>%(_on_port_opt)s:\s*11:  
    <ndre-<mode>-other>  
    ^<F-MLFFORGET><F-MLFGAINED>Accepted \w+</F-MLFGAINED></F-MLFFORGET> for <F-USER>\S+</F-USER> from <HOST>(?:\s+)$  
  
cmnfailed-any = \S+  
cmnfailed-ignore = \b(?!publickey)\S+  
cmnfailed-invalid = <cmnfailed-ignore>  
cmnfailed-nofail = (?:<F-NOFAIL>publickey</F-NOFAIL>|\S+)  
cmnfailed = <cmnfailed-<publickey>>  
ndre-normal =  
ndre-normal-other = ^<F-NOFAIL><F-MLFFORGET>(Connection(?:closed|reset)|Disconnected)</F-MLFFORGET></F-NOFAIL> (?:by|from)%(_authng_user)s <HOST>(?:%(_suff)s|\s*)$  
ndre-ddos = ^Did not receive identification string from <HOST>  
    ^kex_exchange_identification:(?:read: )?:[Cc]lient sent invalid protocol identifier|[Cc]onnection(?:closed by remote host|reset by peer)  
    ^Bad protocol version identification '.*' from <HOST>  
    ^<F-NOFAIL>SSH: Server;Ltype:</F-NOFAIL> (?:Authname|Version|Kex);Remote: <HOST>-\d+[A-Z]\w+:  
    ^Read from socket failed: Connection <F-MLFFORGET>reset</F-MLFFORGET> by peer  
    ^banner exchange: Connection from <HOST><_on_port_opt>: invalid format  
ndre-ddos-other = ^<F-MLFFORGET>(Connection(?:closed|reset)|Disconnected)</F-MLFFORGET> (?:by|from)%(_authng_user)s <HOST>%(_on_port_opt)s+\[preauth\]\s*$  
    ^<F-NOFAIL><F-MLFFORGET>(Connection(?:closed|reset)|Disconnected)</F-MLFFORGET></F-NOFAIL> (?:by|from)%(_authng_user)s <HOST>(?:%(_on_port_opt)s|\s*)$  
ndre-extra = ^Received <F-MLFFORGET>disconnect</F-MLFFORGET> from <HOST>%(_on_port_opt)s:\s*14: No(?: supported)? authentication methods available  
    ^Unable to negotiate with <HOST>%(_on_port_opt)s: no matching <_alg_match> found.  
    ^Unable to negotiate a <_alg_match>  
    ^no matching <_alg_match> found:  
ndre-extra-other = ^<F-MLFFORGET>Disconnected</F-MLFFORGET>(?: from )?: (?:invalid|authenticating)) user <F-USER>\S+.*?</F-USER> <HOST>%(_on_port_opt)s \[preauth\]\s*$  
ndre-aggressive = %(ndre-ddos)  
    %(ndre-extra)s  
ndre-aggressive-other = %(ndre-ddos-other)s  
publickey = nofail  
cmnfailre-failed-pub-invalid = ^Failed publickey for invalid user <F-USER>(?:cond_user>\S+)|(?:(! from ).)*?</F-USER> from <HOST>%(_on_port_opt)s(?: ssh\d*)?(?:cond_user): |(?:(! from ).)*$)  
cmnfailre-failed-pub-any =  
cmnfailre-failed-pub-nofail = <cmnfailre-failed-pub-invalid>  
cmnfailre-failed-pub-ignore =  
cfooterre = ^<F-NOFAIL>Connection from</F-NOFAIL> <HOST>  
failregex = %(cmnfailre)s  
    <ndre-<mode>>  
    %(cfooterre)s  
node = normal  
ignoreregex =  
maxlines = 1  
journalmatch = _SYSTEMD_UNIT=sshd.service + _COMM=sshd  
/etc/fail2ban
```

```
/etc/fail2ban grep -v '^#' filter.d/sshd.conf | sed '/^$/d' | wc -l  
69  
/etc/fail2ban
```

- SSH – Regexe sind vorkonfiguriert (puh)

cmnfailre =

```
^[aA]uthentication(?:failure|error|failed) for <F-USER>.*</F-USER> from <HOST>( via \S+)?%(__suff)s$  
^User not known to the underlying authentication module for <F-USER>.*</F-USER> from <HOST>%(__suff)s$  
<cmnfailre-failed-pub-<publickey>>  
^Failed <cmnfailed> for (?P<cond_inv>invalid user )?<F-USER>(?P<cond_user>\S+)|(?<cond_inv>(?:(?! from ).)*?|[:]*)</F-USER> from <HOST>%(__on_port_opt)s(?:: ssh\d*)?(<cond_us  
^<F-USER>ROOT</F-USER> LOGIN REFUSED FROM <HOST>  
^[(iI)](?:illegal|invalid) user <F-USER>.*?</F-USER> from <HOST>%(__suff)s$  
^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because not listed in AllowUsers%(__suff)s$  
^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because listed in DenyUsers%(__suff)s$  
^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because not in any group%(__suff)s$  
^refused connect from \S+ \(<HOST>\)  
^Received <F-MLFFORGET>disconnect</F-MLFFORGET> from <HOST>%(__on_port_opt)s:\s*3: .*: Auth fail%(__suff)s$  
^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because a group is listed in DenyGroups%(__suff)s$  
^User <F-USER>\S+|.*?</F-USER> from <HOST> not allowed because none of user's groups are listed in AllowGroups%(__suff)s$  
^<F-NOFAIL>%(__pam_auth)s\ssshd:auth\:\s+authentication failure;</F-NOFAIL>(?::\s+(?:logname|e?uid|tty)=\S*)\{0,4}\s+ruser=<F-ALT_USER>\S*</F-ALT_USER>\s+rhost=<HOST>(?:\s+  
^maximum authentication attempts exceeded for <F-USER>.*</F-USER> from <HOST>%(__on_port_opt)s(?:: ssh\d*)?%(__suff)s$
```

/etc/fail2ban/jail.local (2)

```
/etc/fail2ban cat jail.d/sshd.conf
```

```
[sshd]
enabled = true
port = 31337
filter = sshd
logpath = %(sshd_log)s
backend = %(sshd_backend)s
findtime = 7200
bantime = 3700
action = iptables-log
```

```
/etc/fail2ban
```

```
:/etc/fail2ban 0# cat jail.local
[DEFAULT]
ignoreip = 127.0.0.1/8 81.169.0.0/32 81.169.1.0/32 198.245.0.0/32 2a01:238:4308
bantime.increment = true
bantime.rndtime = 360
bantime.factor = 1
bantime.formula = ban.Time * math.exp(float(ban.Count+1)*banFactor)/math.exp(1*banFactor)
:/etc/fail2ban 0#
```

/etc/fail2ban/jail.local (2)

```
:/var/log 0# zgrep -h '193.32.162.80' fail2ban.log-2024*.gz fail2ban.log | grep '[postfix_unknown] Increase'  
2024-02-15 02:31:27,215 fail2ban.observer [1387]: NOTICE [postfix_unknown] Increase Ban 193.32.162.80 (2 # 2:48:44 -> 2024-02-15 05:20:11)  
2024-02-23 17:17:44,542 fail2ban.observer [1387]: NOTICE [postfix_unknown] Increase Ban 193.32.162.80 (2 # 2:45:25 -> 2024-02-23 20:03:09)  
2024-02-23 20:44:40,787 fail2ban.observer [1387]: NOTICE [postfix_unknown] Increase Ban 193.32.162.80 (3 # 7:24:59 -> 2024-02-24 04:09:39)  
2024-02-24 04:30:45,250 fail2ban.observer [1387]: NOTICE [postfix_unknown] Increase Ban 193.32.162.80 (4 # 20:10:11 -> 2024-02-25 00:40:55)  
2024-02-25 00:41:21,155 fail2ban.observer [1387]: NOTICE [postfix_unknown] Increase Ban 193.32.162.80 (5 # 2 days, 6:36:05 -> 2024-02-27 07:17:25)  
2024-02-27 11:36:54,159 fail2ban.observer [1387]: NOTICE [postfix_unknown] Increase Ban 193.32.162.80 (6 # 6 days, 4:26:14 -> 2024-03-04 16:03:07)  
2024-03-04 17:22:17,338 fail2ban.observer [1387]: NOTICE [postfix_unknown] Increase Ban 193.32.162.80 (7 # 16 days, 19:28:10 -> 2024-03-21 12:50:26)  
2024-04-01 12:09:37,347 fail2ban.observer [24933]: NOTICE [postfix_unknown] Increase Ban 193.32.162.80 (8 # 45 days, 16:38:58 -> 2024-05-17 04:48:34)  
2024-05-25 19:26:45,896 fail2ban.observer [1423]: NOTICE [postfix_unknown] Increase Ban 193.32.162.80 (9 # 124 days, 5:00:32 -> 2024-09-27 00:27:17)  
:/var/log 0#
```

/etc/fail2ban/jail.local (2)

https://www.abuseipdb.com/check/193.32.162.80

AbuseIPDB » 193.32.162.80

Check an IP Address, Domain Name, or Subnet
e.g. [\[REDACTED\]](#), [microsoft.com](#), or [5.188.10.0/24](#)

193.32.162.80 was found in our database!

This IP was reported 4,302 times. Confidence of Abuse is 100%:

100%

IP Abuse Reports for 193.32.162.80:

This IP address has been reported a total of 4,302 times from 224 distinct sources. 193.32.162.80 was first reported on February 7th 2024, and the most recent report was 1 day ago.

Recent Reports: We have received reports of abusive activity from this IP address within the last week. It is potentially still actively engaged in abusive activities.

Reporter	IoA Timestamp in UTC	Comment	Categories
✓  CRSSkynet	2024-06-07 11:24:05 (1 day ago)	Jun 7 11:55:16 hosting vpopmail[36225]: vchkpw-smtp: vpopmail user not found info@getonair.uk:193.3 ...	Brute-Force show more
✓  dwmp	2024-06-07 00:56:22 (1 day ago)	Jun 7 02:56:20 plesk postfix/smtpd[166294]: warning: u nknown[193.32.162.80]: SASL LOGIN authenticat ...	Brute-Force SSH show more
✓  swehosting.se	2024-06-07 00:32:08 (1 day ago)	(smtpauth) Failed SMTP AUTH login from 193.32.162.8 0 (NL/The Netherlands/-): 5 in the last 3600 secs ...	Port Scan show more

Web

- Vieles vorkonfiguriert
 - Einiges suboptimal. Einiges verwendbar.
 - Alles: Nicht scharf geschaltet
- Achtung: erstes Beispiel → reines Lehrbeispiel

Web

Auch vieles vorkonfiguriert. Leider einiges „suboptimal“

```
/etc/fail2ban/filter.d ➤ ll apache-*
-rw-r--r-- 1 root root 3.2K Nov  9  2022 apache-auth.conf
-rw-r--r-- 1 root root 2.8K Nov  9  2022 apache-badbots.conf
-rw-r--r-- 1 root root 1.3K Nov  9  2022 apache-botsearch.conf
-rw-r--r-- 1 root root 1.6K Nov  9  2022 apache-common.conf
-rw-r--r-- 1 root root  403 Nov  9  2022 apache-fakegooglebot.conf
-rw-r--r-- 1 root root  511 Nov  9  2022 apache-modsecurity.conf
-rw-r--r-- 1 root root  596 Nov  9  2022 apache-nohome.conf
-rw-r--r-- 1 root root 1.3K Nov  9  2022 apache-noscript.conf
-rw-r--r-- 1 root root 2.2K Nov  9  2022 apache-overflows.conf
-rw-r--r-- 1 root root  362 Nov  9  2022 apache-pass.conf
-rw-r--r-- 1 root root 1020 Nov  9  2022 apache-shellshock.conf
/etc/fail2ban/filter.d ➤ grep -ir 'nessus|nikto|nmap|ffuf|openvas' *
x ➤ /etc/fail2ban/filter.d
```

User-Agent Blocking

- a.k.a. Skript-Kid-Kondom
- User-Agents gehen gut am Webserver
 - (Zumindest solche, die nicht „hämmern“)
- Wer wirklich 5kr1p7k1d5 blocken will
 - Andere Methoden weit aus effektiver

„404-Methode“

- Idee:

1. Zähle 404s

2. Reißleine
nach Gusto

13.89	- - [03/Sep/2023:14:46:44 +0200] "GET //wp-2018.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:44 +0200] "GET //wp-2020.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:44 +0200] "GET //wp-2021.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:44 +0200] "GET //wp-2022.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:44 +0200] "GET //0z.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:44 +0200] "GET //lock360.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:44 +0200] "GET //wp-22.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:45 +0200] "GET //wp-2019.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:45 +0200] "GET //fw.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:45 +0200] "GET //2index.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:45 +0200] "GET //C.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:45 +0200] "GET //c.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:45 +0200] "GET //01.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:45 +0200] "GET //1.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:45 +0200] "GET //02.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:46 +0200] "GET //wp.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:46 +0200] "GET //404.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:46 +0200] "GET //403.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:46 +0200] "GET //admin.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:46 +0200] "GET //good.php HTTP/1.1" 404 514 "-" "Go-http-client/1.1" "-"
13.89	- - [03/Sep/2023:14:46:46 +0200] "GET //wp-content/themes/wp-pridmag/init.php HTTP/1.1" 404 514 "-" "Go-

404-Trick (unbedingt anzupassen)

```
[INCLUDES]
before = common.conf

[Definition]

# failregex = <HOST> - - .*HTTP/[0-2]+(.|[0-1]+)?"(404|403|301|302|308)*
failregex = <HOST> - - .*HTTP/[0-2]+(.|[0-1]+)?"(404|403)*

 ignoreregex = .*(robots\.txt|sitemap\.xml|favicon\.ico|\.\jpg|\.\png)
filter.d/apache-404.conf lines 1-10/10 (END)
```

404-Trick weiter: anzupassen

```
[apache-404]
enabled = true
port    = http,https
filter   = apache-404
logpath  = /var/log/httpd/*access.log
maxretry = 60
findtime = 1200
bantime = 1800
action = firewallcmd-multiport[name=apache-404, port="80,443", protocol=tcp, blocktype=DROP]
datepattern = %%d/%%b/%%Y:%%H:%%M:%%S %%z
```

jail.d/404.conf lines 1-12/12 (END)

In etwa

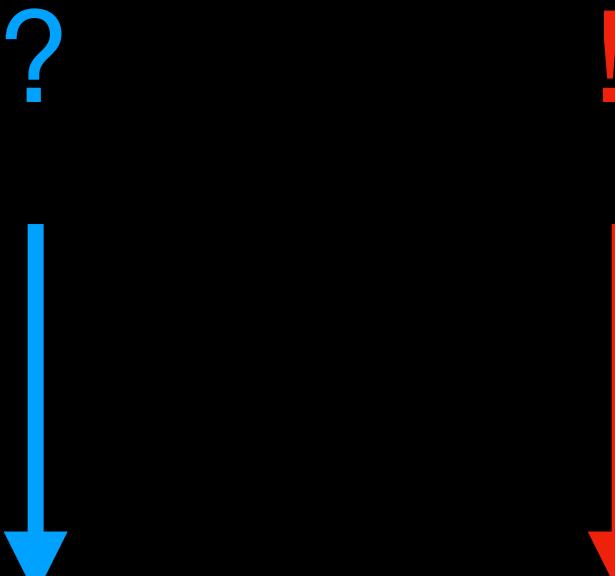
```
/etc/fail2ban/filter.d ➤ head -11 nginx-botsearch.conf
# Fail2Ban filter to match web requests for selected URLs that don't exist
#
[INCLUDES]

# Load regexes for filtering
before = botsearch-common.conf

[Definition]

failregex = ^<HOST> \- \S+ \[\] \"(GET|POST|HEAD) \/<>block> \S+\" 404 .+$

/etc/fail2ban/filter.d ➤
```



Referenzen

```
/etc/fail2ban/filter.d ➤ cat botsearch-common.conf
# Generic configuration file for -botsearch filters

[Init]

# Block is the actual non-found directories to block
block = \/(?(<webmail>|<phpmyadmin>|<wordpress>|cgi-bin|mysqladmin) [^,]*

# These are just convenient definitions that assist the blocking of stuff that
# isn't installed
webmail = roundcube|(ext)?mail|horde|(v-?)?webmail

phpmyadmin = (typo3/xampp/admin/)|(pma|(php)?[Mm]y[Aa]dmin)

wordpress = wp-(login|signup|admin)\.php
```

GET-Request, Web-Hacks

[INCLUDES]

[Definition]

```
failregex = ^<HOST> .* "(GET|POST|HEAD|PROPFIND) .*(?i)(union|select|concat|information_schema\.tables|unhex|benchmark|md5|sleep|order|%%20and%%20|%%20or%%20).* (404|403)
    ^<HOST> .* "(GET|POST|HEAD|PROPFIND) .*(?i)(fromCharCode|ONLOAD|alert|base64|innerHTML|onmouseover|x22|88,83,83|onerror|prompt).* (404|403)
    ^<HOST> .* "(GET|POST|HEAD|PROPFIND) .*(?i)(\.\.|%2e|etc\/passwd|etc\/shadow).* (404|403)
    ^<HOST> .* "(GET|POST|HEAD|PROPFIND) .*(?i)(urldecode|explode|\$_REQUEST|\$_GET).* (404|403)
```

Open Redirect

```
/etc/fail2ban tail -20 filter.d/php-url-fopen.conf
# Example of web requests in Apache access log:
# 66.185.212.172 - - [26/Mar/2009:08:44:20 -0500] "GET /index.php?n=http://eatmyfood.hostinginfive.com/pizza.htm? HTTP/1.1" 2
7)

[Definition]

failregex = ^<HOST> -.*"(GET|POST).*\?.*\=http\:\/\/.* HTTP\/.*$  

           ^<HOST> -.*"(GET|POST).*\?.*\=https\:\/\/.* HTTP\/.*$  

ignoreregex =  
  

# DEV Notes:  

#  

# Version 2  

# fixes the failregex so REFERERS that contain =http:// don't get blocked  

# (mentioned by "fasuto" (no real email provided... blog comment) in this entry:  

# http://blogs.buanzo.com.ar/2009/04/fail2ban-filter-for-php-injection-attacks.html#comment-1489  

#
```



POST-Request

- Nginx kann POST-Parameter loggen

```
~log_format postlogs '$remote_addr - $remote_user [$time_local] '
' "$request" $status $bytes_sent ' '"$http_referer"
"$http_user_agent" "$request_body"';
```

- Apache: mod_dumpio
 - LogLevel dumpio:trace7
 - DumpIOInput On
 - DumpIOOutput On

POST-Request

- Apache: mod_security

```
/etc/fail2ban ➤ head -15 filter.d/apache-modsecurity.conf
# Fail2Ban apache-modsec filter
#
[INCLUDES]

# Read common prefixes. If any customizations available -- read them from
# apache-common.local
before = apache-common.conf

[Definition]

failregex = ^%{_apache_error_client}s(?: \[client [^\]]+\])? ModSecurity:\s+(?:\[(?:\w+ \"[^"]*\"|[^"]+)\]\s*)*Access denied with code [45]\d\d
ignoreregex =
/etc/fail2ban ➤ |
```

POST-Request: ACHTUNG

- Passwörter u.a. !

```
[12/Jun/2024:13:55:16 +0200] "POST /login HTTP/2.0" 200 12 "-" "curl/8.4.0" "user=max,passwd=1234"  
[12/Jun/2024:13:55:30 +0200] "POST /login HTTP/2.0" 200 12 "-" "curl/8.4.0" "user=micheala,passwd=meinpwistvielbesseralsMax"  
[12/Jun/2024:13:56:41 +0200] "POST /login HTTP/2.0" 200 12 "-" "curl/8.4.0" "user=deinciso,passwd=Postlogs: Ganz schlechte Idee"
```

- Besser: mod_security + SecRule sanitiseArg

Logins schützen

The screenshot shows a web browser window with the URL confluence.atlassian.com/doc/using-fail2ban-to-limit-login-attempts. The page content displays two snippets of configuration files.

[apache-shorewall]

```
enabled = true
filter = cac-login
action = shorewall
logpath = /var/log/httpd/confluence-access.log
bantime = 600
maxretry = 3
findtime = 60
backend = polling
```

Configuring for Confluence

⚠️ The following is an example only, and you should adjust it for your site.

filter.d/confluence-login.conf

[Definition]

```
failregex = <HOST>. *"GET /login.action
ignoreregex =
```

Logins schützen

Confluence POST

[Definition]

```
failregex = <HOST> .* "POST /dologin.action
```

Logins

Mitgeliefert: gitlab, grafana

```
/etc/fail2ban/filter.d ➔ cat gitlab.conf  
# Fail2Ban filter for Gitlab  
# Detecting unauthorized access to the Gitlab Web portal  
# typically logged in /var/log/gitlab/gitlab-rails/application.log
```

[Definition]

```
failregex = ^: Failed Login: username=<F-USER>.+</F-USER> ip=<HOST>$
```

```
/etc/fail2ban/filter.d ➔
```

```
/etc/fail2ban ➔ grep -A 1 gitlab jail.conf  
[gitlab]  
port      = http,https  
logpath  = /var/log/gitlab/gitlab-rails/application.log
```

```
/etc/fail2ban ➔ |
```

Logins

Mitgeliefert: gitlab, grafana

```
/etc/fail2ban/filter.d ➔ cat grafana.conf
# Fail2Ban filter for Grafana
# Detecting unauthorized access
# Typically logged in /var/log/grafana/grafana.log
```

```
[Init]
datepattern = ^t=%Y-%m-%dT%H:%M:%S%Z
```

```
[Definition]
failregex = ^(?: lvl=err?or)? msg="Invalid username or password"(?: uname=(?:<F-ALT_USER>[^"]+</F-ALT_USER>"|<F-USER>\S+</F-USER>) |
error=<F-ERROR>[^"]+</F-ERROR>"| \S+=(?:\S*|[^\"]+"))* remote_addr=<ADDR>$
```

```
/etc/fail2ban/filter.d ➔ |
```

```
/etc/fail2ban ➔ grep -A 1 grafana jail.conf
[grafana]
port      = http,https
logpath  = /var/log/grafana/grafana.log

/etc/fail2ban ➔ |
```

Spamkondom

- Formularspammer

```
[apache-form-DoS]
enabled = true
port    = http,https
filter   = apache-form-DoS
logpath  = /var/log/httpd/*access.log
maxretry = 15
findtime = 7200
bantime = 3600
action   = firewallcmd-multiport[name=apache-form-DoS, port="80,443", protocol=tcp, blocktype=DROP]
datepattern = %%d/%%b/%%Y:%%H:%%M:%%S %%Z

fail2ban/jail.d/kontaktform_dos_protection.conf lines 1-11/11 (END)

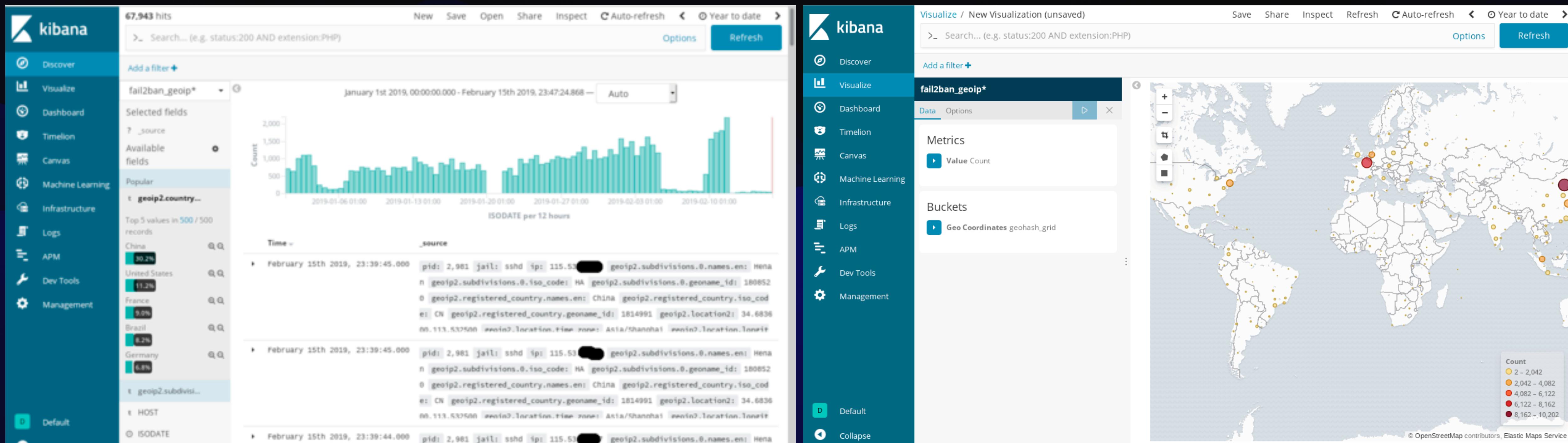
[INCLUDES]
before = common.conf

[Definition]
failregex = <HOST> - - .* "POST /kontakt.* HTTP/[0-2]+(.+[0-1]+)?" 200 *
           fail2ban/filter.d/apache-form-DoS.conf lines 1-7/7 (END)
```



Auswerten

- Grafisch, z.B. ELK



- <https://balagetech.com/visualizing-fail2ban-logs-in-kibana/> (Balázs Németh)

Auswerten

- CMD rules!
 - Demo time
 - Shell :-)
 - Muss nicht Shell sein
 - Siehe Netz

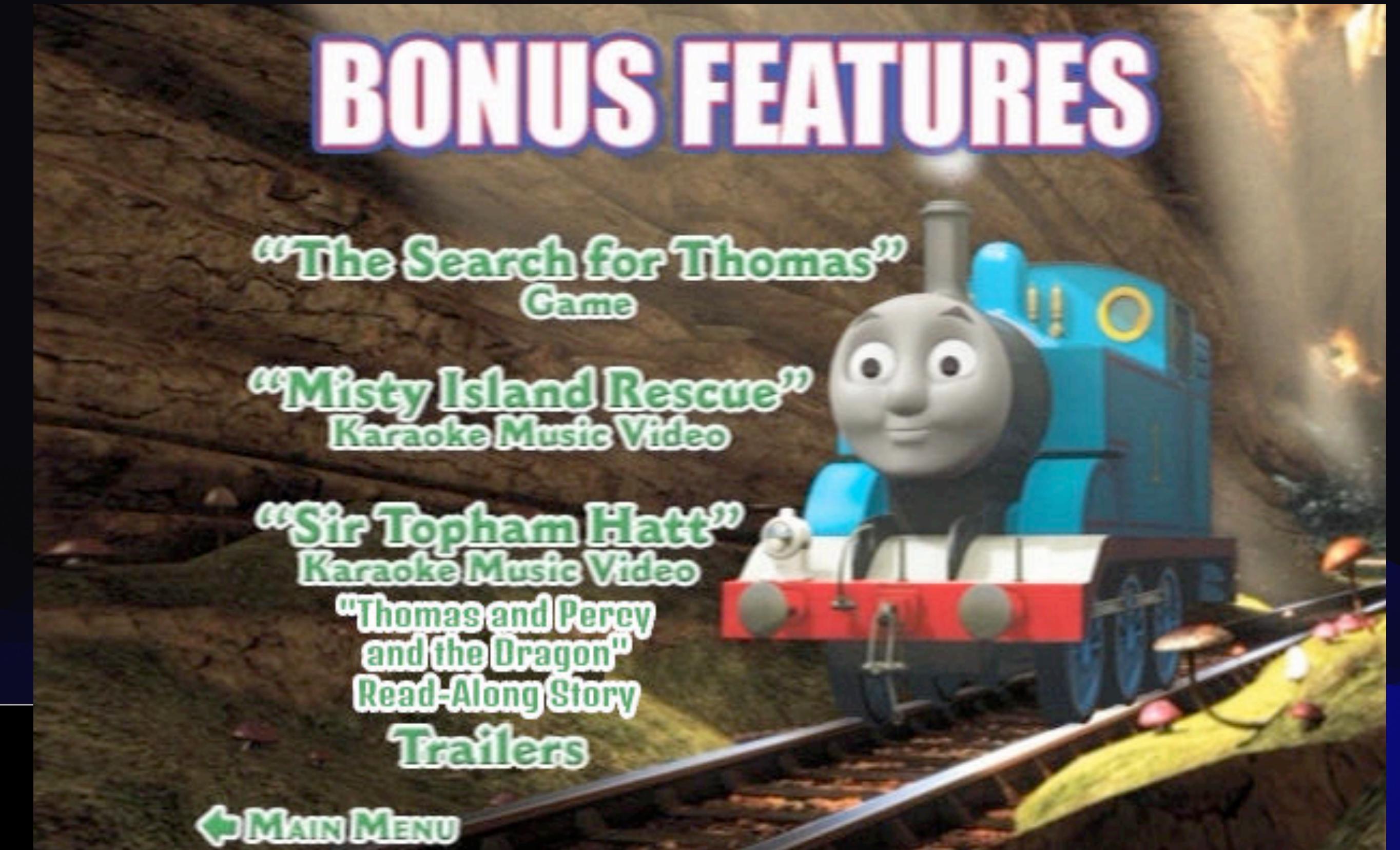
Bonus feature

- Booby trap

User-agent: *

Disallow: /comeontryme

robots.txt lines 1-4/4 (END)



Take aways (1)

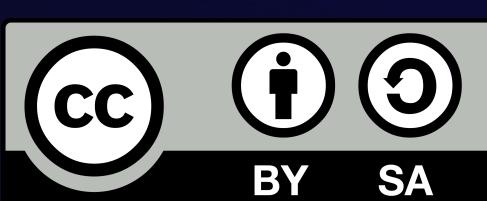
- fail2ban ist 😎
 - Aber: greift erst nach 1+ failed request(s)
- Nicht vergessen:
 - Fail2ban ist eine *reaktive* Maßnahme
 - **Macht Apps / Server besser *proaktiv* sicher!**

Take aways (2)

- Regex testen!
 - regex101.com
 - fail2ban-regex
- Webseite/Service auf Funktion testen
 - Klassiker: (AAA|BBB|CCC|DDD|)
 - Schwellwerte ok?

Danke



- Kontakt: dirk bei owasp punkt org, [linked.in](#) oder <https://drwetter.eu/>
- Folien sind CC-BY-SA 4.0  später auf Webseiten.